TREND MICRO™

11.0 防毒墙网络版™

Service Pack 1 关键 Patch

管理员指南

适用于大中型企业









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

http://docs.trendmicro.com/zh-cn/enterprise/officescan.aspx

Trend Micro、Trend Micro t 球徽标、OfficeScan、Control Manager、Damage Cleanup Services、eManager、InterScan、Network VirusWall、ScanMail、ServerProtect 和 TrendLabs 是趋势科技（中国）有限公司 的商标或注册商标。所有其他产品或公司名称可能是其各自所有者的商标或注册商标。

版权所有 © 2015。趋势科技（中国）有限公司。保留所有权利。

文档编号：OSCM117089/150730

发布日期：2015 年 7 月

受美国专利号保护： 5,951,698

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

前言 xi

防毒墙网络版文档 xii

读者 xii

文档规则 xiii

术语 xiii

部分 I：简介和入门

第 1 章：防毒墙网络版简介

关于防毒墙网络版 1-2

此发行版的新功能 1-2

关键功能和优点 1-9

防毒墙网络版服务器 1-12

防毒墙网络版客户端 1-13

与趋势科技产品和服务集成 1-14

第 2 章：防毒墙网络版入门

Web 控制台 2-2

控制台 2-5

服务器迁移工具 2-30

Active Directory 集成 2-34

防毒墙网络版客户端树 2-38

防毒墙网络版域 2-50

第 3 章：数据保护入门

数据保护安装 3-2
数据保护使用授权 3-3
将数据保护部署到防毒墙网络版客户端 3-5
取证文件夹和 DLP 数据库 3-8
卸载数据保护 3-13

部分 II：保护防毒墙网络版客户端

第 4 章：使用趋势科技云安全智能防护

关于趋势科技云安全智能防护 4-2
云安全智能防护服务 4-3
云安全智能防护源 4-5
云安全智能防护病毒码文件 4-7
设置云安全智能防护服务 4-11
使用云安全智能防护服务 4-29

第 5 章：安装防毒墙网络版客户端

防毒墙网络版客户端全新安装 5-2
安装注意事项 5-2
部署注意事项 5-10
迁移到防毒墙网络版客户端 5-56
安装后 5-60
防毒墙网络版客户端卸载 5-63

第 6 章：使防护保持最新

防毒墙网络版组件与程序 6-2
更新概述 6-13

防毒墙网络版服务器更新 6-15
集成型云安全智能防护服务器更新 6-26
防毒墙网络版客户端更新 6-26
更新代理 6-49
组件更新摘要 6-57

第 7 章：扫描安全风险

关于安全风险 7-2
扫描方法类型 7-7
扫描类型 7-12
所有扫描类型的通用设置 7-22
扫描权限和其他设置 7-47
全局扫描设置 7-62
安全风险通知 7-72
安全风险日志 7-81
安全风险爆发 7-94

第 8 章：使用行为监控

行为监控 8-2
配置全局行为监控设置 8-7
行为监控权限 8-10
针对防毒墙网络版客户端用户的行为监控通知 8-11
行为监控日志 8-13

第 9 章：使用设备控制

设备控制 9-2
存储设备的权限 9-4
非存储设备的权限 9-9
修改设备控制通知 9-16

设备控制日志 9-16

第 10 章：使用数据丢失防护

关于数据丢失防护 (DLP) 10-2
数据丢失防护策略 10-3
数据标识符类型 10-4
数据丢失防护模板 10-18
DLP 通道 10-22
数据丢失防护措施 10-35
数据丢失防护例外 10-38
数据丢失防护策略配置 10-43
数据丢失防护通知 10-48
数据丢失防护日志 10-52

第 11 章：保护计算机免受基于 Web 的威胁

关于 Web 威胁 11-2
命令与控制联系人警报服务 11-2
Web 信誉 11-4
Web 信誉策略 11-4
可疑连接服务 11-12
客户端用户的 Web 威胁通知 11-15
适用于管理员的 C&C 回调通知 11-17
针对客户端用户的 C&C 联系人警报通知 11-19
C&C 回呼爆发 11-21
Web 威胁日志 11-23

第 12 章：使用防毒墙网络版防火墙

关于防毒墙网络版防火墙 12-2

启用或禁用防毒墙网络版防火墙 12-6
防火墙策略和概要文件 12-7
防火墙权限 12-21
全局防火墙设置 12-23
向防毒墙网络版客户端用户发送的防火墙违例通知 12-25
防火墙日志 12-26
防火墙违例爆发 12-28
测试防毒墙网络版防火墙 12-29

部分 III：管理防毒墙网络版服务器和客户端

第 13 章：管理防毒墙网络版服务器

基于角色的管理 13-3
趋势科技防毒墙控制管理中心 13-22
可疑对象列表设置 13-28
参考服务器 13-30
管理员通知设置 13-32
系统事件日志 13-34
日志管理 13-35
使用授权 13-38
防毒墙网络版数据库备份 13-41
SQL Server 迁移工具 13-43
防毒墙网络版 Web 服务器/客户端连接设置 13-47
服务器-客户端通信 13-48
Web 控制台密码 13-53
Web 控制台设置 13-53
隔离管理器 13-54

服务器调节程序 13-55
云安全智能反馈 13-58

第 14 章：管理防毒墙网络版客户端

终端位置 14-2
防毒墙网络版客户端程序管理 14-5
客户端-服务器连接 14-25
防毒墙网络版客户端代理服务器设置 14-44
查看防毒墙网络版客户端信息 14-49
导入和导出客户端设置 14-49
安全合规 14-51
趋势科技虚拟桌面支持 14-67
全局客户端设置 14-80
配置客户端权限和其他设置 14-81

部分 IV：提供其他防护

第 15 章：使用插件管理器

关于插件管理器 15-2
插件管理器安装 15-3
本机防毒墙网络版功能管理 15-4
管理插件程序 15-4
卸载插件管理器 15-10
插件管理器故障排除 15-11

第 16 章：资源故障排除

支持情报系统 16-2
案例诊断工具 16-2
趋势科技性能调整工具 16-2

防毒墙网络版服务器日志 16-2
防毒墙网络版客户端日志 16-15

第 17 章：技术支持

资源故障排除 17-2
与趋势科技联系 17-4
将可疑内容发送给趋势科技 17-5
其他资源 17-6

附录

附录 A：防毒墙网络版中的 IPv6 支持

防毒墙网络版服务器和客户端的 IPv6 支持 A-2
配置 IPv6 地址 A-5
显示 IP 地址的窗口 A-6

附录 B：Windows Server Core 2008/2012 支持

Windows Server Core 2008/2012 支持 B-2
Windows Server Core 安装方法 B-2
Windows Server Core 上的防毒墙网络版客户端功能 B-6
Windows Server Core 命令 B-7

附录 C：Windows 8/8.1/10 和 Windows Server 2012 支持

关于 Windows 8/8.1/10 和 Windows Server 2012 ..... C-2
处于 UI 模式的防毒墙网络版功能支持 C-4
Internet Explorer 10/11 和 Microsoft Edge C-5

附录 D：防毒墙网络版还原

还原防毒墙网络版服务器和防毒墙网络版客户端 D-2

附录 E：词汇表

ActiveUpdate E-2
压缩文件 E-2
Cookie E-2
拒绝服务攻击 E-2
DHCP E-2
DNS E-3
域名 E-3
动态 IP 地址 E-3
ESMTP E-3
最终用户许可协议 E-4
误报 E-4
FTP E-4
GeneriClean E-4
Hotfix E-4
HTTP E-5
HTTPS E-5
ICMP E-5
IntelliScan E-6
IntelliTrap E-6
IP E-6
Java 文件 E-7
LDAP E-7
侦听端口 E-7
MCP 代理 E-7
混合威胁攻击 E-8
NAT E-8

NetBIOS E-8
单向通信 E-8
Patch E-9
Phish Attack（网络钓鱼攻击） E-9
Ping E-9
POP3 ..... E-10
代理服务器 E-10
RPC E-10
安全 Patch E-10
Service Pack E-10
SMTP E-11
SNMP E-11
SNMP 陷阱 E-11
SOCKS 4 ..... E-11
SSL E-11
SSL 证书 E-12
TCP E-12
Telnet E-12
特洛伊木马端口 E-12
可信端口 E-14
双向通信 E-15
UDP E-15
非可清除文件 E-15

索引

索引 IN-1

前言

前言

本文档介绍入门信息、客户端安装过程以及防毒墙网络版服务器和客户端管理。

主题包括：

- 防毒墙网络版文档 第 xii 页
- 读者 第 xii 页
- 文档规则 第 xiii 页
- 术语 第 xiii 页

防毒墙网络版文档

防毒墙网络版文档包括：

表 1. 防毒墙网络版文档

文档	描述
安装和升级指南	PDF 文档，介绍安装防毒墙网络版服务器以及升级服务器和客户端的需求和过程
管理员指南	PDF 文档，介绍入门信息、防毒墙网络版客户端安装过程以及防毒墙网络版服务器和客户端管理
帮助	编译为 WebHelp 或 CHM 格式的 HTML 文件，提供操作指导、使用建议和特定文本框的信息。可通过防毒墙网络版服务器、客户端控制台和防毒墙网络版主安装程序访问帮助。
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。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://cn.trendmicro.com/cn/support/techsupport/index.html

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/enterprise/officescan.aspx

读者

防毒墙网络版文档供以下用户使用：

- 防毒墙网络版管理员：负责防毒墙网络版管理，包括防毒墙网络版服务器和防毒墙网络版客户端的安装和管理。这些用户应具有高级联网和服务器管理知识。
- 最终用户：在其终端上安装了防毒墙网络版客户端的用户。他们的终端技能不一，从初学者到高级用户不等。

文档规则

本文档采用以下约定。

表 2. 文档规则

规则	描述
大写	首字母缩略词、缩写以及某些命令和键盘按键的名称
粗体	菜单和菜单命令、命令按钮、选项卡和选项
斜体	引用其他文档
等距	示例命令行、程序代码、Web URL、文件名和程序输出
导航 > **路径**	访问特定窗口的导航路径 例如，**文件** > **保存**是指在界面上单击**文件**，然后单击**保存**
 **注意**	配置说明
 **提示**	建议
 **重要信息**	与必需或缺省配置设置和产品限制有关的信息
 **警告!**	关键操作和配置选项

术语

下表提供在整个防毒墙网络版文档中使用的正式术语：

表 3. 防毒墙网络版术语

术语	描述
防毒墙网络版客户端	防毒墙网络版客户端程序
客户端 终端	安装防毒墙网络版客户端的终端
客户端用户（或用户）	在客户端终端上管理防毒墙网络版客户端的用户
服务器	防毒墙网络版服务器程序
服务器计算机	安装防毒墙网络版服务器的终端
管理员（或防毒墙网络版管理员）	管理防毒墙网络版服务器的人
控制台	用于配置和管理防毒墙网络版服务器和客户端设置的用户界面 用于防毒墙网络版服务器程序的控制台称为“Web 控制台”，而用于防毒墙网络版客户端程序的控制台称为“客户端控制台”。
安全风险	病毒/恶意软件、间谍软件/灰色软件和 Web 威胁的统称
使用授权服务	包括防病毒、损害清除服务以及 Web 信誉和防间谍软件 – 它们都是在防毒墙网络版服务器安装期间激活的
防毒墙网络版服务	通过 Microsoft 管理控制台 (MMC) 托管的服务。例如，防毒墙网络版主服务的 ofcservice.exe。
程序	包括防毒墙网络版客户端和插件管理器
组件	负责对安全风险进行扫描、检测和采取处理措施
客户端安装文件夹	终端上包含防毒墙网络版客户端文件的文件夹。如果在安装期间接受缺省设置，您将在以下任一位置找到安装文件夹： C:\Program Files\Trend Micro\OfficeScan Client C:\Program Files (x86)\Trend Micro\OfficeScan Client

术语	描述
服务器安装文件夹	终端上包含防毒墙网络版服务器文件的文件夹。如果在安装期间接受缺省设置，您将在以下任一位置找到安装文件夹： C:\Program Files\Trend Micro\OfficeScan C:\Program Files (x86)\Trend Micro\OfficeScan 例如，如果在服务器安装文件夹的\PCCSRV 下找到一个特定的文件，则该文件的完整路径是： C:\Program Files\Trend Micro\OfficeScan\PCCSRV\<file_name>。
云安全扫描客户端	已配置为使用云安全扫描的任何防毒墙网络版客户端
传统扫描客户端	已配置为使用传统扫描的任何防毒墙网络版客户端
双栈	同时具有 IPv4 和 IPv6 地址的实体。 例如： • 同时具有 IPv4 和 IPv6 地址的终端 • 安装在双栈终端上的防毒墙网络版客户端 • 向客户端分发更新的更新代理 • 双栈代理服务器（如 DeleGate）可以在 IPv4 和 IPv6 地址之间实现转换
纯 IPv4	仅具有 IPv4 地址的实体
纯 IPv6	仅具有 IPv6 地址的实体
插件解决方案	通过插件管理器提供的本机防毒墙网络版功能和插件程序

部分 I

简介和入门

第 1 章

防毒墙网络版简介

本章介绍趋势科技™ 防毒墙网络版™ 并提供其特性和功能的概述。

主题包括：

- 关于防毒墙网络版 第 1-2 页
- 此发行版的新功能 第 1-2 页
- 关键功能和优点 第 1-9 页
- 防毒墙网络版服务器 第 1-12 页
- 防毒墙网络版客户端 第 1-13 页
- 与趋势科技产品和服务集成 第 1-14 页

关于防毒墙网络版

趋势科技™ 防毒墙网络版™ 可保护企业网络免受恶意软件、网络病毒、基于 Web 的威胁、间谍软件和混合威胁攻击的危害。防毒墙网络版是集成的解决方案，包括驻留在终端的防毒墙网络版客户端程序和管理所有客户端的服务器程序。此防毒墙网络版客户端会保护终端并将其安全状态报告给服务器。通过基于 Web 的管理控制台。服务器可以轻松在每个客户端上设置协调的安全策略并部署更新。

防毒墙网络版由趋势科技云安全智能防护网络™ 提供支持，该网络是新一代云客户端基础架构，可提供比传统方法更智能的安全性。独特的云端技术和轻量级客户端减少了对传统病毒码下载的依赖，并且消除了通常与桌面更新相关的延迟。企业将受益于网络带宽增加、处理功耗降低及相关的成本节省。无论用户在哪里（公司网络、家中或路途中）进行连接，都可以直接访问最新防护。

此发行版的新功能

趋势科技防毒墙网络版包括以下新功能和增强功能。

防毒墙网络版 11.0 SP1 关键 Patch 中的新增功能

此版本的防毒墙网络版包括以下新增功能和增强功能。

功能	描述
平台和浏览器支持	防毒墙网络版客户端支持 Windows 10（Home、Pro、Education 和 Enterprise 版）。 防毒墙网络版支持 Microsoft Edge。 有关系统要求的列表，请参阅 *“防毒墙网络版的系统要求”* 文档，网址为： http://docs.trendmicro.com/zh-cn/enterprise/officescan.aspx

功能	描述
预启动的防恶意软件防护	作为安全启动标准，防毒墙网络版支持预启动的防恶意软件 (ELAM) 功能，能够在终端上提供启动时防护。管理员可启用此功能，以便当终端启动时，在其他第三方软件驱动程序之前启动防毒墙网络版客户端。此功能可使防毒墙网络版客户端在启动过程中检测恶意软件。 有关详细信息，请参阅在终端上启用预启动的防恶意软件防护 第 7-65 页。
增强的可疑对象订阅过程	当管理员将防毒墙网络版注册到连接至 Deep Discovery 的控制管理中心服务器时，防毒墙网络版将自动订阅控制管理中心，以便同步可疑对象，并检索针对这些对象的处理措施。 可疑对象列表同步是联动威胁治理策略的一部分。有关更多信息，请参阅《联动威胁治理手册》，网址为 http://docs.trendmicro.com/all/ent/tmcm/v6.0-sp3/zh-cn/tmcm_6.0_sp3_ctd_primer/ctd_primer.pdf。

防毒墙网络版 11.0 SP1 中的新增功能

此版本的防毒墙网络版包括以下新增功能和增强功能。

功能	描述
针对文档的勒索软件防护	增强的扫描功能可以识别常见行为并阻止通常与勒索软件程序关联的进程，进而识别和阻止专门攻击在终端上运行的文档的勒索软件程序。
增强的服务器-客户端通信加密	防毒墙网络版使用高级加密标准 (AES) 256 为服务器和客户端之间的通信提供增强的加密，以符合安全合规标准。
联动威胁治理	配置防毒墙网络版，从控制管理中心服务器订阅可疑对象列表。通过控制管理中心控制台，您可以针对可疑对象列表检测到的对象创建定制处理措施，以对特定于您环境的趋势科技产品所保护的终端所识别的威胁进行定制防御。

功能	描述
扫描监控	防毒墙网络版借助以下特性对扫描功能提供更好的可见性和控制： • 重新开始中断的预设扫描：将防毒墙网络版配置为根据已配置的时间表自动重新开始中断的预设扫描 • 扫描操作日志：使用 Web 控制台监控扫描时间、扫描状态和扫描结果
敏感数据加密	数据丢失防护与趋势科技™终端加密™集成，从而可自动加密传输到可移动设备和云存储服务通道的敏感数据。
增强的防毒墙网络版客户端自我保护功能	• 增强的文件完整性监控和 DLL 劫持防护可确保防毒墙网络版客户端程序文件的有效性和可用性 • 防止防毒墙网络版客户端进程被阻止
多语言防毒墙网络版客户端支持	管理员可从 Web 控制台配置防毒墙网络版客户端程序语言。选择该功能可根据已登录用户的语言设置或防毒墙网络版服务器语言设置显示防毒墙网络版客户端控制台。
通过控制管理中心™获得扩展的策略管理	• 管理员现在可使用防毒墙网络版服务器的控制管理中心™ 策略管理创建继承控制管理中心全局设置的子策略。通过控制管理中心控制台，本地防毒墙网络版管理员可以修改这些子策略，以更好地保护需要更多特定设置的区域、部门或卫星服务器。本地防毒墙网络版管理员可以修改预设扫描时间和扫描例外列表，以更好地保护其本地环境，同时还可以维护由控制管理中心管理员配置的保护。 • 控制管理中心™ 管理员可以隔离来自网络的特定防毒墙网络版客户端终端，以防止安全威胁传播。 有关使用控制管理中心™ 配置防毒墙网络版策略的详细信息，请参阅请参阅《趋势科技防毒墙控制管理中心管理员指南》。
可信程序	管理员可配置防毒墙网络版以便把由可信公司签名的文件和进程排除在扫描范围之外，并把已配置的例外列表应用于实时扫描和行为监控，或者为任一功能创建特定的列表。

有关系统要求的列表，请参阅 *“防毒墙网络版的系统要求”* 文档，网址为：

http://docs.trendmicro.com/zh-cn/enterprise/officescan.aspx

防毒墙网络版 11.0 中的新增功能

此版本的防毒墙网络版包括以下新增功能和增强功能。

表 1-1. 服务器增强功能

功能	描述
SQL 数据库迁移工具	管理员可以选择将现有的 CodeBase® 服务器数据库迁移到 SQL Server 数据库。 有关详细信息，请参阅 SQL Server 迁移工具 第 13-43 页。
云安全智能防护服务器增强功能	此版本的防毒墙网络版支持升级的云安全智能防护服务器 3.0。升级的云安全智能防护服务器包括文件信誉服务特征码增强功能。已重新设计特征码文件，以便提供以下优点： • 减少了内存占用 • 进行增量特征码更新和增强文件信誉服务特征码检测，可大大减少带宽消耗
服务器认证	增强服务器认证密钥可确保与服务器进行的所有通信都安全可信。 有关详细信息，请参阅服务器启动的通信的认证 第 13-48 页。
基于角色的管理增强功能	基于角色的管理增强功能简化了管理员配置角色和帐户的方式，使得与趋势科技™ 防毒墙控制管理中心™ 的集成更为简单。 有关详细信息，请参阅基于角色的管理 第 13-3 页。
Web 服务器需求	此版本的防毒墙网络版可与 Apache 2.2.25 Web 服务器集成。
防毒墙网络版服务器界面重新设计	防毒墙网络版界面已进行重新设计，可提供更加简单、更为简化以及更加现代化的体验。先前的防毒墙网络版服务器中的所有功能在更新的版本中仍然可用。 • 顶层菜单项释放窗口空间 • “收藏夹”菜单可帮助您定期查找使用过的窗口 • 面板选项卡的幻灯片视图允许您查看小组件数据，而无需手动控制控制台
基于云的上下文联机帮助	基于云的上下文联机帮助可确保管理员始终了解帮助系统打开时的最新信息。如果 Internet 连接不可用，防毒墙网络版会自动切换到随产品一起发行的本地联机帮助系统。

功能	描述
平台和浏览器支持	防毒墙网络版支持下列操作系统： • Windows Server™ 2012 R2（服务器和客户端） • Windows 8.1（仅限客户端） 防毒墙网络版支持下列浏览器： • Internet Explorer™ 11.0

表 1-2. 客户端增强功能

功能	描述
集中隔离恢复	防毒墙网络版为管理员提供恢复先前检测到的“可疑”文件以及将文件添加到域级“允许”列表以阻止对文件进行进一步操作的能力。 如果已检测到并已隔离程序或文件，管理员可以全局或粒度恢复客户端上的文件。管理员可以使用其他的 SHA1 验证检查来确保要恢复的文件尚未进行任何形式的修改。恢复文件后，防毒墙网络版可自动将文件添加到域级例外列表，以使其免受进一步扫描。 有关详细信息，请参阅恢复隔离文件 第 7-37 页。
高级保护服务	高级保护服务提供了以下全新扫描功能。 • 在防毒墙网络版客户端暴露在威胁中之前，浏览器安全漏洞防御使用沙盒技术实时测试 Web 页面的行为并检测任何恶意脚本或程序。 有关详细信息，请参阅配置 Web 信誉策略 第 11-5 页。 • 增强的内存扫描与行为监控结合使用，可在实时扫描期间检测恶意软件变种，并针对威胁采取隔离措施。 有关详细信息，请参阅扫描设置 第 7-23 页。

功能	描述
数据保护增强功能	已增强防毒墙网络版数据保护，以便提供以下优点： • 通过与控制管理中心™ 集成的数据发现管理员可在控制管理中心配置数据丢失防护策略来扫描防毒墙网络版客户端的文件夹中的敏感文件。在文件中发现敏感数据后，控制管理中心可以记录文件的位置，或通过与趋势科技终端加密集成来对防毒墙网络版客户端上的文件进行自动加密。 • 用户原因支持：管理员可以允许用户提供传输敏感数据的原因或自己阻止传输。防毒墙网络版会记录所有传输尝试和用户提供的原因。 有关详细信息，请参阅数据丢失防护措施 第 10-35 页。 • 智能手机和平板电脑支持：数据丢失防护和设备控制现在可以监控发送到智能设备的敏感数据并对其采取措施，或完全阻止对智能设备的访问。 有关详细信息，请参阅设备控制 第 9-2 页。 • 更新的数据标识符和模板库：数据丢失防护库已更新了 2 个新的关键字列表和 93 个新的模板。 • 与控制管理中心™ 集成的设备控制日志
可疑连接设置增强功能	命令与控制 (C&C) 联系人警报服务已更新为包括以下内容： • 全局用户定义的允许和阻止 IP 列表 有关详细信息，请参阅配置用户定义的全局 IP 列表设置 第 11-13 页。 • 检测 C&C 回呼的恶意软件网络指纹验证 • 检测到可疑连接时的粒度操作配置 有关详细信息，请参阅配置可疑连接设置 第 11-14 页。 • C&C 服务器和客户端日志会记录负责 C&C 回呼的进程

功能	描述
爆发阻止增强功能	爆发阻止已更新，可针对以下内容提供保护： • 压缩可执行文件 有关详细信息，请参阅拒绝访问压缩可执行文件 第 7-104 页。 • 互斥进程 有关详细信息，请参阅在恶意软件进程/文件上创建互相排斥处理 第 7-103 页。
自我保护功能增强	此版本中的自我保护功能同时提供了轻量级和高级别安全解决方案，可用来保护您的服务器和防毒墙网络版客户端程序。 • 轻量级解决方案：缺省情况下，专门为服务器平台保护防毒墙网络版客户端进程和注册表项而设计，不会影响服务器的性能 • 高级别安全解决方案：通过提供以下内容增强了先前版本中的客户端自我保护功能： • IPC 命令认证 • 特征码文件防护和验证 • 特征码文件更新防护 • 行为监控进程防护 有关详细信息，请参阅防毒墙网络版客户端自我保护 第 14-12 页。

功能	描述
扫描性能和检测增强功能	• 实时扫描会对防毒墙网络版客户端每次启动时都会重新加载的持续性扫描缓存进行维护。防毒墙网络版客户端会跟踪由于退出防毒墙网络版客户端导致的文件或文件夹的任何更改，并从缓存中删除这些文件。 • 此版本的防毒墙网络版包括 Windows 系统文件的全局允许列表、可信源的数字签名文件以及趋势科技测试的文件。验证文件为安全文件后，防毒墙网络版不会对该文件执行任何操作。 • 损害清除服务增强功能提供了针对 rootkit 威胁的改进的检测功能，并通过更新的 GeneriClean 扫描降低了误报次数。 • 实时扫描和按需扫描之间的压缩文件设置是分开的，从而有助于提高性能。 有关详细信息，请参阅配置大型压缩文件的扫描设置 第 7-66 页。 • 双层日志针对管理员想要进一步检查的检测提供了一个更为详细的视图。
防毒墙网络版客户端界面重新设计	防毒墙网络版客户端界面已进行重新设计，可提供更加简单、更为简化以及更加现代化的体验。先前的防毒墙网络版客户端程序中的所有功能在更新的版本中仍然可用。 更新的界面还允许管理员直接从防毒墙网络版客户端控制台中“解锁”管理功能，以便不用打开 Web 控制台就能快速解决问题。

关键功能和优点

防毒墙网络版具有以下功能和优点。

表 1-3. 关键功能和优点

功能	优点
插件管理器和插件解决方案	插件管理器可简化插件解决方案的安装、部署和管理。 管理员可安装两种插件解决方案： • 插件程序 • 本机防毒墙网络版功能
集中式管理	通过基于 Web 的管理控制台，管理员可以透明访问网络上的所有客户端和服务器。Web 控制台可协调安全策略、特征码文件和软件更新在每个客户端和服务器上的自动部署。结合爆发阻止服务，Web 控制台可在特征码文件可用前关闭感染站点，以及快速部署特定于攻击的安全策略以阻止或抑制爆发。防毒墙网络版还执行实时监控，提供事件通知以及传递全面的报告。管理员可以执行远程管理，为个别台式机或台式机组设置定制策略以及锁定客户端安全设置。
安全风险防护	防毒墙网络版通过扫描文件，然后对每一个检测到的安全风险执行特定的处理措施来保护计算机免遭安全风险的侵扰。在短时间内检测到数量庞大的安全风险意味着病毒爆发。要抑制爆发，防毒墙网络版会强制执行爆发阻止策略并且隔离受感染的计算机，直到它们完全不存在风险。 防毒墙网络版使用云安全扫描来使扫描进程更有效率。该技术的工作原理是，将先前存储在本地终端上的大量签名转移到云安全智能防护源。使用这种方法，持续增长的签名更新数量对“终端系统”的系统与网络影响将大大降低。 有关云安全扫描以及如何将其部署到客户端的信息，请参阅扫描方法类型 第 7-7 页。

功能	优点
损害清除服务	损害清除服务™ 通过全自动过程，清除计算机中基于文件的病毒和网络病毒以及病毒和蠕虫残留（特洛伊木马、注册表项和含病毒的文件）。要处理由特洛伊木马造成的威胁和损害，损害清除服务将执行以下操作： • 检测和移除活动的特洛伊木马 • 中断特洛伊木马创建的进程 • 修复特洛伊木马修改的系统文件 • 删除特洛伊木马留下的文件和应用程序 由于损害清除服务在后台自动运行，因此不需要对其进行配置。它运行时用户甚至没有察觉。但是，防毒墙网络版可能有时会通知用户重新启动终端以完成移除特洛伊木马的过程。
Web 信誉	Web 信誉技术可前瞻地保护公司网络内外的客户端计算机免受恶意和潜在危险的 Web 站点的危害。Web 信誉可断开感染链并防止下载恶意代码。 通过将防毒墙网络版与云安全智能防护服务器或趋势科技云安全智能防护网络集成来验证 Web 站点和页面的可信度。
防毒墙网络版防火墙	防毒墙网络版防火墙使用基于状态的检查和高性能的网络病毒扫描来保护网络上的客户端和服务器。 创建按应用程序、IP 地址、端口号或协议过滤连接的规则，然后将这些规则应用到不同的用户组中。
数据丢失防护	数据丢失防护可保护组织的数字资产免遭意外或故意泄露。数据丢失防护允许管理员： • 确定要保护的数字资产 • 创建用于限制或阻止通过常用传输通道（如电子邮件和外部设备）传输数字资产的策略 • 按照已建立的隐私标准强制执行合规
设备控制	设备控制能够控制对连接到计算机的外部存储设备与网络资源的访问。设备控制有助于防止数据丢失和泄露，与文件扫描组合使用时可帮助防御安全风险。
行为监控	行为监控会不断地监控客户端上的操作系统或已安装软件是否发生了异常修改。

防毒墙网络版服务器

防毒墙网络版服务器是所有客户端配置、安全风险日志和更新的中央存储库。

该服务器执行两个重要功能：

- 安装、监视和管理防毒墙网络版客户端
- 下载客户端所需的大多数组件。防毒墙网络版服务器从趋势科技 ActiveUpdate 服务器下载组件，然后将其分发到客户端。

注意

某些组件由云安全智能防护源下载。请参阅云安全智能防护源 第 4-5 页以了解详细信息。



图 1-1. 防毒墙网络版服务器的工作原理

防毒墙网络版服务器可提供服务器与防毒墙网络版客户端之间的实时、双向通信。从基于浏览器的 Web 控制台（管理员可从网络中的任何虚拟位置访问）管理客户端。服务器通过超文本传输协议 (HTTP) 与客户端（以及使用服务器的客户端）通信。

防毒墙网络版客户端

通过在每个终端上安装防毒墙网络版客户端可保护 Windows 计算机免受安全风险的危害。

防毒墙网络版客户端会向作为其安装源的父服务器报告。将客户端配置为通过使用客户端迁移程序工具向其他服务器报告。客户端将事件和状态信息实时发送到服务器。事件的示例包括病毒/恶意软件检测、客户端启动、客户端关闭、扫描启动和更新完成。

与趋势科技产品和服务集成

防毒墙网络版与下表中列出的趋势科技产品和服务集成。对于无缝集成，请确保产品运行的是所需或建议的版本。

表 1-4. 与防毒墙网络版集成的产品和服务

产品/服务	描述	版本
ActiveUpdate 服务器	提供防毒墙网络版客户端保护客户端免受安全威胁侵害所需的所有组件	不适用
云安全智能防护网络	向客户端提供文件信誉服务和 Web 信誉服务。 云安全智能防护网络由趋势科技托管。	不适用
独立型云安全智能防护服务器	提供与云安全智能防护网络提供的文件信誉服务和 Web 信誉服务相同的服务。 独立型云安全智能防护服务器旨在将服务局限在公司网络内以提高效率。 **注意** 集成型云安全智能防护服务器与防毒墙网络版服务器一起安装。它具有与独立型云安全智能防护服务器相同的功能，但是容量受限。	• 3.0

产品/服务	描述	版本
控制管理中心	软件管理解决方案使您能从一个中心位置控制防病毒和内容安全程序，而不用管该程序的所处的平台或物理位置如何。	• 6.0 SP3（建议） • 6.0 SP2 • 6.0 SP1 • 6.0 • 5.5 SP1
Deep Discovery Analyzer	Deep Discovery 提供了由定制沙盒和相关实时情报提供支持的网络范围内的监控，从而启用早期攻击检测和快速抑制，并提供定制安全更新以立即增强对进一步攻击的防护。	5.1 及更高版本

第 2 章

防毒墙网络版入门

本章介绍防毒墙网络版入门和初始配置设置。

主题包括：

- Web 控制台 第 2-2 页
- 控制台 第 2-5 页
- 服务器迁移工具 第 2-30 页
- Active Directory 集成 第 2-34 页
- 防毒墙网络版客户端树 第 2-38 页
- 防毒墙网络版域 第 2-50 页

Web 控制台

Web 控制台是监控整个企业网络中的防毒墙网络版的中心点。该控制台提供一组缺省设置和缺省值，您可以根据安全要求和规范来配置这些缺省设置和缺省值。Web 控制台使用标准的 Internet 技术，如 JavaScript、CGI、HTML 和 HTTPS。

注意

从 Web 控制台配置超时设置。请参阅 Web 控制台设置 第 13-53 页。

使用 Web 控制台执行以下操作：

- 管理在联网计算机上安装的客户端
- 将客户端聚集在逻辑域中以便同时配置和管理
- 设置扫描配置并在单个或多个联网计算机上启动手动扫描
- 配置关于网络中安全风险的通知并查看由客户端发送的日志
- 配置爆发条件和通知
- 通过配置角色和用户帐户将 Web 控制台管理任务委派给其他 防毒墙网络版管理员
- 确保客户端符合安全准则

注意

Web 控制台不支持处于 Windows UI 模式的 Windows 8、8.1、10 或 Windows Server 2012。

打开 Web 控制台的要求

从网络上具有下列资源的任何终端打开 Web 控制台：

- 300MHz Intel™ Pentium™ 处理器或同等处理器
- 128MB 内存
- 至少 30MB 的可用磁盘空间
- 在颜色为 256 或更高时，支持分辨率为 1024 x 768 的监视器
- Microsoft Internet Explorer™ 8.0 或更高版本

注意

防毒墙网络版仅支持查看 Web 控制台的 HTTPS 通信。

在 Web 浏览器上，根据防毒墙网络版服务器安装的类型在地址栏中键入以下内容之一：

表 2-1. 防毒墙网络版 Web 控制台 URL

安装类型	URL
缺省站点上有 SSL	https://<防毒墙网络版服务器 FQDN 或 IP 地址>/OfficeScan
虚拟站点上有 SSL	https://<防毒墙网络版服务器 FQDN 或 IP 地址>:<HTTP 端口号>/OfficeScan

注意

如果从先前版本的防毒墙网络版升级，则 Web 浏览器和代理服务器缓存文件可能妨碍防毒墙网络版 Web 控制台正常加载。在浏览器和位于防毒墙网络版服务器和用来访问 Web 控制台的终端之间的代理服务器上清除缓存内存。

登录帐户

在防毒墙网络版服务器安装期间，安装程序会创建一个 root 帐户并提示键入此帐户的密码。首次打开 Web 控制台时，键入 "root" 作为用户名和 root 帐户密码。如果忘记了密码，请与支持提供商联系以帮助重置密码。

定义用户角色并设置用户帐户以允许其他用户不使用 root 帐户访问 Web 控制台。用户登录到控制台时，他们可以使用您为他们设置的用户帐户。有关详细信息，请参阅基于角色的管理 第 13-3 页。

Web 控制台旗标

Web 控制台的旗标区域提供以下选项：



图 2-1. Web 控制台旗标区域

- **支持**：显示“趋势科技技术支持”Web 页面，其中您可以提交问题并查找有关趋势科技产品常见问题的答案
- **帮助**：显示联机帮助 Web 页面。
- **更多**
  - **威胁百科全书**：显示威胁百科全书 Web 站点，这是趋势科技恶意软件相关信息的存储库。趋势科技威胁专家会定期发布对恶意软件、垃圾邮件、恶意 URL 和漏洞的检测。威胁百科全书还说明了知名的 Web 攻击并提供了相关信息。
  - **与趋势科技联系**：显示趋势科技**与我们联系** Web 站点以及全球办事处的相关信息。
  - **关于**：提供了产品概述，检查组件版本详细信息的指导信息和支持情报系统的链接。

    有关详细信息，请参阅支持情报系统 第 16-2 页。
- **<帐户名称>**：单击帐户名称（例如，root）以修改帐户的详细信息，如密码
- **注销**：从 Web 控制台注销用户

控制台

打开防毒墙网络版 Web 控制台，或单击主菜单中的**控制台**时，将显示**控制台**。

每个 Web 控制台用户帐户都具有一个完全独立的控制台。对用户帐户的控制台所做的任何更改都不会影响其他用户帐户的控制台。

如果控制台包含防毒墙网络版客户端数据，显示的数据取决于用户帐户的客户端域权限。例如，如果授予某个用户帐户管理域 A 和 B 的权限，则该用户帐户的控制台将仅显示来自属于域 A 和 B 的客户端的数据。

有关用户帐户的详细信息，请参阅基于角色的管理 第 13-3 页。

控制台窗口包含以下内容：

- “产品使用授权状态”部分
- 小组件
- 选项卡

“产品使用授权状态”部分

此部分位于控制台的顶部，它显示防毒墙网络版使用授权的状态。

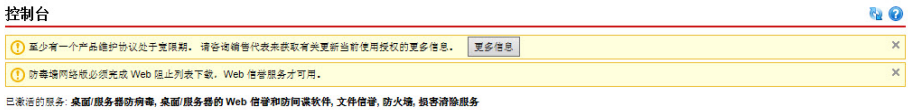


图 2-2. “产品使用授权状态”部分

以下实例中将显示关于使用授权状态的提醒信息：

- 如果您具有完全版使用授权：
  - 使用授权到期前 60 天

  - 在产品的宽限期内。宽限期的持续时间因地区而异。请通过趋势科技代表验证宽限期。
  - 当使用授权到期且宽限期已过时。在此期间，您将无法获得技术支持或无法执行组件更新。扫描引擎将仍然使用过期组件扫描计算机。这些过期组件可能不能完全保护您不受最新安全风险的侵扰。
- 如果您具有试用版使用授权：
  - 使用授权到期前 14 天
  - 当使用授权过期时。在此期间，防毒墙网络版将禁用组件更新、扫描和所有客户端功能组件。

如果已经获取激活码，请转至**管理** > **设置** > **产品使用授权**以续订使用授权。

产品信息栏

防毒墙网络版会在为管理员提供其他信息的**控制台**窗口顶部显示各种消息。

显示的信息包括：

- 防毒墙网络版可用的最新 Service Pack 或 Patch

> **注意**
>
> 单击**详细信息**可从趋势科技下载专区 (http://downloadcenter.trendmicro.com/index.php?regs=ch) 下载 Patch。

- 可用的新小组件
- 在协议临近有效期时显示的维护协议通知
- 评估模式通知
- 认证通知

注意

如果防毒墙网络版使用授权不是正版，会显示通知消息。如果没有获得正版的使用授权，防毒墙网络版会显示警告和停止执行更新。

选项卡和小组件

小组件是控制台的核心组件。小组件提供了有关各种安全相关事件的特定信息。通过某些小组件，您可以执行特定任务，如更新过期的组件。

小组件显示的信息来自：

- 防毒墙网络版 服务器和 客户端
- 插件解决方案及其客户端
- 趋势科技云安全智能防护网络

注意

启用云安全智能反馈可以显示来自云安全智能防护网络的数据。有关云安全智能反馈的详细信息，请参阅云安全智能反馈 第 13-58 页。

选项卡为小组件提供了容器。**控制台**最多支持 30 个选项卡。

使用选项卡

通过执行以下任务管理选项卡：

表 2-2. 选项卡任务

任务	步骤
添加新选项卡	1. 单击控制台顶部的添加图标。将显示一个新窗口。  2. 指定以下内容： • **标题**：选项卡的名称 • **布局**：从可用布局中进行选择 • **自动适应**：如果已选择具有多个框的布局（如“  ”）且每个框仅包含一个小组件，请启用自动适应。自动适应将调整小组件以适应框的大小。 3. 单击**保存**。
修改选项卡设置	1. 单击选项卡右上角的**选项卡设置**。将显示一个新窗口。  2. 修改选项卡名称、布局和自动适应设置。 3. 单击**保存**。
移动选项卡	使用拖放功能更改选项卡的位置。
删除选项卡	单击选项卡标题旁边的删除图标。  删除选项卡会删除选项卡中的所有小组件。

使用小组件

通过执行以下任务管理小组件：

表 2-3. 小组件任务

任务	步骤
播放选项卡幻灯片	单击**播放选项卡幻灯片**在选项卡视图之间进行切换。
添加新的小组件	1. 单击某个选项卡。 2. 单击选项卡右上角的**添加小组件**。将显示一个新窗口。 3. 选择要添加的小组件。有关可用小组件的列表，请参阅可用小组件 第 2-10 页。 • 单击窗口右上部分的显示图标 () 以在详细视图和摘要视图之间进行切换。 • 窗口的左侧是小组件类别。选择一个类别以缩小选择的范围。 • 使用窗口顶部的搜索文本框以搜索特定小组件。 4. 单击**添加**。
移动小组件	使用拖放功能将小组件移动到选项卡内的不同位置。
调整小组件的大小	通过将光标指向小组件的右边缘，然后向左或向右移动光标，可调整多列选项卡上的小组件的大小。
编辑小组件标题	1. 单击编辑图标 ()。将显示一个新窗口。 2. 键入新标题。 **注意** 对于某些小组件（如防毒墙网络版和插件混合），可以修改与小组件相关的项。 3. 单击**保存**。
刷新小组件数据	单击刷新图标 ()。
删除小组件	单击删除图标 ()。

预定义的选项卡和小组件

控制台附带一组预定义的选项卡和小组件。可以更名或删除这些选项卡和小组件。

表 2-4. 控制台中的缺省选项卡

选项卡	描述	小组件
防毒墙网络版	此选项卡包含的信息与先前版本的防毒墙网络版的**控制台**窗口中的信息相同。在此选项卡中，可以查看防毒墙网络版网络的总体安全风险防护。您还可以对需要立即干预的项目（例如爆发或过期的组件）采取处理措施。	• 防病毒客户端连接小组件 第 2-14 页 • 安全风险检测小组件 第 2-18 页 • 爆发小组件 第 2-18 页 • 客户端更新小组件 第 2-20 页
防毒墙网络版和插件	此选项卡显示运行防毒墙网络版客户端和插件解决方案的客户端。使用此选项卡评估客户端的总体安全状态。	防毒墙网络版与插件混合 Web 应用程序小组件 第 2-21 页
云安全智能防护网络	此选项卡包含的信息来自趋势科技云安全智能防护网络，后者向防毒墙网络版客户端提供文件信誉服务和 Web 信誉服务。	• Web 信誉排名居前的威胁源小组件 第 2-28 页 • Web 信誉排名居前的受威胁用户小组件 第 2-29 页 • 文件信誉威胁地图小组件 第 2-30 页

可用小组件

此发行版中提供以下小组件：

表 2-5. 可用小组件

小组件名称	可用性
客户端-服务器连接	开箱即用 有关详细信息，请参阅客户端-服务器连接小组件 第 2-13 页。
防病毒客户端连接	开箱即用 有关详细信息，请参阅防病毒客户端连接小组件 第 2-14 页。
安全风险检测	开箱即用 有关详细信息，请参阅安全风险检测小组件 第 2-18 页。
爆发	开箱即用 有关详细信息，请参阅爆发小组件 第 2-18 页。
客户端更新	开箱即用 有关详细信息，请参阅客户端更新小组件 第 2-20 页。
防毒墙网络版与插件混合 Web 应用程序	开箱即用，但仅显示防毒墙网络版客户端中的数据 激活以下每个插件解决方案后，可以使用这些解决方案中的数据： • 入侵防御防火墙 • 趋势科技虚拟桌面支持 有关详细信息，请参阅防毒墙网络版与插件混合 Web 应用程序小组件 第 2-21 页。
最常见的数据丢失防护事件	激活防毒墙网络版数据保护后可用 有关详细信息，请参阅最常见的数据丢失防护事件小组件 第 2-22 页。
一段时间内的数据丢失防护事件	激活防毒墙网络版数据保护后可用 有关详细信息，请参阅一段时间内的数据丢失防护事件小组件 第 2-24 页。

小组件名称	可用性
Web 信誉排名居前的威胁源	开箱即用 有关详细信息，请参阅 Web 信誉排名居前的威胁源小组件 第 2-28 页。
Web 信誉排名居前的受威胁用户	开箱即用 有关详细信息，请参阅 Web 信誉排名居前的受威胁用户小组件 第 2-29 页。
文件信誉威胁地图	开箱即用 有关详细信息，请参阅文件信誉威胁地图小组件 第 2-30 页。
C&C 回呼事件	开箱即用 有关详细信息，请参阅 C&C 回呼事件小组件 第 2-25 页。
IDF – 警报状态	激活入侵防御防火墙后可用。有关这些小组件的详细信息，请参阅 IDF 文档。
IDF – 计算机状态	
IDF – 网络事件历史	
IDF – 系统事件历史	

客户端-服务器连接小组件

客户端-服务器连接小组件显示所有客户端与防毒墙网络版服务器的连接状态。数据以表和饼图的形式显示。可以通过单击显示图标 () 在表和饼图之间切换。



图 2-3. 显示表的客户端-服务器连接小组件

防病毒客户端连接小组件

防病毒客户端连接小组件显示防病毒客户端与防毒墙网络版服务器的连接状态。数据以表和饼图的形式显示。可以通过单击显示图标 ( ) 在表和饼图之间切换。



图 2-4. 显示表的防病毒客户端连接小组件

以表形式显示的防病毒客户端连接小组件

表按扫描方法划分客户端。

如果特定状态的客户端数量大于或等于 1，则可以单击该数量查看客户端树中的客户端。可以在这些客户端上启动任务或更改其设置。

要仅显示使用特定扫描方法的客户端，请单击**全部**，然后选择扫描方法。



图 2-5. 传统扫描客户端的连接状态



图 2-6. 云安全扫描客户端的连接状态

如果选择了**云安全扫描**：

- 表按与云安全智能防护服务器的连接状态划分联机云安全客户端。

注意

仅联机客户端可以报告其与云安全智能防护服务器的连接状态。

如果客户端已从云安全智能防护服务器断开连接，则通过执行防毒墙网络版客户端图标中所指出问题的解决方案 第 14-36 页中的步骤恢复连接。

- 每台云安全智能防护服务器是一个可单击的 URL，单击后可启动服务器控制台。
- 如果有多台云安全智能防护服务器，请单击**更多**。将打开一个新窗口，其中显示所有云安全智能防护服务器。



图 2-7. 云安全智能防护服务器列表

在此窗口中，可以：

- 查看客户端连接到的所有云安全智能防护服务器和连接到每台服务器的客户端数。单击该数字打开可在其中管理客户端设置的客户端树。
- 通过单击服务器的链接启动服务器的控制台

以饼图形式显示的防病毒客户端连接小组件

饼图仅显示每个状态的客户端的数量，但不按扫描方法划分客户端。单击一个状态可将其与饼图的剩余部分相分隔或将其重新连接到饼图的剩余部分。

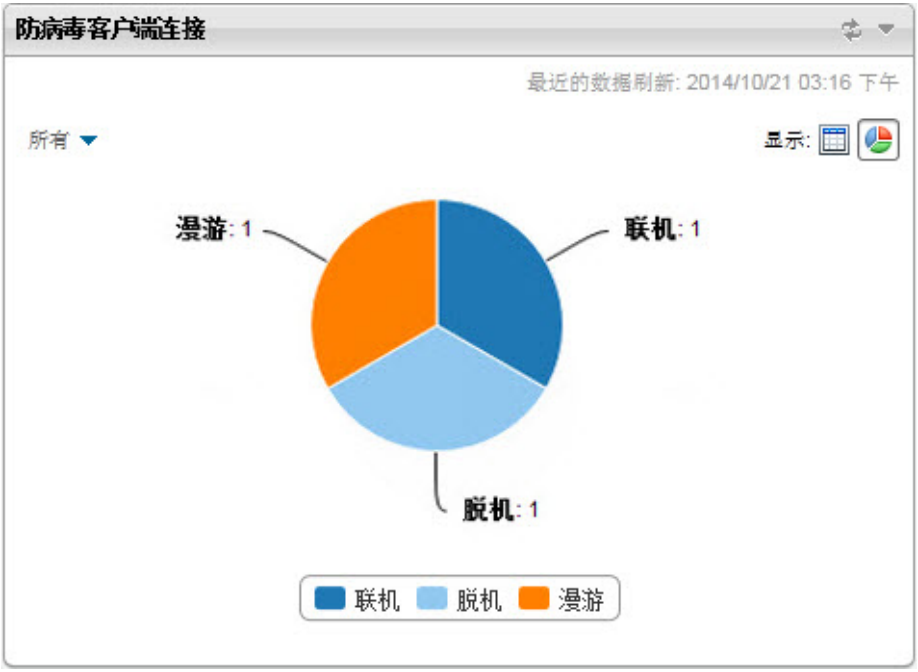


图 2-8. 显示饼图的防病毒客户端连接小组件

安全风险检测小组件

安全风险检测小组件显示安全风险和受感染终端的数量。



图 2-9. 安全风险检测小组件

如果受感染终端的数量大于或等于 1，则可以单击该数量查看客户端树中的受感染终端。可以在这些终端的防毒墙网络版客户端上启动任务或更改其设置。

爆发小组件

爆发小组件提供任何当前安全风险爆发的状态和上次爆发警报。

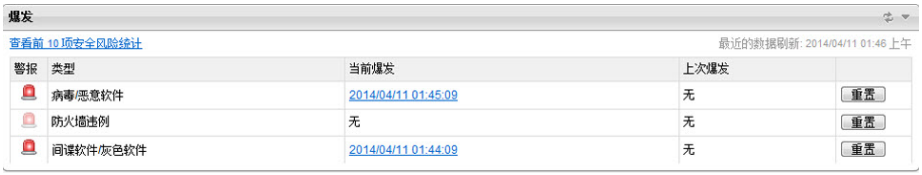


图 2-10. 爆发小组件

在此小组件中，可以：

- 单击警报的日期/时间链接以查看爆发详细信息。
- 当防毒墙网络版检测到爆发时，它会重置爆发警报信息的状态并立即强制执行爆发阻止措施。有关执行爆发阻止措施的详细信息，请参阅爆发阻止策略 第 7-99 页。
- 单击**查看前 10 项安全风险统计**，查看最流行的安全风险、安全风险数量最多的计算机和主要的感染源。将显示一个新窗口。

