TREND MICRO

9.0 安全无忧软件

网络安全版和
邮件与网络安全版

Service Pack 3

管理员手册

全程护航 迈向云端

Protected Cloud

Web Security

文档编号：WFCM97382/160406

发布日期：2016 年 3 月

受美国专利号保护： 5,951,698 和 7,188,369

本文档介绍产品的主要功能和/或提供针对生产环境的安装说明。在安装或使用产品之前，请详细阅读。

有关如何使用产品中特定功能的详细信息，可以在趋势科技联机帮助中心和/或趋势科技知识库中获得。

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何文档有任何问题、意见或建议，请通过 service@trendmicro.com.cn 与我们联系。

请在以下站点评估此文档：

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

目录

前言

第 1 章：安全无忧软件-网络安全版以及邮件与网络安全版简介

第 2 章：入门

第 3 章：安装客户端

第 4 章：管理组

第 5 章：管理安全客户端的基本安全设置

第 6 章：管理邮件安全客户端的基本安全设置（仅限邮件与网络安全版）

第 7 章：管理扫描

第 8 章：管理更新

第 9 章：管理通知

第 10 章：使用爆发防御

第 11 章：管理全局设置

第 12 章：使用日志和报表

第 13 章：执行管理任务

第 14 章：使用管理工具

附录 A：安全客户端图标

附录 B：WFBS 中的 IPv6 支持

附录 C：获取帮助

附录 D：产品术语和概念

索引

前言

前言

欢迎使用《趋势科技™ 安全无忧™软件 *管理员指南*》。本文档介绍了入门信息、客户端安装过程以及安全管理服务器和安全客户端管理。

安全无忧软件文档

安全无忧软件文档包括：

表 1. 安全无忧软件文档

文档	描述
安装和升级指南	PDF 文档，讨论安装安全管理服务器以及升级服务器和客户端的要求和过程
管理员指南	PDF 文档，讨论入门信息、客户机安装过程以及安全管理服务器和安全客户端管理
帮助	编译为 WebHelp 或 CHM 格式的 HTML 文件，提供操作指导、使用建议和文本框的特定信息
自述文件	包含已知问题和基本安装步骤的列表。该文件可能还包含帮助或印刷文档中尚未包括的最新产品信息
知识库	一个包含解决问题和故障排除信息的联机数据库。它提供有关已知产品问题的最新信息。要访问知识库，请转到以下 Web 站点： http://esupport.trendmicro.com/zh-cn/default.aspx

从以下位置下载最新版本的 PDF 文档和自述文件：

http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security.aspx

读者

安全无忧软件文档面向以下用户：

- **安全管理员**：负责安全无忧软件管理，包括安全管理服务器和安全客户端安装及管理。这些用户应具有高级联网和服务器管理知识。
- **最终用户**：在计算机上安装了安全客户端的用户。他们的计算机技能不一，从初学者到高级用户不等。

文档约定

为了帮助您轻松地查找和解释信息，安全无忧软件文档使用以下规则：

表 2. 文档约定

约定	描述
全大写	首字母缩写词、缩写、某些命令名称和键盘上的按键
粗体	菜单和菜单命令、命令按钮、选项卡、选项以及任务
斜体	对其他文档或新技术组件的引用
<文本>	表明应将尖括号内的文本替换为实际数据。例如，`C:\Program Files\<文件名>` 可以是 `C:\Program Files\sample.jpg`。
注意	提供配置说明或建议
提示	提供最佳做法信息和趋势科技建议
警告!	提供有关可能危害网络中计算机的活动的警告

第 1 章

安全无忧™软件-网络安全版以及邮件与网络安全版简介

本章提供安全无忧软件 (WFBS) 的概述。

趋势科技安全无忧软件概述

趋势科技安全无忧软件 (WFBS) 可保护小型企业用户和资产免遭数据偷窃、身份盗用、危险 Web 站点和垃圾邮件（仅限邮件与网络安全版）的侵害。

本文档提供了有关 WFBS 网络安全版和邮件与网络安全版的信息。仅与邮件与网络安全版相关的章节使用了以下标记“（仅限邮件与网络安全版）”。

WFBS 由趋势科技云安全智能防护网络提供支持，具备以下特性：

- **更安全**：可阻止病毒、间谍软件、垃圾邮件（仅限邮件与网络安全版）和 Web 威胁入侵客户机。URL 过滤可阻止对危险 Web 站点的访问，有助于提高用户生产力。
- **更智能**：快速扫描和连续更新可防止新的威胁，同时将对客户机的影响降到最低。
- **更简便**：由于部署简单且不需要进行任何管理，所以 WFBS 可更有效地检测威胁，以便您可以专注于业务，而无需担心安全问题。

此发行版 (WFBS 9.0 SP3) 的新增功能

安全无忧软件提供下列新功能和改进功能。

表 1-1. WFBS 9.0 SP3 的新增功能

功能/增强功能	描述
Windows 10 11 月更新支持	安全无忧软件现在支持在安装有 11 月更新的 Windows 10 计算机上安装安全客户端。
程序检查	安全无忧软件可在端点对进程进行监控和挂钩，进而检测可能危及安全的可执行文件并提高总体检测比率，以此方式提供更强大的勒索软件防护。
文档保护增强功能	安全无忧软件加强了文档保护，可使文档免遭未授权的加密或修改，进而阻止可能的勒索软件攻击。

功能/增强功能	描述
加强了行为监控保护	安全无忧软件现在缺省情况下启用以下行为监控功能： • 执行最近遇到的程序之前发送用户通知 • 保护文档，使其免遭未授权的加密或修改 • 自动备份被可疑程序修改的文件 • 对进程进行监控和挂钩 • 阻止与勒索软件关联的进程
SHA-2 支持	安全无忧软件现在支持使用 SHA-2 签名的证书。

表 1-2. 解决的已知问题

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
1	3150	用户升级到安全无忧软件 9.0 Service Pack 2 后重新安装邮件安全客户端时，趋势科技邮件安全客户端从安全无忧软件服务器管理控制台上的客户端树中消失。	此 Hotfix 确保邮件安全客户端可以成功注册到安全无忧软件 9.0 Service Pack 2 安全管理服务器。
2	3205	由于最近广泛存在勒索软件攻击，用户可能会遇到勒索软件。	此 Hotfix 支持对安全客户端上通过 HTTP 或电子邮件应用程序下载的最近遇到的程序进行监控，进而加强防御可能的勒索软件攻击。
3	3288	启用安全无忧软件 9.0 Service Pack 2 客户端的 Web 信誉功能后，用户可能无法访问任何 Web 站点。	此 Hotfix 可确保 Web 信誉功能正常运行。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
4	3290	用户升级到安全无忧软件 9.0 Service Pack 2 后，安全无忧软件服务器管理控制台上无法正常显示快速链接“编辑设置”。	此 Hotfix 确保安全无忧软件服务器管理控制台正确显示“编辑设置”快速链接。
5	3304	从控制面板卸载安全客户端后，用户无法使用组策略对象 (GPO) 重新部署无忧安全客户端。之所以发生此问题，是因为安全客户端安装程序检测到 GPO 生成的无忧安全客户端产品密钥并据此视为该产品已安装，因此随后触发其终止安装该产品。	此 Hotfix 确保用户可以通过 GPO 成功重新部署安全客户端。
6	3323	用户访问“安全客户端的安全设置”页面时，可能会遇到“本地存储未成功”浏览器错误消息。	此 Hotfix 确保在用户浏览客户端树时，定制用户界面布局设置失败的情况下，浏览器向用户显示缺省用户界面布局。
7	3326	AEGIS 模块可能会触发一些进程意外关闭。	此 Hotfix 更新了行为监控服务模块 2.974.1104，确保 AEGIS 模块不再触发进程意外关闭。
8	3330	用户在启用安全无忧软件的“浏览器利用阻止”功能后浏览某些网站时，其 Internet Explorer 附加软件意外停止。	此 Hotfix 确保启用“浏览器利用阻止”功能时，Internet Explorer 附加软件正常运行。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
9	MSA 11.1.1306	HTTP 授权标头字段不包含任何用户信息时，ActiveSync 不运行。	如果 HTTP 授权标头字段不包含任何用户信息，此 Hotfix 可以使安全无忧软件自动收集用户信息。这有助于确保 ActiveSync 正常运行。 此 Hotfix 还可以解决某些邮件安全客户端用户界面问题。应用此 Hotfix 后，安全无忧软件将在新的 Internet Explorer 选项卡中打开 MSA Web 控制台。

WFBS 9.0 SP2 的新增功能

安全无忧软件提供下列新功能和改进功能。

表 1-3. WFBS 9.0 SP2 的新增功能

功能/增强功能	描述
Windows 10 支持	安全无忧软件 现在支持在 Windows 10 上安装 安全客户端。
针对文档的勒索软件防护	通过识别常见行为并阻止通常与勒索软件程序关联的进程，增强扫描功能可识别并阻止目标为端点上运行的文档的勒索软件程序。

表 1-4. 解决的已知问题

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
1	B2363	在用户禁用 Intuit QuickBooks 防护功能后，安全客户端可能仍会保护 Intuit 文件。	此 Hot Fix 确保用户可以成功禁用 Intuit Quickbooks 防护功能。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
2	B2363	在用户禁用文件夹保护功能后，安全客户端仍可能会保护文件夹。	此 Hot Fix 确保用户可以成功禁用文件夹保护功能。
3	B2453	在启用 POP3 电子邮件扫描的情况下启动 安全无忧软件 9.0 Service Pack 1 客户端时，由于与 趋势科技 安全客户端侦听程序 (TmListen.exe) 服务发生时间冲突，实时扫描 (Ntrtscan.exe) 服务可能无法启动。	此关键 Patch 通过确保让 趋势科技 安全客户端侦听程序服务允许在启动其他服务之前启动实时扫描服务，解决了该时间冲突。
4	B2453	在某些环境中，部分扫描进程可能会挂起，并且 安全无忧软件 9.0 Service Pack 1 客户端可能无法对检测到的恶意软件执行任何处理措施。出现这种情况时，安全无忧软件 不显示弹出警告或生成检测日志。	此关键 Patch 使 安全无忧软件 9.0 Service Pack 1 客户端能够在上述情况下对检测到的恶意软件执行必要操作。
5	B2479	在手动扫描期间，手动扫描进度窗口停止响应。	此 Hot Fix 确保手动扫描可正常运行和完成。
6	B2500	有问题成功阻止 安全无忧软件 9.0 Service Pack 1 服务器更新云安全云端病毒码。出现这种情况时，服务器 Web 控制台上云安全扫描服务的实时状态将变为“不可用”。	此 Hot Fix 确保 安全无忧软件 9.0 Service Pack 1 服务器能够成功更新云安全云端病毒码。
7	B2502	有问题阻止 安全无忧软件 9.0 Service Pack 1 服务器禁用全局设置：“将 Web 信誉和 URL 过滤日志发送至安全管理服务器”。	此 Hot Fix 确保 安全无忧软件 9.0 Service Pack 1 服务器可以禁用设置：“将 Web 信誉和 URL 过滤日志发送至安全管理服务器”。
8	B2503	在 Microsoft(TM) 64 位操作系统上，当 32 位版本的 Internet Explorer 9 与安全客户端共存时可能会崩溃。	此 Hot Fix 确保此浏览器在 Microsoft 64 位操作系统上与安全客户端共存时正常运行。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
9	B2510	在 Microsoft(TM) Windows(TM) 8.0、8.1 或 Server 2012 R2 平台上安装 安全无忧软件 9.0 Service Pack 1 客户端时，缺省情况下启用 SMTP 邮件扫描功能。发生这种情况时，平台的电子邮件服务器和客户端可能会无法发送或接收某些电子邮件。	此 Hot Fix 确保安全客户端与平台电子邮件服务器和客户端正常运行。
10	B2514	在安装 安全无忧软件 9.0 Service Pack 1 客户端的计算机上，用户可能会遇到性能问题。	此 Hot Fix 解决了受影响计算机上的性能问题。
11	B2515	在计算机上安装 安全无忧软件 9.0 Service Pack 1 客户端后，与 “coreTaskManager.dll” 二进制文件相关的问题可能会触发堆内存泄漏问题。	此 Hot Fix 解决了受影响计算机上的堆内存泄漏问题。
12	B2516	用户可能无法在安装 安全无忧软件 9.0 Service Pack 1 服务器的计算机上安装趋势科技远程管理器客户端。出现这种情况时，用户将无法使用其现有 GUID 将 安全无忧软件 注册到趋势科技远程管理器。	此 Hot Fix 解决了这些安装问题，确保用户可以在安装 安全无忧软件 9.0 Service Pack 1 服务器的计算机上安装趋势科技远程管理器客户端。
13	B2517	启用实时扫描功能后，安装 安全无忧软件 9.0 Service Pack 1 客户端的计算机可能会停止响应。	此 Hot Fix 确保启用实时扫描功能后 安全无忧软件 9.0 Service Pack 1 客户端可正常运行。
14	B2519	安装 安全无忧软件 9.0 Service Pack 1 客户端时，用户可能会遇到系统崩溃问题。	此 Hot Fix 解决了安装 安全无忧软件 9.0 Service Pack 1 客户端时的系统崩溃问题。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
15	B2520	有时候，安全无忧软件 9.0 Service Pack 1 无法检测到从受保护计算机中弹出并重新插入其中的 USB 磁盘设备。	此 Hot Fix 确保 安全无忧软件 9.0 Service Pack 1 可以检测到插入受保护计算机的 USB 磁盘设备。
16	B2534	安装 安全无忧软件 9.0 Service Pack 1 客户端后，用户可能会遇到系统崩溃问题。	此 Hot Fix 解决了安装 安全无忧软件 9.0 Service Pack 1 客户端时的系统崩溃问题。
17	B2541	在带有群集共享卷 (CSV) 磁盘的 Microsoft™ Windows™ Server 环境中，安全无忧软件 9.0 Service Pack 1 可能会意外停止或触发蓝屏死机 (BSOD)。	此 Hot Fix 确保 安全无忧软件 9.0 Service Pack 1 与 Windows Server 故障转移群集中的 CSV 磁盘可正常运行。

WFBS 9.0 SP1 的新增功能

安全无忧软件提供下列新功能和改进功能。

表 1-5. WFBS 9.0 SP1 的新增功能

功能/增强功能	描述
检测改进	• 针对压缩可执行文件（加壳软件）的爆发阻止防护 • 改进了损害清除引擎性能
增强功能	Web 信誉日志包括正在运行的进程信息
可使用性改进	• 在登录窗口上会显示安全管理服务器版本 • 更新了 UI 文本，能够更好地反映 WFBS 的工作方式

表 **1-6.** 解决的已知问题

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
1	N/A	用户请求通过某种方式配置邮件安全客户端，以便对已隔离的垃圾电子邮件运行阻止附件扫描 (MSA 11.1.1254)。	此 Hot Fix 添加了一个选项，可对邮件安全客户端进行配置，以便对已隔离的垃圾电子邮件运行阻止附件扫描。
2	1433	将安全无忧软件从 8.0 或 8.0 Service Pack 1 升级到 9.0 版之后，该服务器 Web 控制台上云安全扫描服务的实时状态将变为“不可用”。原因是安全无忧软件 9.0 服务器无法成功更新云安全云端病毒码。	此 Hot Fix 可确保安全无忧软件 9.0 服务器能够成功更新云安全云端病毒码。
3	1439	安全无忧软件 9.0 服务器软件包包含一个 OpenSSL 加密软件库，而该软件库会受到 Heartbleed 漏洞的影响。	此关键 Patch 会更新安全无忧软件 9.0 SP3 服务器软件包中的 OpenSSL 加密软件库以解决此问题。
4	1440	如果 Microsoft™ Windows™ 处于高对比度模式，并且用户可以在 Microsoft Internet Explorer 中访问安全无忧软件 9.0 控制台，则用户无法将客户端从一个组移到另一个组。	此 Hot Fix 会更正一个函数属性，以使 Internet Explorer 能够在 Windows 处于高对比度模式下时正确检索信息。这样有助于确保在此情况下用户可以成功在组间移动客户端。
5	1442	安全无忧软件客户端可能无法对网络驱动器运行手动扫描。	此 Hot Fix 确保安全无忧软件客户端能够对网络驱动器运行手动扫描。
6	1445	安全无忧软件服务器数据库进程在间谍软件日志查询过程中可能会遇到内存泄漏。	此 Hot Fix 确保安全无忧软件服务器数据库进程不会在执行间谍软件日志查询时遇到内存泄漏。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
7	1451	当用户单击服务器用户界面的客户端树中的“检测到的病毒”、“检测到间谍软件”、“检测到的垃圾邮件数”和“被违反的 URL” 列对数据进行排序时，安全无忧软件无法正确排序相应数据。	此 Hot Fix 会更正影响“检测到的病毒”、“检测到间谍软件”、“检测到的垃圾邮件数”和“被违反的 URL” 列的数据排序问题。
8	1452	如果管理员使用 AutoPCC 登录脚本部署客户端，则启动时无法加载安全客户端服务。	此 Hot Fix 确保当管理员使用 AutoPCC 登录脚本部署客户端时，安全客户端服务能够在启动时正确加载。
9	1454	在没有明显原因的情况下，用户会随机收到安全客户端的弹出窗口。	此 Hot Fix 确保用户只在发生必要事件（以该用户的通知配置为准）时才会收到安全客户端的弹出窗口。
10	1456	在 Microsoft™ 64 位操作系统 (OS) 上，当 32 位版本的 Internet Explorer 9 与安全客户端共存时可能会崩溃。	此 Hot Fix 确保此浏览器在 Microsoft 64 位操作系统上与安全客户端共存时正常运行。
11	1457	从安全无忧软件服务器导出的病毒日志中的“采取的处理措施”字段不包含任何信息。	此 Hot Fix 确保病毒日志从安全无忧软件服务器正确导入。
12	1458	安全无忧软件服务器的 POP3 邮件日志和安全客户端日志的“日期/时间”字段不一致。	此 Hot Fix 确保安全无忧软件服务器的 POP3 日志与安全客户端的日志中的信息完全一致。
13	1459	用户可能无法从 HTTP 重定向源更新云安全云端病毒码。	此 Hot Fix 确保更新过程能够正确处理 HTTP 重定向响应中的美元符号，以便用户成功从 HTTP 重定向源更新云安全云端病毒码。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
14	1459	安全客户端会在客户端更新其程序文件时收到气球通知。客户请求通过某种方式禁用此类型的气球通知。	此 Hot Fix 提供了一个选项，可禁用客户端更新其程序文件时出现的气球通知。
15	1466	安装安全无忧软件客户端之后，进程 PccNTMon.exe 可能遇到句柄泄漏问题。	此 Hot Fix 解决了受影响计算机上的句柄泄漏问题。
16	2062	安全无忧软件软件包附带并与第三方驱动程序一同使用的 EYES 驱动程序有时可能出现误报。	此 Hot Fix 将更新 EYES 驱动程序，帮助避免其误报问题。
17	2063	安装完安全无忧软件客户端之后，TmListen 可能会意外停止。	此 Hot Fix 确保安装完安全无忧软件客户端之后，TmListen 能够成功运行。
18	5215	当用户使用非管理员帐户登录 Windows 时，运行 Windows XP 的计算机上安装的安全客户端无法检测到 USB 设备引导扇区中的恶意软件。	此 Hot Fix 将更新安全客户端文件以解决此问题。
19	5215	当安全客户端对路径长度超过 260 个字符的位置执行手动扫描时，Ntrtscan.exe 服务可能会意外停止。	此 Hot Fix 允许安全客户端在扫描时使用一个灵活变量取代固定变量存储文件路径，避免 Ntrtscan.exe 出现意外停止的情况。
20	5215	某些时候，当安全客户端启动时，安全客户端 Listener 服务 TmListen.exe 会意外停止。	此 Hot Fix 增强了安全客户端的错误处理机制，防止 TmListen.exe 在安全客户端启动时意外停止。
21	5215	某些时候，即使计算机中已启用安全客户端，安全客户端计算机的状态在 Microsoft™ Windows™ 操作中心中也会显示为“趋势科技安全客户端已关闭”。	此 Hot Fix 将更新安全客户端文件，以确保 Windows 操作中心中显示正确的安全客户端状态。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
22	5227	由于病毒扫描引擎设置的问题，在 Novell™ ZENworks™ 应用程序平台中，需要较长时间才能登录安全客户端控制台。	此 Hot Fix 解决该问题的方法是允许用户修改安全无忧软件服务器中的病毒扫描引擎设置并将新的病毒扫描引擎设置全局部署到安全无忧软件客户端。
23	5238	安全管理服务器 `cgiCheckIP.exe` 功能允许用户扫描任何网络内的任何端口。	此 Hot Fix 增强了 `cgiCheckIP.exe` 功能的端口检查机制，以便在扫描端口之前正确验证从客户端发送的端口号。
24	5245	在共享文件夹中打开 Office 文件时，Microsoft™ Office™ 会挂起。此问题可通过部署 `CheckRtPCWOplock` 参数得到解决。	此 Hot Fix 允许用户在**全局设置**中设置以下 `CheckRtPCWOplock` 参数并部署到客户端，从而解决挂起问题。
25	5248	某些时候，在 Microsoft™ Windows™ 操作中心中，VPN 网络环境下的安全客户端计算机状态会显示为“趋势科技安全客户端已关闭”。	此 Hot Fix 将更新安全客户端文件，以确保 Windows 操作中心显示正确的客户端状态。
26	5248	安全客户端 始终会改写以下客户端注册表项并将其设置为防火墙模块的缺省值：`HKLM \SYSTEM\CurrentControlSet \services\tmtdi \Parameters\ RedirectIpv6`	此 Hot Fix 将修改重定向 IPv6 功能，方法是手动（非强制）覆盖 `RedirectIpv6` 注册表项，将其设为默认值。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
27	5274	更新安全客户端时，安全客户端会从 ClientAllSetting.ini 文件检索“其他更新源”(OUS) 设置，并使用已检索的信息更新 OUS.ini 文件。但是，当安全管理服务器主服务停止后，ClientAllSetting.ini 文件会被清空。因此，安全客户端将无法检索任何 OUS 设置以更新 OUS.ini 文件，从而导致安全客户端更新失败。	此 Hot Fix 会添加一项检查机制，防止安全客户端在无法从 ClientAllSetting.ini 文件检索任何 OUS 设置的情况下对 OUS.ini 文件进行更改。这确保安全客户端仍然能够在 ClientAllSetting.ini 文件为空时完成更新。
28	5339	某些时候，安全客户端控制台上的病毒清除模板版本会在客户端更新该模板并加载新版本之后变为“0”。	此 Hot Fix 增强了版本检查机制，确保安全客户端控制台上显示正确的病毒清除模板版本。
29	5350	当安全客户端使用 IPv6 将 URL 重定向到 Web 信誉服务 (WRS) 时，用户可能无法访问内部网站。	此 Hot Fix 解决了此问题，方法是提供一个选项，可将安全客户端配置为使用 IPv4 代替 IPv6 将 URL 重定向到 WRS 并全局部署该设置。
30	5366	当 Microsoft™ Outlook™ 在运行安全客户端行为监控服务的计算机上启动时会停止响应。	此 Hot Fix 提供了部署行为监控的设置，可防止 Outlook 在此情况下意外停止。
31	5369	当安全客户端检测到自解压压缩文件中存在间谍软件但对该文件的所有处理措施都失败时，不会生成间谍软件日志。	此 Hot Fix 确保安全客户端检测到压缩文件中存在间谍软件但对该文件的所有处理措施都失败时生成间谍软件日志。
32	5390	更新完成后，安全客户端的 OUS.ini 文件会被截断。如果 OUS.ini 文件比为复制功能分配的内存缓存要大，从而迫使该功能截断该文件以适应此缓存，则会发生这种情况。	此 Hot Fix 会增加用于 OUS.ini 复制功能的内存缓存，避免该功能在更新期间截断安全客户端的 OUS.ini 文件。

项目编号	HOT FIX/关键 PATCH 编号	问题	解决方案
33	5399	有时，在客户端更新病毒清除模板并加载新版本后，防毒墙网络版客户端控制台上的病毒清除模板版本会变为“0”。	此 Hot Fix 增强了版本检查机制，可确保防毒墙网络版客户端控制台上显示正确的病毒清除模板版本。
34	5443	云安全客户端和病毒码文件的还原过程可能无法正常进行。	此 Hot Fix 可确保云安全客户端和病毒码文件的还原过程能够正常进行。
35	5463	如果同时启用了客户端的未授权更改阻止服务和防火墙服务，则第三方软件可能会在安全客户端计算机上停止响应。	可以使用户部署一项防火墙设置，以防止在同时启用了客户端的未授权更改阻止服务和防火墙服务的情况下第三方软件在安全客户端计算机上意外停止。
36	5485	在安全客户端执行手动扫描时，如果扫描路径的长度超过 63 个字符，则相应的扫描日志不会显示在“病毒日志”查看器中。	此 Hot Fix 可确保扫描路径的长度超过 63 个字符时能够成功记录扫描日志。
37	5492	64 位平台上安装的安全客户端可能无法使用更新代理进行更新。	此 Hot Fix 确保安全客户端能够成功从更新代理进行更新。
38	5495	在安全客户端更新期间，如果某些组件的模块正在由某些功能使用，则这些组件可能无法更新。	此 Hot Fix 可确保在安全客户端更新期间所有组件都能得以更新。

WFBS 9.0 的新增功能

安全无忧软件提供下列新功能和改进功能。

表 1-7. WFBS 9.0 的新增功能

功能/增强功能	描述
Microsoft Exchange 支持	WFBS 当前支持 Microsoft Exchange Server 2010 SP3 和 Microsoft Exchange Server 2013。
Windows 支持	WFBS 当前支持 Microsoft Windows 8.1 和 Windows Server 2012 R2。

移动设备安全	WFBS 邮件与网络安全版当前支持移动设备数据保护和访问控制。移动设备安全具有以下功能：
	• 设备访问控制
	  • 允许根据用户、操作系统和/或电子邮件客户端访问 Exchange Server
	  • 指定授予特定邮箱组件的访问权限
	• 设备管理
	  • 在丢失或被盗设备上执行设备擦除
	  • 将安全设置套用至特定用户，包括：
	  • 密码强度要求
	  • 在非活动之后自动锁定设备
	  • 加密
	  • 清除不成功的登录数据

激活码增强	付费后激活码支持
检测改进	• 用于实时扫描的增强式内存扫描 • 用于行为监控的已知和潜在威胁模式 • 浏览器利用阻止 • 最近遇到的程序下载检测
性能改进	• 安全客户端的安装和卸载时间 • 用于实时扫描的同步流扫描

功能/增强功能	描述
可使用性改进	• 用于 Web 信誉和 URL 过滤的全局和组核准/阻止列表 • 全局设置中用于 Web 信誉和 URL 过滤的 IP 异常列表 • 从客户机树和远程安装页面移除 ActiveX • 定制的爆发防御 • Outlook 2013 和 Windows Live Mail 2012 支持趋势科技反垃圾邮件工具栏 • 用于仅从趋势科技 ActiveUpdate 进行更新的更新代理 • 停止服务器更新 • 升级服务器和代理时保留特征码 • 帮助链接和感染源病毒日志

关键功能和优点

安全无忧软件提供下列功能和优点：

趋势科技™ 云安全智能防护网络™

趋势科技™ 云安全智能防护网络™ 是下一代云客户端内容安全基础架构，旨在保护客户免遭安全风险和 Web 威胁。它提供了内部部署和趋势科技托管解决方案来保护用户安全，无论用户是位于网络上、在家中还是外出。云安全智能防护网络使用轻量级客户端访问其提供的独特云中电子邮件、Web 和文件信誉相关技术以及威胁数据库。随着更多的产品、服务和用户访问此网络，客户防护会自动更新和加强，从而实时紧密查看网络用户的防护服务。

有关云安全智能防护网络的更多信息，请访问：

http://www.trendmicro.com.cn/cn/technology-innovation/our-technology/smart-protection-network/index.html

文件信誉服务

文件信誉服务对照庞大的云端数据库检查每个文件的信誉。恶意软件信息存储在云端后，所有用户可立即使用该信息。高性能内容传递网络和本地缓存服务器可保证检查期间的延迟为最小。云客户端体系结构提供了更及时的防护，消除了部署特征码的负担，此外还显著降低了整体的客户端资源占用。

安全客户端必须在处于云安全扫描模式时才能使用文件信誉服务。在本文档中，这些客户端称为**云安全客户端**。不处于云安全扫描模式下的客户端不使用文件信誉服务，这些客户端称为**传统扫描客户端**。安全无忧软件 管理员可以将所有或多个客户端配置为处于云安全扫描模式。

Web 信誉服务

趋势科技 Web 信誉技术使用全球最大的域信誉数据库之一来跟踪 Web 域的可信度，方法是根据 Web 站点的建站时间、历史位置更改和通过恶意软件行为分析发现的可疑活动的出现次数等因素来指定信誉分值。然后，Web 信誉将继续扫描站点并阻止用户访问受感染站点。Web 信誉功能可帮助确保用户访问的页面是安全的且不存在 Web 威胁，如恶意软件、间谍软件和旨在欺骗用户提供个人信息的网络钓鱼邮件。为提高精确度并减少误报，趋势科技 Web 信誉技术为站点内的具体页面或链接指定信誉分值，而不是分类或阻止全部站点，因为通常只有合法站点的某些部分会被黑客控制，并且信誉可随时动态更改。

受 Web 信誉策略限制的客户端使用 Web 信誉服务。安全无忧软件 管理员可以使所有或多个客户端受限于 Web 信誉策略。

电子邮件信誉（仅限邮件与网络安全版）

趋势科技电子邮件信誉评价技术通过针对已知垃圾邮件源信誉数据库检查 IP 地址以及使用可实时评估电子邮件发件人信誉的动态服务，来验证 IP 地址。通过持续分析 IP 地址的行为、活动范围及以前的历史记录，可以对信誉评级

进行优化。基于发件人的 IP 地址，在云端就阻止了恶意电子邮件，从而防止诸如僵尸或僵尸网络等威胁进入网络或用户的 PC。

电子邮件信誉评价技术可根据始发邮件传输客户端 (MTA) 的信誉确定垃圾邮件。这可减轻安全管理服务器的任务负担。启用“电子邮件信誉评价”后，将会根据 IP 数据库检查所有的入站 SMTP 通信，以查看始发 IP 地址是正常的还是已作为已知垃圾邮件源列入黑名单。

“电子邮件信誉评价”有两个服务级别：

- **标准**：标准服务使用一个可跟踪约二十亿个 IP 地址信誉的数据库。总是与垃圾邮件传递关联的 IP 地址将添加到此数据库中，并且一般不会将其删除。
- **高级**：高级服务级别是一个 DNS，它是基于查询的服务，类似于标准服务。此服务的核心是标准信誉评价数据库和一个动态信誉评价的实时数据库，该数据库可阻止来自已知和可疑的垃圾邮件源的邮件。

如果发现来自已阻止或可疑 IP 地址的电子邮件，则电子邮件信誉服务 (ERS) 会在其进入邮件系统基础架构前将其阻止。如果 ERS 阻止的电子邮件来自您认为安全的 IP 地址，则请将此 IP 地址添加到“允许的 IP 地址”列表。

云安全智能反馈

趋势科技云安全智能反馈在趋势科技产品与其 24x7 全天候威胁研究和技术中心之间提供不间断的通信。通过每个单一客户的例行信誉检查识别到的每个新威胁，都会自动更新所有趋势科技威胁数据库，从而阻止任何后续客户遇到已知的威胁。

通过持续不断地利用其庞大的全球性客户和合作伙伴网络收集威胁情报，趋势科技可提供自动化的实时防护，以抵御最新的威胁，并提供最佳的协同防护安全性。这很像是一种自动化的居民区监视系统，让社区参与相互保护的工作。由于威胁信息是根据通信源的信誉而不是具体的通信内容收集的，因此客户的个人信息或商业信息的隐私性始终会得到保护。

发送到趋势科技的信息示例：

- 文件校验和

- 已访问的 Web 站点
- 文件信息，包括大小和路径
- 可执行文件的名称

可以随时从 Web 控制台终止参与该计划。

有关详细信息，请参阅参与智能反馈计划 第 13-4 页。

提示

无需参与云安全智能反馈便可为您的客户端提供防护。您可以选择参与，也可以随时退出。趋势科技建议您参与云安全智能反馈以帮助为所有趋势科技客户提供更好的整体防护。

有关云安全智能防护网络的更多信息，请访问：

http://www.trendmicro.com.cn/cloudsecurity/

URL 过滤

URL 过滤有助于控制对 Web 站点的访问，以减少非生产性雇员的时间、降低 Internet 带宽占用，并创造更安全的 Internet 环境。您可选择 URL 过滤防护等级，或定制想要屏蔽的 Web 站点的类型。

防护的优势

下表描述了安全无忧软件的不同组件如何保护计算机免遭威胁。

表 1-8. 防护的优势

威胁	防护
病毒/恶意软件。病毒、特洛伊木马、蠕虫病毒、后门程序以及 Rootkit **间谍软件/灰色软件**。间谍软件、拨号程序、黑客工具、密码破解程序、广告程序、恶作剧程序以及按键记录软件	基于文件的扫描（实时扫描、手动扫描、预设扫描）
通过电子邮件传输的安全威胁	安全客户端中的 **POP3 邮件扫描**
网络蠕虫/病毒和入侵	安全客户端中的防火墙
可能有害的 Web 站点/网络钓鱼站点	安全客户端中的 Web 信誉和 URL 过滤
通过 USB 和其他外部设备传播的安全威胁	安全客户端中的设备控制
恶意行为	安全客户端中的行为监控

了解威胁

没有专门的安全人员且采用宽松安全策略的组织，即使具备基本的安全基础架构，仍越来越多地面临威胁的侵害。发现之时，这些威胁可能已经蔓延到了许多计算资源，因此需要耗费大量时间和精力才能完全消除。而与消除威胁有关的不可预见的成本也可能是非常巨大的。

趋势科技网络安全情报和云端服务器作为势科技云安全智能防护网络的组成部分，可识别并响应新一代威胁。

病毒和恶意软件

存在成千上万种病毒/恶意软件，而且数量还在每日剧增。虽然计算机病毒一度流行于 DOS 或 Windows，如今，通过利用企业网络、电子邮件系统和 Web 站点的漏洞，计算机病毒会导致更大量的损害。

- **恶作剧程序**：象病毒一样的程序，经常操纵计算机显示器上的内容。

- **可能的病毒/恶意软件**：具有某些病毒/恶意软件特征的可疑文件。有关详细信息，请参阅趋势科技威胁百科全书：

  http://about-threats.trendmicro.com/threatencyclopedia.aspx?language=cn&tab=malware

- **Rootkit**:在最终用户不同意或不知情的情况下在系统上安装并执行代码的程序（或程序集），通过隐藏保持在计算机上永久存在而不被检测到。Rootkit 并不感染计算机，但却为恶意代码的执行提供了一个无法检测到的环境。Rootkit 通过社交工程、执行恶意软件甚至只是浏览恶意网站来安装到系统上。一旦安装，攻击者事实上可以在系统上执行任何功能，以加入远程访问、窃听以及隐藏进程、文件、注册表项和通信通道。

- **特洛伊木马**：此类病毒常常使用端口获得计算机或可执行程序的访问权。特洛伊木马程序并不进行复制，而是驻留在系统上，执行一些恶意行为，例如为电脑黑客潜入打开端口。传统防病毒解决方案可以检测并删除病毒而不是特洛伊木马，特别是已经在系统上运行的这些特洛伊木马。

- **病毒**：执行复制的程序。要执行此操作，病毒需要将自己附在其他程序文件中，宿主程序一运行病毒就运行，包括：

  - **ActiveX 恶意代码**：驻留在 Web 页面上执行 ActiveX™ 控件的代码
  - **引导区病毒**：感染分区或磁盘的引导扇区的病毒。
  - **COM 和 EXE 文件感染源**：扩展名为 `.com` 或 `.exe` 的可执行程序
  - **Java 恶意代码**：用 Java™ 编写或嵌入在其中的不依赖操作系统的病毒代码
  - **宏病毒**：用应用程序宏编码且通常包含在文档中的病毒。
  - **打包程序**：压缩和/或加密的 Windows 或 Linux™ 可执行程序，通常为特洛伊木马程序。压缩可执行文件使防病毒产品更难以检测到打包程序。
  - **测试病毒**：一种行为类似真正病毒的无害文件，病毒扫描软件可检测到。使用测试病毒（如 EICAR 测试脚本）验证防病毒安装是否正常扫描。
  - **VBScript**、**JavaScript** 或 **HTML virus** 病毒驻留在 Web 页面上且通过浏览器下载的病毒。

- **蠕虫病毒**：一个独立程序（或一组程序），能将自身或片段的功能副本传播到其它计算机系统（通常通过电子邮件）。
- **其他**：未划入任何其他病毒/恶意软件类型下的病毒/恶意软件。

间谍软件和灰色软件

端点面临来自潜在威胁而非病毒/恶意软件的风险。间谍软件/灰色软件是指不归类为病毒或特洛伊木马，但是仍然可以对网络上的客户端性能产生不利影响，并为贵组织带来重大安全、机密和法律风险的应用程序或文件。通常间谍软件/灰色软件将执行各种不受欢迎并有威胁性的操作，如使用弹出窗口引起用户不愉快，记录用户的击键，以及将客户端漏洞暴露于攻击的威胁之下。

如果发现某个应用程序或文件未被安全无忧软件检测为灰色软件，但您认为是某种类型的灰色软件，请将其发送给趋势科技以便进行分析：

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

类型	描述
间谍软件	收集帐户用户名和密码等数据并将其传递到第三方。
广告程序	显示广告并收集数据（例如，Web 冲浪首选项），用于在用户使用 Web 浏览器期间显示目标广告。
拨号程序	更改客户端的 Internet 设置，并强制客户端通过调制解调器拨打预配置的电话号码。这些号码通常是来电付费或国际号码，可导致贵组织必须支付巨额费用。
恶作剧程序	导致客户端行为异常，例如，打开和关闭 CD-ROM 托盘以及显示许多消息框。
黑客工具	帮助黑客进入计算机。
远程访问工具	帮助黑客远程访问及控制计算机。
密码破解程序	帮助黑客破解帐户用户的名称和密码。
其他	其他类型的潜在恶意程序。

垃圾邮件

垃圾邮件包括不请自来的电子邮件（垃圾电子邮件），通常出于商业目的，大范围地发送至多个邮件列表、个人或新闻组。垃圾邮件有两种类型：不请自来的商业电子邮件 (UCE) 和不请自来的群发电子邮件 (UBE)。

入侵

入侵是指强制或者未经允许而进入网络或客户端。也可以指绕开网络或客户端安全防护。

恶意行为

恶意行为是指通过软件对操作系统、注册表项、其他软件或文件和文件夹进行未经授权的更改。

假冒接入点

假冒接入点也称为 Evil Twin（双面恶魔），是描述欺诈性 Wi-Fi 接入点的术语，该接入点看上去是合法提供的，但实际上由黑客建立用以窃听无线通信。

网络钓鱼事件

网络钓鱼是一种快速增长的欺诈形式，旨在通过模仿合法 Web 站点来诱使 Web 用户泄漏个人信息。

在通常情况下，可信任用户会收到一封看似紧急（并且看上去真实）的电子邮件，告知他们帐户出现问题，必须立即修复才能避免帐户终止。电子邮件将包含看上去完全真实的 Web 站点的 URL。复制合法电子邮件和合法 Web 站点非常简单，但是然后会更改所谓的后端，该后端接收收集的数据。

电子邮件告知用户登录该站点并确认一些帐户信息。黑客会收到用户提供的登录名、密码、信用卡号码或身份证号码等数据。

网络钓鱼欺诈快速、廉价并且易于传播。实施网络钓鱼的这些罪犯也会获取潜在的巨大利益。即使精通计算机的用户也难以检测到网络钓鱼。并且执法部分难以对其进行追查。更糟糕地是，几乎无法进行严惩。

请将您怀疑是网络钓鱼站点的任何 Web 站点报告给趋势科技。请参阅将可疑内容发送给趋势科技 第 C-3 页以了解更多信息。

群发邮件攻击

电子邮件感知型病毒/恶意软件具有通过自动操纵被感染计算机的电子邮件客户端或自行散布病毒/恶意软件来通过电子邮件进行传播的能力。群发邮件行为是指感染在 Microsoft Exchange 环境中迅速传播的情况。趋势科技设计了扫描引擎来检查通常伴随群发邮件攻击而出现的行为。这些行为记录在病毒码文件中；病毒码文件可通过趋势科技 ActiveUpdate 服务器得到更新。

您可以使邮件安全客户端（仅限邮件与网络安全版）无论何时检测到群发邮件行为，都对群发邮件攻击采取特定的处理措施。为群发邮件行为设置的处理措施优先于所有其他处理措施。针对群发邮件攻击的缺省处理措施是删除整个邮件。

例如：配置邮件安全客户端，使之在检测到受蠕虫病毒或特洛伊木马感染的邮件时隔离邮件。您也可以启用群发邮件行为，并将客户端设置为删除所有表现出群发邮件行为的邮件。客户端收到包含诸如 MyDoom 变种等蠕虫病毒的邮件。该蠕虫病毒使用其自己的 SMTP 引擎将其自身发送到从受感染计算机上收集到的电子邮件地址。当客户端检测到 MyDoom 蠕虫病毒并识别出其群发邮件行为时，它将删除含有该蠕虫病毒的电子邮件；对于未表现出群发邮件行为的蠕虫病毒，它将采取隔离处理措施。

Web 威胁

Web 威胁包括源自 Internet 的各种威胁。Web 威胁的方法非常复杂，使用各种文件或技术的组合，而不是单个文件或方法。例如，Web 威胁的作者会不断地更改使用的版本或变种。由于 Web 威胁位于 Web 站点的固定位置而不是受感染客户端上，因此 Web 威胁的作者会不断地修改其代码以避开检测。

在最近几年，以前称为黑客、病毒编写者、垃圾邮件发送者和间谍软件制作者的个人现在称为网络罪犯。Web 威胁可帮助这些个人达到以下两个目的之一。其中一个目的是窃取信息以进行后续销售。由此产生的影响是造成身份丢失，从而泄漏机密信息。受感染客户端还可能成为传递网络钓鱼攻击或其他信息捕捉活动的媒介。在其他影响中，该威胁会潜在地损害 Web 商业中的机密，破坏 Internet 事务所需的信任。第二个目的是劫持用户的 CPU 能力，将其用作进行盈利活动的工具。活动包括发送垃圾邮件或以分布式拒绝服务器攻击或按点击付费活动的形式进行敲诈。

第 2 章

入门

本章讨论如何使安全无忧软件启动并运行。

安全无忧软件网络

安全无忧软件包含以下组件：

- 安全管理服务器 第 2-2 页
- 客户端 第 2-3 页
- Web 控制台 第 2-4 页

安全管理服务器

安全无忧软件的核心是安全管理服务器。安全管理服务器托管 Web 控制台，该控制台是安全无忧软件的基于 Web 的集中式管理控制台。安全管理服务器将客户端安装到网络上的客户机中，与客户端一起，形成一种客户端-服务器关系。可以使用安全管理服务器查看安全状态信息、查看客户端、配置系统安全并从中央位置下载组件。安全管理服务器还包含数据库，其中存储有检测到的 Internet 威胁的日志（由客户端报告给安全管理服务器）。

安全管理服务器执行以下重要功能：

- 安装、监控和管理客户端。
- 下载客户端所需的组件。缺省情况下，安全管理服务器会从趋势科技 ActiveUpdate 服务器下载组件，然后将这些组件分发给客户端。

扫描服务器

安全管理服务器包括一项称为扫描服务器的服务，在安全管理服务器安装期间会自动安装该服务，因此不需要单独安装。扫描服务器运行的进程名称为 `iCRCService.exe`，在 Microsoft 管理控制台中显示为**趋势科技云安全扫描服务**。

当安全客户端使用称为**云安全扫描**的扫描方法时，扫描服务器会帮助这些客户端更高效地运行扫描。云安全扫描进程如下所述：

- 安全客户端会使用 **Smart Scan Agent Pattern**（轻量版传统病毒码），扫描客户机是否存在安全威胁。云安全客户端病毒码具有适用于传统病毒码的大多数威胁签名。
- 在扫描期间无法确定文件风险的安全客户端，会将扫描查询发送到扫描服务器，以验证风险。扫描服务器会使用**云安全云端病毒码**（具有不适用于云安全客户端病毒码的威胁签名）验证风险。
- 安全客户端会“缓存”扫描服务器提供给的扫描查询结果，以改善扫描性能。

通过托管某些威胁定义，扫描服务器有助于减少安全客户端下载组件式的带宽消耗。安全客户端会下载明显较小的云安全客户端病毒码，而不会下载传统病毒码。

如果安全客户端无法连接到扫描服务器，则会将扫描查询发送到与扫描服务器具有相同功能的趋势科技云安全智能防护网络。

无法从安全管理服务器单独卸载扫描服务器。如果不想使用扫描服务器，请执行以下操作：

1. 在安全管理服务器计算机上，打开 Microsoft 管理控制台，然后禁用**趋势科技云安全扫描服务**。
2. 在 Web 控制台上，导航到**首选项** > **全局设置** > **安全客户端**选项卡，然后选择**禁用云安全扫描服务**选项，以将安全客户端切换到传统扫描。

客户端

客户端保护客户机免遭安全威胁。客户机包括台式机、服务器和 Microsoft Exchange Server。WFBS 客户端是：

表 2-1. WFBS 客户端

客户端	描述
安全客户端	保护台式机和服务器免遭安全威胁和入侵

客户端	描述
邮件安全客户端（仅限邮件与网络安全版）	保护 Microsoft Exchange Server 免遭电子邮件附带的安全威胁

客户端向其安装自的安全管理服务器报告。为给安全管理服务器提供最新的客户机信息，客户端实时发送事件状态信息。客户端报告威胁检测、启动、关闭、开始扫描以及更新完成等事件。

Web 控制台

Web 控制台是监控整个企业网络中的客户机的中心点。它带有一组缺省设置和值，您可以根据自己的安全要求和规范对其进行配置。Web 控制台使用标准的 Internet 技术，如 Java、CGI、HTML 和 HTTP。

使用 Web 控制台执行以下操作：

- 将客户端部署到客户机。
- 将客户端组织为逻辑组，以同时进行配置和管理。
- 配置产品设置并在单个组或多个组上启动“手动扫描”。
- 接收威胁相关活动的通知，并查看威胁相关活动的日志报表。
- 接收通知，并且当在客户端上检测到威胁时通过电子邮件发送爆发警报。
- 通过配置并启用“爆发防御”来控制病毒爆发。

打开 Web 控制台

开始之前

从网络上具有下列资源的任何客户机打开 Web 控制台：

- Internet Explorer 7.0 或更高版本

- 分辨率为 1024x768 或更高的增强色显示器
- HTTPS 通道上的 Microsoft Edge

提示

邮件安全客户端服务器控制台不支持 Windows 10 Microsoft Edge 浏览器。

如果您在使用 Edge 浏览器访问控制台时遇到任何问题，请使用 Internet Explorer 7 或更高版本。

过程

1. 可选择下列选项之一打开 Web 控制台：
   - 在托管安全管理服务器的计算机上，转到“台式机”，然后单击“安全无忧软件”快捷方式。
   - 在托管安全管理服务器的计算机上，单击 **Windows 开始菜单** > **趋势科技安全无忧软件** > **安全无忧软件**。
   - 在网络中的任何客户机上，打开 Web 浏览器并在地址栏中键入以下内容：

     `https://{安全管理服务器名称或 IP 地址}:{端口号}/SMB`

     例如：

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

     `http://my-test-server:8059/SMB`

     `http://192.168.0.10:8059/SMB`

     提示

     如果未使用 SSL，请键入 `http` 来代替 `https`。HTTP 连接的缺省端口为 8059，HTTPS 连接的缺省端口为 4343。

     如果该环境不能通过 DNS 解析服务器名称，则使用服务器名称来代替 IP 地址。

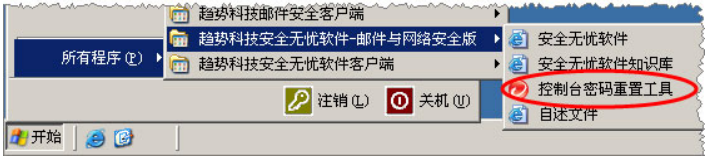
浏览器会显示安全无忧软件登录窗口。

2. 键入密码并单击**登录**。

   浏览器将显示**实时状态**窗口。

后续步骤

如果无法访问 Web 控制台，请检查以下内容。

要检查的项目	详细信息
密码	如果您忘记了密码，请使用控制台密码重置工具重置密码。在安全管理服务器计算机上，可以在 Windows“开始”菜单的 Trend Micro Worry-Free Business Security 文件夹中访问此工具。 
浏览器缓存	如果从早期版本的 WFBS 进行升级，则 Web 浏览器和代理服务器缓存文件可能会阻止 Web 控制台正常加载。请清除浏览器上以及趋势科技安全管理服务器和用于访问 Web 控制台的客户机之间任何代理服务器上的缓存内存。
SSL 证书	请验证确保您的 Web 服务器运行正常。如果正在使用 SSL，请验证确保该 SSL 证书仍然有效。有关详细信息，请参阅您的 Web 服务器文档。