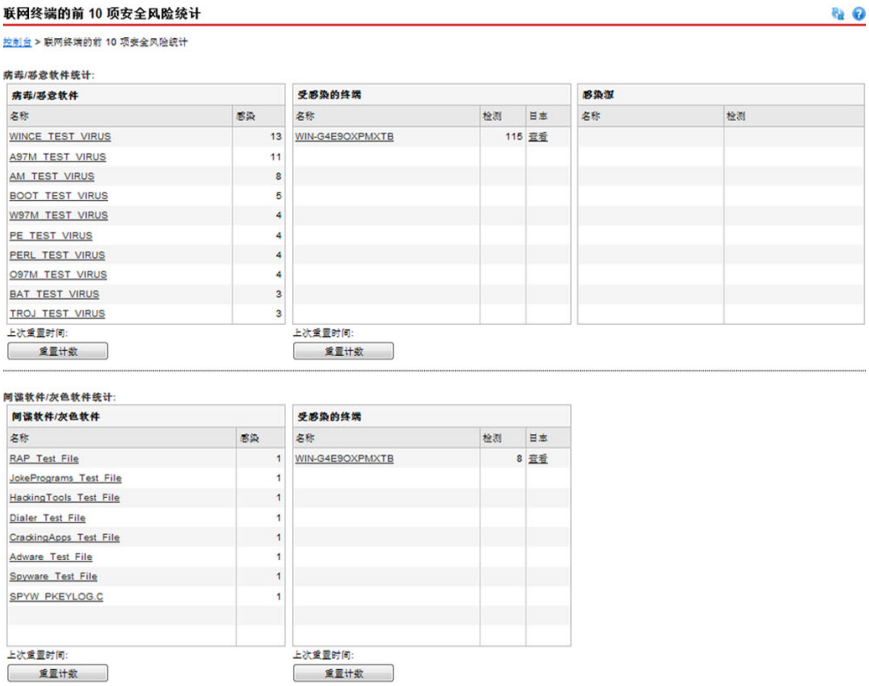


图 2-11. 联网终端的前 10 项安全风险统计窗口

在**前 10 项安全风险统计**窗口中，可以：

- 单击安全风险名以查看该安全风险的详细信息。
- 单击终端名称以查看特定终端的总体状态。

- 单击对应于终端名称的**查看**以查看该终端的安全风险日志。
- 单击**重置计数**以重置每张表的统计信息。

客户端更新小组件

客户端更新小组件显示可保护联网终端免遭安全风险侵害的组件和程序。

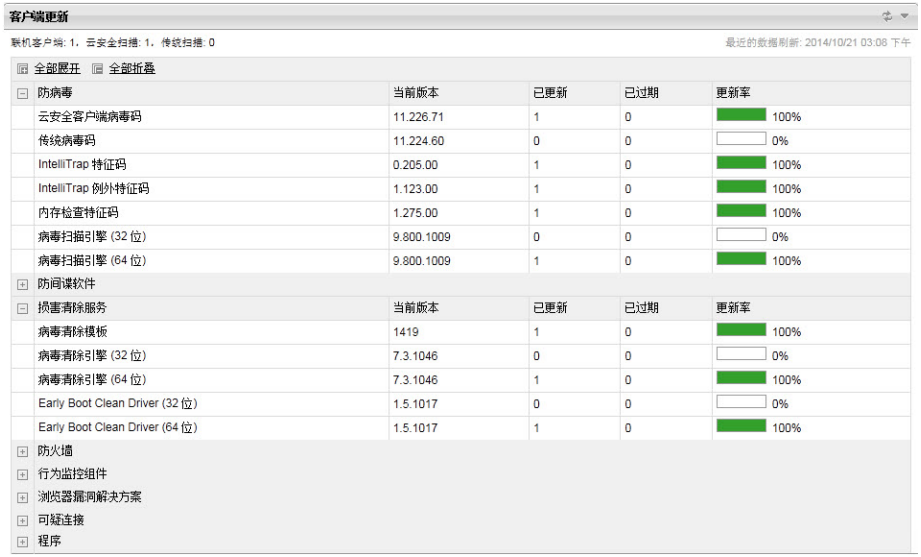


图 2-12. 客户端更新小组件

在此小组件中，可以：

- 查看每个组件的当前版本。
- 在**已过期**列下，查看带有过期组件的客户端数。如果存在需要更新的客户端，则单击数字链接开始更新。
- 对每个程序，通过单击对应于该程序的编号链接查看尚未升级的客户端。

防毒墙网络版与插件混合 Web 应用程序小组件

防毒墙网络版与插件混合 Web 应用程序小组件将防毒墙网络版客户端中的数据和安装的插件程序中的数据相组合，然后在客户端树中显示这些数据。此小组件可帮助快速评估客户端上的保护范围并减少管理各个插件程序所需的开销。

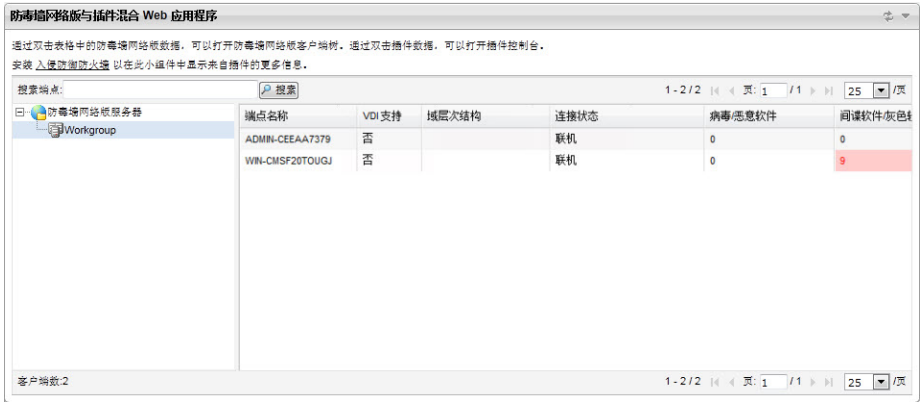


图 2-13. 防毒墙网络版与插件混合 Web 应用程序小组件

此小组件显示以下插件程序的数据：

- 入侵防御防火墙
- 趋势科技虚拟桌面支持

必须激活这些插件程序，混合小组件才能显示数据。如果有更新版本，则升级插件程序。

在此小组件中，可以：

- 选择显示在客户端树中的列。单击小组件右上角的刷新图标（ ），然后在显示的窗口中选择列。

表 2-6. 防毒墙网络版与插件混合 Web 应用程序列

列名称	描述
计算机名称	终端名称 此列始终可用，无法移除。
域层次结构	防毒墙网络版客户端树中的终端域
连接状态	防毒墙网络版客户端与其父防毒墙网络版服务器的连接
病毒/恶意软件	防毒墙网络版客户端检测到的病毒和恶意软件数
间谍软件/灰色软件	防毒墙网络版客户端检测到的间谍软件和灰色软件数
VDI 支持	表明终端是否为虚拟机
IDF 安全配置文件	有关这些列和列显示的数据的详细信息，请参阅 IDF 文档。
IDF 防火墙	
IDF 状态	
IDF DPI	

- 双击表中的数据。如果双击防毒墙网络版数据，将显示防毒墙网络版客户端树。如果双击插件程序数据（**VDI 支持**列中的数据除外），将显示插件程序的主窗口。
- 使用搜索功能查找单个终端。可以键入完整或部分主机名。

最常见的数据丢失防护事件小组件

仅在激活防毒墙网络版数据保护后此小组件才可用。

此小组件显示数字资产传输次数，不管处理措施是阻止还是不予处理。

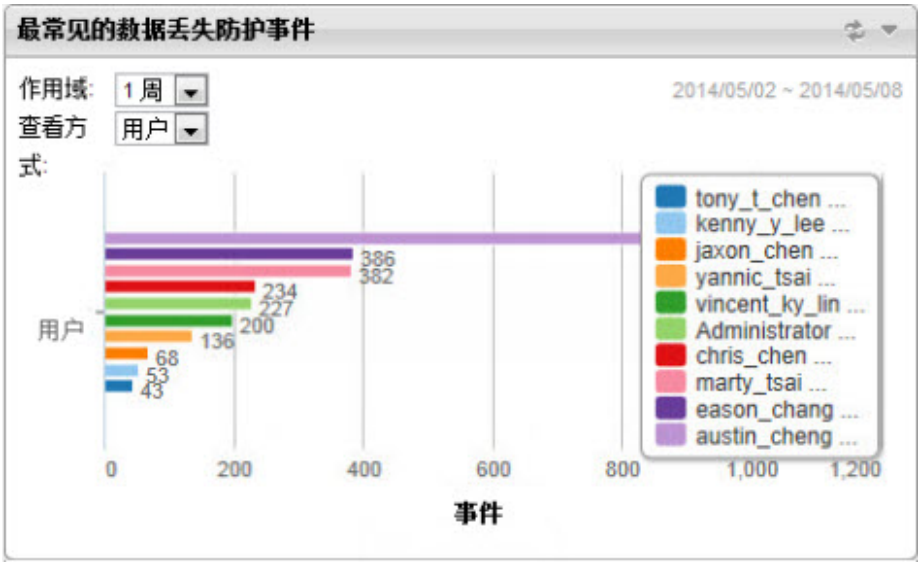


图 2-14. 最常见的数据丢失防护事件小组件

查看数据：

1. 选择检测的时间段。从以下选项中进行选择：
   - **今天**：过去 24 小时（包括当前这一小时）的检测数据
   - **1 周**：最近 7 天（包括当前这一天）的检测数据
   - **2 周**：最近 14 天（包括当前这一天）的检测数据
   - **1 月**：最近 30 天（包括当前这一天）的检测数据
2. 选择时间段后，从以下选项中进行选择：
   - **用户**：传输数字资产次数最多的用户
   - **通道**：传输数字资产最常用的通道

- **模板**：触发检测次数最多的数字资产模板
- **计算机**：传输数字资产次数最多的计算机

注意

此小组件最多显示 10 个用户、通道、模板或计算机。

一段时间内的数据丢失防护事件小组件

仅在激活防毒墙网络版数据保护后此小组件才可用。

此小组件以曲线形式显示一段时间内的数字资产传输次数。传输次数包括那些阻止的或不予处理（允许）的传输次数。

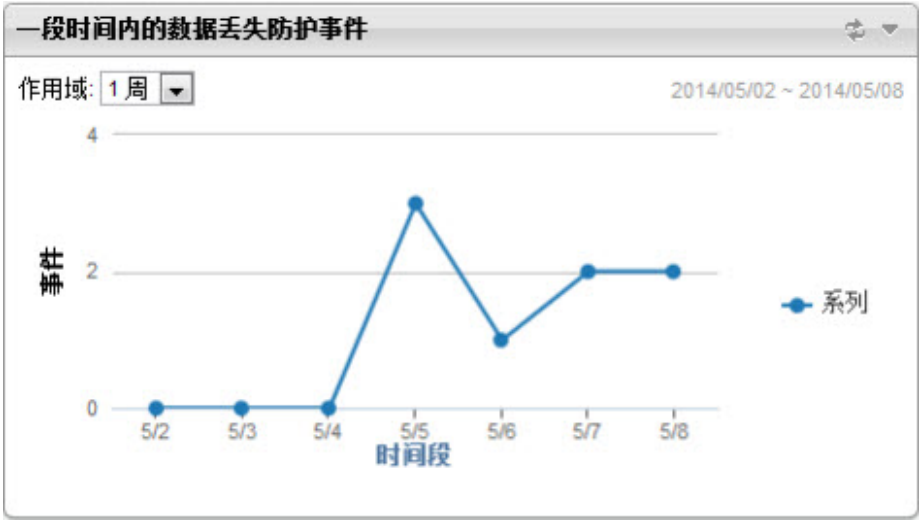


图 2-15. 一段时间内的数据丢失防护事件小组件

要查看数据，请选择检测的时间段。从以下选项中进行选择：

- **今天**：过去 24 小时（包括当前这一小时）的检测数据

- **1 周**：最近 7 天（包括当前这一天）的检测数据
- **2 周**：最近 14 天（包括当前这一天）的检测数据
- **1 月**：最近 30 天（包括当前这一天）的检测数据

C&C 回呼事件小组件

C&C 回呼事件小组件会显示所有 C&C 回呼事件信息，其中包括攻击的目标和源回呼地址。

管理员可以选择查看特定 C&C 服务器列表中的 C&C 回呼信息。要选择列表来源（全局情报或沙盒虚拟平台），请单击编辑图标 (⚙)，然后从 **C&C 列表来源**下拉列表中选择列表。

通过选择以下内容查看 C&C 回呼数据：

- **遭受危害的主机**：显示每个目标终端的最新 C&C 信息



图 2-16. 显示目标信息的 C&C 回呼事件小组件

表 2-7. 遭受危害的主机信息

列	描述
遭受危害的主机	C&C 攻击所针对的终端的名称
回呼地址	终端尝试联系的回呼地址数

列	描述
最新回呼地址	终端上次尝试联系的回呼地址
回呼尝试	目标终端尝试联系回呼地址的次数 **注意** 单击超链接打开 **C&C 回呼日志**窗口并查看更多详细信息。

- **回呼地址**：显示每个 C&C 回呼地址的最新 C&C 信息



图 2-17. 显示回呼地址信息的 C&C 回呼事件小组件

表 2-8. C&C 地址信息

列	描述
回呼地址	源自网络的 C&C 回呼地址
C&C 风险等级	由全局情报或沙盒虚拟平台列表确定的回呼地址的风险等级
遭受危害的主机	回呼地址的目标终端的数量

列	描述
最近遭受危害的主机	最后一次尝试与 C&C 回呼地址联系的终端的名称
回呼尝试	尝试回呼来自网络的地址的次数 **注意** 单击超链接打开 **C&C 回呼日志**窗口并查看更多详细信息。

Web 信誉排名居前的威胁源小组件

此小组件显示 Web 信誉服务进行的安全威胁检测的总数。该信息按地理位置显示在世界地图中。有关使用此小组件的帮助，请单击小组件顶部的帮助按钮（）。



图 2-18. Web 信誉排名居前的威胁源小组件

Web 信誉排名居前的受威胁用户小组件

此小组件显示由 Web 信誉服务检测到的受恶意 URL 影响的用户数量。该信息按地理位置显示在世界地图中。有关使用此小组件的帮助，请单击小组件顶部的帮助按钮（ ）。



图 2-19. Web 信誉排名居前的受威胁用户小组件

文件信誉威胁地图小组件

此小组件显示文件信誉服务进行的安全威胁检测的总数。该信息按地理位置显示在世界地图中。有关使用此小组件的帮助，请单击小组件顶部的帮助按钮（）。



图 2-20. 文件信誉威胁地图小组件

服务器迁移工具

防毒墙网络版提供了服务器迁移工具，管理员可使用该工具将防毒墙网络版设置从先前的防毒墙网络版版本复制到当前版本。服务器迁移工具可迁移以下设置：

功能	迁移的设置
客户端管理	• 手动扫描设置* • 预设扫描设置* • 实时扫描设置* • 立即扫描设置* • Web 信誉设置* • 行为监控设置* • 设备控制设置* • 数据丢失防护设置* • 权限和其他设置* • 其他服务设置* • 间谍软件/灰色软件允许列表* **注意** • 服务器迁移工具不会迁移手动扫描、预设扫描、实时扫描和立即扫描的备份目录。 • 设置同时保留根级和域级配置。
客户端分组	所有设置 **注意** 首次与 Active Directory 同步后将显示 Active Directory 域结构。
全局客户端设置	所有设置
终端位置	• 位置感知设置 • 网关 IP 地址和 MAC 列表
数据丢失防护	• 数据标识符 • 模板

功能	迁移的设置
防火墙	• 策略 • 概要文件
日志维护	所有设置
客户端更新源	• 客户端更新源 • 定制的更新源列表
云安全智能防护源	定制的云安全智能防护源列表
通知	• 常规通知设置 • 管理员通知设置 • 爆发通知设置 • 客户端通知设置
代理服务器	所有设置
非活动客户端	所有设置
隔离管理器	所有设置
Web 控制台	所有设置
ofcscan.ini 设置	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]：所有设置
ofcserver.ini 设置	[INI_SERVER_DISK_THRESHOLD]：所有设置

注意

- 该工具不会备份防毒墙网络版服务器的防毒墙网络版客户端列表；仅会备份域结构。
- 防毒墙网络版客户端仅迁移旧版防毒墙网络版客户端服务器上可用的功能。对于旧版服务器上不可用的功能，防毒墙网络版客户端将应用缺省设置。

使用服务器迁移工具

注意

此版本的防毒墙网络版支持从防毒墙网络版 10.0 及更高版本进行迁移。

旧版的防毒墙网络版可能不包含最新版本中提供的全部设置。对于防毒墙网络版服务器的先前版本中未迁移的所有功能，防毒墙网络版将自动应用缺省设置。

过程

1. 在防毒墙网络版 11.0 SP1 服务器计算机上，导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\ServerMigrationTool。
2. 将服务器迁移工具复制到源防毒墙网络版服务器计算机上。

   重要信息

   必须在源防毒墙网络版服务器版本上使用防毒墙网络版 11.0 SP1 服务器迁移工具，确保所有数据均已针对新的目标服务器正确进行了格式化。防毒墙网络版 11.0 SP1 与服务器迁移工具的旧版本不兼容。

3. 双击 ServerMigrationTool.exe 启动服务器迁移工具。

   此时将打开服务器迁移工具。

4. 从源防毒墙网络版服务器导出设置：

   a. 使用**浏览**按钮指定目标文件夹。

      注意

      导出包的缺省名称为 OsceMigrate.zip。

   b. 单击**导出**。

      将显示确认消息。

   c. 将导出包复制到目标防毒墙网络版服务器。

5. 将设置导入目标防毒墙网络版服务器：

a. 使用**浏览**按钮查找导出包。

b. 单击**导入**。

将显示警告消息。

c. 单击**是**继续。

将显示确认消息。

6. 验证服务器是否包含先前版本的防毒墙网络版的所有设置。

7. 将旧版防毒墙网络版客户端移动到新服务器。

有关移动防毒墙网络版客户端的详细信息，请参阅将防毒墙网络版客户端移动到其他域或防毒墙网络版服务器 第 2-58 页或客户端迁移程序 第 14-22 页。

Active Directory 集成

将防毒墙网络版与 Microsoft™ Active Directory™ 结构集成，以更高效地管理防毒墙网络版客户端，使用 Active Directory 帐户分配 Web 控制台权限，并确定哪些客户端未安装安全软件。网络域中的所有用户都具有对防毒墙网络版控制台的安全访问权限。也可以配置限制特定用户的访问，即使这些用户在其他域中。认证过程和加密密钥为用户提供凭证验证。

Active Directory 集成允许您充分利用下列功能：

- **基于角色的管理**：通过使用用户的 Active Directory 帐户授予其对产品控制台的访问权限，将特定管理职责分配给用户。有关详细信息，请参阅基于角色的管理 第 13-3 页。
- **定制客户端组**：使用 Active Directory 或 IP 地址手动分组客户端并将它们映射到防毒墙网络版 客户端树中的域。有关详细信息，请参阅自动客户端分组 第 2-52 页。
- **不受管理的终端**：确保不受防毒墙网络版服务器管理的网络中的客户端符合贵公司的安全准则。有关详细信息，请参阅不受管理的终端的安全合规 第 14-62 页。

手动或定期将 Active Directory 结构与防毒墙网络版服务器同步以确保数据一致性。有关详细信息，请参阅将数据与 Active Directory 域同步 第 2-36 页。

将 Active Directory 与防毒墙网络版集成

过程

1. 转至**管理** > **Active Directory** > **Active Directory 集成**。
2. 在 **Active Directory 域**下，指定 Active Directory 域名。
3. 指定防毒墙网络版服务器在将数据与指定的 Active Directory 域同步时使用的凭证。如果服务器不在域内，则必须输入凭证。在其他情况下，这些凭证是可选的。请确保这些凭证没有过期，否则服务器将无法同步数据。
   a. 单击**指定域凭证**。
   b. 在打开的弹出窗口中，键入用户名和密码。可以使用以下任一格式指定用户名：
      - `域\用户名`
      - `用户名@域`
   c. 单击**保存**。
4. 单击 (+) 按钮添加更多域。如有需要，为任何添加的域指定域凭证。
5. 单击 (-) 按钮以删除域。
6. 如果指定了域凭证，请指定加密设置。作为一项安全措施，防毒墙网络版会在将指定的域凭证保存到数据库之前对它们进行加密。当防毒墙网络版将数据与任何指定的域同步时，它将使用加密密钥来解密域凭证。
   a. 转至**域凭证的加密设置**部分。
   b. 键入不超过 128 个字符的加密密钥。
   c. 指定要在其中保存加密密钥的文件。可以选择常见的文件格式，如 .txt。键入文件的完整路径和名称，如 C:\AD_Encryption\EncryptionKey.txt。

警告!

如果该文件已被删除或文件路径发生更改，防毒墙网络版无法将数据与所有指定的域同步。

7. 单击下列操作之一：
   - **保存**：仅保存设置。因为同步数据可能会耗费大量的网络资源，因此可以选择仅保存设置并稍后同步，如在非重要营业时间同步。
   - **保存并同步**：保存设置并将数据与 Active Directory 域同步。
8. 预设定期同步。有关详细信息，请参阅将数据与 Active Directory 域同步 第 2-36 页。

将数据与 Active Directory 域同步

定期将数据与 Active Directory 域同步以使防毒墙网络版客户端树结构保持最新，并查询不受管理的客户端。

手动将数据与 Active Directory 域同步

过程

1. 转至**管理** > **Active Directory** > **Active Directory 集成**。
2. 验证域凭证和加密设置是否未更改。
3. 单击**保存并同步**。

自动将数据与 Active Directory 域同步

过程

1. 转至**管理** > **Active Directory** > **预设同步**。
2. 选择**启用预设 Active Directory 同步**。
3. 指定同步预设。

   注意

   对每日、每周和每月同步而言，此时间段即防毒墙网络版将 Active Directory 与防毒墙网络版服务器同步的小时数。

4. 单击**保存**。

防毒墙网络版客户端树

防毒墙网络版客户端树显示服务器当前管理的所有客户端（分组为域）。将客户端分组为域，可以同时对所有域成员配置、管理和应用相同的配置。

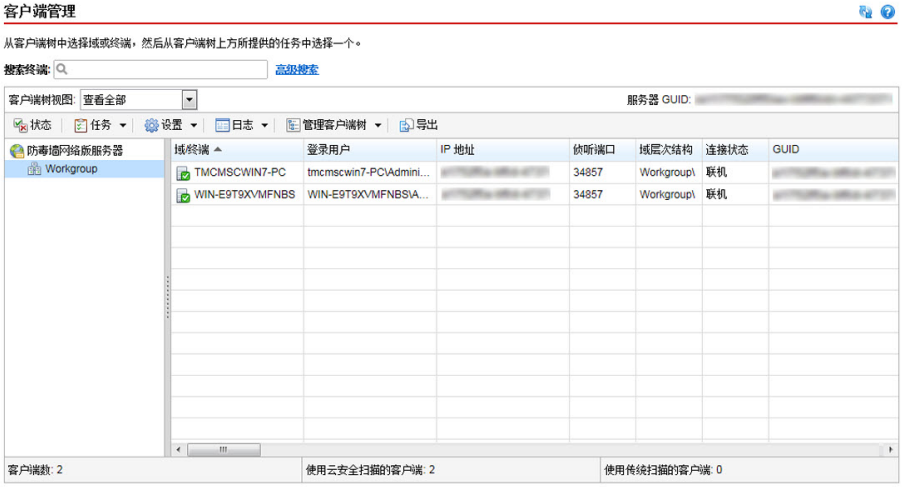


图 2-21. 防毒墙网络版 客户端树

客户端树图标

防毒墙网络版客户端树图标提供视觉提示，指出终端类型和防毒墙网络版管理的防毒墙网络版客户端的状态。

表 2-9. 防毒墙网络版客户端树图标

图标	描述
	域

图标	描述
	根
	更新代理
	传统扫描客户端
	云安全扫描可用的防毒墙网络版客户端
	云安全扫描不可用的防毒墙网络版客户端
	云安全扫描可用的更新代理
	云安全扫描不可用的更新代理

客户端树常规任务

下面是客户端树显示时可以执行的常规任务：

过程

- 单击根域图标 () 以选择所有域和客户端。当选择根域图标然后选择客户端树上的某个任务时，将显示用于配置设置的窗口。在该窗口上，从下列常规选项作出选择：
  - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
  - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

- 选择多个相邻的域或客户端：
  - 在右面板中，选择第一个域，按住 SHIFT 键，然后单击范围内的最后一个域或客户端。
- 要选择一系列间断的域或客户端，则在右面板中，按住 CTRL 键，然后单击您想要选择的域或客户端。
- 通过在**搜索终端**文本框中指定客户端名称来搜索要管理的任何客户端。

  结果列表在客户端树中显示。要获取更多搜索选项，请单击**高级搜索**。

  注意

  搜索特定客户端时不能指定 IPv6 或 IPv4 地址。使用“高级搜索”可根据 IPv4 或 IPv6 地址进行搜索。有关详细信息，请参阅高级搜索选项 第 2-41 页。

- 选择域后，客户端树表将展开以显示属于该域的客户端和包含每个客户端相关信息的所有列。要仅查看一组相关的列，请在客户端树视图中选择一项。
  - **查看全部**：显示所有列
  - **更新视图**：显示所有组件和程序
  - **防病毒视图**：显示防病毒组件
  - **防间谍软件视图**：显示防间谍软件组件
  - **数据保护视图**：显示客户端上数据保护模块的状态
  - **防火墙视图**：显示防火墙组件
  - **云安全智能防护视图**：显示客户端（传统扫描或云安全扫描）和云安全智能防护组件使用的扫描方法
  - **更新代理视图**：显示由防毒墙网络版服务器管理的所有更新代理的信息
- 通过单击列名称根据列信息对客户端进行排序。
- 通过单击刷新图标 ( ) 刷新客户端树。

- 查看客户端树下的客户端统计，如客户端总数、云安全客户端数和传统扫描客户端数。

高级搜索选项

基于以下条件搜索客户端：

过程

- **基本条件**：包括关于终端的基本信息，如 IP 地址、操作系统、域、MAC 地址、扫描方法和 Web 信誉状态
  - 按 IPv4 段搜索要求 IP 地址的一部分以第一个八位组开始。搜索将返回 IP 地址包含上述条目的所有终端。例如，键入 10.5 将返回 IP 地址范围从 10.5.0.0 到 10.5.255.255 的所有计算机。
  - 按 IPv6 地址范围搜索要求输入前缀和长度。
  - 按 MAC 地址搜索要求输入用十六进制计数法表示的 MAC 地址范围，例如，000A1B123C12。
- **组件版本**：选中组件名称旁边的复选框，通过选择**早于**或**早于并包括**来缩小条件，然后键入版本号。缺省显示当前版本号。
- **状态**：包括客户端设置
- 指定搜索条件后单击**搜索**。满足条件的终端名称列表将显示在客户端树中。

客户端树特定任务

在 Web 控制台上访问某些窗口时，将显示客户端树。客户端树上的菜单项特定于已访问过的窗口。这些菜单项允许执行特定任务，如配置客户端设置或启动客户端任务。要执行其中任何一项任务，请首先选择该任务目标，然后选择菜单项。

以下窗口将显示客户端树：

- 客户端管理窗口 第 2-42 页
- 爆发阻止窗口 第 2-45 页
- 客户端选择窗口 第 2-46 页
- 还原窗口 第 2-47 页
- 安全风险日志窗口 第 2-48 页

客户端管理窗口

要查看此窗口，请转至**客户端** > **客户端管理**。

管理**客户端管理**窗口上的常规客户端设置并查看特定客户端的相关状态信息（例如，**登录用户**、**IP 地址**和**连接状态**）。

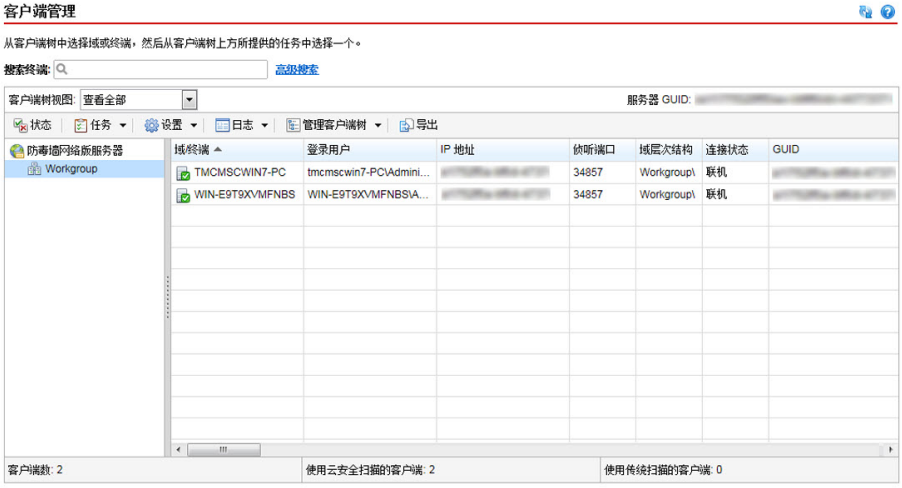


图 2-22. 客户端管理窗口

下表列出了可以执行的任务：

表 2-10. 客户端管理任务

菜单按钮	任务
状态	查看客户端详细信息。有关详细信息，请参阅查看防毒墙网络版客户端信息 第 14-49 页。
任务	• 在客户端计算机上运行立即扫描。有关详细信息，请参阅启动立即扫描 第 7-21 页。 • 卸载客户端。有关详细信息，请参阅从 Web 控制台卸载防毒墙网络版客户端 第 5-64 页。 • 恢复可疑文件检测。有关详细信息，请参阅恢复隔离文件 第 7-37 页。 • 恢复间谍软件/灰色软件组件。有关详细信息，请参阅恢复间谍软件/灰色软件 第 7-45 页。

菜单按钮	任务
设置	• 配置扫描设置。有关详细信息，请参阅以下主题： • 扫描方法类型 第 7-7 页 • 手动扫描 第 7-15 页 • 实时扫描 第 7-12 页 • 预设扫描 第 7-17 页 • 立即扫描 第 7-19 页 • 配置 Web 信誉设置。有关详细信息，请参阅 Web 信誉策略 第 11-4 页。 • 配置可疑连接设置。有关详细信息，请参阅配置可疑连接设置 第 11-14 页。 • 配置行为监控设置。有关详细信息，请参阅行为监控 第 8-2 页。 • 配置设备控制设置。有关详细信息，请参阅设备控制 第 9-2 页。 • 配置数据丢失防护策略。有关详细信息，请参阅数据丢失防护策略配置 第 10-43 页。 • 将客户端指定为更新代理。有关详细信息，请参阅更新代理配置 第 6-50 页。 • 配置客户端权限和其他设置。有关详细信息，请参阅配置客户端权限和其他设置 第 14-81 页。 • 启用或禁用防毒墙网络版客户端服务。有关详细信息，请参阅防毒墙网络版客户端服务 第 14-6 页。 • 配置间谍软件/灰色软件允许列表。有关详细信息，请参阅间谍软件/灰色软件允许列表 第 7-43 页。 • 配置可信程序列表。有关详细信息，请参阅配置可信程序列表 第 7-46 页。 • 导入和导出客户端设置。有关详细信息，请参阅导入和导出客户端设置 第 14-49 页。

菜单按钮	任务
日志	查看下列日志： • 病毒/恶意软件日志（有关详细信息，请参阅查看病毒/恶意软件日志 第 7-81 页） • 间谍软件/灰色软件日志（有关详细信息，请参阅查看间谍软件/灰色软件日志 第 7-88 页） • 防火墙日志（有关详细信息，请参阅防火墙日志 第 12-26 页） • Web 信誉日志（有关详细信息，请参阅 Web 威胁日志 第 11-23 页） • 可疑连接日志（有关详细信息，请参阅查看可疑连接日志 第 11-25 页） • 可疑文件日志（有关详细信息，请参阅查看可疑文件日志 第 7-92 页） • C&C 回呼日志（有关详细信息，请参阅查看 C&C 回呼日志 第 11-24 页。） • 行为监控日志（有关详细信息，请参阅行为监控日志 第 8-13 页） • 设备控制日志（有关详细信息，请参阅设备控制日志 第 9-16 页） • DLP 日志（有关详细信息，请参阅数据丢失防护日志 第 10-52 页） • 扫描操作日志（有关详细信息，请参阅查看扫描操作日志 第 7-93 页） 删除日志。有关详细信息，请参阅日志管理 第 13-35 页。
管理客户端树	管理客户端树。有关详细信息，请参阅客户端分组任务 第 2-56 页。
导出	将客户端列表导出为逗号分隔值 (.csv) 文件。

爆发阻止窗口

要查看此窗口，请转至**客户端** > **爆发阻止**。

在“爆发阻止”窗口中指定并激活**爆发阻止**设置。有关详细信息，请参阅配置安全风险爆发阻止 第 7-98 页。

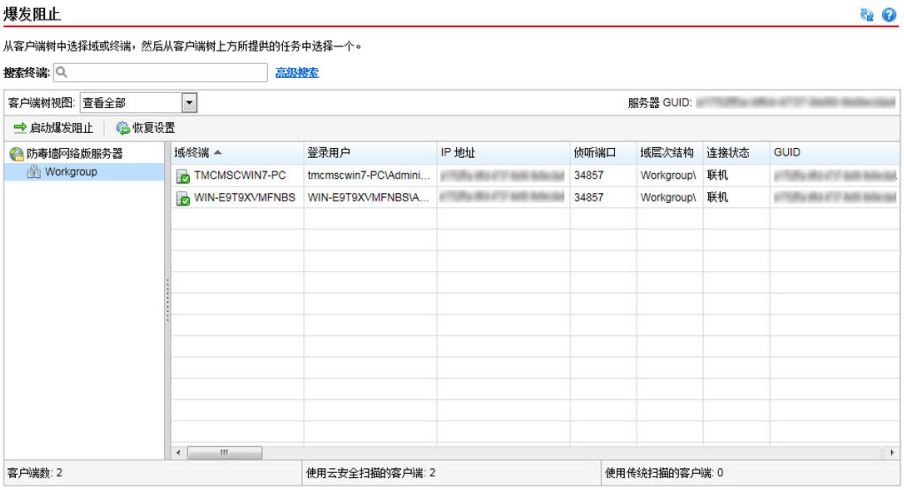


图 2-23. 爆发阻止窗口

客户端选择窗口

要查看此窗口，请转至**更新** > **客户端** > **手动更新**。选择**手动选择客户端**，然后单击**选择**。

在**客户端选择**窗口中启动手动更新。有关详细信息，请参阅防毒墙网络版客户端手动更新 第 6-40 页。

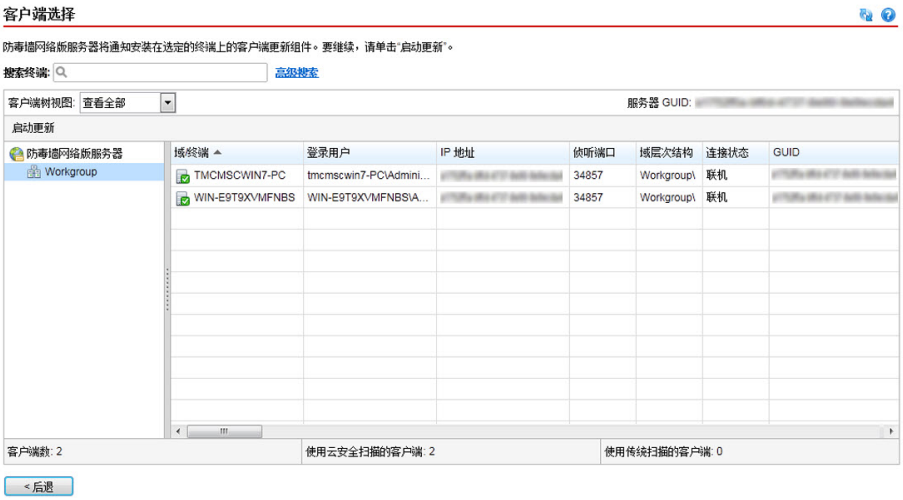


图 2-24. 客户端选择窗口

还原窗口

要查看此窗口，请转至**更新** > **还原**。单击**与服务器同步**。

在**还原**窗口中还原客户端组件。有关详细信息，请参阅还原防毒墙网络版客户端的组件 第 6-47 页。

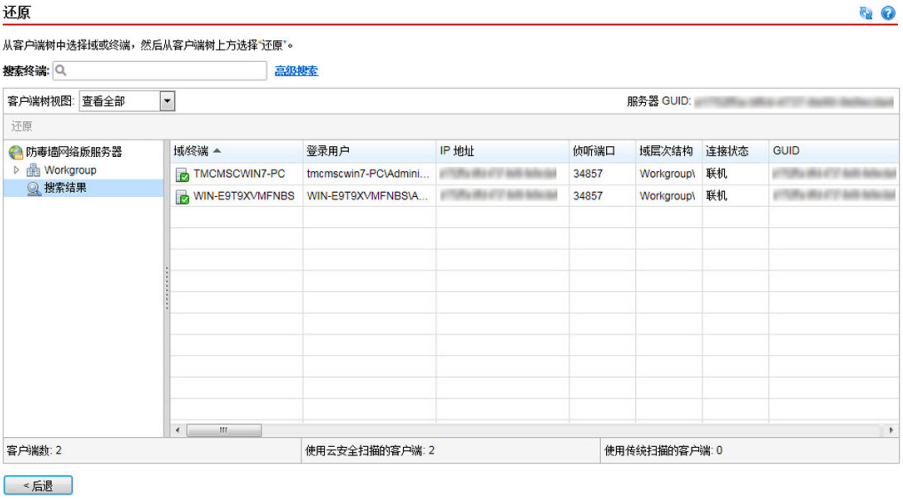


图 2-25. 还原窗口

安全风险日志窗口

要查看此窗口，请转至**日志** > **客户端** > **安全风险**。

在**安全风险日志**窗口中查看和管理日志。

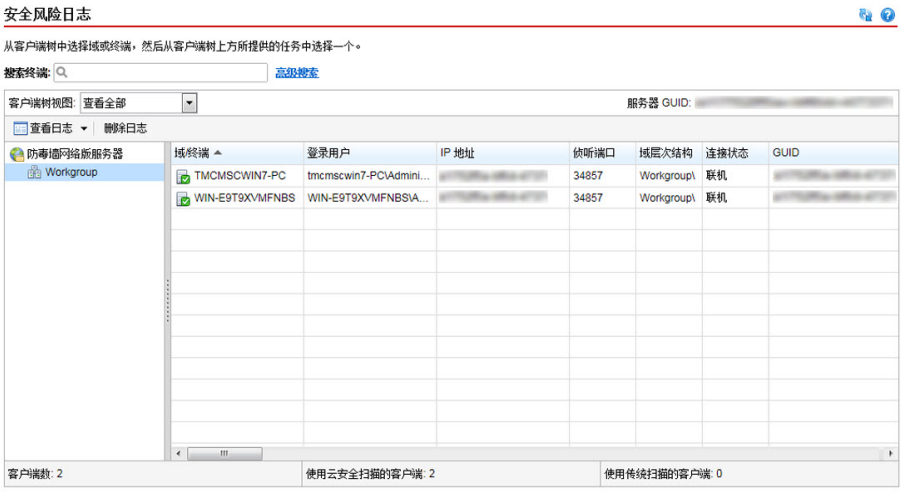


图 2-26. 安全风险日志窗口

执行以下任务：

1. 查看客户端发送至服务器的日志。有关详细信息，请参阅：
   - 查看病毒/恶意软件日志 第 7-81 页
   - 查看间谍软件/灰色软件日志 第 7-88 页
   - 查看防火墙日志 第 12-27 页
   - 查看 Web 信誉日志 第 11-23 页
   - 查看可疑连接日志 第 11-25 页
   - 查看可疑文件日志 第 7-92 页
   - 查看 C&C 回呼日志 第 11-24 页
   - 查看行为监控日志 第 8-13 页

- 查看设备控制日志 第 9-17 页
- 查看数据丢失防护日志 第 10-53 页

2. 删除日志。有关详细信息，请参阅日志管理 第 13-35 页。

防毒墙网络版域

防毒墙网络版中的域是一组共享相同配置、运行相同任务的客户端。通过将客户端分组为域，可以对所有域成员配置、管理和应用相同的配置。有关客户端分组的详细信息，请参阅客户端分组 第 2-50 页。

客户端分组

使用客户端分组手动或自动创建和管理防毒墙网络版客户端树上的域。

有两种方法可将客户端分组为域。

表 2-11. 客户端分组方法

方法	客户端分组	描述
手动	• NetBIOS 域 • Active Directory 域 • DNS 域	手动客户端分组定义了新安装的客户端应属于的域。当该客户端显示在客户端树中时，可以将其移动到其他域或其他防毒墙网络版服务器。 通过手动客户端分组，还可以在客户端树中创建、管理和删除域。 有关详细信息，请参阅手动客户端分组 第 2-51 页。
自动	定制客户端组	自动客户端分组使用规则对客户端树中的客户端进行排序。定义规则之后，可以在发生特定事件时访问客户端树以手动排序客户端，或允许防毒墙网络版以预设的时间间隔自动排序客户端。 有关详细信息，请参阅自动客户端分组 第 2-52 页。

手动客户端分组

防毒墙网络版仅在客户端全新安装时使用此设置。安装程序检查目标终端所属的网络域。如果客户端树中已存在该域名，防毒墙网络版会将目标终端上的客户端分组到该域下，并应用为该域配置的设置。如果该域名不存在，防毒墙网络版将该域添加到该客户端树，将该客户端分组到该域下，然后将根设置应用到该域和该客户端。

配置手动客户端分组

过程

1. 转至**客户端** > **客户端分组**。
2. 指定客户端分组方法：
   - NetBIOS 域
   - Active Directory 域
   - DNS 域
3. 单击**保存**。

后续步骤

通过执行以下任务来管理域和分组在其下的客户端：

- 添加域
- 删除域或客户端
- 更名域
- 将单个客户端移动到其他域

有关详细信息，请参阅客户端分组任务 第 2-56 页。

自动客户端分组

自动客户端分组使用基于 IP 地址或 Active Directory 域定义的规则。如果某个规则定义了 IP 地址或 IP 地址范围，防毒墙网络版服务器会将带有匹配 IP 地址的客户端分组到客户端树中的特定域。同样，如果某个规则定义了一个或多个 Active Directory 域，防毒墙网络版服务器将属于特定 Active Directory 域的客户端分组到客户端树中的特定域。

客户端每次仅应用一个规则。设置规则的优先次序，以便当客户端符合多个规则时，只应用具有最高优先级的规则。

配置自动客户端分组

过程

1. 转至**客户端** > **客户端分组**。
2. 转到**客户端分组**部分，然后选择**定制客户端组**。
3. 转到**自动客户端分组**部分。
4. 要开始创建规则，请单击**添加**，然后选择 **Active Directory** 或 **IP 地址**。
   - 如果选择 **Active Directory**，请参阅按 Active Directory 域定义客户端分组规则 第 2-53 页中的配置说明。
   - 如果选择 **IP 地址**，请参阅按 IP 地址定义客户端分组规则 第 2-54 页中的配置说明。
5. 如果创建了多个规则，请通过执行以下步骤来设置规则的优先次序：
   a. 选择某个规则。
   b. 单击**分组优先级**列下的箭头以在列表中上移或下移该规则。规则的 ID 号会发生更改以反映新位置。
6. 在客户端排序期间使用规则：
   a. 选中要使用的规则对应的复选框。
   b. 通过将**状态**控制切换为**开**启用规则。

注意

如果不选中某个规则的复选框或如果禁用某个规则，则在客户端树中对客户端进行排序时将不会使用该规则。例如，如果该规则指定客户端应移动到新域，则该客户端将不会进行移动并将留在其当前域中。

7. 在**预设域创建**部分中指定排序时间表。

   a. 选择**启用预设域创建**。

   b. 在**预设域创建**下指定时间表。

8. 从下列选项中选择：

   - **立即保存并创建域**：在按 IP 地址定义客户端分组规则 第 2-54 页中的步骤 7 或按 Active Directory 域定义客户端分组规则 第 2-53 页中的步骤 7 中已指定新域时选择此选项。
   - **保存**：如果未指定新域，或者仅当客户端排序运行时才要创建新域，请选择此选项。

注意

完成此步骤后，将不会启动客户端排序。

按 Active Directory 域定义客户端分组规则

确保您在执行以下过程中的步骤之前已配置 Active Directory 集成设置。有关详细信息，请参阅Active Directory 集成 第 2-34 页。

过程

1. 转至**客户端 > 客户端分组**。
2. 转到**客户端分组**部分，然后选择**为现有防毒墙网络版客户端创建自定义客户端组**。
3. 转到**自动客户端分组**部分。

4. 单击**添加**，然后选择 **Active Directory**。

   将显示一个新窗口。

5. 选择**启用分组**。

6. 为该规则指定一个名称。

7. 在 **Active Directory 源**下，选择 Active Directory 域或子域。

8. 在**客户端树**下，选择 Active Directory 域映射到的现有防毒墙网络版域。如果所需的防毒墙网络版域不存在，则执行以下步骤：

   a. 将鼠标悬停在特定防毒墙网络版域上并单击“添加域”图标 (+)。

   b. 在提供的文本框中键入域名。

   c. 单击文本框旁边的复选标记。将添加新域并自动选择该域。

9. （可选）选择 **将 Active Directory 结构复制到防毒墙网络版客户端树**。此选项将选定的 Active Directory 域的层次结构复制到选定的防毒墙网络版域。

10. 单击**保存**。

按 IP 地址定义客户端分组规则

使用网络 IP 地址创建定制客户端组，以便在防毒墙网络版客户端树中对客户端进行排序。此功能可以帮助管理员在客户端注册到防毒墙网络版服务器之前安排防毒墙网络版客户端树的结构。

过程

1. 转至**客户端** > **客户端分组**。

2. 转到**客户端分组**部分，然后选择**为现有防毒墙网络版客户端创建自定义客户端组**。

3. 转到**自动客户端分组**部分。

4. 单击**添加**，然后选择 **IP 地址**。

   将显示一个新窗口。

5. 选择**启用分组**。

6. 指定分组名称。

7. 指定以下内容之一：

   - 单个 IPv4 或 IPv6 地址
   - IPv4 地址范围
   - IPv6 前缀和长度



注意

如果双栈客户端的 IPv4 和 IPv6 地址属于两个单独的客户端组，则该客户端将被分在 IPv6 组下。如果在客户端的主机上禁用了 IPv6，则该客户端将移动到 IPv4 组。

8. 选择 IP 地址或 IP 地址范围映射到的防毒墙网络版域。如果该域不存在，则执行以下操作：

   a. 将鼠标悬停在客户端树上的任意位置并单击“添加域”图标。



图 2-27. “添加域”图标

   b. 在提供的文本框中键入域。

   c. 单击文本框旁边的复选标记。将添加新域并自动选择该域。

9. 单击**保存**。

客户端分组任务

分组域中的客户端时，可以执行下列任务：

- 添加域。请参阅 添加域 第 2-56 页 以了解详细信息。
- 删除域或客户端。请参阅 删除域或客户端 第 2-57 页 以了解详细信息。
- 更名域。请参阅 更名域 第 2-57 页 以了解详细信息。
- 将单个客户端移动到其他域或其他防毒墙网络版服务器。请参阅将防毒墙网络版客户端移动到其他域或防毒墙网络版服务器 第 2-58 页以了解详细信息。

添加域

过程

1. 导航至**客户端** > **客户端管理**。
2. 单击**管理客户端树** > **添加域**。
3. 键入要添加的域名。
4. 单击**添加**。

   新的域将显示在客户端树中。
5. （可选）创建子域。
   a. 选择父域。
   b. 单击**管理客户端树** > **添加域**。
   c. 键入子域名称。

删除域或客户端

过程

1. 导航至**客户端** > **客户端管理**。
2. 在客户端树中，选择：
   - 一个或多个域
   - 属于某个域的一个、多个或所有客户端
3. 单击**管理客户端树** > **删除域/客户端**。
4. 要删除空域，请单击**删除域/客户端**。如果该域具有客户端且您单击**删除域/客户端**，则防毒墙网络版服务器将重新创建域，并在下次客户端连接到防毒墙网络版服务器时将所有客户端分组到该域下。在删除该域之前，可以执行以下任务：
   a. 将客户端移动到其他域。要将客户端移动到其他域，可以把客户端拖放到目标域。
   b. 删除所有客户端。
5. 要删除单个客户端，请单击**删除域/客户端**。



注意

从客户端树删除客户端不会从客户端终端删除防毒墙网络版客户端。防毒墙网络版客户端仍可以执行独立于服务器的任务，例如更新组件。但服务器无法识别客户端的存在，因此将不会部署配置，也不会向该客户端发送通知。

更名域

过程

1. 导航至**客户端** > **客户端管理**。
2. 在客户端树中选择某个域。

3. 单击**管理客户端树** > **更名域**。
4. 键入域的新名称。
5. 单击**更名**。

   新的域名称将显示在客户端树中。

将防毒墙网络版客户端移动到其他域或防毒墙网络版服务器

过程

1. 导航至**客户端** > **客户端管理**。
2. 在客户端树中，选择一个、多个或所有客户端。
3. 单击**管理客户端树** > **移动客户端**。
4. 将客户端移动到其他域：
   - 选择**将选定的客户端移动到另一个域**。
   - 选择域。
   - （可选）将新域的设置应用到客户端。

   提示

   还可以将客户端拖放到客户端树中的其他域。
5. 将客户端移动到其他防毒墙网络版服务器：
   - 选择**将选定的客户端移动到另一个防毒墙网络版服务器**。
   - 键入服务器名称或 IPv4/IPv6 地址，以及 HTTP 端口号。
6. 单击**移动**。

第 3 章

数据保护入门

本章讨论如何安装并激活数据保护模块。

主题包括：

- 数据保护安装 第 3-2 页
- 数据保护使用授权 第 3-3 页
- 将数据保护部署到防毒墙网络版客户端 第 3-5 页
- 取证文件夹和 DLP 数据库 第 3-8 页
- 卸载数据保护 第 3-13 页

数据保护安装

数据保护模块包括下列功能：

- **数据丢失防护 (DLP)**：防止未经授权传输数字资产
- **设备控制**：控制对外部设备的访问

注意

防毒墙网络版自带设备控制功能，可控制对常用设备（如 USB 存储设备）的访问。设备控制（数据保护模块的一部分）可扩大监控的设备范围。有关受监控设备的列表，请参阅设备控制 第 9-2 页。

数据丢失防护和设备控制是本机防毒墙网络版功能，但需要单独进行授权。安装防毒墙网络版服务器之后，这些功能即可用，但未正常运行，且无法部署到客户端。安装数据保护表示需要从 ActiveUpdate 服务器或定制更新源（如果已设置定制更新源）下载文件。将文件整合至防毒墙网络版服务器之后，可以激活数据保护使用授权，以启用其完整功能。从**插件管理器**执行安装和激活操作。

重要信息

如果独立型趋势科技数据丢失防护软件已安装在终端上并正在运行，则无需安装数据保护模块。

安装数据保护

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口上，转至**防毒墙网络版数据保护**部分，然后单击**下载**。

   要下载的文件的大小会显示在**下载**按钮旁。

   插件管理器会将下载的文件存储到 <服务器安装文件夹>\PCCSRV\Download\Product。

注意

如果插件管理器无法下载文件，它会在 24 小时后自动重新下载。要手动触发插件管理器下载该文件，请从 Microsoft 管理控制台重新启动防毒墙网络版插件管理器服务。

3. 监控下载进度。

   在下载过程中可以离开该窗口。

   如果在下载文件时遇到问题，请查看防毒墙网络版 Web 控制台上的服务器更新日志。在主菜单上，单击**日志** > **服务器更新**。

   插件管理器下载完文件后，防毒墙网络版数据保护会显示在一个新窗口中。

注意

如果未显示防毒墙网络版数据保护，请参阅插件管理器故障排除 第 15-11 页中的原因和解决方案。

4. 要立即安装防毒墙网络版数据保护，请单击**立即安装**，如果要稍后安装，请执行下列操作：

   a. 单击**稍后安装**。

   b. 打开**插件管理器**窗口。

   c. 转到**防毒墙网络版数据保护**部分，然后单击**安装**。

5. 阅读许可协议，然后单击**同意**以接受其中的条款。

   安装即开始。

6. 监控安装进度。安装之后，将显示防毒墙网络版数据保护版本。

数据保护使用授权

可以从插件管理器查看、激活和续订数据保护使用授权。

从趋势科技获取激活码，然后激活使用授权。

激活插件程序许可证

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**管理程序**。

   此时将显示**产品使用授权新激活码**窗口。
3. 在文本框中键入或复制并粘贴激活码。
4. 单击**保存**。

   此时将显示插件控制台。

查看和续订使用授权信息

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**管理程序**。
3. 单击**查看使用授权信息**，在趋势科技 Web 站点上查看当前使用授权的相关信息。
4. 在打开的窗口中查看以下使用授权详细信息。

选项	说明
状态	显示“已激活”、“尚未激活”或“已过期”
版本	显示“完全版”或“试用版”

选项	说明
	注意 同时激活完全版和试用版时，只显示为“完全版”。
座席数	显示插件程序能够管理的终端数量
使用授权过期日期	如果插件程序有多个使用授权，则将显示最晚过期日期。 例如，如果使用授权到期日期为 12/31/2011 和 06/30/2011，则将显示 12/31/2011。
激活码	显示激活码
提醒	根据当前的使用授权版本，插件会在宽限期内（仅限完全版）或使用授权到期时显示关于使用授权到期日期的提醒

注意

宽限期的持续时间因地区而异。请与趋势科技代表核实插件程序宽限期。

5. 要更新窗口以显示最新的使用授权信息，请单击**更新信息**。
6. 单击**新激活码**以打开**产品使用授权新激活码**窗口。

   有关详细信息，请参阅激活插件程序许可证 第 3-4 页。

将数据保护部署到防毒墙网络版客户端

激活数据保护模块的使用授权之后，就可以将其部署到防毒墙网络版客户端。部署之后，防毒墙网络版客户端将开始使用数据丢失防护和设备控制。

重要信息

- 缺省情况下，Windows Server 2003、Windows Server 2008 和 Windows Server 2012 会禁用该模块，以避免主机的性能受到影响。如果要启用此模块，请持续监控系统性能，并在发现性能下降时采取必要的处理措施。

  可以从 Web 控制台启用或禁用此模块。有关详细信息，请参阅防毒墙网络版客户端服务 第 14-6 页。

- 如果趋势科技数据丢失防护软件已存在于终端上，防毒墙网络版不会将其替换为数据保护模块。
- 联机客户端会立即安装数据保护模块。脱机和漫游客户端会在变为联机状态时安装此模块。
- 用户必须重新启动计算机才能完成数据丢失防护驱动程序的安装。重新启动之前请先通知用户。
- 趋势科技建议启用调试日志记录功能，以帮助您解决部署问题。有关详细信息，请参阅启用数据保护模块的调试日志记录 第 10-58 页。

将数据保护模块部署到防毒墙网络版客户端

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，您可以：
   - 单击根域图标 ()，以将该模块部署到所有现有的和未来的客户端。
   - 选择特定域，以将该模块部署到该域下的所有现有的和未来的客户端。
   - 选择特定客户端，以只将该模块部署到该客户端。
3. 使用两种不同方式部署模块：
   - 单击**设置** > **DLP 设置**。
   - 单击**设置** > **设备控制设置**。

注意

如果您通过**设置** > **DLP 设置**进行部署，且数据保护模块已成功部署，则会安装数据丢失防护驱动程序。如果成功安装这些驱动程序，则会显示一条消息以通知用户重新启动终端以完成驱动程序安装。

如果未显示该消息，则安装驱动程序时可能出现了问题。如果已启用调试日志记录功能，请查看调试日志，以获得有关驱动程序安装问题的详细信息。

4. 将显示一条消息，指明尚未安装该模块的客户端数量。单击**是**以开始部署。

注意

如果单击**否**（或者如果由于某种原因，未将该模块部署到一个或多个客户端），则当您再次单击**设置** > **DLP 设置**或**设置** > **设备控制设置**时，会显示相同的消息。

防毒墙网络版客户端开始从服务器下载该模块。

5. 检查该模块是否已部署到客户端。

   a. 在客户端树中，选择域。

   b. 在客户端树视图中，选择**数据保护视图**或**查看全部**。

   c. 检查**数据保护状态**列。部署状态可能是以下任何状态：

      - **正在运行**：模块已经部署成功，而且其功能已经启用。
      - **需要重新启动**：因为用户尚未重新启动计算机，所以尚未安装数据丢失防护驱动程序。如果未安装驱动程序，数据丢失防护将不起作用。
      - **已停止**：模块的服务尚未启动，或者已经正常关闭目标终端。要启动数据保护服务，请转至**客户端** > **客户端管理** > **设置** > **其他服务设置**，然后启用数据保护服务。
      - **无法安装**：将模块部署到客户端时出现问题。您将需要从客户端树重新部署该模块。

- **无法安装 (数据丢失防护已存在)**：趋势科技数据丢失防护软件已经存在于终端上。防毒墙网络版不会将其替换为数据保护模块。
- **未安装**：该模块尚未部署到客户端。如果选择不要将该模块部署到客户端，或客户端的状态在部署时为脱机或漫游，则会显示此状态。

取证文件夹和 DLP 数据库

在数据丢失防护事件发生后，防毒墙网络版将事件详细信息记录到专门的取证数据库。防毒墙网络版还将创建一个加密的文件（其中包含触发事件的敏感数据的副本），并生成一个哈希值用于进行验证并确保敏感数据的完整性。防毒墙网络版将在客户端计算机上创建加密的取证文件，然后将这些文件上传到服务器的指定位置。

重要信息

- 加密的取证文件包含高度敏感的数据，管理员在被授权访问这些文件时应当小心谨慎。
- 防毒墙网络版与控制管理中心集成，以为具备 DLP Incident Reviewer 或者 DLP Compliance Officer 角色的控制管理中心用户提供在加密的文件内访问数据的能力。有关 DLP 角色以及对控制管理中心内取证文件数据的访问权限的详细信息，请参阅《控制管理中心管理员指南 6.0 Patch 2》或更高版本。

修改取证文件夹和数据库设置

管理员可以通过修改防毒墙网络版的 INI 文件更改取证文件夹的位置和删除时间表，以及客户端上传的最大文件大小。

警告!

在记录数据丢失防护事件之后更改取证文件夹的位置会造成数据库数据和现有取证文件位置之间的连接断开。趋势科技建议在修改取证文件夹的位置之后，将现有的所有取证文件手动迁移至新的取证文件夹。

下表概述了位于防毒墙网络版服务器上的 <服务器安装文件夹>\PCCSRV\Private\ofcserver.ini 文件中可用的服务器设置。

表 3-1. PCCSRV\Private\ofcserver.ini 中的取证文件夹服务器设置

目标	INI 设置	值
启用用户定义的取证文件夹位置	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0：禁用（缺省值） 1：启用
配置用户定义的取证文件夹位置	[INI_IDLP_SECTION] `UserDefinedUploadFolder` **注意** • 在数据丢失防护应用该设置前，管理员必须启用 `EnableUserDefinedUploadFolder` 设置。 • 取证文件夹的缺省位置为： <服务器安装文件夹>\PCCSRV\Private\DLPForensicData • 用户定义的取证文件夹位置必须为服务器计算机上的物理驱动器（内部或外部）。防毒墙网络版不支持映射网络驱动器位置。	缺省值：<请使用客户定义的文件夹路径替换此值。例如：C:\VolumeData\OfficeScanDlpForensicData> 用户定义的值：必须为服务器计算机上驱动器的物理位置
启用取证数据文件的清除	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0：禁用 1：启用（缺省值）

目标	INI 设置	值
配置取证数据文件清除检查的时间频率	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **注意** • 在防毒墙网络版应用该设置前，管理员必须启用 `ForensicDataPurgeEnable` 设置。 • 防毒墙网络版仅删除过了 `ForensicDataExpiredPeriodInDays` 设置中指定的有效期的数据文件。	1：每月，在当月第一天的 00:00 2：每周（缺省值），在每周日的 00:00 3：每天，在每天的 00:00 4：每小时，在每小时的 HH:00
配置在服务器上存储取证数据文件的时间长度	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	缺省值（以天为单位）：180 最小值：1 最大值：3650
配置取证文件磁盘空间检查的时间频率	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **注意** 如果取证数据文件夹中的可用磁盘空间少于 `InformUploadOnDiskFreeSpaceInGb` 设置所配置的值，防毒墙网络版将在 Web 控制台上记录事件日志。	缺省值（以秒为单位）：5
配置取证文件磁盘空间检查的上传频率	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **注意** 如果取证数据文件夹中的可用磁盘空间少于 `InformUploadOnDiskFreeSpaceInGb` 设置所配置的值，防毒墙网络版将在 Web 控制台上记录事件日志。	缺省值（以文件数为单位）：200

目标	INI 设置	值
配置触发磁盘空间受限通知的最小磁盘空间值	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **注意** 如果取证数据文件夹中的可用磁盘空间少于所配置的值，防毒墙网络版将在 Web 控制台上记录事件日志。	缺省值（以 GB 为单位）：10
配置从客户端上传取证数据文件的最小可用空间	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **注意** 如果取证数据文件夹中的可用磁盘空间少于所配置的值，防毒墙网络版客户端将不把取证数据文件上传到服务器，防毒墙网络版将在 Web 控制台上记录事件日志。	缺省值（以 GB 为单位）：1

下表概述了位于防毒墙网络版服务器上的 <服务器安装文件夹>\PCCSRV\ofcscan.ini 文件中可用的防毒墙网络版客户端设置。

表 3-2. PCCSRV\ofcscan.ini 中的取证文件客户端设置

目标	INI 设置	值
启用取证数据文件到服务器的上传	`UploadForensicDataEnable`	0：禁用 1：启用（缺省值）
配置防毒墙网络版客户端上传到服务器的最大文件大小	`UploadForensicDataSizeLimitInMb` **注意** 防毒墙网络版客户端仅将小于此大小的文件发送至服务器。	缺省值（以 MB 为单位）：10 最小值：1 最大值：2048

目标	INI 设置	值
配置在防毒墙网络版客户端上存储取证数据文件的时间长度	ForensicDataKeepDays **注意** 防毒墙网络版客户端将于每天上午 11:00 删除已过指定有效期的取证数据文件。	缺省值（以天为单位）：180 最小值：1 最大值：3650
配置防毒墙网络版客户端检查服务器连接的频率	ForensicDataDelayUploadFrequenceInMinutes **注意** 无法将取证文件上传到服务器的防毒墙网络版客户端客户端将按指定的时间间隔自动尝试重新发送文件。	缺省值（以分钟为单位）：5 最小值：5 最大值：60

创建取证数据的备份

根据公司的安全策略，存储取证数据信息的必要时间长度可能截然不同。为了释放服务器上的磁盘空间，趋势科技建议手动备份取证文件夹数据和取证数据库。

过程

1. 转到服务器上的取证数据文件夹位置。
   - 缺省位置：<服务器安装文件夹>\PCCSRV\Private\DLPForensicData
   - 要查找定制的取证文件夹位置，请参见配置用户定义的取证文件夹位置 第 3-9 页。
2. 将文件夹复制到一个新位置。
3. 要手动备份取证数据数据库，请导航到 <服务器安装文件夹>\PCCSRV\Private。

4. 将 DLPForensicDataTracker.db 文件复制到一个新位置。

卸载数据保护

如果从插件管理器卸载数据保护模块：

- 系统会从防毒墙网络版服务器删除所有数据丢失防护配置、设置和日志。
- 系统会从服务器删除数据保护模块所提供的所有设备控制配置和设置。
- 系统会从客户端删除数据保护模块。必须重新启动客户端 终端，才能完全删除数据保护。
- 系统再也不会在客户端上实施数据丢失防护策略。
- 设备控制不会再监控对下列设备的访问：
  - Bluetooth 无线收发器
  - COM 和 LPT 端口
  - IEEE 1394 接口
  - 图像处理设备
  - 红外设备
  - 调制解调器
  - PCMCIA 卡
  - 打印屏幕键
  - 无线 NIC

随时重新安装数据保护模块。重新安装之后，请使用有效的激活码来激活使用授权。

从插件管理器卸载数据保护

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口上，转至**防毒墙网络版数据保护**部分，然后单击**卸载**。
3. 监控卸载进度。在卸载过程中可以离开该窗口。
4. 卸载之后，请刷新**插件管理器**窗口。您可以再次安装防毒墙网络版数据保护。

部分 II

保护防毒墙网络版客户端

第 4 章

使用趋势科技云安全智能防护

本章讨论趋势科技云安全智能防护解决方案，并说明如何设置使用这些解决方案所需的环境。

主题包括：

- 关于趋势科技云安全智能防护 第 4-2 页
- 云安全智能防护服务 第 4-3 页
- 云安全智能防护源 第 4-5 页
- 云安全智能防护病毒码文件 第 4-7 页
- 设置云安全智能防护服务 第 4-11 页
- 使用云安全智能防护服务 第 4-29 页

关于趋势科技云安全智能防护

趋势科技™ 云安全智能防护是下一代云客户端内容安全基础架构，旨在保护客户免受安全风险和 Web 威胁的危害。它使用轻量级客户端访问其提供的独特云端电子邮件、Web 和文件信誉相关技术以及威胁数据库，提供了本地和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。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。

通过结合云端信誉、扫描和相关技术，趋势科技云安全智能防护解决方案减少了对传统病毒码文件下载的依赖，并且消除了通常与桌面更新相关的延迟。

需要新的解决方案

在当前处理基于文件的威胁的方法中，保护终端所需的大多数病毒码（或定义）都按预设发送。病毒码分批从趋势科技发送到客户端。当接收到新的更新时，客户端上的病毒/恶意阻止软件将这批新的病毒/恶意软件风险的特征码定义重新加载到内存中。如果出现新的病毒/恶意软件风险，需要再次部分或完全更新此病毒码并在客户端上重新加载，以确保持续获得保护。

随着时间的推移，新出现的独特威胁的数量将显著增长。从威胁数量的增长可以推算出，在未来几年里威胁将以接近指数的速度增长。按照增长率计算出的威胁数量远远超出当前所知的安全风险数量。进一步讲，这一急剧增长的安全风险数量反映了一种新的安全风险。安全风险的数量可能影响服务器和工作站性能、网络带宽使用率以及通常其用于提供高质量防护所需的总体时间（或防护时间）。

趋势科技率先开发了一种用于处理威胁数量的新方法，该方法旨在使趋势科技客户可以抵御病毒/恶意软件数量的威胁。开发此新方法时使用的技术和体系结构利用的技术原理是，将存储的病毒/恶意软件签名和病毒码转移到云中。通过将这些存储的病毒/恶意软件签名转移到云中，趋势科技能够更好地保护客户免受将来新出现的大量安全风险的威胁。

云安全智能防护服务

云安全智能防护包括的服务提供了云端存储的防恶意软件签名、Web 信誉和威胁数据库。

云安全智能防护服务包括：

- **文件信誉服务**：文件信誉服务将先前存储在客户端计算机上的大量防恶意软件签名转移到云安全智能防护源。

  有关详细信息，请参阅文件信誉服务 第 4-3 页。

- **Web 信誉服务**：通过 Web 信誉服务，本地云安全智能防护源可以托管以前由趋势科技单独托管的 URL 信誉数据。这两种技术可确保在更新特征码或检查 URL 的有效性时占用较小的带宽。

  有关详细信息，请参阅Web 信誉服务 第 4-4 页。

- **云安全智能反馈**：趋势科技不断获取从全球趋势科技产品匿名发送的信息，前瞻性地判断每种新威胁。

  有关详细信息，请参阅云安全智能反馈 第 4-4 页。

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。由于恶意软件信息存储在云端，因此所有用户可以立即获得。高性能内容传输网络和本地缓存服务器可确保在检查过程中延迟时间最短。云客户端体系结构提供了更多的即时防护，消除了病毒码部署的负担，并极大地减少了客户端占用的总体资源。

客户端必须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。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。防毒墙网络版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。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 信誉策略限制的防毒墙网络版客户端使用 Web 信誉服务。防毒墙网络版管理员可以将所有或多个客户端受限于 Web 信誉策略。

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。

提示

无需参与云安全智能反馈便可为您的终端提供防护。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/

云安全智能防护源

趋势科技向防毒墙网络版和云安全智能防护源提供文件信誉服务和 Web 信誉服务。

云安全智能防护源通过托管大多数病毒/恶意软件病毒码定义来提供文件信誉服务。防毒墙网络版客户端托管剩余定义。如果客户端自身的病毒码定义无法确定文件风险，它会向云安全智能防护源发送扫描查询。云安全智能防护源使用标识信息来确定风险。

云安全智能防护源通过托管以前仅由趋势科技托管的服务器提供的 Web 信誉数据来提供 Web 信誉服务。客户端向云安全智能防护源发送 Web 信誉查询来检查用户尝试访问的 Web 站点的信誉。该客户端将 Web 站点的信誉与终端上实施的特定 Web 信誉策略关联，以便确定将允许访问该站点还是阻止访问该站点。

客户端连接的云安全智能防护源取决于客户端的位置。客户端可以连接到趋势科技云安全智能防护网络或云安全智能防护服务器。

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/cloudsecurity/

云安全智能防护服务器

云安全智能防护服务器适用于能够访问其本地公司网络的用户。本地服务器将云安全智能防护服务局限在公司网络内以提高效率。

有两种类型的云安全智能防护服务器：

- **集成型云安全智能防护服务器**：防毒墙网络版安装程序包括集成型云安全智能防护服务器，该服务器在防毒墙网络版服务器的终端上安装。安装完成后，便可以从防毒墙网络版 Web 控制台管理此服务器的设置。集成型服务器用于防毒墙网络版的小规模部署。对于较大规模的部署，需要独立型云安全智能防护服务器。
- **独立型云安全智能防护服务器**：独立型云安全智能防护服务器在 VMware 或 Hyper-V 服务器上安装。独立型服务器具有单独的管理控制台，不通过防毒墙网络版 Web 控制台进行管理。

云安全智能防护源对比

下表重点介绍云安全智能防护网络与云安全智能防护服务器之间的差别。

表 4-1. 云安全智能防护源对比

比较的基础	云安全智能防护服务器	趋势科技云安全智能防护网络
可用性	可用于内部客户端，即符合防毒墙网络版 Web 控制台上指定的位置条件的客户端	主要可用于外部客户端，即不符合防毒墙网络版 Web 控制台上指定的位置条件的客户端

比较的基础	云安全智能防护服务器	趋势科技云安全智能防护网络
用途	设计用于将云安全智能防护服务局限在公司网络内以提高效率	基于 Internet 的全球范围的基础架构，用于将云安全智能防护服务提供给无法直接访问其公司网络的客户端
管理	防毒墙网络版管理员安装和管理这些云安全智能防护源	趋势科技负责维护此源
特征码更新源	趋势科技 ActiveUpdate 服务器	趋势科技 ActiveUpdate 服务器
客户端连接协议	HTTP 和 HTTPS	HTTPS

云安全智能防护病毒码文件

云安全智能防护病毒码文件用于文件信誉服务和 Web 信誉服务。趋势科技通过趋势科技 ActiveUpdate 服务器发布这些病毒码文件。

云安全客户端病毒码

云安全客户端病毒码每天更新一次并由防毒墙网络版客户端的更新源（防毒墙网络版服务器或定制更新源）下载。然后，更新源将病毒码部署到云安全客户端。

注意

云安全客户端是管理员已将其配置为使用文件信誉服务的防毒墙网络版客户端。不使用文件信誉服务的客户端称为传统扫描客户端。

在扫描安全风险时，云安全客户端使用云安全客户端病毒码。如果该病毒码无法确定文件的风险，它将利用称为云安全云端病毒码的另一个病毒码。

云安全云端病毒码

云安全云端病毒码每小时更新一次并由云安全智能防护源下载。云安全客户端不下载此云安全云端病毒码。客户端通过将扫描查询发送到云安全智能防护源，根据云安全云端病毒码验证潜在威胁。

Web 阻止列表

Web 阻止列表由云安全智能防护源下载。受 Web 信誉策略限制的防毒墙网络版客户端不会下载 Web 阻止列表。



注意

管理员可以将所有或多个客户端受限于 Web 信誉策略。

受 Web 信誉策略限制的客户端通过向云安全智能防护源发送 Web 信誉查询，来对照 Web 阻止列表验证 Web 站点的信誉。该客户端将从云安全智能防护源接收的信誉数据与在终端上执行的 Web 信誉策略关联。根据该策略，客户端将允许或阻止对站点的访问。

云安全智能防护病毒码更新过程

云安全智能防护病毒码更新源自趋势科技 ActiveUpdate 服务器。

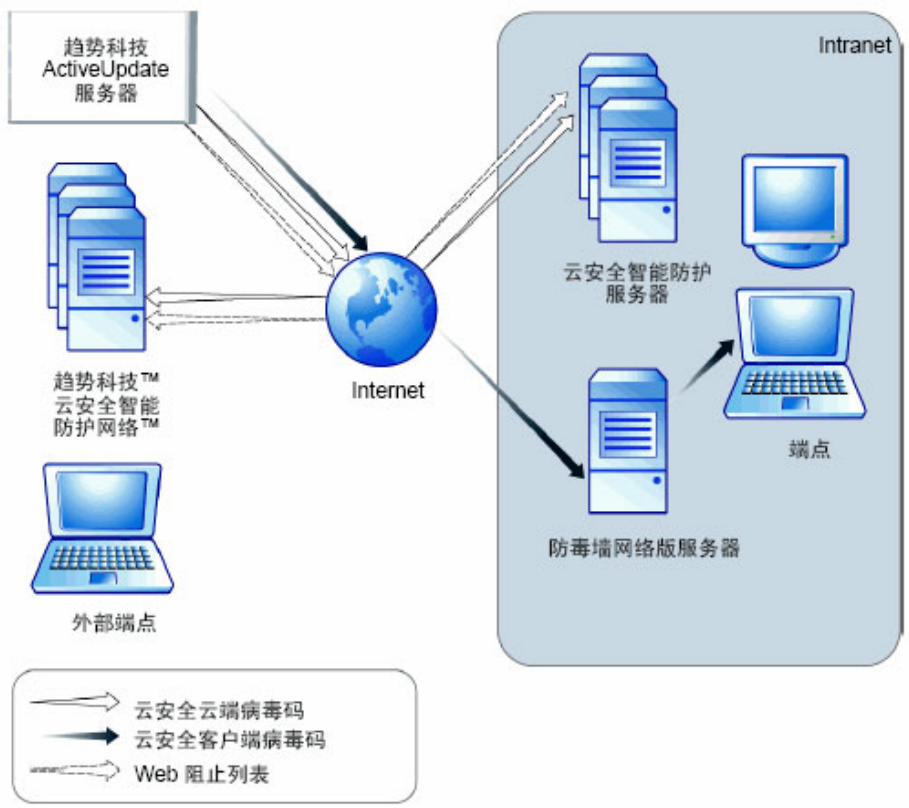


图 4-1. 病毒码更新过程

使用云安全智能防护病毒码

防毒墙网络版客户端使用云安全客户端特征码扫描安全风险，且仅当该云安全客户端病毒码无法确定文件的风险时才查询云安全云端病毒码。在用户尝试访

问 Web 站点时，客户端会查询 Web 阻止列表。通过高级筛选技术，客户端可以“缓存”查询结果。这样便不需要多次发送相同的查询。

当前在 Intranet 中的客户端可以连接到云安全智能防护服务器，以查询云安全云端病毒码或 Web 阻止列表。要连接到云安全智能防护服务器，必须使用网络连接。如果已设置多个云安全智能防护服务器，管理员可以确定连接优先级。

提示

安装多个云安全智能防护服务器可以确保在无法连接到云安全智能防护服务器时提供持续防护。

当前不在 Intranet 中的客户端可以连接趋势科技云安全智能防护网络来进行查询。要连接到云安全智能防护网络，必须使用 Internet 连接。

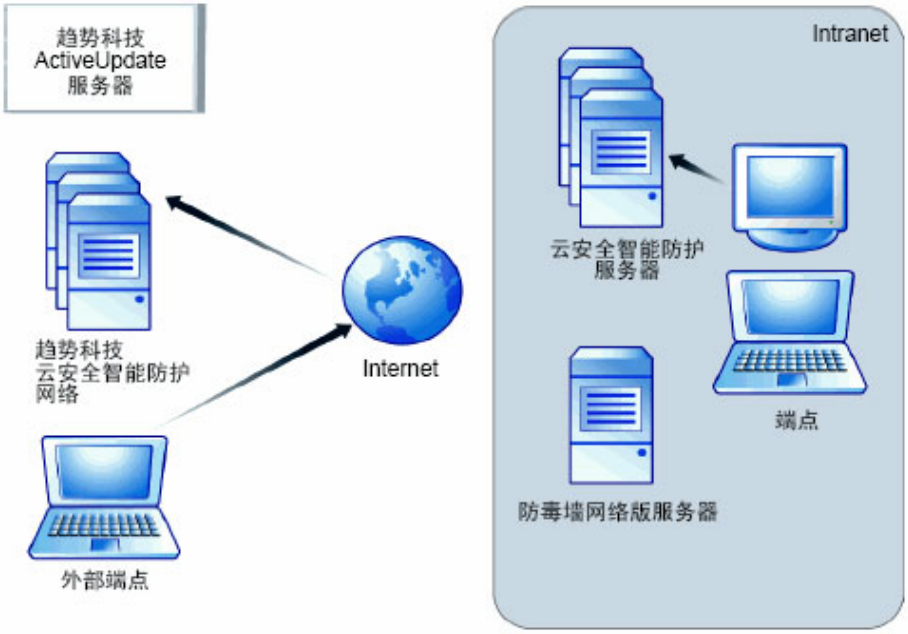


图 4-2. 查询过程

无法访问网络或 Internet 的客户端仍受由云安全客户端病毒码和包含先前查询结果的缓存提供的防护。仅当需要执行新查询且客户端在重复尝试后仍无法访问任何云安全智能防护源时，防护才会降低。在这种情况下，客户端会将文件标记为要进行验证并暂时允许访问该文件。当恢复与云安全智能防护源的连接后，会重新扫描所有的已标记文件。然后，对已经被确认为威胁的文件采取适当的扫描处理措施。

下表根据客户端的位置汇总了防护的范围。

表 4-2. 基于位置的防护行为

位置	病毒码文件和查询行为
具有 Intranet 访问权限	• **病毒码文件**：客户端从防毒墙网络版服务器或定制更新源下载云安全客户端病毒码文件。 • **文件和 Web 信誉查询**：客户端连接到云安全智能防护服务器以进行查询。
无 Intranet 访问权限但可连接到云安全智能防护网络	• **病毒码文件**：客户端不会下载最新的云安全客户端病毒码文件，除非可以连接到防毒墙网络版服务器或定制更新源。 • **文件和 Web 信誉查询**：客户端连接到云安全智能防护网络以进行查询。
无 Intranet 访问权限且无法连接到云安全智能防护网络	• **病毒码文件**：客户端不会下载最新的云安全客户端病毒码文件，除非可以连接到防毒墙网络版服务器或定制更新源。 • **文件和 Web 信誉查询**：客户端不接收查询结果且必须依赖云安全客户端病毒码和包含先前查询结果的缓存。

设置云安全智能防护服务

请确保已正确设置云安全智能防护环境，客户端才能利用文件信誉服务和 Web 信誉服务。检查下列各项：

- 云安全智能防护服务器安装 第 4-12 页
- 集成型云安全智能防护服务器管理 第 4-17 页

- 云安全智能防护源列表 第 4-21 页
- 客户端连接代理服务器设置 第 4-28 页
- 趋势科技网络病毒墙安装 第 4-28 页

云安全智能防护服务器安装

如果客户端数是 1,000 或更少，可安装集成型或独立型云安全智能防护服务器。如果客户端数超过 1,000，则安装独立型云安全智能防护服务器。

趋势科技建议您安装多个云安全智能防护服务器以用于故障转移。无法连接到特定服务器的客户端将尝试连接到已安装的其他服务器。

由于集成型服务器和防毒墙网络版服务器在同一终端上运行，因此在这两个服务器的流量高峰期终端的性能可能会大大降低。请考虑将独立型云安全智能防护服务器用作客户端的主要云安全智能防护源，并将集成型服务器用作备份源。

独立型云安全智能防护服务器安装

有关安装和管理独立型云安全智能防护服务器的说明，请参阅《*云安全智能防护服务器安装和升级指南*》。

集成型云安全智能防护服务器安装

如果在防毒墙网络版服务器安装期间安装了集成服务器：

- 启用集成服务器并配置该服务器的设置。有关详细信息，请参阅集成型云安全智能防护服务器管理 第 4-17 页。
- 如果集成服务器和防毒墙网络版客户端位于同一台服务器计算机上，请考虑禁用防毒墙网络版防火墙。防毒墙网络版防火墙用于客户端终端，当在服务器上启用时可能会影响性能。有关禁用防火墙的说明，请参阅启用或禁用防毒墙网络版防火墙 第 12-6 页。

注意

请考虑禁用防火墙的影响并确保此操作符合您的安全计划。

提示

完成防毒墙网络版安装之后，使用集成型云安全智能防护服务器工具 第 4-13 页安装集成型云安全智能防护服务器。

集成型云安全智能防护服务器工具

趋势科技防毒墙网络版集成型云安全智能防护工具可帮助管理员在完成防毒墙网络版服务器安装后安装或卸载集成型云安全智能防护服务器。防毒墙网络版服务器安装完成之后，当前的防毒墙网络版版本不允许管理员安装/移除集成型云安全智能防护服务器。此工具使安装功能的灵活性与之前的防毒墙网络版版本相比有所增强。

在安装集成型云安全智能防护服务器之前，请将以下内容导入到已升级的防毒墙网络版 11.0 SP1 服务器中：

- 域结构
- 以下根和域级别设置：
  - 所有扫描类型（手动扫描、实时扫描、预设扫描和立即扫描）的扫描配置
  - Web 信誉设置
  - 行为监控设置
  - 设备控制设置
  - 数据丢失防护设置
  - 权限和其他设置
  - 其他服务设置
  - 间谍软件/灰色软件允许列表

- 全局客户端设置
- 终端位置
- 防火墙策略和概要文件
- 云安全智能防护源
- 服务器更新时间表
- 客户端更新源和时间表
- 通知
- 代理服务器设置

过程

1. 打开命令提示符并转至 <服务器安装文件夹>\PCCSRV\Admin\Utility\ISPSInstaller 目录（ISPSInstaller.exe 位于该位置）。
2. 使用以下命令之一运行 ISPSInstaller.exe：

表 4-3. 安装程序选项

命令	描述
`ISPSInstaller.exe /i`	使用缺省端口设置安装集成型云安全智能防护服务器。 有关缺省端口设置的详细信息，请参阅下表。

命令	描述
`ISPSInstaller.exe /i /f:[端口号] /s:[端口号] /w:[端口号]`	使用指定的端口安装集成型云安全智能防护服务器。 **注意** 只能在使用 Apache Web 服务器时配置端口。 其中： • `/f:[端口号]` 表示 HTTP 文件信誉端口 • `/s:[端口号]` 表示 HTTPS 文件信誉端口 • `/w:[端口号]` 表示 Web 信誉端口 **注意** 未指定的端口自动分配有缺省值。
`ISPSInstaller.exe /u`	卸载集成型云安全智能防护服务器

表 4-4. 集成型云安全智能防护服务器的信誉服务的端口

Web 服务器和设置	文件信誉服务的端口		用于 Web 信誉服务的 HTTP 端口
	HTTP	HTTPS (SSL)	
启用了 SSL 的 Apache Web 服务器	8082	4345（不可配置）	5274（不可配置）
禁用了 SSL 的 Apache Web 服务器	8082	4345（不可配置）	5274（不可配置）
启用了 SSL 的 IIS 缺省 Web 站点	80	443（不可配置）	80（不可配置）
禁用了 SSL 的 IIS 缺省 Web 站点	80	443（不可配置）	80（不可配置）
启用了 SSL 的 IIS 虚拟 Web 站点	8080	4343（可配置）	8080（可配置）

Web 服务器和设置	文件信誉服务的端口		用于 Web 信誉服务的 HTTP 端口
	HTTP	HTTPS (SSL)	
禁用了 SSL 的 IIS 虚拟 Web 站点	8080	4343（可配置）	8080（可配置）

3. 安装完成后，打开防毒墙网络版 Web 控制台并验证以下内容：

   - 打开 **Microsoft 管理控制台**（通过在**开始**菜单中键入 `services.msc`），然后检查趋势科技本地 Web 分类服务器和趋势科技云安全服务器是否以“已启动”状态列出。
   - 打开 **Windows 任务管理器**。在**进程**选项卡中，检查 iCRCService.exe 和 LWCSService.exe 是否正在运行。
   - 在防毒墙网络版 Web 控制台上，检查菜单项**管理** > **云安全智能防护** > **集成服务器**是否已显示。

云安全智能防护服务器最佳做法

通过执行以下操作来优化云安全智能防护服务器的性能：

- 避免同时执行手动扫描和预设扫描。以组为单位错开扫描。
- 避免将所有客户端配置为同时执行立即扫描。
- 通过更改 ptngrowth.ini 文件，可定制云安全智能防护服务器以实现较慢的网络连接（大约 512Kbps）。

为独立型服务器定制 ptngrowth.ini

过程

1. 打开 /var/tmcss/conf/ 中的 ptngrowth.ini 文件。
2. 使用以下建议值修改 ptngrowth.ini 文件：

- `[COOLDOWN]`
- `ENABLE=1`
- `MAX_UPDATE_CONNECTION=1`
- `UPDATE_WAIT_SECOND=360`

3. 保存 ptngrowth.ini 文件。
4. 通过在命令行界面 (CLI) 中键入以下命令，重新启动 lighttpd 服务：
   - `service lighttpd restart`

为集成服务器定制 ptngrowth.ini

过程

1. 打开 <服务器安装文件夹>\PCCSRV\WSS\ 中的 ptngrowth.ini 文件。
2. 使用以下建议值修改 ptngrowth.ini 文件：
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. 保存 ptngrowth.ini 文件。
4. 重新启动趋势科技云安全智能防护服务器服务。

集成型云安全智能防护服务器管理

通过执行以下任务来管理集成型云安全智能防护服务器：

- 启用集成服务器的文件信誉服务和 Web 信誉服务
- 记录集成服务器的地址
- 更新集成服务器的组件
- 配置集成服务器的允许/阻止 URL 列表

有关详细信息，请参阅配置集成型云安全智能防护服务器设置 第 4-20 页。

启用集成服务器的文件信誉服务和 Web 信誉服务

要使客户端向集成服务器发送扫描和 Web 信誉查询，必须启用文件信誉服务和 Web 信誉服务。通过启用这些服务，集成服务器还可以从 ActiveUpdate 服务器更新组件。

如果选择在防毒墙网络版服务器安装期间安装集成服务器，则这些服务将自动启用。

如果禁用这些服务，请确保已安装客户端可向其发送查询的独立型云安全智能防护服务器。

有关详细信息，请参阅配置集成型云安全智能防护服务器设置 第 4-20 页。

记录集成服务器的地址

在为内部客户端配置云安全智能防护源列表时，将需要集成型服务器的地址。有关该列表的详细信息，请参阅云安全智能防护源列表 第 4-21 页。

在客户端向集成型服务器发送扫描查询时，这些客户端通过两个文件信誉服务地址（HTTP 或 HTTPS 地址）中的一个来识别服务器。通过 HTTPS 地址的连接更安全，而 HTTP 连接使用的带宽更小。

在客户端发送 Web 信誉查询时，这些客户端通过集成型服务器的 Web 信誉服务地址来识别该服务器。

提示

由另一个防毒墙网络版服务器管理的客户端也可以连接到此集成型服务器。在其他防毒墙网络版服务器的 Web 控制台上，将集成服务器的地址添加到云安全智能防护源列表。

有关详细信息，请参阅配置集成型云安全智能防护服务器设置 第 4-20 页。

更新集成服务器的组件

集成服务器更新以下组件：

- **云安全云端病毒码**：防毒墙网络版客户端通过将扫描查询发送到集成型服务器，根据云安全云端病毒码验证潜在威胁。
- **Web 阻止列表**：受 Web 信誉策略限制的防毒墙网络版客户端通过向集成型服务器发送 Web 信誉查询，来对照 Web 阻止列表验证 Web 站点的信誉。

您可以手动更新这些组件或配置更新时间表。集成服务器从 ActiveUpdate 服务器下载组件。

注意

纯 IPv6 集成服务器无法直接从趋势科技 ActiveUpdate 服务器进行更新。需要使用可以转换 IP 地址的双栈代理服务器（例如 DeleGate）才能将集成服务器连接到 ActiveUpdate 服务器。

有关详细信息，请参阅配置集成型云安全智能防护服务器设置 第 4-20 页。

集成服务器的允许/阻止 URL 列表配置

客户端负责维护各自的允许/阻止 URL 列表。可以在设置 Web 信誉策略时配置客户端的该列表（有关详细信息，请参阅 Web 信誉策略 第 11-4 页）。将自动允许或阻止客户端的列表中的任何 URL。

集成服务器具有自己的允许/阻止 URL 列表。如果 URL 不在客户端的列表中，客户端会向集成服务器发送 Web 信誉查询（如果该集成服务器已被指定为云安

全智能防护源）。如果在集成服务器的允许/阻止 URL 列表中找到了该 URL，集成服务器会通知客户端允许或阻止该 URL。

注意

阻止 URL 列表具有的优先级高于 Web 阻止列表。

要将 URL 添加到集成服务器的允许/阻止列表，请从独立型云安全智能防护服务器中导入列表。无法手动添加 URL。

有关详细信息，请参阅配置集成型云安全智能防护服务器设置 第 4-20 页。

配置集成型云安全智能防护服务器设置

过程

1. 转至**管理** > **云安全智能防护** > **集成服务器**。
2. 选择**启用文件信誉服务**。
3. 选择客户端向集成服务器发送扫描查询时将使用的协议（HTTP 或 HTTPS）。
4. 选择**启用 Web 信誉服务**。
5. 记录在**服务器地址**列下找到的集成服务器的地址。
6. 更新集成服务器的组件：
   - 查看云安全云端病毒码和 Web 阻止列表的当前版本。如果存在更新，请单击**立即更新**。更新结果将显示在窗口顶部。
   - 自动更新病毒码：
     a. 选择**启用预设更新**。
     b. 选择是每小时更新一次还是每 15 分钟更新一次。
     c. 选择**文件信誉服务**下的更新源。将从此源更新云安全云端病毒码。

d. 选择 **Web 信誉服务**下的更新源。将从此源更新 Web 阻止列表。

注意

- 如果选择 ActiveUpdate 服务器作为更新源，请确保该服务器具有 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。请参阅用于防毒墙网络版服务器更新的代理服务器 第 6-19 页以了解详细信息。
- 如果选择定制更新源，请为此更新源设置相应的环境和更新资源。此外，还应确保服务器计算机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。

7. 配置集成服务器的允许/阻止列表：

   a. 单击**导入**以使用预先设置格式的 .csv 文件中的 URL 填充该列表。可以从独立型云安全智能防护服务器中获取 .csv 文件。

   b. 如果具有现有列表，请单击**导出**以将该列表保存到.csv 文件。

8. 单击**保存**。

云安全智能防护源列表

客户端扫描安全风险并确定 Web 站点的信誉时，会向云安全智能防护源发送查询。

云安全智能防护源的 IPv6 支持

纯 IPv6 客户端无法将查询直接发送到纯 IPv4 源，如：

- 云安全智能防护服务器 2.0（集成型或独立型）

注意

云安全智能防护服务器自版本 2.5 开始支持 IPv6。

- 趋势科技云安全智能防护网络

同样，纯 IPv4 客户端也无法向纯 IPv6 云安全智能防护服务器发送查询。

要使客户端连接到源，需提供可以转换 IP 地址的双栈代理服务器（如 DeleGate）。

云安全智能防护源和终端位置

客户端连接到哪个云安全智能防护源取决于客户端终端所处的位置。

有关配置位置设置的详细信息，请参阅终端位置 第 14-2 页。

表 4-5. 云安全智能防护源（按位置）

位置	云安全智能防护源
外部	外部客户端向趋势科技云安全智能防护网络发送扫描和 Web 信誉查询。
内部	内部客户端向云安全智能防护服务器或趋势科技云安全智能防护网络发送扫描和 Web 信誉查询。 如果已安装云安全智能防护服务器，则在防毒墙网络版 Web 控制台上配置云安全智能防护源列表。如果内部客户端需要进行查询，会从列表中选取一个服务器。如果客户端无法连接到第一个服务器，会选取列表上的另一个服务器。 **提示** 分配独立型云安全智能防护服务器作为主要扫描源，将集成服务器作为备份。这减少了定向到托管防毒墙网络版服务器和集成服务器的终端的流量。独立型服务器也可以处理更多查询。 可以配置云安全智能防护源的标准列表或定制列表。标准列表由所有的内部客户端使用。定制列表定义 IP 地址范围。如果内部客户端的 IP 地址在此范围内，该客户端使用定制列表。

配置云安全智能防护源的标准列表

过程

1. 转至**管理** > **云安全智能防护** > **云安全智能防护源**。
2. 单击**内部客户端**选项卡。
3. 选择**使用标准列表 (适用于所有内部客户端)**。
4. 单击**标准列表**链接。

   此时打开一个新窗口。
5. 单击**添加**。

   此时打开一个新窗口。
6. 指定云安全智能防护服务器的主机名或 IPv4/IPv6 地址。如果指定的是 IPv6 地址，则使用括号将该地址括起来。

   注意

   如果有 IPv4 和 IPv6 客户端连接到云安全智能防护服务器，请指定主机名。
7. 选择“文件信誉服务”。客户端使用 HTTP 或 HTTPS 协议发送扫描查询。HTTPS 的连接更安全，而 HTTP 使用的带宽更小。

   a. 如果希望客户端使用 HTTP，请键入服务器的 HTTP 请求侦听端口。如果希望客户端使用 HTTPS，请选择 SSL 并键入服务器的 HTTPS 请求侦听端口。

   b. 单击**测试连接**，检查是否可以建立到服务器的连接。

   提示

   侦听端口构成服务器地址的一部分。获取服务器地址：

   对于集成服务器，打开防毒墙网络版 Web 控制台，然后转至**管理** > **云安全智能防护** > **集成服务器**。

   对于独立型服务器，打开独立型服务器的控制台，然后转至**摘要**窗口。

8. 选择 **Web 信誉服务**。客户端使用 HTTP 协议发送 Web 信誉查询。不支持 HTTPS。

   a. 键入服务器的 HTTP 请求侦听端口。

   b. 单击**测试连接**，检查是否可以建立到服务器的连接。

9. 单击**保存**。

   窗口随即关闭。

10. 通过重复以上步骤来添加更多服务器。

11. 在窗口顶部，选择**顺序**或**随机**。

    - **顺序**：客户端按服务器在列表中出现的顺序选取服务器。如果选择**顺序**，请使用**顺序**列下的箭头将服务器在列表中上下移动。
    - **随机**：客户端随机选取服务器。



提示

由于集成型云安全智能防护服务器和防毒墙网络版服务器在同一终端上运行，因此在这两个服务器的流量高峰期终端的性能可能会大大降低。要减少定向到防毒墙网络版服务器计算机的流量，请将独立型云安全智能防护服务器指定为主要云安全智能防护源，并将集成服务器指定为备份源。

12. 在窗口中执行其他任务。

    - 如果已从其他服务器导出列表，并希望将该列表导入到此窗口，请单击**导入**并找到该 .dat 文件。该列表将加载到窗口中。
    - 要将列表导出到 .dat 文件，请单击**导出**，然后单击**保存**。
    - 要刷新服务器的服务状态，请单击**刷新**。
    - 单击服务器名称，执行以下操作之一：
      - 查看或编辑服务器信息。
      - 查看 Web 信誉服务或文件信誉服务的完整服务器地址。
    - 要打开云安全智能防护服务器的控制台，请单击**启动控制台**。

- 对于集成型云安全智能防护服务器，将显示服务器的配置窗口。
- 对于独立型云安全智能防护服务器和其他防毒墙网络版服务器的集成型云安全智能防护服务器，将显示控制台登录窗口。

- 要删除某个条目，请选中该服务器对应的复选框并单击**删除**。

13. 单击**保存**。

    窗口随即关闭。

14. 单击**通知所有客户端**。

配置云安全智能防护源的定制列表

过程

1. 转至**管理** > **云安全智能防护** > **云安全智能防护源**。
2. 单击**内部客户端**选项卡。
3. 选择**使用基于客户端 IP 地址的定制列表**。
4. （可选）选择**当定制列表中的所有服务器都不可用时，请使用标准列表**。
5. 单击**添加**。

   此时打开一个新窗口。

6. 在 **IP 范围**部分中，指定 IPv4 或 IPv6 地址范围，或两者都指定。

   注意

   使用 IPv4 地址的客户端可以连接到纯 IPv4 或双栈云安全智能防护服务器。
   使用 IPv6 地址的客户端可以连接到纯 IPv6 或双栈云安全智能防护服务器。
   使用 IPv4 和 IPv6 地址的客户端可以连接到任意云安全智能防护服务器。

7. 在**代理服务器设置**部分中，指定将用于连接到云安全智能防护服务器的代理服务器设置客户端。

a. 选择**使用代理服务器进行客户端和云安全智能防护服务器通信**。

b. 指定代理服务器名称或 IPv4/IPv6 地址，以及端口号。

c. 如果代理服务器要求认证，请键入用户名和密码。

8. 在**定制云安全智能防护服务器列表**中，添加云安全智能防护服务器。

a. 指定云安全智能防护服务器的主机名或 IPv4/IPv6 地址。如果指定的是 IPv6 地址，则使用括号将该地址括起来。



注意

如果有 IPv4 和 IPv6 客户端连接到云安全智能防护服务器，请指定主机名。

b. 选择**文件信誉服务**。客户端使用 HTTP 或 HTTPS 协议发送扫描查询。HTTPS 的连接更安全，而 HTTP 使用的带宽更小。

i. 如果希望客户端使用 HTTP，请键入服务器的 HTTP 请求侦听端口。如果希望客户端使用 HTTPS，请选择 **SSL** 并键入服务器的 HTTPS 请求侦听端口。

ii. 单击**测试连接**，检查是否可以建立到服务器的连接。



提示

侦听端口构成服务器地址的一部分。获取服务器地址：

对于集成服务器，打开防毒墙网络版 Web 控制台，然后转至**管理** > **云安全智能防护** > **集成服务器**。

对于独立型服务器，打开独立型服务器的控制台，然后转至摘要窗口。

c. 选择 **Web 信誉服务**。客户端使用 HTTP 协议发送 Web 信誉查询。不支持 HTTPS。

i. 键入服务器的 HTTP 请求侦听端口。

ii. 单击**测试连接**，检查是否可以建立到服务器的连接。

d. 单击**添加到列表**。

e. 通过重复以上步骤来添加更多服务器。

f. 选择**顺序**或**随机**。

- **顺序**：客户端按服务器在列表中出现的顺序选取服务器。如果选择**顺序**，请使用**顺序**列下的箭头将服务器在列表中上下移动。
- **随机**：客户端随机选取服务器。