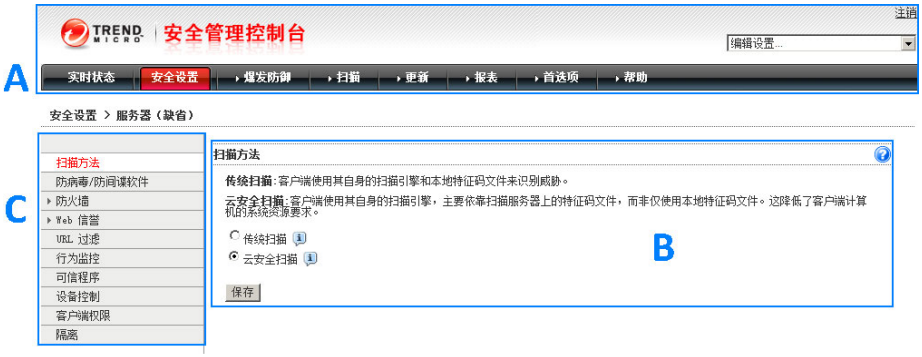
要检查的项目	详细信息

虚拟目录设置	如果在 IIS 服务器上运行 Web 控制台并且出现以下消息，则虚拟目录设置可能存在问题：
	该页无法显示
	`HTTP Error 403.1 - 已禁止：拒绝执行访问。`
	`Internet 信息服务 (IIS)`
	当使用以下任一地址访问控制台时，可能出现此消息：
	`http://{服务器名称}/SMB/`
	`http://{服务器名称}/SMB/default.htm`
	但使用以下地址时，打开控制台可能不会出现任何问题：
	`http://{服务器名称}/SMB/console/html/cgi/cgichkmasterpwd.exe`
	要解决此问题，请检查 SMB 虚拟目录的执行权限。
	启用脚本：
	1. 打开 Internet 信息服务 (IIS) 管理器。
	2. 在 SMB 虚拟目录中，选择**属性**。
	3. 选择“虚拟目录”选项卡并将执行权限从无改为脚本。还可以更改客户端安装虚拟目录的执行权限。

Web 控制台导航

Web 控制台的主要部分

Web 控制台包含以下主要部分：



部分	描述
A. 主菜单	主菜单位于 Web 控制台的顶部。 右上角是一个下拉框，其中包含管理员经常执行的任务的快捷方式。 还提供了**注销**链接，让您能够结束当前会话。
B. 配置区	主菜单项下面是配置区。在此区域中，可以根据您选择的菜单项选择选项。
C. 菜单边栏（并非所有窗口上都提供）	从**安全设置**窗口中选择安全客户端组，然后单击**配置设置**后，会显示菜单边栏。使用边栏可为属于该组的台式机和服务器配置安全设置和扫描。 从“安全设置”窗口中选择邮件安全客户端时（仅限邮件与网络安全版），您可以使用边栏为 Microsoft Exchange Server 配置安全设置和扫描。

Web 控制台的菜单选项

使用 Web 控制台中的以下菜单选项：

菜单选项	描述
实时状态	在安全无忧软件策略中发挥中枢功能。使用“实时状态”可查看有关爆发及严重安全风险的警报与通知。 • 查看趋势科技发布的红色或黄色警报警告 • 查看网络中客户机面临的最新威胁 • 查看 Microsoft Exchange Server 面临的最新威胁（仅限邮件与网络安全版） • 对有风险的客户端部署更新
安全设置	• 为客户端定制安全设置 • 在组之间复制设置
爆发防御	配置并部署爆发防御、漏洞评估和损害清除。
扫描	• 扫描客户机是否存在威胁 • 客户端预设扫描
更新	• 检查趋势科技 ActiveUpdate 服务器（或定制更新源）是否具有更新后的最新组件，包括对病毒码、扫描引擎、清除组件和客户端程序的更新 • 配置更新源 • 将安全客户端指定为更新代理
报表	生成报表，以跟踪威胁和其他安全相关事件
首选项	• 对异常的威胁相关事件或系统相关事件设置通知 • 设置全局设置以便于维护 • 使用管理工具帮助管理网络与客户机的安全 • 查看产品使用授权信息，维护管理员密码，并且通过参与智能反馈计划，帮助保持业务环境中数据信息交换的安全

菜单选项	描述
帮助	• 搜索特定内容和主题 • 查看《管理员指南》 • 访问知识库 (KB) 中的最新信息 • 查看安全、销售、支持和版本信息

Web 控制台图标

下表介绍 Web 控制台上显示的图标，并解释各自的用途。

表 2-2. Web 控制台图标

图标	描述
	“帮助”图标。打开联机帮助。
	“刷新”图标。刷新当前窗口的视图。
	“展开/折叠部分”图标。显示/隐藏各个部分。一次只能展开一个部分。
	“信息”图标。显示有关特定项的信息。
	“定制通知”图标。显示各种通知选项。

实时状态

使用**实时状态**窗口可以获取网络威胁安全性的总体信息。

实时状态窗口中所显示的信息的刷新率各部分并不一样。一般来说，刷新率在 1 到 10 分钟之间。要手动刷新窗口信息，请单击浏览器的**刷新**按钮。

了解图标

这些图标会警告您是否需要采取处理措施。展开一个部分可查看更多信息。可单击表中的项以查看特定信息。要了解有关特定客户端的更多信息，请单击表中显示的编号链接。

表 2-3. “实时状态”图标

图标	描述
	正常 仅有少数客户端需要安装 Patch。您的设备上和网络中的病毒、间谍软件及其他恶意软件活动未表现出明显的风险。

图标	描述
	警告 请采取措施，以免网络上的风险加大。通常，该警告图标表示有一些易受攻击的计算机报告说有很多病毒或其他恶意软件事件。在趋势科技发出黄色警报时，会显示“爆发防御”警告。
	需要采取处理措施 警告图标表示管理员必须采取处理措施才能解决安全问题。

“实时状态”窗口中显示的信息是基于从客户端收集的数据由 WFBS 生成的。

威胁状态

此部分提供以下信息：

表 2-4. “威胁状态”部分和所显示的信息

部分	描述
爆发防御	网络中可能出现的病毒爆发。
防病毒	从通知进行配置后，状态图标会改为显示警告图标。如果您必须采取处理措施： • 安全客户端未成功执行设置要执行的处理措施。单击编号链接可查看有关安全客户端无法执行和对其采取处理措施的计算机的详细信息。 • 在安全客户端上，实时扫描被禁用。单击**立即启用**可重新启动“实时扫描”。 • “实时扫描”在邮件安全客户端上处于禁用状态。
防间谍软件	显示最新的间谍软件扫描结果和间谍软件日志条目。“间谍软件威胁事件”表的**事件数**列显示最新间谍软件扫描的结果。 要了解有关特定客户机的更多信息，请单击“间谍软件威胁事件”表的**检测到的事件数**列下的编号链接。从中可以找到正在感染客户端的特定间谍软件威胁的有关信息。
反垃圾邮件	单击**高**、**中**或**低**链接，重定向到所选 Microsoft Exchange Server 的配置窗口，然后从“反垃圾邮件”窗口设置阈值等级。单击**禁用**将重定向到相应窗口。该信息每小时更新一次。

部分	描述
Web 信誉	由趋势科技确定的潜在危险 Web 站点。
URL 过滤	由管理员确定的受限 Web 站点。
行为监控	行为监控策略违例。
网络病毒	由防火墙设置确定的检测。
设备控制	限制对 USB 设备和网络驱动器的访问 **注意** WFBS 支持通过 USB 接口连接的所有种类的存储设备，智能电话和数码相机除外。

系统状态

此部分显示有关已安装客户端的客户机上更新的组件和可用空间的信息。

表 2-5. “系统状态”部分和所显示的信息

部分	描述
组件更新	更新的组件在客户端上的部署的组件更新状态。
云安全扫描	无法连接到扫描服务器的安全客户端。 **注意** 扫描服务器是托管在安全管理服务器上的一项服务。
系统异常事件	有关用作服务器的客户机（运行服务器操作系统）的磁盘空间信息。

为触发 Web 控制台使之显示“警告”或“需要采取处理措施”图标，可以在**管理** > **通知**中定制触发参数。

使用授权状态

此部分显示有关产品使用授权状态的信息，特别是过期信息。

实时状态更新间隔

要了解更新“实时状态”信息的频率，请参阅下表。

表 2-6. 实时状态更新间隔

项目	更新时间间隔（分钟）	多长时间之后客户端将日志发送到服务器（分钟）
爆发防御	3	N/A
防病毒	1	安全客户端：立即 邮件安全客户端：5
防间谍软件	3	1
反垃圾邮件	3	60
Web 信誉	3	立即
URL 过滤	3	立即
行为监控	3	2
网络病毒	3	2
设备控制	3	2
云安全扫描	60	N/A
使用授权	10	N/A
组件更新	3	N/A
系统异常事件	10	在启动侦听服务 TmListen 时

第 3 章

安装客户端

本章说明安装安全客户端和邮件安全客户端（仅限邮件与网络安全版）所需执行的必要步骤。此外，还提供有关移除这些客户端的信息。

安全客户端安装

在 Windows 客户机（台式机和服务器）上执行安全客户端的全新安装。使用最能满足您的需求的安装方法。

安装安全客户端前，请关闭客户机上所有正在运行的应用程序。如果在有其他应用程序运行时安装，安装过程有可能花费较长时间才能完成。

注意

有关将安全客户端升级到此版本的信息，请参阅《*安装和升级指南*》。

安全客户端安装要求

有关安装要求和可兼容第三方产品的完整列表，请访问以下 Web 站点：

http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security.aspx

安全客户端安装注意事项

安装安全客户端之前，请先考虑以下因素：

- **客户端功能：**某些安全客户端功能在特定 Windows 平台上不可用。有关详细信息，请参阅可用的安全客户端功能 第 3-3 页。
- **x64 平台：**安全客户端提供了针对 x64 平台的简缩版。但是，当前对于 IA-64 平台不提供支持。
- **IPv6 支持：**安全客户端可以安装在双栈或纯 IPv6 客户机上。但是：
  - 某些可安装客户端的 Windows 操作系统不支持 IPv6 寻址。
  - 对于某些安装方法，成功安装客户端具有特殊的要求。

  有关详细信息，请参阅安全客户端安装和 IPv6 支持 第 3-6 页。

- **例外列表**:确保已正确配置以下功能的例外列表：
  - **行为监控**：将关键的客户机应用程序添加到“允许的程序”列表，以防止安全客户端阻止这些应用程序。有关更多信息，请参阅配置行为监控 第 5-19 页。
  - **Web 信誉**：将认为安全的 Web 站点添加到“允许的 URL”列表，以防止安全客户端阻止对这些 Web 站点的访问。有关更多信息，请参阅为安全客户端配置 Web 信誉 第 5-15 页。
- **客户端安装目录**：在安全管理服务器安装期间，安装程序会提示您指定客户端安装目录，缺省情况下为 `$ProgramFiles\Trend Micro\Security Agent`。如果想要将安全客户端安装到其他目录，请在**首选项** > **全局设置** > **系统** > **安全客户端安装**部分指定新目录。

可用的安全客户端功能

客户机上的可用安全客户端功能取决于客户机的操作系统。将客户端安装到特定操作系统时，请了解不受支持的功能。

表 3-1. 安全客户端功能

功能	Windows 操作系统								
	XP	Vista	7	8/8.1	10	Server/SBS 2003	Server/SBS 2008	Server 2008 R2/SBS 2011	Server 2012/R2
手动扫描、实时扫描和预设扫描	是	是	是	是	是	是	是	是	是
防火墙	是	是	是	是	是	是	是	是	是
Web 信誉	是	是	是	是	是	是	是	是	是

功能	Windows 操作系统								
	XP	Vista	7	8/8.1	10	Server/SBS 2003	Server/SBS 2008	Server 2008 R2/SBS 2011	Server 2012/R2
URL 过滤	是	是	是	是	是	是	是	是	是
行为监控	是（32 位） 否（64 位）	是（32/64 位） 否（64 位，不带 SP1）	是	是	是	是（32 位） 否（64 位）	是	是	是
设备控制	是（32 位） 否（64 位）	是（32/64 位） 否（64 位，不带 SP1）	是	是	是	是（32 位） 否（64 位）	是	是	是
损害清除服务	是	是	是	是	是	是	是	是	是
邮件扫描 (POP3)	是	是	是	是	是	是	是	是	是
手动和预设更新	是	是	是	是	是	是	是	是	是
更新代理	是	是	是	是	是	是	是	是	是

功能	Windows 操作系统								
	XP	Vista	7	8/8.1	10	Server/SBS 2003	Server/SBS 2008	Server 2008 R2/SBS 2011	Server 2012/R2
客户端插件管理器	是	是	是	是	是	是	是	是	是
智能反馈	是	是	是	是	是	是	是	是	是
趋势科技反垃圾邮件工具栏	是（32 位） 否（64 位）	是	是	是	是	否	否	否	否
	支持的电子邮件客户端： • Microsoft Outlook 2003（32 位）、2007（32 位）、2010（32 和 64 位）、2013（32 和 64 位） • Outlook Express 6.0，含 Service Pack 2 或更高版本 • Windows Mail 6.0 • Windows Live Mail 2011 和 2012								
HouseCall	是	是	是	是	是	是	是	是	是
案例诊断工具	是	是	是	是	是	是	是	是	是
Wi-Fi Advisor	是	是	是	是	是	否	否	否	否

安全客户端安装和 IPv6 支持

本主题讨论将安全客户端安装到双栈或纯 IPv6 客户机时的注意事项。

操作系统

安全客户端只能安装在以下支持 IPv6 寻址的操作系统上：

- Windows Vista（所有版本）
- Windows Server 2008/2008 R2（所有版本）
- Windows 7（所有版本）
- Windows SBS 2008/2011
- Windows 8/8.1（所有版本）
- Windows 10（所有版本）
- Windows Server 2012/2012 R2（所有版本）

有关系统要求的完整列表，请访问以下 Web 站点：

http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security.aspx

支持的安装方法

可以使用所有可用的安装方法将安全客户端安装在纯 IPv6 或双栈客户机上。对于某些安装方法，成功安装安全客户端具有特殊的要求。

表 3-2. 安装方法和 IPv6 支持

安装方法	要求/考虑事项
内部 Web 页和电子邮件通知安装	如果您要安装到纯 IPv6 客户机，则安全管理服务器必须为双栈或纯 IPv6 服务器，而且其主机名称或 IPv6 地址必须是 URL 的一部分。 对于双栈客户机，安装状态窗口中显示的 IPv6 地址取决于在以下部分中选择的选项：**首选项** > **全局设置** > **安全客户端**选项卡中的**首选 IP 地址**部分。

安装方法	要求/考虑事项
漏洞扫描程序和远程安装	纯 IPv6 安全管理服务器无法在纯 IPv4 客户机上安装安全客户端。同样，纯 IPv4 安全管理服务器无法在纯 IPv6 客户机上安装客户端。

安全客户端 IP 地址

安装在支持 IPv6 寻址的环境中的安全管理服务器可以管理下列安全客户端：

- 安装在纯 IPv6 客户机上的安全管理服务器可以管理纯 IPv6 安全客户端。
- 安装在双栈客户机上且已指定 IPv4 和 IPv6 地址的安全管理服务器可以管理纯 IPv6、双栈和纯 IPv4 安全客户端。

安装或升级安全客户端之后，客户端会使用 IP 地址向安全管理服务器注册。

- 纯 IPv6 安全客户端会使用其 IPv6 地址进行注册。
- 纯 IPv4 安全客户端会使用其 IPv4 地址进行注册。
- 双栈安全客户端会使用其 IPv4 或 IPv6 地址进行注册。在**首选项** > **全局设置** > **安全客户端**选项卡中的**首选 IP 地址**部分中，可以选择这些客户端将使用的 IP 地址。

安全客户端安装方法

本节概要介绍执行安全客户端全新安装的不同安装方法。所有安装方法都需要目标客户机上的本地管理员权限。

如果您要安装安全客户端且要启用 IPv6 支持，请阅读安全客户端安装和 IPv6 支持 第 3-6 页中的准则。

表 3-3. 安装方法

安装方法/操作系统支持	部署注意事项					
	WAN 部署	集中管理	要求用户干预	要求 IT 资源	大规模部署	占用的带宽
内部 Web 页 所有操作系统都支持	是	是	是	否	否	低（如果已预设）
电子邮件通知 所有操作系统都支持	是	是	是	否	否	高，如果安装同时启动
远程安装 除以下操作系统外的所有操作系统都支持： • Windows Vista Home Basic 和 Home Premium 版 • Windows XP Home 版 • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 Basic • Windows 10 Home	否	是	否	是	是	低（如果已预设）
登录脚本安装 所有操作系统都支持	否	是	否	是	是	高，如果安装同时启动
客户端打包程序 所有操作系统都支持	是	否	是	是	否	低（如果已预设）

安装方法/操作系统支持	部署注意事项					
	WAN 部署	集中管理	要求用户干预	要求 IT 资源	大规模部署	占用的带宽
趋势科技漏洞扫描程序 (TMVS) 除以下操作系统外的所有操作系统都支持： • Windows Vista Home Basic 和 Home Premium 版 • Windows XP Home 版 • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 Basic • Windows 10 Home	否	是	否	是	是	低（如果已预设）

对于单站点部署和在严格强制实施 IT 策略的组织中，IT 管理员可以选择使用**远程安装**或**登录脚本安装**进行部署。

在并非严格强制实施 IT 策略的组织中，趋势科技建议使用**内部 Web 页**安装安全客户端。但是，使用此方法要求安装安全客户端的最终用户具有管理员权限。

对于使用 Active Directory 的网络，**远程安装**效率较高。如果您的网络未使用 Active Directory，请使用“内部 Web 页”。

从内部 Web 页安装

开始之前

要从内部 Web 页安装，需要满足以下条件：

要检查的项目	要求
安全管理服务器	安全管理服务器安装必须满足以下条件： • 安装在 Windows XP、Vista、7、8、8.1、Server 2003/2008/2008 R2/2012/2012 R2 或 SBS 2003/2008/2011 上 • 具备 Internet Information Server (IIS) 6.0、7.0、7.5、8.0、8.5 或 Apache 2.0.6x
目标客户机	• 目标客户机上必须安装 Internet Explorer 7.0 或更高版本。 • 用户必须使用管理员帐户登录客户机。 **注意** 如果目标客户机运行 Windows 7，则首先启用内置管理员帐户。缺省情况下，Windows 7 禁用内置管理员帐户。有关详细信息，请参考 Microsoft 支持站点 (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx)。
运行 Windows XP、7、8、8.1、10、Vista、Server 2003、2008、2008 R2、2012、2012 R2 或 SBS 2003、2008、2011 的目标客户机	用户必须执行以下步骤： 1. 启动 Internet Explorer，并将安全管理服务器 URL（例如 `https://<安全管理服务器名称>:4343/SMB/console/html/client`）添加到可信站点列表。在 Windows XP 上，通过转到**工具** > **Internet 选项** > **安全**选项卡，然后选择**可信站点**图标并单击**站点**，来访问该列表。 2. 修改 Internet Explorer 安全设置以启用 **ActiveX 控件自动提示**。在 Windows XP 上，转到**工具** > **Internet 选项** > **安全**选项卡，然后单击**自定义级别**。
运行 Windows Vista 的目标客户机	用户必须启用受保护模式。要启用受保护模式，请在 Internet Explorer 中单击**工具** > **Internet 选项** > **安全**选项卡。

要检查的项目	要求
IPv6	如果您的环境是包含纯 IPv4、纯 IPv6 和双栈客户机的混合环境，则安全管理服务器必须具有 IPv4 和 IPv6 地址，以便所有客户机都可以连接到安全管理服务器上的内部 Web 页。

从内部 Web 页向用户发送以下指导信息，以安装安全客户端。要通过电子邮件发送安装通知，请参阅使用电子邮件通知安装 第 3-28 页。

过程

1. 使用管理员帐户登录客户机。
2. 打开 Internet Explorer 窗口，然后键入以下内容之一：
   - 具有 SSL 的安全管理服务器：

     `https://<`**安全管理服务器名称或 IP 地址**`>:4343/SMB/console/html/client`

   - 无 SSL 的安全管理服务器：

     `http://<`**安全管理服务器名称或 IP 地址**`>:8059/SMB/console/html/client`

3. 单击**立即安装**开始安装安全客户端。

   安装开始。出现提示时，允许 ActiveX 控件安装。安装后，安全客户端的图标将出现在 Windows 任务栏中。

   注意

   有关显示在 Windows 任务栏中的图标列表，请参阅检查安全客户端状态 第 A-2 页。

后续步骤

如果用户报告无法从内部 Web 页进行安装，请尝试以下方法。

- 使用 ping 和 telnet 来验证客户端-服务器通信是否存在。

- 检查客户端上的 TCP/IP 是否已启用并正确配置。
- 如果客户端-服务器通信使用代理服务器，请检查代理服务器设置是否正确配置。
- 在 Web 浏览器中，删除趋势科技加载项及浏览历史记录。

使用登录脚本安装进行安装

登录脚本安装可以在不受保护的客户机登录到网络时，将安全客户端自动安装到这些客户机上。“登录脚本安装”会向服务器登录脚本中添加一个名为 `AutoPcc.exe` 的程序。

`AutoPcc.exe` 将安全客户端安装到不受保护的客户机并更新程序文件和组件。客户机必须属于域，才能通过登录脚本使用 AutoPcc。

如果您已经具有现有登录脚本，登录脚本安装会追加一条执行 `AutoPcc.exe` 的命令。否则，将创建一个名为 `ofcscan.bat` 的批处理文件，其中包含运行 `AutoPcc.exe` 的命令。

“登录脚本安装”会在脚本末尾追加以下内容：

`\\<`**服务器名称**`>\ofcscan\autopcc`

其中：

- <**服务器名称**> 是安全管理服务器计算机的计算机名称或 IP 地址。
- "`ofcscan`" 是安全管理服务器上的共享文件夹名称。
- "`autopcc`" 是安装安全客户端的 autopcc 可执行文件的链接。

所有 Windows Server 版本上的登录脚本位置（通过网络登录共享目录）：

```
\\Windows server\system drive\windir\sysvol\domain\scripts
\ofcscan.bat
```

过程

1. 在用来运行服务器安装的计算机上，打开 <**安全管理服务器安装文件夹**> `\PCCSRV\Admin`。

2. 双击 `SetupUsr.exe`。

   登录脚本安装实用程序载入。将在控制台上以树形显示网络上的所有域。

3. 找到要修改登录脚本的服务器，选中该服务器，然后单击**选择**。确保该服务器是主要域控制器，并确保您具有对该服务器的管理员访问权限。

   “登录脚本安装”会提示输入用户名和密码。

4. 键入用户名和密码。单击**确定**继续。

   出现**用户选择**窗口。**用户**列表将显示登录到该服务器上的用户的概要文件。**选定的用户**列表将显示要修改其登录脚本的用户配置文件。

5. 要修改用户配置文件的登录脚本，请从“用户”列表中选择用户配置文件，然后单击**添加**。

6. 要修改所有用户的登录脚本，请单击**全部添加**。

7. 要排除先前选择的用户配置文件，请从**选定的用户**列表中选择该名称，然后单击**删除**。

8. 要重置选择，请单击**全部删除**。

9. 当所有目标用户配置文件都出现在**选定的用户**列表中时，单击**应用**。

   将显示一条消息提示您已成功修改了服务器登录脚本。

10. 单击**确定**。

    “登录脚本安装”将返回到其初始窗口。

11. 要关闭“登录脚本安装”，请单击**退出**。

使用客户端打包程序安装

客户端打包程序可创建安装包，而且您可以使用常规介质（如 CD-ROM）将安装包发送给用户。用户可以在客户机上运行该软件包，以安装或升级安全客户端并更新组件。

客户机打包程序在以下情况下尤其有用：

- 在低带宽远程办公室中，为客户机部署安全客户端或组件。
- 您的环境限制您连接到 Internet，例如在封闭的局域网中或没有 Internet 连接。

使用客户机打包程序安装的安全客户端会向服务器报告创建软件包的位置。

过程

1. 在安全管理服务器计算机上，浏览到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\ClientPackager。
2. 双击 ClnPack.exe。

   客户端打包程序控制台将打开。
3. 选择要为其创建软件包的操作系统。仅将软件包部署到运行该操作系统类型的客户机。创建另一个软件包以部署到其他操作系统类型。
4. 选择软件包的扫描方法。

   有关扫描方法的详细信息，请参阅扫描方法 第 5-3 页。

   软件包中包括的组件取决于所选的扫描方法。对于云安全扫描，将包括除传统病毒码之外的所有组件。对于传统扫描，除云安全客户端病毒码以外的所有组件都将包含在内。
5. 选择要创建的软件包类型。

表 3-4. 客户端软件包类型

软件包类型	描述
安装	选择**安装**，将软件包创建为 MSI 文件，以符合 Microsoft 安装程序软件包格式。软件包安装安全客户端程序以及安全管理服务器上当前可用的组件。 如果目标客户机安装了早期版本的安全客户端，并且您想要升级，则需要从管理该客户端的安全管理服务器上创建 MSI 文件。否则，客户端将不会升级。

软件包类型	描述
更新	选择**更新**可创建一个包含安全管理服务器上当前可用组件的软件包。软件包将创建为可执行文件。如果在安装了安全客户端的客户机上更新组件时出现问题，则可以使用此软件包。

6. 单击**静默模式**，以创建在客户机后台安装的软件包，客户机用户注意不到，也不显示安装状态窗口。如果打算将软件包远程部署到客户机，请启用此选项。

7. 如果不想在安装安全客户端之前扫描客户机威胁，请单击**禁用预扫描 (仅适用于全新安装)**。只有在确定客户机不存在威胁的情况下才执行此操作。

   如果启用预扫描，则安装程序将扫描计算机的最易受攻击区域以查找病毒/恶意软件，最易受攻击区域包括：

   - 引导区和引导目录（检查引导区病毒）
   - Windows 文件夹
   - Program files 文件夹

8. 再选择**源文件**，确保 `ofcscan.ini` 文件的位置正确。要修改路径，请单击 (...) 以浏览 `ofcscan.ini` 文件。缺省情况下，此文件位于 <**服务器安装文件夹**>\`PCCSRV` 下。

9. 在输出文件中，单击 (...) 以指定要创建软件包的位置，然后键入软件包文件名（例如 `ClientSetup.exe`）。

10. 单击**创建**。

    客户端打包程序创建完软件包后，将出现“成功创建软件包”消息。找到位于上一步骤指定的目录中的软件包。

后续步骤

将软件包部署到客户机。

客户机要求：

- 1GB 可用磁盘空间（针对软件包的扫描方法是传统扫描）或 500MB 可用磁盘空间（针对软件包的扫描方法是云安全扫描）
- Windows Installer 3.0 （运行 MSI 软件包）

软件包部署准则：

- 将软件包发送给用户，请他们在计算机上通过双击文件（`.msi` 或 `.exe`）来运行软件包。

> **注意**
> 仅把软件包发送给其安全客户端向创建该软件包的服务器报告的用户。

- 如果您的用户将在运行 Windows Vista、7、8/8.1、10、Server 2008、SBS 2011、Server 2012 或 Server 2012 R2 的计算机上运行 `.exe` 软件包，请指示他们右键单击 `.exe` 文件并选择**以管理员身份运行**。
- 如果使用 Active Directory，您可以使用 `.msi` 文件，自动将安全客户端同时部署到所有客户机，无需每个用户自己安装安全客户端。使用**计算机配置**而非（**用户配置**），以确保无论哪个登录到客户机的用户都可安装安全客户端。
- 如果新安装的安全客户端无法连接到安全管理服务器，则安全客户端将保留缺省设置。安全客户端连接到安全管理服务器时，将获得 Web 控制台中其所在组的设置。
- 如果使用客户机打包程序升级安全客户端时遇到问题，趋势科技建议先卸载早期版本的安全客户端，然后再安装新版本。有关卸载的指导信息，请参阅移除客户端 第 3-34 页。

以远程安装方式安装

开始之前

将安全客户端远程安装到连接到网络的一台或多台客户机上。

要使用远程安装进行安装，需要满足以下条件：

要检查的项目	要求
目标客户机	• 使用管理员帐户登录每台目标客户机。 **注意** 如果目标客户机运行 Windows 7，则首先启用内置管理员帐户。缺省情况下，Windows 7 禁用内置管理员帐户。有关详细信息，请参考 Microsoft 支持站点 (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx)。 • 目标客户机上不能有已安装的安全管理服务器。远程安装不会在已经运行安全管理服务器的客户机上安装安全客户端。
运行 Windows Vista、7、8/8.1、10、Server 2008、2012/2012 R2 或 SBS 2011 的目标客户端	执行以下任务： **注意** 在 Windows 8/8.1 或 10 上执行远程安装时，不能通过 Microsoft 帐户登录到目标客户端 1. 在客户端上，临时启用“文件和打印机共享”。 **注意** 如果公司的安全策略是禁用 Windows 防火墙，则直接执行步骤 2 启动 Remote Registry 服务。 a. 在“控制面板”中打开 Windows 防火墙。 b. 单击**允许程序通过 Windows 防火墙**。如果系统提示输入管理员密码或进行确认，请键入密码或提供确认。此时将显示 Windows 防火墙设置。 c. 在**例外**选项卡的**程序或端口列表**下，请确保**文件和打印机共享**的复选框已选中。 d. 单击**确定**。 2. 禁用用户帐户控制。

要检查的项目	要求
	注意 对于 Windows 8/8.1、10 或 2012/2012 R2：修改以下注册表项以关闭用户帐户控制：`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` “`EnableLUA`”=`dword:00000000`。 3. 临时启动 Remote Registry 服务。 a. 打开 Microsoft 管理控制台。 **注意** 在“运行”窗口中键入 `services.msc`，打开 Microsoft 管理控制台。 b. 右键单击 **Remote Registry**，然后选择**启动**。 4. 在 Windows Vista、7、8/8.1 或 10 客户端上安装安全客户端后，如果有必要可恢复原始设置。
运行 Windows XP 的目标客户机	在客户机上，暂时禁用“简单文件共享”： 1. 打开 Windows 资源管理器。 2. 单击**工具** > **文件夹选项**。 3. 在“查看”选项卡中，取消选中**使用简单文件共享 (建议)**。 4. 单击**应用**。
IPv6	双栈安全管理服务器可以将安全客户端安装到任何客户机。纯 IPv6 安全管理服务器只能将安全客户端安装到纯 IPv6 或双栈客户机。

过程

1. 在 web 控制台中，导航至**安全设置** > **添加计算机**。

   此时打开一个新窗口。

2. 从**计算机类型**部分选择**台式机或服务器**。

3. 从**方法**部分选择**远程安装**。

4. 单击**下一步**。

   将显示一个新窗口。

5. 从**组与计算机**框中的客户机列表中，选择一台客户机，然后单击**添加**。此时会出现提示，要求输入客户机的用户名和密码。

6. 键入您的用户名和密码，然后单击**登录**。客户机会显示在**选定的计算机**列表框中。

7. 重复上述步骤，直到**选定的计算机**列表框中显示所有客户机。

8. 单击**安装**。

   此时会显示一个确认框。

9. 单击**是**确认要将客户端安装到客户机上。

   当程序将安全客户端文件复制到每台客户机上时，将显示进度窗口。

   在客户机上完成安全管理服务器安装后，安装状态将显示在**选定的计算机**列表框的**状态**文本框中，而且客户机名称带有绿色复选标记。

后续步骤

如果通过远程安装执行的安装不成功，则请执行以下任务：

- 使用 ping 和 telnet 来验证客户端-服务器通信是否存在。
- 检查客户端上的 TCP/IP 是否已启用并正确配置。
- 如果客户端-服务器通信使用客户端服务器，请检查客户端服务器设置是否配置正确。
- 在 Web 浏览器中，删除趋势科技加载项及浏览历史记录。

使用漏洞扫描程序安装

开始之前

运行漏洞扫描可以检测已安装的防病毒解决方案、搜索网络上不受保护的客户机，并在客户机上安装安全客户端。

要使用漏洞扫描程序进行安装，需要满足以下条件：

要检查的项目	要求
启动漏洞扫描程序的位置	您可以在安全管理服务器或网络中的任何客户机上启动漏洞扫描程序。客户机上不应运行终端服务器。
目标客户机	• 目标客户机上不能有已安装的安全管理服务器。漏洞扫描程序不会在已经运行安全管理服务器的客户机上安装安全客户端。 • 用户必须使用管理员帐户登录客户机。 **注意** 如果目标客户机运行 Windows 7，则首先启用内置管理员帐户。缺省情况下，Windows 7 禁用内置管理员帐户。有关详细信息，请参考 Microsoft 支持站点 (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx)。

有多种方法可以运行漏洞扫描。

- 运行手动漏洞扫描 第 3-20 页
- 运行 DHCP 扫描 第 3-22 页
- 配置预设漏洞扫描 第 3-24 页

运行手动漏洞扫描

按需运行漏洞扫描。

过程

1. 启动漏洞扫描程序。

要在以下机器上启动漏洞扫描程序：	步骤
安全管理服务器	a. 导航至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS。 b. 双击 TMVS.exe。
网络中的客户机	a. 在安全管理服务器上，导航至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility。 b. 将 TMVS 文件夹复制到另一台客户机。 c. 在另一台客户机上，打开 TMVS 文件夹，然后双击 TMVS.exe。

2. 转至**手动扫描**部分。
3. 键入要检查的客户机的 IP 地址范围。
   a. 键入 IPv4 地址范围。

   注意
   如果在纯 IPv4 或双栈客户机上运行漏洞扫描程序，它只能查询 IPv4 地址范围。漏洞扫描程序仅支持 B 类 IP 地址范围，例如，168.212.1.1 到 168.212.254.254。

   b. 对于 IPv6 地址范围，请键入 IPv6 前缀和长度。

   注意
   如果在纯 IPv6 或双栈客户机上运行漏洞扫描程序，它只能查询 IPv6 地址范围。

4. 单击**设置**。

   显示**设置**窗口。
5. 配置漏洞扫描设置。有关详细信息，请参阅漏洞扫描设置 第 3-26 页。
6. 单击**确定**。

   “设置”窗口将关闭。

7. 单击**开始**。

   漏洞扫描结果将显示在**手动扫描**选项卡下的**结果**表中。

   注意

   如果计算机运行的是 Windows Server 2008，则在**结果**表中不显示 MAC 地址信息。

8. 要将结果保存为逗号分隔值 (CSV) 文件，请单击**导出**，找到要保存该文件的文件夹，键入文件名称，然后单击**保存**。

运行 DHCP 扫描

对从 DHCP 服务器请求 IP 地址的客户机运行漏洞扫描。

漏洞扫描程序侦听端口 67（DHCP 服务器针对 DHCP 请求的侦听端口）。如果它检测到来自客户机的 DHCP 请求，则会在该客户机上运行漏洞扫描。

注意

如果您在 Windows Server 2008 或 Windows 7 上启动漏洞扫描程序，则它无法检测 DHCP 请求。

过程

1. 在位于以下文件夹的 `TMVS.ini` 文件中配置 DHCP 设置：<**服务器安装文件夹**>`\PCCSRV\Admin\Utility\TMVS`。

   表 3-5. `TMVS.ini` 文件中的 DHCP 设置

设置	描述
DhcpThreadNum=x	指定 DHCP 模式的线程数。最小值为 3，最大值为 100。缺省值为 3。
DhcpDelayScan=x	这是检查请求计算机已安装防病毒软件前的延迟时间。 最小值为 0（不等待），最大值为 600。缺省值为 60。

设置	描述
LogReport=x	0 表示禁用日志记录，1 表示启用日志记录。 漏洞扫描程序将扫描结果发送到 WFBS 服务器。日志显示在 Web 控制台的 **系统事件日志**窗口中。
OsceServer=x	这是 WFBS 服务器的 IP 地址或 DNS 名称。
OsceServerPort=x	这是 WFBS 服务器上的 Web 服务器端口。

2. 启动漏洞扫描程序。

要在以下机器上启动漏洞扫描程序：	步骤
安全管理服务器	a. 导航至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS。 b. 双击 TMVS.exe。
网络中的客户机	a. 在安全管理服务器上，导航至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility。 b. 将 TMVS 文件夹复制到另一台客户机。 c. 在另一台客户机上，打开 TMVS 文件夹，然后双击 TMVS.exe。

3. 在**手动扫描**部分旁边，单击**设置**。

   显示**设置**窗口。

4. 配置漏洞扫描设置。有关详细信息，请参阅漏洞扫描设置 第 3-26 页。

5. 单击**确定**。

   “设置”窗口将关闭。

6. 在**结果**表中，单击 **DHCP 扫描**选项卡。

注意

DHCP 扫描选项卡在运行 Windows Server 2008 和 Windows 7 的计算机上不可用。

7. 单击 **DHCP 启动**。

   漏洞扫描程序开始侦听 DHCP 请求并在客户机登录到网络时对其执行漏洞检查。

8. 要将结果保存为逗号分隔值 (CSV) 文件，请单击**导出**，找到要保存该文件的文件夹，键入文件名称，然后单击**保存**。

配置预设漏洞扫描

漏洞扫描将根据安排自动运行。

过程

1. 启动漏洞扫描程序。

要在以下机器上启动漏洞扫描程序：	步骤
安全管理服务器	a. 导航至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS。 b. 双击 TMVS.exe。
网络中的客户机	a. 在安全管理服务器上，导航至 <**服务器安装文件夹**>\PCCSRV\Admin\Utility。 b. 将 TMVS 文件夹复制到另一台客户机。 c. 在另一台客户机上，打开 TMVS 文件夹，然后双击 TMVS.exe。

2. 转至**预设扫描**部分。
3. 单击**添加/编辑**。

   将显示**预设扫描**窗口。

4. 键入预设漏洞扫描的名称。
5. 键入要检查的计算机的 IP 地址范围。

a. 键入 IPv4 地址范围。

注意

如果在纯 IPv4 或具有可用的 IPv4 地址的双栈主机上运行漏洞扫描程序，它只能查询 IPv4 地址范围。漏洞扫描程序仅支持 B 类 IP 地址范围，例如，168.212.1.1 到 168.212.254.254。

b. 对于 IPv6 地址范围，请键入 IPv6 前缀和长度。

注意

如果在纯 IPv6 或具有可用的 IPv6 地址的双栈主机上运行漏洞扫描程序，它只能查询 IPv6 地址范围。

6. 使用 24 小时制格式指定开始时间，然后选择扫描将运行的频率。从每天一次、每周一次或每月一次中进行选择。

7. 如果已配置手动漏洞扫描设置，且希望使用这些设置，请选择**使用当前设置**。有关手动漏洞扫描设置的详细信息，请参阅运行手动漏洞扫描 第 3-20 页。

   如果未指定手动漏洞扫描设置，或者希望使用另一组设置，请选择**修改设置**，然后单击**设置**。显示**设置**窗口。配置扫描设置，然后单击**确定**。有关详细信息，请参阅漏洞扫描设置 第 3-26 页。

8. 单击**确定**。

   预设扫描窗口将关闭。您创建的预设漏洞扫描将显示在**预设扫描**部分下。如果已启用通知，漏洞扫描程序会将预设漏洞扫描结果发送给您。

9. 要立即执行预设漏洞扫描，请单击**立即运行**。

   漏洞扫描结果将显示在**预设扫描**选项卡下的**结果**表中。

注意

如果计算机运行的是 Windows Server 2008，则在**结果**表中不显示 MAC 地址信息。

10. 要将结果保存为逗号分隔值 (CSV) 文件，请单击**导出**，找到要保存该文件的文件夹，键入文件名称，然后单击**保存**。

11. 要停止运行预设漏洞扫描，请转到**预设扫描**部分，选择预设扫描，然后单击**删除**。

漏洞扫描设置

运行漏洞扫描时，请配置以下设置。有关不同漏洞扫描类型的详细信息，请参阅使用漏洞扫描程序安装 第 3-19 页。

设置	描述和指导信息
产品查询	漏洞扫描程序可以检查目标客户机上是否有安全软件。 1. 选择要检查的安全软件。 2. 漏洞扫描程序使用窗口上显示的缺省端口来检查软件。如果软件管理员更改了缺省端口，则需要执行必要的更改，否则漏洞扫描程序不会检测软件。 3. 对于 Norton Antivirus Corporate Edition，可以通过单击**设置**来更改超时设置。
	其他产品查询设置 要设置漏洞扫描程序同时检查有无安全软件的客户机数量： 1. 导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\TMVS，然后使用文本编辑器（如记事本）打开 TMVS.ini。 2. 要设置检查的客户机数量： • 对于手动漏洞扫描，更改 ThreadNumManual 的值。指定一个 8 至 64 之间的值。 例如，如果希望漏洞扫描程序在同一时间检查 60 台客户机，则键入 ThreadNumManual=60。 • 对于预设漏洞扫描，更改 ThreadNumSchedule 的值。指定一个 8 至 64 之间的值。 例如，如果希望漏洞扫描程序在同一时间检查 50 台客户机，则键入 ThreadNumSchedule=50。 3. 保存 TMVS.ini。

设置	描述和指导信息
描述检索设置	当漏洞扫描程序可以 "ping" 客户机时，它可以检索客户机的其他相关信息。检索信息的方法有两种： • **标准检索**：检索域信息和计算机信息 • **快速检索**：只检索计算机名称
警报设置	自动将漏洞扫描结果发送给您或贵组织中的其他管理员： 1. 选择**通过电子邮件将结果发送给系统管理员**。 2. 单击**配置**，以指定电子邮件设置。 3. 在**收件人**栏中，键入收件人的电子邮件地址。 4. 在**发件人**中，键入发件人的电子邮件地址。 5. 在 **SMTP 服务器**中，键入 SMTP 服务器地址。 例如，键入 `smtp.company.com`。SMTP 服务器信息是必需的。 6. 在**主题**中，为该消息键入新的主题或接受缺省主题。 7. 单击**确定**。 通知用户其计算机未安装安全软件： 1. 选择**在不受保护的计算机上显示通知**。 2. 单击**定制**来配置通知消息。 3. 在**通知消息**窗口中，键入新消息或接受缺省消息。 4. 单击**确定**。
另存为 CSV 文件	将漏洞扫描结果保存到一个逗号分隔值 (CSV) 文件。 文件将保存到启动了漏洞扫描程序的客户机。接受缺省文件路径或根据喜好进行更改。

设置	描述和指导信息
Ping 设置	使用 "ping" 设置来验证客户机是否存在并确定其操作系统。如果这些设置已禁用，漏洞扫描程序将扫描指定 IP 地址范围中的所有 IP 地址（甚至包含任何客户机上未使用的地址），因此扫描时间会比预期久。 1. 在**数据包大小**和**超时**文本框中，接受或修改缺省值。 2. 选择**使用 ICMP OS 指纹验证来检测操作系统的类型**。 如果选择此选项，漏洞扫描程序可确定客户机运行的是 Windows 操作系统还是其他操作系统。对于运行 Windows 的客户机，漏洞扫描程序可识别其 Windows 版本。
	其他 Ping 设置 要设置漏洞扫描程序同时 ping 的客户机数量： 1. 导航到 `<服务器安装文件夹>\PCCSRV\Admin\Utility\TMVS`，然后使用文本编辑器（如记事本）打开 `TMVS.ini`。 2. 更改 `EchoNum` 的值。指定一个 1 至 64 之间的值。 例如，如果希望漏洞扫描程序同时 ping 60 台客户机，请键入 `EchoNum=60`。 3. 保存 `TMVS.ini`。
安全管理服务器设置	1. 选择**在不受保护的计算机上自动安装安全客户端**，以将安全客户端安装到漏洞扫描程序将要扫描的客户机上。 2. 键入安全管理服务器主机名称或 IPv4/IPv6 地址以及端口号。通过漏洞扫描程序安装的安全客户端将向此服务器报告。 3. 配置在登录客户机时使用的管理凭证，方法是：单击**安装帐户**，在**帐户信息**窗口中键入用户名和密码，然后单击**确定**。

使用电子邮件通知安装

使用此安装方法可发送一封带有指向安装程序的链接的电子邮件。

过程

1. 在 Web 控制台中，导航至**安全设置** > **添加计算机**。

   此时打开一个新窗口。

2. 从**计算机类型**部分选择**台式机或服务器**。

3. 从**方法**部分选择**电子邮件通知安装**。

4. 单击**下一步**。

   将显示一个新窗口。

5. 键入电子邮件主题和收件人。

6. 单击**应用**。缺省的电子邮件客户端将打开（带有收件人、主题和指向安装程序的链接）。

迁移到安全客户端

安装安全客户端时，安装程序将检查在客户机上安装的任何趋势科技或第三方端点安全软件。

安装程序可执行以下处理措施：

- 移除当前安装在客户机上的其他端点安全软件，并使用安全客户端替换
- 检测其他端点安全软件，但不移除

有关端点安全软件的列表，请访问以下 Web 站点：

http://esupport.trendmicro.com/solution/zh-CN/1060980.aspx

如果无法自动移除客户机上的软件，或者只可以检测到但不可移除，请先手动卸载。根据软件卸载过程，卸载后客户机可能需要也可能不需要重新启动。

迁移问题和可能的解决方案

自动卸载第三方端点安全软件可能因为以下原因而导致不成功：

- 第三方软件的版本号或产品密钥不一致。
- 第三方软件的卸载程序无法运行。
- 第三方软件的某些文件已缺失或已遭破坏。
- 第三方软件的注册表项无法清除。
- 第三方软件没有卸载程序。

这些问题的可能解决方案：

- 手动删除第三方软件。
- 停止第三方软件的服务。
- 退出第三方软件的服务或进程。

在安全客户端上执行安装后任务

过程

1. 确认以下内容：
   - 安全客户端快捷方式显示在客户机上的 Windows 开始菜单中。
   - **趋势科技安全无忧软件客户端**列在客户机控制面板的“添加/删除程序”列表中。
   - 安全客户端显示在 Web 控制台上的“安全设置”窗口并分组在**服务器 (缺省)** 或**台式机 (缺省)** 组中，具体取决于客户机操作系统的类型。

     注意

     如果看不到安全客户端，请从**首选项** > **全局设置** > **系统（选项卡）** > **客户端连接验证**中运行连接验证任务。

   - 在 **Microsoft 管理控制台**上显示以下安全客户端服务：

- 趋势科技安全客户端侦听程序 (tmlisten.exe)
- 趋势科技安全客户端实时扫描 (ntrtscan.exe)
- 趋势科技安全客户端 NT 代理服务器服务 (TmProxy.exe)

注意

在 Windows 8/8.1、10、Server 2012 和 Server 2012 R2 上此服务不可用。

- 趋势科技安全客户端防火墙 (TmPfw.exe) - 如果在安装期间已启用防火墙
- 趋势科技未授权更改阻止服务 (TMBMSRV.exe) - 如果在安装期间已启用“行为监控”或“设备控制”

2. 如果安全客户端未显示在 Web 控制台中，则它可能无法向服务器发送其状态。执行以下任一步骤：

   - 打开客户机上的 Web 浏览器，在地址文本框中键入 https://{Trend Micro Security Server_Name}:{端口号}/SMB/cgi/cgionstart.exe，然后按 ENTER 键。

     如果下一窗口显示 -2，则表示客户端可以与服务器通信。同时，这还表明问题可能出在服务器数据库中；数据库中可能没有该客户端的记录。

   - 使用 ping 和 telnet 来验证客户端-服务器通信是否存在。
   - 如果带宽有限，检查它是否会引起服务器和客户端之间的连接超时。
   - 检查服务器上的 \PCCSRV 文件夹是否有共享权限，并检查是否所有用户都被授予完全控制权限
   - 验证趋势科技安全管理服务器代理设置是否正确。

3. 使用 EICAR 测试脚本测试安全客户端。

   欧洲计算机防病毒研究所 (EICAR) 已开发出一个测试“病毒”，用于测试安装和配置。该文件是一个无传染性的文本文件，大多数防病毒产品供应商的病毒码文件已包含其二进制特征码。它不是病毒，并且不包含任何程序代码。

可以从以下 URL 下载 EICAR 测试病毒：

http://www.eicar.org/anti_virus_test_file.htm

另外，您也可以自行创建 EICAR 测试病毒，方法是将以下内容键入一个文本文件，然后将其命名为 eicar.com：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

注意

在测试之前请清除缓存服务器和本地浏览器中的缓存内容。

邮件安全客户端安装

只有在您具有安全无忧软件-邮件与网络安全版的情况下，才可以安装邮件安全客户端。

在 Microsoft Exchange Server 上执行邮件安全客户端的全新安装。

注意

有关将邮件安全客户端升级到此版本的信息，请参阅《安装和升级指南》。

邮件安全客户端安装要求

有关安装要求的完整列表，请访问以下 Web 站点：

http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security.aspx

安装邮件安全客户端（仅限邮件与网络安全版）

开始之前

安装说明和提醒：

- 安装之前或之后无需停止或启动 Microsoft Exchange 服务。
- 如果客户机上存在有关之前的邮件安全客户端安装的信息，则将无法成功安装邮件安全客户端。请使用 Windows Installer 清除实用程序清除以前安装的残留信息。要下载 Windows Installer 清除实用程序，请访问：

  http://support.microsoft.com/kb/290301/en-us
- 如果在正在运行锁定工具的服务器上安装邮件安全客户端，请移除该锁定工具，以便不会禁用 IIS 服务并导致安装不成功。
- 邮件安全客户端还可以在安全管理服务器安装期间进行安装。有关详细信息，请参阅《安装和升级指南》。
- 邮件安全客户端不支持某些 Microsoft Exchange Server Enterprise 功能，例如数据可用性组 (DAG)。