提示

由于集成型云安全智能防护服务器和防毒墙网络版服务器在同一台计算机上运行，因此在这两个服务器的流量高峰期计算机的性能可能会大大降低。要减少定向到防毒墙网络版服务器计算机的流量，请将独立型云安全智能防护服务器指定为主要云安全智能防护源，并将集成服务器指定为备份源。

g. 在窗口中执行其他任务。

- 要刷新服务器的服务状态，请单击**刷新**。
- 要打开云安全智能防护服务器的控制台，请单击**启动控制台**。
  - 对于集成型云安全智能防护服务器，将显示服务器的配置窗口。
  - 对于独立型云安全智能防护服务器和其他防毒墙网络版服务器的集成型云安全智能防护服务器，将显示控制台登录窗口。
- 要删除某个条目，请单击**删除**（ 

）。

9. 单击**保存**。

窗口随即关闭。刚才添加的列表显示为 **IP 范围**表下的 IP 范围链接。

10. 重复步骤 4 到步骤 8 以添加更多定制列表。

11. 在窗口中执行其他任务。

- 要修改列表，请单击 IP 范围链接，然后在打开的窗口中修改设置。
- 要将列表导出到 .dat 文件，请单击**导出**，然后单击**保存**。

- 如果已从其他服务器导出列表，并希望将该列表导入到此窗口，请单击**导入**并找到该 .dat 文件。该列表将加载到窗口中。

12. 单击**通知所有客户端**。

客户端连接代理服务器设置

如果连接到云安全智能防护网络需要代理服务器认证，请指定认证凭证。有关详细信息，请参阅防毒墙网络版客户端的外部代理服务器 第 14-46 页。

配置内部代理服务器设置，以便客户端在连接到云安全智能防护服务器时使用。有关详细信息，请参阅防毒墙网络版客户端的内部代理服务器 第 14-44 页。

终端位置设置

防毒墙网络版包括位置感知功能，可识别客户端计算机的位置，确定客户端连接到云安全智能防护网络还是云安全智能防护服务器。这样可确保无论客户端处于什么位置，都可以受到保护。

要配置位置设置，请参阅终端位置 第 14-2 页。

趋势科技网络病毒墙安装

如果安装了趋势科技™ 网络病毒墙™：

- 安装 Hot Fix（网络病毒墙 2500 为 Build 1047，网络病毒墙 1200 为 Build 1013）。
- 将 OPSWAT 引擎更新到 2.5.1017 版，使产品可以检测客户端的扫描方法。

使用云安全智能防护服务

正确设置云安全智能防护环境后，客户端便准备好使用文件信誉服务和 Web 信誉服务。还可以开始配置云安全智能反馈设置。



注意

有关设置云安全智能防护环境的说明，请参阅设置云安全智能防护服务 第 4-11 页。

要受益于由文件信誉服务提供的防护，客户端必须使用称为云安全扫描的扫描方法。有关云安全扫描以及如何在客户端上启用云安全扫描的详细信息，请参阅扫描方法类型 第 7-7 页。

要允许防毒墙网络版客户端使用 Web 信誉服务，请配置 Web 信誉策略。有关详细信息，请参阅 Web 信誉策略 第 11-4 页。



注意

扫描方法和 Web 信誉策略的设置是粒度化的。根据您的需求，可以配置适用于所有客户端的设置，也可以为各个客户端或客户端组配置单独的设置。

有关配置云安全智能反馈的说明，请参阅云安全智能反馈 第 13-58 页。

第 5 章

安装防毒墙网络版客户端

本章介绍防毒墙网络版系统要求和防毒墙网络版客户端安装过程。

有关升级防毒墙网络版客户端的详细信息，请参阅《防毒墙网络版安装和升级指南》。

主题包括：

- 防毒墙网络版客户端全新安装 第 5-2 页
- 安装注意事项 第 5-2 页
- 部署注意事项 第 5-10 页
- 迁移到防毒墙网络版客户端 第 5-56 页
- 安装后 第 5-60 页
- 防毒墙网络版客户端卸载 第 5-63 页

防毒墙网络版客户端全新安装

防毒墙网络版客户端可以安装在运行 Microsoft Windows 平台的计算机上。防毒墙网络版还与各种第三方产品相兼容。

有关系统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/enterprise/officescan.aspx

安装注意事项

安装客户端之前，请先考虑以下因素：

表 5-1. 客户端安装注意事项

注意事项	描述
Windows 功能支持	某些防毒墙网络版客户端功能在特定 Windows 平台上不可用。
IPv6 支持	防毒墙网络版客户端可以安装在双栈或纯 IPv6 客户端上。但是： • 某些可安装防毒墙网络版客户端的 Windows 操作系统不支持 IPv6 寻址。 • 对于某些安装方法，成功安装防毒墙网络版客户端具有特殊的要求。
防毒墙网络版客户端 IP 地址	对于均具有 IPv4 和 IPv6 地址的客户端，您可以选择在客户端向服务器进行注册时将使用的 IP 地址。
例外列表	确保已正确配置以下功能的例外列表： • **行为监控**：将关键的终端应用程序添加到允许的程序列表，以防止防毒墙网络版客户端阻止这些应用程序。有关详细信息，请参阅行为监控例外列表 第 8-5 页。 • **Web 信誉**：将认为安全的 Web 站点添加到允许的 URL 列表，以防止防毒墙网络版客户端阻止对这些 Web 站点的访问。有关详细信息，请参阅 Web 信誉策略 第 11-4 页。

防毒墙网络版客户端功能

终端上的可用防毒墙网络版客户端功能取决于终端的操作系统。

表 5-2. 服务器平台上的防毒墙网络版客户端功能

功能	Windows 操作系统		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
手动扫描、实时扫描和预设扫描	是	是	是
组件更新（手动和预设更新）	是	是	是
更新代理	是	是	是
Web 信誉	是，但缺省情况下在安装服务器期间处于禁用状态	是，但缺省情况下在安装服务器期间处于禁用状态	是，但对 Microsoft Edge 浏览器仅提供有限支持
损害清除服务	是	是	是
防毒墙网络版防火墙	是，但缺省情况下在安装服务器期间处于禁用状态	是，但缺省情况下在安装服务器期间处于禁用状态	是，但缺省情况下在安装服务器期间处于禁用状态，并且不支持应用程序过滤
行为监控	是（32 位），但缺省情况下处于禁用状态	是（32 位），但缺省情况下处于禁用状态	是（64 位），但缺省情况下处于禁用状态
	否（64 位）	是（64 位），但缺省情况下处于禁用状态	

功能	Windows 操作系统		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
下列对象的客户端自我保护： • 注册表项 • 进程	是（32 位），但缺省情况下处于禁用状态	是（32 位），但缺省情况下处于禁用状态	是（64 位），但缺省情况下处于禁用状态
	否（64 位）	是（64 位），但缺省情况下处于禁用状态	
下列对象的客户端自我保护： • 服务 • 文件保护	是	是	是
设备控制 未授权更改阻止服务	是（32 位），但缺省情况下处于禁用状态	是（32 位），但缺省情况下处于禁用状态	是（64 位），但缺省情况下处于禁用状态
	否（64 位）	是（64 位），但缺省情况下处于禁用状态	
数据保护 （包括用于设备控制的数据保护）	是（32 位），但缺省情况下处于禁用状态	是（32 位），但缺省情况下处于禁用状态	是（64 位），但缺省情况下处于禁用状态
	是（64 位），但缺省情况下处于禁用状态	是（64 位），但缺省情况下处于禁用状态	
POP3 邮件扫描	是	是	是
客户端插件管理器	是	是	是
漫游模式	是	是 (Server) 否 (Server Core)	是
云安全智能反馈	是	是	是

表 5-3. 桌面平台上的防毒墙网络版客户端功能

功能	Windows 操作系统				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
手动扫描、实时扫描和预设扫描	是	是	是	是	是
组件更新（手动和预设更新）	是	是	是	是	是
更新代理	是	是	是	是	是
Web 信誉	是	是	是	是，但仅限制对 Windows UI 模式的支持	是
损害清除服务	是	是	是	是	是
防毒墙网络版防火墙	是	是	是	是，但不支持应用程序过滤	是，但不支持应用程序过滤
行为监控	是（32 位）	是（32 位）	是（32 位）	是（32 位）	是（32 位）
	否（64 位）	是（64 位） Vista 64 位支持需要 SP1 或 SP2	是（64 位）	是（64 位）	是（64 位）

功能	WINDOWS 操作系统				
	XP	VISTA	WINDOWS 7	WINDOWS 8/8.1	WINDOWS 10
下列对象的客户端自我保护： • 注册表项 • 进程	是（32 位）	是（32 位）	是（32 位）	是（32 位）	是（32 位）
	否（64 位）	是（64 位） Vista 64 位支持需要 SP1 或 SP2	是（64 位）	是（64 位）	是（64 位）
下列对象的客户端自我保护： • 服务 • 文件保护	是	是	是	是	是
设备控制 未授权更改阻止服务	是（32 位）	是（32 位）	是（32 位）	是（32 位）	是（32 位）
	否（64 位）	是（64 位） Vista 64 位支持需要 SP1 或 SP2	是（64 位）	是（64 位）	是（64 位）
数据保护 （包括用于设备控制的数据保护）	是（32 位）	是（32 位）	是（32 位）	是（32 位），处于桌面模式	是（32 位）
	是（64 位）	是（64 位）	是（64 位）	是（64 位），处于桌面模式	是（64 位）
POP3 邮件扫描	是	是	是	是	是

功能	Windows 操作系统				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
客户端插件管理器	是	是	是	是	是
漫游模式	是	是	是	是	是
云安全智能反馈	是	是	是	是	是

防毒墙网络版客户端安装和 IPv6 支持

此主题讨论将防毒墙网络版客户端安装到双栈或纯 IPv6 客户端时的注意事项。

操作系统

防毒墙网络版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（所有版本）
- Windows 7（所有版本）
- Windows Server 2012（所有版本）
- Windows 8/8.1（所有版本）
- Windows 10（Home、Pro、Education 和 Enterprise 版）

有关系统要求的完整列表，请访问以下 Web 站点：

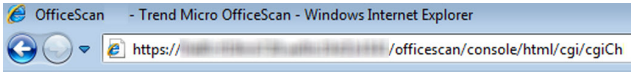
http://docs.trendmicro.com/zh-cn/enterprise/officescan.aspx

安装方法

可以使用所有防毒墙网络版客户端安装方法将防毒墙网络版客户端安装在纯 IPv6 或双栈客户端上。对于某些安装方法，成功安装防毒墙网络版客户端具有特殊的要求。

无法使用 ServerProtect 标准服务器迁移工具将 ServerProtect™ 迁移到防毒墙网络版客户端，因为该工具不支持 IPv6 寻址。

表 5-4. 安装方法和 IPv6 支持

安装方法	要求/考虑事项
Web 安装页面和基于浏览器的安装	安装页面的 URL 包含防毒墙网络版服务器的主机名或其 IP 地址。  如果您要安装到纯 IPv6 客户端，则服务器必须为双栈或纯 IPv6 客户端，而且其主机名或 IPv6 地址必须是 URL 的一部分。 对于双栈客户端，安装状态窗口中显示的 IPv6 地址取决于在**客户端** > **全局客户端设置**的**首选 IP 地址**部分中选择的选项。
客户端打包程序	运行打包程序工具时，您将需要选择是否要将“更新代理”权限分配给客户端。请记住纯 IPv6 更新代理只能将更新分发到纯 IPv6 或双栈客户端。
安全合规、漏洞扫描程序和远程安装	纯 IPv6 服务器无法在纯 IPv4 终端上安装防毒墙网络版客户端。同样，纯 IPv4 服务器也无法在纯 IPv6 终端上安装防毒墙网络版客户端。

客户端 IP 地址

安装在支持 IPv6 寻址的环境中的防毒墙网络版服务器可以管理下列防毒墙网络版客户端：

- 安装在纯 IPv6 主机上的防毒墙网络版服务器可以管理纯 IPv6 客户端。

- 安装在双栈主机上且已指定 IPv4 和 IPv6 地址的防毒墙网络版服务器可以管理纯 IPv6、双栈和纯 IPv4 客户端。

安装或升级客户端之后，客户端会使用 IP 地址向服务器注册。

- 纯 IPv6 客户端会使用其 IPv6 地址进行注册。
- 纯 IPv4 客户端会使用其 IPv4 地址进行注册。
- 双栈客户端会使用其 IPv4 或 IPv6 地址进行注册。您可以选择这些客户端将使用的 IP 地址。

配置双栈客户端向服务器注册时使用的 IP 地址

此设置仅在双栈防毒墙网络版服务器上可用，且仅由双栈客户端应用。

过程

1. 转至**客户端** > **全局客户端设置**。
2. 转到**首选 IP 地址**部分。
3. 从下列选项中选择：
   - **仅 IPv4**：客户端用其 IPv4 地址。
   - **先使用 IPv4，再使用 IPv6**：客户端首先使用其 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**：客户端首先使用其 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。
4. 单击**保存**。

部署注意事项

本节概要介绍执行防毒墙网络版客户端全新安装的不同防毒墙网络版客户端客户端安装方法。所有安装方法都要求目标计算机上的本地管理员权限。

如果您要安装客户端且要启用 IPv6 支持，请阅读防毒墙网络版客户端安装和 IPv6 支持 第 5-7 页中的指南。

表 5-5. 安装的部署注意事项

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
Web 安装页面 除 Windows Server Core 2008 及处于 Windows UI 模式的 Windows 8/8.1/ Server 2012/Server Core 2012 之外，所有操作系统都支持	否	否	是	否	否	高
基于浏览器安装 所有操作系统都支持 **注意** 不支持在 Windows UI 模式下运行的 Windows 8、Windows 8.1 或 Windows Server 2012。	否	否	是	是	否	高，如果安装同时启动

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
基于 UNC 的安装 所有操作系统都支持	否	否	是	是	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 版） • Windows 10 Home 版	否	是	否	是	否	高
登录脚本安装 所有操作系统都支持	否	否	是	是	否	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	否	否	是	是	否	低，如果已预设
客户端打包程序（通过 Microsoft SMS 部署的 MSI 软件包） 所有操作系统都支持	是	是	是/否	是	是	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
客户端打包程序（通过 Active Directory 部署的 MSI 软件包） 所有操作系统都支持	是	是	是/否	是	是	高，如果安装同时启动
客户端磁盘镜像 所有操作系统都支持	否	否	否	是	否	低
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 8/8.1（Basic 版） • Windows 10 Home 版	否	是	否	是	否	高

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
安全合规安装 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 版） • Windows 10 Home 版	否	是	否	是	否	高

Web 安装页面安装

如果已将防毒墙网络版服务器安装到运行以下平台的终端，则用户可以从 Web 安装页面安装防毒墙网络版客户端程序：

- 具有 Internet Information Server (IIS) 6.0 或 Apache 2.0.x 的 Windows Server 2003
- 具有 Internet Information Server (IIS) 7.0 的 Windows Server 2008
- 具有 Internet Information Server (IIS) 7.5 的 Windows Server 2008 R2
- 具有 Internet Information Server (IIS) 8.0 的 Windows Server 2012

要从 Web 安装页安装，您需要以下项：

- 安全级别设置为允许 ActiveX™ 控件的 Internet Explorer。所需版本如下：
  - Windows XP 和 Windows Server 2003 上为 6.0
  - Windows Vista 和 Windows Server 2008 上为 7.0
  - Windows 7 上为 8.0
  - Windows 8/8.1 和 Windows Server 2012 上为 10.0
  - Windows 10 上为 11.0
- 终端上的管理员权限

从 Web 安装页向用户发送以下指令，以安装防毒墙网络版客户端。要通过电子邮件发送安装通知，请参阅启动基于浏览器的安装 第 5-16 页。

从 Web 安装页面安装

过程

1. 使用内置管理员帐户登录到终端。

   注意

   对于 Windows 7、8、8.1 或 10 平台，首先必须启用内置管理员帐户。缺省情况下，Windows 7、8、8.1 和 10 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)。

2. 如果安装到运行 Windows XP、Vista、Server 2008、7、8、8.1、10 或 Server 2012 的终端，请执行以下步骤：

   a. 启动 Internet Explorer 并将防毒墙网络版服务器 URL（如 https://<OfficeScan server name>:4343/officescan）添加到受信任的站点列表。在 Windows XP Home 中，通过转至**工具** > **Internet 选项** > **安全**选项卡，选择**受信任的站点**图标并单击**站点**，访问该列表。

b. 修改 Internet Explorer 安全设置以启用 **ActiveX 控件自动提示**。在 Windows XP 中，转至**工具** > **Internet 选项** > **安全**选项卡，然后单击**自定义级别**。

3. 打开 Internet Explorer 窗口，然后键入：

   https://<OfficeScan server name>:<port>/officescan

4. 单击登录页面的**安装程序**链接显示以下安装选项：

   - **基于浏览器的客户端安装**（仅限 Internet Explorer）：根据您的操作系统窗口上的指导信息操作。
   - **MSI 客户端安装**：根据您的操作系统下载 32 位或 64 位软件包，并按照窗口上的指导信息操作。

   注意

   出现提示时，允许 ActiveX 控件安装。

5. 安装完成后，防毒墙网络版客户端图标会显示在 Windows 系统托盘中。

   注意

   有关在系统托盘上显示的图标的列表，请参阅防毒墙网络版客户端图标 第 14-26 页。

基于浏览器安装

设置用于指示网络上的用户安装防毒墙网络版客户端的电子邮件。用户单击该电子邮件中提供的防毒墙网络版客户端安装程序链接可启动安装。

安装防毒墙网络版客户端前：

- 检查防毒墙网络版客户端安装要求。
- 确定网络上的哪些计算机当前尚不具有抵御安全风险的防护。执行以下任务：

- 运行趋势科技漏洞扫描程序。此工具根据您指定的 IP 地址范围分析终端，查找已安装的防病毒软件。有关详细信息，请参阅漏洞扫描程序用法 第 5-33 页。
- 运行“安全合规”。有关详细信息，请参阅不受管理的终端的安全合规 第 14-62 页。

启动基于浏览器的安装

过程

1. 转至**客户端** > **客户端安装** > **基于浏览器**。
2. 如果需要则修改电子邮件的主题行。
3. 单击**创建电子邮件**。

   将打开缺省邮件程序。
4. 向预期的收件人发送电子邮件。

执行基于 UNC 的安装

AutoPcc.exe 是一个独立程序，将防毒墙网络版客户端安装到不受保护的终端并更新程序文件和组件。终端必须属于域，才能通过统一命名约定 (UNC) 路径使用 AutoPcc。

过程

1. 转至**客户端** > **客户端安装** > **基于 UNC**。
   - 使用 AutoPcc.exe 将防毒墙网络版客户端安装到不受保护的终端：
     a. 连接到服务器计算机。转到 UNC 路径：

        \\<服务器计算机名称>\ofcscan

b. 右键单击 AutoPcc.exe，并选择**以管理员身份运行**。

- 使用 AutoPcc.exe 进行远程桌面安装：

  a. 以控制台模式打开远程桌面连接 (Mstsc.exe)。这强制 AutoPcc.exe 安装在会话 0 中运行。

  b. 转至 \\<服务器计算机名称>\ofscan 目录并执行 AutoPcc.exe。

从防毒墙网络版 Web 控制台远程安装

将防毒墙网络版客户端远程安装到已经连接到网络中的一台或多台终端上。确保您对目标终端具有管理员权限，以执行远程安装。远程安装程序不会在正在运行防毒墙网络版服务器的终端上安装防毒墙网络版客户端。

注意

此安装方法不适用于运行 Windows XP Home、Windows Vista Home Basic 和 Home Premium 版、Windows 7 Home Basic 和 Home Premium 版（32 位和 64 位）、Windows 8/8.1（32 位和 64 位 Basic 版）以及 Windows 10 Home 版的终端。纯 IPv6 服务器无法在纯 IPv4 客户端上安装防毒墙网络版客户端。同样，纯 IPv4 服务器也无法在纯 IPv6 客户端上安装防毒墙网络版客户端。

过程

1. 在您的 Windows 版本上执行以下安装前任务。

   - 如果运行 Windows XP：

     a. 启用内置域管理员帐户并为该帐户设置密码。

     b. 在终端上，转至**我的电脑** > **工具** > **文件夹选项** > **查看**选项卡并禁用**使用简单文件共享**。

     c. 转至**开始** > **程序** > **Windows 防火墙** > **例外**选项卡并启用**文件和打印机共享**例外。

     d. 打开 Microsoft 管理控制台（单击**开始** > **运行**，键入 `services.msc`），然后启动 **Remote Registry** 和 **Remote**

Procedure Call 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。

- 如果运行 Windows Vista：
  a. 启用内置域管理员帐户并为该帐户设置密码。
  b. 单击**开始** > **控制面板** > **安全** > **Windows 防火墙** > **更改设置**。
  c. 单击**例外**选项卡并启用**文件和打印机共享**例外。
  d. 打开 Microsoft 管理控制台（单击**开始** > **运行**，键入 `services.msc`），然后启动 **Remote Registry** 和 **Remote Procedure Call** 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。
- 如果运行 Windows 7、Windows 8（Pro、Enterprise）、Windows 8.1、Windows 10（Pro、Education、Enterprise）或 Windows Server 2012：
  a. 启用内置域管理员帐户并为该帐户设置密码。
  b. 转至**开始** > **程序** > **管理工具** > **高级安全 Windows 防火墙**。
  c. 根据您的网络环境，对“域”、“专用”和/或“公用”启用**文件和打印机共享**规则。
  d. 打开 Microsoft 管理控制台（单击**开始** > **运行**，键入 `services.msc`），然后启动 **Remote Registry** 和 **Remote Procedure Call** 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。

2. 在 Web 控制台上，转至**客户端** > **客户端安装** > **远程**。
3. 选择目标终端。
   - **域和终端**列表显示网络上所有的 Windows 域。双击域名以显示域下的终端。选择任何终端，然后单击**添加**。
   - 如果您记得特定终端的名称，在页面上方的**搜索终端**文本框中键入终端名称，然后按 ENTER。

   防毒墙网络版会提示您输入目标计算机的用户名和密码。使用管理员帐户用户名和密码才能继续。

4. 键入用户名和密码，然后单击**登录**。

   目标终端显示在**选定的终端**表中。

5. 重复步骤 3 和步骤 4，添加多个计算机。

6. 准备好在目标终端上安装防毒墙网络版客户端时，单击**安装**。

   将显示确认框。

7. 单击**是**，确认要在目标终端上安装防毒墙网络版客户端。

   程序文件复制到每个目标终端时，将显示运行窗口。

当防毒墙网络版完成一个目标终端的安装后，该终端名称将在**选定的终端**列表中消失，但显示在**域和终端**列表中，并带红色复选标记。

当所有目标终端带着红色复选标记显示在**域和终端**列表中时，远程安装已完成。

注意

如果安装到多个终端上，防毒墙网络版会在日志中记录不成功的安装（有关详细信息，请参阅全新安装日志 第 16-16 页），但不会推迟其他的安装。单击**安装**后，不必监督安装程序。以后再检查日志以查看安装结果。

使用“登录脚本安装”安装

“登录脚本安装”可以在无保护的终端登录到网络上时，将防毒墙网络版客户端自动安装到这些终端上。“登录脚本安装”会将名为 AutoPcc.exe 的程序添加到服务器登录脚本中。

AutoPcc.exe 将防毒墙网络版客户端安装到不受管理的终端并更新程序文件和组件。终端必须属于域，才能通过登录脚本使用 AutoPcc。

防毒墙网络版客户端安装

当不受保护的 Windows Server 2003 终端登录到您修改过登录脚本的服务器上时，AutoPcc.exe 会自动将防毒墙网络版客户端安装到该终端上。但是，

AutoPcc.exe 不会自动将防毒墙网络版客户端安装到 Windows Vista、7、8、8.1、10、Server 2008 和 Server 2012 计算机上。用户需要连接到服务器计算机，转至 \\<服务器计算机名称>\ofcscan，右键单击 AutoPcc.exe，然后选择**以管理员身份运行**。

使用 AutoPcc.exe 进行远程桌面安装：

- 终端必须在 Mstsc.exe /console mode 下运行。这强制 AutoPcc.exe 安装在会话 0 中运行。
- 将一个驱动器映射到 "ofcscan" 文件夹并从该处执行 AutoPcc.exe。

程序和组件更新

AutoPcc.exe 更新程序文件以及防病毒、防间谍软件和损害清除服务组件。

Windows Server 2003、2008 和 2012 脚本

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，防毒墙网络版将创建一个名为 ofcscan.bat 的批处理文件，包含运行 AutoPcc.exe 的命令。

登录脚本安装将以下内容追加到脚本的末尾：

\\<Server_name>\ofcscan\autopcc

其中：

- <Server_name> 是防毒墙网络版服务器终端的终端名称或 IP 地址。
- "ofcscan" 是服务器上的防毒墙网络版共享文件夹名称。
- "autopcc" 是安装防毒墙网络版客户端的 AutoPcc 可执行文件的链接。

登录脚本位置（通过网络登录共享目录）：

- Windows Server 2003: \\Windows 2003 server\system drive\windir\sysvol\domain\scripts \ofcscan.bat

- Windows Server 2008：\\Windows 2008 server\system drive\windir\sysvol\domain \scripts\ofcscan.bat
- Windows Server 2012：\\Windows 2012 server\system drive\windir\sysvol\domain \scripts\ofcscan.bat

使用登录脚本安装将 Autopcc.exe 添加到登录脚本中

过程

1. 在用于运行服务器安装的终端上，从 Windows“开始”菜单中依次单击**程序** > **趋势科技防毒墙网络版服务器 <服务器名称>** > **登录脚本安装**。

   将加载**登录脚本安装**实用工具。将在控制台上以树形显示网络上的所有域。

2. 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”将提示您输入用户名和密码。

3. 键入用户名和密码。单击**确定**继续。

   将显示**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。

4. 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**。

5. 要修改所有用户的登录脚本，请单击**全部添加**。

6. 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**。

7. 要重置选择，请单击**全部删除**。

8. 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。

9. 单击**确定**。

“登录脚本安装”将返回到其初始窗口。

10. 要修改其他服务器的登录脚本，请重复步骤 2 到 4。

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。用户可以在客户端终端上运行该软件包，以安装或升级防毒墙网络版客户端和更新组件。

当向低带宽远程办公室中的客户端部署防毒墙网络版客户端或组件时，客户端打包程序作用突出。使用客户端打包程序安装的防毒墙网络版客户端会向服务器报告创建软件包的位置。

客户端打包程序的需求如下：

- 350MB 可用磁盘空间
- Windows Installer 2.0 （运行 MSI 软件包）

软件包部署准则

1. 将软件包发送给用户，请他们在终端上通过双击 EXE 或 MSI 文件运行防毒墙网络版客户端软件包。

   注意

   仅把软件包发送给其防毒墙网络版客户端向创建该软件包的服务器报告的用户。

2. 如果您的用户将在运行 Windows Vista、Server 2008、7、8、8.1、10 或 Server 2012 的终端上安装 EXE 软件包，请指示他们右键单击 EXE 文件，然后选择**以管理员身份运行**。

3. 如果已创建 MSI 文件，请通过执行下列任务部署软件包：

- 使用 Active Directory 或 Microsoft SMS。请参阅使用 Active Directory 部署 MSI 软件包 第 5-27 页或使用 Microsoft SMS 部署 MSI 软件包 第 5-28 页。

4. 从命令提示符窗口启动 MSI 软件包，以静默方式将防毒墙网络版客户端安装到运行 Windows XP、Vista、Server 2008、7、8、8.1、10 或 Server 2012 的远程终端。

客户端软件包的扫描方法指南

选择软件包的扫描方法。请参阅扫描方法类型 第 7-7 页以了解详细信息。

软件包中包括的组件取决于所选的扫描方法。有关每种扫描方法可用的组件的详细信息，请参阅防毒墙网络版客户端更新 第 6-26 页。

在选择扫描方法之前，请注意以下准则以帮助您高效部署软件包：

- 如果您将使用软件包将客户端升级到此版本的防毒墙网络版，请在 Web 控制台上检查域级扫描方法。在控制台上，转至**客户端** > **客户端管理**，选择客户端所属的客户端树域，然后单击**设置** > **扫描设置** > **扫描方法**。域级扫描方法应该与软件包的扫描方法一致。
- 如果您将使用软件包执行防毒墙网络版客户端的全新安装，请检查客户端分组设置。在 Web 控制台上，转至**客户端** > **客户端分组**。
- 如果按 NetBIOS、Active Directory 或 DNS 域对客户端进行分组，则检查目标终端所属的域。如果该域存在，请检查为该域配置的扫描方法。如果该域不存在，请检查根级扫描方法（选择客户端树中的根域图标 ()，然后单击**设置** > **扫描设置** > **扫描方法**）。域级或根级扫描方法应该与软件包的扫描方法一致。

- 如果按定制客户端组对客户端进行分组，则检查**分组优先级**和**源**。

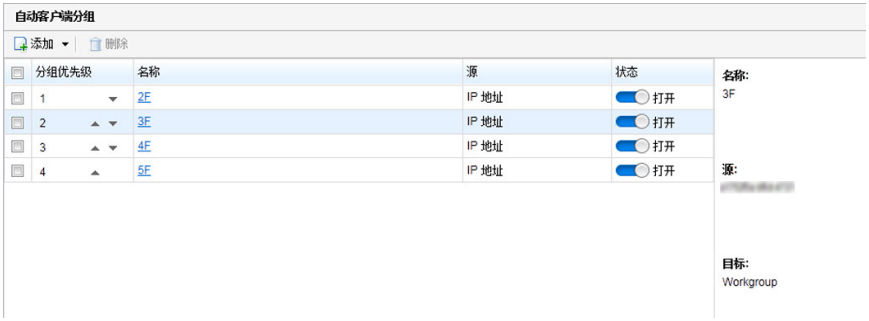


图 5-1. “自动客户端分组”预览窗格

如果目标终端属于特定源，则检查相应的**目标**。该目标是显示在客户端树中的域名。客户端将在安装后对该域应用扫描方法。

- 如果将使用软件包在使用此版本的防毒墙网络版的客户端上更新组件，请检查为客户端所属的客户端树域配置的扫描方法。域级扫描方法应该与软件包的扫描方法一致。

使用客户端打包程序创建安装软件包

过程

1. 在防毒墙网络版服务器计算机上，浏览到 <服务器安装文件夹>\PCCSRV\Admin\Utility\ClientPackager。
2. 双击 ClnPack.exe 运行该工具。

   客户端打包程序控制台将打开。
3. 选择要创建的软件包类型。

表 5-6. 客户端软件包类型

软件包类型	描述
安装	选择**安装**可将软件包创建为可执行文件。软件包安装防毒墙网络版客户端程序以及服务器上当前可用的组件。如果目标终端已安装早期版本的客户端，运行可执行文件将升级客户端。
更新	选择**更新**可创建一个包含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。如果在任何客户端终端上更新组件时存在问题，请使用此软件包。
MSI	选择 **MSI** 可创建一个符合 Microsoft Installer 软件包格式的软件包。软件包还将安装防毒墙网络版客户端程序以及服务器上当前可用的组件。如果目标终端已安装早期版本的客户端，运行 MSI 文件将升级客户端。

4. 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此操作系统类型的终端。创建另一个软件包以部署到其他操作系统类型。

5. 选择客户端软件包部署的扫描方法。

   有关如何选择扫描方法的指南，请参阅客户端软件包的扫描方法指南 第 5-23 页。

6. 在**域**下，选择以下操作之一：

   - **允许客户端自动报告其域**：安装防毒墙网络版客户端之后，客户端将查询防毒墙网络版服务器数据库并将其域设置报告给服务器。
   - 列表中的任何域：客户端打包程序与防毒墙网络版服务器同步，并列出客户端树中当前使用的域。

7. 在**选项**下，从以下选项中选择：

选项	说明
静默方式	此选项创建在客户端终端后台安装的软件包，客户端注意不到，也不显示安装状态窗口。如果打算将软件包远程部署到目标终端，请启用此选项。
强制用最新版本覆盖	此选项用服务器上当前可用的版本覆盖客户端上的组件版本。启用此选项可确保服务器和客户端上的组件保持同步。

选项	说明
禁用预扫描（仅用于全新安装）	如果目标终端未安装防毒墙网络版客户端，则软件包在安装防毒墙网络版客户端之前先扫描终端以查找安全风险。如果您确信目标终端没有感染安全风险，请禁用预扫描。 如果启用预扫描，则安装程序将扫描终端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. 在**更新代理功能**下，选择更新代理可部署的功能。

9. 在**组件**下，选择要包含在软件包中的组件和功能。

   - 有关组件的详细信息，请参阅防毒墙网络版组件与程序 第 6-2 页。
   - 仅当您安装并激活数据保护之后，才能使用数据保护模块。有关数据保护的详细信息，请参阅数据保护入门 第 3-1 页。

10. 再选择**源文件**，确保 ofcscan.ini 文件的位置正确。要修改该路径，单击 (...) 以浏览 ofcscan.ini 文件。

    缺省情况下，此文件位于防毒墙网络版服务器的 <服务器安装文件夹>\PCCSRV 文件夹中。

11. 在**输出文件**中，单击 (...) 指定要创建防毒墙网络版客户端软件包的位置，并键入软件包文件名（例如，`AgentSetup.exe`）。

12. 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。

13. 部署软件包。

使用 Active Directory 部署 MSI 软件包

利用 Active Directory 的功能将 MSI 软件包同时部署到多个客户端终端。

有关创建 MSI 文件的指导信息，请参阅使用客户端打包程序安装 第 5-22 页。

过程

1. 执行以下操作：
   - 对于 Windows Server 2003 和早期版本：
     a. 打开 Active Directory 控制台。
     b. 右键单击您要将 MSI 软件包部署到的组织单元 (OU)，然后单击**属性**。
     c. 单击**组策略**选项卡中的**新建**。
   - 对于 Windows Server 2008 和 Windows Server 2008 R2：
     a. 打开**组策略管理控制台**。单击**开始** > **控制面板** > **管理工具** > **组策略管理**。
     b. 在控制台树中，展开包含要编辑的 GPO 的林和域中的**组策略对象**。
     c. 右键单击要编辑的 GPO，然后单击**编辑**。这将打开**组策略对象编辑器**。
   - 对于 Windows Server 2012：
     a. 打开**组策略管理控制台**。单击**服务器管理** > **工具** > **组策略管理**。
     b. 在控制台树中，展开包含要编辑的 GPO 的林和域中的**组策略对象**。
     c. 右键单击要编辑的 GPO，然后单击**编辑**。这将打开**组策略对象编辑器**。
2. 在**计算机配置**和**用户配置**之间选择一个，然后打开下面的**软件设置**。

提示

趋势科技建议使用**计算机配置**，而不使用**用户配置**，以确保无论哪个登录到该终端的用户都可成功安装 MSI 软件包。

3. 在**软件设置**下面，右键单击**软件安装**，然后选择**新建**和**程序包**。
4. 查找并选择 MSI 软件包。
5. 选择部署方法，然后单击**确定**。
   - **已分配**：下次用户登录到终端（如果您选择“用户配置”）或终端重新启动（如果您选择“计算机配置”）时，MSI 软件包将自动部署。此方法不需要任何用户干预。
   - **已发布**：要运行 MSI 软件包，通知用户转到“控制面板”，打开“添加/删除程序”窗口，然后选择在网络上添加/删除程序的选项。显示防毒墙网络版客户端 MSI 软件包时，用户可继续安装防毒墙网络版客户端。

使用 Microsoft SMS 部署 MSI 软件包

如果服务器上安装了 Microsoft BackOffice SMS，请使用 Microsoft System Management Server (SMS) 部署 MSI 软件包。

有关创建 MSI 文件的指导信息，请参阅使用客户端打包程序安装 第 5-22 页。

SMS 服务器需要先从防毒墙网络版服务器获取 MSI 文件，然后才能将软件包部署到目标终端。

- 本地：SMS 服务器和防毒墙网络版服务器在同一个终端上。
- 远程：SMS 服务器和防毒墙网络版服务器在不同终端上。

与 Microsoft SMS 一起安装时的已知问题：

- SMS 控制台的**运行时间**列将显示“未知”。
- 如果安装不成功，SMS 程序的监控程序上安装状态可能仍然显示安装已完成。

有关如何检查是否成功安装的指导信息，请参阅安装后 第 5-60 页。

如果您使用 Microsoft SMS 2.0 和 2003，以下指导信息将适用。

本地获取软件包

过程

1. 打开 **SMS 管理员**控制台。
2. 单击**树**选项卡的**软件包**。
3. 在**操作**菜单上，单击**新建** > **软件包（从定义）**。

   将显示**从定义创建软件包向导**的**欢迎**窗口。
4. 单击**下一步**。

   将显示**软件包定义**窗口。
5. 单击**浏览**。

   将显示**打开**窗口。
6. 浏览并选择由客户端打包程序创建的 MSI 软件包文件，然后单击**打开**。

   软件包定义窗口将显示 MSI 软件包名称。此软件包将显示“防毒墙网络版客户端”和程序版本。
7. 单击**下一步**。

   将显示**源文件**窗口。
8. 单击**总是从源目录获取文件**，然后单击**下一步**。

   将显示**源目录**窗口，显示您要创建的软件包名称和源目录。
9. 单击**站点服务器上的本地驱动器**。
10. 单击**浏览**，然后选择包含该 MSI 文件的源目录。
11. 单击**下一步**。

向导将创建软件包。完成此过程后，软件包名称将出现在 **SMS 管理员**控制台上。

远程获取软件包

过程

1. 在防毒墙网络版服务器上，使用客户端打包程序创建具有 EXE 扩展名的“安装”软件包（不可创建 MSI 软件包）。请参阅使用客户端打包程序安装 第 5-22 页以了解详细信息。
2. 在您要存储源文件的终端上，创建一个共享文件夹。
3. 打开 SMS 管理员控制台。
4. 单击**树**选项卡的**软件包**。
5. 在**操作**菜单上，单击**新建** > **软件包（从定义）**。

   将显示**从定义创建软件包向导**的**欢迎**窗口。
6. 单击**下一步**。

   将显示**软件包定义**窗口。
7. 单击**浏览**。

   将显示**打开**窗口。
8. 浏览 MSI 软件包文件。此文件位于您创建的共享文件夹上。
9. 单击**下一步**。

   将显示**源文件**窗口。
10. 单击**总是从源目录获取文件**，然后单击**下一步**。

    将显示**源目录**窗口。
11. 单击**网络路径（UNC 名）**。
12. 单击**浏览**，然后选择包含该 MSI 文件的源目录（您创建的共享文件夹）。

13. 单击**下一步**。

    向导将创建软件包。完成此过程后，软件包名称将出现在 **SMS 管理员**控制台上。

将软件包分发至目标终端

过程

1. 单击**树**选项卡的**公布**。
2. 在**操作**菜单上，单击**所有任务** > **分发软件**。

   将显示**分发软件向导**的**欢迎**窗口。
3. 单击**下一步**。

   将显示**软件包**窗口。
4. 单击**分发现有软件包**，然后单击您创建的“安装”软件包的名称。
5. 单击**下一步**。

   将显示**分发点**窗口。
6. 选择您要复制此软件包的一个分发点，然后单击**下一步**。

   将显示**公布程序**窗口。
7. 单击**是**公布防毒墙网络版客户端“安装”软件包，然后单击**下一步**。

   将显示**公布目标**窗口。
8. 单击**浏览**选择目标终端。

   将显示**浏览集合**窗口。
9. 单击**所有 Windows NT 系统**。
10. 单击**确定**。

    将再次显示**公布目标**窗口。

11. 单击**下一步**。

    将显示**公布名称**窗口。

12. 在文本框中键入名称和您对此公布的注释，然后单击**下一步**。

    将显示**公布至子集**窗口。

13. 选择是否将此软件包公布至子集。选择仅将此程序公布至指定集合或子集的成员。

14. 单击**下一步**。

    将显示**公布时间表**窗口。

15. 通过键入或选择日期和时间指定何时公布防毒墙网络版客户端“安装”软件包。

    注意

    如果您希望 Microsoft SMS 在特定日期停止公布软件包，请单击**是。此公布应到期**，然后在**到期日期和时间**列表框中指定日期和时间。

16. 单击**下一步**。

    将显示**指定程序**窗口。

17. 单击**是，指定此程序**，然后单击**下一步**。

    Microsoft SMS 将创建此公布并显示在 SMS 管理员控制台上。

18. 当 Microsoft SMS 分发此公布程序（即防毒墙网络版客户端程序）至目标终端时，每个目标终端上都将显示一个窗口。指导用户单击**是**，然后遵循向导提供的指令，把防毒墙网络版客户端安装到他们的终端上。

使用客户端磁盘镜像安装

通过磁盘镜像技术，可以使用磁盘镜像软件创建某个防毒墙网络版客户端的镜像并在网络中的其他计算机上进行复制。

每个防毒墙网络版客户端安装都需要一个全局唯一标识号 (GUID)，这样服务器就可以分别识别客户端。使用名为 imgsetup.exe 的防毒墙网络版程序来为每个副本创建不同的 GUID。

创建防毒墙网络版客户端的磁盘镜像

过程

1. 在终端上安装防毒墙网络版客户端。
2. 将 ImgSetup.exe 从 <服务器安装文件夹>\PCCSRV\Admin\Utility\ImgSetup 复制到此终端。
3. 在此终端上运行 ImgSetup.exe。

   将在 HKEY_LOCAL_MACHINE 下创建一个 RUN 注册码。
4. 使用磁盘镜像软件创建防毒墙网络版客户端的磁盘镜像。
5. 重新启动复制。

   ImgSetup.exe 将自动启动并创建一个新的 GUID 值。防毒墙网络版客户端会将此新的 GUID 报告给服务器，而服务器将为新的防毒墙网络版客户端创建一个新的记录。

警告!

为避免防毒墙网络版数据库中两个计算机具有相同的名称，请手动更改被复制的防毒墙网络版客户端的终端名称或域名。

漏洞扫描程序用法

使用漏洞扫描程序可以检测安装的防病毒解决方案、在网络上搜索未受保护的计算机，以及将防毒墙网络版客户端安装到计算机。

使用漏洞扫描程序时的注意事项

为帮助您决定是否使用漏洞扫描程序，请考虑以下因素：

- 网络管理 第 5-34 页
- 网络拓扑和体系结构 第 5-35 页
- 软件/硬件规格 第 5-35 页
- 域结构 第 5-35 页
- 网络通信 第 5-36 页
- 网络规模 第 5-36 页

网络管理

表 5-7. 网络管理

安装	漏洞扫描程序的效力
具有严格安全策略的管理	非常高效。漏洞扫描程序会报告是否所有计算机已安装防病毒软件。
分布在不同地点的管理职责	效率中等
集中式管理	效率中等
外包服务	效率中等
用户管理自己的计算机	效率不高。由于漏洞扫描程序会扫描网络的防病毒安装程序，因此让用户扫描自己的计算机并不可行。

网络拓扑和体系结构

表 5-8. 网络拓扑和体系结构

安装	漏洞扫描程序的效力
单个位置	非常高效。通过漏洞扫描程序可以扫描整个 IP 段，还可以轻松地在 LAN 上安装防毒墙网络版客户端。
具有高速连接的多个位置	效率中等
具有低速连接的多个位置	效率不高。需要在各个位置上运行漏洞扫描程序并且防毒墙网络版客户端安装程序必须指向本地防毒墙网络版服务器。
远程计算机和隔离的计算机	效率中等

软件/硬件规格

表 5-9. 软件/硬件规格

安装	漏洞扫描程序的效力
基于 Windows NT 的操作系统	非常高效。漏洞扫描程序可以轻松地将防毒墙网络版客户端远程安装到运行基于 NT 操作系统的计算机。
混合操作系统	效率中等。漏洞扫描程序仅能将防毒墙网络版客户端安装到运行基于 Windows NT 操作系统的计算机。
桌面管理软件	效率不高。漏洞扫描程序不能和桌面管理软件一起使用。但是，它可以帮助跟踪防毒墙网络版客户端安装的进度。

域结构

表 5-10. 域结构

安装	漏洞扫描程序的效力
Microsoft Active Directory	非常高效。在漏洞扫描程序中指定域管理员帐户以允许远程安装防毒墙网络版客户端。

安装	漏洞扫描程序的效力
Workgroup	效率不高。漏洞扫描程序使用不同管理帐户和密码将防毒墙网络版客户端安装到这些计算机时，可能会有困难。
Novell™ 目录服务	效率不高。漏洞扫描程序需要 Windows 域帐户来安装防毒墙网络版客户端。
对等	效率不高。漏洞扫描程序使用不同管理帐户和密码将防毒墙网络版客户端安装到这些计算机时，可能会有困难。

网络通信

表 5-11. 网络通信

安装	漏洞扫描程序的效力
LAN 连接	非常高效
512 Kbps	效率中等
T1 连接或更高	效率中等
拨号	效率不高。要花很长时间才可以完成防毒墙网络版客户端的安装。

网络规模

表 5-12. 网络规模

安装	漏洞扫描程序的效力
超大型企业	非常高效。网络规模越大，越需要漏洞扫描程序来检查防毒墙网络版客户端安装。
中小企业	效率中等。对于小型网络，漏洞扫描程序可以是安装防毒墙网络版客户端的一个选项。其他防毒墙网络版客户端的安装方法更加容易执行。

使用漏洞扫描程序安装防毒墙网络版客户端时的准则

如果存在以下情况，则漏洞扫描程序将不安装防毒墙网络版客户端：

- 目标主机上已安装防毒墙网络版服务器或其他安全软件。
- 远程终端运行的是 Windows XP Home、Windows Vista Home Basic、Windows Vista Home Premium、Windows 7 Home Basic、Windows 7 Home Premium、Windows 8（Basic 版）、Windows 8.1（Basic 版）或 Windows 10 Home。

注意

可以使用部署注意事项 第 5-10 页中讨论的其他安装方法，将防毒墙网络版客户端安装到目标主机。

使用漏洞扫描程序安装防毒墙网络版客户端之前，请执行以下步骤：

- 对于 Windows Vista（Business、Enterprise 或 Ultimate Edition）或 Windows 7（Professional、Enterprise 或 Ultimate Edition）、Windows 8（Pro、Enterprise）、Windows 8.1（Pro、Enterprise）、Windows 10（Pro、Education、Enterprise）或 Windows Server 2012 (Standard)：
  1. 启用内置管理员帐户并为该帐户设置密码。
  2. 单击**开始** > **程序** > **管理工具** > **高级安全 Windows 防火墙**。
  3. 针对域概要文件、专用概要文件和通用概要文件，将防火墙状态设置为“关闭”。
  4. 打开 Microsoft 管理控制台（单击**开始** > **运行**，键入 `services.msc`），然后启动**远程注册表**服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。
- 对于 Windows XP Professional（32 位或 64 位版本）：
  1. 打开 Windows 资源管理器，然后单击**工具** > **文件夹选项**。
  2. 单击**查看**选项卡并禁用**使用简单文件共享（推荐）**。

漏洞扫描方法

漏洞扫描可检查主机上是否有安全软件，并将防毒墙网络版客户端安装到未受保护的主机中。

有多种方法可以运行漏洞扫描。

表 5-13. 漏洞扫描方法

方法	详细信息
手动漏洞扫描	管理员可按需运行漏洞扫描。
DHCP 扫描	管理员可以在从 DHCP 服务器请求 IP 地址的主机上运行漏洞扫描。 漏洞扫描程序侦听端口 67（DHCP 服务器侦听 DHCP 请求的端口）。如果它检测到来自主机的 DHCP 请求，则会在该计算机上运行漏洞扫描。  **注意** 如果在 Windows Server 2008、Windows 7、Windows 8、Windows 8.1、Windows 10 或 Windows Server 2012 上启动漏洞扫描程序，则该扫描程序无法检测 DHCP 请求。
预设漏洞扫描	系统会根据管理员配置的时间表自动运行漏洞扫描。

漏洞扫描程序运行之后，它会在目标主机上显示防毒墙网络版客户端的状态。状态可能是以下任一选项：

- **正常**：防毒墙网络版客户端已启动并运行，且工作正常
- **异常**：防毒墙网络版客户端服务未运行，或客户端无实时防护
- **未安装**：TMListen 服务丢失或尚未安装防毒墙网络版客户端
- **无法访问**：漏洞扫描程序无法与主机建立连接并确定防毒墙网络版客户端的状态

运行手动漏洞扫描

过程

1. 要在防毒墙网络版服务器计算机上运行漏洞扫描，请导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\TMVS，然后双击 TMVS.exe。将显示**趋势科技漏洞扫描程序**控制台。在另一台运行 Windows Server 2003、Server 2008、Vista、7、8、8.1、10 或 Server 2012 的终端上运行漏洞扫描：

   a. 在防毒墙网络版服务器计算机上，转到 <服务器安装文件夹>\PCCSRV\Admin\Utility。

   b. 将 TMVS 文件夹复制到其他终端。

   c. 在其他终端上，打开 TMVS 文件夹，然后双击 TMVS.exe。

      将显示**趋势科技漏洞扫描程序**控制台。

   注意

   无法从终端服务器启动该工具。

2. 转至**手动扫描**部分。

3. 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 或双栈主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**。

   将显示**设置**窗口。

5. 配置下列设置：

选项	说明
Ping 设置	漏洞扫描可以 "ping" 在上一步中指定的 IP 地址，以确认这些地址当前是否正在使用中。如果目标主机正在使用某个 IP 地址，则漏洞扫描程序可以确定该主机的操作系统。 有关详细信息，请参阅 Ping 设置 第 5-52 页。
检索计算机描述的方法	对于响应 "ping" 命令的主机，漏洞扫描程序可以检索这些主机的其他相关信息。 有关详细信息，请参阅检索终端描述的方法 第 5-49 页。
产品查询	漏洞扫描程序可以检查目标主机上是否有安全软件。 有关详细信息，请参阅产品查询 第 5-46 页。
防毒墙网络版服务器设置	如果希望漏洞扫描程序自动将防毒墙网络版客户端 安装到未受保护的主机，则可配置这些设置。这些设置可识别防毒墙网络版客户端的父服务器以及用来登录主机的管理凭证。 有关详细信息，请参阅防毒墙网络版服务器设置 第 5-53 页。 **注意** 某些情况可能会阻止防毒墙网络版客户端安装到目标主机中。 有关详细信息，请参阅使用漏洞扫描程序安装防毒墙网络版客户端时的准则 第 5-37 页。
通知	漏洞扫描程序可将漏洞扫描结果发送给防毒墙网络版管理员。它还可以在未受保护的主机上显示通知。 有关详细信息，请参阅通知 第 5-50 页。
保存结果	除了将漏洞扫描结果发送给管理员之外，漏洞扫描还可以将结果保存为 .csv 文件。 有关详细信息，请参阅漏洞扫描结果 第 5-51 页。

6. 单击**确定**。

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

   如果终端运行的是 Windows Server 2008 或 Windows Server 2012，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

过程

1. 在以下文件夹下找到的 TMVS.ini 文件中配置 DHCP 设置：<服务器安装文件夹>\PCCSRV\Admin\Utility\TMVS。

   表 5-14. 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 8。
DhcpDelayScan=x	这是检查请求终端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 30。
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防毒墙网络版服务器。日志显示在 Web 控制台的 **系统事件日志**窗口中。
OsceServer=x	这是防毒墙网络版服务器的 IP 地址或 DNS 名称。
OsceServerPort=x	这是防毒墙网络版服务器上的 Web 服务器端口。

2. 要在防毒墙网络版服务器计算机上运行漏洞扫描，请导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\TMVS，然后双击 TMVS.exe。将显示**趋势科**

技漏洞扫描程序控制台。在另一台运行 Windows Server 2003、Server 2008、Vista、7、8、8.1、10 或 Server 2012 的终端上运行漏洞扫描：

a. 在防毒墙网络版服务器计算机上，转到 <服务器安装文件夹>\PCCSRV\Admin\Utility。

b. 将 TMVS 文件夹复制到其他终端。

c. 在其他终端上，打开 TMVS 文件夹，然后双击 TMVS.exe。

将显示**趋势科技漏洞扫描程序**控制台。

注意

无法从终端服务器启动该工具。

3. 在**手动扫描**部分下，单击**设置**。

将显示**设置**窗口。

4. 配置下列设置：

选项	说明
产品查询	漏洞扫描程序可以检查目标主机上是否有安全软件。 有关详细信息，请参阅产品查询 第 5-46 页。
防毒墙网络版服务器设置	如果希望漏洞扫描程序自动将防毒墙网络版客户端 安装到未受保护的主机，则可配置这些设置。这些设置可识别防毒墙网络版客户端的父服务器以及用来登录主机的管理凭证。 有关详细信息，请参阅防毒墙网络版服务器设置 第 5-53 页。 **注意** 某些情况可能会阻止防毒墙网络版客户端安装到目标主机中。 有关详细信息，请参阅使用漏洞扫描程序安装防毒墙网络版客户端时的准则 第 5-37 页。
通知	漏洞扫描程序可将漏洞扫描结果发送给防毒墙网络版管理员。它还可以在未受保护的主机上显示通知。 有关详细信息，请参阅通知 第 5-50 页。

选项	说明
保存结果	除了将漏洞扫描结果发送给管理员之外，漏洞扫描还可以将结果保存为 .csv 文件。 有关详细信息，请参阅漏洞扫描结果 第 5-51 页。

5. 单击**确定**。
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、Windows 7、Windows 8、Windows 8.1、Windows 10 和 Windows Server 2012 的计算机上不可用。

7. 单击**开始**。

   漏洞扫描程序开始侦听 DHCP 请求并在计算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

过程

1. 要在防毒墙网络版服务器计算机上运行漏洞扫描，请导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\TMVS，然后双击 TMVS.exe。将显示**趋势科技漏洞扫描程序**控制台。在另一台运行 Windows Server 2003、Server 2008、Vista、7、8、8.1、10 或 Server 2012 的终端上运行漏洞扫描：

   a. 在防毒墙网络版服务器计算机上，转到 <服务器安装文件夹>\PCCSRV\Admin\Utility。

   b. 将 TMVS 文件夹复制到其他终端。

   c. 在其他终端上，打开 TMVS 文件夹，然后双击 TMVS.exe。

      将显示**趋势科技漏洞扫描程序**控制台。

注意

无法从终端服务器启动该工具。

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**时间表**的开始时间，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. 选择一组要使用的漏洞扫描设置。

   a. 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 5-39 页。

   b. 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**。

将显示**设置**窗口。

c. 配置下列设置：

Ping 设置	漏洞扫描可以 "ping" 在上一步中指定的 IP 地址，以确认这些地址当前是否正在使用中。如果目标主机正在使用某个 IP 地址，则漏洞扫描程序可以确定该主机的操作系统。 有关详细信息，请参阅 Ping 设置 第 5-52 页。
检索计算机描述的方法	对于响应 "ping" 命令的主机，漏洞扫描程序可以检索这些主机的其他相关信息。 有关详细信息，请参阅检索终端描述的方法 第 5-49 页。
产品查询	漏洞扫描程序可以检查目标主机上是否有安全软件。 有关详细信息，请参阅产品查询 第 5-46 页。
防毒墙网络版服务器设置	如果希望漏洞扫描程序自动将防毒墙网络版客户端 安装到未受保护的主机，则可配置这些设置。这些设置可识别防毒墙网络版客户端的父服务器以及用来登录主机的管理凭证。 有关详细信息，请参阅防毒墙网络版服务器设置 第 5-53 页。 **注意** 某些情况可能会阻止防毒墙网络版客户端安装到目标主机中。 有关详细信息，请参阅使用漏洞扫描程序安装防毒墙网络版客户端时的准则 第 5-37 页。
通知	漏洞扫描程序可将漏洞扫描结果发送给防毒墙网络版管理员。它还可以在未受保护的主机上显示通知。 有关详细信息，请参阅通知 第 5-50 页。
保存结果	除了将漏洞扫描结果发送给管理员之外，漏洞扫描还可以将结果保存为 .csv 文件。 有关详细信息，请参阅漏洞扫描结果 第 5-51 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

   如果终端运行的是 Windows Server 2008 或 Windows Server 2012，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**。

漏洞扫描设置

漏洞扫描设置是从趋势科技漏洞扫描程序 (TMVS.exe) 或 TMVS.ini 文件进行配置的。

注意

有关如何收集漏洞扫描程序的调试日志的信息，请参阅服务器调试日志（使用 LogServer.exe） 第 16-3 页。

产品查询

漏洞扫描程序可以检查客户端上是否有安全软件。下表讨论漏洞扫描程序检查安全产品的方法：

表 5-15. 漏洞扫描程序检查的安全产品

产品	描述
防毒墙服务器版 for Windows	漏洞扫描程序使用 RPC 终端来检查 SPNTSVC.exe 是否正在运行。它返回包括操作系统及病毒扫描引擎、病毒码和产品版本在内的信息。漏洞扫描程序无法检测防毒墙服务器版信息服务器或防毒墙服务器版管理控制台。

产品	描述
防毒墙服务器版 for Linux	如果目标终端没有运行 Windows，则漏洞扫描程序通过尝试连接到端口 14942 来检查其是否安装了防毒墙服务器版 for Linux。
防毒墙网络版客户端	漏洞扫描程序使用防毒墙网络版客户端的端口来检查是否安装了防毒墙网络版客户端。还检查 TmListen.exe 进程是否正在运行。如果从其缺省位置执行，则自动检索端口号。 如果已在防毒墙网络版服务器之外的任何终端上启动了漏洞扫描程序，请检查其他终端的通信端口，然后使用该端口。
PortalProtect™	漏洞扫描程序加载 Web 页面 http://localhost:port/PortalProtect/index.html 来检查产品安装。
防毒墙群件版™ for Microsoft Exchange™	漏洞扫描程序加载 Web 页面 http://ipaddress:port/scanmail.html 来检查防毒墙群件版安装。缺省情况下，ScanMail 使用端口 16372。如果 ScanMail 使用不同端口号，则指定端口号。否则，漏洞扫描程序无法检测到防毒墙群件版。
InterScan™ 系列	对于不同的产品，漏洞扫描程序加载各自的 Web 页面检查产品安装。 • 趋势科技防毒墙邮件安全版 5.x：http://localhost:port/eManager/cgi-bin/eManager.htm • InterScan eManager 3.x: http://localhost:port/eManager/cgi-bin/eManager.htm • InterScan VirusWall™ 3.x: http://localhost:port/InterScan/cgi-bin/interscan.dll
趋势科技网络安全版™ (PC-cillin)	漏洞扫描程序使用端口 40116 检查是否安装了趋势科技网络安全版。
McAfee VirusScan ePolicy Orchestrator	漏洞扫描程序向 TCP 端口 8081（提供服务器和客户端之间连接的 ePolicy Orchestrator 缺省端口）发送一个特殊令牌。安装有该防病毒产品的终端使用特殊令牌类型响应。漏洞扫描程序无法检测到独立的 McAfee VirusScan。
Norton Antivirus™ Corporate Edition	漏洞扫描程序向 UDP 端口 2967（Norton Antivirus 企业版 RTVScan 的缺省端口）发送一个特殊令牌。安装有该防病毒产品的终端使用特殊令牌类型响应。由于 Norton Antivirus 企业版通过 UDP 通信，因此不保证精确率。另外，网络通信可能会影响 UDP 等待时间。

漏洞扫描程序使用以下协议检测产品和计算机：

- **RPC**：检测防毒墙服务器版 for NT
- **UDP**：检测 Norton AntiVirus 企业版客户端
- **TCP**：检测 McAfee VirusScan ePolicy Orchestrator
- **ICMP**：通过发送 ICMP 数据包检查计算机
- **HTTP**：检测防毒墙网络版客户端
- **DHCP**：如果它检测到一个 DHCP 请求，则漏洞扫描程序检查请求终端上是否已安装了防病毒软件。

配置产品查询设置

产品查询设置是漏洞扫描设置的子集。有关漏洞扫描设置的详细信息，请参阅漏洞扫描方法 第 5-38 页。

过程

1. 从漏洞扫描程序 (TMVS.exe) 指定产品查询设置：
   a. 启动 TMVS.exe。
   b. 单击**设置**。
      将显示**设置**窗口。
   c. 转至**产品查询**部分。
   d. 选择要检查的产品。
   e. 单击产品名称旁边的**设置**，然后指定漏洞扫描程序要检查的端口号。
   f. 单击**确定**。
      “设置”窗口将关闭。
2. 设置漏洞扫描程序要同时检查有无安全软件的计算机数量：
   a. 转到 <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。

b. 要设置手动漏洞扫描期间检查的计算机数量，请更改 `ThreadNumManual` 的值。请指定一个介于 8 到 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 台计算机，则键入 `ThreadNumManual=60`。

c. 要设置预设漏洞扫描期间检查的计算机数量，请更改 `ThreadNumSchedule` 的值。请指定一个介于 8 到 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 台计算机，则键入 `ThreadNumSchedule=50`。

d. 保存 TMVS.ini。

检索终端描述的方法

当漏洞扫描程序可以 "ping" 主机时，它可以检索主机的其他相关信息。检索信息的方法有两种：

- **快速检索**：只检索终端名称
- **标准检索**：检索域信息和终端信息

配置检索设置

检索设置是漏洞扫描设置的子集。有关漏洞扫描设置的详细信息，请参阅漏洞扫描方法 第 5-38 页。

过程

1. 启动 TMVS.exe。
2. 单击**设置**。

   将显示**设置**窗口。
3. 转至**检索计算机描述的方法**部分。
4. 选择**标准**或**快速**。

5. 如果已选择**标准**，请选择**在可用时检索计算机描述**。
6. 单击**确定**。

   “设置”窗口将关闭。

通知

漏洞扫描程序可将漏洞扫描结果发送给防毒墙网络版管理员。它还可以在未受保护的主机上显示通知。

配置通知设置

通知设置是漏洞扫描设置的子集。有关漏洞扫描设置的详细信息，请参阅漏洞扫描方法 第 5-38 页。

过程

1. 启动 TMVS.exe。
2. 单击**设置**。

   将显示**设置**窗口。
3. 转至**通知**部分。
4. 自动将漏洞扫描结果发送给您或贵组织中的其他管理员：
   a. 选择**通过电子邮件将结果发送给系统管理员**。
   b. 单击**配置**，以指定电子邮件设置。
   c. 在**收件人**中，键入收件人的电子邮件地址。
   d. 在**发件人**中，键入发件人的电子邮件地址。
   e. 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。
   f. 在**主题**中，键入邮件的新主题或接受缺省主题。

g. 单击**确定**。

5. 通知用户其计算机未安装安全软件：

   a. 选择**在不受保护的计算机上显示通知**。

   b. 单击**定制**来配置通知消息。

   c. 在**通知消息**窗口中，键入新消息或接受缺省消息。

   d. 单击**确定**。

6. 单击**确定**。

   “设置”窗口将关闭。

漏洞扫描结果

可以配置漏洞扫描程序，以将漏洞扫描结果保存为逗号分隔值 (CSV) 文件。

配置扫描结果

漏洞扫描结果设置是漏洞扫描设置的子集。有关漏洞扫描设置的详细信息，请参阅漏洞扫描方法 第 5-38 页。

过程

1. 启动 TMVS.exe。
2. 单击**设置**。

   将显示**设置**窗口。
3. 转至**保存结果**部分。
4. 选择**自动将结果另存为 CSV 文件**。
5. 更改用来保存 CSV 文件的缺省文件夹：

   a. 单击**浏览**。

   b. 在终端或网络上选择目标文件夹。

c. 单击**确定**。

6. 单击**确定**。

“设置”窗口将关闭。

Ping 设置

使用 "ping" 设置来验证目标计算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所指定 IP 地址范围中的所有 IP 地址（包含任何主机上未使用的地址），因此扫描时间会比预期久。

配置 Ping 设置

Ping 设置是漏洞扫描设置的子集。有关漏洞扫描设置的详细信息，请参阅漏洞扫描方法 第 5-38 页。

过程

1. 从漏洞扫描程序 (TMVS.exe) 指定 ping 设置：

   a. 启动 TMVS.exe。

   b. 单击**设置**。

      将显示**设置**窗口。

   c. 转至 **Ping 设置**部分。

   d. 选择**允许漏洞扫描程序对网络上的计算机执行 ping 操作以检查其状态**。

   e. 在**数据包大小**和**超时**文本框中，接受或修改缺省值。

   f. 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主机运行的是 Windows 操作系统还是其他操作系统。对于运行 Windows 的主机，漏洞扫描程序可识别其 Windows 版本。

   g. 单击**确定**。

“设置”窗口将关闭。

2. 设置漏洞扫描程序要同时 ping 的计算机数量：

   a. 转到 <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。

   b. 更改 EchoNum 的值。请指定一个介于 1 到 64 之间的值。

      例如，如果要漏洞扫描程序在同一时间 ping 60 台计算机，则键入 EchoNum=60。

   c. 保存 TMVS.ini。

防毒墙网络版服务器设置

在下列情况中，会使用防毒墙网络版服务器设置：

- 漏洞扫描程序将防毒墙网络版客户端安装到未受保护的目标计算机中。通过服务器设置，漏洞扫描程序可识别防毒墙网络版客户端的父服务器以及登录目标计算机时要使用的管理凭证。

  注意

  某些情况可能会阻止防毒墙网络版客户端安装到目标主机中。

  有关详细信息，请参阅使用漏洞扫描程序安装防毒墙网络版客户端时的准则 第 5-37 页。

- 漏洞扫描程序会将客户端安装日志发送到防毒墙网络版服务器。

配置防毒墙网络版服务器设置

防毒墙网络版服务器设置是漏洞扫描设置的子集。有关漏洞扫描设置的详细信息，请参阅漏洞扫描方法 第 5-38 页。

过程

1. 启动 TMVS.exe。

2. 单击**设置**。

   将显示**设置**窗口。

3. 转至**防毒墙网络版服务器设置**部分。

4. 键入防毒墙网络版服务器的名称和端口号。

5. 选择**为不受保护的计算机自动安装防毒墙网络版客户端**。

6. 配置管理凭证：

   a. 单击**安装到帐户**。

   b. 在**帐户信息**窗口中，键入用户名和密码。

   c. 单击**确定**。

7. 选择**向防毒墙网络版服务器发送日志**。

8. 单击**确定**。

   “设置”窗口将关闭。

使用安全合规安装

在网络域中的计算机上安装防毒墙网络版客户端，或使用目标终端的 IP 地址将防毒墙网络版客户端安装到目标终端。

在安装防毒墙网络版客户端之前，请注意以下事项：

过程

1. 记录每个终端的登录凭证。在安装期间，防毒墙网络版将提示您指定登录凭证。

2. 如果以下情况属实，则终端上不会安装防毒墙网络版客户端：

   - 已将防毒墙网络版服务器安装在终端上。

- 终端运行 Windows XP Home、Windows Vista Home Basic、Windows Vista Home Premium、Windows 7™ Starter、Windows 7 Home Basic、Windows 7 Home Premium、Windows 8（Basic 版）、Windows 8.1（Basic 版）以及 Windows 10 Home。如果计算机运行这些平台，则选择其他安装方法。请参阅 部署注意事项 第 5-10 页 以了解详细信息。

3. 如果目标终端运行 Windows Vista（Business、Enterprise 或 Ultimate 版）、Windows 7（Professional、Enterprise 或 Ultimate 版）、Windows 8（Pro、Enterprise）、Windows 8.1（Pro、Enterprise）、Windows 10（Pro、Education、Enterprise）或 Windows Server 2012 (Standard)，则在终端上执行以下步骤：

   a. 启用内置管理员帐户并为该帐户设置密码。

   b. 禁用 Windows 防火墙。

   c. 单击**开始** > **所有程序** > **管理工具** > **高级安全 Windows 防火墙**。

   d. 针对域概要文件、专用概要文件和通用概要文件，将防火墙状态设置为“关闭”。

   e. 打开 Microsoft 管理控制台（单击 **开始** > **运行**，键入 `services.msc`），然后启动 **Remote Registry** 服务。安装防毒墙网络版客户端时，请使用内置管理员帐户和密码。

4. 如果终端上安装有趋势科技或第三方终端安全程序，则检查防毒墙网络版是否可以自动卸载该软件并将其替换为防毒墙网络版客户端。有关防毒墙网络版自动卸载的客户端安全软件的列表，请打开 <服务器安装文件夹>\PCCSRV\Admin 中的下列文件。可以使用文本编辑器（如记事本）打开这些文件。

   - tmuninst.ptn
   - tmuninst_as.ptn

   如果目标终端上的软件不包括在列表中，请首先手动卸载它。根据软件卸载过程，卸载后终端可能需要（或可能不需要）重新启动。

安装防毒墙网络版客户端

过程

1. 转至**评估** > **不受管理的终端**。
2. 单击客户端树顶部的**安装**。
   - 如果终端上安装有早期防毒墙网络版客户端版本时单击**安装**，则会跳过安装而不会将客户端升级到此版本。要升级客户端，必须禁用一个设置。
     a. 转至**客户端** > **客户端管理**。
     b. 单击**设置** > **权限和其他设置** > **其他设置**选项卡。
     c. 禁用选项**防毒墙网络版客户端可以更新组件，但不能升级客户端程序，也不能部署 hotfix**。
3. 为每个终端指定管理员登录帐户，并单击**登录**。防毒墙网络版 starts installing the 客户端 on the target 终端。
4. 查看安装状态。

迁移到防毒墙网络版客户端

将在目标终端上安装的客户端安全软件替换为防毒墙网络版客户端。

从其他终端安全软件迁移

安装防毒墙网络版客户端时，安装程序将检查在目标终端上安装的任何趋势科技或第三方终端安全软件。安装程序可以自动卸载该软件，并将它替换为防毒墙网络版客户端。

有关防毒墙网络版自动卸载的终端安全软件的列表，请打开 <服务器安装文件夹>\PCCSRV\Admin 中的下列文件。使用文本编辑器（如记事本）打开这些文件。

- tmuninst.ptn
- tmuninst_as.ptn

如果目标终端上的软件不包括在列表中，请首先手动卸载它。根据软件卸载过程，卸载后终端可能需要（或可能不需要）重新启动。

防毒墙网络版客户端迁移问题

- 如果自动客户端迁移成功，但是用户安装防毒墙网络版客户端后使用时遇到问题，请重新启动终端。
- 如果防毒墙网络版安装程序继续安装防毒墙网络版客户端，但是无法卸载其他安全软件，则这两个软件之间将存在冲突。卸载两个软件，然后使用部署注意事项 第 5-10 页中介绍的任何一种方法安装防毒墙网络版客户端。

从 ServerProtect 标准服务器迁移

ServerProtect™ 标准服务器迁移工具是一种可帮助您将运行趋势科技防毒墙服务器版标准服务器的计算机迁移到防毒墙网络版客户端的工具。

ServerProtect 标准服务器迁移工具要求与防毒墙网络版服务器相同的硬件和软件规格。在运行 Windows Server 2003 或 Windows Server 2008 的计算机上运行该工具。

成功卸载 ServerProtect 标准服务器后，该工具将安装防毒墙网络版客户端。它还将扫描例外列表设置（用于所有扫描类型）迁移到防毒墙网络版客户端。

安装防毒墙网络版客户端时，迁移工具客户端安装程序有时也许会超时，并通知您安装未成功。但是，可能已成功安装防毒墙网络版客户端。从防毒墙网络版 Web 控制台验证客户端终端上的安装是否成功。

迁移在以下情况下是不成功的：

- 远程客户端只有 IPv6 地址。迁移工具不支持 IPv6 寻址。
- 远程客户端无法使用 NetBIOS 协议。
- 端口 455、337 和 339 被封闭。
- 远程客户端无法使用 RPC 协议。
- 远程注册表服务停止。

注意

ServerProtect 标准服务器迁移工具不会卸载控制管理中心™客户端（防毒墙服务器版）。有关如何卸载该客户端的说明，请参考防毒墙服务器版和/或控制管理中心文档。

使用 ServerProtect 标准服务器迁移工具

过程

1. 在防毒墙网络版服务器计算机上，打开 <服务器安装文件夹>\PCCSRV\Admin\Utility\SPNSXfr 并将 SPNSXfr.exe 和 SPNSX.ini 文件复制到 <服务器安装文件夹>\PCCSRV\Admin。
2. 双击 SPNSXfr.exe 打开该工具。

   将打开 **ServerProtect 标准服务器迁移工具**控制台。
3. 选择防毒墙网络版服务器。防毒墙网络版服务器的路径将显示在防毒墙网络版服务器路径下。如果该路径不正确，单击**选择**，然后在防毒墙网络版安装所在的目录中选择 PCCSRV 文件夹。要使该工具在您下次打开时再次自动查找防毒墙网络版服务器，请选中 **自动查找服务器路径** 复选框（缺省选中）。
4. 选择要在哪个运行 ServerProtect 标准服务器的计算机上执行迁移，请在**目标终端**下单击以下选项之一：
   - **Windows 网络树**：显示网络中的域树。要使用这种方法选择计算机，请单击要从中搜索客户端计算机的域。

- **信息服务器名称**：通过信息服务器名称搜索。要通过这种方法选择计算机，请在文本框中键入网络中信息服务器的名称。要搜索多个信息服务器，请在服务器名称之间插入半角分号“;”。
- **特定标准服务器名称**：通过标准服务器名称搜索。要通过这种方法选择计算机，请在文本框中键入网络中标准服务器的名称。要搜索多个标准服务器，请在服务器名称之间输入半角分号“;”。
- **IP 范围搜索**：通过 IP 地址范围搜索。要通过这种方法搜索计算机，在“IP 范围”下输入 B 类 IP 地址范围。



注意

如果网络中的 DNS 服务器在搜索客户端时没有响应，则搜索将停止响应。等待搜索超时。

5. 选择**安装后重新启动**，以在迁移后自动重新启动目标计算机。

   只有重新启动后迁移才会成功完成。如果不选择此选项，请在迁移后手动重新启动计算机。

6. 单击**搜索**。

   搜索结果将显示在 **ServerProtect 标准服务器**下面。

7. 单击要执行迁移的计算机。

   a. 要选择所有计算机，请单击**全选**。

   b. 要取消选择所有计算机，请单击**取消全选**。

   c. 要将列表导出到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。

8. 如果登录到目标计算机需要用户名和密码，请执行以下操作：

   a. 选中**使用组帐户/密码**复选框。

   b. 单击**设置登录帐户**。

      将显示输入管理员信息窗口。

   c. 键入用户名和密码。

注意

使用本地/域管理员帐户登录到目标终端。如果使用权限不足的帐户（例如“Guest”或“标准用户”）登录，将无法执行安装。

d. 单击**确定**。

e. 单击**如果登录失败则再次询问**以便在迁移过程中无法登录时，能够再次键入用户名和密码。

9. 单击**迁移**。

10. 如果未选择**安装后重新启动**选项，请重新启动目标计算机以完成迁移。

安装后

完成安装后，验证以下内容：

- 防毒墙网络版客户端快捷方式 第 5-61 页
- 程序列表 第 5-61 页
- 防毒墙网络版客户端服务 第 5-61 页
- 防毒墙网络版客户端安装日志 第 5-62 页

防毒墙网络版客户端快捷方式

防毒墙网络版客户端快捷方式显示在客户端终端上的 Windows“开始”菜单中。

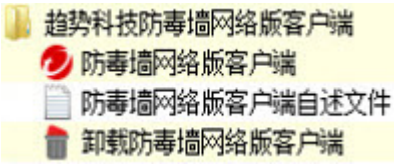


图 5-2. 防毒墙网络版客户端快捷方式

程序列表

安全客户端列在客户端终端的控制面板中的**添加/删除程序**列表中。

防毒墙网络版客户端服务

在 **Microsoft 管理控制台**上显示以下防毒墙网络版客户端服务：

- 防毒墙网络版 NT Listener (TmListen.exe)
- 防毒墙网络版 NT 实时扫描 (NTRtScan.exe)
- 防毒墙网络版 NT 代理服务 (TmProxy.exe)

> **注意**
>
> 防毒墙网络版 NT 代理服务在 Windows 7/8/8.1/10 或 Windows Server 2008 R2/2012 平台上不存在。

- 防毒墙网络版 NT 防火墙 (TmPfw.exe)；如果安装过程中启用了该防火墙
- 趋势科技未授权更改阻止服务 (TMBMSRV.exe)

- 趋势科技通用客户端解决方案框架 (TmCCSF.exe)

防毒墙网络版客户端安装日志

防毒墙网络版客户端安装日志 OFCNT.LOG 存在于以下位置：

- %windir%（对于除 MSI 软件包安装之外的所有安装方法）
- %temp%（对于 MSI 软件包安装方法）

建议的安装后任务

趋势科技建议执行以下安装后任务：

组件更新

更新防毒墙网络版客户端组件，以确保客户端有抵御安全风险的最新防护。可以从 Web 控制台运行手动客户端更新，或者指示用户从其计算机运行“立即更新”。

使用 EICAR 测试脚本测试扫描

欧洲计算机防病毒研究所（European Institute for Computer Antivirus Research，EICAR）开发了 EICAR 测试脚本作为确认防病毒软件安装和配置是否正确的安全方法。有关详细信息，请访问 EICAR 网站：

http://www.eicar.org

EICAR 测试脚本是一种扩展名为 .com 的无害文本文件。它不是病毒并且不包含任何含病毒碎片，但大部分防病毒软件将其作为病毒来响应。使用该文件来模拟病毒事件，确认电子邮件通知且病毒日志正常工作。

警告!

请勿使用真实病毒来测试防病毒产品。

执行测试扫描

过程

1. 启用客户端实时扫描。
2. 将以下字符串复制、粘贴到记事本或任何纯文本编辑器：`X5O!P %@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. 将文件另存为 EICAR.com，存放到一个临时目录。防毒墙网络版立即检测到该文件。
4. 要检测网络上的其他计算机，请将 EICAR.com 文件附加到电子邮件中并发送到其中一台计算机。

提示

趋势科技建议使用压缩软件（如 WinZip）对 EICAR 文件进行打包，然后执行其他测试扫描。

防毒墙网络版客户端卸载

有两种方法可以从计算机卸载防毒墙网络版客户端：

- 从 Web 控制台卸载防毒墙网络版客户端 第 5-64 页
- 运行防毒墙网络版客户端卸载程序 第 5-65 页

如果使用上述方法无法卸载防毒墙网络版客户端，请手动卸载防毒墙网络版客户端。有关详细信息，请参阅手动卸载防毒墙网络版客户端 第 5-66 页。

从 Web 控制台卸载防毒墙网络版客户端

从 Web 控制台卸载防毒墙网络版客户端程序。仅当遇到程序问题时才执行卸载，然后立即重新安装它，以保护终端免受安全风险的危害。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**任务** > **客户端卸载**。
4. 单击**客户端卸载**窗口中的**启动卸载**。服务器将发送通知给该客户端。
5. 检查通知状态，并检查是否存在未收到通知的客户端。
   a. 单击**选择未通知的终端**，然后再单击**启动卸载**立即将通知重新发送给未通知的客户端。
   b. 单击**停止卸载**可提示防毒墙网络版停止通知当前正通知的客户端。已收到通知并已执行卸载的客户端暂不处理此命令。

防毒墙网络版客户端卸载程序

授予用户卸载防毒墙网络版客户端程序的权限，然后指示他们从其计算机上运行客户端卸载程序。

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。

授予防毒墙网络版客户端卸载权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转到**卸载**部分。
5. 要允许在没有密码的情况下进行卸载，请选择**用户需要密码才能卸载防毒墙网络版客户端**。如果要求输入密码，请选择**用户需要密码才能卸载防毒墙网络版客户端**，然后键入密码并确认。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

运行防毒墙网络版客户端卸载程序

过程

1. 在 Windows **开始**菜单上单击**程序** > **趋势科技防毒墙网络版客户端** > **卸载防毒墙网络版客户端**。

   还可以执行以下步骤：

   a. 单击**控制面板** > **添加或删除程序**。

   b. 找到**趋势科技防毒墙网络版客户端**，然后单击**更改**。

c. 按照窗口上的指导信息操作。

2. 在系统提示时，键入卸载密码。防毒墙网络版通知用户卸载的进度与卸载完成。用户不需要重新启动客户端终端来完成卸载。

手动卸载防毒墙网络版客户端

仅当从 Web 控制台卸载防毒墙网络版客户端或运行卸载程序后遇到问题时，才执行手动卸载。

过程

1. 使用具有管理员权限的帐户登录到客户端终端。
2. 右键单击系统托盘中的防毒墙网络版客户端图标，然后选择**退出防毒墙网络版**。如果系统提示您输入密码，则指定退出密码，然后单击**确定**。

   注意

   - 对于 Windows 8、8.1、10 和 Windows Server 2012，请切换到桌面模式以退出防毒墙网络版客户端。
   - 在将退出防毒墙网络版客户端的计算机上禁用密码。有关详细信息，请参阅配置客户端权限和其他设置 第 14-81 页。

3. 如果未指定退出密码，则从 Microsoft 管理控制台停止以下服务：
   - 防毒墙网络版 NT Listener
   - 防毒墙网络版 NT 防火墙
   - 防毒墙网络版 NT 实时扫描
   - 防毒墙网络版 NT 代理服务

   注意

   防毒墙网络版 NT 代理服务在 Windows 7、8、8.1、10 或 Windows Server 2008R2、2012 平台上不存在。

- 趋势科技未授权更改阻止服务
- 趋势科技通用客户端解决方案框架

4. 从“开始”菜单中删除防毒墙网络版客户端的快捷方式。
   - 在 Windows 8、8.1、10 和 Windows Server 2012 上：
     a. 切换到桌面模式。
     b. 将鼠标光标移动到窗口的右下角，然后从显示的菜单中单击**开始**。

        将显示**主页**窗口。
     c. 右键单击**趋势科技防毒墙网络版**。
     d. 单击**从开始菜单取消固定**。
   - 在所有其他 Windows 平台上：

     单击**开始** > **程序**，右键单击**趋势科技防毒墙网络版客户端**，然后单击**删除**。
5. 打开注册表编辑器 (regedit.exe)。



警告!

接下来的步骤要求您删除注册表项。不正确地更改注册表会导致严重的系统问题。请始终在进行任何注册表更改前创建备份副本。有关详细信息，请参阅注册表编辑器帮助。

6. 删除以下注册表项：
   - 如果在终端上未安装其他趋势科技产品：
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

       对于 64 位计算机：

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`
   - 如果终端上安装了其他趋势科技产品，则仅删除以下注册码：

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog

  对于 64 位计算机：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp

  对于 64 位计算机：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\PC-cillinNTCorp

7. 删除以下注册表项/值：
   - 对于 32 位系统：
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下的 OfficeScanNT 监控程序（REG_SZ）
   - 对于 64 位系统：
     - HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 下的 OfficeScanNT 监控程序 (REG_SZ)
8. 删除以下位置中以下注册表项的所有实例：
   - 位置：
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
     - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services

- 注册表项：
  - NTRtScan
  - tmcfw
  - tmcomm
  - TmFilter
  - TmListen
  - tmpfw
  - TmPreFilter
  - TmProxy

    注意

    TmProxy 在 Windows 7/8/8.1/10 或 Windows Server 2008 R2/2012 平台上不存在。

  - tmtdi

    注意

    tmtdi 在 Windows 8/8.1/10 或 Windows Server 2012 平台上不存在。

  - VSApiNt
  - tmlwf（对于 Windows Vista/Server 2008/7/8/8.1/10/Server 2012 计算机）
  - tmwfp（对于 Windows Vista/Server 2008/7/8/8.1/10/Server 2012 计算机）
  - tmactmon

- TMBMServer
- TMebc
- tmevtmgr
- tmeevw（对于 Windows 7/8/8.1/10/Server 2008 R2/Server 2012 计算机）
- tmusa（对于 Windows 7/8/8.1/10/Server 2008 R2/Server 2012 计算机）
- tmnciesc
- tmeext（适用于 Windows XP/2003）

9. 关闭注册表编辑器。
10. 单击**开始** > **设置** > **控制面板**，然后双击 **系统**。

注意

对于 Windows 8/8.1/10 和 Windows Server 2012 系统，请跳过此步骤。

11. 单击**硬件**选项卡，然后单击**设备管理器**。

注意

对于 Windows 8/8.1/10 和 Windows Server 2012 系统，请跳过此步骤。

12. 单击**查看** > **显示隐藏的设备**。

注意

对于 Windows 8/8.1/10 和 Windows Server 2012 系统，请跳过此步骤。

13. 展开**非即插即用驱动程序**，然后卸载以下设备（对于 Windows XP/Vista/7/Server 2003/Server 2008）：
    - tmcomm
    - tmactmon

- tmevtmgr
- Trend Micro Filter
- Trend Micro PreFilter
- Trend Micro TDI Driver
- Trend Micro VSAPI NT
- 趋势科技未授权更改阻止服务
- Trend Micro WFP Callout Driver（对于 Windows Vista/Server 2008/7 计算机）

14. 使用以下命令通过命令行编辑器手动删除趋势科技驱动程序（仅限 Windows 8/8.1/10/Server 2012）：

- `sc delete tmcomm`
- `sc delete tmactmon`
- `sc delete tmevtmgr`
- `sc delete tmfilter`
- `sc delete tmprefilter`
- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`



注意

使用管理员权限运行命令行编辑器（例如，右键单击 cmd.exe，然后单击**以管理员身份运行**）以确保成功执行命令。

15. 卸载通用防火墙驱动程序。

    a. 右键单击**网上邻居**，然后单击**属性**。

    b. 右键单击**本地连接**，然后单击**属性**。

    c. 在**常规**选项卡上，选择**趋势科技通用防火墙驱动程序**，然后单击**卸载**。

    注意

    以下步骤仅适用于 Windows Vista/Server 2008/7/8/8.1/10/Server 2012 操作系统。使用所有其他操作系统的客户端将跳转到步骤 15。

    d. 右键单击**网络**，然后单击**属性**。

    e. 单击**管理网络连接**。

    f. 右键单击**本地连接**，然后单击**属性**。

    g. 在**网络**选项卡上，选择**趋势科技 NDIS 6.0 过滤器驱动程序**，然后单击**卸载**。

16. 重新启动客户端终端。

17. 如果终端上没有安装其他趋势科技产品，请删除 Trend Micro 安装文件夹（通常为 C:\Program Files\Trend Micro）。对于 64 位计算机，可在 C:\Program Files (x86)\Trend Micro 下找到安装文件夹。

18. 如果安装了其他趋势科技产品，则删除以下文件夹：

    - <客户端安装文件夹>
    - Trend Micro 安装文件夹下的 BM 文件夹（通常，对于 32 位系统为 C:\Program Files\Trend Micro\BM，对于 64 位系统为 C:\Program Files (x86)\Trend Micro\BM）

第 6 章

使防护保持最新

本章介绍防毒墙网络版组件和更新过程。

主题包括：

- 防毒墙网络版组件与程序 第 6-2 页
- 更新概述 第 6-13 页
- 防毒墙网络版服务器更新 第 6-15 页
- 集成型云安全智能防护服务器更新 第 6-26 页
- 防毒墙网络版客户端更新 第 6-26 页
- 更新代理 第 6-49 页
- 组件更新摘要 第 6-57 页

防毒墙网络版组件与程序

防毒墙网络版利用组件和程序来保护客户端计算机免受最新安全风险的危害。通过运行手动或预设更新，使这些组件和程序保持最新。

除这些组件外，防毒墙网络版 客户端还从防毒墙网络版服务器接收更新的配置文件。客户端需要这些配置文件应用新的设置。每次通过 Web 控制台修改防毒墙网络版设置时，配置文件也随之更改。

组件分为以下几组：

- 防病毒组件 第 6-2 页
- 损害清除服务组件 第 6-5 页
- 防间谍软件组件 第 6-6 页
- 防火墙组件 第 6-7 页
- Web 信誉组件 第 6-8 页
- 行为监控组件 第 6-8 页
- 程序 第 6-10 页
- 可疑连接组件 第 6-12 页
- 浏览器漏洞解决方案 第 6-12 页

防病毒组件

防病毒组件包含以下特征码、驱动程序和引擎：

- 病毒码 第 6-3 页
- 病毒扫描引擎 第 6-3 页
- 病毒扫描驱动程序 第 6-4 页
- IntelliTrap 特征码 第 6-5 页

- IntelliTrap 例外特征码 第 6-5 页
- 内存检查特征码 第 6-5 页

病毒码

客户端终端上的可用病毒码取决于客户端使用的扫描方法。

有关扫描方法的信息，请参阅扫描方法类型 第 7-7 页。

表 6-1. 病毒码

扫描方法	使用的特征码
传统扫描	病毒码包含帮助防毒墙网络版识别最新病毒/恶意软件和混合威胁攻击的信息。趋势科技将每周创建和发布几次新版本的病毒码，并且将在发现有特殊损害性的病毒/恶意软件后随时创建和发布新版本。 趋势科技建议将自动更新预设为至少每小时一次，这是所有已发布产品的缺省设置。
云安全扫描	在云安全扫描模式中，防毒墙网络版客户端使用协同工作的两个轻量级病毒码，这两个病毒码可提供传统防恶意软件和防间谍软件病毒码提供的相同防护。 云安全智能防护源托管**云安全云端病毒码**。此特征码每小时更新一次，它包含多数特征码定义。云安全客户端不下载此病毒码。客户端通过将扫描查询发送到云安全智能防护源，根据病毒码验证潜在威胁。 客户端更新源（防毒墙网络版服务器或定制更新源）托管**云安全客户端病毒码**。此病毒码每天更新一次，它包含在云安全云端病毒码中未找到的所有其他特征码定义。客户端使用下载其他防毒墙网络版组件的相同方法，从更新源下载此病毒码。 有关云安全云端病毒码和云安全客户端病毒码的详细信息，请参阅云安全智能防护病毒码文件 第 4-7 页。

病毒扫描引擎

所有趋势科技产品的核心是扫描引擎，它最初是为了响应早期基于文件的终端病毒而开发的。如今的扫描引擎非常完善，能够检测出各种类型的病毒和恶意

软件 第 7-2 页。扫描引擎还可检测出以研究为目的而开发和使用的受控病毒。

扫描引擎不会扫描每个文件的每一字节，而是和特征码文件协作以识别以下项：

- 病毒代码的指示特征
- 文件中可能存在病毒的精确位置

防毒墙网络版可在检测到病毒/恶意软件后移除，并恢复文件的完整性。

更新扫描引擎

通过将最具时效性的病毒/恶意软件信息存储在病毒码中，趋势科技最大程度地减少了扫描引擎更新次数，同时可使防护保持最新。然而，趋势科技将定期提供新的扫描引擎版本。趋势科技将在以下情况下发布新的引擎：

- 将新的扫描和检测技术纳入软件中
- 发现扫描引擎无法处理的新的可能有害的病毒/恶意软件
- 扫描性能的增强
- 添加了文件格式、脚本语言、编码和/或压缩格式

病毒扫描驱动程序

病毒扫描驱动程序监控用户对文件的操作。这些操作包括打开或关闭文件以及执行应用程序。此驱动程序有两个版本。分别为 TmXPFlt.sys 和 TmPreFlt.sys。TmXPFlt.sys 用于实时配置病毒扫描引擎，TmPreFlt.sys 用于监视用户操作。

注意

此组件不显示在控制台上。要检查其版本，请转到 <服务器安装文件夹>\PCCSRV\Pccnt\Drv。右键单击 .sys 文件，选择**属性**，然后转到**版本**选项卡。

IntelliTrap 特征码

IntelliTrap 特征码（有关详细信息，请参阅 IntelliTrap 第 E-6 页）。 特征码可以检测打包为可执行文件的实时压缩文件。

IntelliTrap 例外特征码

IntelliTrap 例外特征码包含“允许的”压缩文件的列表。

内存检查特征码

实时扫描使用内存检查特征码来评估行为监控识别的压缩可执行文件。实时扫描对压缩可执行文件执行以下操作：

1. 验证进程镜像路径后，在内存中创建映射文件。

   注意

   扫描例外列表会覆盖文件扫描。

2. 将进程 ID 发送到高级保护服务，该服务随后会执行以下操作：

   a. 使用病毒扫描引擎执行内存扫描。

   b. 通过 Windows 系统文件的全局允许列表、可信源的数字签名的文件以及趋势科技测试的文件过滤进程。验证文件为安全文件后，防毒墙网络版不会对该文件执行任何操作。

3. 处理内存扫描后，高级保护服务会将结果发送给实时扫描。

4. 然后，实时扫描会隔离任何检测到的恶意软件威胁并终止该进程。

损害清除服务组件

损害清除服务组件包含以下引擎和模板。

- 病毒清除引擎 第 6-6 页
- 病毒清除模板 第 6-6 页
- 预启动的清除驱动程序 第 6-6 页

病毒清除引擎

病毒清除引擎扫描并移除特洛伊木马和特洛伊木马进程。此引擎支持 32 位和 64 位平台。

病毒清除模板

病毒清除引擎使用病毒清除模板来识别特洛伊木马文件和进程，以便进行清除。

预启动的清除驱动程序

趋势科技预启动的清除驱动程序在操作系统驱动程序之前加载，可检测和阻止引导类型的 rootkit。加载防毒墙网络版客户端后，趋势科技预启动的清除驱动程序会调用损害清除服务来清除 rootkit。

防间谍软件组件

防间谍软件组件包含以下引擎和特征码：

- 间谍软件特征码 第 6-7 页
- 间谍软件扫描引擎 第 6-7 页
- 间谍软件主动监控特征码 第 6-7 页

间谍软件特征码

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。

间谍软件扫描引擎

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。此引擎支持 32 位和 64 位平台。

间谍软件主动监控特征码

间谍软件主动监控特征码用于实时间谍软件/灰色软件扫描。只有传统扫描客户端才使用此特征码。

云安全客户端使用云安全客户端病毒码实时扫描间谍软件/灰色软件。如果在扫描期间无法确定扫描目标的风险，则客户端会将扫描查询发送到云安全智能防护源。

防火墙组件

防火墙组件包含以下驱动程序和特征码：

- 通用防火墙驱动程序 第 6-7 页
- 通用防火墙特征码 第 6-8 页

通用防火墙驱动程序

通用防火墙驱动程序与通用防火墙特征码结合使用，以扫描客户端计算机中是否有网络病毒。此驱动程序支持 32 位和 64 位平台。

通用防火墙特征码

通用防火墙特征码类似于病毒码，可帮助防毒墙网络版识别病毒特征（表示存在网络病毒的独特位和字节模式）。

Web 信誉组件

Web 信誉组件是 URL 过滤引擎。

URL 过滤引擎

URL 过滤引擎可促进防毒墙网络版和趋势科技 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防毒墙网络版的系统。

行为监控组件

行为监控组件包含以下特征码、驱动程序和服务：

- 行为监控检测特征码 第 6-8 页
- 行为监控驱动程序 第 6-9 页
- 行为监控核心服务 第 6-9 页
- 行为监控配置特征码 第 6-9 页
- 数字签名特征码 第 6-9 页
- 策略强制特征码 第 6-9 页

行为监控检测特征码

此特征码包含用于检测可疑威胁行为的规则。

行为监控驱动程序

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。

行为监控核心服务

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

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。

数字签名特征码

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

行为监控核心服务根据此特征码中的策略检查系统事件。

内存扫描触发特征码

行为监控在检测到以下操作后使用内存扫描触发特征码识别潜在威胁：

- 文件写入操作
- 注册表写入操作
- 新进程创建

识别这些操作中的其中一个后，行为监控会调用实时扫描的内存检查特征码以检查安全风险。

有关实时扫描操作的详细信息，请参阅内存检查特征码 第 6-5 页。

程序

防毒墙网络版利用以下程序和产品更新：

- 防毒墙网络版客户端程序 第 6-10 页
- HotFix、Patch 和 Service Pack 第 6-10 页

防毒墙网络版客户端程序

防毒墙网络版客户端程序提供抵御安全风险的实际防护。

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：

- Hotfix 第 E-4 页
- Patch 第 E-9 页
- 安全 Patch 第 E-10 页
- Service Pack 第 E-10 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。

Hot Fix 和 Patch 历史

当防毒墙网络版服务器将 hotfix 或 patch 文件部署到防毒墙网络版客户端时，防毒墙网络版客户端程序会在注册表编辑器中记录有关 hotfix 或 patch 的信息。可以使用后勤软件（如 Microsoft SMS、LANDesk™ 或 BigFix™）查询多个客户端的此信息。

注意

此功能不记录仅部署到服务器的 Hot Fix 和 Patch。

此功能从带有 Patch 3.1 的防毒墙网络版 8.0 Service Pack 1 开始可用。

- 从带有 Patch 3.1 或更高版本的 8.0 Service Pack 1 版本升级的客户端记录为版本 8.0 和更高版本安装的 Hot Fix 和 Patch。
- 从带有 Patch 3.1 的 8.0 Service Pack 1 之前的版本升级的客户端记录为版本 10.0 和更高版本安装的 Hot Fix 和 Patch。

信息存储在以下项中：

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- 对于运行 x64 类型平台的计算机：

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

检查以下项：

- **注册表项**：`HotFix_installed`

  类型：`REG_SZ`

  值：`<Hotfix 或 patch 名称>`

- **注册表项**：HotfixInstalledNum

  类型：DWORD

  值：<Hotfix 或 patch 编号>

可疑连接组件

可疑连接组件包含以下列表和特征码：

- 全局 C&C IP 列表 第 6-12 页
- 关联规则特征码 第 6-12 页

全局 C&C IP 列表

全局 C&C IP 列表与网络内容检查引擎 (NCIE) 结合使用，以检测与已知 C&C 服务器的网络连接。NCIE 通过任何网络通道检测 C&C 服务器联系人。

防毒墙网络版在全局 C&C IP 列表中记录服务器的所有连接信息，以便进行评估。

关联规则特征码

可疑连接服务会使用关联规则特征码来检测位于网络数据包头中的唯一恶意软件系列签名。

浏览器漏洞解决方案

浏览器漏洞解决方案包括以下特征码：

- 浏览器漏洞防护特征码 第 6-13 页
- 脚本分析器特征码 第 6-13 页

浏览器漏洞防护特征码

此特征码会识别最新的 Web 浏览器漏洞并阻止这些漏洞被利用而危及 Web 浏览器的安全。

脚本分析器特征码

此特征码会分析 Web 页面中的脚本并识别恶意脚本。

更新概述

所有组件更新都源自趋势科技 ActiveUpdate 服务器。如果有可用更新，防毒墙网络版服务器和云安全智能防护源（云安全智能防护服务器或云安全智能防护网络）将下载更新的组件。防毒墙网络版服务器与云安全智能防护源之间不存在重叠的组件下载，因为每台服务器下载一组特定的组件。



注意

可以将防毒墙网络版服务器和云安全智能防护服务器都配置为从趋势科技 ActiveUpdate 服务器之外的源更新。为此，需要设置定制更新源。如果在设置此更新源时需要帮助，请联系技术支持提供商。

防毒墙网络版服务器和防毒墙网络版客户端更新

防毒墙网络版服务器下载客户端需要的大多数组件。它唯一不下载的组件是云安全云端病毒码（由云安全智能防护源下载）。

如果防毒墙网络版服务器管理大量的客户端，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，防毒墙网络版提供了更新代理功能，允许某些客户端共享向其他客户端分发更新的任务。