过程

1. 导航至**安全设置** > **添加计算机**。

   此时打开一个新窗口。
2. 选择 **Exchange Server**。
3. 在 **Exchange Server 信息**下，键入以下信息：
   - **服务器名称**：要安装客户端的 Microsoft Exchange Server 的名称。
   - **帐户**：内置域管理员用户名。
   - **密码**：内置域管理员密码。
4. 单击**下一步**。

   根据安装类型的不同，安装向导会显示相应的窗口。

- **全新安装**：Microsoft Exchange Server 上不存在客户端，将予以安装。
- **升级**：Microsoft Exchange Server 上存在早期版本的客户端，将升级到当前版本。
- **无需安装**：Microsoft Exchange Server 上存在当前版本的客户端。如果安全组树中当前未显示客户端，则将自动添加。
- **无效**：安装客户端时出现问题。

注意

对于**垃圾邮件管理类型**，将使用**最终用户隔离**。

5. 在**目录**下，更改或接受邮件安全客户端安装的缺省目标目录和共享目录。缺省目标和共享目录分别是 `C:\Program Files\Trend Micro\Messaging Security Agent` 和 `C$`。
6. 单击**下一步**。

   此时打开一个新窗口。
7. 验证在先前窗口中指定的 Microsoft Exchange Server 设置是否正确，然后单击**下一步**开始安装。
8. 要查看安装的状态，请单击**实时状态**选项卡。

移除客户端

移除**安全客户端**和**邮件安全客户端**（仅限邮件与网络安全版）的方法有两种：

从 Web 控制台移除客户端

针对非活动的客户端使用此选项。非活动的客户端在 Web 控制台上持续显示为脱机状态，这是因为在可卸载该客户端之前，安装该客户端的客户机可能已断电或重新格式化。

从 Web 控制台移除客户端时：

- 如果客户端仍存在于客户机上，将不会被卸载。
- 服务器会停止管理客户端。
- 客户端再次开始与服务器通信时（例如，打开客户机电源后），该客户端会重新添加到 Web 控制台。安全客户端会应用其初始组的设置。如果该组不再存在，客户端将分组在**服务器 (缺省)** 或**台式机 (缺省)** 下（具体取决于客户机的操作系统），并应用该组的设置。

提示

WFBS 还提供了其他功能来检查是否有非活动客户端，并从 Web 控制台将其移除。使用此功能可自动执行客户端移除任务。要使用此功能，请导航到**首选项** > **全局设置** > **系统**选项卡，然后转到“非活动安全客户端移除”部分。

卸载客户端

如果遇到客户端程序相关问题，您可以卸载该客户端（从而将其从 Web 控制台移除）。趋势科技建议立即重新安装客户端，以免客户机受到威胁的侵害。

从 Web 控制台移除客户端

过程

1. 导航至**安全设置**。
2. 要移除安全客户端，请选择一个组，然后选择客户端。要移除邮件安全客户端，请将其选定。

   提示

   要选择多个邻近的安全客户端，请单击范围中的第一个客户端，按住 Shift 键，然后单击范围中的最后一个客户端。要选择一系列非连续的客户端，请单击范围中的第一个客户端，按住 Ctrl 键，然后单击您想要选择的客户端。

3. 单击**管理客户端树** > **删除组/客户端**。

   将显示一个新窗口。

4. 单击**移除选定的客户端**。
5. 单击**应用**。

从 Web 控制台卸载客户端

在卸载邮件安全客户端时，IIS Admin Service/Apache 服务器及所有相关服务将自动停止并重新启动。

过程

1. 导航至**安全设置**。
2. 要卸载安全客户端，请选择一个组，然后选择客户端。要卸载邮件安全客户端，请将其选定。

   提示

   要选择多个邻近的安全客户端，请单击范围中的第一个客户端，按住 Shift 键，然后单击范围中的最后一个客户端。要选择一系列非连续的客户端，请单击范围中的第一个客户端，按住 Ctrl 键，然后单击您想要选择的客户端。

3. 单击**管理客户机树** > **删除组/客户机**。

   将显示一个新窗口。

4. 单击**卸载选定的客户端**。
5. 单击**应用**。

   将出现弹出窗口，并显示由服务器发出的卸载通知数量和收到通知的客户端数量。

   注意

   针对邮件安全客户端，在出现提示时键入相应的 Microsoft Exchange Server 帐户名称和密码。

6. 单击**确定**。
7. 要验证客户端是否已卸载，请刷新“安全设置”窗口。客户端应不再出现在安全组树中。

   如果安全客户端卸载失败，请参阅使用 SA 卸载工具 第 3-37 页。

从客户机卸载安全客户端

用户可从客户机卸载客户端。

卸载时可能需要或不需要输入密码，具体取决于您的配置。如果需要密码，请确保您只将该密码提供给需要运行卸载程序的用户；如果该密码已泄漏给其他用户，请立即更改密码。

可通过**首选项** > **全局设置** > **安全客户端（选项卡）** > **安全客户端卸载密码**设置或禁用密码。

过程

1. 单击**控制面板** > **添加或删除程序**。
2. 找到**趋势科技安全无忧软件客户端**，然后单击**更改**或**卸载**（任一选项皆可）。
3. 遵循窗口上的指导信息。
4. 在系统提示时，键入卸载密码。

   安全管理服务器会通知用户卸载的进度与卸载完成。用户无需重新启动客户机即可完成卸载。

   如果此过程失败，请参阅使用 SA 卸载工具 第 3-37 页。

使用 SA 卸载工具

在以下情况下，可使用 SA 卸载工具：

- 安装失败或需要完全卸载时。该工具会自动移除客户机中的所有安全客户端组件。
- 退出安全客户端时

过程

1. 在安全管理服务器上，导航到 <**服务器安装文件夹**>\PCCSRV\Private。
2. 将 SA_Uninstall.exe 文件复制到目标客户机。
3. 在目标客户机上，运行 SA_Uninstall.exe。
4. 以管理员身份（或具有管理员权限的任何帐户）登录 Windows。
5. 遵循以下步骤执行所需任务。

任务	步骤
卸载安全客户端	a. 运行 **Uninstall.bat**。执行此步骤的方法有多种。 • 在 Windows Vista、7、8/8.1、10、Server 2008/2012/2012 R2 或 SBS 2011 上，导航至该工具的目录并右键单击 **Uninstall.bat**，然后选择**以管理员身份运行**。在 UAC 窗口中，选择**同意**。 • 在 Windows XP/2003 上，双击 **Uninstall.bat**。 b. 当出现**是否要立即重新启动?(Y/N)** 消息时，做出下列任意选择： • **N [Enter]**：在重新启动之前，某些驱动程序不会卸载。 • **Y [Enter]**：在倒计时 30 秒后进行重新启动。 SA 卸载工具会自动停止该客户端。

任务	步骤
退出安全客户端	a. 运行 **Stop.bat**。执行此步骤的方法有多种。 • 在 Windows Vista、7、8/8.1、10、Server 2008/2012/2012 R2 或 SBS 2011 上，导航至该工具的目录并右键单击 **Stop.bat**，然后选择**以管理员身份运行**。在 UAC 窗口中，选择**同意**。 • 在 Windows XP/2003 上，双击 **Stop.bat**。 b. 验证客户端停止时该程序结束。

从 Microsoft Exchange Server 卸载邮件安全客户端（仅限邮件与网络安全版）

在卸载邮件安全客户端时，IIS Admin Service/Apache 服务器及所有相关服务将自动停止并重新启动。

过程

1. 使用具有管理员权限的帐户登录到 Microsoft Exchange Server。
2. 单击**控制面板** > **添加或删除程序**。
3. 找到**趋势科技邮件安全客户端**，然后单击**更改**。
4. 遵循窗口上的指导信息。

第 4 章

管理组

本章说明安全无忧软件中组的概念和用法。

组

在安全无忧软件中，组是共享相同配置、运行相同任务的客户端的集合。在“安全设置”窗口中，将客户端组织到组中，以便您可以同时配置和管理这些客户端。

安全组树和客户端列表

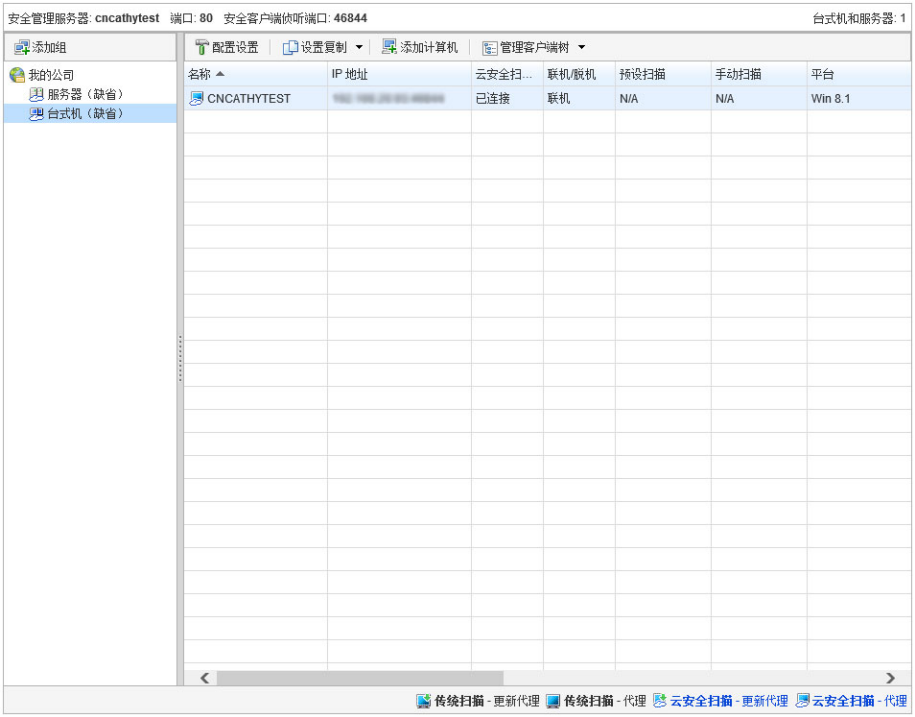


图 4-1. 显示组中客户端的“安全设置”窗口

在“安全设置”窗口中，组显示在左侧的**安全组树**部分下面。为便于管理，请创建代表公司部门或职能的组。您也可以创建特殊的组。例如，在更易受感染的客户机上创建包括安全客户端的组，以便您可以将更为严格的安全策略和设置应用到组。

单击组时，属于该组的客户端将显示在右侧的**客户端列表**中。

客户端列表中的列

客户端列表中的列显示每个客户端的以下信息：

提示

客户端列表中带红色阴影的单元格包含需要您注意的信息。

列	显示的信息
针对安全客户端	
名称	安装客户端的客户机主机名称
IP 地址	安装客户端的客户机 IP 地址
联机/脱机	• **联机**：客户端已连接到安全管理服务器 • **脱机**：客户端已与安全管理服务器断开连接
预设扫描	上次预设扫描的日期和时间
手动扫描	上次手动扫描的日期和时间
平台	安装客户端的客户机操作系统
体系结构	• **x64**：64 位操作系统 • **x86**：32 位操作系统
扫描方法	• **云安全**：本地扫描和云端扫描 • **传统**：仅本地扫描 有关详细信息，请参阅扫描方法 第 5-3 页。
病毒引擎	病毒扫描引擎版本

列	显示的信息
云安全客户端病毒码 **注意** 此列仅在扫描方法为云安全扫描时才会显示。	云安全客户端病毒码版本
云安全扫描服务 **注意** 此列仅在扫描方法为云安全扫描时才会显示。	• **已连接**：客户端已连接到云安全扫描服务 • **已断开连接**：客户端已与云安全扫描服务断开连接 **注意** 云安全扫描服务托管于安全管理服务器上。如果客户端已断开连接，则表示其无法连接到安全管理服务器，或者云安全扫描服务未正常运行（例如，如果服务已停止）。
病毒码 **注意** 此列仅在扫描方法为传统扫描时才会显示。	病毒码版本
检测到的病毒	检测到的病毒/恶意软件数
检测到的间谍软件	检测到的间谍软件/灰色软件数
版本	客户端的版本
违例的 URL	已访问的受禁止 URL 数
检测到的垃圾邮件	垃圾电子邮件数
POP3 扫描	• **已启用** • **已禁用**
针对邮件安全客户端（仅限邮件与网络安全版）	

列	显示的信息
名称	安装客户端的客户机主机名称
IP 地址	安装客户端的客户机 IP 地址
联机/脱机	• **联机**：客户端已连接到安全管理服务器 • **脱机**：客户端已与安全管理服务器断开连接
平台	安装客户端的客户机操作系统
体系结构	• **x64**：64 位操作系统 • **x86**：32 位操作系统
Exchange 版本	Microsoft Exchange Server 版本
病毒码	病毒码版本
病毒引擎	病毒扫描引擎版本
版本	客户端的版本

组和客户端的任务

在组或者一个或多个客户端上运行任务。

运行任务分两个步骤：

1. 选择目标。
2. 单击任务的按钮。

下表列出了您可以执行的任务。

任务	目标	描述
配置	一个安全客户端组（台式机或服务器）	为属于选定组的所有安全客户端配置以下基本安全设置： • 扫描方法。请参阅配置扫描方法 第 5-4 页。 • 防病毒/防间谍软件。请参阅配置安全客户端实时扫描 第 5-6 页。 • 防火墙。请参阅配置防火墙 第 5-9 页。 • Web 信誉。请参阅为安全客户端配置 Web 信誉 第 5-15 页。 • URL 过滤。请参阅配置 URL 过滤 第 5-16 页。 • 允许的/阻止的 URL。请参阅允许的/阻止的 URL 第 5-17 页。 • 行为监控。请参阅配置行为监控 第 5-19 页。 • 设备控制。请参阅配置设备控制 第 5-23 页。 • 用户工具（仅限台式机组）。请参阅配置用户工具 第 5-25 页。 • 客户端权限。请参阅配置客户端权限 第 5-26 页。 • 隔离。请参阅配置隔离目录 第 5-30 页。

任务	目标	描述
配置	一个邮件安全客户端（仅限邮件与网络安全版）	为选定的邮件安全客户端配置以下基本安全设置： • 防病毒。请参阅为邮件安全客户端配置实时扫描： 第 6-5 页。 • 反垃圾邮件。请参阅配置电子邮件信誉评价 第 6-7 页和配置内容扫描 第 6-8 页。 • 内容过滤。请参阅管理内容过滤规则 第 6-14 页。 • 阻止附件。请参阅配置阻止附件 第 6-40 页。 • Web 信誉。请参阅为邮件安全客户端配置 Web 信誉 第 6-43 页。 • 隔离。请参阅查询隔离目录 第 6-55 页、维护隔离目录 第 6-58 页和配置隔离目录 第 6-59 页。 • 操作。请参阅配置邮件安全客户端的通知设置 第 6-61 页、配置垃圾邮件维护 第 6-62 页和生成系统调试报表 第 6-66 页。
复制设置	一个安全客户端组（台式机或服务器）	相同类型的其他组（台式机组或服务器组）将应用选定组的设置。 有关详细信息，请参阅复制设置 第 4-15 页。
导入	一个安全客户端组（台式机或服务器）	将源组的设置导入选定的目标组。 导入之前，请确保已将源组的设置导出到文件中。 有关详细信息，请参阅导入和导出安全客户端组的设置 第 4-17 页。
导出	一个安全客户端组（台式机或服务器）	将选定目标组的设置导出到文件中。 执行此任务，以备份设置或将它们导入其他组。 有关详细信息，请参阅导入和导出安全客户端组的设置 第 4-17 页。

任务	目标	描述
添加组	安全组树 ( )	添加一个新的安全客户端组（台式机组或服务器组）。 有关详细信息，请参阅添加组 第 4-9 页。
添加	安全组树 ( )	安装下列其中一项： • **安全客户端**，安装到客户机（台式机或服务器） • **邮件安全客户端**，安装到 Microsoft Exchange Server（仅限邮件与网络安全版） 有关详细信息，请参阅将客户端添加到组 第 4-10 页。
删除	一个安全客户端组（台式机或服务器）	将选定组从**安全组树**中移除。 请确保组中没有任何客户端，否则将无法删除该组。 有关详细信息，请参阅移除客户端 第 3-34 页。
	属于组的一个或多个安全客户端	您有两种选择： • 将选定的安全客户端从其组中移除。 • 将选定的安全客户端从其客户机中卸载，然后将它们从其组中移除。 有关详细信息，请参阅移除客户端 第 3-34 页。
	一个邮件安全客户端（仅限邮件与网络安全版）	您有两种选择： • 移除选定的邮件安全客户端及其组。 • 将选定的邮件安全客户端从 Microsoft Exchange Server 中卸载，然后移除其组。 有关详细信息，请参阅移除客户端 第 3-34 页。
移动	属于组的一个或多个安全客户端	将选定的安全客户端移至其他组或其他安全管理服务器。 有关详细信息，请参阅移动客户端 第 4-11 页。

任务	目标	描述
重置计数器	安全组树 ( )	将所有安全客户端上的威胁计数重置为零。特别是，**客户端列表**中以下列下的值将重置为： • 检测到的病毒 • 检测到的间谍软件 • 检测到的垃圾邮件 • 违例的 URL

添加组

添加服务器组或台式机组，其中可以包含一个或多个安全客户端。

无法添加包含邮件安全客户端的组。邮件安全客户端安装完成并向安全管理服务器报告之后，它将自动在**安全组树**中自成一组。

过程

1. 导航至**安全设置**。
2. 单击**添加组**。

   将显示一个新窗口。
3. 选择组的类型。
   - **台式机**
   - **服务器**
4. 键入组的名称。
5. 要将现有组的设置应用到所添加的组，请单击**从组导入设置**，然后选择现有的组。将只显示符合选定的组类型的组。
6. 单击**保存**。

将客户端添加到组

客户端在安装并向安全管理服务器报告后，服务器会将其添加到组。

- 服务器平台（例如 Windows Server 2003 和 Windows Server 2008）上安装的安全客户端，会添加到**服务器 (缺省)** 组。
- 台式机平台（例如 Windows XP、Windows Vista 和 Windows 7）上安装的安全客户端，会添加到**台式机 (缺省)** 组。

注意

您可以移动安全客户端，将它们指定给其他组。有关详细信息，请参阅移动客户端 第 4-11 页。

- 每个邮件安全客户端（仅限邮件与网络安全版）都自成一组。无法将多个邮件安全客户端组织到一个组中。

如果安全组树上显示的客户端数不正确，则可能是客户端已移除且服务器未收到通知（例如，在移除客户端时，如果客户机-服务器通信中断）。这会导致服务器在其数据库中保留客户端信息，并在 Web 控制台上将客户端显示为脱机状态。重新安装客户端后，服务器会在数据库中创建一条新记录，并将客户端视为新的，从而导致安全组树上显示重复的客户端。要检查是否有重复的客户端记录，请使用**首选项** > **全局设置** > **系统**中的“客户端连接验证”功能。

安装安全客户端

请参阅下列主题：

- 安全客户端安装要求 第 3-2 页
- 安全客户端安装注意事项 第 3-2 页
- 安全客户端安装方法 第 3-7 页
  - 从内部 Web 页安装 第 3-10 页
  - 使用登录脚本安装进行安装 第 3-12 页
  - 使用客户端打包程序安装 第 3-13 页

- 以远程安装方式安装 第 3-16 页
- 使用漏洞扫描程序安装 第 3-19 页
- 使用电子邮件通知安装 第 3-28 页

- 在安全客户端上执行安装后任务 第 3-30 页

安装邮件安全客户端（仅限邮件与网络安全版）

请参阅下列主题：

- 邮件安全客户端安装要求 第 3-32 页
- 安装邮件安全客户端（仅限邮件与网络安全版） 第 3-33 页

移动客户端

移动客户端有多种方法。

要移动的客户端	详细信息	如何移动客户端
安全客户端	在组之间移动安全客户端。移动后，客户端将继承新组的设置。	使用 Web 控制台，移动一个或多个客户端。请参阅在组之间移动安全客户端 第 4-12 页。
	如果您有至少两个安全管理服务器，则在服务器之间移动安全客户端。 移动后，客户端将分组到其他安全管理服务器的**台式机 (缺省)** 或**服务器 (缺省)** 组下，具体取决于客户机的操作系统。客户端将继承新组的设置。	• 使用 Web 控制台，移动一个或多个客户端。请参阅使用 Web 控制台，在安全管理服务器之间移动客户端 第 4-12 页。 • 运行客户机上的客户端迁移程序工具，以移动该客户机上安装的客户端。请参阅使用客户机迁移程序，在安全管理服务器之间移动安全客户端 第 4-14 页。

要移动的客户端	详细信息	如何移动客户端
邮件安全客户端（仅限邮件与网络安全版）	如果您有至少两个安全管理服务器，则在服务器之间移动邮件安全客户端。 移动后，客户端将在其他安全管理服务器中自成一组，并保留其设置。	使用 Web 控制台，一次移动一个客户端。请参阅使用 Web 控制台，在安全管理服务器之间移动客户端 第 4-12 页。

在组之间移动安全客户端

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 选择要移动的客户端。

> **提示**
> 要选择多个邻近的安全客户端，请单击范围中的第一个客户端，按住 Shift 键，然后单击范围中的最后一个客户端。要选择一系列非连续的客户端，请单击范围中的第一个客户端，按住 Ctrl 键，然后单击您想要选择的客户端。

4. 将客户端拖放到新组。

使用 Web 控制台，在安全管理服务器之间移动客户端

开始之前

在安全管理服务器之间移动客户端时：

- 如果将运行早期版本的客户端移动至运行当前版本的安全管理服务器，则客户端将自动升级。

- 请勿将运行当前版本的客户端移动到运行早期版本的安全管理服务器，因为这样将导致客户端不受管理（客户端将从之前的服务器取消注册，但无法注册到新服务器，因此它将不会显示在任何 Web 控制台中）。客户端将保持其当前版本并且不会降级。
- 安全管理服务器必须具有相同的语言版本。
- 记录客户端将移动到的安全管理服务器的主机名称和侦听端口。主机名称和侦听端口位于安全管理服务器“安全设置”窗口（“任务”面板上方）中。

过程

1. 在当前管理客户端的安全管理服务器的 Web 控制台中，导航至**安全设置**。
2. 要移动安全客户端，请选择一个组，然后选择客户端。要移动邮件安全客户端，请选择相应的客户端。

   提示

   要选择多个邻近的安全客户端，请单击范围中的第一个客户端，按住 Shift 键，然后单击范围中的最后一个客户端。要选择一系列非连续的客户端，请单击范围中的第一个客户端，按住 Ctrl 键，然后单击您想要选择的客户端。

3. 单击**管理客户端树** > **移动客户端**。

   将显示一个新窗口。

4. 键入客户端将移动到的安全管理服务器的主机名称和侦听端口。
5. 单击**移动**。
6. 要检查客户端现在是否向其他安全管理服务器报告，请打开该服务器的 Web 控制台并在安全组树中找到客户端。

   注意

   如果安全组树中未显示客户端，请重新启动服务器的主服务 (`ofservice.exe`)。

使用客户机迁移程序，在安全管理服务器之间移动安全客户端

开始之前

在安全管理服务器之间移动客户端时：

- 如果将运行早期版本的客户端移动至运行当前版本的安全管理服务器，则客户端将自动升级。
- 请勿将运行当前版本的客户端移动到运行早期版本的安全管理服务器，因为这样将导致客户端不受管理（客户端将从之前的服务器取消注册，但无法注册到新服务器，因此它将不会显示在任何 Web 控制台中）。客户端将保持其当前版本并且不会降级。
- 安全管理服务器必须具有相同的语言版本。
- 记录客户端将移动到的安全管理服务器的主机名称和侦听端口。主机名称和侦听端口位于安全管理服务器“安全设置”窗口（“任务”面板上方）中。
- 使用管理员帐户登录客户机。

过程

1. 在客户机上，打开命令提示符。

   注意

   您必须以管理员身份打开命令提示符。

2. 键入 `cd` 和安全客户端安装文件夹的路径。例如：`cd C:\Program Files\Trend Micro\Security Agent`
3. 使用以下语法运行客户端迁移程序：

   <可执行文件名> -s <服务器名称> -p <服务器侦听端口> -c <客户端侦听端口>

表 4-1. 客户端迁移程序参数

参数	说明
<可执行文件名>	IpXfer.exe
<服务器名称>	目标 WFBS 服务器（客户端要转移到的服务器）的名称
<服务器侦听端口>	目标安全管理服务器的侦听端口（或可信端口）。
<客户端侦听端口>	安全客户端用来与服务器通信的端口号

示例：

```
ipXfer.exe -s Server01 -p 8080 -c 21112
```

4. 要检查安全客户端现在是否向其他安全管理服务器报告，请打开该服务器的 Web 控制台并在安全组树中找到该客户端。

注意

如果安全组树中未显示客户端，请重新启动服务器的主服务 (ofservice.exe)。

复制设置

在安全客户端组或邮件安全客户端（仅限邮件与网络安全版）之间复制设置。

复制安全客户端组设置

使用此功能可将特定台式机或服务器组的设置应用到相同类型的其他组。不能将服务器组的设置复制到台式机组，反之亦然。

如果某特定组类型只有一个组，将禁用此功能。

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**更多** > **复制设置**。

   将显示一个新窗口。
4. 选择将继承设置的目标组。
5. 单击**应用**。

复制邮件安全客户端设置（仅限邮件与网络安全版）

如果邮件安全客户端共享同一域，则只能在它们之间复制设置。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**更多** > **复制设置**。

   将显示一个新窗口。
4. 选择将继承设置的邮件安全客户端。
5. 单击**应用**。
6. 如果复制不成功，请执行以下操作：
   a. 启动注册表编辑器 (regedit)。
   b. 转到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`。

c. 右键单击 **winreg** > **权限**。

d. 添加目标域的 **Smex Admin Group**，然后启用**允许读取**。

导入和导出安全客户端组的设置

将台式机组或服务器组的设置导出为 .dat 文件，以备份设置。此外，还可以使用 .dat 文件，将设置导入到另一个组。

注意

您可以在台式机和服务器组之间导入/导出设置。设置与组类型无关。此外，还可以使用“复制设置”功能，但此功能取决于组类型。有关“复制设置”功能的详细信息，请参阅复制设置 第 4-15 页。

可以导入和导出的设置

可以导入和导出的设置取决于您是选择安全组树图标 ( )，还是选择特定的台式机/服务器组。

选择	包含设置的窗口	可以导出/导入的设置
安全组树图标 ( )	安全设置（**安全设置** > **配置设置**）	适用于**服务器 (缺省)** 和**台式机 (缺省)** 组的以下设置： • 扫描方法 • 防火墙 • Web 信誉 • URL 过滤 • 允许的/阻止的 URL • 行为监控 • 可信程序 • 用户工具（仅适用于台式机组） • 客户端权限 • 隔离 • 设备控制
	手动更新（**更新** > **手动**）	在“手动更新”窗口中选择的组件
	预设更新（**更新** > **预设**）	在“预设更新”窗口中选择和预设的组件
	预设报告（**报告** > **预设报告**）	所有设置
	报告维护（**报告** > **维护**）	所有设置
	通知（**首选项** > **通知**）	所有设置
	全局设置（**首选项** > **全局设置**）	以下选项卡上的所有设置： • **代理** • **SMTP** • **安全客户端** • **系统**

选择	包含设置的窗口	可以导出/导入的设置
台式机组（）或服务器组（）	安全设置（**安全设置** > **配置设置**）	• 防病毒/防间谍软件实时扫描 • 防火墙 • Web 信誉 • URL 过滤 • 行为监控 • 可信程序 • 用户工具（**仅适用于台式机组**） • 客户端权限 • 隔离 • 设备控制
	手动扫描窗口（**扫描** > **手动扫描**）	所有设置
	预设扫描窗口（**扫描** > **预设扫描**）	所有设置

导出设置

过程

1. 导航至**安全设置**。
2. 选择安全组树或台式机/服务器组。
3. 单击**更多** > **导出**。

   将显示一个新窗口。
4. 如果已选择安全组树，则选择要导出的设置。
5. 单击**更多** > **导出**。

此时会显示一个对话框。

6. 单击**保存**，然后浏览到首选位置，单击**保存**。

导入设置

过程

1. 导航至**安全设置**。
2. 选择安全组树或台式机/服务器组。
3. 单击**更多** > **导入**。

   将显示一个新窗口。
4. 单击**浏览**，查找文件，然后单击**导入**。

第 5 章

管理安全客户端的基本安全设置

本章说明如何配置安全客户端的基本安全设置。

安全客户端的基本安全设置摘要

表 5-1. 安全客户端的基本安全设置摘要

选项	描述	缺省
扫描方法	配置是否启用或禁用云安全扫描。	在安装期间选择启用或禁用。
防病毒/防间谍软件	配置实时扫描、防病毒和防间谍软件选项	已启用（实时扫描）
防火墙	配置防火墙选项	已禁用
Web 信誉	配置“在办公室”和“不在办公室” Web 信誉选项	在办公室：已启用，低 不在办公室：已启用，中
URL 过滤	URL 过滤可阻止违反配置的策略的 Web 站点。	已启用，低
允许的/阻止的 URL	配置全局允许的/阻止的列表	已禁用
行为监控	配置行为监控选项	对台式机组启用 对服务器组禁用
可信程序	指定不需要监控哪些程序的可疑行为	N/A
设备控制	配置自动运行以及 USB 和网络访问	已禁用
用户工具	配置 Wi-Fi Advisor 和趋势科技反垃圾邮件工具栏	已禁用：Wi-Fi Advisor 已禁用：受支持电子邮件客户端中的反垃圾邮件工具栏
客户端权限	从客户端控制台配置对设置的访问 禁用安全客户端升级和 Hotfix 部署	N/A
隔离	指定隔离目录	http://<安全管理服务器名称或 IP 地址>

扫描方法

在扫描安全威胁时，安全客户端可以使用两种扫描方法中的任意一种。

- **云安全扫描**：使用云安全扫描的安全客户端在本文档中称为**云安全客户端**。云安全客户端将受益于文件信誉服务提供的本地扫描和云端查询。
- **传统扫描**：在本文档中，不使用云安全扫描的安全客户端称为**传统客户端**。传统客户端将所有组件存储在客户端上，并在本地扫描所有文件。

下表提供了这两种扫描方法之间的对比。

表 5-2. 传统扫描和云安全扫描之间的对比

比较的基础	传统扫描	云安全扫描
扫描行为	传统安全客户端在客户端上执行扫描。	• 云安全客户端在客户端上执行扫描。 • 如果安全客户端在扫描期间无法确定文件的风险，则该安全客户端会将扫描查询发送到扫描服务器（针对已连接到云安全服务器的安全客户端）或趋势科技云安全智能防护网络（针对已与云安全服务器断开连接的安全客户端），验证风险。 **注意** 扫描服务器是在云安全服务器上运行的一项服务。 • 安全客户端会“缓存”扫描查询结果，以改善扫描性能。
正在使用且已更新的组件	除云安全客户端病毒码外，所有安全客户端组件在更新源上均可用	在更新源上可用的所有组件（传统病毒码除外）
典型更新源	ActiveUpdate 服务器	ActiveUpdate 服务器

配置扫描方法

开始之前

如果您已安装安全管理服务器，则可选择启用云安全扫描。启用该选项之后，缺省扫描方法即为云安全扫描，这表示所有安全客户端均将使用云安全扫描。否则，缺省为传统扫描。您可以根据当前要求，为客户端切换使用这两种扫描方法。例如：

- 如果客户端当前使用传统扫描且扫描需要很长时间才能完成，您可以切换到云安全扫描，以提高扫描的速度和效率。此外，如果客户端上的磁盘空间不足，也可以切换到云安全扫描，这是因为云安全客户端下载的病毒码较小，所以需要的磁盘空间也较小。

  切换到云安全扫描之前，请导航到**首选项** > **全局设置** > **安全客户端**选项卡，然后转到**通用扫描设置**部分。请确保已禁用**禁用云安全扫描服务**选项。

- 如果您发现安全管理服务器性能下降（这可能表示该服务器无法及时处理来自客户端的所有扫描查询），可将客户端切换到传统扫描。

下表列出了切换扫描方法时的一些注意事项：

表 5-3. 切换扫描方法时的注意事项

注意事项	详细信息
安全管理服务器连接	确保安全客户端可以连接到安全管理服务器。仅联机客户端会收到切换到其他扫描方法的通知。脱机客户端变为联机状态后才会收到通知。 此外，还要验证安全管理服务器是否具有最新组件，这是因为客户端需要从安全管理服务器下载新组件，即云安全客户端病毒码（针对将切换到云安全扫描的客户端）和传统病毒码（针对将切换到传统扫描的客户端）。
要切换的安全客户端数量	一次切换较少数量的安全客户端，可以高效利用安全管理服务器资源。在客户端更改其扫描方法的同时，安全管理服务器可以执行其他关键任务。

注意事项	详细信息
时间选择	首次切换安全客户端时，客户端需要下载**完全版**的云安全客户端病毒码（针对将切换到云安全扫描的客户端）或传统病毒码（针对将切换到传统扫描的客户端）。 请考虑在非高峰时段切换，以确保下载过程可在短时间内完成。此外，还要暂时禁用客户端上的“立即更新”，以阻止用户启动的更新，并在客户端切换到云安全扫描后将其重新启用。 **注意** 随后，客户端将下载**较小的增量**版云安全客户端病毒码或传统病毒码（如果它们经常更新）。
IPv6 支持	脱机的纯 IPv6 云安全客户端无法将查询直接发送到趋势科技云安全智能防护网络。 要使云安全客户端发送查询，需提供可以转换 IP 地址的双栈代理服务器（如 DeleGate）。

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 选择首选扫描方法。
5. 单击**保存**。

安全客户端实时扫描

实时扫描是持续进行的扫描。在每次打开、下载、复制或修改文件时，**安全客户端**中的实时扫描都会扫描该文件是否存在威胁。

配置安全客户端实时扫描

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**防病毒/防间谍软件**。

   将显示一个新窗口。
5. 选择**启用实时防病毒/防间谍软件**。
6. 配置扫描设置。有关详细信息，请参阅安全客户端的扫描目标和处理措施 第 7-7 页：

   注意

   如果您授予用户配置其自身扫描设置的权限，则在扫描期间将使用用户配置的设置。
7. 单击**保存**。

防火墙

防火墙通过在客户端和网络之间创建屏障，可以阻止或允许特定类型的网络通信。另外，防火墙将确定网络数据包中可能预示对客户端进行攻击的特征码。

配置防火墙时，WFBS 有两个选项可供选择：简单模式和高级模式。简单模式用趋势科技建议的缺省设置来启用防火墙。使用高级模式可以定制防火墙设置。

提示

趋势科技建议在部署并启用“趋势科技防火墙”之前卸载其他基于软件的防火墙。

缺省防火墙简单模式设置

防火墙提供了一些缺省设置，为用户启动其客户端防火墙防护策略奠定了基础。这些缺省值旨在包括客户端上可能存在的一般条件，如需要访问 Internet 并使用 FTP 下载或上传文件。

注意

缺省情况下，WFBS 在所有新组和安全客户端上禁用防火墙。

表 5-4. 缺省防火墙设置

设置	状态
安全等级	低 入站与出站通信均允许，只阻止网络病毒。
入侵检测系统	已禁用
警报消息（发送）	已禁用

表 5-5. 缺省防火墙例外

例外名称	处理措施	方向	协议	端口
DNS	允许	传入和传出	TCP/UDP	53
NetBIOS	允许	传入和传出	TCP/UDP	137, 138, 139, 445
HTTPS	允许	传入和传出	TCP	443
HTTP	允许	传入和传出	TCP	80
Telnet	允许	传入和传出	TCP	23
SMTP	允许	传入和传出	TCP	25
FTP	允许	传入和传出	TCP	21
POP3	允许	传入和传出	TCP	110
MSA	允许	传入和传出	TCP	16372, 16373
LDAP	允许	传入和传出	TCP/UDP	389

表 5-6. 基于位置的缺省防火墙设置

位置	防火墙设置
在办公室	关闭
不在办公室	关闭

通信过滤

防火墙过滤所有传入和传出的网络通信，可根据以下标准阻止某些类型的网络通信：

- 方向（入站/出站）
- 协议 (TCP/UDP/ICMP/ICMPv6)
- 目标端口
- 目标计算机

扫描网络病毒

防火墙还会在每个数据包中查找是否有网络病毒。

状态检测型

防火墙是基于状态进行检查的防火墙；它监视客户机的所有连接并记住所有连接状态。它可以确定任何连接中的特定条件，预测应采取的处理措施及检测正常连接中是否存在中断。因此，有效使用防火墙不仅涉及创建概要文件和策略，而且涉及分析连接和过滤通过防火墙的数据包。

通用防火墙驱动程序

“通用防火墙驱动程序”，结合用户定义的防火墙设置，在爆发期间封闭端口。“通用防火墙驱动程序”还使用网络病毒特征码文件来检测网络病毒。

配置防火墙

为“在办公室”和“不在办公室”配置防火墙。如果禁用了“位置感知”，则“在办公室”设置将用于“不在办公室”连接。有关位置感知的详细信息，请参阅配置安全客户端设置 第 11-4 页。

缺省情况下，趋势科技禁用防火墙。

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。
4. 单击**防火墙** > **在办公室**或**防火墙** > **不在办公室**。
5. 选择**启用防火墙**。
6. 从以下选项中选择：
   - **简单模式**：使用缺省设置启用防火墙。

     有关详细信息，请参阅防火墙 第 5-7 页。

- **高级模式**：使用定制设置启用防火墙。

7. 如果已选择**高级模式**，则根据需要更新以下选项：

   - **安全等级**：安全等级可控制要为不属于例外列表的端口强制执行的通信规则。

     - **高**：除例外列表中允许的网络通信外，阻止所有传入和传出的网络通信。

     - **中**：除例外列表中允许和阻止的网络通信外，阻止所有传入的网络通信并允许所有传出的网络通信。

     - **低**：除例外列表中阻止的网络通信外，允许所有传入和传出的网络通信。这是“简单模式”的缺省设置。

   - **设置**

     - **启用入侵检测系统**：入侵检测系统可识别网络数据包中可能导致攻击的特征码。请参阅入侵检测系统 第 D-4 页。

     - **启用警报消息**：在 WFBS 检测到违例时，会通知客户机。

   - **例外**：不会阻止例外列表中的端口。

     有关详细信息，请参阅使用防火墙例外 第 5-10 页。

8. 单击**保存**。

使用防火墙例外

防火墙例外列表包含您可以进行配置以根据客户机端口号和 IP 地址来允许或阻止不同类型网络通信的条目。在爆发期间，安全管理服务器将例外应用到趋势科技策略，而后者会自动部署以保护您的网络。

例如，在病毒爆发期间，可以选择阻止所有客户端通信，包括 HTTP 端口（端口 80）。但是，如仍想授予被阻止的客户端访问 Internet 的权限，则可以将 Web 代理端服务器添加到例外列表中。

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**防火墙** > **在办公室**或**防火墙** > **不在办公室**。

   将显示一个新窗口。
5. 选择**启用防火墙**。
6. 选择**高级模式**。
7. 添加例外：

   a. 单击**添加**。

      将显示一个新窗口。

   b. 键入例外的名称。

   c. 在**处理措施**旁边，单击下列选项之一：

      - **允许所有网络通信**
      - **拒绝所有网络通信**

   d. 在**方向**旁边，单击**入站**或**出站**，以选择要应用例外设置的网络通信类型。

   e. 从“协议”列表中选择网络协议的类型：

      - **全部**
      - **TCP/UDP**（缺省值）
      - **TCP**
      - **UDP**

- **ICMP**
- **ICMPv6**

f. 单击下列选项之一，指定客户端端口：

- **所有端口**（缺省）
- **范围**：键入端口的范围
- **指定的端口**：指定单独的端口。使用半角逗号“,”分隔端口号。

g. 在**计算机**下，选择要包含在例外中的客户机 IP 地址。例如，如果您选择**拒绝所有网络通信（传入和传出）**并键入网络上一台客户机的 IP 地址，则在策略中具有此例外的任何客户机都无法使用该 IP 地址发送或接收数据。单击下列选项之一：

- **所有 IP 地址**（缺省值）
- **单个 IP**：键入 IPv4 或 IPv6 地址，或键入主机名。要将客户端主机名解析为 IP 地址，请单击**解析**。
- **IP 范围 (对于 IPv4 或 IPv6)**：在**从**和**到**文本框中键入两个 IPv4 或两个 IPv6 地址。无法在一个文本框中键入 IPv6 地址，而在另一个文本框中键入 IPv4 地址。
- **IP 范围 (对于 IPv6)**：键入 IPv6 地址前缀和长度。

h. 单击**保存**。

8. 要编辑例外，请单击**编辑**，然后在显示的窗口中修改设置。

9. 要在列表中向上或向下移动例外，请选择该例外，然后单击**上移**或**下移**，直到移动到所需的位置。

10. 要移除例外，请选择该例外，然后单击**移除**。

禁用一组客户端上的防火墙

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**防火墙** > **在办公室**或**防火墙** > **不在办公室**。

   将显示一个新窗口。
5. 选择**禁用防火墙**。
6. 单击**保存**。

禁用所有客户端上的防火墙

过程

1. 导航至**首选项** > **全局设置** > **安全客户端**选项卡。
2. 在**防火墙设置**下，选择**禁用防火墙并卸载驱动程序**。
3. 单击**保存**。

Web 信誉

Web 信誉有助于防止访问 Web 上或嵌在电子邮件中的存在安全风险的 URL。Web 信誉对照趋势科技 Web 信誉服务器检查 URL 的信誉，然后将信誉与在客户机上执行的 Web 信誉策略关联。根据使用的策略：

- 安全客户端将阻止或允许访问 Web 站点。
- 邮件安全客户端（仅限邮件与网络安全版）将隔离、删除或标记包含恶意 URL 的电子邮件，或者允许发送邮件（如果 URL 是安全的）。

Web 信誉在进行检测时，会向管理员发送电子邮件通知，并向用户发送在线通知。

对于安全客户端，可根据该客户端的位置（“在办公室”/“不在办公室”）配置不同等级的安全性。

如果 Web 信誉阻止了 URL，并且您感觉此 URL 是安全的，请将此 URL 添加到“允许的 URL”列表中。

提示

为了节省网络带宽，趋势科技建议将企业内部 Web 站点添加到 Web 信誉允许的 URL 列表。

信誉分值

URL 的“信誉分值”可确定其是否为 Web 威胁。趋势科技使用专有的度量方法来计算该分值。

如果某 URL 的分值在定义的阈值范围之内，趋势科技就会将该 URL 视为 Web 威胁；如果分值超出该阈值，则将其视为安全 URL。

安全客户端有三个安全等级，可确定是允许还是阻止访问某 URL。

- **高**：阻止以下页面：
  - **危险**：已证实为欺诈或已知的威胁源
  - **高度可疑**：怀疑为欺诈或可能的威胁源
  - **可疑**：与垃圾邮件关联或可能危及安全的页面
  - **未测试**：尽管趋势科技会主动测试 Web 页面的安全性，但用户在访问新的或不常见的 Web 站点时，可能会遇到未经测试的页面。虽然阻止访问未经测试的页面可以提高安全性，但也会阻止访问安全页面。
- **中**：阻止以下页面：

  - **危险**：已证实为欺诈或已知的威胁源
  - **高度可疑**：怀疑为欺诈或可能的威胁源
- **低**：阻止以下页面：
  - **危险**：已证实为欺诈或已知的威胁源

为安全客户端配置 Web 信誉

在每次请求 HTTP/HTTPS 时，Web 信誉会通过查询趋势科技安全数据库来评估所有请求的 URL 的潜在安全风险。

注意

（仅限网络安全版）为“在办公室”和“不在办公室”配置 Web 信誉设置。如果禁用了“位置感知”，则“在办公室”设置将用于“不在办公室”连接。有关位置感知的详细信息，请参阅配置安全客户端设置 第 11-4 页。

如果同时启用“Web 信誉”和“浏览器利用阻止”，“浏览器利用阻止”会扫描“Web 信誉”未阻止的 URL。“浏览器利用阻止”会扫描 URL Web 页中的嵌入物件，例如 jar、class、pdf、swf、html、js。

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击 **Web 信誉** > **在办公室**或 **Web 信誉** > **不在办公室**。

   将显示一个新窗口。
5. 根据需要进行以下更新：
   - **启用 Web 信誉**

- 安全等级：**高**、**中**或**低**
- 浏览器利用阻止：**阻止包含恶意脚本的页面**

6. 单击**保存**。

URL 过滤

URL 过滤有助于控制对 Web 站点的访问，以减少非生产性雇员的时间、降低 Internet 带宽占用，并创造更安全的 Internet 环境。您可选择 URL 过滤防护等级，或定制想要屏蔽的 Web 站点的类型。

注意

为保护用户，趋势科技会自动阻止包含世界大部分地区认为非法的内容的所有 URL。

配置 URL 过滤

您可以通过选择**定制**来选择要在一天内的不同时间段阻止的特定类型的 Web 站点。

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击 **URL 过滤**。

   将显示一个新窗口。

5. 根据需要进行以下更新：
   - **启用 URL 过滤**
   - **过滤强度**
     - **高**：阻止已知或潜在的安全威胁、不适当的或可能带有攻击性的内容、可能会影响生产力或带宽的内容和未评级的页面
     - **中**：阻止已知安全威胁和不适当的内容
     - **低**：阻止已知安全威胁
     - **定制**：选择您自己的类别，并选择要在工作时间还是业余时间阻止这些类别。
   - **过滤规则**：选择要阻止的整个类别或子类别。
   - **工作时间**：所定义的工作时间以外的天或小时称为业余时间。
6. 单击**保存**。

允许的/阻止的 URL

自动化 URL 允许和阻止有助于您控制对网站的访问，创造一个更加安全的 Internet 环境。在“全局设置”中标识允许的或阻止的 URL。

也可以针对特定的组创建自定义 URL 允许和阻止列表。选择**针对该组自定义允许的/阻止的 URL** 选项后，“安全客户端”将通过该组自定义允许的或阻止的 URL 列表控制对网站的访问。

配置允许/阻止的 URL

过程

1. 导航至**安全设置**。

2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**允许/阻止的 URL**。

   将显示一个新窗口。
5. 根据需要进行以下更新。
   - **为该组自定义允许/阻止的 URL**：在此列表中指定的 URL 将覆盖所有其他设置。
   - 在**要允许的 URL** 文本框中键入网站的 URL，以从“Web 信誉和 URL 过滤”验证中将它们排除。多个 URL 之间用半角分号 (;) 隔开。单击**添加**。

     提示

     单击**从全局设置导入**以插入所有条目。然后您可以自定义此组的 URL。
   - 在**要阻止的 URL** 文本框中键入网站的 URL，以在“URL 过滤”过程中将它们拦截。多个 URL 之间用半角分号 (;) 隔开。单击**添加**。

     提示

     单击**从全局设置导入**以插入所有条目。然后您可以自定义此组的 URL。
6. 单击**保存**。

行为监控

安全客户端持续监控客户机是否对操作系统或在安装的软件上进行了异常修改。在发现某一受监控的更改违例时，管理员（或用户）可以创建让某些程序

启动的例外列表，或者完全阻止某些程序。此外，具有有效数字签名的程序始终允许启动。

行为监控的另一个功能是保护 EXE 和 DLL 文件，防止它们被删除或修改。启用行为监控时，用户创建例外以允许或阻止特定程序。此外，用户还可以选择保护所有的 Intuit QuickBooks 程序。

配置行为监控

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。
4. 单击**行为监控**。
5. 根据需要进行以下更新：
   - **启用行为监控**

     注意

     要允许用户定制自己的“行为监控”设置，请转至**安全设置** > **{组}** > **配置** > **客户端权限** > **行为监控**，然后选择**允许用户修改“行为监控”设置**。

   - **对已知和潜在威胁启用阻止恶意软件行为**：恶意软件行为阻止可以通过**特征码文件**中定义的一系列内部规则实现。这些规则可识别恶意软件中常见的已知和可疑威胁行为。可疑行为包括突然出现无法说明的新运行服务、防火墙的更改以及系统文件修改等。
     - **已知威胁**：阻止与已知威胁相关联的行为
     - **已知和潜在威胁**：阻止与已知威胁相关联的行为，并对可能是恶意的行为采取处理措施

- **在对通过 HTTP 下载的最近遇到的程序执行操作前提示用户 (服务器平台除外)**：行为监控和 Web 信誉可以验证通过 HTTP 通道或电子邮件应用程序下载的文件的普遍性。检测“最近遇到的”文件后，管理员可以选择在执行文件前提示用户。根据云安全智能防护网络确定的文件检测次数或文件的存在时间，趋势科技可确定是否将程序归类为最近遇到的程序。

注意

对于 HTTP 通道，会扫描可执行 (.exe) 文件。对于电子邮件应用程序（仅限 Outlook 和 Windows Live Mail），会扫描非密码保护归档 (zip/rar) 文件中的可执行 (.exe) 文件。

- **启用 Intuit QuickBooks 防护**：保护所有 Intuit QuickBooks 文件和文件夹，防止其他程序进行未经授权的更改。启用此功能将不会影响在 Intuit QuickBooks 程序中所做的更改，只会防止其他未经授权的应用程序更改此文件。