下表描述了防毒墙网络版服务器和客户端的不同组件更新选项，以及建议的使用时机：

表 6-2. 服务器-客户端更新选项

更新选项	描述	建议
ActiveUpdate 服务器 > 服务器 > 客户端	防毒墙网络版服务器将从趋势科技 ActiveUpdate 服务器（或其他更新源）接收更新的组件，并将在客户端上启动组件更新。	如果防毒墙网络版服务器和客户端之间无“低带宽”部分，请使用此方法。
ActiveUpdate 服务器 > 服务器 > 更新代理 > 客户端	防毒墙网络版服务器将从 ActiveUpdate 服务器（或其他更新源）接收更新的组件，并将在客户端上启动组件更新。然后充当更新代理的客户端将通知客户端更新组件。	如果防毒墙网络版服务器和客户端之间有“低带宽”部分，请使用此方法来平衡网络通信负载。
ActiveUpdate 服务器 > 更新代理 > 客户端	更新代理将直接从 ActiveUpdate 服务器（或其他更新源）接收更新的组件，并通知客户端更新组件。	仅当在从防毒墙网络版服务器或其他更新代理更新更新代理的过程中遇到问题时，使用此方法。 在多数情况下，更新代理从防毒墙网络版服务器或其他更新代理处接收更新的速度比从外部更新源处接收的速度快。
ActiveUpdate 服务器 > 客户端	防毒墙网络版客户端直接从 ActiveUpdate 服务器（或其他更新源）处接收更新的组件。	仅当在从防毒墙网络版服务器或其他更新代理更新客户端的过程中遇到问题时，使用此方法。 在多数情况下，客户端从防毒墙网络版服务器或更新代理处接收更新的速度比从外部更新源处接收的速度快。

云安全智能防护源更新

云安全智能防护源（云安全智能防护服务器或云安全智能防护网络）下载云安全云端病毒码。云安全客户端不下载此病毒码。客户端通过将扫描查询发送到云安全智能防护源，根据病毒码验证潜在威胁。

注意

有关云安全智能防护源的详细信息，请参阅云安全智能防护源 第 4-5 页。

下表描述了云安全智能防护源的更新过程。

表 6-3. 云安全智能防护源更新过程

更新过程	描述
ActiveUpdate 服务器 > 云安全智能防护网络	趋势科技云安全智能防护网络从趋势科技 ActiveUpdate 服务器接收更新。未连接到公司网络的云安全客户端向趋势科技云安全智能防护网络发送查询。
ActiveUpdate 服务器 > 云安全智能防护服务器	云安全智能防护服务器（集成型或独立型）从趋势科技 ActiveUpdate 服务器接收更新。连接到公司网络的云安全智能防护客户端向云安全智能防护服务器发送查询。
云安全智能防护网络 > 云安全智能防护服务器	云安全智能防护服务器（集成型或独立型）从趋势科技云安全智能防护网络接收更新。连接到公司网络的云安全智能防护客户端向云安全智能防护服务器发送查询。

防毒墙网络版服务器更新

防毒墙网络版服务器下载以下组件并将它们部署到客户端：

表 6-4. 由防毒墙网络版服务器下载的组件

组件	分发	
	传统扫描客户端	云安全扫描客户端
防病毒		
云安全客户端病毒码	否	是
病毒码	是	否
IntelliTrap 特征码	是	是
IntelliTrap 例外特征码	是	是

组件	分发	
	传统扫描客户端	云安全扫描客户端
内存检查特征码	是	是
病毒扫描引擎（32 位）	是	是
病毒扫描引擎（64 位）	是	是
防间谍软件		
间谍软件特征码	是	是
间谍软件主动监控特征码	是	否
间谍软件扫描引擎（32 位）	是	是
间谍软件扫描引擎（64 位）	是	是
损害清除服务		
病毒清除模板	是	是
病毒清除引擎（32 位）	是	是
病毒清除引擎（64 位）	是	是
预启动的清除驱动程序（32 位）	是	是
预启动的清除驱动程序（64 位）	是	是
防火墙		
通用防火墙特征码	是	是
行为监控组件		
行为监控检测特征码（32 位）	是	是
行为监控驱动程序（32 位）	是	是
行为监控核心服务（32 位）	是	是
行为监控检测特征码（64 位）	是	是
行为监控驱动程序（64 位）	是	是

组件	分发	
	传统扫描客户端	云安全扫描客户端
行为监控核心服务（64 位）	是	是
行为监控配置特征码	是	是
策略强制特征码	是	是
数字签名特征码	是	是
内存扫描触发特征码（32 位）	是	是
内存扫描触发特征码（64 位）	是	是
C&C 联系人警报服务		
全局 C&C IP 列表	是	是
关联规则特征码	是	是
浏览器漏洞解决方案		
浏览器漏洞防护特征码	是	是
脚本分析器特征码	是	是

更新提醒和提示：

- 要允许服务器将更新的组件部署到客户端，请启用自动客户端更新。有关详细信息，请参阅防毒墙网络版客户端自动更新 第 6-35 页。如果禁用自动客户端更新，则服务器会下载更新，但不会将它们部署到客户端。
- 纯 IPv6 防毒墙网络版服务器无法直接向纯 IPv4 客户端分发更新。同样，纯 IPv4 防毒墙网络版服务器无法直接向纯 IPv6 客户端分发更新。为允许防毒墙网络版服务器向客户端分发更新，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。
- 趋势科技会定期发布病毒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，因此防毒墙网络版将使用一个名称为**组件复制**的机制，该机制允许更快速地下载特征码文件。请参阅防毒墙网络版服务器组件复制 第 6-20 页以获取详细信息。

- 如果使用代理服务器连接到 Internet，请使用正确的代理服务器设置成功下载更新。
- 在 Web 控制台的控制台上，添加**客户端更新**小组件以查看组件的当前版本，并确定带有更新组件和过期组件的客户端数。

防毒墙网络版服务器更新源

将防毒墙网络版服务器配置为从趋势科技 ActiveUpdate 服务器或从其他源下载组件。如果防毒墙网络版服务器无法直接访问 ActiveUpdate 服务器，则可以指定其他源。有关示例场景，请参阅隔离的防毒墙网络版服务器更新 第 6-23 页。

服务器下载任何可用更新后，可以基于在**更新** > **客户端** > **自动更新**中指定的设置，自动通知客户端更新其组件。如果组件更新非常重要，则允许服务器通过转至**更新** > **客户端** > **手动更新**立即通知客户端。

注意

如果在**更新** > **客户端** > **自动更新**中未指定部署时间表或事件触发的更新设置，则服务器将下载更新但不通知客户端更新。

防毒墙网络版服务器更新的 IPv6 支持

纯 IPv6 防毒墙网络版服务器无法直接从纯 IPv4 更新源更新，例如：

- 趋势科技 ActiveUpdate 服务器
- 任何纯 IPv4 定制更新源

同样，纯 IPv4 防毒墙网络版服务器无法直接从纯 IPv6 定制更新源更新。

为允许服务器连接到更新源，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

用于防毒墙网络版服务器更新的代理服务器

将在服务器计算机上托管的服务器程序配置为从趋势科技 ActiveUpdate 服务器下载更新时使用代理服务器设置。服务器程序包括防毒墙网络版服务器和集成型云安全智能防护服务器。

配置代理服务器设置

过程

1. 转至**管理** > **设置** > **代理服务器**。
2. 单击**外部代理服务器**选项卡。
3. 转至**防毒墙网络版服务器更新**部分。
4. 选择**使用代理服务器进行特征码、引擎和使用授权更新**。
5. 指定代理服务器协议、服务器名称或 IPv4/IPv6 地址以及端口号。
6. 如果代理服务器要求认证，请键入用户名和密码。
7. 单击**保存**。

配置服务器更新源

过程

1. 转至**更新** > **服务器** > **更新源**。
2. 选择想要下载组件更新的位置。

   如果选择 ActiveUpdate 服务器，请确保该服务器具有 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，请参阅用于防毒墙网络版服务器更新的代理服务器 第 6-19 页。

如果选择定制更新源，请为此更新源设置相应的环境和更新资源。此外，还应确保服务器计算机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。

注意

从更新源下载组件时，防毒墙网络版服务器使用组件复制。请参阅防毒墙网络版服务器组件复制 第 6-20 页以了解详细信息。

3. 单击**保存**。

防毒墙网络版服务器组件复制

可以从趋势科技 ActiveUpdate 服务器下载最新版本的完全病毒码文件时，也可以下载 14 个“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 V175 中但不在 V173 中的签名（由于特征码编号以 2 为增量发布，因此 V173 是前一完全特征码版本。增量特征码 v_171.175 包含在 V175 中但不在 V171 中的签名。

要减小下载最新特征码时生成的网络流量，防毒墙网络版执行组件复制（防毒墙网络版服务器或更新代理只下载增量特征码的组件更新方式）。有关更新代理如何执行组件复制的信息，请参阅更新代理组件复制 第 6-54 页。

组件复制适用于以下组件：

- 病毒码
- 云安全客户端病毒码
- 病毒清除模板
- IntelliTrap 例外特征码
- 间谍软件特征码
- 间谍软件主动监控特征码

组件复制场景

要解释用于服务器的组件复制，请参考以下场景：

表 6-5. 服务器组件复制场景

防毒墙网络版服务器上的完全特征码	当前的版本：171 其他可用版本： 169	167	165	161	159	
ActiveUpdate 服务器上的最新版本	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. 防毒墙网络版服务器将其当前完全特征码版本与 ActiveUpdate 服务器上的最新版本进行比较。如果两个版本之间的差值小于等于 14，则服务器只下载代表这两个版本差值的增量特征码。

   注意

   如果此差值大于 14，则服务器自动下载完全版的特征码文件和 14 个增量特征码。

   基于示例说明：

   - V171 和 V175 之间的差值是 2。换言之，服务器没有 V173 和 V175。
   - 服务器将下载增量特征码 171.175。此增量特征码代表 V171 和 V175 之间的差值。

2. 服务器将增量特征码和其当前完全特征码合并以生成最新的完全特征码。

   基于示例说明：

   - 在服务器上，防毒墙网络版将 V171 与增量特征码 171.175 合并以生成 V175。
   - 服务器具有 1 个增量特征码 (171.175) 和最新的完全特征码 (V175)。

3. 服务器基于服务器上可用的其他完全特征码生成增量特征码。如果服务器没有生成这些增量特征码，未下载较早增量特征码的客户端将自动下载完全特征码文件，继而会产生更多网络通信。

   基于示例说明：

   - 由于服务器具有特征码 V169、V167、V165、V163、V161 和 V159，因此它可以生成以下增量特征码：

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 由于服务器已经具有增量特征码 171.175，因此它不需要使用 V171。

   - 服务器现在具有 7 个增量特征码：

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 服务器保留最后 7 个完全特征码版本（V175、V171、V169、V167、V165、V163 和 V161）。并删除任何较旧版本 (V159)。

4. 服务器将其当前增量特征码与 ActiveUpdate 服务器上可用的增量特征码进行比较。服务器将下载它所没有的增量特征码。

   基于示例说明：

   - ActiveUpdate 服务器具有 14 个增量特征码：

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - 防毒墙网络版服务器具有 7 个增量特征码：

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 防毒墙网络版服务器下载其他 7 个增量特征码：

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - 该服务器现在具有 ActiveUpdate 服务器上可用的所有增量特征码。

5. 客户端可以使用最新的完全特征码和这 14 个增量特征码。

隔离的防毒墙网络版服务器更新

如果防毒墙网络版服务器属于与所有外部源完全隔离的网络，则可通过从包含最新组件的内部源进行更新来使服务器组件保持最新。

本主题说明更新隔离的防毒墙网络版服务器时所需执行的任务。

更新隔离的防毒墙网络版服务器

提供此过程以供参考。如果可以完成此过程中的所有任务，请向技术支持提供商询问各任务的详细步骤。

过程

1. 确定更新源，例如趋势科技防毒墙控制管理中心或随机主机。更新源必须具备：
   - 可靠的 Internet 连接，以便可以从趋势科技 ActiveUpdate 服务器下载最新组件。如果无法连接到 Internet，则更新源获取最新组件的唯一方式是自行从趋势科技获取组件，然后将组件复制到更新源中。
   - 与防毒墙网络版服务器之间的有效连接。如果防毒墙网络版服务器与更新源之间存在代理服务器，则配置代理服务器设置。有关详细信息，请参阅用于防毒墙网络版服务器更新的代理服务器 第 6-19 页。
   - 足够的磁盘空间用于保存下载的组件
2. 使防毒墙网络版服务器指向新的更新源。有关详细信息，请参阅防毒墙网络版服务器更新源 第 6-18 页。
3. 确定服务器部署到客户端的组件。有关可部署组件的列表，请参阅防毒墙网络版客户端更新 第 6-26 页。

提示

用来确定组件是否要部署到客户端的方法之一是转至 Web 控制台上的**更新摘要**窗口（**更新** > **摘要**）。在此窗口中，要部署的组件的更新率始终大于 0%。

4. 确定下载组件的频率。特征码文件更新很频繁（有些是每天更新），因此定期对其进行更新是一个好习惯。对于引擎和驱动程序，可以让技术支持提供商通知您重要的更新。

5. 在更新源中：

   a. 连接到 ActiveUpdate 服务器。服务器的 URL 取决于防毒墙网络版的版本。

   b. 下载以下项：

      - server.ini 文件。此文件包含有关最新组件的信息。
      - 在步骤 3 中确定的组件。

   c. 将下载的项保存到更新源的某个目录中。

6. 运行防毒墙网络版服务器的手动更新。有关详细信息，请参阅手动更新防毒墙网络版服务器 第 6-25 页。

7. 每次需要更新组件时，重复步骤 5 至步骤 6。

防毒墙网络版服务器更新方法

手动更新防毒墙网络版服务器组件，或通过配置更新时间表来更新它们。

要允许服务器将更新的组件部署到客户端，请启用自动客户端更新。有关详细信息，请参阅防毒墙网络版客户端自动更新 第 6-35 页。如果禁用自动客户端更新，则服务器会下载更新，但不会将它们部署到客户端。

更新方法包括：

- **手动服务器更新**：如果更新非常重要，请执行手动更新以便服务器可以立即获取更新。请参阅手动更新防毒墙网络版服务器 第 6-25 页以了解详细信息。
- **预设服务器更新**：防毒墙网络版服务器在预设的日期和时间连接到更新源，以获取最新组件。请参阅预设更新防毒墙网络版服务器 第 6-25 页以了解详细信息。

手动更新防毒墙网络版服务器

在安装或升级服务器之后以及存在爆发时，在防毒墙网络版服务器上手动更新组件。

过程

1. 转至**更新** > **服务器** > **手动更新**。
2. 选择要更新的组件。
3. 单击**更新**。

   服务器将下载更新过的组件。

预设更新防毒墙网络版服务器

将防毒墙网络版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。由于客户端通常从服务器获得更新，因此使用预设更新是确保安全风险防护始终保持最新的简单有效的方法。

过程

1. 转至**更新** > **服务器** > **预设更新**。
2. 选择**启用防毒墙网络版服务器的预设更新**。
3. 选择要更新的组件。
4. 指定更新时间表。

   对每日、每周和每月更新而言，这段时间即防毒墙网络版将执行更新的小时数。防毒墙网络版在此时间段的任意给定时间内进行更新。
5. 单击**保存**。

防毒墙网络版服务器更新日志

检查服务器更新日志，以确定更新某些组件时是否存在问题。日志包括防毒墙网络版服务器的组件更新。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看更新日志

过程

1. 转至**日志** > **服务器更新**。
2. 检查**结果**列以查看是否存在未更新的组件。
3. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

集成型云安全智能防护服务器更新

集成型云安全智能防护服务器下载两个组件，即云安全云端病毒码和 Web 阻止列表。有关这些组件及如何更新它们的详细信息，请参阅集成型云安全智能防护服务器管理 第 4-17 页。

防毒墙网络版客户端更新

要确保客户端处于不受最新安全风险危害的状态，请定期更新客户端组件。

更新客户端之前，请检查其更新源（防毒墙网络版服务器或定制更新源）是否具有最新的组件。有关如何更新防毒墙网络版服务器的信息，请参阅防毒墙网络版服务器更新 第 6-15 页。

下表列出了更新源部署到客户端的所有组件和使用特定扫描方法时正在使用的组件。

表 6-6. 部署到客户端的防毒墙网络版组件

组件	分发	
	传统扫描客户端	云安全扫描客户端
防病毒		
云安全客户端病毒码	否	是
病毒码	是	否
IntelliTrap 特征码	是	是
IntelliTrap 例外特征码	是	是
病毒扫描引擎（32 位）	是	是
病毒扫描引擎（64 位）	是	是
内存检查特征码	是	是
防间谍软件		
间谍软件/灰色软件特征码	是	是
间谍软件主动监控特征码	是	否
间谍软件/灰色软件扫描引擎（32 位）	是	是
间谍软件/灰色软件扫描引擎（64 位）	是	是
损害清除服务		
损害清除模板	是	是
损害清除引擎（32 位）	是	是
损害清除引擎（64 位）	是	是
预启动的清除驱动程序（32 位）	是	是
预启动的清除驱动程序（64 位）	是	是

组件	分发	
	传统扫描客户端	云安全扫描客户端
Web 信誉服务		
URL 过滤引擎	是	是
防火墙		
防火墙特征码	是	是
防火墙驱动程序（32 位）	是	是
防火墙驱动程序（64 位）	是	是
行为监控组件		
行为监控检测特征码（32 位）	是	是
行为监控核心驱动程序（32 位）	是	是
行为监控核心服务（32 位）	是	是
行为监控检测特征码（64 位）	是	是
行为监控核心驱动程序（64 位）	是	是
行为监控核心服务（64 位）	是	是
行为监控配置特征码	是	是
策略强制特征码	是	是
数字签名特征码	是	是
内存扫描触发特征码（32 位）	是	是
内存扫描触发特征码（64 位）	是	是
可疑连接		
全局 C&C IP 列表	是	是
关联规则特征码	是	是
浏览器漏洞		

组件	分发	
	传统扫描客户端	云安全扫描客户端
浏览器漏洞防护特征码	是	是
脚本分析器特征码	是	是

防毒墙网络版客户端更新源

客户端可以从标准更新源（防毒墙网络版服务器）获取更新，或从定制更新源（如趋势科技 ActiveUpdate 服务器）获取特定组件。有关详细信息，请参阅防毒墙网络版客户端的标准更新源 第 6-29 页和防毒墙网络版客户端的定制更新源 第 6-31 页。

防毒墙网络版客户端更新的 IPv6 支持

纯 IPv6 客户端无法直接从纯 IPv4 更新源更新，例如：

- 纯 IPv4 防毒墙网络版服务器
- 纯 IPv4 更新代理
- 任何纯 IPv4 定制更新源
- 趋势科技 ActiveUpdate 服务器

同样，纯 IPv4 客户端无法直接从纯 IPv6 更新源（例如纯 IPv6 防毒墙网络版服务器或更新代理）更新。

为允许客户端连接到更新源，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

防毒墙网络版客户端的标准更新源

防毒墙网络版服务器是客户端的标准更新源。

如果无法访问防毒墙网络版服务器，客户端将没有备份源，因此仍将处于过期状态。要更新无法访问防毒墙网络版服务器的客户端，趋势科技建议使用客户端打包程序。使用此工具可创建具有服务器上可用的最新组件的软件包，然后在客户端上运行该软件包。

注意

客户端的 IP 地址（IPv4 或 IPv6）确定是否可以与防毒墙网络版服务器建立连接。有关客户端更新的 IPv6 支持的详细信息，请参阅防毒墙网络版客户端更新的 IPv6 支持 第 6-29 页。

配置防毒墙网络版客户端的标准更新源

过程

1. 转至**更新** > **客户端** > **更新源**。
2. 选择**标准更新源 (从防毒墙网络版服务器更新)**。
3. 单击**通知所有客户端**。

防毒墙网络版客户端更新过程

注意

本主题讨论防毒墙网络版客户端的更新过程。更新代理的更新过程在防毒墙网络版客户端的标准更新源 第 6-29 页中进行讨论。

如果将防毒墙网络版客户端配置为直接从防毒墙网络版服务器更新，则更新过程按如下方式进行：

1. 防毒墙网络版客户端从防毒墙网络版服务器获取更新。
2. 如果无法从防毒墙网络版服务器更新，则在**客户端** > **客户端管理**中单击**设置** > **权限和其他设置** > **其他设置（选项卡）** > **更新设置**来启用**防毒墙网络版客户端从趋势科技 ActiveUpdate 服务器下载更新**选项时，防毒墙网络版客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器。

注意

只能从 ActiveUpdate 服务器更新组件。只能从防毒墙网络版服务器或更新代理下载域设置、程序和 Hot Fix。可以通过将防毒墙网络版客户端配置为仅从 ActiveUpdate 服务器下载特征码文件来加速更新过程。有关详细信息，请参阅作为防毒墙网络版客户端更新源的 ActiveUpdate 服务器 第 6-34 页。

防毒墙网络版客户端的定制更新源

除了防毒墙网络版服务器外，防毒墙网络版客户端还可以从定制更新源进行更新。定制更新源可帮助减少定向到防毒墙网络版服务器的防毒墙网络版客户端更新流量，并允许无法连接到防毒墙网络版服务器的防毒墙网络版客户端获取及时的更新。在定制的更新源列表（最多可容纳 1024 个更新源）上指定定制的更新源。

提示

趋势科技建议指定一些防毒墙网络版客户端为更新代理，然后将它们添加到此列表中。

配置防毒墙网络版客户端的定制更新源

过程

1. 转至**更新** > **客户端** > **更新源**。
2. 选择**定制的更新源**，然后单击**添加**。
3. 在显示的窗口中，指定客户端的 IP 地址。可以键入 IPv4 范围和/或 IPv6 前缀和长度。
4. 指定更新源。可以选择更新代理（如果已分配），或键入特定源的 URL。

注意

请确保防毒墙网络版客户端可以使用其 IP 地址连接到更新源。例如，如果指定了 IPv4 地址范围，则更新源必须具有 IPv4 地址。如果指定 IPv6 前缀和长度，则更新源必须具有 IPv6 地址。有关客户端更新的 IPv6 支持的详细信息，请参阅 防毒墙网络版客户端更新源 第 6-29 页。

5. 单击**保存**。
6. 在窗口中执行其他任务。
   a. 选择以下任何设置。关这些设置的工作方式的详细信息，请参阅防毒墙网络版客户端更新过程 第 6-30 页。
      - **只能从防毒墙网络版服务器下载更新客户端更新组件、域设置以及客户端程序和 Hot Fix**
      - 如果所有定制源均不可用或未找到，则防毒墙网络版客户端从防毒墙网络版服务器更新以下项目：
        - **组件**
        - **域设置**
        - **防毒墙网络版客户端程序和 Hot Fix**

   b. 如果至少指定了一个更新代理作为源，则单击**更新代理分析报告**生成一份报告，突出显示客户端的更新状态。有关该报告的详细信息，请参阅更新代理分析报告 第 6-56 页。

   c. 通过单击 IP 地址范围链接来编辑更新源。在显示的窗口中修改设置，然后单击**保存**。

   d. 通过选中复选框然后单击**删除**将更新源从该列表中移除。

   e. 要移动更新源，请单击向上箭头或向下箭头。每次仅可移动一个源。
7. 单击**通知所有客户端**。

防毒墙网络版客户端更新过程

注意

本主题讨论防毒墙网络版客户端的更新过程。更新代理的更新过程在更新代理的定制更新源 第 6-52 页中进行讨论。

在设置并保存定制更新源列表后，更新过程按如下方式进行：

1. 防毒墙网络版客户端从列表上的第一个源更新。
2. 如果无法从第一个源更新，则防毒墙网络版客户端将从第二个源更新，依此类推。
3. 如果无法从所有源更新，防毒墙网络版客户端将检查**更新源**窗口上的以下设置：

表 6-7. 定制更新源的其他设置

设置	描述
只能从防毒墙网络版服务器下载更新客户端更新组件、域设置以及客户端程序和 Hot Fix	如果启用此设置，更新代理将直接从防毒墙网络版服务器更新，并忽略定制的更新源列表。 如果禁用此设置，更新代理将应用为普通客户端配置的定制更新源设置。
如果所有定制源均不可用或未找到，则防毒墙网络版客户端从防毒墙网络版服务器更新以下项目：	

设置	描述
组件	如果启用该设置，则客户端从防毒墙网络版服务器更新组件。 如果禁用该设置，则在满足以下任一条件时，客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器： • 在**客户端** > **客户端管理**中，单击**设置** > **权限和其他设置** > **其他设置（选项卡）** > **更新设置**，将启用**防毒墙网络版客户端从趋势科技 ActiveUpdate 服务器下载更新**选项。 • ActiveUpdate 服务器未包括在“定制的更新源列表”中。 **注意** 只能从 ActiveUpdate 服务器更新组件。只能从防毒墙网络版服务器或更新代理下载域设置、程序和 Hot Fix。可以通过将客户端配置为仅从 ActiveUpdate 服务器下载特征码文件来加速更新过程。有关详细信息，请参阅作为防毒墙网络版客户端更新源的 ActiveUpdate 服务器 第 6-34 页。
域设置	如果启用该设置，则客户端从防毒墙网络版服务器更新域级设置。
防毒墙网络版客户端程序和 Hot Fix	如果启用该设置，则客户端从防毒墙网络版服务器更新程序和 Hot Fix。

4. 如果无法从所有可能的源更新，则客户端将退出更新过程。

作为防毒墙网络版客户端更新源的 ActiveUpdate 服务器

防毒墙网络版客户端直接从趋势科技 ActiveUpdate 服务器下载更新时，您可以限制仅下载特征码文件以减少更新时消耗的带宽并加速更新过程。

扫描引擎和其他组件的更新不像特征码文件的更新那样频繁，这是限制仅下载特征码文件的另一个原因。

无法直接通过趋势科技 ActiveUpdate 服务器更新纯 IPv6 客户端。要使防毒墙网络版客户端连接到 ActiveUpdate 服务器，需提供可以转换 IP 地址的双栈代理服务器（如 DeleGate）。

限制从 ActiveUpdate 服务器下载

过程

1. 转至**客户端** > **全局客户端设置**。
2. 转至**更新**部分。
3. 选择**执行更新时仅从 Activeupdate 服务器下载特征码文件**。

防毒墙网络版客户端更新方法

从防毒墙网络版服务器或定制的更新源更新组件的防毒墙网络版客户端可以使用以下更新方法：

- **自动更新**：客户端更新在发生某些事件时自动运行，或根据时间表运行。有关详细信息，请参阅防毒墙网络版客户端自动更新 第 6-35 页。
- **手动更新**：如果更新非常重要，请使用手动更新以立即通知客户端执行组件更新。有关详细信息，请参阅防毒墙网络版客户端手动更新 第 6-40 页。
- **基于权限的更新**：具有更新权限的用户可更好地控制在其计算机上更新防毒墙网络版客户端的方式。有关详细信息，请参阅配置更新权限和其他设置 第 6-42 页。

防毒墙网络版客户端自动更新

自动更新免除了您通知所有客户端更新的负担，并消除了客户端计算机没有最新组件的风险。

除这些组件外，防毒墙网络版客户端还可在自动更新过程中接收更新的配置文件。客户端需要这些配置文件应用新的设置。每次通过 Web 控制台修改防毒墙

网络版设置时，配置文件也随之更改。要指定将配置文件应用于客户端的频率，请参阅步骤 3 配置防毒墙网络版客户端自动更新 第 6-37 页。

注意

可以将客户端配置为在自动更新过程中使用代理服务器设置。请参阅用于防毒墙网络版客户端组件更新的代理服务器 第 6-45 页以了解详细信息。

有以下两种类型的自动更新：

- 事件触发更新 第 6-36 页
- 基于时间表更新 第 6-37 页

事件触发更新

服务器可以通知联机客户端在下载最新组件后更新组件，还可以在脱机客户端重新启动并连接到服务器时通知它们。可选择在更新后是否对防毒墙网络版客户端计算机启动立即扫描（手动扫描）。

表 6-8. 由事件触发的更新选项

选项	描述
防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新	服务器在完成更新后立即通知客户端进行更新。频繁更新的客户端只需下载增量特征码，因此缩短了完成更新所用的时间（有关增量特征码的详细信息，请参阅防毒墙网络版服务器组件复制 第 6-20 页）。但是，频繁更新可能会对服务器性能产生负面影响，尤其是大量的客户端同时更新时。 如果具有处于漫游模式的客户端，并且还希望更新这些客户端，请选择包括漫游客户端和脱机客户端。有关漫游模式的详细信息，请参阅防毒墙网络版客户端漫游权限 第 14-19 页。
使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新 (漫游客户端除外)	错过更新的任何客户端在建立与服务器的连接时立即下载组件。如果客户端处于脱机状态，或者安装了客户端的终端没有启动和运行，则客户端可能会错过更新。
更新后执行“立即扫描”（漫游客户端除外）	服务器通知客户端在事件触发更新之后扫描。如果特定更新是对网络内已传播的安全风险的响应，请考虑启用此选项。

注意

如果防毒墙网络版服务器在下载组件后，无法向客户端成功发送更新通知，则会在 15 分钟自动重新发送通知。服务器在客户端响应之前连续发送更新通知，最多 5 次。如果第五次尝试未成功，则服务器会停止发送通知。如果选择在客户端重新启动时更新组件的选项，然后连接到服务器，则组件更新将仍然继续。

基于时间表更新

运行预设更新是一种权限。需要首先选择具有该权限的防毒墙网络版客户端，然后这些防毒墙网络版客户端将基于时间表运行更新。

注意

要将基于时间表的更新与网络地址转换一起使用，请参阅配置使用 NAT 的预设防毒墙网络版客户端更新 第 6-38 页。

配置防毒墙网络版客户端自动更新

过程

1. 转至**更新** > **客户端** > **自动更新**。
2. 选择**事件触发更新**的事件。
   - **防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新**
     - **包括漫游客户端和脱机客户端**
   - **使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新 (漫游客户端除外)**
   - **更新后执行“立即扫描”（漫游客户端除外）**

   有关可用选项的详细信息，请参阅事件触发更新 第 6-36 页。
3. 配置**基于时间表更新**的时间表。
   - **分钟**或**小时**

当预设每小时一次或以分钟计算的更新频率时，**每天只更新一次客户端配置**选项可用。配置文件包含使用 Web 控制台配置的所有防毒墙网络版客户端设置。

提示

趋势科技会经常更新组件；但是，防毒墙网络版配置设置可能更改不是很频繁。使用组件更新配置文件需要更多的带宽，还会增加防毒墙网络版完成更新所需的时间。出于这个原因，趋势科技建议每天只更新一次防毒墙网络版客户端配置。

- **每日一次**或**每周一次**

  指定更新的时间以及防毒墙网络版服务器通知客户端更新组件的时间段。

  提示

  此设置可防止所有的联机客户端在指定的开始时间同时连接到服务器，极大地减少指向服务器的流量。例如，如果开始时间为中午 12 点，时间段为 2 个小时，则防毒墙网络版会随机通知所有联机客户端从中午 12 点到下午 2 点更新组件。

注意

配置更新时间表后，启用选定客户端上的时间表。有关启用基于时间表的更新的详细信息，请参阅配置更新权限和其他设置 第 6-42 页的步骤 4。

4. 单击**保存**。

   防毒墙网络版无法立即通知脱机客户端。选择**使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新（漫游客户端除外）**更新在时间段到期后变为联机的脱机客户端。未启用此设置的脱机客户端会在下一个时间表或在手动更新期间更新组件。

配置使用 NAT 的预设防毒墙网络版客户端更新

如果本地网络使用 NAT，则可能出现下列问题：

- 防毒墙网络版客户端在 Web 控制台上显示为脱机。
- 防毒墙网络版服务器无法成功通知客户端更新和配置更改。

通过使用如下所述的预设更新将更新的组件和配置文件从服务器部署到防毒墙网络版客户端来解决这些问题。

过程

- 在客户端计算机上安装防毒墙网络版客户端之前：
  a. 在**更新** > **客户端** > **自动更新**的**基于时间表更新**部分中配置客户端更新时间表。
  b. 在**客户端** > **客户端管理**中授予客户端启用预设更新的权限，单击**设置** > **权限和其他设置** > **权限选项卡** > **组件更新**。
- 如果在客户端计算机上已存在防毒墙网络版客户端：
  a. 在**客户端** > **客户端管理**中授予客户端“立即更新”的权限，单击**设置** > **权限和其他设置** > **权限选项卡** > **组件更新**。
  b. 指导用户手动更新客户端终端上的组件（通过右键单击系统托盘中的防毒墙网络版客户端图标，然后单击“立即更新”）以获取更新的配置设置。

防毒墙网络版客户端客户端更新时，会收到更新的组件和配置文件。

使用域预设更新工具

在自动客户端更新中配置的更新时间表仅适用于具有预设更新权限的客户端。对于其他客户端，可以设置单独的更新时间表。要执行此操作，您需要按客户端树域配置时间表。属于域的所有客户端都将应用此时间表。

注意

无法为特定客户端或特定子域设置更新时间表。所有子域都应用为其父域配置的时间表。

过程

1. 记录客户端树域名称和更新时间表。
2. 转到 <服务器安装文件夹>\PCCSRV\Admin\Utility\DomainScheduledUpdate。
3. 将以下文件复制到 <服务器安装文件夹>\PCCSRV：
   - DomainSetting.ini
   - dsu_convert.exe
4. 使用文本编辑器（如记事本）打开 DomainSetting.ini。
5. 指定客户端树域，然后配置域的更新时间表。重复执行该步骤可以添加更多域。

   注意

   该 .ini file 文件中提供了详细的配置说明。

6. 保存 DomainSetting.ini。
7. 打开命令提示符，然后更改为 PCCSRV 文件夹的目录。
8. 键入以下命令并按 `Enter` 键。

   ```
   dsuconvert.exe DomainSetting.ini
   ```

9. 在 Web 控制台上，转至**客户端** > **全局客户端设置**。
10. 单击**保存**。

防毒墙网络版客户端手动更新

防毒墙网络版客户端组件严重过期和有爆发时手动更新防毒墙网络版客户端组件。防毒墙网络版客户端较长时间无法从更新源更新组件时，防毒墙网络版客户端件将严重过期。

除这些组件外，防毒墙网络版客户端还可在手动更新过程中接收更新的配置文件。防毒墙网络版客户端需要这些配置文件应用新的设置。每次通过 Web 控制台修改防毒墙网络版设置时，配置文件也随之更改。

注意

除启动手动更新外，还可以授予用户运行手动更新（在防毒墙网络版客户端终端上也称为**立即更新**）的权限。有关详细信息，请参阅配置更新权限和其他设置 第 6-42 页。

手动更新防毒墙网络版客户端

过程

1. 转至**更新** > **客户端** > **手动更新**。
2. 在窗口的顶部将显示防毒墙网络版服务器上当前可用的组件和上次更新这些组件的日期。在通知客户端更新之前，请确保组件是最新的。

   注意

   手动更新服务器上的任何过期组件。请参阅防毒墙网络版客户端手动更新 第 6-40 页以了解详细信息。

3. 仅更新带有过期组件的客户端：
   a. 单击**选择带有过期组件的客户端**。
   b. （可选）选择**包括漫游客户端和脱机客户端**：
      - 更新与服务器具有有效连接的漫游客户端。
      - 脱机客户端变为联机状态时，更新它们。
   c. 单击**开始更新**。

   注意

   服务器搜索其组件版本早于服务器上版本的客户端，然后通知这些客户端进行更新。要检查通知状态，请转至**更新** > **摘要**窗口。

4. 更新选择的客户端：

   a. 选择**手动选择客户端**。

   b. 单击**选择**。

   c. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。

   d. 单击**启动组件更新**。

   注意

   服务器开始通知每台客户端下载更新过的组件。要检查通知状态，请转至**更新** > **摘要**窗口。

配置更新权限和其他设置

配置更新设置并授予客户端用户某些权限，如执行“立即更新”和启用预设更新。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡并配置**更新设置**部分中的以下选项：

选项	说明
防毒墙网络版客户端从趋势科技 ActiveUpdate	启动更新时，防毒墙网络版客户端首先从**更新** > **客户端** > **更新源**窗口中指定的更新源中获得更新。

选项	说明
服务器下载更新	如果更新未成功，则客户端会尝试从防毒墙网络版服务器进行更新。如果从防毒墙网络版服务器更新未成功，则选择此选项可使客户端能够尝试从趋势科技 ActiveUpdate 服务器进行更新。 **注意** 无法直接通过趋势科技 ActiveUpdate 服务器更新纯 IPv6 客户端。要使客户端连接到 ActiveUpdate 服务器，需提供可以转换 IP 地址的双栈代理服务器（如 DeleGate）。
在防毒墙网络版客户端上启用基于时间表的更新	缺省情况下，选择此选项会将所有防毒墙网络版客户端配置为启用基于时间表更新。具有**启用/禁用基于时间表的更新**权限的用户可以覆盖此设置。 有关配置该更新时间表的详细信息，请参阅配置防毒墙网络版客户端自动更新 第 6-37 页。
防毒墙网络版客户端可以更新组件，但不能升级客户端程序，也不能部署 hotfix	此选项允许继续进行组件更新，但是会阻止部署 Hot Fix 和升级防毒墙网络版客户端。 **注意** 禁用此选项可能会严重影响服务器的性能，因为所有客户端会同时连接到服务器进行升级或安装 hotfix。

5. 单击**权限**选项卡并配置**组件更新**部分中的以下选项：

选项	说明
执行“立即更新”	具有此权限的用户可以右键单击系统托盘上的防毒墙网络版客户端图标并选择**立即更新**以按需更新组件。 **注意** 防毒墙网络版客户端用户可以在“立即更新”的过程中使用代理服务器设置。 请参阅客户端的代理服务器配置权限 第 14-46 页以了解详细信息。
启用/禁用基于时间表的更新	选择此选项允许防毒墙网络版客户端用户使用防毒墙网络版客户端右键单击菜单来启用和禁用预设更新，还可以覆盖**启用基于时间表的更新**设置。

选项	说明
	注意 管理员必须首先在**其他设置**选项卡上选择**在客户端上启用基于时间表的更新**设置，然后菜单项才会显示在防毒墙网络版客户端菜单上。

6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

配置为防毒墙网络版客户端更新保留的磁盘空间

防毒墙网络版可以为 Hotfix、特征码文件、扫描引擎和程序更新分配一定量的客户端磁盘空间。缺省情况下，防毒墙网络版保留 60MB 的磁盘空间。

过程

1. 转至**客户端 > 全局客户端设置**。
2. 转至**保留的磁盘空间**部分。
3. 选择**保留 __ MB 磁盘空间用于更新**。
4. 选择磁盘空间量。
5. 单击**保存**。

用于防毒墙网络版客户端组件更新的代理服务器

在自动更新期间，或者如果防毒墙网络版客户端具有执行“立即更新”的权限，则它们可以使用代理服务器设置。

表 6-9. 防毒墙网络版客户端组件更新过程中使用的代理服务器设置

更新方法	使用的代理服务器设置	用法
自动更新	• 自动代理服务器设置。有关详细信息，请参阅防毒墙网络版客户端的自动代理服务器设置 第 14-48 页。 • 内部代理服务器设置。有关详细信息，请参阅防毒墙网络版客户端的内部代理服务器 第 14-44 页。	1. 防毒墙网络版客户端将首先使用自动代理服务器设置来更新组件。 2. 如果未启用自动代理服务器设置，则将使用内部代理服务器设置。 3. 如果两种设置都禁用，则客户端将不使用任何代理服务器设置。
立即更新	• 自动代理服务器设置。有关详细信息，请参阅防毒墙网络版客户端的自动代理服务器设置 第 14-48 页。 • 用户配置的代理服务器设置。可以授予客户端用户配置代理服务器设置的权限。有关详细信息，请参阅客户端的代理服务器配置权限 第 14-46 页。	1. 防毒墙网络版客户端将首先使用自动代理服务器设置来更新组件。 2. 如果未启用自动代理服务器设置，则将使用用户配置的代理服务器设置。 3. 如果两种配置都禁用，或者如果禁用了自动代理服务器设置且客户端用户没有所需的权限，则更新组件时客户端将不使用任何代理服务器。

配置防毒墙网络版客户端更新通知

当发生与更新相关的事件时，防毒墙网络版将通知客户端用户。

过程

1. 转至**客户端 > 全局客户端设置**。
2. 转至**警报设置**部分。
3. 选择下列选项：
   - **如果病毒码文件在 __ 天后没有更新，则在 Windows 任务栏上显示警报图标**：在 Windows 任务栏上显示一个警报图标，提醒用户更新在指定天数内未更新的病毒码。要更新病毒码，请使用防毒墙网络版客户端更新方法 第 6-35 页中介绍的任何一种更新方法。

     服务器管理的所有客户端都将应用此设置。
   - **如果终端需要重新启动以加载内核模式驱动程序，则显示通知消息**：安装 hotfix 或包括新版本的内核模式驱动程序的升级软件包后，驱动程序的前一版本可能仍然在终端上。退出前一版本并安装新版本的唯一方法是重新启动终端。重新启动终端后，将自动安装新版本，无需再重新启动。

     客户端终端在安装 Hotfix 或升级软件包后，通知消息会立即显示。
4. 单击**保存**。

查看防毒墙网络版客户端更新日志

检查客户端更新日志，以确定在客户端上更新病毒码时是否存在问题。

注意

在此产品版本中，只能从 Web 控制台查询病毒码更新的日志。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

过程

1. 转至**日志** > **客户端** > **客户端组件更新**。
2. 要查看客户端更新数，请单击**进度**列下的**查看**。在显示的**组件更新进度**窗口中，查看每间隔 15 分钟更新的客户端数以及更新的客户端总数。
3. 要查看已更新病毒码的客户端，请单击**详细信息**列下的**查看**。
4. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

执行防毒墙网络版客户端更新

使用安全合规可确保客户端具有最新组件。安全合规可确定防毒墙网络版服务器和客户端之间不一致的组件。客户端无法连接到服务器以更新组件时，通常会发生不一致。如果客户端从其他源（例如 ActiveUpdate 服务器）获得更新，则客户端中的组件可能会比服务器中的组件更新。

有关详细信息，请参阅受管理客户端的安全合规 第 14-51 页。

还原防毒墙网络版客户端的组件

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。防毒墙网络版保留病毒扫描引擎的当前版本和先前版本，以及病毒码和云安全客户端病毒码的最近五个版本。

注意

只能还原上述组件。

防毒墙网络版对于运行 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. 转至**更新** > **还原**。
2. 单击相应部分下面的**与服务器同步**。
   a. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
   b. 单击**还原**。
   c. 单击**查看更新日志**检查结果，或单击**上一步**返回到“还原”窗口。
3. 如果服务器上存在较早版本的特征码文件，则单击**还原服务器和客户端版本**同时还原防毒墙网络版客户端和服务器的特征码文件。

运行防毒墙网络版客户端 Hot Fix 的触探工具

“触探工具”会将一个文件的时间戳与另一个文件的时间戳或终端的系统时间进行同步。如果您尝试在防毒墙网络版服务器上部署 Hot Fix 未成功，请使用“触探工具”更改该 Hot Fix 的时间戳。这将使防毒墙网络版将该 Hot Fix 文件解释为新文件，从而使服务器再次尝试自动部署此 Hot Fix。

过程

1. 在防毒墙网络版服务器上，转到 <服务器安装文件夹>\PCCSRV\Admin\Utility\Touch。
2. 将 TMTouch.exe 复制到包含有要更改的文件的文件夹。如果要将文件的时间戳与另一个文件的时间戳进行同步，请使用“触探工具”将两个文件放在同一位置。
3. 打开命令提示窗口，然后转到“触探工具”的位置。
4. 键入以下命令：

   ```
   TmTouch.exe <目标文件名> <源文件名>
   ```

   其中：

- `<目标文件名>` 是要更改其时间戳的 Hotfix 文件的名称
- `<源文件名>` 是要复制其时间戳的文件的名称



注意

如果未指定源文件名，该工具会将目标文件时间戳设置为终端的系统时间。对目标文件使用通配符 (*)，但不能对源文件名使用。

5. 要检查时间戳是否已更改，请在命令提示符下键入 `dir`，或者在 Windows 资源管理器中检查文件的属性。

更新代理

要向防毒墙网络版客户端分发部署组件、域设置或客户端程序和 hotfix 的任务，请指定一些防毒墙网络版客户端充当更新代理或其他客户端的更新源。这有助于确保客户端及时接收更新，而不用将大量的网络通信定向于防毒墙网络版服务器。

如果网络按位置分段，且各段之间的网络链路流量负载较大，应在每个位置上至少指定一个更新代理。



注意

指定从更新代理更新组件的防毒墙网络版客户端仅从更新代理接收更新的组件和设置。所有防毒墙网络版客户端仍会将它们的状态报告返回给防毒墙网络版服务器。

更新代理的系统要求

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/enterprise/officescan.aspx

更新代理配置

更新代理配置过程分为两步：

1. 将防毒墙网络版客户端指定为特定组件的更新代理。
2. 指定将从此更新代理更新的客户端。

注意

单个更新代理可以处理的并行客户端连接的数量取决于终端的硬件规格。

将防毒墙网络版客户端指定为更新代理

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，选择要指定为更新代理的客户端。

注意

无法选择根域图标，因为这会将所有客户端指定为更新代理。纯 IPv6 更新代理无法直接向纯 IPv4 客户端分发更新。同样，纯 IPv4 更新代理也无法直接向纯 IPv6 客户端分发更新。为允许更新代理向客户端分发更新，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

3. 单击**设置** > **更新代理设置**。
4. 选择更新代理可以共享的项目。
   - 组件更新
   - 域设置
   - 防毒墙网络版客户端程序和 Hot Fix
5. 单击**保存**。

指定将从更新代理更新的防毒墙网络版客户端

过程

1. 转至**更新** > **客户端** > **更新源**。
2. 在**定制的更新源列表**下，单击**添加**。
3. 在显示的窗口中，指定客户端的 IP 地址。可以键入 IPv4 范围和/或 IPv6 前缀和长度。
4. 在**更新代理**文本框中，选择要为客户端指定的更新代理。

   注意

   确保客户端可以使用其 IP 地址连接到更新代理。例如，如果指定了 IPv4 地址范围，更新代理必须具有 IPv4 地址。如果指定 IPv6 前缀和长度，更新代理必须具有 IPv6 地址。

5. 单击**保存**。

更新代理的更新源

更新代理可以从各种源（如防毒墙网络版服务器或定制的更新源）获取更新。可以从 Web 控制台的“更新源”窗口配置更新源。

更新代理的 IPv6 支持

纯 IPv6 更新代理无法直接从纯 IPv4 更新源更新，例如：

- 纯 IPv4 防毒墙网络版服务器
- 任何纯 IPv4 定制更新源
- 趋势科技 ActiveUpdate 服务器

同样，纯 IPv4 更新代理无法直接从纯 IPv6 更新源（例如纯 IPv6 防毒墙网络版服务器）更新。

为允许更新代理连接到更新源，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

更新代理标准更新源

防毒墙网络版服务器是更新代理的标准更新源。如果将客户端配置为直接从防毒墙网络版服务器更新，则更新过程按如下方式进行：

1. 更新代理从防毒墙网络版服务器获取更新。
2. 如果无法从防毒墙网络版服务器更新，则在满足以下任一条件时，客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器：
   - 在**客户端** > **客户端管理**中，单击**设置** > **权限和其他设置** > **其他设置** > **更新设置**，将启用**防毒墙网络版客户端从趋势科技 ActiveUpdate 服务器下载更新**选项。
   - ActiveUpdate 服务器是“定制的更新源列表”中的第一个条目。

   提示

   仅当从防毒墙网络版服务器更新遇到问题时，才将 ActiveUpdate 服务器放置在列表的顶部。当更新代理直接从 ActiveUpdate 服务器更新时，在网络和 Internet 之间会占用很大的带宽。
3. 如果无法从所有可能的源更新，则更新代理将退出更新过程。

更新代理的定制更新源

除了防毒墙网络版服务器外，更新代理还可以从定制更新源进行更新。定制更新源有助于减少定向到防毒墙网络版服务器的客户端更新流量。在定制的更新源列表（最多可容纳 1024 个更新源）上指定定制的更新源。有关配置列表的步骤，请参阅防毒墙网络版客户端的定制更新源 第 6-31 页。

注意

为了将更新代理连接到定制更新源，请确保在**客户端的更新源**窗口（**更新** > **客户端** > **更新源**）上禁用**只能从防毒墙网络版服务器下载更新代理更新组件、域设置以及客户端程序和 Hot Fix** 选项。

在设置并保存列表后，更新过程按如下方式进行：

1. 更新代理从列表上的第一个条目更新。
2. 如果无法从第一个条目更新，则客户端将从第二个条目更新，依此类推。
3. 如果无法从所有条目中更新，则客户端将检查**如果所有定制源均不可用或未找到，则防毒墙网络版客户端从防毒墙网络版服务器更新以下项目**标题下的以下选项：
   - **组件**：如果已启用，则客户端从防毒墙网络版服务器更新。

     如果禁用该选项，则在满足以下任一条件时，客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器：

     注意

     只能从 ActiveUpdate 服务器更新组件。只能从服务器或更新代理下载域设置、程序和 Hot Fix。

     - 在**客户端** > **客户端管理**中，单击**设置** > **权限和其他设置** > **其他设置** > **更新设置**，将启用**客户端从趋势科技 ActiveUpdate 服务器下载更新**选项。
     - ActiveUpdate 服务器未包括在“定制的更新源列表”中。
   - **域设置**：如果已启用，则客户端从防毒墙网络版服务器更新。
   - **防毒墙网络版客户端程序和 Hot Fix**：如果已启用，则客户端从防毒墙网络版服务器更新。
4. 如果无法从所有可能的源更新，则更新代理将退出更新过程。

如果选项**标准更新源 (从防毒墙网络版服务器更新)** 已启用，并且防毒墙网络版服务器通知客户端更新组件，则更新过程有所不同。过程如下：

1. 客户端直接从防毒墙网络版服务器更新，并忽略更新源列表。
2. 如果无法从服务器更新，则在满足以下任一条件时，客户端会尝试直接连接到趋势科技 ActiveUpdate 服务器：
   - 在**客户端** > **客户端管理**中，单击**设置** > **权限和其他设置** > **其他设置** > **更新设置**，将启用**防毒墙网络版客户端从趋势科技 ActiveUpdate 服务器下载更新**选项。
   - ActiveUpdate 服务器是“定制的更新源列表”中的第一个条目。



提示

仅当从防毒墙网络版服务器更新遇到问题时，才将 ActiveUpdate 服务器放置在列表的顶部。当防毒墙网络版客户端直接从 ActiveUpdate 服务器更新时，在网络和 Internet 之间会占用大量带宽。