  支持以下产品：

  - QuickBooks Simple Start
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Online

注意

所有 Intuit 可执行文件均具有数字签名，对这些文件的更新不会被阻止。如果其他程序尝试更改 Intuit 二进制文件，客户端会显示一条消息，指出正尝试更改该二进制文件的程序名称。可以允许其他程序更新 Intuit 文件。要允许其他程序进行更新，请将所需的程序添加到客户端上的行为监控例外列表。更新之后，不要忘记将该程序从例外列表中删除。

- 在**勒索软件防护**下，根据需要更新以下各项：

注意

勒索软件防护可防止“勒索软件”威胁在未经授权的情况下修改或加密计算机上的文件。勒索软件是以一种恶意软件，它会限制对文件的访问，要求付款才能还原受影响的文件。

- **启用文档保护，使其免遭未授权的加密或修改**：保护文档，避免未授权更改。
  - **自动备份文件被可疑程序更改**：如果文档保护已启用，则自动备份被可疑程序修改的文件。
- **启用程序检查以检测并阻止可能危及安全的可执行文件**：通过监控进程中类似勒索软件的行为来提升检测。
- **针对通常与勒索软件关联的进程启用阻止**：阻止通常与网络劫持尝试相关的进程，从而保护终端免受勒索软件的攻击。

注意

为了减少 WFBS 将安全进程检测为恶意进程的机会，请确保计算机具有 Internet 连接，可使用 趋势科技 服务器执行其他验证过程。

- **例外**：例外包括一个允许的程序列表和一个阻止的程序列表。允许的程序列表中的程序即使违反监控更改，也可以启动；而阻止的程序列表中的程序则无法启动。
  - **输入程序完整路径**：键入程序的完整 Windows 路径或 UNC 路径。多个条目之间用半角分号隔开。单击**添加到允许列表**或**添加到阻止列表**。如果需要，可使用环境变量指定路径。

环境变量	指向...
$windir$	Windows 文件夹
$rootdir$	根文件夹
$tempdir$	Windows 临时文件夹
$programdir$	Program Files 文件夹

- **允许的程序列表**：此列表中的程序（最多 100 个）都可以启动。单击相应的图标可以删除条目
- **阻止的程序列表**：此列表中的程序（最多 100 个）永远不能启动。单击相应的图标可以删除条目

6. 单击**保存**。

可信程序

将不会监视“可信程序列表”中所列出程序的可疑文件访问活动。

配置可信程序

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**可信程序**。

   将显示一个新窗口。
5. 若要从可疑文件访问活动监控中排除某个程序，请键入完整的文件路径，使用一个特定的文件路径，并单击**添加到可信程序列表**。

   <驱动器名称>:/<路径>/<文件名>

   示例 1：`C:\Windows\system32\regedit.exe`

   示例 2：`D:\backup\tool.exe`

这会阻止黑客使用例外列表中的程序名称，但会执行其他文件路径中的程序名称。

6. 单击**保存**。

设备控制

设备控制用于控制对连接到客户端的外部存储设备和网络资源的访问权限。明确地讲，设备控制限制对通过 USB 接口连接的所有种类的存储设备（智能手机和数码相机除外）的访问。

配置设备控制

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置策略**。

   将显示一个新窗口。
4. 单击**设备控制**。

   将显示一个新窗口。
5. 根据需要进行以下更新：
   - **启用设备控制**
   - **启用阻止 USB 自动运行**
   - **权限**：为 USB 设备和网络资源设置权限。

表 5-7. 设备控制权限

权限	设备上的文件	传入文件
完全访问	允许的操作：复制、移动、打开、保存、删除、执行	允许的操作：保存、移动、复制 这意味着可以将文件保存、移动和复制到设备。
修改	允许的操作：复制、移动、打开、保存、删除 禁止的操作：执行	允许的操作：保存、移动、复制
读取和执行	允许的操作：复制、打开、执行 禁止的操作：保存、移动、删除	禁止的操作：保存、移动、复制
读取	允许的操作：复制、打开 禁止的操作：保存、移动、删除、执行	禁止的操作：保存、移动、复制
无访问权限	禁止的操作：所有操作 设备及其包含的文件对用户可见（例如，在 Windows 资源管理器中对用户可见）。	禁止的操作：保存、移动、复制

- **例外**：即使用户没有被授予对特定设备的读取权限，仍允许该用户运行或打开允许列表中的任何文件或程序。

  但是，如果启用“阻止自动运行”，即使文件包括在允许列表中，也不允许运行此文件。

  要将例外添加到允许列表中，请输入文件名（包括路径或数字签名），然后单击**添加到允许列表**。

6. 单击**保存**。

用户工具

- **反垃圾邮件工具栏：**过滤 Microsoft Outlook 中的垃圾邮件、提供统计信息，并允许您更改某些设置。
- **HouseCall：**该工具可以根据接入点 SSID 的有效性、认证方法及加密要求检查接入点的可靠性，以此来确定无线连接的安全性。如果连接不安全，会显示弹出警告。
- **案例诊断工具：**趋势科技情况诊断工具 (CDT) 会在发生问题时收集来自客户产品的必要调试信息。CDT 可自动打开和关闭产品的调试状态，以及根据问题类别收集必要文件。趋势科技将使用此信息解决与产品相关的问题。

  此工具仅可在安全客户端控制台上可用。
- **客户机迁移程序：**使用此工具可以将客户机从一个服务器转移到另一个服务器。服务器必须具有相同的语言版本和类型。
- **客户端-服务器通信工具：**使用此工具可解决客户端-服务器通信的问题。

配置用户工具

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**使用工具**。

   将显示一个新窗口。
5. 根据需要进行以下更新：

- **Wi-Fi Advisor**:根据无线网络 SSID 的有效性、认证方法及加密要求检查无线网络的安全性。
- **反垃圾邮件工具栏**：该工具可以过滤 Microsoft Outlook 中的垃圾邮件。

6. 单击**保存**。

客户端权限

授予客户端权限，允许用户修改客户机上的安全客户端设置。

提示

要在组织中强制实施经过调制的安全策略，趋势科技建议仅向用户授予有限的权限。这可确保用户不能修改扫描设置或退出安全客户端。

配置客户端权限

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。
4. 单击**客户端权限**。
5. 根据需要进行以下更新：

部分	权限
防病毒/防间谍软件	• 手动扫描设置 • 预设扫描设置 • 实时扫描设置 • 跳过预设扫描
防火墙	防火墙设置
云安全扫描 - 继续浏览	系统会显示一个链接让用户继续浏览特定恶意 URL，直至计算机重新启动。系统会继续针对其他恶意 URL 显示警告。
URL 过滤 - 继续浏览	系统会显示一个链接让用户继续浏览特定受限制的 URL，直至计算机重新启动。系统会继续针对其他受限制的 URL 显示警告。
行为监控	允许用户修改行为监控设置。
受信任的程序	允许用户修改受信任的程序列表。
代理服务器设置	允许用户配置代理服务器设置。 **注意** 禁用此功能会将代理服务器设置重置为缺省设置。

部分	权限
更新权限	• 允许用户执行手动更新 • 将趋势科技 ActiveUpdate 用作次要更新来源 • 禁用 Hotfix 部署 **注意** 将 Hotfix、Patch、安全/关键修补程序和 Service Pack 同时部署到大量客户端会大大增加网络流量。不妨考虑为多个组启用此选项，以便错开部署。 启用此选项还会禁用在客户端上自动进行 **Build 升级**（例如，从测试版 Build 升级至当前产品版本的发行 Build），但不会禁用自动**版本升级**（例如，从版本 7.x 升级至当前版本）。要禁用自动版本升级，请运行安全管理服务器安装包，然后选择相应选项以延迟升级。
客户端安全	防止用户或其他进程修改趋势科技程序文件、注册表和进程。

6. 单击**保存**。

隔离目录

如果针对受感染文件的处理措施是“隔离”，则安全客户端将加密文件并**临时**将其移动至位于以下位置的隔离文件夹：

- <**安全客户端安装文件夹**>`\quarantine`，用于从 6.x 版本或更早版本升级的客户端
- <**安全客户端安装文件夹**>`\SUSPECT\Backup`，用于新安装的客户端和从 7.x 版本或更高版本升级的客户端

安全客户端将受感染文件发送到集中隔离目录，您可以从 Web 控制台的**安全设置** > **{组}** > **配置** > **隔离**上进行配置。

缺省集中隔离目录

缺省集中隔离目录位于安全管理服务器上。该目录采用 URL 格式，并且包含安全管理服务器的主机名称或 IP 地址，例如 `http://server`。同等的绝对路径是 <**安全管理服务器安装文件夹**>`\PCCSRV\Virus`。

- 如果服务器同时管理 IPv4 和 IPv6 客户端，则使用主机名称，以便所有客户端都可以将隔离文件发送到该服务器。
- 如果服务器只具有 IPv4 地址，或只通过其 IPv4 地址进行标识，则只有纯 IPv4 和双栈客户端可以将隔离文件发送到该服务器。
- 如果服务器只具有 IPv6 地址，或只通过其 IPv6 地址进行标识，则只有纯 IPv6 和双栈客户端可以将隔离文件发送到该服务器。

备用集中隔离目录

也可以使用 URL、UNC 路径或绝对文件路径的格式键入位置，来指定备用集中隔离目录。安全客户端应该可以连接到此目录。例如，如果目录将接收来自双栈客户端和纯 IPv6 客户端的隔离文件，该目录应具有 IPv6 地址。趋势科技建议指定双栈备用目录、通过其主机名称识别目录并在键入目录时使用 UNC 路径。

有关指定集中隔离目录的准则

有关何时使用 URL、UNC 路径或绝对文件路径的指导，请参考下表：

表 5-8. 隔离目录

隔离目录	可接受的格式	示例	注意：
安全管理服务器上的缺省目录	URL	`http://`<**服务器主机名称或 IP**>	如果保留缺省目录，请在**首选项** > **全局设置** > **系统（选项卡）** > **隔离维护**部分，配置目录的维护设置，例如隔离文件夹的大小。
	UNC 路径	`\\`<**服务器主机名称或 IP**>`\ofcscan\Virus`	

隔离目录	可接受的格式	示例	注意：
安全管理服务器上的其他目录	UNC 路径	\\<服务器主机名称或 IP>\D$\Quarantined Files	如果不想使用缺省目录（例如，如果磁盘空间不足），请键入其他目录的 UNC 路径。要这样做，请在**首选项** > **全局设置** > **系统（选项卡）** > **隔离维护**部分键入同等的绝对路径，以使维护设置生效。
另一台安全管理服务器计算机上的目录（如果网络上具有其他安全管理服务器）	URL	http://<服务器 2 主机名称或 IP>	确保客户端可以连接到此目录。如果指定了不正确的目录，则客户端会保留隔离文件，直到指定了正确的隔离目录。在服务器的病毒/恶意软件日志中，扫描结果是“无法将隔离文件发送到指定的隔离文件夹中”。 如果使用 UNC 路径，请确保隔离目录文件夹共享给“所有人”组并且向该组分配了读写权限。
	UNC 路径	\\<服务器 2 主机名称或 IP>\ofcscan\Virus	
网络上的其他计算机	UNC 路径	\\<计算机名称>\temp	
该客户机上的其他目录	绝对路径	C:\temp	在以下情况下，指定绝对路径： • 希望隔离文件只驻留在客户机上。 • 不希望客户端将文件存储到客户机上的缺省目录。 如果路径不存在，安全客户端会自动创建路径。

配置隔离目录

过程

1. 导航至**安全设置**。
2. 选择台式机组或服务器组。
3. 单击**配置设置**。

将显示一个新窗口。

4. 单击**隔离**。

   将显示一个新窗口。

5. 配置隔离目录。有关详细信息，请参阅隔离目录 第 5-28 页。

6. 单击**保存**。

第 6 章

管理邮件安全客户端的基本安全设置（仅限邮件与网络安全版）

本章介绍邮件安全客户端，并说明如何为客户端设置实时扫描选项以及配置反垃圾邮件、内容过滤、阻止附件和隔离维护选项。

邮件安全客户端

邮件安全客户端可保护 Microsoft Exchange Server。客户端通过扫描传入和传出 Microsoft Exchange 邮箱存储的电子邮件以及在 Microsoft Exchange Server 和外部目标之间传递的电子邮件，来帮助阻止电子邮件附带的威胁。此外，邮件安全客户端可以：

- 减少垃圾邮件
- 根据内容阻止电子邮件
- 阻止或限制带有附件的电子邮件
- 检测电子邮件中的恶意 URL
- 阻止机密数据泄露

关于邮件安全客户端的重要信息

- 邮件安全客户端只能安装在 Microsoft Exchange Server 上。
- 邮件安全客户端不支持某些 Microsoft Exchange Server Enterprise 功能，例如数据可用性组 (DAG)。
- Web 控制台中的安全组树显示所有邮件安全客户端。多个邮件安全客户端不能合并成为一个组；必须分别管理每个邮件安全客户端。
- WFBS 使用邮件安全客户端，从 Microsoft Exchange Server 收集安全信息。例如，邮件安全客户端会向安全管理服务器报告垃圾邮件检测情况或组件更新完成。此信息会显示在 Web 控制台中。安全管理服务器也会使用此信息来生成有关 Microsoft Exchange Server 安全状态的日志和报表。

  每个检测到的威胁会生成一个日志条目/通知。这就意味着如果邮件安全客户端在一封电子邮件中检测到了多个威胁，它就会生成多个日志条目和通知。当同一威胁被检测到多次时，特别是如果正在 Outlook 2003 中使用缓存模式时，也会有多个日志条目和通知。当启用缓存模式时，可能会在传输列队文件夹和已发送邮件文件夹或 Outbox 文件夹中检测到同一威胁。
- 在运行 Microsoft Exchange Server 2007 的计算机上，邮件安全客户端使用 SQL Server 数据库。为防止出现问题，邮件安全客户端服务被设计为依赖

于 SQL Server 服务实例 MSSQL$SCANMAIL。只要此实例停止或重新启动，以下邮件安全客户端服务也会停止：

- ScanMail_Master
- ScanMail_RemoteConfig

如果 MSSQL$SCANMAIL 停止或重新启动，请手动重新启动这些服务。不同事件（包括更新 SQL Server 时）可导致 MSSQL$SCANMAIL 重新启动或停止。

邮件安全客户端如何扫描电子邮件

邮件安全客户端按下列顺序扫描电子邮件：

1. 扫描垃圾邮件（反垃圾邮件）
   a. 将电子邮件与管理员的“允许的发件人”/“阻止的发件人”列表相比较
   b. 检查是否出现网络钓鱼
   c. 将电子邮件与趋势科技提供的例外列表相比较
   d. 将电子邮件与垃圾邮件特征码数据库相比较
   e. 应用启发式扫描规则
2. 扫描内容过滤规则违例情况
3. 扫描超出用户定义参数的附件
4. 扫描病毒/恶意软件（防病毒）
5. 扫描恶意 URL

缺省邮件安全客户端设置

考虑表中列出的选项，以帮助您优化邮件安全客户端配置。

表 6-1. 邮件安全客户端的趋势科技缺省处理措施

扫描选项	实时扫描	手动扫描和预设扫描
反垃圾邮件		
垃圾邮件	将邮件隔离到用户的垃圾邮件文件夹（缺省情况，如果安装了“Outlook 垃圾邮件”或“最终用户隔离”）	不适用
网络钓鱼	删除整个邮件	不适用
内容过滤		
过滤满足任一定义条件的邮件	隔离整个邮件	替换
过滤满足所有已定义条件的邮件	隔离整个邮件	不适用
监控特定电子邮件帐户的邮件内容	隔离整个邮件	替换
创建特定电子邮件帐户的例外	不予处理	不予处理
阻止附件		
处理措施	用文本/文件替换附件	用文本/文件替换附件
其他		
加密的文件和受密码保护的文件	不予处理（在将处理措施配置为“不予处理”时，加密的文件和受密码保护的文件将不予处理，且该事件不被记录）	不予处理（在将处理措施配置为“不予处理”时，加密的文件和受密码保护的文件将不予处理，且该事件不被记录）
排除的文件（超出指定扫描限制的文件）	不予处理（在将处理措施配置为“不予处理”时，超出指定扫描限制的文件或邮件正文将不予处理，且该事件不被记录）	不予处理（在将处理措施配置为“不予处理”时，超出指定扫描限制的文件或邮件正文将不予处理，且该事件不被记录）

邮件安全客户端实时扫描

实时扫描是持续进行的扫描。**邮件安全客户端**（仅限邮件与网络安全版）中的实时扫描通过扫描所有传入邮件、SMTP 邮件、公共文件夹上发布的文档以及从其他 Microsoft Exchange Server 复制的文件，来保护所有已知的病毒入口点。

为邮件安全客户端配置实时扫描：

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**防病毒**。

   将显示一个新窗口。
5. 选择**启用实时防病毒**。
6. 配置扫描设置。有关详细信息，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页。
7. 单击**保存**。

   配置当发生事件时接收通知的用户。请参阅配置通知事件 第 9-3 页。

反垃圾邮件

WFBS 提供了两种抵御垃圾邮件的方法—**电子邮件信誉**和**内容扫描**。

邮件安全客户端使用以下组件过滤电子邮件中的垃圾邮件与网络钓鱼事件:

- 趋势科技反垃圾邮件引擎
- 趋势科技垃圾邮件特征码文件

趋势科技经常更新引擎和特征码文件并供用户下载。安全管理服务器可以通过手动或预设更新下载这些组件。

反垃圾邮件引擎使用垃圾邮件特征码和启发式规则来过滤电子邮件。它扫描电子邮件，并根据每个电子邮件与特征码文件中的规则和特征的匹配程度为其分配一个垃圾邮件分值。邮件安全客户端将垃圾邮件分值与用户定义的垃圾邮件检测标准进行比较。当垃圾邮件分值超过检测等级时，客户端就会对垃圾邮件采取处理措施。

例如：垃圾邮件发送者经常在其电子邮件中使用许多感叹号或者多个连续的感叹号 (!!!!)。当邮件安全客户端检测到以这种方式使用感叹号的邮件时，它会加大该电子邮件的垃圾邮件分值。

提示

除了使用反垃圾邮件过滤垃圾邮件外，还可以配置“内容过滤”来过滤邮件标题、主题、正文和附件信息，以滤出垃圾邮件和其他不需要的内容。

用户不能修改反垃圾邮件引擎分配垃圾邮件分值的方法，但可以调整邮件安全客户端用以确定哪些邮件是垃圾邮件和哪些邮件不是垃圾邮件的检测标准。

注意

Microsoft Outlook 会自动过滤被邮件安全客户端检测为垃圾邮件的邮件，并将它们发送到垃圾邮件文件夹。

电子邮件信誉

电子邮件信誉评价技术可根据始发邮件传输客户端 (MTA) 的信誉确定垃圾邮件。这可减轻安全管理服务器的任务负担。启用“电子邮件信誉”后，将会根据 IP 数据库检查所有的入站 SMTP 通信，以查看始发 IP 地址是正常的还是已作为已知垃圾邮件源列入黑名单。

“电子邮件信誉评价”有两个服务级别。分别是：

- **标准**：标准服务使用一个可跟踪约二十亿个 IP 地址信誉的数据库。总是与垃圾邮件传递关联的 IP 地址将添加到此数据库中，并且一般不会将其删除。
- **高级**：高级服务级别是一个 DNS，它是基于查询的服务，类似于标准服务。此服务的核心是标准信誉评价数据库和一个动态信誉评价的实时数据库，该数据库可阻止来自已知和可疑的垃圾邮件源的邮件。

在发现来自阻止的或可疑的 IP 地址的电子邮件时，“电子邮件信誉评价”在该邮件到达您的网关之前即会将其阻止。

配置电子邮件信誉评价

配置电子邮件信誉评价可阻止来自已知和可疑的垃圾邮件源的邮件。另外，创建例外可允许或阻止来自其他发件人的邮件。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**反垃圾邮件** > **电子邮件信誉**。

   将显示一个新窗口。
5. 从**目标**选项卡中，根据需要更新以下选项：
   - **启用实时反垃圾邮件（电子邮件信誉评价）**
   - **服务级别：**
     - **标准**
     - **高级**
   - **允许的 IP 地址**：来自这些 IP 地址的电子邮件将永远不被阻止。键入要允许的 IP 地址，然后单击**添加**。如果需要，您可以从文本文件中

导入 IP 地址的列表。要移除 IP 地址，请选择该地址，然后单击**移除**。

- **阻止的 IP 地址**：来自这些 IP 地址的电子邮件将总是被阻止。键入要阻止的 IP 地址，然后单击**添加**。如果需要，您可以从文本文件中导入 IP 地址的列表。要移除 IP 地址，请选择该地址，然后单击**移除**。

6. 单击**保存**。
7. 转到：http://ers.trendmicro.com/ 查看报表。

注意

电子邮件信誉评价是一种基于 Web 的服务。管理员只能从 Web 控制台配置该服务级别。

内容扫描

内容扫描根据邮件内容而非始发 IP 来识别垃圾邮件。在每封电子邮件传递到“信息存储”之前，邮件安全客户端将使用趋势科技反垃圾邮件引擎和垃圾邮件特征码文件来对其进行过滤。Microsoft Exchange Server 将不处理被拒绝的垃圾邮件，并且这些被拒绝的邮件也不会堆积在用户的邮箱中。

注意

请不要将“内容扫描”（基于特征码和启发式的反垃圾邮件）与“内容过滤”（基于归类关键字的电子邮件扫描和阻止）混淆。请参阅内容过滤 第 6-13 页。

配置内容扫描

邮件安全客户端**实时**检测垃圾邮件并采取处理措施，以保护 Microsoft Exchange Server。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**反垃圾邮件** > **内容扫描**。

   将显示一个新窗口。
5. 选择**启用实时反垃圾邮件**。
6. 选择**目标**选项卡，选择邮件安全客户端过滤垃圾邮件所用的方法和垃圾邮件检测率：

   a. 从垃圾邮件检测率列表中选择检测级别**低**、**中**或**高**。邮件安全客户端使用该比率来过滤所有邮件。

      - **高**：此为最严格的垃圾邮件检测等级。邮件安全客户端会监控所有的电子邮件是否包含可疑文件或文本，但选择此项极可能导致误判。误判是指合法电子邮件被邮件安全客户端视为垃圾邮件过滤的情况。
      - **中**：此项为缺省设置并且是建议的设置。邮件安全客户端以较高的垃圾邮件检测等级进行监控，同时导致误判的可能性适中。
      - **低**：此为最宽松的垃圾邮件检测等级。邮件安全客户端将只过滤最明显和常见的垃圾邮件，基本不会出现误判。按垃圾邮件分值进行过滤。

   b. 单击**检测网络钓鱼**，使邮件安全客户端过滤网络钓鱼事件。有关详细信息，请参阅网络钓鱼事件 第 1-23 页。

   c. 将地址添加到允许的发件人与阻止的发件人列表中。有关详细信息，请参阅允许的发件人和阻止的发件人列表 第 6-11 页。

      - **允许的发件人**：来自这些地址或域名的电子邮件将永远不被阻止。键入要允许的地址或域名，然后单击**添加**。如果需要，您可

以从文本文件中导入地址或域名列表。要移除地址或域名，请选择该地址，并单击**移除**。

- **阻止的发件人**：来自这些地址或域名的电子邮件将总是被阻止。键入要阻止的地址或域名，然后单击**添加**。如果需要，您可以从文本文件中导入地址或域名列表。要移除地址或域名，请选择该地址，并单击**移除**。

注意

Microsoft Exchange 管理员为 Microsoft Exchange Server 维护单独的“允许的发件人”和“阻止的发件人”列表。如果最终用户创建了“允许的发件人”，但该发件人又在管理员的“阻止的发件人”列表中，则邮件安全客户端会将来自该“阻止的发件人”的邮件检测为垃圾邮件并对这些邮件采取处理措施。

7. 单击**处理措施**选项卡，设置邮件安全客户端在检测到垃圾邮件或网络钓鱼事件时采取的处理措施。

注意

有关处理措施的详细信息，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页。

根据配置，邮件安全客户端采取以下某项处理措施：

- **将邮件隔离到服务器端垃圾邮件文件夹**
- **将邮件隔离到用户的垃圾邮件文件夹**

注意

如果选择此处理措施，则配置“最终用户隔离”。有关详细信息，请参阅配置垃圾邮件维护 第 6-62 页。

- **删除整个邮件**
- **添加标记并递交**

8. 单击**保存**。

允许的发件人和阻止的发件人列表

“允许的发件人”列表是可信电子邮件地址的列表。除非启用了**检测网络钓鱼事件**，否则邮件安全客户端并不过滤发自这些地址的邮件中的垃圾邮件。在启用**检测网络钓鱼事件**后，如果客户端在电子邮件中检测到网络钓鱼事件，则即使其发件人属于“允许的发件人”列表，该电子邮件也不会递交。“阻止的发件人”列表是可疑电子邮件地址的列表。客户端始终将发自“阻止的发件人”的电子邮件归类为垃圾邮件并采取适当的处理措施。

“允许的发件人”列表有两个：一个列表供 Microsoft Exchange 管理员使用，另一个列表供最终用户使用。

- Microsoft Exchange 管理员的“允许的发件人”和“阻止的发件人”列表（在**反垃圾邮件**窗口）控制邮件安全客户端处理发往 Microsoft Exchange Server 的电子邮件的方式。
- 最终用户管理安装期间为他们创建的“垃圾邮件文件夹”。最终用户的列表仅影响发往每个单独最终用户的服务器端邮箱存储的邮件。

一般准则

- Microsoft Exchange Server 上“允许的发件人”和“阻止的发件人”列表将覆盖客户端上的相应列表。例如，发件人“user@example.com”在管理员的“阻止的发件人”列表中，但最终用户已将该地址添加到他自己的“允许的发件人”列表中。当发自该发件人的邮件到达 Microsoft Exchange 存储时，邮件安全客户端将这些邮件检测为垃圾邮件并对其采取处理措施。如果客户端采取的处理措施是“将邮件隔离到用户的垃圾邮件文件夹”，它将尝试将邮件递交到最终用户的“垃圾邮件”文件夹，但此后该邮件将被重定向到最终用户的收件箱，因为最终用户允许了该发件人。
- 在使用 Outlook 时，对列表中地址的数量和大小存在限制。为防止出现系统错误，邮件安全客户端会限制最终用户可以包括在其“允许的发件人”列表中的地址数量（该限制根据电子邮件地址的长度和数量计算）。

通配符匹配

对于“允许的发件人”与“阻止的发件人”列表，邮件安全客户端支持通配符匹配。它使用星号 (*) 作为通配符。

邮件安全客户端不支持用户名部分的通配符匹配。但是，如果键入 "*@trend.com" 之类的特征码，客户端仍会将其视为 "@trend.com"。

只能在以下情况下使用通配符：

- 作为一个字符串的第一个或最后一个字符，且旁边有一个句点
- 位于 @ 符号左侧且作为字符串的第一个字符
- 作为作用与通配符相同的字符串的缺失部分，且位于该字符串的开头或结尾

表 6-2. 电子邮件地址的通配符匹配

特征码	匹配的示例	不匹配的示例
john@example.com	john@example.com	与范式不同的所有地址
@example.com *@example.com	john@example.com mary@example.com	john@ms1.example.com john@example.com.us mary@example.com.us
example.com	john@example.com john@ms1.example.com mary@ms1.rd.example.com mary@example.com	john@example.com.us mary@myexample.com.us joe@example.comon
*.example.com	john@ms1.example.com mary@ms1.rd.example.com joe@ms1.example.com	john@example.com john@myexample.com.us mary@ms1.example.comon
example.com.*	john@example.com.us john@ms1.example.com.us john@ms1.rd.example.com.us mary@example.com.us	john@example.com mary@ms1.example.com john@myexample.com.us

特征码	匹配的示例	不匹配的示例
.example.com.	john@ms1.example.com.us john@ms1.rd.example.com.us mary@ms1.example.com.us	john@example.com john@ms1.example.com john@trend.example.us
..*.example.com *****.example.com	与 "*.example.com" 相同	
example.com example.com example.*.com @*.example.com	无效范式	

内容过滤

内容过滤可根据用户定义的规则来评估入站和出站电子邮件。每个规则都包含一系列关键字和短语。“内容过滤”通过将邮件与关键字列表进行比较来评估邮件标题和/或邮件内容。当内容过滤器发现与某个关键字匹配的词时，它将采取处理措施以防将不需要的内容传递到 Microsoft Exchange 客户端。每次对不需要的内容采取处理措施时，邮件安全客户端都可以发送通知。

注意

请不要将“内容扫描”（基于特征码和启发式的反垃圾邮件）与“内容过滤”（基于归类关键字的电子邮件扫描和阻止）混淆。请参阅内容扫描 第 6-8 页。

“内容过滤”为管理员提供了基于邮件文本自身来评估和控制电子邮件传递的方法。可以使用“内容过滤”来监控入站和出站邮件，以检查是否存在骚扰性、冒犯性或其他形式的不当内容。“内容过滤”还提供了同义词检查功能，从而可以扩展策略的能力。例如，可以创建规则以检查有无：

- 色情语言
- 种族歧视语言
- 嵌在电子邮件正文中的垃圾内容

注意

缺省情况下，内容过滤处于禁用状态。

管理内容过滤规则

邮件安全客户端在**内容过滤**窗口中显示所有内容过滤规则。通过导航至以下部分可访问此窗口：

- 对于实时扫描：

  安全设置 > **{邮件安全客户端}** > **配置** > **内容过滤**

- 对于手动扫描：

  扫描 > **手动** > **{展开邮件安全客户端}** > **内容过滤**

- 对于预设扫描：

  扫描 > **预设** > **{展开邮件安全客户端}** > **内容过滤**

过程

1. 查看有关规则的摘要信息，包括：

   - **规则**：WFBS 自带的缺省规则是根据以下类别过滤内容：**亵渎**、**种族歧视**、**性别歧视**、**谣言**和**连环邮件**。缺省情况下，这些规则已禁用。您可以根据需要修改或删除这些规则。如果这些规则都无法满足您的要求，您可以添加自己的规则。

   - **处理措施**：邮件安全客户端在检测到不适当的内容时采取此处理措施。

- **优先级**：邮件安全客户端按照本页所示的顺序依次应用每个过滤器。
- **已启用**：绿色图标表示已启用的规则，红色图标表示已禁用的规则。

2. 执行以下任务：

任务	步骤
启用/禁用“内容过滤”	选择或清除窗口顶部的**启用实时内容过滤**。
添加规则	单击**添加**。 将显示新窗口，供您选择要添加的规则类型。有关详细信息，请参阅内容过滤规则的类型 第 6-17 页。
修改规则	a. 单击规则名称。 此时打开一个新窗口。 b. 窗口中显示的选项取决于规则的类型。要确定规则类型，请查看窗口顶部的面包屑导航，并记下面包屑导航中的第二个项目。例如： “内容过滤” > **匹配任何条件规则** >“编辑规则” 有关您可以修改的规则设置的详细信息，请参阅以下任意主题： • 添加满足任意匹配条件的内容过滤规则 第 6-20 页 • 添加满足所有匹配条件的内容过滤规则 第 6-18 页 **注意** 这种类型的规则不适用于手动和预设内容过滤扫描。 • 添加内容过滤监控规则 第 6-23 页 • 创建内容过滤规则的例外 第 6-25 页

任务	步骤
对规则重新排序	邮件安全客户端按照**内容过滤**窗口上显示的顺序对电子邮件应用内容过滤规则。配置规则的应用顺序。客户端根据各个规则来过滤所有电子邮件，直到内容违例触发了可阻止进一步扫描的处理措施（例如删除或隔离）。更改这些规则的顺序以优化内容过滤功能。 a. 选择与要更改顺序的规则对应的复选框。 b. 单击**重新排序**。 在该规则的顺序号周围会出现一个框。 c. 在**优先级**列框中，删除现有的编号并键入新编号。 **注意** 确保输入的数值不大于列表中规则的总数。如果输入的数值大于规则的总数，WFBS 会忽略该条目，且不更改该规则的顺序。 d. 单击**保存重新排序**。 该规则将移到您输入的优先级级别，所有其他规则的顺序号也将相应地发生改变。 例如，如果选择顺序号为 5 的规则并将其顺序号改为 3，则顺序号为 1 和 2 的规则将保持不变，但顺序号为 3 或更高顺序号的规则将增加一个数。
启用/禁用规则	单击“已启用”列下的图标。
移除规则	删除规则时，邮件安全客户端会更新其他规则的顺序以反映所做的更改。 **注意** 删除规则的操作是不能撤消的，因此请考虑使用禁用规则的方式而不使用删除规则的方式。 a. 选择某个规则。 b. 单击**删除**。

3. 单击**保存**。

内容过滤规则的类型

可以创建按照指定的条件或者发件人或收件人的电子邮件地址来过滤电子邮件的规则。规则中可以指定的条件包括：要扫描哪些邮件标题域，是否扫描电子邮件正文，以及搜索什么关键字。

可以创建以下用途的规则：

- **过滤满足任意已定义条件的邮件**：这种类型的规则能够在扫描期间过滤任何邮件中的内容。有关详细信息，请参阅添加满足任意匹配条件的内容过滤规则 第 6-20 页。
- **过滤满足所有已定义条件的邮件**：这种类型的规则能够在扫描期间过滤任何邮件中的内容。有关详细信息，请参阅添加满足所有匹配条件的内容过滤规则 第 6-18 页。

注意

这种类型的规则不适用于手动和预设内容过滤扫描。

- **监控特定电子邮件帐户的邮件内容**：这种类型的规则可监控特定电子邮件帐户的邮件内容。监控规则类似于一般内容过滤器规则，不同的是它们仅可过滤来自特定电子邮件帐户的内容。有关详细信息，请参阅添加内容过滤监控规则 第 6-23 页。
- **创建特定电子邮件帐户的例外**：这种类型的规则创建特定电子邮件帐户的例外。当豁免特定电子邮件帐户时，将不过滤此帐户中的内容规则违例。有关详细信息，请参阅创建内容过滤规则的例外 第 6-25 页。

创建规则之后，邮件安全客户端开始按照您的规则过滤所有传入和传出的邮件。当出现内容违例时，邮件安全客户端会对违例的电子邮件采取处理措施。安全管理服务器采取的处理措施也取决于用户在规则中设置的处理措施。

添加满足所有匹配条件的内容过滤规则

这种类型的规则不适用于手动和预设内容过滤扫描。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**内容过滤**。

   将显示一个新窗口。
5. 单击**添加**。

   将显示一个新窗口。
6. 选择**过滤满足所有已定义条件的邮件**。
7. 单击**下一步**。
8. 在**规则名称**文本框中键入规则的名称。
9. 选择要过滤其中不适当内容的邮件部分。邮件安全客户端可以按以下内容过滤电子邮件：
   - 标题（发件人、收件人和抄送）
   - 主题
   - 邮件正文或附件的大小
   - 附件文件名

注意

邮件安全客户端仅在“实时扫描”期间支持邮件标题和主题内容的过滤。

10. 单击**下一步**。

11. 选择邮件安全客户端在检测到不适当的内容时将采取的处理措施。邮件安全客户端可以执行以下处理措施（有关描述，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页）：

    - 用文本/文件替换

      注意

      不能替换“发件人”、“收件人”、“抄送”或“主题”文本框中的文本。

    - 隔离整个邮件
    - 隔离邮件部分内容
    - 删除整个邮件
    - 归档
    - 不予处理整个邮件

12. 选择**通知收件人**可使邮件安全客户端通知内容被过滤的电子邮件的目标收件人。

    选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

13. 选择**通知发件人**可使邮件安全客户端通知内容被过滤的电子邮件的发件人。

    选择**不通知外部发件人**，以使邮件安全客户端只向内部邮件发件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

14. 在**高级选项**部分中，单击加号 (+) 图标展开**归档设置**子部分。

    a. 在**隔离目录**文本框中，键入“内容过滤”功能放置隔离电子邮件的文件夹路径，或接受缺省值：`<邮件安全客户端安装文件夹>\storage\quarantine`

b. 在**归档目录**文本框中，键入“内容过滤”功能放置归档电子邮件的文件夹路径，或接受缺省值：<**邮件安全客户端安装文件夹**>`\storage \backup for content filter`

15. 单击加号 (+) 图标展开**替换设置**子部分。

a. 在**替换文件名**文本框中，键入文件的名称（当触发处理措施为“用文本/文件替换”的规则时，“内容过滤”功能会使用该文件替换电子邮件），或接受缺省值。

b. 在**替换文本**文本框中，键入或粘贴替换文本的内容（当电子邮件触发处理措施为“用文本/文件替换”的规则时，“内容过滤”功能会使用此内容），或接受缺省文本。

16. 单击**完成**。

向导关闭并返回“内容过滤”窗口。

添加满足任意匹配条件的内容过滤规则

- 对于实时扫描：

  安全设置 > **{邮件安全客户端}** > **配置设置** > **内容过滤**

- 对于手动扫描：

  扫描 > **手动** > **{展开邮件安全客户端}** > **内容过滤**

- 对于预设扫描：

  扫描 > **预设** > **{展开邮件安全客户端}** > **内容过滤**

过程

1. 单击**添加**。

将显示一个新窗口。

2. 选择**过滤满足任意已定义条件的邮件**。

3. 单击**下一步**。
4. 在**规则名称**文本框中键入规则的名称。
5. 选择要过滤其中不适当内容的邮件部分。邮件安全客户端可以按以下内容过滤电子邮件：
   - 标题（发件人、收件人和抄送）
   - 主题
   - 正文
   - 附件

   注意
   邮件安全客户端仅在“实时扫描”期间支持邮件标题和主题内容的过滤。

6. 单击**下一步**。
7. 添加目标部分的关键字，以便过滤不想要的内容。有关使用关键字的详细信息，请参阅关键字 第 D-5 页。
   a. 如有必要，请选择是否使“内容过滤”区分大小写。
   b. 如果需要，使用 `.txt` 文件类型导入新的关键字文件。
   c. 定义同义词列表。
8. 单击**下一步**。
9. 选择邮件安全客户端在检测到不适当的内容时将采取的处理措施。邮件安全客户端可以执行以下处理措施（有关描述，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页）：
   - 用文本/文件替换

   注意
   不能替换“发件人”、“收件人”、“抄送”或“主题”文本框中的文本。

- 隔离整个邮件
- 隔离邮件部分内容
- 删除整个邮件
- 归档

10. 选择**通知收件人**可使邮件安全客户端通知内容被过滤的电子邮件的目标收件人。

    选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

11. 选择**通知发件人**可使邮件安全客户端通知内容被过滤的电子邮件的发件人。

    选择**不通知外部发件人**，以使邮件安全客户端只向内部邮件发件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

12. 在**高级选项**部分中，单击加号 (+) 图标展开**归档设置**子部分。

    a. 在**隔离目录**文本框中，键入“内容过滤”功能放置隔离电子邮件的文件夹路径，或接受缺省值：**<邮件安全客户端安装文件夹>**`\storage\quarantine`

    b. 在**归档目录**文本框中，键入“内容过滤”功能放置归档电子邮件的文件夹路径，或接受缺省值：**<邮件安全客户端安装文件夹>**`\storage\backup for content filter`

13. 单击加号 (+) 图标展开**替换设置**子部分。

    a. 在**替换文件名**文本框中，键入文件的名称（当触发处理措施为“用文本/文件替换”的规则时，“内容过滤”功能会使用该文件替换电子邮件），或接受缺省值。

    b. 在**替换文本**文本框中，键入或粘贴替换文本的内容（当电子邮件触发处理措施为“用文本/文件替换”的规则时，“内容过滤”功能会使用此内容），或接受缺省文本。

14. 单击**完成**。

向导关闭并返回“内容过滤”窗口。

添加内容过滤监控规则

- 对于实时扫描：

  安全设置 > **{邮件安全客户端}** > **配置设置** > **内容过滤**

- 对于手动扫描：

  扫描 > **手动** > **{展开邮件安全客户端}** > **内容过滤**

- 对于预设扫描：

  扫描 > **预设** > **{展开邮件安全客户端}** > **内容过滤**

过程

1. 单击**添加**。

   将显示一个新窗口。

2. 选择**监控特定电子邮件帐户的邮件内容**。
3. 单击**下一步**。
4. 在**规则名称**文本框中键入规则的名称。
5. 设置要监控的电子邮件帐户。
6. 单击**下一步**。
7. 选择要过滤其中不适当内容的邮件部分。邮件安全客户端可以按以下内容过滤电子邮件：

   - 主题
   - 正文
   - 附件

注意

邮件安全客户端仅在“实时扫描”期间支持这些电子邮件部分的过滤。在“手动扫描”和“预设扫描”期间，不支持邮件标题和主题内容的过滤。

8. 添加目标部分的关键字，以便过滤不想要的内容。有关使用关键字的详细信息，请参阅关键字 第 D-5 页。

   a. 如有必要，请选择是否使“内容过滤”区分大小写。

   b. 如果需要，使用 `.txt` 文件类型导入新的关键字文件。

   c. 定义同义词列表。

9. 单击**下一步**。

10. 选择邮件安全客户端在检测到不适当的内容时将采取的处理措施。邮件安全客户端可以执行以下处理措施（有关描述，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页）：

    - 用文本/文件替换

      注意

      不能替换“发件人”、“收件人”、“抄送”或“主题”文本框中的文本。

    - 隔离整个邮件
    - 隔离邮件部分内容
    - 删除整个邮件
    - 归档

11. 选择**通知收件人**可使邮件安全客户端通知内容被过滤的电子邮件的目标收件人。

    选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

12. 选择**通知发件人**可使邮件安全客户端通知内容被过滤的电子邮件的发件人。

选择**不通知外部发件人**，以使邮件安全客户端只向内部邮件发件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

13. 在**高级选项**部分中，单击加号 (+) 图标展开**归档设置**子部分。

    a. 在**隔离目录**文本框中，键入“内容过滤”功能放置隔离电子邮件的文件夹路径，或接受缺省值：`<邮件安全客户端安装文件夹>\storage\quarantine`

    b. 在**归档目录**文本框中，键入“内容过滤”功能放置归档电子邮件的文件夹路径，或接受缺省值：`<邮件安全客户端安装文件夹>\storage\backup for content filter`

14. 单击加号 (+) 图标展开**替换设置**子部分。

    a. 在**替换文件名**文本框中，键入文件的名称（当触发处理措施为“用文本/文件替换”的规则时，“内容过滤”功能会使用该文件替换电子邮件），或接受缺省值。

    b. 在**替换文本**文本框中，键入或粘贴替换文本的内容（当电子邮件触发处理措施为“用文本/文件替换”的规则时，“内容过滤”功能会使用此内容），或接受缺省文本。

15. 单击**完成**。

    向导关闭并返回“内容过滤”窗口。

创建内容过滤规则的例外

- 对于实时扫描：

  安全设置 > **{邮件安全客户端}** > **配置设置** > **内容过滤**

- 对于手动扫描：

  扫描 > **手动** > **{展开邮件安全客户端}** > **内容过滤**

- 对于预设扫描：

  扫描 > **预设** > **{展开邮件安全客户端}** > **内容过滤**

过程

1. 单击**添加**。

   将显示一个新窗口。

2. 选择**创建特定电子邮件帐户的例外**。

3. 单击**下一步**。

4. 键入规则名称。

5. 在提供的空栏中键入要从内容过滤中豁免的电子邮件帐户，然后单击**添加**。

   该电子邮件帐户将添加到您的豁免电子邮件帐户列表中。对于此列表中的电子邮件帐户，邮件安全客户端不会应用优先级低于此规则的内容规则。

6. 在确定满意电子邮件帐户列表后，单击**完成**。

   向导关闭，并返回**内容过滤**窗口。

数据丢失预防

使用“数据丢失防护”功能可防止通过传出的电子邮件丢失数据。此功能可以保护与设置的范式匹配的身份证号、电话号码、银行账号和其他机密商业信息等数据。

此版本支持以下 Microsoft Exchange 版本：

表 6-3. 支持的 Microsoft Exchange 版本

支持	不支持
2007 x64	2003 x86/x64
2010 x64	2007 x86
	2010 x86

准备工作

监控可能丢失的敏感数据之前，请确定以下内容：

- 需要保护哪些数据不受未经授权用户的访问
- 数据存放的位置
- 数据传输的位置和传输方式
- 哪些用户有权访问或传输这些信息

此重要审核通常需要组织内熟悉敏感信息的多个部门和人员提供内容。以下步骤假定您已经确定敏感信息，并且已经创建了有关处理商业机密信息的安全策略。

“数据丢失防护”功能包含三个基本组成部分：

- **规则**（要搜索的特征码）
- 从过滤中**排除的域**
- **允许的发件人**（从过滤中排除的电子邮件帐户）

有关详细信息，请参阅管理数据丢失防护规则 第 6-27 页。

管理数据丢失防护规则

邮件安全客户端在**数据丢失防护**窗口（**安全设置** > **{邮件安全客户端}** > **配置设置** > **数据丢失防护**）上显示所有数据丢失防护规则。

过程

1. 查看有关规则的摘要信息，包括：
   - **规则**：WFBS 自带缺省规则（请参阅缺省的数据丢失防护规则 第 6-34 页）。缺省情况下，这些规则已禁用。您可以根据需要修改或删除这些规则。如果这些规则都无法满足您的要求，您可以添加自己的规则。

提示

将鼠标指针移至规则名称上方可查看该规则。使用正则表达式的规则会带有放大镜 ( ) 图标标记。

- **处理措施**：邮件安全客户端在触发规则时采取此处理措施。
- **优先级**：邮件安全客户端按照本页所示的顺序依次应用每个规则。
- **已启用**：绿色图标表示已启用的规则，红色图标表示已禁用的规则。

2. 执行以下任务：

任务	步骤
启用/禁用数据丢失防护	选择或清除窗口顶部的**启用实时数据丢失防护**。
添加规则	单击**添加**。 将显示新窗口，供您选择要添加的规则类型。有关详细信息，请参阅添加数据丢失防护规则 第 6-35 页。
修改规则	单击规则名称。 此时打开一个新窗口。有关您可以修改的规则设置的详细信息，请参阅添加数据丢失防护规则 第 6-35 页。

任务	步骤
导入和导出规则	从纯文本文件导入一个或多个规则（或将一个或多个规则导出到纯文本文件），如下文所示。如果需要，您可以使用该文件直接编辑规则。 [SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599] RuleName=Bubbly UserExample= Value=Bubbly [SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6] RuleName=Master Card No. UserExample=Value=.REG.\b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
	要将规则导出到纯文本文件，请在列表中选择一个或多个规则，然后单击**导出**。 **提示** 您只能选择一个窗口页中显示的规则。要选择其他窗口页当前显示的规则，请增加规则列表顶部的“每页行数”的值，以便显示足够多的行来涵盖所有要导出的规则。

任务	步骤
	要导入规则： a. 使用如上所示的格式创建纯文本文件。您也可以单击表下方的**下载更多缺省规则**，然后保存规则。 b. 单击**导入**。 将打开新窗口。 c. 单击**浏览**，找到要导入的文件，然后单击**导入**。 数据丢失防护会导入文件中的规则，并将规则追加到当前规则列表的尾部。 **提示** 如果已有规则超过 10 条，新导入的规则将不会显示在首页。请使用规则列表顶部或底部的页面导航图标显示列表的最后一页。这时便会看到新导入的规则。

任务	步骤
对规则重新排序	邮件安全客户端按照**数据丢失防护**窗口上显示的顺序对电子邮件应用数据丢失防护规则。配置规则的应用顺序。客户端根据各个规则来过滤所有电子邮件，直到内容违例触发了可阻止进一步扫描的处理措施（例如删除或隔离）。更改这些规则的顺序可以优化数据丢失预防功能。 a. 选择与要更改顺序的规则对应的复选框。 b. 单击**重新排序**。 在该规则的顺序号周围会出现一个框。 c. 在**优先级**列框中，删除现有的编号并键入新编号。 **注意** 确保输入的数值不大于列表中规则的总数。如果输入的数值大于规则的总数，WFBS 会忽略该条目，且不更改该规则的顺序。 d. 单击**保存重新排序**。 该规则将移到您输入的优先级级别，所有其他规则的顺序号也将相应地发生改变。 例如，如果选择顺序号为 5 的规则并将其顺序号改为 3，则顺序号为 1 和 2 的规则将保持不变，但顺序号为 3 或更高顺序号的规则将增加一个数。
启用/禁用规则	单击“已启用”列下的图标。
移除规则	删除规则时，邮件安全客户端会更新其他规则的顺序以反映所做的更改。 **注意** 删除规则的操作是不能撤消的，因此请考虑使用禁用规则的方式而不使用删除规则的方式。 a. 选择某个规则。 b. 单击**删除**。

任务	步骤
排除特定域帐户	在公司范围内，机密商业信息的交换是每天必不可少的事情。而且，如果数据丢失防护功能必须过滤所有内部邮件的话，安全管理服务器的处理负担会极重。由于这些原因，您需要设置一个或多个缺省域来代表公司内部的邮件通信，以使“数据丢失预防”不过滤公司域内帐户之间的邮件往来。 此列表允许所有内部电子邮件（隶属于公司域）绕开数据丢失预防规则。至少需要一个这种域。如果您使用多个域，请将其添加到此列表中。 例如：`*@example.com` a. 单击加号 (+) 图标展开**已从数据丢失预防中排除的特定域帐户**部分。 b. 将光标置于**添加**文本框，然后使用以下范式键入域：`*@example.com` c. 单击**添加**。 此时域将出现在**添加**文本框下方显示的列表中。 d. 单击**保存**完成添加过程。 **警告!** 直到您单击**保存**，数据丢失防护功能才会添加域。如果单击**添加**，但没有单击**保存**，则不会添加域。

任务	步骤
向“允许的发件人”列表中添加电子邮件帐户	来自允许的发件人的邮件在您的网络外部进行传递，不会被“数据丢失预防”功能过滤。“数据丢失预防”功能将忽略来自允许列表中的电子邮件帐户的任何邮件内容。 a. 单击加号 (+) 图标展开**允许的发件人**部分。 b. 将光标置于**添加**文本框，然后使用以下范式键入完整的电子邮件地址：`example@example.com` c. 单击**添加**。 此时地址将出现在**添加**文本框下方显示的列表中。 d. 单击**保存**完成添加过程。 **注意** 直到您单击**保存**后，数据丢失防护功能才会添加地址。如果单击**添加**，但没有单击**保存**，则不会添加地址。

向“允许的发件人”列表中导入电子邮件帐户	您可以从纯文本文件中导入电子邮件地址列表，纯文本文件采取每行一个电子邮件帐户的格式：
	`admin@example.com`
	`ceo@example.com`
	`president@example.com`
	a. 单击加号 (+) 图标展开**允许的发件人**部分。
	b. 单击**导入**。
	将打开新窗口。
	c. 单击**浏览**，找到要导入的纯文本文件，然后单击**导入**。
	数据丢失防护会导入文件中的规则，并将规则追加到当前列表的尾部。

3. 单击**保存**。

缺省的数据丢失防护规则

“数据丢失预防”功能自带了一些缺省规则，如下表所示。

表 6-4. 缺省的数据丢失防护规则

规则名称	示例	正则表达式
Visa 卡账号	4111-1111-1111-1111	.REG.\b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
MasterCard 账号	5111-1111-1111-1111	.REG.\b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
American Express 账号	3111-111111-11111	.REG.\b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Diners Club/ Carte Blanche 账号	3111-111111-1111	.REG.[^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG.[^\w]((([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift BIC	BANK US 99	.REG.[^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
ISO 日期	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG.[^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-]

注意

可从 Web 控制台下载包含更多 DLP 规则的 zip 文件。导航到**安全设置** > **{邮件安全客户端}** > **配置设置** > **数据丢失防护**，然后单击**下载更多缺省规则**。

添加数据丢失防护规则

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**数据丢失防护**。

   将显示一个新窗口。
5. 单击**添加**。

   将显示一个新窗口。
6. 选择要评测的邮件部分。邮件安全客户端可以按以下内容过滤电子邮件：
   - 标题（发件人、收件人和抄送）
   - 主题
   - 正文
   - 附件
7. 添加规则。

   添加基于关键字的规则：

   a. 选择**关键字**。

   b. 在所示文本框中键入关键字。关键字的长度必须介于 1 到 64 个字母数字字符之间。

   c. 单击**下一步**。

   添加基于自动生成的表达式的规则：

a. 有关定义正则表达式的准则，请参阅正则表达式 第 D-9 页。

b. 选择**正则表达式 (自动生成)**。

c. 在提供的文本框中，键入**规则名称**。此文本框为必填项。

d. 在**示例**文本框中，键入或粘贴正则表达式要匹配的字符串类型（最大长度为 40 个字符）作为示例。字母数字字符以全部大写形式显示在**示例**文本框下方的阴影区域中，并带有成行的方框。

e. 如果表达式中存在任何常量，请单击包含字符的方框进行选择。

当您单击每个方框时，边框变为红色，表示其为常量，并且自动生成工具会修改阴影区域下方显示的正则表达式。

注意

非数字字母字符（如空格、半角分号和其他标点符号）将被自动视为常量，且无法切换为变量。

---

f. 要验证生成的正则表达式是否与预期范式匹配，请选中**提供另一示例以验证规则 (可选)**。

此选项下方将出现一个测试文本框。

g. 键入另一条您刚才输入的范式的示例。

例如，如果此表达式要匹配特征码为 "01-EX?????20??" 的一连串账号，那么键入另一条匹配的示例，例如 "01-Extreme 2010"，然后单击**测试**。

该工具将验证新示例是否与现有正则表达式匹配，如果匹配，会在文本框旁添加绿色的复选标记图标。如果正则表达式与新示例不匹配，文本框旁将显示红色的 X 图标。

警告!

使用此工具创建的正则表达式不区分大小写。这些表达式只能匹配字符数与示例完全相同的范式；它们无法计算具有“一个或多个”给定字符的范式。

---

h. 单击**下一步**。

添加基于用户定义的表达式的规则：

警告!

正则表达式是一种功能强大的字符串匹配工具。请确保在使用这些表达式前，您已掌握正则表达式的语法。不严谨的正则表达式会极大地影响性能。趋势科技建议从简单的正则表达式开始。在创建新规则时，使用“归档”处理措施并观察“数据丢失防护”功能如何使用规则管理邮件。当确信规则不会产生意外后果时，可以更改处理措施。

---

a. 有关定义正则表达式的准则，请参阅正则表达式 第 D-9 页。

b. 选择**正则表达式 (用户定义)**。

随即将显示**规则名称**和**正则表达式**文本框。

c. 在提供的文本框中，键入**规则名称**。此文本框为必填项。

d. 在**正则表达式**文本框中，键入一条以“`.REG.`”前缀开头的正则表达式，表达式最长为 255 个字符（包括前缀）。

警告!

在向此文本框粘贴内容时，请务必非常小心。如果剪贴板的内容中包含任何无关字符，如特定于操作系统的换行符或 HTML 标记，粘贴的表达式将不准确。鉴于此原因，趋势科技建议手动键入表达式。

---

e. 要验证该正则表达式是否与预期特征码匹配，请选择**提供另一示例以验证规则 (可选)**。

此选项下方将出现一个测试文本框。

f. 键入另一条刚才输入的范式的示例（不超过 40 个字符）。

例如，如果此表达式要匹配特征码为 "ACC-?????20??” 的一连串帐号，那么键入另一条匹配的示例，例如 "Acc-65432 2012"，然后单击**测试**。

该工具将验证新示例是否与现有正则表达式匹配，如果匹配，会在文本框旁添加绿色的复选标记图标。如果正则表达式与新示例不匹配，文本框旁将显示红色的 X 图标。

g. 单击**下一步**。

8. 为邮件安全客户端选择在触发规则时采取的处理措施（有关描述，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页）：

- 用文本/文件替换

> **注意**
> 不能替换“发件人”、“收件人”、“抄送”或“主题”文本框中的文本。

- 隔离整个邮件
- 隔离邮件部分内容
- 删除整个邮件
- 归档
- 不予处理整个邮件

9. 选择**通知收件人**，以将邮件安全客户端设置为：在“数据丢失防护”功能针对特定电子邮件采取措施时，通知目标收件人。

   由于各种原因，您可能希望避免外部收件人接到含有敏感信息的邮件已被阻止的通知。选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

10. 选择**通知发件人**，将邮件安全客户端设置为在数据丢失防护对特定电子邮件采取处理措施时通知预期发件人。

    由于各种原因，您可能希望避免外部发件人接到含有敏感信息的邮件已被阻止的通知。选择**不通知外部发件人**，以使邮件安全客户端只向内部邮件发件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

11. 在**高级选项**部分中，单击加号 (+) 图标展开**归档设置**子部分。

    a. 在**隔离目录**文本框中，键入“数据丢失防护”功能放置隔离电子邮件的文件夹路径，或接受缺省值：`<邮件安全客户端安装文件夹>\storage\quarantine`

b. 在**归档目录**文本框中，键入“数据丢失防护”功能放置归档电子邮件的文件夹路径，或接受缺省值：<**邮件安全客户端安装文件夹**>`\storage\backup for content filter`

12. 单击加号 (+) 图标展开**替换设置**子部分。

a. 在**替换文件名**文本框中，键入文件的名称（当触发处理措施为“用文本/文件替换”的规则时，“数据丢失防护”功能会使用该文件替换电子邮件），或接受缺省值。

b. 在**替换文本**文本框中，键入或粘贴替换文本的内容（当电子邮件触发处理措施为“用文本/文件替换”的规则时，“数据丢失防护”功能会使用此内容），或接受缺省文本。

13. 单击**完成**。

向导关闭并返回“数据丢失防护”窗口。

阻止附件

“阻止附件”功能可防止电子邮件中的附件递交到 Microsoft Exchange 信息存储中。配置邮件安全客户端，使之根据附件类型或附件名称阻止附件，然后“替换”、“隔离”或“删除”带有与条件匹配的附件的所有邮件。

可以在实时、手动和预设扫描中进行阻止，但在手动扫描和预设扫描中不能执行“删除”和“隔离”处理措施。

附件的扩展名可以标识文件类型，例如 `.txt`、`.exe` 或 `.dll`。但是，邮件安全客户端通过检查文件标题（而非文件名）来确定实际的文件类型。许多病毒/恶意软件与特定类型的文件具有密切联系。通过配置邮件安全客户端以根据文件类型来执行阻止，可以降低这些类型的文件给 Microsoft Exchange Server 带来的安全风险。同理，特定的攻击经常与特定的文件名相关联。

提示

使用阻止是控制病毒爆发的一种有效方法。可以临时隔离所有高风险文件类型或具有与已知病毒/恶意软件关联的特定名称的文件。然后，在时间充裕时，可以检查隔离文件夹并对受感染文件采取措施。

配置阻止附件

配置 Microsoft Exchange Server 的阻止附件选项包括设置对包含特定附件的邮件的阻止规则。

- 对于实时扫描：

  安全设置 > **{邮件安全客户端}** > **配置设置** > **阻止附件**

- 对于手动扫描：

  扫描 > **手动** > **{展开邮件安全客户端}** > **阻止附件**

- 对于预设扫描：

  扫描 > **预设** > **{展开邮件安全客户端}** > **阻止附件**

过程

1. 从**目标**选项卡中，根据需要更新以下选项：

   - **所有附件**：客户端可以阻止所有含有附件的电子邮件。但这种扫描方式需要大量处理过程。通过选择要排除的附件类型或名称，可以改进这种类型的扫描。

     - **要排除的附件类型**
     - **要排除的附件名称**

   - **特定附件**：选择这种类型的扫描时，客户端只扫描包含指定附件的电子邮件。这种扫描类型可以非常专一，对检测含有可疑威胁附件的电子邮件非常理想。在指定相对少量的附件名称或类型时，这种扫描运行得非常快。

- **附件类型**：客户端通过检查文件标题（而非文件名）来确定实际的文件类型。
- **附件名称**：缺省情况下，客户端通过检查文件标题（而非文件名）来确定实际的文件类型。在设置“阻止附件”以扫描特定名称时，客户端将根据附件的名称来检测其类型。

- **阻止 ZIP 文件中的附件类型或名称**

2. 单击**处理措施**选项卡，以设置邮件安全客户端在检测附件时所采取的处理措施。邮件安全客户端可以执行以下处理措施（有关描述，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页）：

   - 用文本/文件替换
   - 隔离整个邮件
   - 隔离邮件部分内容
   - 删除整个邮件

3. 选择**通知收件人**可将邮件安全客户端设置为通知包含附件的电子邮件的目标收件人。

   选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

4. 选择**通知发件人**可将邮件安全客户端设置为通知包含附件的电子邮件的发件人。

   选择**不通知外部发件人**，以使邮件安全客户端只向内部邮件发件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

5. 单击加号 (+) 图标展开**替换设置**子部分。

   a. 在**替换文件名**文本框中，键入文件的名称（当触发处理措施为“用文本/文件替换”的规则时，“阻止附件”功能会使用该文件替换电子邮件），或接受缺省值。

   b. 在**替换文本**文本框中，键入或粘贴替换文本的内容（当电子邮件触发处理措施为“用文本/文件替换”的规则时，“阻止附件”功能会使用此内容），或接受缺省文本。

6. 单击**保存**。

Web 信誉

Web 信誉有助于防止访问 Web 上或嵌在电子邮件中的存在安全风险的 URL。Web 信誉对照趋势科技 Web 信誉服务器检查 URL 的信誉，然后将信誉与在客户机上执行的 Web 信誉策略关联。根据使用的策略：

- 安全客户端将阻止或允许访问 Web 站点。
- 邮件安全客户端（仅限邮件与网络安全版）将隔离、删除或标记包含恶意 URL 的电子邮件，或者允许发送邮件（如果 URL 是安全的）。

Web 信誉在进行检测时，会向管理员发送电子邮件通知，并向用户发送在线通知。

对于安全客户端，可根据该客户端的位置（“在办公室”/“不在办公室”）配置不同等级的安全性。

如果 Web 信誉阻止了 URL，并且您感觉此 URL 是安全的，请将此 URL 添加到“允许的 URL”列表中。

提示

为了节省网络带宽，趋势科技建议将企业内部 Web 站点添加到 Web 信誉允许的 URL 列表。

信誉分值

URL 的“信誉分值”可确定其是否为 Web 威胁。趋势科技使用专有的度量方法来计算该分值。

如果某 URL 的分值在定义的阈值范围之内，趋势科技就会将该 URL 视为 Web 威胁；如果分值超出该阈值，则将其视为安全 URL。

安全客户端有三个安全等级，可确定是允许还是阻止访问某 URL。

- **高**：阻止以下页面：

  - **危险**：已证实为欺诈或已知的威胁源
  - **高度可疑**：怀疑为欺诈或可能的威胁源
  - **可疑**：与垃圾邮件关联或可能危及安全的页面
  - **未测试**：尽管趋势科技会主动测试 Web 页面的安全性，但用户在访问新的或不常见的 Web 站点时，可能会遇到未经测试的页面。虽然阻止访问未经测试的页面可以提高安全性，但也会阻止访问安全页面。
- **中**：阻止以下页面：
  - **危险**：已证实为欺诈或已知的威胁源
  - **高度可疑**：怀疑为欺诈或可能的威胁源
- **低**：阻止以下页面：
  - **危险**：已证实为欺诈或已知的威胁源

为邮件安全客户端配置 Web 信誉

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击 **Web 信誉**。

   将显示一个新窗口。
5. 根据需要进行以下更新：
   - **启用 Web 信誉**
   - 安全等级：**高**、**中**或**低**

- 允许的 URL
  - **要允许的 URL：**多个 URL 之间用半角分号 (;) 隔开。单击**添加**。

    注意

    允许 URL 表示允许其所有子域。

    请慎重使用通配符，因为它们可能会允许大量 URL。

  - **允许的 URL 列表：**将不阻止此列表中的 URL。

6. 单击**处理措施**选项卡，并为邮件安全客户端选择在触发 Web 信誉策略时采取的处理措施（有关描述，请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页）：

   - 用文本/文件替换

     注意

     不能替换“发件人”、“收件人”、“抄送”或“主题”文本框中的文本。

   - 将邮件隔离到用户的垃圾邮件文件夹
   - 删除整个邮件
   - 添加标记并递交

7. 选择**对趋势科技尚未评估的 URL 采取处理措施**，以将未分类的 URL 视为可疑对象。将对包含未分类 URL 的电子邮件执行之前步骤中指定的相同处理措施。

8. 选择**通知收件人**，以将邮件安全客户端设置为：在“Web 信誉”功能针对特定电子邮件采取措施时，通知目标收件人。

   由于各种原因，您可能希望避免外部邮件收件人接收“含有恶意 URL 的邮件已被阻止”的通知。选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

9. 选择**通知发件人**，将邮件安全客户端设置为在 Web 信誉对特定电子邮件采取处理措施时通知预期发件人。

由于各种原因，您可能希望避免外部发件人接到含有恶意 URL 的邮件已被阻止的通知。选择**不通知外部发件人**，以使邮件安全客户端只向内部邮件发件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**定义内部地址。

10. 单击**保存**。

移动安全精灵

移动安全精灵设置防止未经授权的设备访问 Microsoft Exchange 服务器以及从该服务器中下载信息。管理员可以识别哪些设备允许访问 Microsoft Exchange 服务器，然后确定这些设备的用户是否可以下载或更新其电子邮件、日历、联系人或任务。

管理员还可以将安全策略应用到设备。这些策略控制密码的长度和复杂性、设备在经过一段时间的不活动后是否应该锁定、设备是否需要使用加密以及一系列不成功的登录尝试后是否应该擦除设备数据。

移动安全精灵支持

表 6-5. 移动设备支持

操作系统	IIS 版本	设备数据保护策略		访问控制		
		EXCHANGE 2007（或更高版本）64 位	EXCHANGE 2003 32 位	EXCHANGE 2010（及更高版本）64 位	EXCHANGE 2007 64 位	EXCHANGE 2003 32 位
• Windows 2008（64 位） • SBS 2008（64 位）	7 +	是	不兼容	是	否	不兼容
Windows 2003（64 位）	6.0	是	不兼容	否	否	不兼容
• Windows 2003（32 位） • SBS 2003（32 位）	6.0	不兼容	否	不兼容	不兼容	否

表 6-6. 移动设备操作系统支持

移动操作系统	操作系统版本
iOS	3.0 - 6.1 (4.3 - 7.0)

移动操作系统	操作系统版本
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

配置设备访问控制

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**移动安全精灵** > **设备访问控制**。

   将显示一个新窗口。
5. 选择**启用设备访问控制**。
6. 单击**添加**。
7. 键入策略名称和有效的策略描述。
8. 通过确认设备所有者，选择允许/拒绝访问 Microsoft Exchange Server 的设备。
   - **任何人**
   - **指定设备所有者**
9. 选择**指定设备所有者**后：
   a. 输入设备所有者的名称并单击**搜索**，以便在 Microsoft Exchange Server 的全球地址列表中查找设备所有者。

b. 选择设备所有者并单击**添加**。

10. 如果设备所有者已知，则从**类型**下拉列表中选择设备的操作系统。
11. 如果是已知的设备所有者，则选择**指定版本号范围**并确认允许的操作系统版本。
12. 指定邮件安全客户端是否应允许访问设备所有者的邮件、日历、联系人或任务。
13. 单击**保存**。

取消等待中的设备擦除

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**移动安全精灵** > **设备擦除**。

   将显示一个新窗口。
5. 确定设备擦除表中的设备，然后单击**取消擦除**。
6. 单击**确定**。

手动擦除设备

过程

1. 导航至**安全设置**。

2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**移动安全精灵** > **设备擦除**。

   将显示一个新窗口。
5. 单击**选择设备**。

   将显示一个新窗口。
6. 输入设备所有者的名字，然后单击**搜索**来查找其设备。
7. 如果设备可以擦除，请选择设备，然后单击**擦除**。

注意

如果搜索后设备状态显示为**成功擦除**或**等待擦除**，则无法选择设备。

配置安全策略

WFBS 使用 Microsoft Exchange 缺省策略作为缺省策略。缺省策略显示在安全策略列表中。

WFBS 不会保留使用 Microsoft Exchange 管理控制台或 Exchange Cmdlet 添加的非缺省策略。

趋势科技建议管理员从 WFBS 管理控制台或 Microsoft Exchange 管理安全策略。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。

3. 单击**配置设置**。

   将显示一个新窗口。

4. 单击**移动安全精灵** > **安全策略**。

   将显示一个新窗口。

5. 单击**添加**。

6. 为策略键入名称和有效的描述。

7. 输入设备所有者的名称并单击**搜索**，以便在 Microsoft Exchange 服务器的全球地址列表中查找设备所有者。

8. 选择设备所有者并单击**添加**。

9. 选择要应用到设备中的安全标准：

   - **最小密码长度**：有关移动设备密码的准则，请参阅“密码复杂度要求 第 6-50 页”。
   - **最小必需字符集数**：有关移动设备密码的准则，请参阅“密码复杂度要求 第 6-50 页”。
   - **设备不活动后锁定设备**
   - **需要在设备上加密**：移动设备必须支持加密。
   - **登录不成功后擦除设备**

10. 单击**保存**。

密码复杂度要求

对不同的设备类型和操作系统有不同的密码复杂度要求。

下表列出了在发行 WFBS 9.0 SP3 时测试的设备的各个复杂度“选项”的行为。

注意

密码复杂度的功能取决于设备类型和操作系统版本。如果指定的密码不符合复杂度要求，大多数设备会向用户提供信息来指示设备的特定要求。

表 6-7. Android 设备

复杂度等级	复杂度要求	
	ANDROID 4	**ANDROID 2**
选项 1	以下类型字符的组合： • 至少一个大写 (A-Z) 或小写 (a-z) 字符 • 至少一个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	字母数字
选项 2	以下类型字符的组合： • 至少一个大写 (A-Z) 或小写 (a-z) 字符 • 至少两个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	以下类型字符的组合： • 字母数字 • 至少两个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 3	以下类型字符的组合： • 至少一个大写 (A-Z) 或小写 (a-z) 字符 • 至少三个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	以下类型字符的组合： • 字母数字 • 至少三个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 4	以下类型字符的组合： • 至少一个大写 (A-Z) 或小写 (a-z) 字符 • 至少四个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	以下类型字符的组合： • 字母数字 • 至少四个数字 (0-9) 或特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

表 6-8. iOS 设备

复杂度等级	复杂度要求
选项 1	以下类型字符的组合： • 字母数字 • 至少一个特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 2	以下类型字符的组合： • 字母数字 • 至少两个特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 3	以下类型字符的组合： • 字母数字 • 至少三个特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 4	以下类型字符的组合： • 字母数字 • 至少四个特殊字符 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

表 6-9. Windows Phone 设备

复杂度等级	复杂度要求	
	Windows Phone 8	**Windows Phone 7**
选项 1	下列至少一种类型的字符： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下至少两种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

复杂度等级	复杂度要求	
	WINDOWS PHONE 8	WINDOWS PHONE 7
选项 2	以下至少两种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下至少两种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 3	以下至少三种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下至少三种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 4	以下所有类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下所有类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

表 6-10. BlackBerry 设备

复杂度等级	复杂度要求
选项 1	至少一个大写 (A-Z) 或小写 (a-z) 字符

复杂度等级	复杂度要求
选项 2	以下至少两种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 3	以下至少三种类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
选项 4	以下所有类型字符的组合： • 大写字符 (A-Z) • 小写字符 (a-z) • 数字字符 (0-9) • 特殊字符 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

邮件安全客户端隔离

当邮件安全客户端在电子邮件中检测到威胁、垃圾邮件、限制的附件和/或限制的内容时，该客户端可以将此邮件移动到隔离文件夹中。此过程将作为邮件/附件删除的备选处理措施，并可防止用户打开受感染的邮件和扩散威胁。

邮件安全客户端上的缺省隔离文件夹是：

<**邮件安全客户端安装文件夹**>\storage\quarantine

为了增加安全性，隔离的文件已进行了加密。要打开加密文件，请使用“恢复加密的病毒和间谍软件”(VSEncode.exe) 工具。请参阅恢复加密文件 第 14-9 页。

管理员可以查询隔离数据库以收集有关被隔离邮件的信息。

使用隔离可以：

- 在设置严格的过滤条件时，消除由于误检重要邮件而将其永久删除的可能性
- 检查触发内容过滤的邮件以确定策略违例的严重性
- 保留员工可能滥用公司邮件系统的证据

注意

不要将隔离文件夹与最终用户的垃圾邮件文件夹混淆。隔离文件夹是一种基于文件的文件夹。不论邮件安全客户端何时隔离电子邮件，它都会将此邮件发送到隔离文件夹。最终用户的垃圾邮件文件夹位于每个用户邮箱的“信息存储”中。最终用户的垃圾邮件文件夹仅接收在执行反垃圾邮件隔离措施时隔离到用户垃圾邮件文件夹的电子邮件，而不接收在执行内容过滤、防病毒/防间谍软件或阻止附件策略隔离措施时隔离的电子邮件。

查询隔离目录

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**隔离** > **查询**。

   将显示一个新窗口。
5. 根据需要进行以下更新：
   - 日期/时间范围

- 隔离原因
  - **所有原因**
  - **指定的类型**：选择“病毒扫描”、“反垃圾邮件”、“内容过滤”、“阻止附件”和/或“无法扫描的邮件部分”。
- 重新发送状态
  - **从未重新发送**
  - **重新发送至少一次**
  - **以上皆是**
- 高级标准
  - **发件人**：发自特定发件人的邮件。如果需要，可以使用通配符。
  - **收件人**：发给特定收件人的邮件。如果需要，可以使用通配符。
  - **主题**：具有特定主题的邮件。如果需要，可以使用通配符。
  - **排序依据**：为结果页设置排序条件。
  - **显示**：每页中的结果数。

6. 单击**搜索**。请参阅查看查询结果并采取处理措施 第 6-56 页。

查看查询结果并采取处理措施

隔离查询结果窗口显示关于邮件的以下信息：

- **扫描时间**
- **发件人**
- **收件人**
- **主题**

- **原因**：隔离此电子邮件的原因。
- **文件名**：电子邮件中被阻止的文件名称。
- **隔离路径**：电子邮件的隔离位置。管理员可以使用 VSEncoder.exe（请参阅恢复加密文件 第 14-9 页）解密文件，然后将其重命名为 `.eml` 进行查看。

警告!
查看受感染文件可能会传播感染。

- **重新发送状态**

过程

1. 如果认为某封邮件不安全，请删除该邮件。

警告!
隔离文件夹中所含的电子邮件具有较高的被感染风险。在处理隔离文件夹中的电子邮件时请格外小心，以免这些邮件意外感染客户端。

2. 如果认为某封邮件安全，请选择该邮件并单击“重新发送”图标 ( )。

注意
如果要重新发送最初用 Microsoft Outlook 发送的隔离邮件，收件人可能会收到同一邮件的多个副本。出现这种情况的原因是“病毒扫描”引擎将其扫描的每封邮件剥离成几个部分。