3. 如果无法从所有可能的源更新，则更新代理将退出更新过程。

配置更新代理的更新源

过程

1. 转至**更新** > **客户端** > **更新源**。
2. 选择是从更新代理的标准更新源（防毒墙网络版服务器）还是更新代理的定制更新源更新。
3. 单击**通知所有客户端**。

更新代理组件复制

与防毒墙网络版服务器类似，更新代理也可在下载组件时使用组件复制。有关服务器如何执行组件复制的详细信息，请参阅防毒墙网络版服务器组件复制 第 6-20 页。

更新代理的组件复制过程如下所述：

1. 更新代理将其当前完整特征码版本与更新源上的最新版本进行比较。如果两个版本之间的差值小于等于 14，则更新代理只下载代表这两个版本差值的增量特征码。

   注意

   如果此差值大于 14，则更新代理自动下载完全版的特征码文件。

2. 更新代理将其下载的增量特征码和其当前完全特征码合并以生成最新的完全特征码。
3. 更新代理下载更新源上的所有剩余增量特征码。
4. 客户端可以使用最新的完全特征码和所有增量特征码。

更新代理的更新方法

更新代理使用可供常规客户端使用的相同更新方法。有关详细信息，请参阅防毒墙网络版客户端更新方法 第 6-35 页。

也可以使用预设更新配置工具，在使用客户端打包程序安装的更新代理上启用和配置预设更新。

注意

如果更新代理是使用其他安装方法安装的，则此工具不可用。请参阅部署注意事项 第 5-10 页以获取详细信息。

使用预设更新配置工具

过程

1. 在更新代理终端上，导航到 <客户端安装文件夹>。
2. 双击 SUCTool.exe 运行该工具。预设更新配置工具控制台将打开。
3. 选择**启用预设更新**。

4. 指定更新频率和时间。

5. 单击**应用**。

更新代理分析报告

生成更新代理分析报告来分析更新基础架构，并确定哪些客户端从更新代理和其他更新源下载部分更新。

注意

该报告包括配置为从更新代理获取部分更新的所有防毒墙网络版客户端。如果已将管理一个或多个域的任务委派给其他管理员，则他们还将看到所有防毒墙网络版客户端，这些客户端配置为从属于不在其管理范围内的域中的更新代理获取部分更新。

防毒墙网络版将更新代理分析报告导出为逗号分隔值 (.csv) 文件。

此报告包含以下信息：

- 防毒墙网络版客户端 终端
- IP 地址
- 客户端树路径
- 更新源
- 如果客户端从更新代理下载以下内容：
  - 组件
  - 域设置
  - 防毒墙网络版客户端程序和 Hot Fix

重要信息

更新代理分析报告仅列出已配置为从更新代理中获取部分更新的防毒墙网络版客户端。报告中将不会显示已配置为从更新代理（包括组件、域设置和防毒墙网络版客户端程序和 Hot Fix）中执行完整更新的防毒墙网络版客户端。

有关生成报告的详细信息，请参阅防毒墙网络版客户端的定制更新源 第 6-31 页。

组件更新摘要

Web 控制台提供了**更新摘要**窗口（转至**更新** > **摘要**），通知您总体组件更新状态，使您可以更新过期的组件。如果启用服务器预设更新，则该窗口还将显示下一个更新时间表。

定期刷新窗口以查看最新的组件更新状态。

注意

要在集成型云安全智能防护服务器上查看组件更新，请转至**管理** > **云安全智能防护** > **集成服务器**。

防毒墙网络版客户端的更新状态

如果启动了对客户端的组件更新，请查看此部分中的以下信息：

- 已通知更新组件的客户端数。
- 尚未收到通知，但已经在通知队列中的客户端数。要取消通知这些客户端，请单击**取消通知**。

组件

在**更新状态**表中，查看防毒墙网络版服务器下载和分发的每个组件的更新状态。

对于每个组件，查看其当前版本和上次更新日期。单击编号链接以查看具有过期组件的客户端。手动更新具有过期组件的客户端。

第 7 章

扫描安全风险

本章讲述如何使用基于文件的扫描来保护终端免遭安全风险的危害。

主题包括：

- 关于安全风险 第 7-2 页
- 扫描方法类型 第 7-7 页
- 扫描类型 第 7-12 页
- 所有扫描类型的通用设置 第 7-22 页
- 扫描权限和其他设置 第 7-47 页
- 全局扫描设置 第 7-62 页
- 安全风险通知 第 7-72 页
- 安全风险日志 第 7-81 页
- 安全风险爆发 第 7-94 页

关于安全风险

安全风险是病毒/恶意软件和间谍软件/灰色软件的统称。防毒墙网络版通过扫描文件，然后对每一个检测到的安全风险执行特定的处理措施来保护计算机免遭安全风险的侵扰。在短时间内检测到数量庞大的安全风险意味着病毒爆发。通过强制执行爆发阻止策略并且隔离受感染的计算机直到它们完全不存在风险，防毒墙网络版可以帮助抑制爆发。如果需要立即采取措施，通知和日志可帮助您跟踪安全风险和警报。

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。虽然终端病毒一度流行于 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，其会导致更大量的损害。

表 7-1. 病毒/恶意软件类型

病毒/恶意软件类型	描述
恶作剧程序	恶作剧程序是类似病毒的程序，它通常通过某种操控而使终端显示器中显示某些内容。
其他	“其他”包括未归类在任何其他病毒/恶意软件类型下的病毒/恶意软件。
加壳软件	加壳软件是压缩和/或加密的 Windows 或 Linux™ 可执行程序，通常是特洛伊木马程序。压缩可执行文件会使防病毒产品检测加壳软件更加困难。
Rootkit	rootkit 是在最终用户未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。
测试病毒	测试病毒是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。

病毒/恶意软件类型	描述
特洛伊木马	特洛伊木马程序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	病毒是会执行复制的程序。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。 • **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他终端系统（通常通过电子邮件）。
网络病毒	严格地讲，通过网络传播的病毒不一定是网络病毒。只有部分病毒/恶意软件类型（例如，蠕虫病毒）才称得上是网络病毒。明确地讲，网络病毒是指利用网络协议（比如 TCP、FTP、UDP、HTTP 和电子邮件协议）进行复制的一类病毒。它们通常不篡改系统文件或修改硬盘驱动器的引导区。网络病毒感染客户端终端的内存，强制客户端用通信淹没网络，引起延迟甚至网络完全瘫痪。由于网络病毒保留在内存里，因此一般的基于 I/O 的文件扫描方法通常检测不到。

病毒/恶意软件类型	描述
潜在病毒/恶意软件	潜在病毒/恶意软件是具有某些病毒/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 **注意** 不能对潜在病毒/恶意软件执行清除，但是扫描处理措施是可配置的。

间谍软件和灰色软件

终端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终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，以及将终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防毒墙网络版检测为灰色软件，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	更改终端的 Internet 设置，并强制终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。

类型	描述
恶作剧程序	导致终端行为异常，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。

间谍软件/灰色软件如何侵入网络

间谍软件/灰色软件通常在用户下载安装包中附带灰色软件应用程序的正版软件时侵入公司网络。大多数软件程序都包含最终用户许可协议 (EULA)，用户必须接受该协议才能继续下载。通常，EULA 确实包含有关应用程序以及收集个人数据的预定用途的信息；但是，用户经常会忽视此信息或对法律专用术语不了解。

潜在风险和威胁

如果网络上存在有间谍软件和其他类型的灰色软件，则可能会导致以下后果：

表 7-2. 潜在风险和威胁

风险或威胁	描述
降低终端性能	为完成它们的任务，间谍软件/灰色软件应用程序经常需要大量的 CPU 和系统内存资源。
与 Web 浏览器相关的崩溃增加	某些类型的灰色软件（例如，广告程序），经常会在一个浏览器框或窗口中显示信息。根据这些应用程序中的代码与系统进程交互的方式，灰色软件有时可以导致浏览器崩溃或锁死，甚至可能要求终端重新启动。
降低用户效率	由于需要关闭经常出现的弹出广告及处理恶作剧程序的负面影响，用户将不必要地打断他们的主要任务。

风险或威胁	描述
降低网络带宽	间谍软件/灰色软件应用程序通常会将它们收集的数据定期传送给网络上或网络之外运行的其他应用程序。
丢失个人和公司信息	间谍软件/灰色软件应用程序收集的所有数据并非都如同用户访问的 Web 站点列表一样是无害的。间谍软件/灰色软件还可以收集用户凭证，例如用于访问联机银行帐户和公司网络的凭证。
法律责任风险增加	如果网络上的终端资源被劫持，黑客就有可能利用客户端计算机在网络外的计算机上发动攻击或安装间谍软件/灰色软件。如果网络资源参与这些类型的活动，将可能使组织承担由其他方造成的损失而引发的法律责任。

防御间谍软件/灰色软件及其他威胁

可以采取许多步骤以阻止在您的 终端 上安装间谍软件/灰色软件。趋势科技推荐以下步骤：

- 配置所有类型的扫描（手动扫描、实时扫描、预设扫描和立即扫描）以扫描和移除间谍软件/灰色软件文件和应用程序。请参阅扫描类型 第 7-12 页以获取详细信息。
- 培养您的客户端进行以下操作：
  - 阅读已下载并安装到他们的计算机上的应用程序的“最终用户许可协议 (EULA)”以及随附的文档。
  - 对于要求授权以下载并安装软件的任何消息都单击否，除非客户端用户确信该软件的创建者和他们查看的 Web 站点都可信。
  - 忽略不请自来的商业电子邮件（垃圾邮件），特别是要求用户单击按钮或超链接的垃圾邮件。
- 配置 Web 浏览器设置，以确保使用严格的安全级别。趋势科技建议要求 Web 浏览器在安装 ActiveX 控件之前提示用户。
- 如果使用 Microsoft Outlook，请配置安全设置以使 Outlook 不会自动下载 HTML 项，例如通过垃圾邮件发送的图片。
- 请勿使用对等文件共享服务。间谍软件及其他灰色软件应用程序威胁可能会伪装成用户希望下载的其他类型的文件，例如 MP3 音乐文件。

- 定期检查客户端计算机上已安装的软件，并查找可能属于间谍软件或其他灰色软件的应用程序。
- 为 Windows 操作系统安装 Microsoft 提供的最新修补程序使之保持最新状态。有关详细信息，请访问 Microsoft Web 站点。

扫描方法类型

在扫描安全风险时，防毒墙网络版客户端可以使用两种扫描方法中的任意一种。扫描方法包括云安全扫描和传统扫描。

- **云安全扫描**

  使用云安全扫描的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**

  不使用云安全扫描的客户端称为**传统扫描客户端**。传统扫描客户端将所有防毒墙网络版组件存储在客户端 终端上，并在本地扫描所有文件。

缺省扫描方法

在此版本的防毒墙网络版中，全新安装的缺省扫描方法是云安全扫描。这就意味着，如果您执行防毒墙网络版服务器全新安装且没有在 Web 控制台上更改扫描方法，则该服务器管理的所有客户端都将使用云安全扫描。

如果防毒墙网络版服务器是从早期版本升级而来，并且启用了自动客户端升级，则该服务器管理的所有客户端仍将使用在升级之前配置的扫描方法。例如，如果从支持云安全扫描和传统扫描的防毒墙网络版 10 进行升级，则使用云安全扫描的所有已升级客户端将继续使用云安全扫描，且使用传统扫描的所有客户端将继续使用传统扫描。

扫描方法对比

下表提供了这两种扫描方法之间的对比：

表 7-3. 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
可用性	可在该防毒墙网络版版本及所有早期防毒墙网络版版本中使用	在防毒墙网络版 10 及更高版本中均可用
扫描行为	传统扫描客户端在本地终端上执行扫描。	• 云安全扫描客户端在本地终端上执行扫描。 • 在扫描期间，如果客户端无法确定文件的风险，客户端会通过向云安全智能防护源发送扫描查询来验证风险。 • 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，所有组件在更新源上均可用	除病毒码和间谍软件主动监控特征码外，所有组件在更新源上均可用
典型更新源	防毒墙网络版服务器	防毒墙网络版服务器

更改扫描方法

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **扫描设置** > **扫描方法**。
4. 选择**传统扫描**或**云安全扫描**。

5. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

从云安全扫描切换到传统扫描

将客户端切换到传统扫描时，请考虑以下因素：

1. 要切换的客户端数量

   一次切换较少数量的客户端可以高效使用防毒墙网络版服务器和云安全智能防护服务器资源。在客户端更改其扫描方法的同时，这些服务器可以执行其他关键任务。

2. 时间选择

   切换回传统扫描时，客户端很可能会从防毒墙网络版服务器下载病毒码和间谍软件主动监控特征码的完全版。这些特征码文件仅由传统扫描客户端使用。

   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。另请考虑在没有客户端预设为从服务器更新时进行切换。此外，在客户端上暂时禁用“立即更新”，并在客户端切换到云安全扫描后重新启用。

3. 客户端树设置

   扫描方法是可在根级、域级或单个客户端级上设置的粒度设置。切换到传统扫描时，可以：

   - 创建新的客户端树域，并分配传统扫描作为其扫描方法。移动到此域的任何客户端都将使用传统扫描。移动客户端时，启用**将新域的设置应用到选定的客户端**设置。
   - 选择一个域并将它配置为使用传统扫描。属于该域的云安全客户端将切换到传统扫描。

- 从域中选择一个或多个云安全客户端，然后将它们切换到传统扫描。

注意

对域扫描方法进行的任何更改都将覆盖为单个客户端配置的扫描方法。

从传统扫描切换到云安全扫描

如果将客户端从传统扫描切换到云安全扫描，请确保已设置云安全智能防护服务。有关详细信息，请参阅设置云安全智能防护服务 第 4-11 页。

下表提供了切换到云安全扫描时的其他注意事项：

表 7-4. 切换到云安全扫描时的注意事项

注意事项	详细信息
产品使用授权	要使用云安全扫描，请确保已激活以下服务的使用授权，并确保这些使用授权没有过期： • 防病毒 • Web 信誉和防间谍软件
防毒墙网络版服务器	确保客户端可以连接到防毒墙网络版服务器。仅通知联机客户端切换到云安全扫描。脱机客户端变为联机状态时会收到通知。当漫游客户端变为联机状态时，或者运行预设更新（如果客户端具有预设更新权限）时，会收到通知。 此外，验证防毒墙网络版服务器是否具有最新的组件，因为云安全客户端需要从服务器下载云安全客户端病毒码。要更新组件，请参阅防毒墙网络版服务器更新 第 6-15 页。
要切换的客户端数量	一次切换较少数量的客户端可以高效使用防毒墙网络版服务器资源。在客户端更改其扫描方法的同时，防毒墙网络版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	首次切换到云安全扫描时，客户端需要从防毒墙网络版服务器下载云安全客户端病毒码的完全版。云安全云端病毒码仅由云安全客户端使用。 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。另请考虑在没有客户端预设为从服务器更新时进行切换。此外，在客户端上暂时禁用“立即更新”，并在客户端切换到云安全扫描后重新启用。
客户端树设置	扫描方法是可在根级、域级或单个客户端级上设置的粒度设置。切换到云安全扫描时，可以： • 创建新的客户端树域，并分配云安全扫描作为其扫描方法。移动到此域的任何客户端都将使用云安全扫描。移动客户端时，启用**将新域的设置应用到选定的客户端**设置。 • 选择一个域并将它配置为使用云安全扫描。属于该域的传统扫描客户端将切换到云安全扫描。 • 从域中选择一个或多个传统扫描客户端，然后将它们切换到云安全扫描。 **注意** 对域扫描方法进行的任何更改都将覆盖为单个客户端配置的扫描方法。
IPv6 支持	云安全客户端向云安全智能防护源发送扫描查询。 纯 IPv6 云安全客户端无法将查询直接发送到纯 IPv4 源，如： • 云安全智能防护服务器 2.0（集成型或独立型） **注意** 云安全智能防护服务器自版本 2.5 开始支持 IPv6。 • 趋势科技云安全智能防护网络 同样，纯 IPv4 云安全客户端无法向纯 IPv6 云安全智能防护服务器发送查询。 要使云安全客户端连接到源，需提供可以转换 IP 地址的双栈代理服务器（如 DeleGate）。

扫描类型

防毒墙网络版提供了以下扫描类型来保护防毒墙网络版客户端计算机免受安全风险的危害：

表 7-5. 扫描类型

扫描类型	描述
实时扫描	在接收、打开、下载、复制或修改终端上的文件时，会自动扫描该文件 请参阅实时扫描 第 7-12 页以了解详细信息。
手动扫描	用户启动的扫描，它会扫描用户请求的一个文件或一组文件 请参阅手动扫描 第 7-15 页以了解详细信息。
预设扫描	根据管理员或最终用户配置的时间表，自动扫描终端上的文件 请参阅预设扫描 第 7-17 页以了解详细信息。
立即扫描	管理员启动的扫描，扫描一个或多个目标计算机上的文件 请参阅立即扫描 第 7-19 页以了解详细信息。

实时扫描

实时扫描是持续进行的扫描。每次接收、打开、下载、复制或修改文件时，实时扫描就会扫描文件以查找安全风险。如果防毒墙网络版未检测到安全风险，则文件会留在其原位置，用户可以继续访问该文件。如果防毒墙网络版检测到安全风险或可能的病毒/恶意软件，会显示一条通知消息，显示受感染文件的名称和特定的安全风险。

实时扫描会对防毒墙网络版客户端每次启动时都会重新加载的持续性扫描缓存进行维护。防毒墙网络版客户端会跟踪由于退出防毒墙网络版客户端导致的文件或文件夹的任何更改，并从缓存中删除这些文件。



注意

要修改该通知消息，请打开 Web 控制台，并转至**管理** > **通知** > **客户端**。

配置实时扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置实时扫描设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **扫描设置** > **实时扫描设置**。
4. 选择下列选项：
   - **启用病毒/恶意软件扫描**
   - **启用间谍软件/灰色软件扫描**

   注意

   如果禁用病毒/恶意软件扫描，则间谍软件/灰色软件扫描也会被禁用。在病毒爆发期间，不能禁用实时扫描（如果原来处于禁用状态，将自动启用），以防止病毒修改或删除客户端计算机上的文件和文件夹。
5. 在**目标**选项卡上，配置以下内容：
   - 用户对文件执行的活动 第 7-22 页
   - 要扫描的文件 第 7-23 页
   - 扫描设置 第 7-23 页
6. 单击**处理措施**选项卡，然后配置以下内容：

表 7-6. 扫描处理措施

处理措施	参考
病毒/恶意软件处理措施	主要处理措施（选择一个）： • 使用 ActiveAction 第 7-32 页 • 对所有病毒/恶意软件类型使用相同的处理措施 第 7-33 页 • 对每种病毒/恶意软件类型使用特定的处理措施 第 7-33 页 **注意** 有关不同处理措施的详细信息，请参阅病毒/恶意软件扫描处理措施 第 7-30 页。 其他病毒/恶意软件处理措施： • 隔离目录 第 7-34 页 • 清除前备份文件 第 7-35 页 • 损害清除服务 第 7-35 页 • 检测到病毒/恶意软件时显示通知消息 第 7-36 页 • 检测到可能的病毒/恶意软件时显示通知消息 第 7-37 页
间谍软件/灰色软件处理措施	主要处理措施： • 间谍软件/灰色软件扫描处理措施 第 7-41 页 其他间谍软件/灰色软件处理措施： • 检测到间谍软件/灰色软件时显示通知消息 第 7-42 页

7. 在**扫描例外**选项卡上，配置要排除扫描的目录、文件和扩展名。

   有关详细信息，请参阅扫描例外 第 7-26 页。

8. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

- **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
- **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

手动扫描

手动扫描是按需扫描，用户在防毒墙网络版客户端控制台上运行该扫描后会立即启动。完成扫描所需时间取决于要扫描的文件的数量及防毒墙网络版客户端终端的硬件资源。

配置手动扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置手动扫描设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **扫描设置** > **手动扫描设置**。
4. 在**目标**选项卡上，配置以下内容：
   - 要扫描的文件 第 7-23 页
   - 扫描设置 第 7-23 页
   - CPU 使用率 第 7-25 页
5. 单击**处理措施**选项卡，然后配置以下内容：

表 7-7. 扫描处理措施

处理措施	参考
病毒/恶意软件处理措施	主要处理措施（选择一个）： • 使用 ActiveAction 第 7-32 页 • 对所有病毒/恶意软件类型使用相同的处理措施 第 7-33 页 • 对每种病毒/恶意软件类型使用特定的处理措施 第 7-33 页 **注意** 有关不同处理措施的详细信息，请参阅病毒/恶意软件扫描处理措施 第 7-30 页。 其他病毒/恶意软件处理措施： • 隔离目录 第 7-34 页 • 清除前备份文件 第 7-35 页 • 损害清除服务 第 7-35 页
间谍软件/灰色软件处理措施	主要处理措施： • 间谍软件/灰色软件扫描处理措施 第 7-41 页

6. 在**扫描例外**选项卡上，配置要排除扫描的目录、文件和扩展名。

   有关详细信息，请参阅扫描例外 第 7-26 页。

7. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

预设扫描

预设扫描按指定的日期和时间自动运行。使用预设扫描在客户端上使例行任务扫描自动化并提高扫描管理效率。

配置预设扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置预设扫描设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **扫描设置** > **预设扫描设置**。
4. 选择下列选项：
   - **启用病毒/恶意软件扫描**
   - **启用间谍软件/灰色软件扫描**

   注意

   如果禁用病毒/恶意软件扫描，则间谍软件/灰色软件扫描也会被禁用。
5. 在**目标**选项卡上，配置以下内容：
   - 时间表 第 7-25 页
   - 用户对文件执行的活动 第 7-22 页
   - 要扫描的文件 第 7-23 页
   - 扫描设置 第 7-23 页

6. 单击**处理措施**选项卡，然后配置以下内容：

表 7-8. 扫描处理措施

处理措施	参考
病毒/恶意软件处理措施	主要处理措施（选择一个）： • 使用 ActiveAction 第 7-32 页 • 对所有病毒/恶意软件类型使用相同的处理措施 第 7-33 页 • 对每种病毒/恶意软件类型使用特定的处理措施 第 7-33 页 **注意** 有关不同处理措施的详细信息，请参阅病毒/恶意软件扫描处理措施 第 7-30 页。 其他病毒/恶意软件处理措施： • 隔离目录 第 7-34 页 • 清除前备份文件 第 7-35 页 • 损害清除服务 第 7-35 页 • 检测到病毒/恶意软件时显示通知消息 第 7-36 页 • 检测到可能的病毒/恶意软件时显示通知消息 第 7-37 页
间谍软件/灰色软件处理措施	主要处理措施： • 间谍软件/灰色软件扫描处理措施 第 7-41 页 其他间谍软件/灰色软件处理措施： • 检测到间谍软件/灰色软件时显示通知消息 第 7-42 页

7. 在**扫描例外**选项卡上，配置要排除扫描的目录、文件和扩展名。

有关详细信息，请参阅扫描例外 第 7-26 页。

8. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

立即扫描

立即扫描由防毒墙网络版管理员通过 Web 控制台远程启动，并且可以将一台或多台客户端计算机作为目标。

配置立即扫描设置并将其应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。

配置立即扫描设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **扫描设置** > **立即扫描设置**。
4. 选择下列选项：

   - **启用病毒/恶意软件扫描**
   - **启用间谍软件/灰色软件扫描**

   注意

   如果禁用病毒/恶意软件扫描，则间谍软件/灰色软件扫描也会被禁用。

5. 在**目标**选项卡上，配置以下内容：
   - 要扫描的文件 第 7-23 页
   - 扫描设置 第 7-23 页
   - CPU 使用率 第 7-25 页
6. 单击**处理措施**选项卡，然后配置以下内容：

表 7-9. 扫描处理措施

处理措施	参考
病毒/恶意软件处理措施	主要处理措施（选择一个）： • 使用 ActiveAction 第 7-32 页 • 对所有病毒/恶意软件类型使用相同的处理措施 第 7-33 页 • 对每种病毒/恶意软件类型使用特定的处理措施 第 7-33 页 **注意** 有关不同处理措施的详细信息，请参阅病毒/恶意软件扫描处理措施 第 7-30 页。 其他病毒/恶意软件处理措施： • 隔离目录 第 7-34 页 • 清除前备份文件 第 7-35 页 • 损害清除服务 第 7-35 页
间谍软件/灰色软件处理措施	主要处理措施： • 间谍软件/灰色软件扫描处理措施 第 7-41 页

7. 在**扫描例外**选项卡上，配置要排除扫描的目录、文件和扩展名。

   有关详细信息，请参阅扫描例外 第 7-26 页。
8. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

- **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
- **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

启动立即扫描

在怀疑受感染的计算机上启动立即扫描。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**任务** > **立即扫描**。
4. 要在启动扫描前更改预先配置的**立即扫描**设置，请单击**设置**。

   将打开**立即扫描设置**窗口。请参阅立即扫描 第 7-19 页以了解详细信息。
5. 在客户端树中选择将执行扫描的客户端，然后单击**启动立即扫描**。

   服务器将发送通知给该客户端。
6. 检查通知状态并查看是否有未收到通知的客户端。
7. 单击**选择未通知的终端**，然后单击**启动立即扫描**，立即向未通知的客户端重新发送通知。

   示例：客户端总数：50

表 7-10. 未通知的客户端场景

客户端树选择	已通知的客户端（单击“启动立即扫描”后）	未通知的客户端
无（自动选择所有 50 个客户端）	50 个客户端中的 35 个	15 客户端
手动选择（选择了 50 个客户端中的 45 个）	45 个客户端中的 40 个	5 个客户端与其他 5 个客户端未包括在手动选择中

8. 单击**停止通知**可提示防毒墙网络版停止通知当前正通知的客户端。已收到通知并处于扫描进程中的客户端暂不处理此命令。

9. 对于已处于扫描进程的客户端，请单击**停止立即扫描**以通知其停止扫描。

所有扫描类型的通用设置

对于每种扫描类型，配置以下三组设置：扫描条件、扫描例外和扫描处理措施。将这些设置部署到一个或多个客户端和域，或服务器管理的所有客户端。

扫描条件

使用文件属性（如文件类型和扩展名），指定特定扫描类型应该扫描的文件。此外，指定将触发扫描的条件。例如，配置实时扫描，使其在每个文件下载到终端后对文件进行扫描。

用户对文件执行的活动

选择对文件执行哪些活动将触发实时扫描。从以下选项中选择：

- **扫描正在创建/修改的文件**：扫描引入终端的新文件（例如，下载文件后）或正在修改的文件
- **扫描正在检索的文件**：在打开文件时对文件进行扫描

- **扫描正在创建/修改和检索的文件**

例如，如果选择第三个选项，则将扫描下载到终端的新文件，如果未检测到安全风险，则该文件将留在其当前位置中。当用户打开同一文件时（如果用户修改了文件，则在保存修改之前），将会扫描该文件。

要扫描的文件

从以下选项中选择：

- **所有可扫描文件**：扫描所有文件
- **已由 IntelliScan 扫描的文件类型**：只扫描已知可能包含恶意代码的文件，包括用无害扩展名伪装的文件。

  请参阅 IntelliScan 第 E-6 页以了解详细信息。
- **带有以下扩展名的文件**：仅扫描其扩展名包括在文件扩展名列表中的文件。添加新扩展名或删除任何现有的扩展名。

扫描设置

选择以下一个或多个选项：

- **在系统关闭期间扫描软盘**：在关闭终端之前实时扫描会扫描所有软盘以查找引导区病毒。这可防止任何病毒/恶意软件在用户从磁盘重新启动终端时执行。
- **扫描隐藏文件夹**：在手动扫描期间，允许防毒墙网络版在终端检测隐藏文件夹然后扫描它们
- **扫描网络驱动器**：在手动扫描或实时扫描期间扫描映射到防毒墙网络版客户端终端的网络驱动器或文件夹。
- **插入 USB 存储设备后扫描其引导区**：在每次用户插入 USB 存储设备时仅自动扫描其引导区（实时扫描）。
- **插入可移动存储设备后扫描其中的所有文件**：在每次用户插入 USB 存储设备时自动扫描该存储设备上的所有文件（实时扫描）。

- **隔离内存中检测到的恶意软件变种**：行为监控可以扫描系统内存中的可疑进程，实时扫描可以映射进程并扫描其中的恶意软件威胁。如果存在恶意软件威胁，实时扫描会隔离进程和/或文件。

  注意

  此功能要求管理员启用未授权更改阻止服务和高级保护服务。

- **扫描压缩文件**：允许防毒墙网络版最多扫描指定的压缩层数并跳过对任何超出层的扫描。防毒墙网络版还可清理或删除压缩文件中的受感染文件。例如，如果最大值为两层，而要扫描的压缩文件有六层，防毒墙网络版将扫描两层并跳过剩余四层。如果压缩文件包含安全威胁，防毒墙网络版将清除或删除该文件。

  注意

  防毒墙网络版将 Office Open XML 格式的 Microsoft Office 2007 文件视为压缩文件。Office Open XML（Office 2007 应用程序的文件格式）使用 ZIP 压缩技术。如果想要对使用这些应用程序创建的文件进行病毒/恶意软件扫描，需要启用压缩文件扫描功能。

- **扫描 OLE 对象**：当文件包含多个对象链接与嵌入 (OLE) 层时，防毒墙网络版扫描指定的层数，而忽略其余层。

  在手动扫描、实时扫描、预设扫描和立即扫描期间，服务器管理的所有防毒墙网络版客户端会检查此设置。扫描每个层中是否有病毒/恶意软件和间谍软件/灰色软件。

  例如：

  指定的层数是 2。文件中嵌入一个 Microsoft Word 文档（第一层），Word 文档中有一个 Microsoft Excel 电子表格（第二层），电子表格中有一个.exe 文件（第三层）。防毒墙网络版将扫描 Word 文档和 Excel 电子表格，而跳过 .exe 文件。

  - **检测 OLE 文件中的利用代码**：OLE 弱点攻击检测通过检查 Microsoft Office 文件中的利用代码来启发式地识别恶意软件。

    注意

    指定的层数适用于**扫描 OLE 对象**和**检测利用代码**选项。

- **启用 IntelliTrap**：检测并移除压缩可执行文件中的病毒/恶意软件。此选项仅适用于实时扫描。

  请参阅 IntelliTrap 第 E-6 页以了解详细信息。

- **扫描引导区**：在手动扫描、预设扫描和立即扫描期间，扫描客户端终端硬盘的引导区以查找病毒/恶意软件。

CPU 使用率

在扫描一个文件后和扫描下一个文件前，防毒墙网络版客户端可以暂停。此设置在手动扫描、预设扫描和立即扫描期间使用。

从以下选项中选择：

- **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

如果选择“中”或“低”，则启动扫描并且 CPU 使用率在阈值（50% 或 20%）范围内时，防毒墙网络版在扫描之间将不暂停，从而缩短了扫描时间。防毒墙网络版在处理中会使用更多的 CPU 资源，但是由于 CPU 占用率是最佳的，因此终端性能不会受到严重影响。当 CPU 使用率开始超过阈值时，防毒墙网络版将暂停以降低 CPU 使用率，当使用率再次处于阈值范围内时会停止暂停。

如果选择“高”，则防毒墙网络版不检查实际的 CPU 占用率，会一直扫描文件而不暂停。

时间表

配置预设扫描运行的频率（每天、每周或每月）及时间。

对于每月预设扫描，您可以选择某个月中的特定某天，或某周中的某一天以及这一天出现的次序。

- **某个月中的特定某天**：选择介于 1 日和 31 日之间的任何一天。如果您选择的是 29 日、30 日或 31 日，但当月不包含该日期，则防毒墙网络版将在当月的最后一天运行预设扫描。因此：
  - 如果您选择的是 29 日，预设扫描将在 2 月 28 日（闰年除外）运行，其他月份则为 29 日。
  - 如果您选择的是 30 日，预设扫描将在 2 月 28 日或 29 日运行，其他月份则为 30 日。
  - 如果您选择的是 31 日，预设扫描将在 2 月 28 日或 29 日、4 月 30 日、6 月 30 日、9 月 30 日和 11 月 30 日运行，其他月份则为 31 日。
- **某周中的某一天以及这一天出现的次序**：一周中的某一天会在一个月中出现四次或五次。例如，每个月通常包括四个星期一。指定某周中的某一天以及这一天在当月出现的次序。例如，选择在每个月的第二个星期一运行预设扫描。如果您选择在第五次出现这一天时运行，但这一天在某个月中不会出现第五次，则扫描将在第四次出现这一天时运行。

扫描例外

配置扫描例外可提高扫描性能并跳过对导致假警报的文件的扫描。运行特定扫描类型时，防毒墙网络版检查扫描例外列表，以确定终端上的哪些文件将从病毒/恶意软件和间谍软件/灰色软件扫描中排除。

启用扫描例外时，防毒墙网络版在以下情况下将不扫描文件：

- 文件位于特定目录（或其任意子目录）下。
- 文件名与例外列表中的任何名称匹配。
- 文件扩展名与例外列表中的任何扩展名匹配。



提示

如需趋势科技建议从实时扫描中排除的产品列表，请转至：

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

通配符例外

文件和目录的扫描例外列表支持使用通配符。使用 "?" 字符替换一个字符，使用 "*" 替换多个字符。

请慎用通配符。使用错误的字符可能会排除不正确的文件或目录。例如，将 C:* 添加到扫描例外列表（文件）将排除整个 C:\ 驱动器。

表 7-11. 使用通配符的扫描例外

值	已排除	未排除
`c:\director*\fil\*.txt`	c:\directory\fil\doc.txt c:\directories\fil\files\document.txt	c:\directory\file\ c:\directories\files\ c:\directory\file\doc.txt c:\directories\files\document.txt
`c:\director?\file\*.txt`	c:\directory\file\doc.txt	c:\directories\file\document.txt
`c:\director?\file\?.txt`	c:\directory\file\1.txt	c:\directory\file\doc.txt c:\directories\file\document.txt
`c:\*.txt`	C:\ 目录中的所有 .txt 文件	C:\ 目录中的所有其他文件类型
`[]`	不支持	不支持
`*.*`	不支持	不支持

扫描例外列表（目录）

防毒墙网络版不扫描在计算机特定目录下找到的所有文件。最多可以指定 256 个目录。

注意

从扫描中排除某个目录时，防毒墙网络版将自动从扫描中排除该目录的所有子目录。

您也可以选择**排除趋势科技产品的安装目录**。如果选择此选项，防毒墙网络版会自动从扫描中排除以下趋势科技产品的目录：

- <服务器安装文件夹>
- IM 安全
- InterScan eManager 3.5x
- InterScan Web 安全套件 (IWSS)
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11、5.1、5.11 和 5.12
- 防毒墙群件版 for Lotus Notes™ eManager NT
- 防毒墙群件版™ for Microsoft Exchange

如果您有未包括在列表中的趋势科技产品，请将该产品的目录添加到扫描例外列表中。

此外，转至**客户端 > 全局客户端设置**的**扫描设置**部分，将防毒墙网络版配置为排除 Microsoft Exchange 2000/2003 目录。如果使用 Microsoft Exchange 2007 或更高版本，则需将该目录手动添加到扫描例外列表。有关扫描例外的详细信息，请参考以下站点：

http://technet.microsoft.com/en-us/library/bb332342.aspx

配置文件列表时，请从下列选项进行选择：

- **保留当前列表**（缺省选项）：防毒墙网络版提供此选项是为了防止意外覆盖客户端的例外列表。要保存并部署对例外列表进行的更改，请选择其他任何选项。

- **覆盖**：此选项将移除客户端上的整个例外列表，并将其替换为当前列表。单击**应用到全部客户端**后，防毒墙网络版会显示确认警告消息。
- **将路径添加到**：此选项会将当前列表中的项添加到客户端的现有例外列表。如果某个项已存在于客户端的例外列表中，客户端将忽略该项。
- **从以下位置移除路径**：如果从客户端的现有例外列表中找到当前列表中的项，此选项会移除这些项。

扫描例外列表 (文件)

如果一个文件的文件名与此例外列表中包括的任何名称匹配，则防毒墙网络版将不扫描该文件。如果要排除在终端上特定位置找到的文件，请包括文件路径，如 C:\Temp\sample.jpg。

最多可以指定 256 个文件。

配置文件列表时，请从下列选项进行选择：

- **保留当前列表**（缺省选项）：防毒墙网络版提供此选项是为了防止意外覆盖客户端的例外列表。要保存并部署对例外列表进行的更改，请选择其他任何选项。
- **覆盖**：此选项将移除客户端上的整个例外列表，并将其替换为当前列表。单击**应用到全部客户端**后，防毒墙网络版会显示确认警告消息。
- **将路径添加到**：此选项会将当前列表中的项添加到客户端的现有例外列表。如果某个项已存在于客户端的例外列表中，客户端将忽略该项。
- **从以下位置移除路径**：如果从客户端的现有例外列表中找到当前列表中的项，此选项会移除这些项。

扫描例外列表 (文件扩展名)

如果一个文件的文件扩展名与此例外列表中包括的任何扩展名匹配，则防毒墙网络版将不扫描该文件。最多可以指定 256 个文件扩展名。在扩展名之前不需要添加英文句点 (.)。

对于实时扫描，在指定扩展名时，可使用星号 (*) 作为通配符。例如，如果不希望扫描扩展名以 D 开头（例如，DOC、DOT 或 DAT）的所有文件，请键入 D*。

对于手动扫描、预设扫描和立即扫描，可使用问号 (?) 或星号 (*) 作为通配符。

将扫描例外设置应用至所有扫描类型

防毒墙网络版允许您为特定扫描类型配置扫描例外设置，然后将相同设置应用至所有其他扫描类型。例如：

1 月 1 日，防毒墙网络版管理员 Chris 发现客户端计算机上有大量的 JPG 文件，并了解到这些文件不会造成任何安全威胁。Chris 在手动扫描的例外文件列表中添加了 JPG，然后将此设置应用至所有扫描类型。实时扫描、立即扫描和预设扫描现在已设置为跳过对 .jpg 文件的扫描。

一星期后，Chris 从实时扫描的例外列表中移除了 JPG，但是没有将扫描例外设置应用至所有扫描类型。现在将扫描 JPG 文件，但只在实时扫描期间才会扫描。

扫描处理措施

指定特定扫描类型检测到安全风险时防毒墙网络版执行的处理措施。防毒墙网络版对病毒/恶意软件和间谍软件/灰色软件采用两组不同的扫描处理措施。

病毒/恶意软件扫描处理措施

防毒墙网络版执行的扫描处理措施取决于病毒/恶意软件类型，以及检测出病毒/恶意软件的扫描类型。例如，如果在手动扫描（扫描类型）过程中，防毒墙网络版检测到特洛伊木马程序（病毒/恶意软件类型），它将清除（处理措施）受感染文件。

有关不同的病毒/恶意软件类型的信息，请参阅病毒和恶意软件 第 7-2 页。

以下是防毒墙网络版可以对病毒/恶意软件执行的处理措施。

表 7-12. 病毒/恶意软件扫描处理措施

处理措施	描述
删除	防毒墙网络版会删除受感染文件。
隔离	防毒墙网络版更名，然后将受感染的文件移动到客户端终端上 <客户端安装文件夹>\Suspect 中的临时隔离目录。 接下来，防毒墙网络版客户端将隔离文件发送到指定的隔离目录。 请参阅隔离目录 第 7-34 页以了解详细信息。 缺省隔离目录位于防毒墙网络版服务器上的 <服务器安装文件夹>\PCCSRV\Virus 中。防毒墙网络版会对发送至该目录的隔离文件进行加密。 如果需要恢复任何隔离文件，请使用集中隔离恢复。 有关详细信息，请参阅恢复隔离文件 第 7-37 页。
清除	防毒墙网络版会先清除受感染文件，然后才允许对文件进行完全访问。 如果文件无法清除，防毒墙网络版会执行第二项处理措施，它可以是以下处理措施之一：隔离、删除、更名和不予处理。 要配置第二处理措施，请转至**客户端** > **客户端管理**。单击**设置** > **扫描设置** > **{扫描类型}** > **处理措施**选项卡。 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。
更名	防毒墙网络版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	只有当防毒墙网络版在手动扫描、预设扫描和立即扫描期间检测到任何类型的时，才能使用该扫描处理措施。防毒墙网络版不能在实时扫描期间使用该扫描处理措施，因为如果在检测到打开或执行受感染文件的尝试时不执行处理措施，会执行病毒/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	该扫描处理措施只能在实时扫描期间执行。如果防毒墙网络版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。

使用 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。防毒墙网络版使用 ActiveAction 计算这些问题。

ActiveAction 是针对病毒/恶意软件的一组预配置的扫描处理措施。如果您不熟悉扫描处理措施，或者不确定哪种扫描处理措施适合特定类型的病毒/恶意软件，趋势科技建议使用 ActiveAction。

使用 ActiveAction 会提供以下好处：

- ActiveAction 使用趋势科技建议的扫描处理措施。您不必在配置扫描处理措施上花费时间。
- 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。



注意

ActiveAction 不可用于间谍软件/灰色软件扫描。

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

表 7-13. 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/立即扫描	
	第一处理措施	第二项处理措施	第一处理措施	第二项处理措施
恶作剧程序	隔离	无	隔离	无
特洛伊木马程序	隔离	无	隔离	无
病毒	清除	隔离	清除	隔离
测试病毒	拒绝访问	无	不予处理	无
加壳软件	隔离	无	隔离	无
其他	清除	隔离	清除	隔离

病毒/恶意软件类型	实时扫描		手动扫描/预设扫描/立即扫描	
	第一处理措施	第二项处理措施	第一处理措施	第二项处理措施
可能的病毒/恶意软件	拒绝访问或用户配置的处理措施	无	不予处理或用户配置的处理措施	无

对于可能的病毒/恶意软件，实时扫描期间的缺省处理措施是“拒绝访问”，而手动扫描、预设扫描和立即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“隔离”、“删除”或“更名”。

对所有病毒/恶意软件类型使用相同的处理措施

如果希望对除可能的病毒/恶意软件之外的所有类型的病毒/恶意软件执行相同的处理措施，请选择此选项。如果选择“清除”作为第一项处理措施，请选择在清除不成功时防毒墙网络版执行的第二项处理措施。如果第一项处理措施不是“清除”，则第二项处理措施不可配置。

如果选择“清除”作为第一项处理措施，则防毒墙网络版在检测到可能的病毒/恶意软件时会执行第二项处理措施。

对每种病毒/恶意软件类型使用特定的处理措施

手动选择每种病毒/恶意软件类型的扫描处理措施。

对于可能的病毒/恶意软件以外的所有病毒/恶意软件类型，所有扫描处理措施均可用。如果选择“清除”作为第一项处理措施，请选择在清除不成功时防毒墙网络版执行的第二项处理措施。如果第一项处理措施不是“清除”，则第二项处理措施不可配置。

对于可能的病毒/恶意软件，“清除”以外的所有扫描处理措施均可用。

隔离目录

如果受感染文件的处理措施是“隔离”，则防毒墙网络版客户端将加密该文件，并将其移动到临时隔离文件夹（位于 <客户端安装文件夹>\SUSPECT 中），然后将该文件发送到指定的隔离目录。

注意

如果将来需要访问加密的隔离文件，则可以恢复它们。

有关详细信息，请参阅恢复加密的文件 第 7-38 页。

接受位于防毒墙网络版服务器计算机上的缺省隔离目录。此目录采用 URL 格式，并且包含服务器的主机名或 IP 地址。

- 如果服务器同时管理 IPv4 和 IPv6 客户端，则使用主机名，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，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，只有纯 IPv6 和双栈客户端可以将隔离文件发送到该服务器。

也可以通过键入 URL、UNC 路径或绝对文件路径格式的位置来指定备用隔离目录。客户端应该可以连接到此备用目录。例如，如果备用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、通过其主机名识别目录并在键入目录时使用 UNC 路径。

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 7-14. 隔离目录

隔离目录	可接受的格式	示例	注意
防毒墙网络版服务器计算机上的目录	URL	http:// <osceserver>	这是缺省目录。 配置此目录的设置，如隔离文件夹的大小。 有关详细信息，请参阅隔离管理器 第 13-54 页。
	UNC 路径	\\<osceserver>\ ofcscan\Virus	
另一台防毒墙网络版服务器计算机上的目录（如果网络上具有其他防毒墙网络版服务器）	URL	http:// <osceserver2>	确保客户端可以连接到此目录。如果指定了不正确的目录，则防毒墙网络版客户端会将隔离文件保留在 SUSPECT 文件夹中，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	\\<osceserver2>\ ofcscan\Virus	
网络上的其他终端	UNC 路径	\\<computer_ name> \temp	
该防毒墙网络版客户端上的其他目录	绝对路径	C:\temp	

清除前备份文件

如果防毒墙网络版设置为清除受感染文件，则它可以首先备份该文件。备份文件后，如果将来需要该文件，就可以恢复它。防毒墙网络版加密备份文件以防止文件被打开，然后将文件存储在 <客户端安装文件夹>\Backup 文件夹中。

要恢复加密的备份文件，请参阅恢复加密的文件 第 7-38 页。

损害清除服务

损害清除服务可清除计算机中基于文件的病毒和网络病毒以及病毒和蠕虫残留（特洛伊木马、注册表项和含病毒的文件）。

客户端会在病毒/恶意软件扫描之前或之后触发损害清除服务，具体取决于扫描类型。

- 当手动扫描、预设扫描或立即扫描运行时，防毒墙网络版客户端会首先触发损害清除服务，然后继续执行病毒/恶意软件扫描。在病毒/恶意软件扫描期间，如果需要进行清除，客户端可能会再次触发损害清除服务。
- 在实时扫描期间，如果需要进行清除，防毒墙网络版客户端会首先执行病毒/恶意软件扫描，然后触发损害清除服务。

可以选择损害清除服务运行的清除类型：

- **标准清除**：防毒墙网络版客户端在标准清除期间执行以下任意操作：
  - 检测和移除活动的特洛伊木马
  - 中断特洛伊木马创建的进程
  - 修复特洛伊木马修改的系统文件
  - 删除特洛伊木马留下的文件和应用程序
- **高级清除**：除了标准清除操作之外，防毒墙网络版客户端还通过流氓安全软件（也称为 FakeAV）和某些 rootkit 变种停止活动。防毒墙网络版客户端还可以使用高级清除规则来前瞻地检测并停止存在 FakeAV 和 rootkit 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。

损害清除服务不会对可能的病毒/恶意软件运行清除，除非选择**检测到可能的病毒/恶意软件时运行清除**选项。如果对可能的病毒/恶意软件的处理措施既不是**不予处理**也不是**拒绝访问**，则只能选择该选项。例如，如果防毒墙网络版客户端在实时扫描期间检测到可能的病毒/恶意软件，且处理措施为“隔离”，防毒墙网络版客户端会首先隔离受感染文件，然后根据需要运行清除。清除类型（标准或高级）取决于您的选择。

检测到病毒/恶意软件时显示通知消息

当防毒墙网络版在实时扫描和预设扫描期间检测到病毒/恶意软件时，它可以显示通知消息，以通知用户有关检测的信息。

要修改通知消息，请从**管理** > **通知** > **客户端**中的**类型**下拉菜单中选择**病毒/恶意软件**。

检测到可能的病毒/恶意软件时显示通知消息

当防毒墙网络版在实时扫描和预设扫描期间检测到可能的病毒/恶意软件时，它可以显示通知消息，以通知用户有关检测的信息。

要修改通知消息，请从**管理** > **通知** > **客户端**中的**类型**下拉菜单中选择**病毒/恶意软件**。

恢复隔离文件

如果您认为检测不准确，则可以恢复防毒墙网络版隔离的文件。集中隔离恢复功能允许您在隔离目录中搜索文件并执行 SHA1 验证检查，确保您要恢复的文件没有以任何方式进行修改。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，选择一个域或选择任何客户端。
3. 单击**任务** > **集中隔离恢复**。

   将显示**集中隔离恢复条件**窗口。
4. 请在**受感染的文件/对象**文本框中键入您要恢复的数据的名称。
5. 可根据需要指定时间段、安全威胁名称和数据的文件路径。
6. 单击**搜索**。

   将显示**集中隔离恢复**窗口，该窗口会显示搜索结果。
7. 选择**将已恢复的文件添加到域级例外列表**，可确保恢复文件的域中的所有防毒墙网络版客户端将文件添加到扫描例外列表中。

   这可以确保防毒墙网络版在未来扫描期间不会将文件检测为一种威胁。

8. 也可根据需要键入文件的 SHA1 值以进行验证。

9. 从列表中选择要恢复的文件，然后单击**恢复**。



提示

要查看恢复文件的各个防毒墙网络版客户端，请单击**终端**列的链接。

10. 在确认对话框中单击**关闭**。

要验证防毒墙网络版是否已成功恢复隔离文件，请参阅查看集中隔离恢复日志 第 7-88 页。

恢复加密的文件

为防止打开受感染文件，防毒墙网络版在以下实例中对文件进行加密：

- 隔离文件之前
- 在清除文件之前备份文件时

防毒墙网络版提供了一种工具，用于在需要从文件检索信息时解密和恢复该文件。防毒墙网络版可以解密和恢复以下文件：

表 7-15. 防毒墙网络版可以解密和恢复的文件

文件	描述
客户端终端上的隔离文件	这些文件可在 <客户端安装文件夹>\SUSPECT\Backup 文件夹中找到，7 天后会被自动清除。这些文件还会上传到防毒墙网络版服务器上的指定隔离目录。
指定隔离目录中的隔离文件	缺省情况下，此目录位于防毒墙网络版服务器计算机上。 有关详细信息，请参阅隔离目录 第 7-34 页。

文件	描述
备份的加密文件	这些文件是防毒墙网络版能够清除的受感染文件的备份。这些文件可在 <客户端安装文件夹>\Backup 文件夹中找到。要恢复这些文件，用户需要将它们移动到 <客户端安装文件夹>\SUSPECT\Backup 文件夹。 仅当在转至**客户端** > **客户端管理**，单击**设置** > **扫描设置** > **{扫描类型}** > **处理措施**选项卡并选择**清除前备份文件**时，防毒墙网络版才在清除前备份和加密文件。