3. 如果无法重新发送邮件，可能因为 Microsoft Exchange Server 上的系统管理员帐户不存在。
   a. 使用 Windows 注册表编辑器，在服务器中打开下列注册表项：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
   Exchange\CurrentVersion
   ```

   b. 按如下方法编辑项：

警告!

错误地编辑注册表可能会严重损害您的系统。在对注册表项进行更改之前，请将您计算机中所有有价值的数据进行备份。

- `ResendMailbox` {**管理员邮箱**}

  示例：`admin@example.com`

- `ResendMailboxDomain` {**管理员的域**}

  示例：`example.com`

- `ResendMailSender` {**管理员的电子邮件帐户**}

  示例：`admin`

c. 关闭注册表编辑器。

维护隔离目录

使用此功能可手动或自动删除隔离的邮件。此功能可删除所有邮件，包括已重新发送的邮件和尚未重新发送的邮件。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。

4. 单击**隔离** > **维护**。

   将显示一个新窗口。

5. 根据需要进行以下更新：

- **启用自动维护**：只适用于自动维护。
- 要删除的文件
  - **所有被隔离文件**
  - **从未重新发送过的被隔离文件**
  - **至少重新发送过一次的被隔离文件**
- **处理措施**：邮件应存储的天数。例如，如果当天是 11 月 21 日，您在**删除超过多少天的选定文件**中键入的是 `10`，则邮件安全客户端在执行自动删除时会删除 11 月 11 日之前的所有文件。

6. 单击**保存**。

配置隔离目录

在 Microsoft Exchange Server 上配置隔离目录。该隔离目录会免予扫描。

注意

隔离目录基于文件，不驻留在“信息存储”中。

邮件安全客户端会按照配置的处理措施来隔离电子邮件。以下是隔离目录：

- **防病毒**：隔离包含病毒/恶意软件、间谍软件/灰色软件、蠕虫病毒、特洛伊木马和其他恶意威胁的电子邮件。
- **反垃圾邮件**：隔离垃圾邮件和网络钓鱼电子邮件。
- **阻止附件**：隔离包含受限制附件的电子邮件。
- **内容过滤**：隔离包含受限制内容的电子邮件。

缺省情况下，所有目录的路径一样（`<`**邮件安全客户端安装文件夹**`>\storage\quarantine`）。您可以更改每个目录或所有目录的路径。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**隔离** > **目录**。

   将显示一个新窗口。
5. 为以下隔离目录设置路径：
   - **防病毒**
   - **反垃圾邮件**
   - **内容过滤**
   - **阻止附件**
6. 单击**保存**。

邮件安全客户端的通知设置

WFBS 可针对各种警报，以电子邮件的形式发送通知。

通过使用“定制内部电子邮件定义”,您可以将通知配置为仅应用到内部电子邮件。如果您的公司具有两个或多个域，并且您希望将来自这些域的电子邮件视为内部电子邮件，则这将非常有用。例如，example.com 和 example.net。

当选择了**防病毒**、**内容过滤**和**阻止附件**的“通知设置”下的**不通知外部收件人**复选框后，“内部电子邮件定义”列表上的收件人将会收到通知邮件。请不要将“内部电子邮件定义”列表与“允许的发件人”列表混淆。

要防止将所有来自具有外部域地址的电子邮件标记为垃圾邮件，请将外部电子邮件地址添加到反垃圾邮件的**允许的发件人**列表中。

关于定制内部电子邮件定义

邮件安全客户端将电子邮件通信分成两种网络类别：内部和外部。客户端会查询 Microsoft Exchange Server，以了解内部地址和外部地址是如何定义的。所有内部地址都共享相同的域，而所有外部地址都不属于该域。

例如，如果内部域地址是“@trend_1.com”，则邮件安全客户端会将“abc@trend_1.com”和“xyz@trend_1.com”之类的地址归类为内部地址。客户端将“abc@trend_2.com”和“jondoe@123.com”等所有其他地址归类为外部地址。

只能将一个域定义为邮件安全客户端的内部地址。如果使用 Microsoft Exchange 系统管理器更改服务器上的首选地址，则邮件安全客户端无法将新地址识别为内部地址，因为邮件安全客户端无法检测到收件人策略已更改。

例如，公司有两个域地址：@example_1.com 和 @example2.com。您将 @example_1.com 设置为首选地址。则邮件安全客户端将带有该首选地址的电子邮件地址识别为内部地址（即 abc@example_1.com 或 xyz@example_1.com 是内部地址）。然后，您使用 Microsoft Exchange 系统管理器将首选地址改为 @example_2.com。这意味着 Microsoft Exchange 现在应该将 abc@example_2.com 和 xyz@example_2.com 等地址识别为内部地址。

配置邮件安全客户端的通知设置

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**操作** > **通知设置**。

   将显示一个新窗口。
5. 根据需要进行以下更新：

- **电子邮件地址**：WFBS 将代表其发送通知邮件的地址。
- **内部电子邮件定义**
  - **缺省**：WFBS 将把来自同一域的电子邮件视为“内部电子邮件”。
  - **定制**：指定各个电子邮件地址或域，以将其视为内部电子邮件。

6. 单击**保存**。

配置垃圾邮件维护

在**垃圾邮件维护**窗口中，可以为最终用户隔离 (EUQ) 或服务器端隔离配置设置。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**操作** > **垃圾邮件维护**。

   将显示一个新窗口。
5. 单击**启用最终用户隔离工具**。

   当启用 EUQ 工具时，将在每个客户机邮箱的服务器端创建隔离文件夹，并在最终用户的 Outlook 文件夹树中显示“**垃圾邮件**”文件夹。启用 EUQ 并创建“垃圾邮件”文件夹后，EUQ 将把垃圾邮件过滤到用户的“垃圾邮件”文件夹。有关详细信息，请参阅管理最终用户隔离 第 6-63 页。

提示

如果选择此选项，趋势科技建议禁用客户端上的趋势科技反垃圾邮件工具栏选项，以提高客户机性能。

清除**启用最终用户隔离工具**可对 Microsoft Exchange Server 上的所有邮箱禁用最终用户隔离工具。当禁用 EUQ 工具时，用户的“垃圾邮件”文件夹将保留，但是不会将检测为垃圾邮件的邮件移动到该文件夹中。

6. 单击**创建垃圾邮件文件夹并删除垃圾邮件**，立即为新创建的邮件客户机及已删除“垃圾邮件”文件夹的现有邮件客户机创建“垃圾邮件”文件夹。对于其他的现有邮件客户端，则会删除超过“客户端垃圾邮件文件夹设置”文本框中指定天数的垃圾邮件。

7. 在**删除超过 {number} 天的垃圾邮件**中，修改邮件安全客户端保留垃圾邮件的时间长度。缺省值是 14 天，最大时间限制是 30 天。

8. 要为特定用户禁用“最终用户隔离”工具，请执行以下操作：

   a. 在**最终用户隔离工具例外列表**下，键入希望禁用其 EUQ 的最终用户的电子邮件地址。

   b. 单击**添加**。

      该最终用户的电子邮件地址被添加到禁用了 EUQ 的地址列表中。

      要从该列表中移除最终用户并恢复 EUQ 服务，请从此列表中选择该最终用户的电子邮件地址，然后单击**删除**。

9. 单击**保存**。

管理最终用户隔离

在安装期间，邮件安全客户端会向每个最终用户的服务器端邮箱添加一个**垃圾邮件**文件夹。当垃圾邮件到达时，系统会根据邮件安全客户端预定义的垃圾邮件过滤器规则，将这些邮件隔离到此文件夹中。最终用户可以查看该垃圾邮件文件夹以打开、阅读或删除可疑的电子邮件。请参阅配置垃圾邮件维护 第 6-62 页。

另外，管理员也可以在 Microsoft Exchange 上创建“垃圾邮件”文件夹。当管理员创建一个邮箱帐户时，邮箱实体不会在 Microsoft Exchange Server 中立即创建，但会在下列情况下创建：

- 最终用户首次登录其邮箱时
- 第一封电子邮件到达邮箱时

EUQ 创建垃圾邮件文件夹之前，管理员必须首先创建邮箱实体。

客户端端垃圾邮件文件夹

最终用户可以打开隔离进垃圾邮件文件夹中的电子邮件。打开其中一封邮件后，实际的电子邮件上将显示两个按钮：**允许的发件人**和**查看允许的发件人列表**。

- 当最终用户打开“垃圾邮件”文件夹中的电子邮件并单击**允许的发件人**时，该电子邮件的发件人地址会添加到最终用户的**允许的发件人**列表。
- 单击**查看允许的发件人列表**可打开另一个窗口，最终用户在该窗口中可以按电子邮件地址或域查看和修改其允许的发件人列表。

允许的发件人

当最终用户在“垃圾邮件”文件夹中收到电子邮件并单击**允许的发件人**时，邮件安全客户端会将此邮件移到最终用户的本地收件箱中，并将发件人的地址添加到最终用户自己的“允许的发件人”列表中。邮件安全客户端会将事件记录在日志中。

当 Microsoft Exchange Server 收到来自最终用户“允许的发件人”列表中的地址的邮件时，它会将这些邮件递交到最终用户的收件箱中，而不论邮件标题或内容中包含哪些信息。

注意

邮件安全客户端还为管理员提供了“允许的发件人”和“阻止的发件人”列表。邮件安全客户端先应用管理员的“允许的发件人”和“阻止的发件人”，然后考虑最终用户的列表。

最终用户隔离整理功能

邮件安全客户端整理功能每 24 小时在缺省时间上午 2:30 执行下列任务：

- 自动删除过期的垃圾邮件
- 重新创建垃圾邮件文件夹（如果已删除）
- 为新创建的邮件帐户创建垃圾邮件文件夹
- 维护电子邮件规则

整理功能是邮件安全客户端不可或缺的一部分，无需进行配置。

趋势科技支持/调试程序

支持/调试程序可帮助您调试或只报告邮件安全客户端进程的状态。在遇到意外的困难时，可以使用调试程序创建调试报表并将其发送给趋势科技技术支持进行分析。

每个邮件安全客户端都将邮件插入到程序中，然后在执行时将处理措施记录到日志文件中。可以将日志转发给趋势科技技术支持人员以帮助他们调试您环境中的实际程序流。

可以使用调试程序生成有关以下模块的日志：

- 邮件安全客户端主服务
- 邮件安全客户端远程配置服务器
- 邮件安全客户端系统看护程序
- 病毒扫描 API (VSAPI)
- 简单邮件传输协议 (SMTP)
- 公共网关接口 (CGI)

缺省情况下，MSA 将日志保存在以下目录中：

<邮件安全客户端安装文件夹>`\Debug`

可使用任何文本编辑器查看输出。

生成系统调试报表

生成调试报表可帮助趋势科技技术支持解决您遇到的问题。

过程

1. 导航至**安全设置**。
2. 选择邮件安全客户端。
3. 单击**配置设置**。

   将显示一个新窗口。
4. 单击**操作** > **支持/调试程序**。

   将显示一个新窗口。
5. 选择要监控的模块：
   - 邮件安全客户端**主服务**
   - 邮件安全客户端**远程配置服务器**
   - 邮件安全客户端**系统看护程序**
   - Exchange Server 2003、2007 或 2010 中的**病毒扫描 API (VSAPI)**
   - Exchange Server 2013 中的**存储级扫描**
   - Exchange Server 2003 中的**简单邮件传输协议 (SMTP)**
   - Exchange Server 2007、2010 或 2013 中的**传输服务**
   - **公共网关接口 (CGI)**
6. 单击**应用**。

   调试程序开始收集选定模块的数据。

实时监控程序

实时监控程序可显示有关选定 Microsoft Exchange Server 及其邮件安全客户端的最新信息。它显示有关已扫描邮件的信息和防护统计信息，包括发现的病毒和垃圾邮件数量、阻止的附件数量和内容违例数量。还会检查客户端是否正常运行。

使用实时监控程序

过程

1. 通过 Web 控制台访问实时监控程序的步骤：
   a. 导航至**安全设置**。
   b. 选择客户端。
   c. 单击**配置设置**。

      将显示一个新窗口。
   d. 单击窗口右上部分中的**实时监控程序**链接。
2. 要通过 Windows“开始”菜单访问实时监控程序，请单击**所有程序** > **趋势科技邮件安全客户端** > **实时监控程序**。
3. 单击**重置**可将防护统计信息重置为零。
4. 单击**清除内容**可清除有关已扫描邮件的旧信息。

向出站电子邮件添加免责声明

您只能向传出电子邮件添加免责声明邮件。

过程

1. 创建一个文本文件，并向该文件添加免责声明文本。
2. 修改注册表中的下列项：
   - 第一项：

     路径：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     注册表项：`EnableDisclaimer`

     类型：`REG_DWORD`

     数据值：`0` — **禁用**，`1` — **启用**
   - 第二项：

     路径：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     注册表项：`DisclaimerSource`

     类型：`REG_SZ`

     值：免责声明内容文件的完整路径。

     例如，`C:\Data\Disclaimer.txt`

     注意

     缺省情况下，WFBS 会检测出站邮件是发送到内部域还是外部域，并为发送到外部域的每个邮件添加一个免责声明。用户可以覆盖缺省设置，并给除以下注册表项中包括的域以外的每个出站邮件添加一个免责声明：
   - 第三项：

     路径：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     注册表项：`InternalDomains`

类型：`REG_SZ`

值：键入要排除的域名。使用分号 (;) 分隔多个项。

例如：`domain1.org;domain2.org`

注意

这里的域名是 Exchange Server 的 DNS 名称。

第 7 章

管理扫描

本章介绍如何在安全客户端和邮件安全客户端（仅限邮件与网络安全版）上运行扫描，以保护您的网络和客户机免遭威胁。

关于扫描

扫描期间，趋势科技扫描引擎通过称为特征匹配的过程，结合使用特征码文件执行第一级检测。由于每种威胁都含有有别于任何其他代码的独特签名或迹象字符串，因此可以将这些代码的稳定片段捕获到特征码文件中。然后，引擎将每个被扫描文件的特定部分与特征码文件中的特征码进行比较，以查看有无匹配现象。

当扫描引擎检测到含有威胁或的文件时，它会执行清除、隔离、删除或用文本/文件替换（仅限邮件与网络安全版）之类的处理措施。在设置扫描任务时，可以定制这些处理措施。

安全无忧软件提供**三种类型的扫描**。每种扫描都有不同的目的与用途，但所有扫描的配置方式都大体相同。

- 实时扫描。有关详细信息，请参阅实时扫描 第 7-2 页。
- 手动扫描。有关详细信息，请参阅手动扫描 第 7-3 页。
- 预设扫描。有关详细信息，请参阅预设扫描 第 7-5 页。

运行扫描时，安全客户端可以使用以下两种扫描方法中的任意一种：

- 云安全扫描
- 传统扫描

有关详细信息，请参阅扫描方法 第 5-3 页。

实时扫描

实时扫描是持续进行的扫描。

在每次打开、下载、复制或修改文件时，**安全客户端**中的实时扫描都会扫描该文件是否存在威胁。有关配置实时扫描的详细信息，请参阅配置安全客户端实时扫描 第 5-6 页。

在处理电子邮件时，**邮件安全客户端**（仅限邮件与网络安全版）中的实时扫描会扫描所有传入邮件、SMTP 邮件、公共文件夹上发布的文档和从其他

Microsoft Exchange Server 复制的文件，来保护所有已知的病毒入口。有关配置实时扫描的详细信息，请参阅为邮件安全客户端配置实时扫描： 第 6-5 页。

手动扫描

手动扫描是按需扫描。

安全客户端上的手动扫描可消除来自文件的威胁并根除旧的感染（如果有），来使再次感染的可能性降至最低。

邮件安全客户端（仅限邮件与网络安全版）上的手动扫描可扫描 Microsoft Exchange Server 信息存储中的所有文件。

扫描所用的时间取决于客户机的硬件资源和要扫描的文件数。如果从 Web 控制台远程运行扫描，则可以由安全管理服务器管理员停止正在进行的手动扫描，如果在客户机上直接运行扫描，则可以由用户停止正在进行的手动扫描。

提示

趋势科技建议在威胁爆发后运行手动扫描。

运行手动扫描

此过程描述安全管理服务器管理员如何从 Web 控制台运行**安全客户端**和**邮件安全客户端**（仅限邮件与网络安全版）上的手动扫描。

注意

右键单击 Windows 任务栏中的安全客户端图标并单击**立即扫描**，还可以从客户机直接运行手动扫描。无法在 Microsoft Exchange Server 上直接运行手动扫描。

过程

1. 导航至**扫描** > **手动扫描**。

2. （可选）在运行手动扫描之前自定义扫描设置。

指导信息和说明	建议的扫描设置
要自定义**安全客户端**的扫描设置，请单击台式机组或服务器组。 请参阅安全客户端的扫描目标和处理措施 第 7-7 页。 **注意** 用户从客户机直接运行手动扫描时，也可以使用安全客户端扫描设置。但是，如果您授予用户配置自己的扫描设置的权限，则将在扫描期间使用用户配置的设置。	目标 • 所有可扫描文件：包括所有可扫描文件。无法扫描的文件是受密码保护的文件、加密文件或超出用户定义的扫描限制的文件。 • 扫描压缩文件，最多压缩层数为 1：扫描位于 1 层压缩层深度的压缩文件。缺省服务器组的缺省设置为“关闭”，缺省台式机组的缺省设置为“开启”。 例外 • 不扫描安装有趋势科技产品的目录 高级设置 • 修改间谍软件/灰色软件允许列表（只适用于防间谍软件）
要自定义**邮件安全客户端**的扫描设置，请展开客户端，并单击以下选项： • **防病毒**：单击此项会使客户端扫描病毒和其他恶意软件。请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页。 • **内容过滤**：单击此项会使客户端扫描电子邮件中是否有被禁止的内容。请参阅管理内容过滤规则 第 6-14 页。 • **阻止附件**：单击此项会使客户端扫描电子邮件中是否有违反附件规则的附件。请参阅配置阻止附件 第 6-40 页。	• 客户端将扫描所有可扫描文件。电子邮件的正文也包括在扫描对象之列。 • 当客户端在文件中检测到病毒或其他恶意软件时，它会清除该文件。如不能清除文件，则会用文本/文件加以替换。 • 当客户端在文件中检测到特洛伊木马或蠕虫病毒时，它会用文本或文件替换特洛伊木马或蠕虫病毒。 • 当客户端检测到带有加壳软件的文件时，它会用文本或文件替换加壳软件。 • 客户端不清除受感染的压缩文件。这样可以减少“实时扫描”过程所需的时间。

3. 选择要扫描的组或邮件安全客户端。

4. 单击**立即扫描**。

   安全管理服务器向客户端发送通知，以运行手动扫描。出现的“扫描通知结果”窗口将显示收到通知的客户端数量和未收到通知的客户端数量。

5. 要停止正在进行的扫描，请单击**停止扫描**。

   安全管理服务器向客户端发送另一条通知，以停止手动扫描。出现的“停止扫描通知结果”窗口将显示收到通知的客户端数量和未收到通知的客户端数量。如果安全客户端因运行扫描而脱机或者出现了网络中断，则它们可能收不到通知。

预设扫描

预设扫描类似于手动扫描，但是它按配置的时间和频率扫描所有文件和电子邮件（仅限邮件与网络安全版）。使用预设扫描可以对客户机自动执行例行扫描，并提高威胁管理的效率。

提示

在非高峰时段运行预设扫描，以最大限度地减少可能对用户和网络造成的中断。

配置预设扫描

趋势科技建议不要将扫描和更新预设在同一时间运行。这样会导致预设扫描提前停止。同理，如果在预设扫描运行期间启动手动扫描，则预设扫描会停止，但是会根据其时间表重新运行。

过程

1. 导航至**扫描** > **预设扫描**。

2. 单击**时间表**选项卡。

a. 配置扫描频率（每天一次、每周一次或每月一次）和开始时间。每个组或邮件安全客户端都可具有自身的时间表。

> **注意**
> 对于每月预设报表，如果您选择 31、30 或 29 日，而该月没有该日期，则该月将不会运行扫描。

b. （可选）选择**完成预设扫描后关闭客户机**。

c. 单击**保存**。

3. （可选）单击**设置**选项卡，定制预设扫描设置。

指导信息和说明	建议的扫描设置
要自定义**安全客户端**的扫描设置，请单击台式机组或服务器组。请参阅安全客户端的扫描目标和处理措施 第 7-7 页。 **注意** 如果您授予用户配置其自身扫描设置的权限，则在扫描期间将使用用户配置的设置。	目标 • 所有可扫描文件：包括所有可扫描文件。无法扫描的文件是受密码保护的文件、加密文件或超出用户定义的扫描限制的文件。 • 扫描压缩文件，最多压缩层数为 2：扫描位于 2 层压缩层深度的压缩文件。
	例外 • 不扫描安装有趋势科技产品的目录
	高级设置 • 修改间谍软件/灰色软件允许列表（只适用于防间谍软件）

指导信息和说明	建议的扫描设置
要自定义**邮件安全客户端**的扫描设置，请展开客户端，并单击以下选项： • **防病毒**：单击此项会使客户端扫描病毒和其他恶意软件。请参阅邮件安全客户端的扫描目标和处理措施 第 7-14 页。 • **内容过滤**：单击此项会使客户端扫描电子邮件中是否有被禁止的内容。请参阅管理内容过滤规则 第 6-14 页。 • **阻止附件**：单击此项会使客户端扫描电子邮件中是否有违反附件规则的附件。请参阅配置阻止附件 第 6-40 页。	• 客户端在每周日的上午 5:00 开始执行扫描。 • 定制该时间表使之在客户端的非高峰时间中运行。客户端将扫描所有可扫描文件。电子邮件的正文也包括在扫描对象之列。 • 当客户端在文件中检测到病毒或其他恶意软件时，它会清除该文件。如不能清除文件，则会用文本/文件加以替换。 • 当客户端检测到文件中带有特洛伊木马或蠕虫病毒时，它会用文本/文件替换这种病毒。 • 当客户端检测到文件中带有加壳软件时，它会用文本/文件替换该软件。 • 客户端不清除受感染的压缩文件。

4. 选择将应用预设扫描设置的组或邮件安全客户端。

注意

要禁用预设扫描，请清除组或邮件安全客户端所对应的复选框。

5. 单击**保存**。

安全客户端的扫描目标和处理措施

为每种扫描类型（手动扫描、预设扫描和实时扫描）配置以下设置：

目标选项卡

选择方法:

- **所有可扫描文件**：包括所有可扫描文件。无法扫描的文件是受密码保护的文件、加密文件或超出用户定义的扫描限制的文件。

注意

此选项提供最大的安全可能性。但扫描所有文件需要占用大量时间和资源，在某些情况下可能是不需要的。因此，您可能希望限制客户端要扫描的文件数量。

- **IntelliScan 使用“真实文件类型”标识**：基于真实文件类型扫描文件。请参阅 IntelliScan 第 D-2 页。
- **扫描带以下扩展名的文件**：基于扩展名手动指定要扫描的文件。多个条目之间用逗号隔开。

选择扫描触发：

- **读取**：扫描正在读取其内容的文件；在打开、执行、复制或移动文件时读取这些文件。
- **写入**：扫描正在写入其内容的文件；在修改、保存、下载或从其他位置复制文件时写入该文件的内容。
- **读取或写入**

扫描例外

下列设置是可配置的：

- 启用或禁用例外
- 从扫描中排除趋势科技产品目录
- 从扫描中排除其他目录

  指定目录路径中的所有子目录也将被排除
- 从扫描中排除带有完整路径的文件名
- 排除文件扩展名

  文件扩展名中不允许使用通配符，例如 "*"

注意

（仅限邮件与网络安全版）如果客户机上正在运行 Microsoft Exchange Server，趋势科技建议从扫描中排除所有 Microsoft Exchange Server 文件夹。要在全局基础上排除扫描 Microsoft Exchange Server 文件夹，请转到**首选项** > **全局设置** > **安全客户端 {选项卡}** > **通用扫描设置**，然后选择**当安装到 Microsoft Exchange Server 时排除 Microsoft Exchange Server 文件夹**。

高级设置

扫描类型	选项
实时扫描	**扫描 POP3 邮件**：缺省情况下，邮件扫描只能扫描“收件箱”和“垃圾邮件”文件夹中通过端口 110 发送的新邮件。它不支持安全 POP3 (SSL-POP3)。 • 装有 Service Pack 2 的 Outlook Express™ 6.0（仅在 Windows XP 上） • Windows Mail™（仅在 Microsoft Vista 上） • Microsoft Outlook 2000、2002 (XP)、2003、2007、2010 或 2013 • Mozilla Thunderbird 1.5 或更高版本 邮件扫描无法检测 IMAP 邮件中的安全风险。使用邮件安全客户端（仅限邮件与网络安全版）可以检测 IMAP 邮件中的安全风险和垃圾邮件。
实时扫描、手动扫描	**扫描网络上的映射驱动器和共享文件夹**：选中该项可扫描物理位于其他计算机但已映射到本地计算机的目录。
实时扫描	**在系统关闭期间扫描软盘**
实时扫描	**启用 IntelliTrap**：IntelliTrap 可检测压缩文件中的恶意代码，如 bot 程序。请参阅 IntelliTrap 第 D-2 页。
实时扫描	**在内存中检测到的隔离恶意软件变种**：启用实时扫描和行为监控并选择该选项后，将扫描正在运行的进程内存中的压缩恶意软件。“行为监控”检测到的任何打包恶意软件都会被隔离。

扫描类型	选项
实时扫描、手动扫描和预设扫描	**扫描压缩文件，最多压缩层数为 __**：压缩文件每压缩一次都会生成一个层。如果受感染文件已压缩了多层，则必须扫描其指定数量的压缩层以检测感染情况。但是，扫描多个压缩层会需要更长的时间和更多的资源。
实时扫描、手动扫描和预设扫描	**修改间谍软件/灰色软件允许列表**：此设置无法从客户端控制台进行配置。
手动扫描、预设扫描	**CPU 利用率/扫描速度**：安全客户端可以在扫描一个文件之后、开始扫描下一个文件之前暂停。 从以下选项中进行选择： • **高**：不间断连续扫描文件 • **中**：如果 CPU 占用高于 50%，则在文件扫描时暂停，如果等于或低于 50%，则不暂停 • **低**：如果 CPU 占用高于 20%，则在文件扫描时暂停，如果等于或低于 20%，则不暂停
手动扫描、预设扫描	**运行高级清除**：安全客户端会停止流氓安全软件（也称为 FakeAV）进行的活动。客户端还可以使用高级清除规则来主动检测并停止存在 FakeAV 行为的应用程序。 **注意** 提供前瞻性保护的同时，高级清除也会导致大量误报。

间谍软件/灰色软件允许列表

某些应用程序之所以被趋势科技归类为间谍软件/灰色软件，不是因为它们会损害所安装的系统，而是因为它们可能会使客户机或网络面临恶意软件或黑客的攻击。

安全无忧软件包括具有潜在风险的应用程序列表，缺省情况下，将防止在客户机上执行这些应用程序。

如果客户端需要运行被趋势科技归类为间谍软件/灰色软件的任何应用程序，则您需要将该应用程序名称添加到间谍软件/灰色软件允许列表中。

处理措施选项卡

以下是安全客户端可针对病毒/恶意软件执行的处理措施：

表 7-1. 病毒/恶意软件扫描处理措施

处理措施	描述
删除	删除受感染文件。
隔离	更名受感染文件，然后将其移动到客户机上的临时隔离目录。 然后，安全客户端会将隔离文件发送至指定的隔离目录（缺省情况下位于安全管理服务器上）。 安全客户端会对发送至此目录的隔离文件进行加密。 如果需要恢复任何隔离文件，请使用 VSEncrypt 工具。
清除	先清除受感染文件，然后才允许对该文件进行完全访问。 如果该文件无法清除，则安全客户端会执行第二种处理措施，其可以是下列任何一种处理措施：隔离、删除、更名和不予处理 可对所有类型的恶意软件执行此处理措施，可能的病毒/恶意软件除外。 **注意** 某些文件无法清除。有关详细信息，请参阅非可清除文件 第 D-24 页。
更名	将受感染文件的扩展名更改为 "vir"。用户最初不能打开更名的文件，但是将该文件与特定应用程序关联后，即可打开该文件。 打开更名的受感染文件时，病毒/恶意软件可能会执行。
不予处理	仅在手动扫描和预设扫描期间执行。安全客户端不能在实时扫描期间使用此扫描处理措施，这是因为，如果在检测到打开或执行受感染文件的企图时不执行处理措施，则会允许执行病毒/恶意软件。实时扫描期间可以使用所有其他扫描处理措施。
拒绝访问	仅在实时扫描期间执行。如果安全客户端检测到打开或执行受感染文件的企图，它会立即阻止该操作。 用户可以手动删除受感染文件。

安全客户端执行的扫描处理措施取决于检测到间谍软件/灰色软件的扫描类型。虽然可以为每种病毒/恶意软件类型配置特定的处理措施，但是只能为所有类型的间谍软件/灰色软件配置一种处理措施。例如，如果安全客户端在手动扫描（扫描类型）期间检测到任何类型的间谍软件/灰色软件，它会清除（处理措施）受影响的系统资源。

以下是安全客户端可针对恶意软件/灰色软件执行的处理措施：

表 7-2. 间谍软件/灰色软件扫描处理措施

处理措施	描述
清除	终止进程或删除注册表、文件、cookie 和快捷方式。
不予处理	不对检测到的间谍软件/灰色软件组件执行任何处理措施，但会在日志中记录间谍软件/灰色软件检测情况。此处理措施只能在手动扫描和预设扫描期间执行。在实时扫描期间，处理措施是“拒绝访问”。 如果检测到的间谍软件/灰色软件包括在允许列表中，安全客户端将不会执行任何处理措施。
拒绝访问	拒绝访问（复制、打开）检测到的间谍软件/灰色软件组件。此处理措施只能在实时扫描期间执行。在手动扫描和预设扫描期间，处理措施是“不予处理”。

ActiveAction

不同类型的病毒/恶意软件需要不同的扫描处理措施。定制扫描处理措施需要有关病毒/恶意软件的知识，并且可能会是冗长而乏味的任务。安全无忧软件使用 ActiveAction 来应对这些问题。

ActiveAction 是针对病毒/恶意软件的一组预配置的扫描处理措施。如不熟悉扫描处理措施或者不能确定何种扫描处理措施适合特定类型的病毒/恶意软件，那么趋势科技建议您使用 ActiveAction。

使用 ActiveAction 具有以下好处：

- ActiveAction 使用趋势科技建议的扫描处理措施。用户不必花费时间配置扫描处理措施。
- 病毒编写者会不断改变病毒/恶意软件攻击计算机的方式。更新 ActiveAction 设置以抵御最新威胁和最新的病毒/恶意软件攻击方法。

下表详细说明了 ActiveAction 如何处理各种类型的病毒/恶意软件：

表 7-3. 趋势科技建议的对病毒和恶意软件的扫描处理措施

病毒/恶意软件类型	实时扫描		手动扫描/预设扫描	
	第一处理措施	第二处理措施	第一处理措施	第二处理措施
恶作剧程序	隔离	删除	隔离	删除
特洛伊木马程序/蠕虫病毒	隔离	删除	隔离	删除
加壳软件	隔离	N/A	隔离	N/A
潜在病毒/恶意软件	隔离	N/A	不予处理或用户配置的处理措施	N/A
病毒	清除	隔离	清除	隔离
测试病毒	拒绝访问	N/A	N/A	N/A
其他恶意软件	清除	隔离	清除	隔离

说明和提醒：

- 对于潜在病毒/恶意软件，实时扫描期间的缺省处理措施是“隔离”，而手动扫描和预设扫描期间的缺省处理措施是“不予处理”。如果这些不是您的首选处理措施，则可以将其更改为“删除”或“更名”。
- 某些文件无法清除。有关详细信息，请参阅非可清除文件 第 D-24 页。
- ActiveAction 不可用于间谍软件/灰色软件扫描。
- 在提供新的特征码文件时，这些设置的缺省值可能会更改。

高级设置

扫描类型	选项
实时扫描、预设扫描	**检测到病毒/间谍软件时在台式机或服务器上显示警报消息**
实时扫描、预设扫描	**检测到潜在病毒/间谍软件时在台式机或服务器上显示警报消息**
手动扫描、实时扫描和预设扫描	**检测到潜在病毒/恶意软件时运行清除操作：**仅当选择 ActiveAction 且已针对潜在病毒/恶意软件定制处理措施时才可用。

邮件安全客户端的扫描目标和处理措施

为每种扫描类型（手动扫描、预设扫描和实时扫描）配置以下设置：

目标选项卡

- 扫描目标
- 其他威胁扫描设置
- 扫描例外

处理措施选项卡

- 扫描处理措施/ActiveAction
- 通知
- 高级设置

扫描目标

选择扫描目标：

- **所有附件文件**：仅排除加密或受密码保护的文件。

注意

此选项提供最大的安全可能性。但扫描所有文件需要占用大量时间和资源，在某些情况下可能是不需要的。因此，您可能希望限制客户端要扫描的文件数量。

- **IntelliScan**:根据真实文件类型扫描文件。请参阅 IntelliScan 第 D-2 页。
- **特定文件类型**：WFBS 将扫描选定类型且带有选定扩展名的文件。多个条目之间用半角分号 (;) 隔开。

选择其他选项：

- **启用 IntelliTrap**：IntelliTrap 可检测到压缩文件中的恶意代码，如 bot 程序。请参阅 IntelliTrap 第 D-2 页。

- **扫描邮件正文**：扫描可能包含嵌入威胁的电子邮件正文。

其他威胁扫描设置

选择客户端应扫描的其他威胁。有关这些威胁的详细信息，请参阅了解威胁 第 1-20 页。

选择其他选项：

- **清除前备份受感染的文件**：WFBS 在清除威胁之前，会进行备份。加密备份文件并将文件存储在客户端的以下目录：

  `<邮件安全客户端安装文件夹>\storage\backup`

  您可以在**高级选项**部分的**备份设置**子部分中更改该目录。

  要解密文件，请参阅恢复加密文件 第 14-9 页。

- **不清除受感染的压缩文件以优化性能**

扫描例外

在**目标**选项卡下，转到**例外**部分，然后从以下条件中选择客户端在将电子邮件从扫描中排除时将使用的条件：

- **邮件正文大小超过**：邮件安全客户端仅在邮件正文大小小于或等于指定大小时才扫描电子邮件。
- **附件大小超过**：邮件安全客户端仅在附件文件大小小于或等于指定大小时才扫描电子邮件。

> **提示**
> 趋势科技建议限制为 30 MB。

- **解压缩文件数超过**：当压缩文件内解压缩文件的总数超过此数值时，邮件安全客户端最多只扫描此选项所限制的文件数。
- **解压缩文件大小超过**：邮件安全客户端仅扫描在解压缩后小于或等于此大小的压缩文件。
- **压缩层数超过**：邮件安全客户端仅扫描具有的压缩层数小于或等于指定数量的压缩文件。例如，如果将该限制设置为 5 个压缩层，则邮件安全客户端将扫描前 5 层的压缩文件，但不扫描第 6 层或更高层中的压缩文件。

- **解压缩文件大小为压缩文件大小的 "x" 倍**：邮件安全客户端仅在解压缩文件大小与压缩文件大小的比率小于该数值时才扫描压缩文件。此功能可阻止邮件安全客户端扫描可能导致“拒绝服务 (DoS)”攻击的压缩文件。当邮件服务器的资源被不需要的任务大量占用时，就会发生 DoS 攻击。阻止邮件安全客户端扫描解压缩为大型文件的文件可帮助防止此问题发生。

  示例：在下表中，为 "x" 键入的值为 100。

文件大小（未压缩）	文件大小（未压缩）	结果
500 KB	10 KB（比率为 50:1）	已扫描
1,000 KB	10 KB（比率为 100:1）	已扫描
1,001 KB	10 KB（比率超过 100:1）	未扫描 *
2,000 KB	10 KB（比率为 200:1）	未扫描 *

* 邮件安全客户端采取用户针对排除的文件所配置的处理措施。

扫描处理措施

管理员可以配置邮件安全客户端使之根据病毒/恶意软件、特洛伊木马及蠕虫病毒呈现的威胁类型采取相应处理措施。如果使用定制的处理措施，则可以为每种威胁类型设置处理措施。

表 7-4. 邮件安全客户端定制的处理措施

处理措施	描述
清除	从受感染邮件的正文和附件中删除恶意代码。剩余的电子邮件文本、任何未感染的文件和已清除的文件都将传递到目标收件人。趋势科技建议对病毒/恶意软件使用的缺省扫描处理措施是清除。 在有些情况下，邮件安全客户端无法清除某个文件。 在手动扫描或预设扫描期间，邮件安全客户端会更新“信息存储”，并用已清除的文件替换原先的文件。

处理措施	描述
用文本/文件替换	删除受感染/过滤的内容，并用文本或文件加以替换。电子邮件将传递给目标收件人，但会通过替换的文本通知收件人原始内容已受感染并被替换。 对于内容过滤和数据丢失防护，您只能替换正文或附件文本框（不包括“发件人”、“收件人”、“抄送”或“主题”）中的文本。
隔离整个邮件	（仅适用于实时扫描）仅将受感染的内容隔离到隔离目录中，且收件人将收到不含此内容的邮件。 对于内容过滤、数据丢失防护和阻止附件，会将整个邮件移动到隔离目录。
隔离邮件部分内容	（仅适用于实时扫描）仅将受感染或过滤的内容隔离到隔离目录中，且收件人将收到不含此内容的邮件。
删除整个邮件	（仅适用于实时扫描）删除整个电子邮件。原始收件人将不会收到邮件。
不予处理	将恶意文件的病毒感染情况记录在病毒日志中，但不采取任何措施。被排除的文件，加密文件或密码保护的文件会传递至收件人，而不会更新日志。 对于内容过滤，按原样递交邮件。
归档	将邮件移动到归档目录中，并将邮件传递给原始收件人。
将邮件隔离到服务器端垃圾邮件文件夹	将整个邮件发送到安全管理服务器以便隔离。
将邮件隔离到用户的垃圾邮件文件夹	将整个邮件发送到用户的垃圾邮件文件夹以便隔离。文件夹位于“信息存储”的服务器端。
添加标记并递交	向电子邮件标题信息中添加一个标记，该标记将其标识为垃圾邮件，然后将其递交给目标收件人。

除了这些处理措施以外，您还可以配置以下选项：

- **对群发邮件行为启用处理措施：**为群发邮件行为类型的威胁选择“清除”、“用文本/文件替换”、“删除整个邮件”、“不予处理”或“隔离邮件部分内容”。

- **当清除不成功时执行**：为不成功的清除尝试设置辅助处理措施。从“用文本/文件替换”、“删除整个邮件”、“不予处理”或“隔离邮件的一部分”中选择处理措施。

ActiveAction

下表详细说明了 ActiveAction 如何处理各种类型的病毒/恶意软件：

表 7-5. 趋势科技建议的对病毒和恶意软件的扫描处理措施

病毒/恶意软件类型	实时扫描		手动扫描/预设扫描	
	第一处理措施	第二处理措施	第一处理措施	第二处理措施
病毒	清除	删除整个邮件	清除	用文本/文件替换
特洛伊木马程序/蠕虫病毒	用文本/文件替换	N/A	用文本/文件替换	N/A
加壳软件	隔离邮件部分内容	N/A	隔离邮件部分内容	N/A
其他恶意代码	清除	删除整个邮件	清除	用文本/文件替换
其他威胁	隔离邮件部分内容	N/A	用文本/文件替换	N/A
群发邮件行为	删除整个邮件	N/A	用文本/文件替换	N/A

扫描处理措施通知

选择**通知收件人**，以将邮件安全客户端设置为：在针对特定电子邮件采取处理措施时，通知目标收件人。由于各种原因，您可能希望避免外部收件人接到含有敏感信息的邮件已被阻止的通知。选择**不通知外部收件人**，以使邮件安全客户端只向内部邮件收件人发送通知。请从**操作** > **通知设置** > **内部邮件定义**中定义内部地址。

您也可以禁止将通知发送给欺骗性发件人的外部收件人。

高级设置（扫描处理措施）

设置	详细信息

宏	宏病毒是针对特定应用程序的病毒，它们可感染伴随应用程序的宏实用程序。高级宏扫描使用启发式扫描检测宏病毒，或者剥离检测到的所有宏代码。启发式扫描是一种有效的病毒检测方法，它使用病毒码识别和基于规则的技术来搜索恶意宏代码。这种方法在检测不包含已知病毒特征的先前未被发现的病毒和威胁时非常有用。
	
	邮件安全客户端会根据您配置的处理措施，对恶意宏代码采取处理措施。
	
	• **启发式级别**
	  • 级别 1 使用最精确的条件，但检测到的宏代码最少。
	  • 级别 4 检测到的宏代码最多，但使用的条件最不精确，因此可能错误地将安全的宏代码识别为包含恶意宏代码。
	
	提示
	趋势科技建议将启发式扫描级别设置为 2。此级别在扫描未知宏病毒时具有较高的检测率、扫描速度快，并且它只使用必要的规则来检查宏病毒字符串。使用级别 2 时，将安全的宏代码错误地识别为恶意代码的比率也非常低。
	
	• **删除高级宏扫描检测到的所有宏**：剥离在所扫描文件上检测到的所有宏代码

无法扫描的邮件部分	为加密的和/或受密码保护的文件设置处理措施和通知条件。从“用文本/文件替换”、“隔离整个邮件”、“删除整个邮件”、“不予处理”或“隔离邮件部分内容”中选择处理措施。
排除的邮件部分	为已经排除的邮件部分设置处理措施和通知条件。从“用文本/文件替换”、“隔离整个邮件”、“删除整个邮件”、“不予处理”或“隔离邮件部分内容”中选择处理措施。
备份设置	在客户端清除受感染文件之前保存这些文件备份的位置。
替换设置	为替换文本配置文本和文件。如果处理措施为**用文本/文件替换**，WFBS 将用此文本字符串和文件替换威胁。

第 8 章

管理更新

本章介绍安全无忧软件的组件和更新过程。

更新概述

所有组件更新都来自趋势科技 ActiveUpdate 服务器。如果有更新可用，安全管理服务器将下载更新的组件，然后将它们分发给安全客户端和邮件安全客户端（仅限邮件与网络安全版）。

如果安全管理服务器管理大量安全客户端，则更新可能会占用大量的服务器计算机资源，从而影响服务器的稳定性和性能。为解决此问题，安全无忧软件提供了**更新代理**功能，允许某些安全客户端共享向其他安全客户端分发更新的任务。

下表介绍了安全管理服务器和安全客户端的组件更新选项，以及建议的使用时机：

表 8-1. 更新选项

更新顺序	描述	建议事项
1. ActiveUpdate 服务器或定制更新源 2. 安全管理服务器 3. 客户端	趋势科技安全管理服务器从 ActiveUpdate 服务器或定制更新源接收更新的组件，并将它们直接部署到客户端（安全客户端和邮件安全客户端）。	如果安全管理服务器与安全客户端之间无低带宽网段，请使用此方法。
1. ActiveUpdate 服务器或定制更新源 2. 安全管理服务器 3. 更新代理、邮件安全客户端、不含更新代理的安全客户端 4. 所有其他安全客户端	趋势科技安全管理服务器从 ActiveUpdate 服务器或定制更新源接收更新的组件，并将它们直接部署到： • 更新代理 • 邮件安全客户端 • 不含更新代理的安全客户端 然后，更新代理会将这些组件部署到各自的安全客户端。如果这些安全客户端无法更新，则会直接从安全管理服务器进行更新。	如果安全管理服务器与安全客户端之间有低带宽网段，请使用此方法来平衡网络上的通信负载。

更新顺序	描述	建议事项
1. ActiveUpdate 服务器 2. 安全客户端	无法从任何源更新的安全客户端会直接从 ActiveUpdate 服务器进行更新。 **注意** 邮件安全客户端绝对不会直接从 ActiveUpdate 服务器进行更新。如果所有源均不可用，邮件安全客户端会退出更新过程。	此机制只能作为最后手段。

可更新组件

安全无忧软件利用组件确保客户端免遭最新安全威胁的侵害。运行手动或预设更新可使这些组件保持最新。

可从**实时状态**窗口查看“爆发防御”、“防病毒”、“防间谍软件”与“网络病毒”组件的状态。如果 安全无忧软件 正在保护 Microsoft Exchange Server（仅限邮件与网络安全版），则您还可以查看“反垃圾邮件”组件的状态。安全无忧软件 会在需要进行组件更新时向管理员发送通知。

下表列出了安全管理服务器从 ActiveUpdate 服务器下载的组件：

表 8-2. 邮件组件（仅限邮件与网络安全版）

组件	分发对象	描述
邮件安全客户端反垃圾邮件特征码	邮件安全客户端	反垃圾邮件特征码可识别电子邮件和电子邮件附件中的最新垃圾邮件。
邮件安全客户端反垃圾邮件引擎（32 位/64 位）	邮件安全客户端	反垃圾邮件引擎可检测到电子邮件和电子邮件附件中的垃圾邮件。

组件	分发对象	描述
邮件安全客户端扫描引擎（32 位/64 位）	邮件安全客户端	扫描引擎可检测到电子邮件和电子邮件附件中的 Internet 蠕虫病毒、群发邮件程序、特洛伊木马、网络钓鱼站点、间谍程序、网络漏洞以及病毒。
邮件安全客户端 URL 过滤引擎（32 位/64 位）	邮件安全客户端	URL 过滤引擎可促进 安全无忧软件 和趋势科技 URL 过滤服务之间的通信。URL 过滤服务是对 URL 进行分级并将分级信息提供给 安全无忧软件 的系统。

表 8-3. 防病毒和云安全扫描

组件	分发对象	描述
病毒扫描引擎（32 位/64 位）	安全客户端	所有趋势科技产品的核心在于扫描引擎，最初，开发扫描引擎是为了响应早期基于文件的病毒。如今的扫描引擎极其完善，能够检测不同类型的病毒和恶意软件。扫描引擎也会检测开发并用于研究的受控病毒。 此引擎并非扫描每个文件的每个字节，而是与特征码文件结合起来识别以下内容： • 病毒代码的迹象特征 • 病毒在文件中的准确位置

组件	分发对象	描述
云安全云端病毒码	不会分发给安全客户端。此病毒码将保留在安全管理服务器中，并且会在响应接收自安全客户端的扫描查询时加以使用。	在云安全扫描模式中，安全客户端使用协同工作的两个轻量级特征码，这两个特征码可提供传统防恶意软件和防间谍软件特征码提供的相同防护。 **云安全云端病毒码**包含多数病毒码定义。**云安全客户端病毒码**包含在云安全云端病毒码中找不到的所有其他病毒码定义。 安全客户端使用**云安全客户端病毒码**扫描安全威胁。在扫描期间无法确定文件风险的安全客户端，会将扫描查询发送到扫描服务器（安全管理服务器上托管的服务），以验证风险。扫描服务器使用**云安全云端病毒码**验证风险。安全客户端会“缓存”扫描服务器提供的扫描查询结果，以改善扫描性能。
云安全客户端病毒码	使用云安全扫描的安全客户端	
病毒码	使用传统扫描的安全客户端	病毒码包含帮助安全客户端识别最新病毒/恶意软件和混合威胁攻击的信息。趋势科技每周都会多次创建和发布新版本的病毒码，而在发现特别具有破坏性的病毒/恶意软件时会随时创建和发布新版本的病毒码。
IntelliTrap 特征码	安全客户端	IntelliTrap 特征码可以检测打包为可执行文件的实时压缩文件。 有关详细信息，请参阅 IntelliTrap 第 D-2 页。
IntelliTrap 例外特征码	安全客户端	IntelliTrap 例外特征码包含“允许的”压缩文件的列表。
损害清除引擎（32 位/64 位）	安全客户端	损害清除引擎会扫描并移除特洛伊木马和特洛伊木马进程。
损害清除模板	安全客户端	损害清除引擎使用损害清除模板来识别特洛伊木马文件和进程，以便引擎将它们清除。

组件	分发对象	描述
内存检查特征码	安全客户端	该技术通过模拟文件执行提供增强的多歧或变种病毒扫描，并加强基于病毒码的扫描。然后结果会在受控的环境中进行分析，获得恶意企图证据，从而极大减少对系统性能的影响。

表 8-4. 防间谍软件

组件	分发对象	描述
间谍软件/灰色软件扫描引擎 v.6（32 位/64 位）	安全客户端	间谍软件扫描引擎扫描间谍软件/灰色软件，并对其执行适当的扫描处理措施。
间谍软件/灰色软件特征码 v.6	安全客户端	间谍软件特征码识别以下位置中的间谍软件/灰色软件：文件和程序、内存中的模块、Windows 注册表和 URL 快捷方式。
间谍软件/灰色软件特征码	安全客户端	

表 8-5. 网络病毒

组件	分发对象	描述
防火墙特征码	安全客户端	防火墙特征码类似于病毒码，可帮助客户端识别病毒特征（表示存在网络病毒的独特位和字节的特征码）。

表 8-6. 行为监控和设备控制

组件	分发对象	描述
行为监控检测特征码（32 位/64 位）	安全客户端	此特征码包含用于检测可疑威胁行为的规则。
行为监控核心驱动程序（32 位/64 位）	安全客户端	此内核模式驱动程序监控系统事件并将其传递给行为监控核心服务，以便实施策略。

组件	分发对象	描述
行为监控核心服务（32 位/64 位）	安全客户端	此用户模式服务有下列功能： • 提供 rootkit 检测 • 控制对外部设备的访问 • 保护文件、注册表项和服务
行为监控配置特征码	安全客户端	行为监控驱动程序使用此特征码来识别普通系统事件并将其从策略实施范围中排除。
损害恢复引擎	安全客户端	损害恢复引擎会在可疑威胁修改文件和执行其他恶意行为之前接收系统事件和备份文件。此引擎也会在它收到文件恢复请求之后还原受影响的文件。
损害恢复特征码	安全客户端	损害恢复特征码包含用于监控可疑威胁行为的策略。
数字签名特征码	安全客户端	此特征码包含有效数字签名的列表，行为监控核心服务使用该列表来确定造成系统事件的源程序是否安全。
策略强制特征码	安全客户端	行为监控核心服务将针对此特征码中的策略检查系统事件。
内存扫描触发特征码（32/64 位）	安全客户端	如果内存扫描触发服务检测到内存中的进程未压缩，则会执行其他扫描引擎。

表 8-7. 爆发防御

组件	分发对象	描述
漏洞检查特征码（32 位/64 位）	安全客户端	含有有关所有漏洞的数据库的文件。漏洞检查特征码为扫描引擎扫描已知漏洞提供指示。

表 8-8. 浏览器利用

组件	分发对象	描述
浏览器利用阻止特征码	安全客户端	该特征码会识别最新的 web 浏览器利用，并阻止这些形式的利用损害 web 浏览器。

组件	分发对象	描述
脚本分析器特征码	安全客户端	该特征码能够分析 web 页面中的脚本，并识别恶意脚本。

HotFix、Patch 和 Service Pack

在官方产品发布后，趋势科技经常会开发以下项，以解决问题，增强产品性能或添加新功能：

- 关键 Patch 第 D-2 页
- Hotfix 第 D-2 页
- Patch 第 D-8 页
- Service Pack 第 D-23 页

当上述项目可用时，供应商或技术支持供应商可能会联系您。请访问趋势科技 Web 站点来获取有关新 Hot Fix、Patch 和 Service Pack 发布的信息：

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

所有发布都包括一个包含有安装、部署和配置信息的自述文件。执行安装前，请仔细阅读该自述文件。

安全管理服务器更新

自动更新

安全管理服务器会自动执行以下更新：

- 安装安全管理服务器后，该服务器会立即从趋势科技 ActiveUpdate 服务器更新。
- 只要启动安全管理服务器，它就会更新组件与“爆发防御”策略。

- 缺省情况下，预设更新每隔一小时运行一次（可从 Web 控制台更改更新频率）。

手动更新

如果更新比较紧迫，则从 Web 控制台运行手动更新。

服务器更新提醒和提示

- 更新之后，安全管理服务器会自动将组件更新分发给客户端。有关分发给客户端的组件的详细信息，请参阅可更新组件 第 8-3 页。
- 纯 IPv6 安全管理服务器无法执行以下任务：
  - 直接从趋势科技 ActiveUpdate 服务器或纯 IPv4 定制更新源获得更新。
  - 将更新直接分发给纯 IPv4 客户端。

  同样，纯 IPv4 安全管理服务器也无法直接从纯 IPv6 定制更新源获得更新，以及将更新分发给纯 IPv6 客户端。

  在这些情况下，要使安全管理服务器能够获得并分发更新，需使用可以转换 IP 地址的双栈代理服务器（如 DeleGate）。
- 如果使用代理服务器连接到 Internet，请在**首选项** > **全局设置** > **代理服务器**选项卡中设置正确的代理服务器设置，以便成功下载更新。

组件复制

趋势科技会定期发布特征码文件以使客户端防护保持最新。由于定期提供特征码文件更新，因此安全管理服务器会使用一种称为**组件复制**的机制，该机制可以更快速地下载特征码文件。

可以从趋势科技 ActiveUpdate 服务器下载最新版本的完全特征码文件时，也可以下载增量特征码。增量特征码是完全特征码文件的较小版本，说明了最新特征码文件和先前完全特征码文件版本之间的差异。例如，如果最新版本为 175，则增量特征码 v_173.175 包含在版本 175 中而不在版本 173 中的签名（特征码编号以 2 为增量发布，因此 V173 是前一完全特征码版本）。增量病毒码 v_171.175 包括 V175 中的签名，在 V171 中没有这些签名。

要减少下载最新特征码时生成的网络流量，安全管理服务器会执行组件复制（一种服务器仅下载增量特征码的组件更新方式）。要利用组件复制，请确保定期更新安全管理服务器。否则，将强制服务器下载完全特征码文件。

组件复制适用于以下组件：

- 病毒码
- Smart Scan Agent Pattern
- 损害清除模板
- IntelliTrap 例外特征码
- 间谍软件特征码

配置安全管理服务器更新源

开始之前

缺省情况下，安全管理服务器从趋势科技 ActiveUpdate 服务器获取更新。如果安全管理服务器无法直接访问 ActiveUpdate 服务器，则可以指定定制更新源。

- 如果源为**趋势科技 ActiveUpdate 服务器**，请确保安全管理服务器具有 Internet 连接；如果使用代理服务器，请测试是否可以使用代理服务器设置建立 Internet 连接。有关详细信息，请参阅配置 Internet 代理服务器设置 第 11-2 页。
- 如果源为定制更新源（**含有当前文件副本的 Intranet 位置**或**备用更新源**），请为此更新源设置适当的环境和更新资源。此外，还应确保安全管理服务器和此更新源之间存在有效连接。如果在设置更新源时需要帮助，请联系技术支持提供商。
- 纯 IPv6 安全管理服务器无法直接从趋势科技 ActiveUpdate 服务器，或其他纯 IPv4 定制更新源更新。同样，纯 IPv4 安全管理服务器也无法直接从纯 IPv6 定制更新源更新。为使安全服务器能够连接到更新源，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

过程

1. 导航至**更新** > **源**。
2. 在**服务器**选项卡上，选择一个更新源。

- **趋势科技 ActiveUpdate 服务器**
- **含有当前文件副本的 Intranet 位置：**键入源的通用命名约定 (UNC) 路径，例如 `\\Web\ActiveUpdate`。还要指定安全管理服务器将用来连接此源的登录凭证（用户名和密码）。
- **备用更新源：**键入此源的 URL。请确保目标 HTTP 虚拟目录（Web 共享）可用于安全管理服务器。

3. 单击**保存**。

手动更新安全管理服务器

安装或升级服务器之后（无论是否存在爆发），请手动更新安全管理服务器上的组件。

过程

1. 开始手动更新有两种方法：
   - 导航至**更新** > **手动**。
   - 导航至**实时状态**并转到**系统状态** > **组件更新**，然后单击**立即更新**。
2. 选择要更新的组件。

   有关组件的详细信息，请参阅可更新组件 第 8-3 页。
3. 单击**更新**。

   此时将出现新窗口，显示更新状态。如果更新成功，安全管理服务器将自动向客户端分发更新的组件。

为安全管理服务器配置预设更新

将安全管理服务器配置为定期检查其更新源并自动下载任何可用更新。使用预设更新是确保针对威胁的防护措施保持最新的一种简便有效的方式。

在发生病毒/恶意软件爆发时，趋势科技快速作出响应以更新病毒码文件（每周可能发布多次更新）。扫描引擎和其他组件也会定期更新。趋势科技建议每天更新一次组件（在病毒/恶意软件爆发时更新更频繁）以帮助确保客户端具有最新的组件。

重要信息

避免预设扫描与运行更新同时进行。这样会导致“预设扫描”意外停止。

过程

1. 导航至**更新** > **预设**。
2. 选择要更新的组件。

   有关组件的详细信息，请参阅可更新组件 第 8-3 页。
3. 单击**时间表**选项卡，然后指定更新时间表。
   - **传统扫描更新**包括除云安全云端病毒码和云安全客户端病毒码之外的所有组件。选择每日、每周还是每月更新一次，然后指定**更新间隔**的值，即安全管理服务器将执行更新的小时数。安全管理服务器会在此时间段的任意给定时间进行更新。

     注意

     对于每月预设更新（不推荐），如果您选择 31、30 或 29 日，而该月没有该日期，则该月将不会运行更新。
   - **云安全扫描更新**仅包括云安全云端病毒码和云安全客户端病毒码。如果您的所有客户端均未使用云安全扫描，请忽略此项。
4. 单击**保存**。

还原组件

还原是指恢复到病毒码、云安全客户端病毒码和病毒扫描引擎的先前版本。如果这些组件未正常运行，则将它们还原到其先前的版本。安全管理服务器会保

留病毒扫描引擎的当前版本和先前版本，以及传统病毒码和云安全客户端病毒码的最近三个版本。

注意

只能还原上述组件。

安全无忧软件 对于运行 32 位和 64 位平台的客户端使用不同的扫描引擎。您需要分别还原这些扫描引擎。还原过程对于所有类型的扫描引擎都相同。

过程

1. 导航到**更新** > **还原**。
2. 针对特定组件单击**同步**，以通知客户端将其组件版本与服务器上的版本同步。
3. 针对特定组件单击**还原**，以在安全管理服务器和客户端上还原该组件。

安全客户端和邮件安全客户端更新

自动更新

安全客户端和邮件安全客户端（仅限邮件与网络安全版）可自动执行以下更新：

- 安装后立即从安全管理服务器更新客户端。
- 安全管理服务器每次完成更新后，自动将更新发送至客户端。
- 更新代理每次完成更新后，自动将更新发送至各自的安全客户端。
- 缺省情况下，预设更新：
  - 在“在办公室”的安全客户端上每 8 小时运行一次

- 在“不在办公室”的安全客户端上每 2 小时运行一次

- 缺省情况下，邮件安全客户端会每隔 24 小时在上午 12:00 运行一次预设更新。

手动更新

如果更新紧急，请从 Web 控制台上运行手动更新。导航至**实时状态**，转到**系统状态** > **组件更新**，然后单击**立即部署**。

客户端更新提醒和提示

- 安全客户端从安全管理服务器、更新代理或趋势科技 ActiveUpdate 服务器进行更新。

  仅从安全管理服务器上更新邮件安全客户端。

  有关更新过程的详细信息，请参阅更新概述 第 8-2 页。

- 纯 IPv6 客户端无法直接从纯 IPv4 安全管理服务器/更新代理和趋势科技 ActiveUpdate 服务器获得更新。

  同样，纯 IPv4 客户端无法直接从纯 IPv6 安全管理服务器/更新代理获得更新。

  在这些情况下，要使客户端获得更新，需使用可以转换 IP 地址的双栈代理服务器（如 DeleGate）。

- 有关客户端更新的组件的详细信息，请参阅可更新组件 第 8-3 页。

- 客户端在从安全管理服务器更新时，除了更新组件，还接收更新的配置文件。客户端需要配置文件来应用新设置。每次通过 Web 控制台修改客户端设置时，配置文件也随之更改。

更新代理

更新代理是安全客户端，它们可以从安全管理服务器或 ActiveUpdate 服务器接收更新的组件，并将它们部署到其他安全客户端。

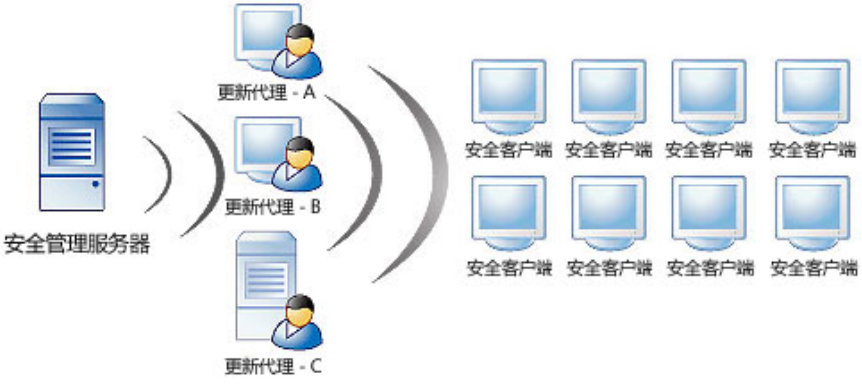
如果您发现客户机和趋势科技安全管理服务器之间的网段为“带宽低”或“流量高”，则可以指定安全客户端充当更新代理。更新代理无需任何安全客户端，即可通过访问安全管理服务器来获取组件更新，从而减少网络带宽消耗。如果网络按位置分段，且各段之间的网络链接经常出现高流量负载，则趋势科技建议在每个段上至少允许一个安全客户端充当更新代理。

更新代理更新过程如下所述：

1. 安全管理服务器会通知更新代理有新的更新。

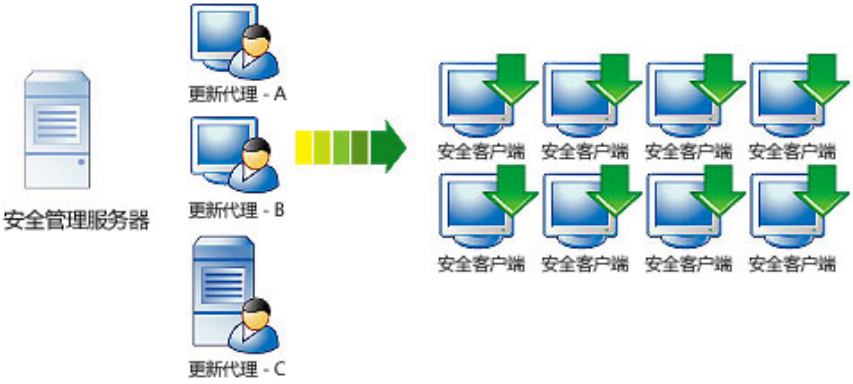
2. 更新代理从安全管理服务器下载更新的组件。

3. 然后，安全管理服务器通知安全客户端有更新的组件可用。



4. 每个安全客户端都会加载一个“更新代理顺序表”副本，以确定合适的更新源。更新代理在“更新代理顺序表”中的顺序，最初由其在 Web 控制台上添加为“备用更新源”时的顺序确定。每个安全客户端都会表中的第一项开始查起，一次查看一项，直到确定其更新源。

5. 然后，安全客户端会从指定的更新代理下载更新的组件。如果由于某种原因，指定的更新代理不可用，则安全客户端将尝试从安全管理服务器下载更新的组件。



配置更新代理

过程

1. 导航至**更新** > **源**。
2. 单击**更新代理**选项卡。
3. 执行以下任务：

任务	步骤
指定安全客户端充当更新代理	a. 在**指定更新代理**部分中，单击**添加**。 此时打开一个新窗口。 b. 从列表框中，选择一个或多个客户端来充当更新代理。 c. 单击**保存**。 窗口随即关闭。 d. 返回到**指定更新代理**部分，如果您希望更新代理始终从安全管理服务器而非其他更新代理下载更新的组件，请选择**更新代理始终仅从安全管理服务器直接更新**。

任务	步骤
将安全客户端配置为从更新代理进行更新	a. 在**备用更新源**部分中，选择**对安全客户端和更新代理启用备用更新源**。 **注意** 禁用此选项可阻止安全客户端从更新代理进行更新，从而有效地将其更新源切换回安全管理服务器。 b. 单击**添加**。 此时打开一个新窗口。 c. 键入将从更新代理进行更新的安全客户端的 IP 地址。 • 键入 IPv4 地址范围。 要指定单个安全客户端，请在**从**和**到**文本框中都输入安全客户端的 IP 地址。 • 对于 IPv6，键入 IP 前缀和长度。 d. 从下拉列表中选择一个更新代理。 如果没有可用的下拉列表，则表示尚未配置任何更新代理。 e. 单击**保存**。 窗口随即关闭。 f. 根据需要定义多个 IP 范围。如果定义了多个 IP 范围，则可以使用**重新排序**选项，设置 IP 范围的优先级。当安全管理服务器通知安全客户端有新的更新可用时，这些客户端会扫描“IP 范围”列表，以确定正确的更新源。安全客户端会扫描列表中的第一项，并继续向下扫描列表，直到确定正确的更新源。 **提示** 针对相同 IP 范围定义多个更新代理，以作为故障转移措施。这意味着，如果安全客户端无法从更新代理进行更新，则会尝试其他更新代理。要执行此操作，请至少创建两 (2) 个具有相同 IP 范围的条目，并对每一条目指定不同的更新代理。

任务	步骤
移除更新代理	要移除更新代理并取消指定已为其指定的所有安全客户端，请转到**指定更新代理**部分，选择与更新代理的计算机名称对应的复选框，然后单击**移除**。 此操作不会移除**备用更新源**部分中安全客户端的 IP 地址范围，而只会导致“孤立的”安全客户端将其更新源切换回安全管理服务器。如果您有其他更新代理，可以将其指定给孤立的安全客户端。
从更新代理取消指定安全客户端	如果您不再希望属于某 IP 地址范围的安全客户端从更新代理进行更新，请转到**备用更新源**部分，选择与安全客户端的 IP 地址范围对应的复选框，然后单击**移除**。

4. 单击**保存**。

第 9 章

管理通知

本章介绍如何使用不同的通知选项。

通知

一旦网络中出现异常事件，管理员便会接收到通知。安全无忧软件 可以通过电子邮件、SNMP 或 Windows 事件日志发送通知。

缺省情况下，**通知**窗口中列出的所有事件都被选中，并触发安全管理服务器向系统管理员发送通知。

威胁事件

- **爆发防御**：TrendLabs 发出一个警报，或检测到高危险漏洞。
- **防病毒**：客户机或 Microsoft Exchange Server（仅限邮件与网络安全版）上检测到的病毒/恶意软件数超过某个数值，针对病毒/恶意软件采取的处理措施不成功，客户机或 Microsoft Exchange Server 上的“实时扫描”已禁用。
- **防间谍软件**：在客户机上检测到间谍软件/灰色软件，包括需要重新启动受感染的客户机才能彻底移除该间谍软件/灰色软件威胁的间谍软件/灰色软件。您可以配置间谍软件/灰色软件通知阈值，即在指定时间段（缺省为一小时）内检测到的间谍软件/灰色软件事件数。
- **反垃圾邮件**（仅限邮件与网络安全版）：垃圾邮件数超过总邮件数的某个百分比。
- **Web 信誉**：一定时间段内的 URL 违例数超过了配置的数量。
- **URL 过滤**：一定时间段内的 URL 违例数超过了配置的数量。
- **行为监控**：一定时间段内的策略违例数超过了配置的数量。
- **设备控制**：设备控制违例的数量超过某个数量。
- **网络病毒**：检测到的网络病毒数超过某个数量。

系统事件

- **云安全扫描**：配置云安全扫描的客户机无法连接到云安全服务器，或此服务器不可用。
- **组件更新**：上次组件更新已超过一定的天数或更新的组件未及时地部署到客户端上。

- **系统异常事件**：运行 Windows Server 操作系统的任意客户机上的剩余磁盘空间少于配置的数量，磁盘空间严重不足。

使用授权事件

- **使用授权**：产品使用授权即将过期或已经过期，使用授权的安装数使用率超过 100%，或使用授权的安装数使用率超过 120%。

配置通知事件

配置通知分两个步骤。首先选择需要通知的事件，然后配置投递方法。

安全无忧软件提供了三种投递方法：

- 电子邮件通知
- SNMP 通知
- Windows 事件日志

过程

1. 导航至**首选项** > **通知**。
2. 从**事件**选项卡中，根据需要更新以下选项：
   - **电子邮件**：选中此复选框以接收该事件的通知。
   - **警报阈值**：配置事件的阈值和/或时间段。
   - **事件名称**：单击事件名称，以修改该事件的通知内容。您可以向内容中添加令牌变量。有关详细信息，请参阅令牌变量 第 9-4 页。
3. 单击**设置**选项卡，然后根据需要更新以下选项：
   - **电子邮件通知**：设置发件人和收件人的电子邮件地址。对于收件人，多个电子邮件地址可用半角分号 (;) 隔开。
   - **SNMP 通知收件人**：SNMP 是网络主机交换网络管理所用信息时所使用的协议。要查看 SNMP 陷阱中的数据，请使用管理信息库浏览器。

- **启用 SNMP 通知**
- **IP 地址**：SNMP 陷阱的 IP 地址。
- **团体**：SNMP 团体字符串。

- **日志记录**：使用 Windows 事件日志的通知
- **写入 Windows 事件日志**

4. 单击**保存**。

令牌变量

使用令牌变量可定制事件通知的主题行与消息正文。

要防止将来自具有外部域地址的电子邮件标记为垃圾邮件，请将外部电子邮件地址添加到反垃圾邮件的“允许的发件人”列表中。

下列令牌表示在安全客户端和 Microsoft Exchange Server 上检测到的威胁事件。

变量	描述
{$CSM_SERVERNAME}	管理客户端的安全管理服务器的名称
%CV	事件数
%CU	时间单位（分钟、小时）
%CT	%CU 数
%CP	垃圾邮件占总电子邮件数的百分比

以下是示例通知：

在 %CT %CU 中，趋势科技在计算机上检测到 %CV 个病毒事件。病毒事件太多或者太频繁可能表示即将发生病毒爆发。

请查看安全管理服务器上的“实时状态”窗口，以获得进一步的指导信息。

第 10 章

使用爆发防御

本章说明安全无忧软件的爆发防御策略、如何配置爆发防御，以及如何用爆发防御来保护网络与客户机。

爆发防御策略

“爆发防御”是 安全无忧软件 解决方案的关键组件，可在公司内威胁爆发期间保护您的企业。

配置爆发防御

过程

1. 转到**爆发防御**。
2. 在**爆发防御实施中设备的状态**部分单击**配置爆发防御**。
3. 要启动爆发防御，请选择**启用黄色警报爆发防御**。
4. **爆发防御启动时通知客户端用户**选项将会自动选择。如果您不希望向用户发送爆发防御通知，请清除该复选框。
5. 缺省情况下，**禁用爆发防御**设置为 2 天。该时间最大可设置为 30 天。
6. 根据需要进行以下更新：

选项	说明
限制/拒绝访问共享文件夹	选择该选项以限制或拒绝访问共享网络文件夹，作为爆发防御策略的一部分。选择以下项之一： • **只读访问权限** • **拒绝完全访问**
封闭端口	选择该选项以阻止端口，作为爆发防御策略的一部分。选择以下项之一： • **所有端口** • **指定的端口** 如果选择**指定的端口**，请单击**添加**并从以下选项中选择一个： • **常用端口**：从列表中选择端口

选项	说明
	• **特洛伊木马程序常用的端口**：当前已知不小于 40 个端口号被特洛伊木马程序使用 • **介于 1 和 65535 之间的端口号或端口范围**：定义端口或端口范围 • **Ping 协议 (ICMP)**
拒绝对文件和文件夹的写访问	选择该选项以拒绝对特定文件和文件夹的写入访问。从以下选项中选择： • **为特定目录保护的文件**：键入目录路径，然后指定拒绝对所有文件的写入访问还是仅拒绝对特定文件类型的写入访问 • **为所有目录保护的文件**：键入要保护的特定文件的名称（包括扩展名）
拒绝访问所有可执行压缩文件	选择该选项以拒绝对可执行压缩文件（加壳软件）的访问。指定是否允许对支持的可执行加壳软件程序创建的信任文件的访问。

7. 单击**保存**。

爆发防御当前状态

导航至**实时状态** > **爆发防御**以查看爆发防御状态。

针对黄色警报的爆发防御

该页面部分显示爆发防御黄色警报的相关信息：

- **开始时间**：管理员激活黄色警报的时间。
- **已激活的爆发防御**：已激活爆发防御的计算机数量。单击已设置超链接的编号以访问爆发防御页面。
- **已停用的爆发防御**：已停用爆发防御的计算机数量。单击已设置超链接的编号以访问爆发防御页面。

需要采取处理措施

该页面部分显示易受攻击的计算机和需要清理的计算机的相关信息：

- **易受攻击的计算机**：存在漏洞的计算机数量。
- **要清理的计算机**：等待清理的计算机数量。

漏洞检查

“漏洞检查”为系统管理员或其他网络安全人员提供检查其网络上安全风险的能力。通过“漏洞检查”所生成的信息，可以清楚地指导用户解决已知的漏洞并加固其网络。

使用“漏洞检查”可以：

- 扫描网络上的计算机有无漏洞。
- 按照标准命名约定来确定漏洞。通过单击漏洞名称，可找出有关漏洞的更多信息及解决漏洞的方法。
- 按计算机和 IP 地址显示漏洞。结果包括漏洞对计算机与整个网络所构成的风险等级。
- 按照单台计算机来报告漏洞，并描述这些计算机对整个网络所构成的安全风险。
- 配置扫描网络上任意或所有计算机的任务。扫描可以搜索单个漏洞或所有已知漏洞的列表。
- 运行手动评估任务或设置按时间表运行的任务。
- 对于那些对网络安全表现出不可接受风险等级的计算机请求阻止。
- 创建按照单台计算机来确定漏洞的报表，并描述整个网络所有计算机上存在的安全风险。报表按照标准命名约定来确定漏洞，管理员可进一步研究解决漏洞并加固网络。
- 查看评估历史数据并比较各种报表，可更好地理解漏洞并更改影响网络安全的风险因素。

配置漏洞评估

过程

1. 转到**爆发防御**。
2. 在**易受攻击的计算机**部分单击**配置预设评估**。
3. 要启动预设漏洞评估，请选择**启用预设漏洞阻止**。
4. 在**预设**部分选择漏洞评估的频率：
   - **每天一次**
   - **每周一次**
   - **每月一次**
   - **开始时间**
5. 在**目标**部分，选择要对其评估漏洞的组：
   - **所有组**：安全组树中的所有组
   - **指定的组**：安全组树中的服务器或台式机组
6. 单击**保存**。

运行按需漏洞评估

过程

1. 转到**爆发防御**。
2. 在**易受攻击的计算机**部分单击**立即扫描漏洞**。
3. 单击**确定**运行漏洞扫描。

   此时会显示**漏洞扫描通知进度**对话框。扫描完成后会显示**漏洞扫描通知结果**对话框。

4. 在**漏洞扫描通知结果**对话框中查看扫描结果，然后单击**关闭**。

损害清除

安全客户端使用损害清除服务，来保护客户机免遭特洛伊木马程序（或特洛伊木马）的侵扰。为解决特洛伊木马及其他恶意软件带来的威胁和问题，损害清除服务执行以下操作：

- 检测并删除活动的特洛伊木马与其他恶意软件应用程序
- 摧毁特洛伊木马与其他恶意软件应用程序所创建的进程
- 修复被特洛伊木马与其他恶意软件修改过的系统文件
- 删除特洛伊木马与其他恶意软件所创建的文件和应用程序

为完成这些任务，损害清除服务使用以下组件：

- **损害清除引擎**：损害清除服务执行扫描和移除特洛伊木马及其进程、蠕虫病毒和间谍软件所用的引擎。
- **病毒清除特征码**：供损害清除引擎使用。该模板可帮助识别特洛伊木马文件及其进程、蠕虫病毒以及间谍软件，以便损害清除引擎可以清除它们。

运行按需清理

过程

1. 转到**爆发防御**。
2. 在**要清理的计算机**部分单击**立即清理**。

   如果安全客户端处于脱机状态或者遇到网络中断之类的意外情形，则可能导致清理不成功。

3. 单击**确定**开始清理。

此时会显示**清理通知进度**对话框。清理完成后会显示**清理通知结果**对话框。

4. 在**清理通知结果**对话框中查看清理结果，然后单击**关闭**。

第 11 章

管理全局设置

本章讨论客户端的全局设置和安全管理服务器的系统设置。

全局设置

从 Web 控制台，您可以为安全管理服务器和安全客户端配置全局设置。

代理

如果网络使用客户端服务器连接到 Internet，请为以下服务指定客户端服务器设置：

- 组件更新和使用授权通知
- Web 信誉、行为监控和云安全扫描

有关详细信息，请参阅配置 Internet 代理服务器设置 第 11-2 页。

SMTP

“SMTP 服务器”设置适用于安全无忧软件生成的所有通知与报表。

有关详细信息，请参阅配置 SMTP 服务器设置 第 11-4 页。

安全客户端

安全客户端选项属于安全无忧软件全局设置。

有关详细信息，请参阅配置安全客户端设置 第 11-4 页。

系统

全局设置窗口中的“系统”部分包含自动移除非活动客户端、检查客户端的连接和维护隔离文件夹的选项。

有关详细信息，请参阅配置系统设置 第 11-9 页。

配置 Internet 代理服务器设置

如果安全管理服务器和安全客户端使用代理服务器连接到 Internet，请指定代理服务器设置以便使用以下功能和趋势科技服务：

- **安全管理服务器**：组件更新和使用授权维护

- **安全客户端**：Web 信誉、URL 过滤、行为监控、智能反馈和云安全扫描
- **邮件安全客户端**（仅限邮件与网络安全版）：Web 信誉和反垃圾邮件

过程

1. 导航至**首选项** > **全局设置**。
2. 从**代理服务器**选项卡中，根据需要更新以下选项：
   - 安全管理服务器代理服务器

     注意
     邮件安全客户端也使用安全管理服务器代理服务器设置。

     - 将代理服务器用于更新和使用授权通知
     - 使用 SOCKS 4/5 代理服务器协议
     - 地址：IPv4/IPv6 地址或主机名称
     - 端口
     - 代理服务器认证
       - 用户名
       - 密码
   - 安全客户端代理服务器
     - 使用为更新代理指定的凭证

       注意
       安全客户端使用 Internet Explorer 代理服务器和端口来连接到 Internet。只有当客户机上的 Internet Explorer 与安全管理服务器共享相同的认证凭证时，才选择此选项。

     - 用户名

- 密码

3. 单击**保存**。

配置 SMTP 服务器设置

“SMTP 服务器”设置适用于安全无忧软件生成的所有通知与报表。

过程

1. 导航至**首选项** > **全局设置**。
2. 单击 **SMTP** 选项卡，然后根据需要更新以下选项：
   - **SMTP 服务器**：SMTP 服务器的 IPv4 地址或名称。
   - **端口**
   - **启用 SMTP 服务器认证**
     - 用户名
     - 密码
3. 要验证设置是否正确，请单击**发送测试电子邮件**。如果发送失败，请修改设置或检查 SMTP 服务器的状态。
4. 单击**保存**。

配置安全客户端设置

安全客户端选项属于安全无忧软件全局设置。单独组的设置优先于这些设置。如果您没有对组配置特定选项，则使用“安全客户端”选项。例如，如果没有为特定组允许任何 URL，则此窗口上的所有允许的 URL 将适用于该组。

过程

1. 导航至**首选项** > **全局设置**。
2. 单击**安全客户端**选项卡，然后根据需要更新以下选项：

设置	描述

位置感知	通过“位置感知”功能，管理员可根据客户端连接网络的方式控制安全设置。
	“位置感知”控制“在办公室/不在办公室”连接设置。
	安全客户端可根据 Web 控制台上配置的网关信息，自动识别客户机的位置，并控制网站用户的访问权限。所施加的限制随用户位置不同而不同：
	• **启用位置感知**：这些设置将影响防火墙、Web 信誉和预设更新频率的“在办公室/不在办公室”连接设置。
	• **网关信息**：当远程连接到网络（使用 VPN）并且启用“位置感知”时，此列表中的客户端和连接将使用“内部连接”设置。
	  • 网关 IP 地址
	  • MAC 地址：添加 MAC 地址只允许连接已配置的设备以增强安全性。
	单击相应的回收站图标以删除项。

支持部门通知	“支持部门通知”在安全客户端上给出了通知，告知用户联系相应的服务人员以获取帮助。根据需要进行以下更新： • **支持部门标记** • **支持部门电子邮件地址** • **其他信息**：在用户鼠标放在标记上时弹出

设置	描述
通用扫描设置	• **禁用云安全扫描服务**：将所有安全客户端切换到传统扫描模式。云安全扫描只有在此处重新启用后才可用。要切换一个或多个安全客户端组，请导航至**安全设置** > **{组}** > **配置** > **扫描方法**。 **注意** 有关在不同扫描方法之间切换安全客户端的准则，请参阅配置扫描方法 第 5-4 页。 • **对文件操作启用延迟扫描**：启用该设置会暂时提高系统性能。 **警告!** 启用延迟扫描可能造成安全风险。 • **排除阴影复制部分**：阴影复制或卷快照服务对特定卷上的文件或文件夹进行手动或自动副本备份或快照。 • **排除安全管理服务器数据库文件夹**：使安装在安全管理服务器上的客户端仅在实时扫描期间免于扫描其自身的数据库。 缺省情况下，WFBS 并不扫描其自身的数据库。趋势科技建议保留这种选择以防扫描期间可能出现的数据库损坏事件。 • **在 Microsoft Exchange 服务器上安装时排除 Microsoft Exchange 服务器文件夹**：防止安装在 Microsoft Exchange Server 上的客户端扫描 Microsoft Exchange 文件夹。 • **排除 Microsoft 域控制文件夹**：防止安装在域控制器上的客户端扫描域控制器文件夹。这些文件夹存储用户信息、用户名称、密码以及其他重要信息。

设置	描述
病毒扫描设置	• **配置大型压缩文件的扫描设置**：指定客户端应扫描的压缩文件解压后的最大大小和其中的文件数量。 • **清理压缩文件**：客户端将尝试清除压缩文件中的受感染文件。 • **最多扫描 {} 个 OLE 层**：客户端将扫描指定数量的对象链接和嵌入 (OLE) 层。OLE 允许用户使用一个应用程序创建对象，然后将这些对象链接或嵌入到另一个应用程序中。例如，嵌入在 .doc 文件中的 .xls 文件。 • **将“手动扫描”添加到客户机的 Windows 快捷菜单中**：将**使用安全客户端进行扫描**的链接添加到上下文相关菜单。这样，用户可以右键单击桌面上或 Windows 资源管理器中的文件或文件夹，并手动扫描文件或文件夹。
间谍软件/灰色软件扫描设置	• **针对 cookie 进行扫描**：安全客户端针对 cookie 进行扫描。 • **将 cookie 检测添加到间谍软件日志中**:将每个检测到的间谍软件 cookie 添加到间谍软件日志。
防火墙设置	选择**禁用防火墙并卸载驱动程序**复选框，以卸载 WFBS 客户机防火墙并移除与防火墙关联的驱动程序。 **注意** 如果禁用防火墙，则重新启用防火墙之前相关设置将不可用。

设置	描述
Web 信誉和 URL 过滤	• **允许列表**：从 Web 信誉和 URL 过滤验证中排除的网站（及其子域）。 **注意** 允许列表优先于阻止列表。当 URL 与允许列表中的条目匹配时，即使该 URL 位于阻止列表中，客户端也始终允许访问它。 针对特定组启用允许或阻止列表，覆盖该组的“全局允许或阻止设置”。 • **阻止列表**：URL 过滤过程中总是阻止的 Web 站点（及其子域）。 • **进程例外列表**：从 Web 信誉和 URL 过滤验证中排除的进程。键入您的组织认为可信的关键进程。 **提示** 当您更新进程例外列表并且服务器向客户端部署更新列表时，客户端计算机上的所有活动 HTTP 连接（通过端口 80、81 或 8080）都将断开连接几秒钟。请考虑在非高峰时间更新进程例外列表。 • **IP 例外列表**：从 Web 信誉和 URL 过滤验证中排除的 IP 地址（例如 192.168.0.1）。键入您的组织认为可信的重要 IP 地址。 • **将 Web 信誉和 URL 过滤日志发送至安全管理服务器**
警报设置	**如果超过 {} 天未更新病毒码文件，在 Windows 任务栏上将显示警报图标**：当特征码文件超过特定天数未更新时，在客户端上显示警报图标。
安全客户端卸载密码	• **允许客户端用户在不提供密码的情况下卸载安全客户端。** • **客户端用户必须输入密码才能卸载安全客户端。**

设置	描述
安全客户端程序退出和解锁密码	• **允许客户端用户在不提供密码的情况下在其计算机上退出并解锁安全客户端。** • **客户端用户必须输入密码才能退出并解锁安全客户端。** **注意** 解锁安全客户端后，用户可以覆盖在**安全设置** > **{组}** > **配置** > **客户机权限**下配置的所有设置。
首选 IP 地址	此设置仅在双栈安全管理服务器上可用，且仅由双栈客户端应用。 安装或升级客户端之后，客户端会使用 IP 地址向安全管理服务器注册。 从下列选项中选择： • **先使用 IPv4，再使用 IPv6**：客户端先使用其 IPv4 地址。如果客户端无法使用其 IPv4 地址进行注册，则会使用其 IPv6 地址。如果使用这两个 IP 地址进行注册都失败，则客户端会使用此选项的 IP 地址优先级进行重试。 • **先使用 IPv6，再使用 IPv4**：客户端先使用其 IPv6 地址。如果客户端无法使用其 IPv6 地址进行注册，则会使用其 IPv4 地址。如果使用这两个 IP 地址进行注册都失败，则客户端会使用此选项的 IP 地址优先级进行重试。

3. 单击**保存**。

配置系统设置

全局设置窗口中的**系统**部分包含自动移除非活动客户端、检查客户端的连接和维护隔离文件夹的选项。

过程

1. 导航至**首选项** > **全局设置**。

2. 单击**系统**选项卡，然后根据需要更新以下选项：

设置	描述
非活动安全客户端删除	当使用客户端上的安全客户端卸载程序从客户端删除安全客户端时，该程序会自动通知安全管理服务器。安全管理服务器收到此通知后，会在“安全组树”中删除客户端图标以表明该客户端不再存在。 但是，如果使用其他方法移除安全客户端（例如重新格式化计算机的硬盘驱动器或手动删除客户机文件），则安全管理服务器将不会觉察到此移除情况，而是会将安全客户端显示为非活动状态。如果用户退出或禁用客户端很长时间，安全管理服务器也会将该安全客户端显示为非活动状态。 为使安全组树仅显示活动客户端，可以对安全管理服务器进行配置，使其从“安全组树”中自动删除非活动安全客户端。 • **启用非活动安全客户端的自动移除**：可自动移除与安全管理服务器失去联系达指定天数的客户机。 • **如果持续 {} 天处于非活动状态，则自动移除安全客户端**：从 Web 控制台移除某客户机前，允许该客户机保持非活动状态的天数。

设置	描述

客户端连接验证	WFBS 在安全组树中使用图标表示客户机连接状态。但是，有些条件可能会使安全组树无法显示正确的客户端连接状态。例如，如果客户机的网线意外拔出，则客户端将无法通知趋势科技安全管理服务器其现在处于脱机状态。此客户端在安全组树中将仍然显示为联机状态。
	
	可以从 Web 控制台中手动或根据时间表验证客户端-服务器连接。
	
	注意
	“连接验证”不允许选择特定的组或客户端。它会验证注册到安全管理服务器的所有客户端的连接。
	
	• **启用预设验证**：启用对客户端-服务器连接的预设验证。
	  • **每小时一次**
	  • **每天一次**
	  • **每周一次，每**
	  • **开始时间**：验证的开始时间。
	• **立即验证**：立即测试连接。

设置	描述
隔离维护	缺省情况下，安全客户端将隔离的受感染文件发送到安全管理服务器中的以下目录： <安全管理服务器安装文件夹>\PCCSRV\Virus 如果您需要更改目录（例如，若目录上的磁盘空间不足），请在**隔离目录**文本框中键入绝对路径，例如 D:\Quarantined Files。如果更改了目录，还要确保在**安全设置** > **{组}** > **配置** > **隔离**中应用相同更改，否则客户端会继续将文件发送到 <安全管理服务器安装文件夹>\PCCSRV\Virus。 此外，还要配置下列维护设置： • **隔离文件夹容量**：隔离文件夹大小 (MB)。 • **最大单个文件大小**：存储在隔离文件夹中的最大单个文件大小 (MB)。 • **删除所有被隔离文件**：删除隔离文件夹中的所有文件。如果文件夹已满并且要上传新文件，将无法存储新文件。 如果不希望客户端将隔离的文件发送到安全管理服务器，请在**安全设置** > **配置** > **隔离**中配置新目录，并忽略所有维护设置。请参阅隔离目录 第 5-28 页以了解指导信息。
安全客户端安装	**安全客户端安装目录**：在安装期间，系统会提示您键入安全客户端安装目录（安装程序安装每个安全客户端的位置）。 如果需要，可通过键入绝对路径来更改目录。只会将以后的客户端安装到此目录；现有客户端将保持其当前目录。 使用以下变量之一设置安装路径： • $BOOTDISK:引导磁盘的驱动器盘符 • $WINDIR:安装 Windows 的文件夹 • $ProgramFiles:程序文件夹

3. 单击**保存**。

第 12 章

使用日志和报表

本章描述了如何使用日志与报表来监控系统并分析防护情况。

日志

安全无忧软件保存了有关病毒/恶意软件和间谍软件/灰色软件事件、活动及更新的完整日志。使用这些日志可以评估组织的防护策略，确定易被病毒感染的客户端并验证更新是否部署成功。

注意

使用 Microsoft Excel 等电子表格应用程序可查看 CSV 格式的日志文件。

WFBS 维护以下类别的日志：

- Web 控制台事件日志
- 安全客户端日志
- Microsoft Exchange Server 日志（仅限邮件与网络安全版）

表 12-1. 日志类型与内容

类型（生成日志条目的实体）	内容（从中获取内容的日志类型）
管理控制台事件	• 手动扫描（从 Web 控制台启动） • 更新（安全管理服务器更新） • 爆发防御事件 • 控制台事件

类型（生成日志条目的实体）	内容（从中获取内容的日志类型）

安全客户端	• 病毒日志
	  • 手动扫描
	  • 实时扫描
	  • 预设扫描
	  • 清除
	• 间谍软件/灰色软件日志
	  • 手动扫描
	  • 实时扫描
	  • 预设扫描
	• Web 信誉日志
	• URL 过滤日志
	• 行为监控日志
	• 更新日志
	• 网络病毒日志
	• 爆发防御日志
	• 事件日志
	• 设备控制日志
	• Hot Fix 部署日志

类型（生成日志条目的实体）	内容（从中获取内容的日志类型）
Exchange Server（仅限邮件与网络安全版）	• 病毒日志 • 阻止附件日志 • 内容过滤 / 数据丢失预防日志 • 更新日志 • 备份日志 • 归档日志 • 爆发防御日志 • 扫描事件日志 • 非可扫描邮件部分日志 • Web 信誉日志 • 移动事件日志

使用日志查询

执行日志查询可从日志数据库收集信息。可以使用**日志查询**窗口来设置和运行查询。可以将结果导出为 CSV 文件或打印。

邮件安全客户端（仅限邮件与网络安全版）每 5 分钟向安全管理服务器发送一次日志（不论日志生成的时间）。

过程

1. 导航至**报表** > **日志查询**。
2. 根据需要更新以下选项：
   - **时间范围**
     - **预配置范围**

- **指定范围**：将查询限制到特定日期。

- **类型**：要查看每个日志类型的内容，请参阅日志 第 12-2 页。
  - **管理控制台事件**
  - **安全客户端**
  - **Exchange Server**（仅限邮件与网络安全版）
- **内容**：可用选项取决于日志**类型**。

3. 单击**显示日志**。
4. 要将日志保存为逗号分隔值 (CSV) 的数据文件，请单击**导出**。使用电子表格应用程序可以查看 CSV 文件。

报表

可以手动生成一次性报表，也可以设置安全管理服务器使之生成预设报表。

可以打印报表，也可以将报表通过电子邮件发送给管理员或其他个人。

报表中提供的数据受生成报表时安全管理服务器上提供的日志数量的影响。在添加新日志及删除现有日志时，日志数量会发生变化。在**报表** > **维护**中，您可以手动删除日志，也可以设置日志删除时间表。

使用一次性报表

过程

1. 导航到**报表** > **一次性报表**。
2. 执行以下任务：

任务	步骤

生成报表	a. 单击**添加**。
	将显示一个新窗口。
	b. 配置以下信息：
	• **报表名称**
	• **时间范围**：将报表限制到特定日期。
	• **内容**：要选择所有威胁，请选择**全选**复选框。要选择单独的威胁，请单击相应复选框。单击加号 (+) 展开所选项。
	• **将报表发送至**
	  • **收件人**：键入收件人的电子邮件地址，用半角分号 (;) 隔开。
	  • **格式**：选择 PDF 或 HTML 报表的链接。如果选择 PDF，该 PDF 将附在电子邮件中。
	c. 单击**添加**。

查看报表	在“报表名称”列下，单击报表链接。第一个链接会打开 PDF 报表，而第二个链接则会打开 HTML 报表。 报表中提供的数据受生成报表时安全管理服务器上提供的日志数量的影响。在添加新日志及删除现有日志时，日志数量会发生变化。在**报表** > **维护**中，您可以手动删除日志，也可以设置日志删除时间表。 有关报表内容的详细信息，请参阅了解报表的含义 第 12-9 页。
删除报表	a. 选择包含报表链接的行。 b. 单击**删除**。 **注意** 要自动删除报表，请导航到**报表** > **维护** > **报表**选项卡，然后设置 WFBS 保留的最大一次性报表数。缺省值为 10 个一次性报表。如果超出最大数，安全管理服务器会从保留时间最长的报表开始，依次删除报表。

使用预设报表

过程

1. 导航到**报表** > **预设报表**。
2. 执行以下任务：

任务	步骤

创建预设报表模板	a. 单击**添加**。
	将显示一个新窗口。
	b. 配置以下信息：
	• **报表模板名称**
	• **时间表**：每天一次、每周一次或每月一次，以及生成报表的时间
	对于每月报表，如果您选择 31、30 或 29 日，而该月没有该日期，则 WFBS 在该月将不会生成报表。
	• **内容**：要选择所有威胁，请选择**全选**复选框。要选择单独的威胁，请单击相应复选框。单击加号 (+) 展开所选项。
	• **将报表发送至**
	  • **收件人**：键入收件人的电子邮件地址，用半角分号 (;) 隔开。
	  • **格式**：选择 PDF 或 HTML 报表的链接。如果选择 PDF，该 PDF 将附在电子邮件中。
	c. 单击**添加**。

任务	步骤
查看预设报表	a. 在包含模板（从中生成预设报表）的行上，单击**报表历史记录**。 此时打开一个新窗口。 b. 在“查看”列下，单击报表链接。第一个链接会打开 PDF 报表，而第二个链接则会打开 HTML 报表。 报表中提供的数据受生成报表时安全管理服务器上提供的日志数量的影响。在添加新日志及删除现有日志时，日志数量会发生变化。在**报表** > **维护**中，您可以手动删除日志，也可以设置日志删除时间表。 有关报表内容的详细信息，请参阅了解报表的含义 第 12-9 页。
模板维护任务	
编辑模板设置	单击模板，然后在出现的新窗口中编辑设置。 保存更改后生成的报表将使用新设置。
启用/禁用模板	单击“已启用”列下的图标。 如果您要暂时停止生成预设报表，可禁用模板，然后在您再次需要报表时将其启用。
删除模板	选择模板，然后单击**删除**。 删除模板不会删除从模板生成的预设报表，但是 Web 控制台将不再提供这些报表的链接。您可以直接从安全管理服务器计算机访问这些报表。如果您从计算机手动删除报表，或者，如果安全管理服务器根据**报表** > **维护** > **报表**选项卡中的预设报表自动删除设置自动删除报表，则仅会删除这些报表。 要自动删除模板，请导航到**报表** > **维护** > **报表**选项卡，然后设置 WFBS 保留的最大模板数。缺省值为 10 个模板。如果超出最大数，安全管理服务器会从保留时间最长的模板开始，依次删除模板。
报表维护任务	

任务	步骤
发送预设报表的链接	通过电子邮件发送预设报表（PDF 格式）的链接。收件人单击电子邮件中的链接可访问该 PDF 文件。请确保收件人能够连接到安全管理服务器计算机，否则该文件将无法显示。 **注意** 电子邮件中仅提供 PDF 文件的链接，而不会附加实际的 PDF 文件。 a. 在包含模板（从中生成预设报表）的行上，单击**报表历史记录**。 此时打开一个新窗口。 b. 选择报表，然后单击**发送**。 您的缺省电子邮件客户机将打开，其中带有包含报表链接的新电子邮件。
删除预设报表	a. 在包含模板（从中生成预设报表）的行上，单击**报表历史记录**。 此时打开一个新窗口。 b. 选择报表，然后单击**删除**。 **注意** 要自动删除报表，请导航到**报表** > **维护** > **报表**选项卡，然后设置 WFBS 保留的每个模板中最大预设报表数。缺省值为 10 个预设报表。如果超出最大数，安全管理服务器会从保留时间最长的报表开始，依次删除报表。

了解报表的含义

安全无忧软件报表包含以下信息。显示的信息可能会根据所选选项的不同而不同。

表 12-2. 报表的内容

报表项	描述
防病毒	**安全客户端病毒摘要** “病毒”报表显示有关扫描引擎检测到的病毒/恶意软件数量和类型以及针对这些病毒/恶意软件所采取的处理措施的详细信息。此报表还会列出前几个病毒/恶意软件的名称。单击病毒/恶意软件的名称可打开一个新的 Web 浏览器页面，并重定向到趋势科技病毒百科全书以了解该病毒/恶意软件的更多信息。
	前 5 个检出病毒的安全客户端 显示前 5 台报告检测到病毒/恶意软件的台式机或服务器。在同一客户端上观察到经常发生的病毒/恶意软件事件，可能预示着这台客户端具有较高的安全风险，需要进一步调查
爆发防御历史记录	**爆发防御历史记录** 显示最近的爆发和爆发的严重性，并确定引起爆发的病毒/恶意软件及其传播途径（通过电子邮件或文件）。
防间谍软件	**安全客户端间谍软件/灰色软件摘要** “间谍软件/灰色软件”报表显示有关客户端上检测到的间谍软件/灰色软件威胁的详细信息，包括 WFBS 对这些威胁进行的检测次数和对这些威胁采取的处理措施次数。报表包括一个饼图，其中显示了已执行的每个防间谍软件扫描处理措施百分比。
	前 5 个检出间谍软件/灰色软件的安全客户端 此报表还会显示检测到的前 5 个间谍软件/灰色软件威胁和检测到间谍软件/灰色软件最多的前 5 个安全客户端。要了解有关已检测到的间谍软件/灰色软件威胁的更多信息，请单击间谍软件/灰色软件名称。此时将打开新的 Web 浏览器页面，并显示趋势科技 Web 站点上这些间谍软件/灰色软件的相关信息。
反垃圾邮件摘要（仅限邮件与网络安全版）	**垃圾邮件摘要** “反垃圾邮件”报表显示有关在已扫描邮件总数中检测到的垃圾邮件数与网络钓鱼事件数的信息。还列出报告的误判情况。
Web 信誉	**前 10 台 Web 信誉策略违例的计算机**

报表项	描述
URL 类别	**前 5 项被违反的 URL 类别策略** 列出违反此策略的最常访问的 Web 站点类别。
	前 10 台 URL 类别策略违例的计算机
行为监控	**前 5 个行为监控策略违例的程序**
	前 10 台行为监控策略违例的计算机
设备控制	**前 10 台违反设备控制策略的计算机**
内容过滤摘要（仅限邮件与网络安全版）	**内容过滤摘要** “内容过滤”报表显示有关邮件安全客户端过滤的邮件总数的信息。
	前 10 项已违例的内容过滤规则 前 10 项违反内容过滤规则的事件的列表。使用这些反馈信息可微调过滤规则。
网络病毒	**检测到的前 10 种最多的网络病毒** 列出通用防火墙驱动程序最常检测到的 10 种网络病毒。 单击病毒的名称可打开一个新的 Web 浏览器页面，并重定向到趋势科技病毒百科全书以了解该病毒的更多信息。
	前 10 台被攻击的计算机 列出网络中报告病毒事件最频繁的计算机。

执行报表和日志维护任务

过程

1. 导航至**报表** > **维护**。
2. 执行以下任务：

任务	步骤
设置报表和模板的最大数量	您可以限制安全管理服务器上可用的一次性报表、预设报表（每个模板）和模板的数量。超出限制的数量时，安全管理服务器会从保留时间最长的报表/模板开始，依次删除多余的报表/模板。 a. 单击**报表**选项卡。 b. 键入要保留的一次性报表、预设报表和报表模板的最大数量。
配置日志自动删除	a. 单击**自动日志删除**选项卡。 b. 选择日志类型并指定日志的最长保留时间。早于此值的日志将被删除。
手动删除日志	a. 单击**手动日志删除**选项卡。 b. 针对每种日志类型，键入日志的最长保留时间。早于此值的日志将被删除。要删除所有日志，请键入 `0`。 c. 单击**删除**。

3. 单击**保存**。

第 13 章

执行管理任务

本章说明如何使用其他管理任务，例如查看产品使用授权、使用插件管理器，以及卸载安全管理服务器。

更改 Web 控制台密码

趋势科技建议对 Web 控制台使用不易破解的密码。密码应至少八个字符长，有一个或多个大写字母 (A-Z)、一个或多个小写字母 (a-z)、一个或多个数字 (0-9)，还有一个或多个特殊字符或标点符号 (!@#$%^&,.:;?) 才会不易破解。不易破解的密码绝对不能是用户的登录名，也不可以在密码中含有登录名。不能包含用户的姓氏或名字、生日，或易于识别用户的任何其他项。

过程

1. 导航至**首选项** > **密码**。
2. 根据需要更新以下选项：
   - **旧密码**
   - **新密码**
   - **确认密码**：请再次键入新密码以确认。
3. 单击**保存**。

使用插件管理器

只要安全管理服务器和安全客户端可用，插件管理器就会在 Web 控制台中显示它们的程序。然后，您可以从 Web 控制台安装并管理上述程序，包括将客户端插件程序部署到客户端。从**首选项** > **插件**下载并安装插件管理器。安装后，可以检查可用的插件程序。有关插件管理器和插件程序的更多信息，请参阅文档。

管理产品使用授权

从“产品使用授权”窗口中，可以续订、升级或查看产品使用授权详细信息。

“产品使用授权”窗口显示有关使用授权的详细信息。根据在安装过程中选择的选项，您可能拥有正式许可版或评估版。无论哪种情况，利用使用授权，您都可以得到维护协议。当维护协议过期时，您网络上的客户端所得到的防护将非常有限。使用“产品使用授权”窗口，可确定您的使用授权到期日期以确保在过期前续订使用授权。

注意

不同地区对各种趋势科技产品组件的使用授权也许不尽相同。在安装之后，您将看到注册码/激活码允许您使用的组件的摘要。请与供应商或经销商联系以验证您具有哪些组件的使用授权。

使用授权续订

您可以购买维护续保，续订或升级到完整许可版本的 WFBS。完整许可版本需要激活码。

续订产品使用授权有两种方法：

- 在 Web 控制台上，导航至“实时状态”窗口并按照窗口上的指导信息操作。这些指导信息在使用授权过期之前 60 天及过期后 30 天内显示。
- 请联系您的趋势科技销售代表或公司经销商来续订您的许可协议。

  经销商可以在安全管理服务器上的文件中留下其联系信息。在以下位置查看该文件：

  {**安全管理服务器安装文件夹**}\PCCSRV\Private\contact_info.ini

  注意

  {**安全管理服务器安装文件夹**}通常为 C:\Program Files\Trend Micro\Security Server。

  趋势科技代表将用“趋势科技产品注册”来更新您的注册信息。

  安全管理服务器会轮询“产品注册”服务器并从中直接接收新的到期日期。在续订使用授权时，不必手动输入新的激活码。

激活新使用授权

使用授权类型决定安全无忧软件的激活码。

表 **13-1.** 由使用授权类型确定的激活码

使用授权类型	激活码
完整许可版本的 WFBS-网络安全版	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
完整许可版本的 WFBS-邮件与网络安全版	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

注意

如果您有关于激活码的问题，请查询趋势科技支持网站，网址为：

http://esupport.trendmicro.com/solution/zh-cn/1093619.aspx

可通过输入新的激活码，使用“产品使用授权”窗口更改使用授权类型。

1. 导航至**首选项** > **产品使用授权**。
2. 单击**输入新的激活码**。
3. 在提供的空栏中键入新的激活码。
4. 单击**激活**。

参与智能反馈计划

有关智能反馈的详细信息，请参阅云安全智能反馈 第 1-18 页。

过程

1. 导航至**首选项** > **云安全智能防护网络**。
2. 单击**启用趋势科技智能反馈**。
3. 要发送有关客户端计算机的文件中的潜在安全威胁的信息，请选中**启用可疑程序文件的反馈**复选框。

注意

发送到智能反馈的文件不包含任何用户数据，并且提交只是为了进行威胁分析。

4. 要帮助趋势科技了解贵组织，请选择**行业**类型。
5. 单击**保存**。

更改客户端界面语言

缺省情况下，客户端界面上使用的语言将与客户机操作系统上配置的语言环境相对应。用户可以从客户端界面上更改语言。

保存和恢复程序设置

可以保存安全管理服务器数据库及重要配置文件的副本，以便还原安全管理服务器。在遇到问题并希望重新安装安全管理服务器或希望恢复为先前的配置时，可能希望这样做。

过程

1. 停止趋势科技安全管理服务器主服务。
2. 从文件夹中将下列文件和文件夹手动拷贝至备用位置：

警告!
不要对此任务使用备份工具或应用程序。

`C:\Program Files\Trend Micro\Security Server\PCCSRV`

- `ofcscan.ini`:包含全局设置。
- `ous.ini`:包含防病毒组件部署的更新源表。
- `Private` 文件夹：包含防火墙和更新源设置。
- `Web\TmOPP` 文件夹：包含爆发防御设置。
- `Pccnt\Common\OfcPfw.dat`:包含防火墙设置。
- `Download\OfcPfw.dat`:包含防火墙部署设置。
- `Log` 文件夹：包含系统事件和验证连接日志。
- `Virus` 文件夹：WFBS 隔离受感染的文件所在的文件夹。
- `HTTDB` 文件夹：包含 WFBS 数据库。

3. 卸载安全管理服务器。请参阅卸载安全管理服务器 第 13-7 页。
4. 执行全新安装。请参阅 WFBS《*安装和升级指南*》。
5. 在主安装程序完成后，请停止目标计算机上的趋势科技安全管理服务器主服务。
6. 从备份文件中更新病毒码版本：
   a. 从新服务器中获取当前病毒码版本。

   `\Trend Micro\Security Server\PCCSRV\Private \component.ini. [6101]`

```
ComponentName=Virus pattern

Version=xxxxxx 0 0
```

b. 更新备份文件中病毒码的版本：

```
\Private\component.ini
```

注意

如果更改安全管理服务器的安装路径，则必须更新备份文件 `ofcscan.ini` 和 `\private\ofcserver.ini` 中的路径信息

7. 使用创建的备份，覆盖 WFBS 数据库以及目标计算机上 PCCSRV 文件夹中的相关文件和文件夹。
8. 重新启动趋势科技安全管理服务器主服务。

卸载安全管理服务器

卸载安全管理服务器时也会卸载扫描服务器。

安全无忧软件可使用卸载程序从计算机中安全移除趋势科技安全管理服务器。移除安全管理服务器前请从所有客户机上移除客户端。

卸载趋势科技安全管理服务器并不会卸载客户端。管理员必须先卸载或移走其他安全管理服务器的所有客户端，然后再卸载趋势科技安全管理服务器。请参阅移除客户端 第 3-34 页。

过程

1. 在用于安装服务器的计算机上，单击**开始** > **控制面板** > **添加或删除程序**。
2. 单击**趋势科技安全管理服务器**，然后单击**更改/删除**。

   显示确认窗口。
3. 单击**下一步**。

主卸载程序（即服务器卸载程序）会提示您输入管理员密码。

4. 在文本框中键入管理员密码，然后单击**确定**。

   主卸载程序开始删除服务器文件。安全管理服务器卸载后会出现一条确认信息。

5. 单击**确定**关闭卸载程序。

第 14 章

使用管理工具

本章说明如何使用管理工具、客户机工具以及附加组件。

工具类型

安全无忧软件包含一组工具，可以帮助您轻松完成包括服务器配置和客户机管理在内的各种任务。

注意

无法从 Web 控制台启动管理工具和客户机工具。但是可从 Web 控制台下载附加组件。

有关如何使用这些工具的说明，请参阅下面的相关部分。

这些工具分为三类：

- **管理工具**
  - **登录脚本安装程序** (`SetupUsr.exe`)：自动化安全客户端安装。请参阅使用登录脚本安装进行安装 第 3-12 页。
  - **漏洞扫描程序** (`TMVS.exe`)：查找网络中无保护的计算机。请参阅使用漏洞扫描程序安装 第 3-19 页。
  - **远程管理器代理**：使经销商可以通过集中式 Web 控制台管理 WFBS。请参阅安装趋势科技远程管理器代理 第 14-3 页。
  - **趋势科技磁盘清理程序**：删除不必要的 WFBS 备份文件、日志文件和未用过的特征码文件。请参阅节省磁盘空间 第 14-5 页。
  - **扫描服务器数据库迁移程序**：将扫描服务器数据库安全移动到其他磁盘驱动器。请参阅移动扫描服务器数据库 第 14-8 页。
- **客户机工具**
  - **客户机打包程序** (`ClnPack.exe`)：创建含有安全客户端与组件的自解压文件。请参阅使用客户端打包程序安装 第 3-13 页。
  - **恢复加密的病毒和间谍软件** (`VSEncode.exe`)：打开 WFBS 加密的受感染文件。请参阅恢复加密文件 第 14-9 页。
  - **客户机迁移程序工具** (`IpXfer.exe`)：将客户端从一台安全管理服务器转移到另一台安全管理服务器。请参阅移动客户端 第 4-11 页。

- **重新生成安全客户端 ClientID** (`WFBS_WIN_All_ReGenID.exe`)：使用 ReGenID 实用程序重新生成安全客户端 ClientID（根据该客户端位于克隆计算机上还是虚拟机上）。请参阅使用 ReGenID 工具 第 14-12 页。
- **安全客户端卸载** (`SA_Uninstall.exe`)：自动删除客户端计算机中的所有安全客户端组件。请参阅使用 SA 卸载工具 第 3-37 页。

- **附加组件**：使管理员能够从受支持的 Windows 操作系统控制台查看实时的安全和系统信息。这是在“实时状态”窗口中可见的相同的高级别信息。请参阅管理 SBS 和 EBS 附加组件 第 14-13 页。

注意

先前版本的 WFBS 中有些工具在本版本中不可用。如果需要使用这些工具，请联系趋势科技技术支持。

安装趋势科技远程管理器代理

趋势科技远程管理器代理允许经销商使用趋势科技远程管理器 (TMRM) 来管理 WFBS。TMRM 代理（版本 3.5）安装在安全管理服务器 9.0 SP1 上。

如果您是经趋势科技认证的合作伙伴，就可以安装趋势科技远程管理器 (TMRM) 代理。如果在安全管理服务器安装完成后选择不安装 TMRM 代理，可以稍后进行安装。

安装要求：

- TMRM 代理 GUID

  要获得 GUID，请打开 TMRM 控制台并转到**客户（选项卡）** > **所有客户（在树中）** > **{客户}** > **WFBS/CSM** > **服务器/客户端详细信息（右侧窗格）** > **WFRM 客户端详细信息**

- 活动的 Internet 连接
- 50MB 的可用磁盘空间

过程

1. 转至安全管理服务器，并导航至以下安装文件夹：`PCCSRV\Admin\Utility\RmAgent`，然后启动应用程序 `TMRMAgentforWFBS.exe`。

   例如：`C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   注意

   如果从安全管理服务器安装窗口启动安装，则跳过此步骤。

2. 在趋势科技远程管理器代理安装向导中，阅读许可协议。如果同意条款，则选择**我接受许可协议中的条款**，然后单击**下一步**。

3. 单击**是**，确认您是经认证的合作伙伴。

4. 选择**我已有趋势科技远程管理器帐户，并且想安装客户端**。单击**下一步**。

5. 确定您的情况。

情况	步骤
新客户	a. 请选择**与新客户关联**。 b. 单击**下一步**。输入客户信息。 **注意** 如果此客户已存在于 TMRM 控制台上，而您使用上述选项与新客户关联，将会导致 TMRM 网络树中出现两个同名的重复客户。要避免此情况，请使用下列方法。
现有客户	a. 选择**此产品已存在于远程管理器中**。 **注意** WFBS 必须已添加至 TMRM 控制台中。有关指导信息，请参阅 TMRM 文档。 b. 键入 GUID。

6. 单击**下一步**。

7. 选择**区域**和**协议**，然后根据需要输入代理服务器信息。
8. 单击**下一步**。

   将打开“安装位置”窗口。
9. 要使用缺省位置，请单击**下一步**。
10. 单击**完成**。

    如果安装成功且设置正确，TMRM 代理应自动注册到趋势科技远程管理器服务器。此代理应在 TMRM 控制台上显示为联机。

节省磁盘空间

通过运行磁盘清理程序，节省安全管理服务器和安全客户端的磁盘空间。

在安全管理服务器上运行磁盘清理程序

开始之前

为节省磁盘空间，磁盘清理程序工具 (`TMDiskCleaner.exe`) 会识别并删除以下目录中未使用的备份、日志和特征码文件：

- {**安全客户端**}`\AU_Data\AU_Temp\*`
- {**安全客户端**}`\Reserve`
- {**安全管理服务器**}`\PCCSRV\TEMP\*`（**隐藏文件除外**）
- {**安全管理服务器**}`\PCCSRV\Web\Service\AU_Data\AU_Temp\*`
- {**安全管理服务器**}`\PCCSRV\wss\*.log`
- {**安全管理服务器**}`\PCCSRV\wss\AU_Data\AU_Temp\*`
- {**安全管理服务器**}`\PCCSRV\Backup\*`

- {安全管理服务器}\PCCSRV\Virus*（删除超过两周的隔离文件，NOTVIRUS 文件除外）
- {安全管理服务器}\PCCSRV\ssaptpn.xxx（仅保留最新特征码）
- {安全管理服务器}\PCCSRV\lpt$vpn.xxx（仅保留最新的三个特征码）
- {安全管理服务器}\PCCSRV\icrc$oth.xxx（仅保留最新的三个特征码）
- {安全管理服务器}\DBBackup*（仅保留最新的两个子文件夹）
- {邮件安全客户端}\AU_Data\AU_Temp*
- {邮件安全客户端}\Debug*
- {邮件安全客户端}\engine\vsapi\latest\pattern*

过程

1. 在安全管理服务器上，转到以下目录：

   {服务器安装文件夹}\PCCSRV\Admin\Utility\

2. 双击 **TMDiskCleaner.exe**。

   将显示趋势科技安全无忧软件磁盘清理程序。

   注意

   文件无法恢复。

3. 单击**删除文件**，以扫描并删除未使用的备份、日志和特征码文件。

使用命令行界面，在安全管理服务器上运行磁盘清理程序

过程

1. 在安全管理服务器上，打开命令提示符窗口。
2. 在命令提示符下，运行以下命令：

   `TMDiskCleaner.exe [/hide] [/log] [/allowundo]`

   - `/hide`:以后台进程方式运行此工具。
   - `/log`:将操作日志保存到位于当前文件夹中的 DiskClean.log。

     注意

     `/log` 仅在使用 `/hide` 时才可用。

   - `/allowundo`:将文件移到回收站，不永久删除文件。
3. 要经常运行磁盘清理程序工具，可使用 Windows 计划任务配置一项新任务。有关更多信息，请参阅 Windows 文档。

节省客户机的磁盘空间

过程

- 在带有安全客户端的台式机/服务器上：
  - 清除隔离文件
  - 清除日志文件
  - 运行 Windows 磁盘清理实用程序
- 在带有邮件安全客户端的 Microsoft Exchange Server 上：

- 清除隔离文件
- 清除日志文件
- 运行 Windows 磁盘清理实用程序
- 清除归档日志
- 清除备份文件
- 检查 Microsoft Exchange 数据库或事务日志的大小

移动扫描服务器数据库

如果安装扫描服务器的磁盘驱动器磁盘空间不足，请使用扫描服务器数据库迁移程序工具，将扫描服务器数据库安全移动到其他磁盘驱动器。

确保安全管理服务器计算机具有 1 个以上的磁盘驱动器，并且新磁盘驱动器具有至少 3GB 的可用磁盘空间。不允许使用映射的驱动器。请勿手动移动数据库或使用其他工具。

过程

1. 在安全管理服务器计算机上，导航至 <**安全管理服务器安装文件夹**>\PCCSRV\Admin\Utility。
2. 启动 ScanServerDBMover.exe。
3. 单击**更改**。
4. 单击**浏览**，然后浏览到其他磁盘驱动器上的目标目录。
5. 单击**确定**，然后在移动数据库后，单击**完成**。

恢复加密文件

为防止打开受感染的文件，在以下情况下，安全无忧软件 会对文件进行加密：

- 隔离文件之前
- 在清除文件之前备份文件时

WFBS 提供了一种工具，用于在需要从文件检索信息时解密和恢复该文件。WFBS 可以解密和恢复以下文件：

表 14-1. WFBS 可以解密和恢复的文件

文件	描述
客户机上的隔离文件	可以在以下目录中找到这些文件： • <安全客户端安装文件夹>\SUSPECT\Backup 或 <安全客户端安装文件夹>\quarantine，任一目录皆可。 • <邮件安全客户端安装文件夹>\storage\quarantine 这些文件还会上传到指定的隔离目录（通常是安全管理服务器上的目录）。
指定隔离目录中的隔离文件	缺省情况下，此目录位于安全管理服务器计算机（<安全管理服务器安装文件夹>\PCCSRV\Virus）。要更改此目录，请导航到**首选项** > **全局设置** > **系统**选项卡，然后转到“隔离维护”部分。
备份的加密文件	这些文件是客户端能够清除的受感染文件的备份。可以在以下文件夹中找到这些文件： • <安全客户端安装文件夹>\Backup • <邮件安全客户端安装文件夹>\storage\backup 要恢复这些文件，用户需要将它们移动到客户机上的隔离目录。

警告!

恢复受感染文件可能将病毒/恶意软件传播到其他文件和客户机。在恢复文件之前，隔离受感染的客户机，并将此客户机上的重要文件移动到备份位置。

解密和恢复安全客户端上的文件

过程

1. 打开命令提示符，并导航到 <**安全客户端安装文件夹**>。
2. 键入以下命令运行 `VSEncode.exe`：

   ```
   VSEncode.exe /u
   ```

   此参数将打开一个窗口，其中包含在 <**安全客户端安装文件夹**>\SUSPECT\Backup 下找到的文件的列表。

   管理员可以从间谍软件/灰色软件选项卡中恢复归类为间谍软件/灰色软件的文件。该窗口将显示文件列表，这些文件位于<**安全客户端安装文件夹**>\BackupAS。
3. 选择一个要恢复的文件，然后单击**恢复**。该工具一次只能恢复一个文件。
4. 在打开的窗口中，指定将文件恢复到的文件夹。
5. 单击**确定**。文件将恢复到指定的文件夹。

   注意

   在恢复文件后，客户端有可能立即再次扫描该文件，并将它视为被感染文件。为防止扫描该文件，请将它添加到扫描例外列表。请参阅安全客户端的扫描目标和处理措施 第 7-7 页。
6. 恢复完文件后，单击**关闭**。

解密和恢复安全客户端、定制隔离目录或邮件安全客户端中的文件

过程

1. 如果文件在安全管理服务器计算机中，请打开命令提示符，并导航到 <**服务器安装文件夹**>\PCCSRV\Admin\Utility\VSEncrypt。

如果文件位于装有邮件安全客户端的客户机或定制隔离目录中，请导航至 <服务器安装文件夹>\PCCSRV\Admin\Utility，并将 VSEncrypt 文件夹复制到该客户机或定制隔离目录。

2. 创建文本文件，然后键入要加密或解密的文件的完整路径。

   例如，要恢复 C:\My Documents\Reports 中的文件，请在文本文件中键入 C:\My Documents\Reports*.*。

   安全管理服务器计算机上的隔离文件可在 <服务器安装文件夹>\PCCSRV\Virus 下找到。

3. 用 INI 或 TXT 扩展名保存文本文件。例如，在 C: 驱动器上将它保存为 ForEncryption.ini。

4. 打开命令提示符并导航到 VSEncrypt 文件夹所在的目录。

5. 键入以下命令运行 VSEncode.exe：

   VSEncode.exe /d /i <INI 或 TXT 文件的位置>

   其中：

   <INI 或 TXT 文件的位置> 是所创建的 INI 或 TXT 文件的路径（例如 C:\ForEncryption.ini）。

6. 使用其他参数发出各种命令。

表 14-2. 恢复参数

参数	描述
无（没有参数）	加密文件
/d	解密文件
/debug	创建调试日志并将其保存到计算机。在客户机上，调试日志 VSEncrypt.log 是在 <客户端安装文件夹> 中创建的。
/o	覆盖加密或解密的文件（如果该文件已存在）
/f <文件名>	加密或解密单个文件
/nr	不恢复原始文件名

参数	描述
/v	显示有关该工具的信息
/u	启动该工具的用户界面
/r <目标文件夹>	将文件恢复到的文件夹
/s <原始加密文件名>	原始加密文件的文件名

例如，键入 VSEncode [/d] [/debug] 可以解密 Suspect 文件夹中的文件，并创建调试日志。解密或加密文件时，WFBS 将在同一文件夹中创建解密的或加密的文件。在解密或加密文件之前，请确保文件未被锁定。

恢复传输中性封装格式电子邮件

传输中性封装格式 (TNEF) 是 Microsoft Exchange/Outlook 所使用的邮件封装格式。该格式通常打包为名为 Winmail.dat 的电子邮件附件，Outlook Express 会自动隐藏该附件。请参阅 http://support.microsoft.com/kb/241538/zh-cn。

如果邮件安全客户端归档此类电子邮件，并且文件的扩展名被更改为 .EML，Outlook Express 将只显示电子邮件的正文。

使用 ReGenID 工具

每当安装安全客户端时，都需要一个全局唯一标识号 (GUID)，这样安全管理服务器就可以分别识别客户端。重复的 GUID 通常出现在克隆的客户机或虚拟机上。

如果两个或多个客户端报告相同的 GUID，则运行 ReGenID 工具为每台客户机生成唯一的 GUID。

过程

1. 在安全管理服务器上，转到以下目录：<服务器安装文件夹>\PCCSRV\Admin\Utility。

2. 在安装安全客户端的客户机上，将 `WFBS_WIN_All_ReGenID.exe` 复制到临时文件夹。

   示例：`C:\temp`

3. 双击 `WFBS_WIN_All_ReGenID.exe`。

   该工具会停止安全客户端并移除客户机 GUID。

4. 重新启动安全客户端。

   安全客户端将生成新的客户机 GUID。

管理 SBS 和 EBS 附加组件

安全无忧软件会提供附加组件，以便管理员能够从以下 Windows 操作系统的控制台查看实时的安全和系统状态信息：

- Windows Small Business Server (SBS) 2008
- Windows Essential Business Server (EBS) 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

手动安装 SBS 和 EBS 附加组件

当您在运行 Windows SBS 2008、EBS 2008、SBS 2011 Standard/Essentials 或 Server 2012/2012 R2 Essentials 的计算机上安装安全管理服务器时，会自动安装 SBS 或 EBS 附加组件。要在运行这些操作系统的其他计算机上使用该附加组件，您需要手动进行安装。

过程

1. 在 Web 控制台上，单击**首选项** > **管理工具**，然后单击**附加组件**选项卡。
2. 单击相应的**下载**链接，以获取安装程序。
3. 先进行复制，然后在目标计算机上启动安装程序。

使用 SBS 或 EBS 附加组件

过程

1. 打开 SBS 或 EBS 控制台。
2. 在**安全**选项卡下，单击**趋势科技安全无忧软件**即可查看状态信息。

附录 A

安全客户端图标

本附录说明客户机上显示的不同安全客户端图标。

检查安全客户端状态

下图显示了各项均为最新且工作正常的安全客户端控制台：

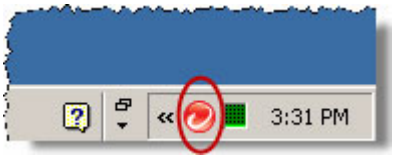
下表列出了安全客户端控制台主用户界面上的图标及其含义：

表 A-1. 安全客户端控制台主用户界面图标

图标	状态	解释和处理措施
	已启用保护：您正处于保护中，并且您的软件为最新版本	软件已为最新且运行正常。无需采取处理措施。
	重新启动计算机：请重新启动计算机，完成安全威胁的解决	安全客户端发现了无法立即解决的威胁。 请重新启动计算机，完成这些威胁的修复。
	防护存在风险：请联系您的管理员	实时扫描已禁用，或者由于其他原因导致防护存在风险。 启用实时扫描，如果仍无法解决问题，请联系支持部门。
	立即更新：在过去 (天数) 天内您没有收到更新。	病毒码超过 3 天。 立即更新安全客户端。
	云安全扫描不可用：请检查您的 Internet 连接	安全客户端无法访问云安全服务器已经超过 15 分钟。 请确保您已连接到网络，以使用最新的病毒码进行扫描。
	重新启动计算机：请重新启动计算机完成更新的安装	请重新启动计算机完成更新。
	更新程序：正在更新安全软件	正在进行更新。在更新完成之前不要断开网络连接。

查看 Windows 任务栏上的安全客户端图标

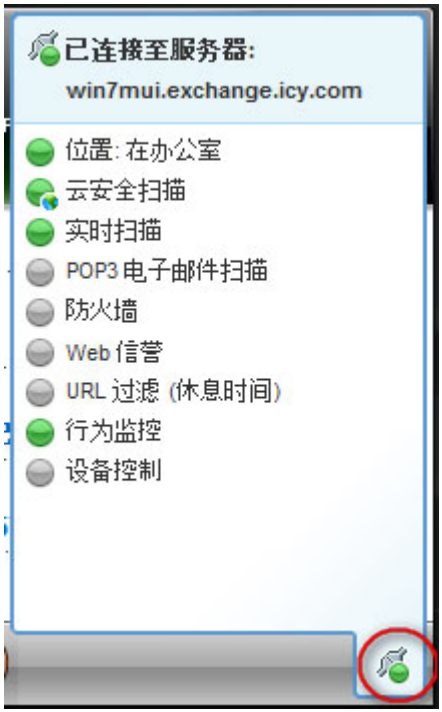
以下安全客户端图标会显示在客户端的 Windows 任务栏中：



图标	含义
	状态正常
	（动画）手动扫描或预设扫描正在运行。安全客户端正在使用传统扫描或云安全扫描。
	安全客户端正在进行更新。
	需要采取处理措施： • 实时扫描已禁用 • 需要重新启动以完全清理恶意软件 • 由于进行了引擎更新，需要重新启动 • 需要更新 **注意** 打开安全客户端主控台查看需要执行何种处理措施。

访问控制台悬停提示

将鼠标指针悬停在安全客户端控制台右下方的小图标上时，会打开安全客户端控制台悬停提示。



下表列出了控制台悬停提示的图标及其含义：

表 A-2. 控制台悬停提示图标

功能	图标	含义
连接		已连接到安全管理服务器
		未连接到安全管理服务器，但实时扫描仍在运行。特征码文件可能不是最新的。右键单击 Windows 任务栏中的客户端图标，然后单击**立即更新**。

功能	图标	含义
实时扫描		打开
		关闭
云安全扫描		已连接到趋势科技云安全智能防护网络
		无法连接到云安全智能防护网络；会防护降低，因为安全客户端无法发送扫描查询。 **注意** 验证云安全扫描服务 TMiCRCScanService 是否正在运行以及安全客户端是否已连接到安全管理服务器。
		云安全扫描已禁用。正在使用传统扫描
• 防火墙 • Web 信誉 • URL 过滤 • 行为监控 • 设备控制		打开
		关闭

附录 B

WFBS 中的 IPv6 支持

本附录的适用对象是打算在支持 IPv6 寻址的环境中部署 WFBS 的用户。本附录包含有关 WFBS 中 IPv6 支持范围的信息。

趋势科技假设读者熟悉 IPv6 概念以及设置支持 IPv6 寻址的网络相关的任务。

WFBS 和 安全客户端 的 IPv6 支持

安全无忧软件从版本 8.0 开始提供 IPv6 支持。早期版本的安全无忧软件不支持 IPv6 寻址。安装或升级满足 IPv6 要求的安全管理服务器、安全客户端和邮件安全客户端之后，IPv6 支持将自动启用。

安全管理服务器 IPv6 要求

安全管理服务器的 IPv6 要求如下：

- 服务器必须安装在 Windows Server 2008/2012、SBS 2008/2011、7、8 和 Vista 上。不能将其安装在 Windows XP 或 Windows Server/SBS 2003 上，因为这些操作系统不完全支持 IPv6 寻址。
- 服务器必须使用 IIS Web 服务器。Apache web server 不支持 IPv6 寻址。
- 如果服务器将管理 IPv4 和 IPv6 客户端，则必须同时具有 IPv4 和 IPv6 地址，且必须用其主机名称进行标识。如果服务器用其 IPv4 地址进行标识，则纯 IPv6 客户端无法连接到该服务器。如果仅支持 IPv4 的客户端连接到用其 IPv6 地址进行标识的服务器，则会发生相同的问题。
- 如果服务器将仅管理 IPv6 客户端，则最低要求为一个 IPv6 地址。服务器可使用其主机名或 IPv6 地址进行标识。当服务器用其主机名进行标识时，会首选使用其全限定域名 (FQDN)。这是因为在纯 IPv6 环境中，WINS 服务器无法将主机名转换为其相应的 IPv6 地址。
- 确认可以使用诸如 "`ping`" 或 "`nslookup`" 等命令检索主机的 IPv6 或 IPv4 地址。
- 如果您正在纯 IPv6 计算机上安装安全管理服务器，请设置可在 IPv4 和 IPv6 地址之间进行转换的双栈代理服务器（例如 DeleGate）。将代理服务器置于安全管理服务器与 Internet 之间，以使服务器能够成功连接到趋势科技托管服务，例如 ActiveUpdate 服务器、在线注册 Web 站点和云安全智能防护网络。

安全客户端要求

安全客户端必须安装在以下操作系统上：

- Windows Vista（所有版本）
- Windows Server 2008（所有版本）
- Windows 7（所有版本）
- Windows SBS 2011
- Windows 8（所有版本）
- Windows Server 2012（所有版本）

不能将其安装在 Windows Server/SBS 2003 和 Windows XP 上，因为这些操作系统不完全支持 IPv6 寻址。

安全客户端最好同时具有 IPv4 和 IPv6 地址，因为它连接到的一些实体仅支持 IPv4 寻址。

邮件安全客户端要求

邮件安全客户端（仅限邮件与网络安全版）必须安装在双栈或纯 IPv6 Microsoft Exchange Server 上。

邮件安全客户端最好同时具有 IPv4 和 IPv6 地址，因为它连接到的一些实体仅支持 IPv4 寻址。

纯 IPv6 服务器限制

下表列出了安全管理服务器在仅具有 IPv6 地址时的限制。

表 B-1. 纯 IPv6 服务器限制

项目	限制
客户端管理	纯 IPv6 服务器无法执行以下操作： • 将客户端部署至纯 IPv4 客户机 • 管理纯 IPv4 客户端。
更新和集中式管理	纯 IPv6 服务器无法从纯 IPv4 更新源进行更新，例如： • 趋势科技 ActiveUpdate 服务器 • 任何纯 IPv4 定制更新源
产品注册、激活和续定	纯 IPv6 服务器无法连接到趋势科技在线注册服务器以注册产品、获取使用授权和激活/续定使用授权。
代理服务器连接	纯 IPv6 服务器无法通过纯 IPv4 代理服务器进行连接。
插件解决方案	纯 IPv6 服务器将具有插件管理器，但将无法将任何插件解决方案部署到： • 纯 IPv4 客户端或纯 IPv4 主机（由于没有直接连接） • 纯 IPv6 客户端或纯 IPv6 主机（由于所有插件解决方案均不支持 IPv6）。

通过设置可在 IPv4 和 IPv6 地址之间进行转换的双栈代理服务器（例如 DeleGate），可以克服上述大多数限制。请将代理服务器置于安全管理服务器与它连接的实体或它服务的实体之间。

纯 IPv6 安全客户端限制

下表列出了安全客户端仅具有 IPv6 地址时的限制。

表 B-2. 纯 IPv6 安全客户端限制

项目	限制
父级安全管理服务器	纯 IPv6 客户端无法由纯 IPv4 安全管理服务器管理。

项目	限制
更新	纯 IPv6 安全客户端无法从纯 IPv4 更新源进行更新，例如： • 趋势科技 ActiveUpdate 服务器 • 纯 IPv4 安全管理服务器 • 纯 IPv4 更新代理 • 任何纯 IPv4 定制更新源
扫描查询和智能反馈	纯 IPv6 安全客户端无法向趋势科技云安全智能防护网络发送查询并且无法使用智能反馈。
插件解决方案	纯 IPv6 客户端无法安装插件解决方案，因为所有插件解决方案均不支持 IPv6。
代理服务器连接	纯 IPv6 安全客户端无法通过纯 IPv4 代理服务器进行连接。

通过设置可在 IPv4 和 IPv6 地址之间进行转换的双栈代理服务器（例如 DeleGate），可以克服上述大多数限制。请将代理服务器置于安全客户端与它们连接的实体之间。

配置 IPv6 地址

通过 Web 控制台可配置 IPv6 地址或 IPv6 地址范围。下面是一些配置准则。

- WFBS 接受标准 IPv6 地址表示法。

  例如：

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- WFBS 也接受链接-本地 IPv6 地址，例如：

  `fe80::210:5aff:feaa:20a2`

警告!

指定链接-本地 IPv6 地址时务必小心，因为即使 WFBS 可以接受该地址，它也可能在某些情况下无法按预期工作。例如，如果更新源位于其他网段且用其链接-本地 IPv6 地址标识，则安全客户端无法从该源进行更新。

- IPv6 地址是 URL 的一部分时，请将该地址括在方括号中 ([])。
- 对于 IPv6 地址范围，前缀和前缀长度通常是必需的。对于需要服务器查询 IP 地址的配置，前缀长度限制用于防止服务器查询大量 IP 地址时可能出现的性能问题。例如，对于外部服务器管理功能，前缀长度只能介于 112（65,536 个 IP 地址）和 128（2 个 IP 地址）之间。
- 涉及 IPv6 地址或地址范围的一些设置会被部署到安全客户端，但是安全客户端会忽略它们。例如，如果配置了云安全智能防护源列表且包括由其 IPv6 地址标识的云安全智能防护服务器，则纯 IPv4 安全客户端将忽略该服务器并连接到其他云安全智能防护源。

显示 IP 地址的窗口

该主题列举了 Web 控制台中显示 IP 地址的位置。

- 安全组树

  无论何时显示安全组树，纯 IPv6 客户端的 IPv6 地址都会显示在 **IP 地址**列下。对于双栈客户端，如果它们使用自身的 IPv6 地址向服务器注册，则会显示它们的 IPv6 地址。

  注意

  在**首选项** > **全局设置** > **安全客户端**选项卡的**首选 IP 地址**部分中，可以控制双栈客户端在向服务器注册时使用的 IP 地址。

  将客户端设置导出至文件时，IPv6 地址也将显示在导出文件中。

- 日志

  双栈客户端和纯 IPv6 客户端的 IPv6 地址将显示在日志中。

附录 C

获取帮助

本附录介绍如何获取帮助、查找其他信息和联系趋势科技。

趋势科技知识库

趋势科技知识库，在趋势科技 Web 站点进行维护，具有对产品问题大部分最新答案。如果在产品文档中找不到答案，还可以用“知识库”来提交您的问题。可在以下地址访问“知识库”：

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

趋势科技不断更新知识库的内容并且每天添加新的解决方案。但是，如果无法找到答案，可以在电子邮件中描述问题然后将电子邮件直接发送给趋势科技技术支持工程师，他们将分析该问题并尽快回复。

与趋势科技联系

在中国，您可以通过电话或电子邮件与趋势科技销售代表取得联系：

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

- 全球技术支持办公室：

  http://cn.trendmicro.com/cn/about/contact_us/index.html

- 趋势科技产品文档：

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

案例诊断工具

趋势科技案例诊断工具 (CDT) 会在发生问题时收集来自客户产品的必要调试信息。CDT 可自动打开和关闭产品的调试状态，以及根据问题类别收集必要文件。趋势科技将使用此信息解决与产品相关的问题。

在 WFBS 支持的所有平台上运行该工具。要获得此工具及相关文档，请联系您的技术支持提供商。

加快支持呼叫的处理速度

为了能够更好地解决问题，请准备好以下信息：

- 重现问题的步骤
- 设备或网络信息
- 计算机品牌、型号和连接到终端的任何其他硬件
- 内存大小和可用硬盘空间
- 操作系统和 Service Pack 版本
- 终端客户端版本
- 序列号或激活码
- 安装环境的详细描述
- 收到的任何错误消息的准确文本

将可疑内容发送给趋势科技

将可疑内容发送给趋势科技进行进一步分析时，有多个选项可供选择。

文件信誉服务

收集系统信息并将可疑文件内容提交给趋势科技：

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

记录案例编号以备跟踪。

电子邮件信誉服务

查询特定 IP 地址的信誉，并提名将邮件传输客户端包括到全局允许列表：

https://ers.trendmicro.com/

要将邮件示例发送给趋势科技，请参考以下知识库条目：

http://esupport.trendmicro.com/solution/zh-CN/1112106.aspx

Web 信誉服务

查询疑似网络钓鱼站点的 URL 或其他所谓的“恶意站点”（Internet 威胁的源意向，例如间谍软件和恶意软件）的安全等级和内容类型：

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

如果分配的等级不正确，请将重新分类请求发送给趋势科技。

威胁百科全书

当今的大多数恶意软件都包含“混合性威胁”，将两种或更多种技术结合起来以绕过计算机安全协议。趋势科技通过可创建定制防御策略的产品来抵御这种复杂恶意软件。威胁百科全书提供了各种混合性威胁的名称和症状完整列表，包括已知恶意软件、垃圾邮件、恶意 URL 和已知漏洞。

请访问 http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=cn&tab=malware 了解更多信息：

- 当前处于活跃状态或“正在传播”的恶意软件和恶意活动代码
- 描述完整的 Web 攻击案例的相关威胁信息页面
- 有关针对性攻击和安全威胁的 Internet 威胁预警
- Web 攻击和联机趋势信息
- 每周恶意软件报告

TrendLabs

TrendLabs℠ 是一个全球性研究、开发和处理中心网络，致力于提供 24x7 威胁监视、攻击预防和及时且无缝的解决方案交付。TrendLabs 是趋势科技服务基础架构的骨干，其团队包括几百名工程师和经过认证的技术支持人员，可提供多种多样的产品和技术支持服务。

TrendLabs 会监控全球的威胁问题，提供有效的安全措施，以便能够检测攻击并尽早采取相应的操作，进而清除攻击。趋势科技会通过频繁的病毒码文件更新和扫描引擎改进，与客户分享每日的工作成果。

请访问以下网址了解有关 TrendLabs 的更多信息：

http://www.trendmicro.com.cn/cn/technology-innovation/experts/index.html

文档反馈

趋势科技一直致力于改进其文档。如果您对此文档或任何趋势科技文档存有疑问、评论或建议，请转到以下站点：

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

附录 D

产品术语和概念

本附录中包含的项目可提供有关趋势科技产品和技术的进一步信息。

关键 Patch

关键 Patch 关注的重点是适合部署到所有客户的安全问题。Windows 关键 Patch 包括一个安装程序，而非 Windows Patch 通常有一个安装脚本。

Hotfix

Hotfix 是针对客户报告的单个问题的解决方法或解决方案。Hotfix 特定于某个问题，因此不会发布给所有客户。Windows Hotfix 包括一个安装程序，而非 Windows Hotfix 没有（通常需要停止守护程序，复制文件以覆盖安装过程中其对应文件，然后再重新启动守护程序）。

IntelliScan

IntelliScan 是一种识别要扫描的文件的方法。对于可执行文件（如 `.exe`），真实文件类型基于文件内容而确定。对于非可执行文件（如 `.txt` 文件），可根据文件头确定真实文件类型。

使用 IntelliScan 具有以下好处：

- 性能优化：由于使用的系统资源最少，因此 IntelliScan 不会影响客户端上的应用程序。
- 更短的扫描周期：因为 IntelliScan 使用真实文件类型识别，它只扫描易受感染的文件。因此，扫描时间比扫描所有文件的时间要短得多。

IntelliTrap

IntelliTrap 是趋势科技的一项启发式技术，用于发现联合使用实时压缩与其他恶意软件特征（如加壳软件）的威胁。这涉及到病毒/恶意软件、蠕虫病毒、特洛伊木马、后门程序和 bot。病毒作者经常试图通过使用不同的文件压缩方式

来绕开病毒/恶意软件过滤。IntelliTrap 是一项实时的基于规则的特征码识别扫描引擎技术，可以在使用 16 种常见压缩类型中任何一种压缩深达六层的文件中检测并删除已知病毒/恶意软件。

注意

IntelliTrap 与病毒扫描使用同一扫描引擎。因此，IntelliTrap 的文件处理和扫描规则与管理员为病毒扫描所定义的文件处理和扫描规则相同。

客户端会将检测到的 bot 和其他恶意软件写到 IntelliTrap 日志中。您可以导出 IntelliTrap 日志的内容以在报表中包括这些内容。

IntelliTrap 在检查 bot 和其他恶意软件程序时使用以下组件：

- 病毒扫描引擎
- IntelliTrap 特征码
- IntelliTrap 例外特征码

真实文件类型

在设置为扫描“真实文件类型”后，扫描引擎将通过检查文件标题（而非文件名）来探知真实文件类型。例如，在将扫描引擎设为扫描所有可执行文件时，如果它遇到名为“`family.gif`”的文件，则不会将该文件假定为图形文件，而会打开文件标题并检查内部注册的数据类型，以确定该文件确实是图形文件，还是有人为了避免检测而故意这样命名的可执行文件。

通过使用真实文件类型扫描和 IntelliScan，可以只扫描那些已知可能存在危险的文件类型。使用这些技术可以减少扫描引擎要检查的文件数（多达三分之二）；但文件扫描减少还可能会带来一些风险，网络上可能会存在有害文件。

例如，`.gif` 文件需要使用大量的 Web 通信，但这些文件不大可能包含病毒/恶意软件、启动可执行代码或者执行任何已知或理论上存在的恶意操作。但是，这并不表示它们是完全安全的。恶意黑客有可能给有害文件使用“安全的”文件名从而蒙混过扫描引擎并进入网络。如果用户更名并运行该文件，则会造成损害。

提示

为确保获得最高等级的安全性，趋势科技建议扫描所有文件。

入侵检测系统

WFBS 防火墙还包括入侵检测系统 (IDS)。启用后，IDS 可帮助确定网络数据包中可能预示针对安全客户端的攻击的特征码。WFBS 防火墙可以帮助阻止以下众所周知的入侵：

入侵	描述
Too Big Fragment	拒绝服务攻击，黑客将特大的 TCP/UDP 数据包定向到目标客户端。这会导致客户端缓存溢出，从而使客户端死机或重新启动。
Ping of Death	拒绝服务攻击，黑客将特大的 ICMP/ICMPv6 数据包定向到目标客户端。这会导致客户端缓存溢出，从而使客户端死机或重新启动。
Conflicted ARP	一种攻击类型，黑客会向目标客户端发送带有相同源和目标 IP 地址的地址解析协议 (ARP) 请求。目标客户端会持续向自身发送 ARP 响应（其 MAC 地址），从而导致其死机或崩溃。
SYN Flood	拒绝服务攻击，程序会将多个 TCP 同步 (SYN) 数据包发送到客户端，从而导致客户端持续发送同步应答 (SYN/ACK) 响应。这可能会耗尽客户端内存并最终使客户端崩溃。
Overlapping Fragment	与 Teardrop 攻击相似，这种拒绝服务攻击会向客户端发送重叠的 TCP 碎片。会覆盖第一个 TCP 碎片中的头信息，并有可能通过防火墙。然后防火墙可能会允许带有恶意代码的后续碎片通过，到达目标客户端。
Teardrop	与 Overlapping Fragment 攻击相似，这种拒绝服务攻击涉及 IP 碎片。第二个或后面的 IP 碎片中的混淆偏移值会导致接收客户端的操作系统在尝试重新整理碎片时崩溃。
Tiny Fragment Attack	一种攻击类型，用一个很小的 TCP 碎片将第一个 TCP 数据包的头信息压到下一个碎片中。这可能会导致过滤通信的路由器忽略后续碎片，而这些碎片中可能会包含恶意数据。
Fragmented IGMP	一种拒绝服务攻击，向目标客户端发送被分割的 IGMP 数据包，导致无法正确处理 IGMP 数据包。这会使客户端死机或运行速度减慢。
LAND Attack	一种攻击类型，向客户端发送带有相同源地址和目标地址的 IP 同步 (SYN) 数据包，导致客户端向自身发送同步应答 (SYN/ACK) 响应。这会使客户端死机或运行速度减慢。

关键字

WFBS 中包括以下用于过滤邮件的关键字：

- 词（guns、bombs 等）
- 数字（1、2、3 等）
- 特殊字符（&、#、+ 等）
- 短语（blue fish、red phone、big house 等）
- 由逻辑运算符连接的词或短语 (apples .AND. oranges)
- 使用正则表达式的词或短语（.REG. a.*e 与 "ace"、"ate" 和 "advance" 匹配，但与 "all"、"any" 或 "antivirus" 不匹配）

WFBS 可以从文本 (`.txt`) 文件导入现有关键字列表。导入的关键字会显示在关键字列表中。

关键字运算符

运算符是组合多个关键字的命令。运算符可以扩大或缩小某一标准的结果。包含带有半角点号 (.) 的运算符。例如：

`apples .AND. oranges` 和 `apples .NOT. oranges`

注意

运算符前后紧挨着都有一个半角点号。最后的点和关键字之间有一个空格。

表 D-1. 使用运算符

操作者	工作原理	示例
任何关键字	邮件安全客户端搜索与词匹配的内容	键入该词并将其添加到关键字列表

操作者	工作原理	示例
OR	邮件安全客户端搜索由 OR 隔开的所有关键字 例如，apple OR orange。客户端搜索 apple 或 orange。如果内容中不包含这两者，则不存在匹配。	在要包括的所有词之间键入“`.OR.`” 例如， “apple .OR. orange”
AND	邮件安全客户端搜索由 AND 隔开的所有关键字 例如，apple AND orange。客户端搜索同时包含 apple 和 orange 的内容。如果内容不同时包含这两者，则不存在匹配。	在要包括的所有词之间键入“`.AND.`” 例如， “apple .AND. orange”
NOT	邮件安全客户端在搜索中排除 NOT 后面的关键字。 例如，.NOT. juice。客户端将搜索不包含 juice 的内容。如果邮件包含 "orange soda"，则存在匹配，但如果邮件包含 "orange juice"，则不存在匹配。	在要排除的词之前键入“`.NOT.`” 例如， ".NOT. juice"
WILD	通配符替换词中缺少的部分。包含通配符之外部分的任何词均构成匹配。 **注意** 邮件安全客户端不支持在通配符命令 ".WILD." 中使用 "?"。	在要包括的词部分之前键入“`.WILD.`” 例如，如果希望匹配包含“valu”的所有词，请键入“`.WILD.valu`”。词 Valumart、valucash 和 valubucks 都构成匹配。
REG	要指定“正则表达式”，请在该模式之前添加 .REG. 运算符（例如 .REG. a.*e）。 请参阅正则表达式 第 D-9 页。	在要检测的范式之前键入“`.REG.`”。 例如，".REG. a.*e" 与“ace”、“ate” 和 “advance” 匹配，但与 “all”、“any” 及 “antivirus” 不匹配

有效使用关键字

邮件安全客户端提供了简单且强大的功能以创建非常具体的过滤器。在创建“内容过滤”规则时，请考虑以下事项：

- 缺省情况下，邮件安全客户端会搜索与关键字完全匹配的内容。使用正则表达式可搜索与关键字部分匹配的内容。请参阅正则表达式 第 D-9 页。
- 邮件安全客户端可分析一行中的多个关键字，每个词都在单独行中的多个关键字，以及用半角逗号/半角点号/连字符/和其他不同的标点符号分隔的多个关键字。有关使用多行中的关键字的更多信息，请参阅下表。
- 也可以将邮件安全客户端设置为搜索实际关键字的同义词。

表 D-2. 使用关键字的方法

情形	示例	匹配/不匹配
两个词位于同一行中	guns bombs	匹配： "Click here to buy guns bombs and other weapons." 不匹配： "Click here to buy guns and bombs."
两个词用逗号隔开	guns, bombs	匹配： "Click here to buy guns, bombs, and other weapons." 不匹配： "Click here to buy used guns, new bombs, and other weapons."

情形	示例	匹配/不匹配
多个词位于多个行中	guns bombs weapons and ammo	当选择**任意指定的关键字**时 匹配： "Guns for sale" 也匹配： "Buy guns, bombs, and other weapons" 当选择**所有指定的关键字** 匹配： "Buy guns bombs weapons and ammo" 不匹配： "Buy guns bombs weapons ammunition." 也不匹配： "Buy guns, bombs, weapons, and ammo"
多个关键字位于同一行中	guns bombs weapons ammo	匹配： "Buy guns bombs weapons ammo" 不匹配： "Buy ammunition for your guns and weapons and new bombs"

Patch

Patch 是解决多个程序问题的一组 Hot Fix 和安全 Patch。趋势科技定期发布 Patch。Windows Patch 包括一个安装程序，而非 Windows Patch 通常有一个安装脚本。

正则表达式

正则表达式用于执行字符串匹配。下表中列出了正则表达式的一些常见示例。要指定正则表达式，请在该特征码之前添加 ".REG." 运算符。

您可以在线访问大量 Web 站点和教程。例如 PerlDoc 站点，其 Web 地址为：

http://www.perl.com/doc/manual/html/pod/perlre.html

警告!

正则表达式是功能强大的字符串匹配工具。因此，趋势科技建议选择使用正则表达式的管理员应该了解并熟悉正则表达式语法。不严谨的正则表达式会对性能产生极大的负面影响。趋势科技建议首先使用不涉及复杂语法的简单正则表达式。当引入新规则时，进行归档并观察邮件安全客户端如何使用规则来管理邮件。在确信规则不会产生意外的结果时，可以进行其他操作。

正则表达式示例

下表中列出了正则表达式的一些常见示例。要指定正则表达式，请在该特征码之前添加 ".REG." 运算符。

表 D-3. 计数和分组

元素	含义	示例
.	点号字符代表除换行字符之外的任何字符。	do. 与 doe、dog、don、dos、dot 等匹配。 d.r 与 deer、door 等匹配。
*	星号表示零个或者更多的前一元素。	do* 与 d、do、doo、dooo、doooo 等匹配。
+	加号字符表示一个或多个前一元素。	do+ 与 do、doo、dooo、doooo 等匹配，但不与 d 匹配。
?	问号字符表示零个或一个前一元素。	do?g 与 dg 或 dog 匹配，但不与 doog、dooog 等匹配。

元素	含义	示例
( )	圆括号字符中包含的任何内容均被视为一个实体。	d(eer)+ 与 deer、deereer 或 deereereer 等匹配。+ 符号应用于圆括号中的子字符串，因此该正则表达式查找后面跟随一组或多组 "eer" 的 d。
[ ]	方括号字符表示一组或一系列字符。	d[aeiouy]+ 与 da、de、di、do、du、dy、daa、dae、dai 等匹配。+ 符号应用于方括号中的集合，因此该正则表达式查找后面跟随一个或多个 [aeioy] 集合中的任意字符的 d。 d[A-Z] 与 dA、dB、dC 依次类推一直到 dZ 匹配。方括号中的集合表示 A 到 Z 之间的所有大写字母。
[^]	方括号中的克拉字符从逻辑上否定一组或一系列指定字符，表示该正则表达式将会与该组或系列以外的任意字符匹配。	d[^aeiouy] 与 db、dc 或 dd、d9、d# 以及其他由 d 后面跟随任何单个非元音字符构成的词匹配。
{ }	大括号字符设定前一元素出现的次数。大括号内的单个值表示仅在出现该值所设定的次数时构成匹配。由逗号分隔的一对数字表示前一字符的一组有效计数。一个数字后面跟随一个逗号表示没有上限。	da{3} 与 daaa--d 匹配，即 d 后面有三个（仅有三个） "a"。da{2,4} 与 daa、daaa、daaaa 和 daaaa 匹配（但不与 daaaaa 匹配），即 d 后面有两个、三个或四个 "a"。da{4,} 与 daaaa、daaaaa、daaaaaa 等匹配，即 d 后面有四个或更多个 "a"。

表 D-4. 字符类（简略方式）

元素	含义	示例
\d	任何数字字符，其功能相当于 [0-9] 或 [[:digit:]]	\d 与 1、12、123 等匹配，但与 1b7 不匹配，即与一个或多个任意数字字符匹配。

元素	含义	示例
\D	任何非数字字符，其功能相当于 [^0-9] 或 [^[:digit:]]	\D 与 a、ab、ab& 匹配，但与 1 不匹配，即与不包含 0、1、2、3、4、5、6、7、8 或 9 的一个或多个任意字符匹配。
\w	任何“词”字符，即任何字母数字字符，其功能相当于 [_A-Za-z0-9] 或 [_[:alnum:]]	\w 与 a、ab、a1 匹配，但与 !& 不匹配，即与一个或多个大写或小写字母或数字匹配，但与标点符号或其他特殊字符不匹配。
\W	任何非字母数字字符，功能相当于 [^_A-Za-z0-9] 或 [^_[:alnum:]]	\W 与 * 和 & 匹配，但与 ace 或 a1 不匹配，即与不包含大写/小写字母和数字的一个或多个任意字符匹配。
\s	任意空白字符，包括空格、换行字符、制表符、非换行空格等，其功能相当于 [[:space]]	vegetable\s 与后跟任意空白字符的 "vegetable" 匹配。因此，短语 "I like a vegetable in my soup" 将触发该正则表达式，而短语 "I like vegetables in my soup" 不会触发该正则表达式。
\S	任意非空白字符，包括空格、换行字符、制表符、非换行空格等字符之外的任意其他字符。其功能相当于 [^[:space]]	vegetable\S 与后跟任意非空白字符的 "vegetable" 匹配。因此，短语 "I like vegetables in my soup" 将触发该正则表达式，而短语 "I like a vegetable in my soup" 不会触发该正则表达式。

表 D-5. 字符类

元素	含义	示例
[:alpha:]	任何字母字符	.REG.[[:alpha:]]与 abc、def、xxx 匹配，但不与 123 或 @#$ 匹配。
[:digit:]	任何数字字符；功能上等同于 \d	.REG.[[:digit:]]匹配 1、12 和 123 等。
[:alnum:]	任何“词”字符，即任何字母数字字符；功能上等同于 \w	.REG.[[:alnum:]]与 abc 和 123 匹配，但不与 ~!@ 匹配。

元素	含义	示例
[:space:]	任意空白字符；空格、换行字符、制表符、非换行空格等；功能上等同于 \s	.REG.(vegetable)[[:space:]]与后跟任意空白字符的 "vegetable" 匹配。因此，短语 "I like a vegetable in my soup" 将触发该正则表达式，而短语 "I like vegetables in my soup" 不会触发该正则表达式。
[:graph:]	除空格、控制字符等之外的任何字符	.REG.[[:graph:]]与 123、abc、xxx、><” 匹配，但与空格或控制字符不匹配。
[:print:]	任何字符（类似于 [:graph:]）但包括空格字符	.REG.[[:print:]]与 123、abc、xxx、><” 和空格字符匹配。
[:cntrl:]	任何控制字符（例如，CTRL + C、CTRL + X）	.REG.[[:cntrl:]]与 0x03、0x08 匹配，但不与 abc、123、!@# 匹配。
[:blank:]	空格和制表符字符	.REG.[[:blank:]]与空格和制表符字符匹配，但不与 123、abc、!@# 匹配
[:punct:]	标点符号字符	.REG.[[:punct:]]与 ; :? ! ~ @ # $ % & * ‘ “ 等，但与 123、abc 不匹配
[:lower:]	任何小写字母字符（注意：必须启用“启用区分大小写匹配”，否则其作用将如同 [:alnum:]）	.REG.[[:lower:]]与 abc、Def、sTress、Do 等匹配，但不与 ABC、DEF、STRESS、DO、123、!@# 匹配。
[:upper:]	任何大写字母字符（注意：必须启用“启用区分大小写匹配”，否则其作用将如同 [:alnum:]）	.REG.[[:upper:]]与 ABC、DEF、STRESS、DO 等匹配，但不与 abc、Def、Stress、Do、123、!@# 匹配。
[:xdigit:]	十六进制数字中允许的数位 (0-9a-fA-F)	.REG.[[:xdigit:]]匹配 0a、7E 和 0f 等。

表 D-6. 范式锚点

元素	含义	示例
^	表示一个字符串的开头。	^(notwithstanding) 与以 "notwithstanding" 开头的任何文本块匹配。因此，短语 "notwithstanding the fact that I like vegetables in my soup" 将触发该正则表达式，而 "The fact that I like vegetables in my soup notwithstanding" 不会触发该正则表达式。
$	表示一个字符串的结尾。	(notwithstanding)$ 与以 "notwithstanding" 结尾的任何文本块匹配。因此，短语 "notwithstanding the fact that I like vegetables in my soup" 不会触发该正则表达式，而 "The fact that I like vegetables in my soup notwithstanding" 将触发该正则表达式。

表 D-7. 转义序列和字母字符串

元素	含义	示例
\	为了与正则表达式中具有特殊含义的某些字符（例如，"+"）匹配。	(1) .REG.C\\C\+\+ 与 "C\C++" 匹配。 (2) .REG.* 匹配 *。 (3) .REG.\? 匹配 ?。
\t	表示制表符字符。	(stress)\t 与包含子字符串 "stress" 且该子字符串后面紧跟制表符 (ASCII 0x09) 字符的任何文本块匹配。

元素	含义	示例
\n	表示换行字符。 **注意** 不同平台中的换行字符具有不同的表示方法。在 Windows 中，换行字符是一对字符，即一个回车符后面跟随一个换行符。在 Unix 和 Linux 中，换行字符只是一个换行符，而在 Macintosh 中换行字符只是一个回车符。	(stress)\n\n 与包含子字符串 "stress" 且该子字符串后面紧跟两个换行 (ASCII 0x0A) 字符的任何文本块匹配。
\r	表示回车字符。	(stress)\r 与包含子字符串 "stress" 且该子字符串后面紧跟一个回车 (ASCII 0x0D) 字符的任何文本块匹配。
\b	表示退格字符。 OR 表示边界。	(stress)\b 与包含子字符串 "stress" 且该子字符串后面紧跟一个退格 (ASCII 0x08) 字符的任何文本块匹配。 词边界 (\b) 的定义为两个字符之间的点，一边是 \w，另一边是 \W（顺序不限）。字符串的开头和结尾之外的虚字计为与 \W 相匹配。（在字符类内，\b 表示退格，而不是词边界。） 例如，以下正则表达式可与身份证号码相匹配：.REG.\b\d{3}-\d{2}-\d{4}\b
\xhh	表示通过给定十六进制代码表示的 ASCII 字符（其中 hh 代表任何两位十六进制值）。	\x7E(\w){6} 与恰好包含六位字母数字字符并且六位字母数字字符前面带有一个 ~（波形符）字符的任何文本块匹配。因此，该表达式与词 "~ab12cd"、"~Pa3499" 匹配，但与 "~oops" 不匹配。

正则表达式生成器

在确定数据丢失预防规则的配置方式时，需要考虑到，正则表达式生成器只能根据以下规则和限制创建简单的表达式：

- 仅字母数字字符可充当变量。
- 所有其他字符，如 [-] 和 [/] 等，仅可以充当常量。
- 变量范围只能从 A-Z 和 0-9；您不能对范围进行限制，如限制为 A-D。
- 此工具生成的正则表达式不区分大小写。
- 此工具生成的正则表达式只能进行正匹配，不能进行负匹配（“如果不匹配”）。
- 基于您的示例的表达式只可以匹配与示例数量完全相同的字符和空格，该工具无法生成可以匹配“一个或多个”给定字符或字符串的特征码。

复杂表达式语法

关键字表达式由令牌组成，令牌是用于将表达式与内容进行匹配的最小单位。令牌可以是运算符、逻辑符号或操作数，即运算符作用的参数或值。

运算符包括 .AND.、.OR.、.NOT.、.NEAR.、.OCCUR.、.WILD.、".(." 和 " .)."。操作数和运算符必须用一个空格分隔开。一个操作数还可以包含多个令牌。请参阅关键字 第 D-5 页。

正则表达式工作原理

以下示例描述了社会保险的缺省过滤器之一 — 内容过滤器的工作原理：

[Format] .REG.\b\d{3}-\d{2}-\d{4}\b

以上表达式使用 \b（一个退格字符），后跟 \d（任何数字），然后跟 {x}（表示数字的数量），最后加 -（表示连字号）。该表达式与社会保险号相匹配。下表描述了与示例正则表达式相匹配的字符串：

表 D-8. 与社会保险正则表达式相匹配的数字

.REG.\b\d{3}-\d{2}-\d{4}\b	
333-22-4444	匹配

333224444	不匹配
333 22 4444	不匹配
3333-22-4444	不匹配
333-22-44444	不匹配

如果将该表达式修改成以下情况，

[Format] .REG.\b\d{3}\x20\d{2}\x20\d{4}\b

新表达式则符合以下顺序：

333 22 4444

扫描例外列表

安全客户端的扫描例外列表

本例外列表包括缺省情况下从扫描对象中排除的所有趋势科技产品。

表 D-9. 安全客户端例外列表

产品名称	安装路径位置

InterScan eManager 3.5x	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion`
	
	`ProgramDirectory=`

ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion`
	
	`ProgramDirectory=`

产品名称	安装路径位置
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
InterScan Web 安全套件 (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Program Directory= C:\Program Files\Trend Micro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=

产品名称	安装路径位置
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

产品名称	安装路径位置
防毒墙群件版 for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder=

产品名称	安装路径位置
防毒墙群件版 for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= 从 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir 获取 exclusion.txt 文件路径 转至 HomeDir 路径（例如，C:\Program Files\Trend Micro\Messaging Security Agent\） 打开 exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

邮件安全客户端的扫描例外列表（仅限邮件与网络安全版）

缺省情况下，当邮件安全客户端安装在 Microsoft Exchange Server（2000 或更高版本）上时，它不会扫描 Microsoft Exchange 数据库、Microsoft Exchange 日志文件、虚拟服务器文件夹或 M:\ 驱动器。例外列表保存在：

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\

priv1.stm|C:\Program Files\Exchsrvr\mdbdata\

priv1.edb|C:\Program Files\Exchsrvr\mdbdata\

pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\
```

对于其他 Microsoft Exchange 建议的文件夹，请将它们手动添加到扫描例外列表。请参阅 http://support.microsoft.com/kb/245822/。

SBS 2003 例外

对于 SBS 2003，手动添加以下内容：

Microsoft Exchange 例外	
Microsoft Exchange Server 数据库	C:\Program Files\Exchsrvr\MDBDATA
Microsoft Exchange MTA 文件	C:\Program Files\Exchsrvr\Mtadata
Microsoft Exchange 邮件跟踪日志文件	C:\Program Files\Exchsrvr\server_name.log
Microsoft Exchange SMTP Mailroot	C:\Program Files\Exchsrvr\Mailroot
Microsoft Exchange 工作文件	C:\Program Files\Exchsrvr\MDBDATA
站点复制服务	C:\Program Files\Exchsrvr\srsdata C:\Program Files\Exchsrvr\conndata
IIS 例外	

IIS 系统文件	C:\WINDOWS\system32\inetsrv
IIS 压缩文件夹	C:\WINDOWS\IIS Temporary Compressed Files
域控制器例外	
Active Directory 数据库文件	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS 数据库文件	C:\WINDOWS\ntfrs
Windows SharePoint 服务例外	
SharePoint 临时文件夹	C:\windows\temp\FrontPageTempDir
客户端桌面文件夹例外	
Windows Update 存储	C:\WINDOWS\SoftwareDistribution\DataStore
其他例外	
可移动存储数据库（由 SBS Backup 使用）	C:\Windows\system32\NtmsData
SBS POP3 connector 失败邮件	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
SBS POP3 connector 传入邮件	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail
Windows Update 存储	C:\WINDOWS\SoftwareDistribution\DataStore
DHCP 数据库存储	C:\WINDOWS\system32\dhcp
WINS 数据库存储	C:\WINDOWS\system32\wins

Service Pack

Service Pack 是足以成为产品升级包的 Hot Fix、Patch 和增强功能的组合。Windows 和非 Windows Service Pack 都包括安装程序和安装脚本。

特洛伊木马端口

特洛伊木马程序通常通过特洛伊木马端口连接到客户端。在爆发期间，WFBS 会封闭特洛伊木马程序可能使用的以下端口号。

表 D-10. 特洛伊木马端口

端口号	特洛伊木马程序	端口号	特洛伊木马程序
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer

端口号	特洛伊木马程序	端口号	特洛伊木马程序
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

非可清除文件

病毒扫描引擎无法清除以下文件：

表 D-11. 非可清除文件解决方案

非可清除文件	说明和解决方案
受特洛伊木马感染的文件	特洛伊木马是一些执行意外或未经授权（通常是恶意）操作的程序；这些操作包括显示消息、删除文件或格式化磁盘等。特洛伊木马并不感染文件，所以不必进行清除。 解决方案：损害清除引擎和损害清除模板可删除特洛伊木马。
受蠕虫病毒感染的文件	蠕虫病毒是一种可向其他客户端系统传播其自身功能副本或片段的自包含程序或程序组。传播通常通过网络连接或电子邮件附件进行。无法清除蠕虫病毒，因为这种文件是自包含的程序。 解决方案：趋势科技建议删除蠕虫病毒。
已写保护的受感染文件	解决方案：去掉写保护以允许清除该文件。
密码保护的文件	密码保护的文件，包括密码保护的压缩文件或密码保护的 Microsoft Office 文件。

非可清除文件	说明和解决方案
	解决方案：去掉密码保护以允许清除该文件。
备份文件	扩展名为 RB0 到 RB9 的文件为受感染文件的备份副本。清除过程将创建受感染文件的备份，以防在清除过程中病毒/恶意软件损坏文件。 解决方案：如果成功清除受感染文件，则不需要保留其备份副本。如果客户端运行正常，可以删除备份文件。
回收站中的受感染文件	系统可能不允许移除回收站中的受感染文件，因为系统正在运行。

	针对使用 NTFS 文件系统的 Windows XP 或 Windows Server 2003 的解决方案：
	1. 以管理员权限登录到客户端。
	2. 关闭所有正在运行的应用程序，以防止应用程序锁定文件从而导致 Windows 无法删除文件。
	3. 打开命令提示符。
	4. 键入下列信息删除文件：
	`cd \`
	`cd recycled`
	`del *.* /S`
	最后的命令删除回收站中的所有文件。
	5. 检查文件是否已被删除。

	针对运行其他操作系统（或不使用 NTFS）的解决方案：
	1. 在 MS-DOS 模式下重新启动客户端。
	2. 打开命令提示符。
	3. 键入下列信息删除文件：
	`cd \`
	`cd recycled`
	`del *.* /S`
	最后的命令删除回收站中的所有文件。

非可清除文件	说明和解决方案
Windows Temp 文件夹或 Internet Explorer 临时文件夹中的受感染文件	系统可能不允许清除 Windows Temp 文件夹或 Internet Explorer 临时文件夹中的受感染文件，因为客户端正在使用它们。要清除的文件可能是 Windows 操作所需的临时文件。

	针对使用 NTFS 文件系统的 Windows XP 或 Windows Server 2003 的解决方案：
	1. 以管理员权限登录到客户端。
	2. 关闭所有正在运行的应用程序，以防止应用程序锁定文件从而导致 Windows 无法删除文件。
	3. 如果受感染文件在 Windows Temp 文件夹中：
	a. 打开命令提示符并转到 Windows Temp 文件夹（缺省情况下，对于 Windows XP 或 Server 2003 客户端，位于 `C:\Windows\Temp`）。
	b. 键入下列信息删除文件：
	`cd temp`
	`attrib -h`
	`del *.* /S`
	最后一条命令会删除 Windows Temp 文件夹中的所有文件。
	4. 如果受感染文件在 Internet Explorer 临时文件夹中：
	a. 打开命令提示符并转到 Internet Explorer Temp 文件夹（缺省情况下，对于 Windows XP 或 Windows Server 2003 客户端，位于 `C:\Documents and Settings\<`您的用户名`>\Local Settings\Temporary Internet Files`）。
	b. 键入下列信息删除文件：
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	最后一条命令会删除 Internet Explorer 临时文件夹中的所有文件。

非可清除文件	说明和解决方案
	c. 检查文件是否已被删除。

	针对运行其他操作系统（或不使用 NTFS）的解决方案：
	1. 在 MS-DOS 模式下重新启动客户端。
	2. 如果受感染文件在 Windows Temp 文件夹中：
	a. 打开命令提示符并转到 Windows Temp 文件夹（缺省情况下，对于 Windows XP 或 Server 2003 客户端，位于 `C:\Windows\Temp`）。
	b. 键入下列信息删除文件：
	`cd temp`
	`attrib -h`
	`del *.* /S`
	最后一条命令会删除 Windows Temp 文件夹中的所有文件。
	c. 在正常模式下重新启动客户端。
	3. 如果受感染文件在 Internet Explorer 临时文件夹中：
	a. 打开命令提示符并转到 Internet Explorer Temp 文件夹（缺省情况下，对于 Windows XP 或 Windows Server 2003 客户端，位于 `C:\Documents and Settings\<`您的用户名`>\Local Settings\Temporary Internet Files`）。
	b. 键入下列信息删除文件：
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	最后一条命令会删除 Internet Explorer 临时文件夹中的所有文件。
	c. 在正常模式下重新启动客户端。

用不支持的压缩格式压缩过的文件	解决方案：解压缩文件。

非可清除文件	说明和解决方案
当前正在执行的被锁定的文件	解决方案：解锁文件，或等待文件执行。
遭破坏的文件	解决方案：删除文件。

索引

趋势科技・中国 趋势科技（中国）有限公司
上海市淮海中路 398 号世纪巴士大厦 8 楼
电话：021-6384 8899 传真：021-6384 1899 service@trendmicro.com.cn

www.trendmicro.com

Item Code: WFCM97382/160406