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计算机。在恢复文件之前，隔离受感染的终端，并将此终端上的重要文件移动到备份位置。

解密和恢复文件

过程

- 如果文件在防毒墙网络版客户端终端上：
  a. 打开命令提示符并转至 <客户端安装文件夹>。
  b. 双击文件或在命令提示符处键入以下内容来运行 VSEncode.exe：

     ```
     VSEncode.exe /u
     ```

     此参数将打开一个窗口，其中包含在 <客户端安装文件夹>\SUSPECT\Backup 下找到的文件的列表。
  c. 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。
  d. 在打开的窗口中，指定将文件恢复到的文件夹。
  e. 单击**确定**。文件将恢复到指定的文件夹。

注意

在恢复文件后，防毒墙网络版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。请参阅扫描例外 第 7-26 页以了解详细信息。

f. 恢复完文件后，单击**关闭**。

- 如果文件在防毒墙网络版服务器或定制隔离目录中：

a. 如果文件在防毒墙网络版服务器计算机中，请打开命令提示符并转至 <服务器安装文件夹>\PCCSRV\Admin\Utility\VSEncrypt。

如果文件在定制隔离目录中，请导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility 并将 VSEncrypt 文件夹复制到定制隔离目录所在的终端。

b. 创建一个文本文件，然后键入想要加密或解密文件的完整路径。

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*.*。

防毒墙网络版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。

c. 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。

d. 打开命令提示符并转至 VSEncrypt 文件夹所在的目录。

e. 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（例如 C:\ForEncryption.ini）。

f. 使用其他参数发出各种命令。

表 7-16. 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终端。在防毒墙网络版客户端终端上，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
/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。加密或解密文件时，防毒墙网络版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。

间谍软件/灰色软件扫描处理措施

防毒墙网络版执行的扫描处理措施取决于检测出间谍软件/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，如果防毒墙网络版在手动扫描（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。

有关不同的间谍软件/灰色软件类型的信息，请参阅间谍软件和灰色软件 第 7-4 页。

注意

间谍软件/灰色软件扫描处理措施仅可通过 Web 控制台配置。防毒墙网络版客户端控制台没有提供对这些设置的访问权限。

下表列出了防毒墙网络版可以对间谍软件/灰色软件执行的处理措施：

表 7-17. 间谍软件/灰色软件扫描处理措施

处理措施	描述
清除	防毒墙网络版终止进程或删除注册表、文件、Cookie 和快捷方式。 清除间谍软件/灰色软件后，防毒墙网络版客户端会备份间谍软件/灰色软件数据，如果您认为访问某间谍软件/灰色软件是安全的，则可以将其恢复。 请参阅恢复间谍软件/灰色软件 第 7-45 页以了解详细信息。
不予处理	防毒墙网络版不会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/灰色软件检测的情况。此处理措施只能在手动扫描、预设扫描和立即扫描期间执行。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，防毒墙网络版将不会执行任何处理措施。 请参阅间谍软件/灰色软件允许列表 第 7-43 页以了解详细信息。
拒绝访问	防毒墙网络版拒绝访问（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、预设扫描和立即扫描期间，处理措施是“不予处理”。

检测到间谍软件/灰色软件时显示通知消息

当防毒墙网络版在实时扫描和预设扫描期间检测到间谍软件/灰色软件时，它可以显示通知消息，以通知用户有关检测的信息。

要修改通知消息，请从**管理** > **通知** > **客户端**中的**类型**下拉菜单中选择**间谍软件/灰色软件**。

间谍软件/灰色软件允许列表

防毒墙网络版提供了间谍软件/灰色软件的“允许”列表，该列表包含不希望视为间谍软件或灰色软件的文件或应用程序。在扫描期间检测到特定间谍软件/灰色软件时，防毒墙网络版将检查允许列表，如果它在允许列表中找到匹配项，则不执行任何处理措施。

将允许列表应用于一个或多个客户端和域，或者应用于服务器管理的所有客户端。允许列表应用于所有，这意味着在手动扫描、实时扫描、预设扫描和立即扫描期间将使用相同的允许列表。

在允许列表中添加已检测到的间谍软件/灰色软件

过程

1. 转到以下项之一：
   - **客户端** > **客户端管理**
   - **日志** > **客户端** > **安全风险**
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **间谍软件/灰色软件日志**或**查看日志** > **间谍软件/灰色软件日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 选择日志，然后单击**添加到允许列表**。
6. 仅将允许的间谍软件/灰色软件应用到选定的客户端计算机或特定域。
7. 单击**保存**。选定的客户端将应用该设置，防毒墙网络版服务器将间谍软件/灰色软件添加到在**客户端** > **客户端管理** > **设置** > **间谍软件/灰色软件允许列表**中找到的允许列表中。

注意

防毒墙网络版的允许列表中最多可容纳 1024 种间谍软件/灰色软件。

管理间谍软件/灰色软件允许列表

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **间谍软件/灰色软件允许列表**。
4. 在**间谍软件/灰色软件名称**表中，选择间谍软件/灰色软件名称。要选择多个名称，请在选择时按住 CTRL 键。
   - 还可以在**搜索**文本框中键入关键字，然后单击**搜索**。防毒墙网络版将刷新该表，显示与该关键字匹配的名称。
5. 单击**添加**。

   名称将移动到**允许列表**表中。
6. 要移除允许列表中的名称，请选择名称，然后单击**移除**。要选择多个名称，请在选择时按住 CTRL 键。
7. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

恢复间谍软件/灰色软件

清除间谍软件/灰色软件后，防毒墙网络版客户端备份间谍软件/灰色软件数据。如果您认为某数据无害，请通知联机客户端恢复该备份数据。根据备份时间选择要恢复的间谍软件/灰色软件数据。

注意

防毒墙网络版客户端用户无法启动间谍软件/灰色软件恢复，也不会得到客户端能够恢复哪些备份数据的通知。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，打开某个域，然后选择任意客户端。

   注意

   每次只有一个客户端可以执行间谍软件/灰色软件恢复。

3. 单击**任务** > **间谍软件/灰色软件恢复**。
4. 要查看各个数据段要恢复的项，请单击**查看**。

   将显示一个新窗口。单击**后退**返回到上一窗口。
5. 请选择要恢复的数据段。
6. 单击**恢复**。

   防毒墙网络版会通知您恢复的状态。检查间谍软件/灰色软件恢复日志来获取完整报告。请参阅查看间谍软件/灰色软件恢复日志 第 7-91 页以了解详细信息。

进程例外管理

可以将防毒墙网络版配置为在实时扫描和行为监控扫描期间跳过对可信进程的扫描。将程序添加到可信程序列表后，防毒墙网络版不会使程序或由该程序启

动的任何进程受实时扫描的限制。将可信程序添加到可信程序列表以提高在终端上执行扫描的性能。

注意

如果满足以下要求，可以将文件添加到可信程序列表中:

- 相应文件不在 Windows 系统目录中。
- 相应文件具有有效数字签名。

将程序添加到可信程序列表后，防毒墙网络版将自动从以下扫描中排除该程序：

- 实时扫描文件检查
- 行为监控
- 实时扫描进程扫描

配置可信程序列表

可信程序列表不包括由程序从实时扫描和行为监控扫描调用的程序和所有子进程。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **可信程序列表**。
4. 键入要从列表中排除的程序的完整程序路径。
5. 单击**添加到“可信程序列表”**。
6. 要从列表中移除程序，请单击**删除**图标。

7. 要导出可信程序列表，请单击**导出**，然后选择文件的位置。



注意

防毒墙网络版将列表保存为 CSV 格式。

8. 要导入可信程序列表，请单击**导入**，然后选择文件的位置。

   a. 单击**浏览...**，然后选择 CSV 文件的位置。

   b. 单击**导入**。

9. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

扫描权限和其他设置

具有扫描权限的用户可更好地控制在其计算机上扫描文件的方式。扫描权限允许用户或防毒墙网络版客户端执行以下任务：

- 用户可以配置手动扫描、预设扫描和实时扫描设置。有关详细信息，请参阅扫描类型权限 第 7-48 页。
- 用户可以推迟、停止或者跳过预设扫描。有关详细信息，请参阅预设扫描权限和其他设置 第 7-50 页。
- 用户允许对 POP3 电子邮件进行扫描以查找病毒/恶意软件。有关详细信息，请参阅邮件扫描权限和其他设置 第 7-56 页。
- 防毒墙网络版客户端可以使用缓存设置来提高其扫描性能。有关详细信息，请参阅扫描的缓存设置 第 7-58 页。

- 用户可以定制单个可信程序列表。有关详细信息，请参阅可信程序列表权限 第 7-61 页。

扫描类型权限

允许用户配置自己的手动扫描、实时扫描和预设扫描设置。

授予扫描类型权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转到**扫描**部分。
5. 选择允许用户配置的扫描类型。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

配置防毒墙网络版客户端的扫描设置

过程

1. 右键单击系统托盘中的防毒墙网络版客户端图标，然后选择**打开防毒墙网络版客户端控制台**。

2. 单击**设置** > **{扫描类型}**。



图 7-1. 防毒墙网络版客户端控制台上的扫描设置

3. 配置下列设置：

- 实时扫描设置：用户对文件执行的活动、要扫描的文件、扫描设置、扫描例外、扫描处理措施
- 手动扫描设置：预设、要扫描的文件、扫描设置、CPU 使用情况、扫描例外、扫描处理措施
- 预设扫描设置：预设、要扫描的文件、扫描设置、CPU 使用情况、扫描例外、扫描处理措施

4. 单击**确定**。

预设扫描权限和其他设置

如果设置为在客户端上运行预设扫描，用户可以推迟和跳过/停止预设扫描。

推迟预设扫描

具有“推迟预设扫描”权限的用户可以执行下列操作：

- 在预设扫描运行前推迟预设扫描，然后指定推迟的时间长度。预设扫描只能推迟一次。
- 如果预设扫描正在进行中，则用户可以停止扫描并在以后重新启动它。然后，用户指定扫描重新开始前应经过的时间长度。当扫描重新开始时，所有以前扫描过的文件都会再扫描一遍。预设扫描在停止后只能重新启动一次。

注意

用户可以指定的最小推迟时间长度/所用时间为 15 分钟。最大时间为 12 小时 45 分钟。

转至**客户端** > **全局客户端设置**可修改推迟时间。在**预设扫描设置**部分，修改**最多推迟预设扫描 __ 小时和 __ 分钟**设置。

跳过并停止预设扫描

此权限允许用户执行以下操作：

- 在预设扫描运行前跳过预设扫描
- 在预设扫描正在进行时停止预设扫描

注意

用户最多只能跳过或停止预设扫描一次。即使重新启动系统，预设扫描也将在下一预定时间恢复扫描。

预设扫描权限通知

要允许用户利用预设扫描权限，请将防毒墙网络版配置为在预设扫描运行前显示通知消息，以提醒用户已授予他们的权限。

授予预设扫描权限和显示权限通知

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转到**预设扫描**部分。
5. 选择下列选项：
   - **推迟预设扫描**
   - **跳过并停止预设扫描**
6. 单击**其他设置**选项卡，然后转至**预设扫描设置**部分。

7. 选择**在进行预设扫描之前显示通知**。

   启用此选项时，通知消息将在预设扫描运行前几分钟在客户端终端上显示。系统会向用户通知扫描时间表（日期和时间）及其预设扫描权限，如推迟、跳过或停止预设扫描。

   注意

   分钟数是可配置的。要配置分钟数，请转至**客户端** > **全局客户端设置**。在**预设扫描设置**部分，修改**在预设扫描运行前 __ 分钟提醒用户**设置。

8. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

推迟/跳过和停止客户端上的预设扫描

过程

- 如果预设扫描尚未启动：

  a. 右键单击系统托盘上的防毒墙网络版客户端图标，然后选择**高级预设扫描设置**。

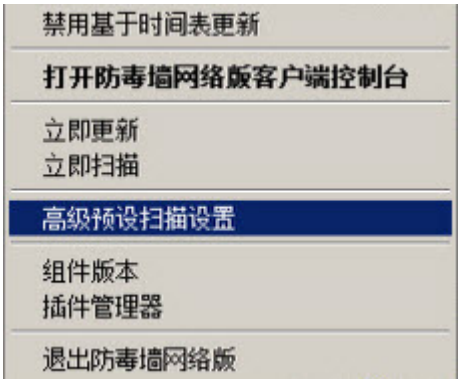


图 7-2. “预设扫描高级设置”选项

注意

如果通知消息已启用并设置为在预设扫描运行前显示分钟数，则用户无需执行此步骤。有关通知消息的详细信息，请参阅预设扫描权限通知 第 7-51 页。

b. 在所显示的通知窗口上，从下列选项中进行选择：

- **推迟扫描 __ 小时 __ 分钟。**
- **跳过此预设扫描。下一次预设扫描在 <日期> 的 <时间> 运行。**



图 7-3. 防毒墙网络版客户端终端上的预设扫描权限

- 如果预设扫描正在进行：

  a. 右键单击系统托盘上的防毒墙网络版客户端图标，然后选择**预设扫描高级设置**。

  b. 在所显示的通知窗口上，从下列选项中进行选择：

  - **停止扫描。在以下时间之后重新启动: __ 小时 __ 分钟。**
  - **停止扫描。下一次预设扫描在 <日期> 的 <时间> 运行。**

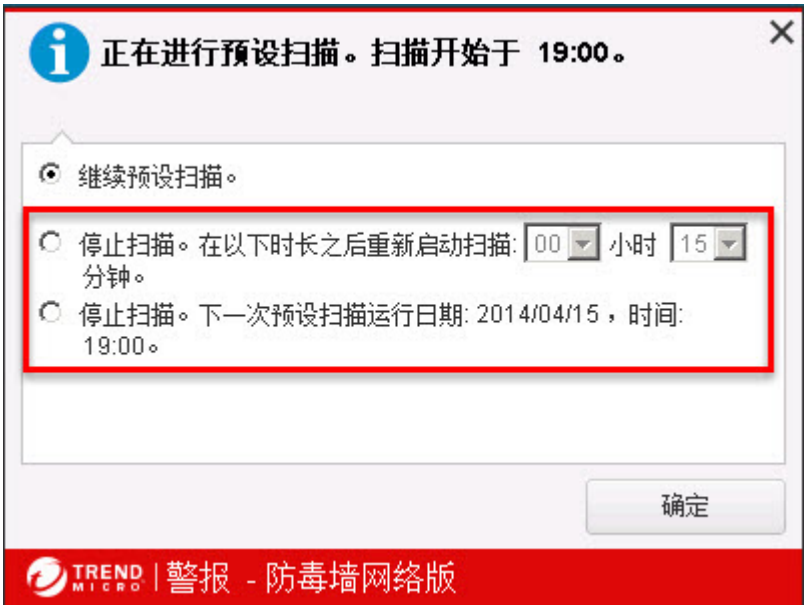


图 7-4. 防毒墙网络版客户端 终端上的预设扫描权限

邮件扫描权限和其他设置

当客户端具有邮件扫描权限时，防毒墙网络版客户端控制台上将显示**邮件扫描**选项。**邮件扫描**选项显示 POP3 邮件扫描。



图 7-5. 防毒墙网络版客户端控制台上的邮件扫描设置

下表介绍了 POP3 邮件扫描程序。

表 7-18. 邮件扫描程序

详细信息	描述
用途	扫描 POP3 电子邮件中是否存在病毒/恶意软件
必备条件	• 必须首先由管理员从 Web 控制台将其启用，然后用户才能使用该程序 **注意** 要启用 POP3 邮件扫描，请参阅授予邮件扫描权限和启用 POP3 邮件扫描 第 7-57 页。 • 可以从防毒墙网络版客户端控制台配置针对病毒/恶意软件的处理措施，但无法从 Web 控制台进行配置
支持的扫描类型	实时扫描 从 POP3 邮件服务器检索电子邮件时，便会执行扫描。
扫描结果	• 有关扫描完成后检测到的安全风险的信息 • 未在防毒墙网络版客户端控制台的**日志**窗口中记录的扫描结果 • 未发送到服务器的扫描结果
其他详细信息	与 Web 信誉功能共享防毒墙网络版 NT 代理服务 (TMProxy.exe)

授予邮件扫描权限和启用 POP3 邮件扫描

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转至**邮件扫描**部分。

5. 选择**在防毒墙网络版客户端控制台上显示“邮件扫描”设置**。
6. 单击**其他设置**选项卡，然后转至 **POP3 电子邮件扫描设置**部分。
7. 选择**扫描 POP3 电子邮件**。
8. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

扫描的缓存设置

防毒墙网络版客户端可以构建数字签名和按需扫描缓存文件以提高其扫描性能。运行按需扫描时，防毒墙网络版客户端会依次检查数字签名缓存文件和按需扫描缓存文件，以选择从扫描中排除的文件。如果从扫描中排除了大量文件，扫描时间则会减少。

数字签名缓存

数字签名缓存文件在手动扫描、预设扫描和立即扫描期间使用。客户端不会扫描签名已添加到数字签名缓存文件的文件。

防毒墙网络版客户端使用用于行为监控的相同数字签名特征码，来构建数字签名缓存文件。数字签名特征码包含趋势科技认为可信从而可从扫描中排除的文件的列表。



注意

Windows 服务器平台上自动禁用行为监控（Windows XP、2003 和不带 SP1 的 Vista 不提供 64 位支持）。如果启用数字签名缓存，这些平台上的防毒墙网络版客户端会下载要在缓存中使用的数字签名特征码，而不会下载其他行为监控组件。

客户端会根据时间表构建数字签名缓存文件，该时间表可从 Web 控制台进行配置。客户端执行此操作的目的如下：

- 为构建上一缓存文件后引入系统的新文件添加签名
- 移除系统中已修改或删除的文件的签名

在缓存构建过程中，客户端会检查以下文件夹中的可信文件，然后将这些文件的签名添加到数字签名缓存文件：

- %PROGRAMFILES%
- %WINDIR%

缓存构建过程不会影响终端的性能，因为客户端在此过程中使用的系统资源最少。客户端还可以继续进行由于某种原因（例如，主机电源关闭或无线终端的交流电适配器未插电时）而中断的缓存构建任务。

按需扫描缓存

按需扫描缓存文件在手动扫描、预设扫描和立即扫描期间使用。防毒墙网络版客户端不会扫描其缓存已添加到按需扫描缓存文件的文件。

每次运行扫描时，防毒墙网络版客户端都会检查不存在威胁的文件的属性。如果某个不存在威胁的文件在一段时间（该时间段可配置）内未经修改，则防毒墙网络版客户端会将该文件的缓存添加到按需扫描缓存文件。如果在下一次扫描时文件的缓存未过期，则不会扫描该文件。

不存在威胁的文件的缓存会在一定天数（该时间段亦可配置）内过期。如果在缓存到期时或到期之后进行扫描，防毒墙网络版客户端会移除过期的缓存并在文件中扫描威胁。如果文件不存在威胁且未经修改，会将该文件的缓存重新添加到按需扫描缓存文件。如果文件不存在威胁但最近进行了修改，则不会添加相应的缓存，并将在下次扫描时重新扫描该文件。

不存在威胁的文件的缓存过期可防止从扫描中排除受感染文件，如以下示例所示：

- 严重过期特征码文件可能已将受感染、未修改的文件视为不存在威胁。如果缓存未过期，受感染文件会保存在系统中，直到该文件被修改并通过实时扫描检测到。

- 如果修改了缓存的文件，且实时扫描在修改文件期间未正常运行，则只有缓存过期后，才能对修改的文件扫描威胁。

添加到按需扫描缓存文件的缓存数取决于扫描类型及其扫描目标。例如，如果在手动扫描期间防毒墙网络版客户端只扫描了终端中 1,000 个文件中的 200 个，缓存数可能会较少。

如果频繁运行按需扫描，则按需扫描缓存文件的扫描时间会显著减少。在所有缓存均未过期的扫描任务中，通常需要 12 分钟的扫描可以减到 1 分钟。降低文件必须保持不变的天数和延长缓存有效期限通常可以提高性能。由于文件必须在相对较短的时间内保持不变，因此可以将更多的缓存添加到缓存文件。缓存还可能会保持较长的有效期，这意味着有更多的文件跳过扫描。

如果很少运行按需扫描，可以禁用按需扫描缓存，因为缓存会在下一次运行扫描时过期。

配置扫描的缓存设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡，然后转至**扫描的缓存设置**部分。
5. 配置数字签名缓存的设置。
   a. 选择**启用数字签名缓存**。
   b. 在**每 __ 天构建缓存**中指定客户端构建缓存的频率。
6. 配置按需扫描缓存的设置。
   a. 选择**启用按需扫描缓存**。
   b. 在**为 __ 天未更改的安全文件添加缓存**中指定文件在缓存之前必须保持不变的天数。

c. 在**每个安全文件的缓存在 __ 天内过期**中指定缓存保留在缓存文件中的最大天数。

注意

为了防止扫描期间添加的所有缓存在同一天过期，缓存将在您指定的最大天数内随机过期。例如，如果今天将 500 个缓存添加到缓存，且指定的最大天数为 10，则一小部分缓存将在次日过期，而大部分缓存将在随后几天过期。在第 10 天，剩余的所有缓存都将过期。

7. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

可信程序列表权限

可以授予最终用户将防毒墙网络版配置为在实时扫描和行为监控扫描期间跳过对可信进程的扫描的权限。将程序添加到可信程序列表后，防毒墙网络版不会使程序或由该程序启动的任何进程受实时扫描的限制。将可信程序添加到可信程序列表以提高在终端上执行扫描的性能。

授予可信程序列表设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。

4. 在**权限**选项卡上，转至**可信程序列表**部分。
5. 选择**在防毒墙网络版客户端控制台上显示“可信程序列表”**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

全局扫描设置

将全局扫描设置应用于客户端有许多种方法。

- 特定扫描设置可以应用于服务器管理的所有客户端，或仅应用于具有某些扫描权限的客户端。例如，如果配置推迟预设扫描持续时间，则只有具有推迟预设扫描权限的客户端将使用该设置。
- 特定扫描设置可以应用于所有扫描类型或仅应用于特定扫描类型。例如，在同时安装了防毒墙网络版服务器和防毒墙网络版客户端的终端上，可以从扫描中排除防毒墙网络版服务器数据库。但是，此设置仅在实时扫描期间应用。
- 扫描病毒/恶意软件或间谍软件/灰色软件，或者同时扫描它们时，可以应用特定扫描设置。例如，评估模式仅在间谍软件/灰色软件扫描期间应用。

配置全局扫描设置

过程

1. 转至**客户端** > **全局客户端设置**。

2. 在每个可用部分中配置全局扫描设置。
   - “扫描设置”部分 第 7-63 页
   - “预设扫描设置”部分 第 7-68 页
   - “病毒/恶意软件日志带宽设置”部分 第 7-70 页
3. 单击**保存**。

“扫描设置”部分

通过**全局客户端设置**窗口的**扫描设置**部分，管理员可以配置以下各项：

- 将手动扫描添加到防毒墙网络版客户端的 Windows 快捷菜单中 第 7-63 页
- 从实时扫描中排除防毒墙网络版服务器数据库文件夹 第 7-64 页
- 从扫描中排除 Microsoft Exchange 服务器文件夹和文件 第 7-64 页
- 对文件操作启用延迟扫描 第 7-65 页
- 在终端上启用预启动的防恶意软件防护 第 7-65 页
- 配置大型压缩文件的扫描设置 第 7-66 页
- 清除/删除压缩文件中的受感染文件 第 7-66 页
- 启用评估模式 第 7-68 页
- 扫描 Cookie 第 7-68 页

将手动扫描添加到防毒墙网络版客户端的 Windows 快捷菜单中

启用此设置时，服务器管理的所有防毒墙网络版客户端都会在 Windows 资源管理器的右键单击菜单中添加一个**使用防毒墙网络版扫描**选项。当用户右键单击

Windows 桌面上或 Windows 资源管理器中的文件或文件夹并选择该选项时，手动扫描将扫描该文件或文件夹中是否有病毒/恶意软件和间谍软件/灰色软件。

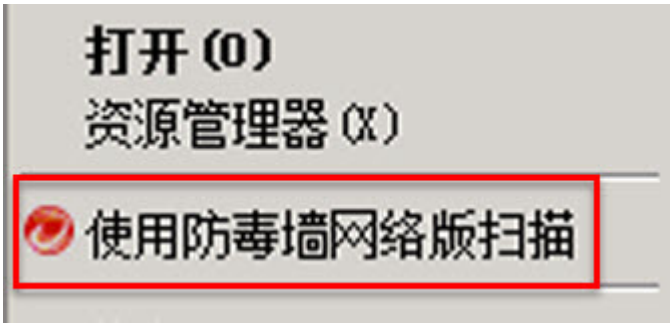


图 7-6. “使用防毒墙网络版扫描”选项

从实时扫描中排除防毒墙网络版服务器数据库文件夹

如果防毒墙网络版客户端和防毒墙网络版服务器位于同一个终端上，则防毒墙网络版客户端在实时扫描期间不会扫描服务器数据库中是否有病毒/恶意软件和间谍软件/灰色软件。

提示

启用此设置可防止扫描期间可能发生的数据库损坏。

从扫描中排除 Microsoft Exchange 服务器文件夹和文件

如果防毒墙网络版客户端与 Microsoft Exchange 2000/2003 服务器位于同一个终端上，则在手动扫描、实时扫描、预设扫描和立即扫描期间，防毒墙网络版不会扫描以下 Microsoft Exchange 文件夹和文件中是否有病毒/恶意软件和间谍软件/灰色软件：

- \Exchsrvr\Mailroot\vsi 1 中的以下文件夹：Queue、PickUp 和 BadMail

- .\Exchsrvr\mdbdata，包括以下文件：priv1.stm、priv1.edb、pub1.stm 和 pub1.edb
- .\Exchsrvr\Storage Group

对于 Microsoft Exchange 2007 或更高版本的文件夹，需要手动将这些文件夹添加到扫描例外列表。有关扫描例外详细信息，请访问以下 Web 站点：

http://technet.microsoft.com/en-us/library/bb332342.aspx

有关配置扫描例外列表的步骤，请参阅扫描例外 第 7-26 页。

对文件操作启用延迟扫描

管理员可以配置防毒墙网络版以延迟文件扫描。防毒墙网络版允许用户复制文件，然后在复制过程完成后进行扫描。该延迟扫描功能提高了复制和扫描过程的性能。

注意

延迟扫描要求病毒扫描引擎 (VSAPI) 版本为 9.713 或更高版本。有关升级该服务器的详细信息，请参阅手动更新防毒墙网络版服务器 第 6-25 页。

在终端上启用预启动的防恶意软件防护

作为安全启动标准，防毒墙网络版支持预启动的防恶意软件 (ELAM) 功能，能够在终端上提供启动时防护。管理员可启用此功能，以便当终端启动时，在其他第三方软件驱动程序之前启动防毒墙网络版客户端。此功能可使防毒墙网络版客户端在启动过程中检测恶意软件。

扫描所有第三方软件驱动程序后，防毒墙网络版客户端将向系统内核报告驱动程序分类信息。管理员可以在 Windows 的“组策略”中根据驱动程序分类定义处理措施，并在终端上使用事件查看器查看扫描结果。

注意

仅 Windows 8、Windows Server 2012 或更高版本支持 ELAM。

配置大型压缩文件的扫描设置

在手动扫描、实时扫描、预设扫描和立即扫描期间，扫描每个层中是否有病毒/恶意软件和间谍软件/灰色软件，服务器管理的所有防毒墙网络版客户端将检查以下设置：

- **配置大型压缩文件的扫描设置**：选择此选项可以启用压缩文件处理。
- 为实时扫描和其他扫描类型（手动扫描、预设扫描和立即扫描）分别配置以下设置：
  - **如果压缩文件大小超过 __ MB，则不扫描其中的文件**：防毒墙网络版不扫描超过该限制的任何文件。
  - **在压缩文件中，仅扫描前 __ 个文件**：对于压缩文件，防毒墙网络版扫描指定数目的文件，而忽略其余文件。

清除/删除压缩文件中的受感染文件

当服务器管理的所有客户端在手动扫描、实时扫描、预设扫描和立即扫描期间在压缩文件中检测到病毒/恶意软件时，如果满足以下条件，则客户端将清除或删除受感染文件。

- ?清除?或?删除?是防毒墙网络版设置执行的处理措施。可通过转至**客户端 > 客户端管理 > 设置 > 扫描设置 > {扫描类型} > 处理措施**选项卡，查看防毒墙网络版对受感染文件执行的处理措施。
- 启用该设置。启用此设置可能增加扫描期间的终端资源占用，扫描可能要用更长时间才能完成。这是因为防毒墙网络版需要解压缩压缩文件，清除或删除压缩文件中的受感染文件，然后重新压缩该文件。
- 支持该压缩文件格式。防毒墙网络版仅支持某些压缩文件格式，包括 ZIP 和 Office Open XML（使用 ZIP 压缩技术）。Office Open XML 是 Microsoft Office 2007 应用程序（例如 Excel、PowerPoint 和 Word）的缺省格式。



注意

有关支持的压缩文件格式的完整列表，请联系技术支持提供商。

例如，将实时扫描设置为删除受病毒感染的文件。在实时扫描解压缩名为 abc.zip 的压缩文件并在压缩文件中检测到受感染文件 123.doc 之后，防毒墙网络版将删除 123.doc，然后重新压缩 abc.zip，现在可以对其进行安全访问。

下表说明了在不符合所有这些条件时会发生的情况。

表 7-19. 压缩文件情形和结果

“清除/删除压缩文件中的受感染文件”的状态	防毒墙网络版设置执行的处理措施	压缩文件格式	结果
已启用	清除或删除	不支持 示例：def.rar 包含受感染文件 123.doc。	防毒墙网络版加密 def.rar，但不会对 123.doc 执行清除、删除或任何其他处理措施。
已禁用	清除或删除	支持/不支持 示例：abc.zip 包含受感染文件 123.doc。	防毒墙网络版不会对 abc.zip 和 123.doc 执行清除、删除或任何其他处理措施。
已启用/已禁用	非清除或删除（即执行以下之一：更名、隔离、拒绝访问或不予处理）	支持/不支持 示例：abc.zip 包含受感染文件 123.doc。	防毒墙网络版对 abc.zip 而不是 123.doc 执行配置的处理措施（更名、隔离、拒绝访问或不予处理）。 如果处理措施为： **更名**：防毒墙网络版会将 abc.zip 更名为 abc.vir，但不会更名 123.doc。 **隔离**：防毒墙网络版会隔离 abc.zip（123.doc 和所有未感染的文件都会被隔离）。 **不予处理**：防毒墙网络版不会对 abc.zip 和 123.doc 执行任何处理措施，但会记录病毒检测情况。 **拒绝访问**：在打开 abc.zip 时防毒墙网络版会拒绝对它的访问（123.doc 和所有未感染文件都无法打开）。

启用评估模式

处于评估模式时，服务器管理的所有客户端都将记录在手动扫描、预设扫描、实时扫描和立即扫描期间检测到的间谍软件/灰色软件，但是不会清除间谍软件/灰色软件组件。清除操作将终止进程或删除注册表项、文件、cookie 和快捷方式。

趋势科技提供评估模式以允许您评估趋势科技检测为间谍软件/灰色软件的项目，然后根据您的评估采取适当的处理措施。例如，如果您认为检测出的间谍软件/灰色软件不存在安全风险，则可以将其添加至间谍软件/灰色软件允许列表。

在评估模式下时，防毒墙网络版会执行以下扫描处理措施：

- **不予处理**：在手动扫描、预设扫描和立即扫描期间
- **拒绝访问**：在实时扫描期间



注意

评估模式会覆盖任何用户配置的扫描处理措施。例如，即使您在手动扫描期间选择“清除”作为扫描处理措施，当客户端处于评估模式下时，“不予处理”仍保留为扫描处理措施。

扫描 Cookie

如果将 Cookie 视为潜在的安全风险，则选择此选项。选择此选项后，在手动扫描、预设扫描、实时扫描和立即扫描期间，服务器管理的所有客户端都将扫描 Cookie 中是否有间谍软件/灰色软件。

“预设扫描设置”部分

仅设置为运行预设扫描的客户端使用下列设置。预设扫描可以扫描病毒/恶意软件和间谍软件/灰色软件。

通过全局扫描设置的预设扫描设置部分，管理员可以配置以下各项：

- 在预设扫描开始前 __ 分钟提醒用户 第 7-69 页
- 最多推迟预设扫描 __ 小时和 __ 分钟 第 7-69 页
- 在扫描持续超过 __ 小时和 __ 分钟时自动停止预设扫描 第 7-69 页
- 当无线终端的电池组可用时间低于 __ % 且其交流电适配器未插电时跳过预设扫描 第 7-70 页
- 重新开始错过的预设扫描 第 7-70 页

在预设扫描开始前 __ 分钟提醒用户

防毒墙网络版将在预设扫描运行前数分钟显示一条通知消息，以提醒用户扫描时间表（日期和时间）和您授予他们的任何预设扫描权限。

可以从**客户端** > **客户端管理** > **设置** > **权限和其他设置** > **其他设置（选项卡）** > **预设扫描设置**中，启用/禁用通知消息。禁用时，不显示提醒。

最多推迟预设扫描 __ 小时和 __ 分钟

只有具有“推迟预设扫描”权限的用户才可以执行下列操作：

- 在预设扫描运行前推迟预设扫描，然后指定推迟的时间长度。
- 如果预设扫描正在进行中，则用户可以停止扫描并在以后重新启动它。然后，用户指定扫描重新开始前应经过的时间长度。当扫描重新开始时，所有以前扫描过的文件都会再扫描一遍。

  用户可以指定的最大推迟时间长度/所用时间为 12 小时 45 分钟，您可以在提供的文本框中指定小时数和/或分钟数来减少该时间。

在扫描持续超过 __ 小时和 __ 分钟时自动停止预设扫描

超过指定的时间长度且扫描尚未完成时，防毒墙网络版将停止扫描。防毒墙网络版会立即将在扫描期间检测到的任何安全风险通知给用户。

当无线终端的电池组可用时间低于 __ % 且其交流电适配器未插电时跳过预设扫描

如果防毒墙网络版检测到无线终端电池电量很低且交流电适配器没有连接到任何电源上，则当预设扫描启动时防毒墙网络版会立即跳过扫描。如果电池电量很低，但交流电适配器已连接到电源上，则扫描会继续进行。

重新开始错过的预设扫描

当由于防毒墙网络版在预设扫描的日期和时间未运行而导致预设扫描未启动时，或如果用户中断了预设扫描（例如，扫描开始后关闭了终端），您可以指定防毒墙网络版何时恢复扫描。

指定要重新启动的预设扫描：

- **重新开始中断的预设扫描**：重新开始由于用户关闭终端而中断的预设扫描
- **重新开始错过的预设扫描**：重新开始由于终端未运行而导致错过的预设扫描

指定何时重新开始扫描：

- **次日同一时间**：如果防毒墙网络版在次日同一时间处于运行状态，则恢复扫描。
- **__ 分钟 (终端启动后)**：防毒墙网络版在用户启动终端一段时间（分钟）后恢复扫描。该时间长度介于 10 到 120 分钟之间。



注意

用户可以推迟或跳过已恢复的预设扫描（如果管理员启用了此权限）。有关详细信息，请参阅预设扫描权限和其他设置 第 7-50 页。

“病毒/恶意软件日志带宽设置”部分

通过全局扫描设置的“病毒/恶意软件日志带宽设置”部分，管理员可以配置以下各项：

使防毒墙网络版客户端对于一小时之内重复检测到的同一病毒/恶意软件只创建一个病毒/恶意软件日志条目 第 7-71 页

使防毒墙网络版客户端对于一小时之内重复检测到的同一病毒/恶意软件只创建一个病毒/恶意软件日志条目

在较短时间内检测到多处由同一病毒/恶意软件导致的感染时，防毒墙网络版将整合病毒日志条目。防毒墙网络版可多次检测到同一单个病毒/恶意软件，从而在防毒墙网络版客户端将日志信息发送到服务器时快速填写病毒/恶意软件日志并占用网络带宽。启用此功能可帮助在将病毒日志信息报告给服务器时同时减少所生成的病毒/恶意软件日志条目数和防毒墙网络版客户端占用的网络带宽量。

安全软件认证服务部分

通过**全局扫描设置**的**安全软件认证服务**部分，管理员可以配置以下各项：

为行为监控、防火墙和防病毒扫描启用安全软件认证服务 第 7-71 页

为行为监控、防火墙和防病毒扫描启用安全软件认证服务

安全软件认证服务会查询趋势科技数据中心，以验证由恶意软件行为阻止、事件监控、防火墙或防病毒扫描检测到的程序的安全性。启用安全软件认证服务可降低误判检测的可能性。

注意

请先确保防毒墙网络版客户端的代理服务器设置正确（有关详细信息，请参阅防毒墙网络版客户端代理服务器设置 第 14-44 页），然后再启用安全软件认证服务。不正确的代理服务器设置和不稳定的 Internet 连接都会导致从趋势科技数据中心接收响应延迟或不成功，从而导致受监控程序看上去处于无响应状态。

另外，纯 IPv6 防毒墙网络版客户端无法直接从趋势科技数据中心进行查询。为允许防毒墙网络版客户端连接到趋势科技数据中心，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

安全风险通知

防毒墙网络版附带有一组缺省通知消息，用于通知您、其他防毒墙网络版管理员和防毒墙网络版客户端用户检测到的安全风险。

有关发送给管理员的通知的详细信息，请参阅针对管理员的安全风险通知 第 7-72 页。

有关发送给防毒墙网络版客户端用户的通知的详细信息，请参阅针对防毒墙网络版客户端用户的安全风险通知 第 7-78 页。

针对管理员的安全风险通知

配置防毒墙网络版在检测到安全风险时向您和其他防毒墙网络版管理员发送通知，或仅当对安全风险的处理措施不成功因此需要您的干预时才发送通知。

防毒墙网络版附带有一组缺省通知消息，用于通知您和其他防毒墙网络版管理员安全风险检测。您可以根据需要修改通知和配置其他通知设置。

表 7-20. 安全风险通知的类型

类型	参考
病毒/恶意软件	配置针对管理员的安全风险通知 第 7-73 页
间谍软件/灰色软件	配置针对管理员的安全风险通知 第 7-73 页

类型	参考
数字资产传输	配置管理员的数据丢失防护通知 第 10-49 页
C&C 回呼	为管理员配置 C&C 回呼通知 第 11-17 页

注意

防毒墙网络版可以通过电子邮件、SNMP 陷阱和 Windows NT 事件日志来发送通知。配置防毒墙网络版何时通过这些通道发送通知的设置。有关详细信息，请参阅管理员通知设置 第 13-32 页。

配置针对管理员的安全风险通知

过程

1. 转至**管理** > **通知** > **管理员**。
2. 在**条件**选项卡中：
   a. 转到**病毒/恶意软件**和**间谍软件/灰色软件**部分。
   b. 指定是在防毒墙网络版检测到病毒/恶意软件和间谍软件/灰色软件时发送通知，还是仅当对这些安全风险的处理措施不成功时发送通知。
3. 在**电子邮件**选项卡中：
   a. 转到**病毒/恶意软件检测**和**间谍软件/灰色软件检测**部分。
   b. 选择**启用电子邮件通知**。
   c. 选择**向拥有客户端树域权限的用户发送通知**。

   可以使用基于角色的管理授予用户客户端树域权限。如果属于特定域的某个防毒墙网络版客户端上发生检测，则会向具有域权限的用户的电子邮件地址发送电子邮件。有关示例，请参阅下表：

表 7-21. 客户端树域和权限

客户端树域	具有域权限的角色	具有该角色的用户帐户	用户帐户的电子邮件地址
域 A	Administrator (内置)	根	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
域 B	Administrator (内置)	根	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果属于域 A 的防毒墙网络版客户端检测到病毒，会向 mary@xyz.com、john@xyz.com 和 chris@xyz.com 发送电子邮件。

如果属于域 B 的防毒墙网络版客户端检测到间谍软件，会向 mary@xyz.com 和 jane@xyz.com 发送电子邮件。

注意

如果启用此选项，具有域权限的所有用户都必须具有相应的电子邮件地址。不会向没有电子邮件地址的用户发送电子邮件通知。用户和电子邮件地址是从**管理** > **帐户管理** > **用户帐户**进行配置的。

d. 选择**向以下电子邮件地址发送通知**，然后键入电子邮件地址。

e. 接受或修改缺省的主题和消息。可以使用标记变量表示**主题**和**消息**文本框中的数据。

表 7-22. 安全风险通知的标记变量

变量	描述
病毒/恶意软件检测	
%v	**病毒/恶意软件名称**
%s	**具有病毒/恶意软件的终端**

变量	描述
%i	终端的 IP 地址
%c	终端的 MAC 地址
%m	终端的域
%p	病毒/恶意软件的位置
%y	病毒/恶意软件的检测日期和时间
%e	病毒扫描引擎版本
%r	病毒码版本
%a	对安全风险执行的处理措施
%n	登录到受感染终端的用户的名称
间谍软件/灰色软件检测	
%s	具有间谍软件/灰色软件的终端
%i	终端的 IP 地址
%m	终端的域
%y	间谍软件/灰色软件的检测日期和时间
%n	检测时登录到终端的用户的名称
%T	间谍软件/灰色软件和扫描结果

4. 在 **SNMP 陷阱**选项卡中：

   a. 转到**病毒/恶意软件检测**和**间谍软件/灰色软件检测**部分。

   b. 选择**启用 SNMP 陷阱通知**。

   c. 接受或修改缺省消息。可以使用下表中的标记变量表示**消息**文本框中的数据。

表 7-23. 安全风险通知的标记变量

变量	描述
病毒/恶意软件检测	
%v	病毒/恶意软件名称
%s	具有病毒/恶意软件的终端
%i	终端的 IP 地址
%c	终端的 MAC 地址
%m	终端的域
%p	病毒/恶意软件的位置
%y	病毒/恶意软件的检测日期和时间
%e	病毒扫描引擎版本
%r	病毒码版本
%a	对安全风险执行的处理措施
%n	登录到受感染终端的用户的名称
间谍软件/灰色软件检测	
%s	具有间谍软件/灰色软件的终端
%i	终端的 IP 地址
%m	终端的域
%y	间谍软件/灰色软件的检测日期和时间
%n	检测时登录到终端的用户的名称
%T	间谍软件/灰色软件和扫描结果
%v	间谍软件/灰色软件名称
%a	对安全风险执行的处理措施

5. 在 **NT 事件日志**选项卡中：

a. 转到**病毒/恶意软件检测**和**间谍软件/灰色软件检测**部分。

b. 选择**启用 NT 事件日志通知**。

c. 接受或修改缺省消息。可以使用下表中的标记变量表示**消息**文本框中的数据。

表 7-24. 安全风险通知的标记变量

变量	描述
病毒/恶意软件检测	
%v	病毒/恶意软件名称
%s	具有病毒/恶意软件的终端
%i	终端的 IP 地址
%c	终端的 MAC 地址
%m	终端的域
%p	病毒/恶意软件的位置
%y	病毒/恶意软件的检测日期和时间
%e	病毒扫描引擎版本
%r	病毒码版本
%a	对安全风险执行的处理措施
%n	登录到受感染终端的用户的名称
间谍软件/灰色软件检测	
%s	具有间谍软件/灰色软件的终端
%i	终端的 IP 地址
%m	终端的域
%y	间谍软件/灰色软件的检测日期和时间
%n	检测时登录到终端的用户的名称

变量	描述
%T	间谍软件/灰色软件和扫描结果
%v	间谍软件/灰色软件名称
%a	对安全风险执行的处理措施

6. 单击**保存**。

针对防毒墙网络版客户端用户的安全风险通知

防毒墙网络版可以在以下情况下在防毒墙网络版客户端终端上显示通知消息：

- 实时扫描和预设扫描检测到病毒/恶意软件和间谍软件/灰色软件后立即显示。启用通知消息，并根据需要修改其内容。
- 必须重新启动客户端终端才能完成清除受感染文件时。对于实时扫描，该消息会在已扫描特定安全风险后显示。对于手动扫描、预设扫描和立即扫描，该消息仅在防毒墙网络版扫描完所有扫描目标后显示一次。

表 7-25. 安全风险客户端通知的类型

类型	参考
病毒/恶意软件	配置病毒/恶意软件通知 第 7-79 页
间谍软件/灰色软件	配置间谍软件/灰色软件通知 第 7-80 页
防火墙违例	修改防火墙通知消息的内容 第 12-26 页
Web 信誉违例	修改 Web 威胁通知 第 11-16 页
设备控制违例	修改设备控制通知 第 9-16 页
行为监控策略违例	修改通知消息的内容 第 8-12 页
数字资产传输	配置客户端的数据丢失防护通知 第 10-52 页
C&C 回呼	修改 Web 威胁通知 第 11-16 页

通知用户病毒/恶意软件与间谍软件/灰色软件检测

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **扫描设置** > **实时扫描设置**或**设置** > **扫描设置** > **预设扫描设置**。
4. 单击**处理措施**选项卡。
5. 选择下列选项：
   - **检测到病毒/恶意软件时在客户端终端上显示通知消息**
   - **检测到可能的病毒/恶意软件时在客户端终端上显示通知消息**
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

配置病毒/恶意软件通知

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择**病毒/恶意软件**。
3. 配置检测设置。

a. 选择为所有与病毒/恶意软件相关的事件显示一个通知，或者根据以下严重性级别分别显示单独通知：

- **高**：防毒墙网络版客户端无法处理严重的恶意软件
- **中**：防毒墙网络版客户端无法处理恶意软件
- **低**：防毒墙网络版客户端无法解决所有威胁

b. 接受或修改缺省消息。

4. 单击**保存**。

配置间谍软件/灰色软件通知

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择**间谍软件/灰色软件**。
3. 接受或修改缺省消息。
4. 单击**保存**。

通知客户端重新启动以完成清除受感染文件

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。

4. 单击**其他设置**选项卡，然后转至**重新启动通知**部分。
5. 选择**如果终端需要重新启动以完成清除受感染文件，则显示通知消息**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

安全风险日志

防毒墙网络版在检测到病毒/恶意软件或间谍软件/灰色软件时以及恢复间谍软件/灰色软件时，会生成日志。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看病毒/恶意软件日志

防毒墙网络版客户端在检测到病毒和恶意软件时会生成日志，并将日志发送到服务器。

过程

1. 转到以下项之一：
   - **日志 > 客户端 > 安全风险**
   - **客户端 > 客户端管理**
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。

3. 单击**日志** > **病毒/恶意软件日志**或**查看日志** > **病毒/恶意软件日志**。

4. 指定日志条件，然后单击**显示日志**。

5. 查看日志。日志包含以下信息：

   - 病毒/恶意软件的检测日期和时间
   - 终端
   - 安全威胁
   - 感染源
   - 受感染的文件或对象
   - 检测到病毒/恶意软件的扫描类型
   - 扫描结果

   注意

   有关扫描结果的详细信息，请参阅病毒/恶意软件扫描结果 第 7-83 页。

   - IP 地址
   - MAC 地址
   - 日志详细信息（单击**查看**可查看详细信息。）

6. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

   CSV 文件包含以下信息：

   - 日志中的所有信息
   - 检测时登录到终端的用户名

病毒/恶意软件扫描结果

病毒/恶意软件日志中将显示以下扫描结果：

表 7-26. 扫描结果

结果	描述
删除	• 第一处理措施是“删除”，并且受感染文件已删除。 • 第一处理措施是“清除”，但清除未成功。第二处理措施是“删除”，并且受感染文件已删除。
隔离	• 第一处理措施是“隔离”，并且受感染文件已隔离。 • 第一处理措施是“清除”，但清除未成功。第二处理措施是“隔离”，并且受感染文件已隔离。
已清除	受感染文件已清除。
已更名	• 第一处理措施是“更名”，并且受感染文件已更名。 • 第一处理措施是“清除”，但清除未成功。第二处理措施是“更名”，并且受感染文件已更名。
拒绝访问	• 第一处理措施是“拒绝访问”，当用户尝试打开受感染文件时，对该文件的访问被拒绝。 • 第一处理措施是“清除”，但清除未成功。第二处理措施是“拒绝访问”，当用户尝试打开受感染文件时，对该文件的访问被拒绝。 • 在实时扫描期间检测到可能的病毒/恶意软件。 • 即使扫描处理措施为“清除”（第一处理措施）和“隔离”（第二处理措施），实时扫描也可能拒绝访问感染了引导区病毒的文件。这是因为尝试清除引导区病毒可能会损害受感染终端的主引导记录 (MBR)。运行“手动扫描”以便防毒墙网络版可以清除或隔离该文件。
已略过	• 第一处理措施是“不予处理”。防毒墙网络版未对受感染文件执行任何处理措施。 • 第一处理措施是“清除”，但清除未成功。第二处理措施是“不予处理”，因此防毒墙网络版未对受感染文件执行任何处理措施。

结果	描述
已略过一个潜在安全风险	仅当防毒墙网络版在手动扫描、预设扫描和立即扫描期间检测到“可能的病毒/恶意软件”时，才显示此扫描结果。有关可能的病毒/恶意软件以及如何向趋势科技提交可疑文件以进行分析的信息，请参考趋势科技联机病毒百科全书上的以下页面。 http://www.trendmicro.com/vinfo/zh-cn/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn
无法清除或隔离文件	“清除”是第一处理措施。“隔离”是第二处理措施，两项处理措施都未成功。 解决方案：请参阅无法隔离文件/无法更名文件 第 7-84 页。
无法清除或删除文件	“清除”是第一处理措施。“删除”是第二处理措施，两项处理措施都未成功。 解决方案：请参阅无法删除文件 第 7-84 页。
无法清除或更名文件	“清除”是第一处理措施。“更名”是第二处理措施，两项处理措施都未成功。 解决方案：请参阅无法隔离文件/无法更名文件 第 7-84 页。
暂时无法隔离/暂时无法更名	说明 1 受感染的文件可能由另外一个应用程序锁定、正在执行或位于 CD 中。防毒墙网络版将在应用程序释放文件或文件执行完毕后再隔离/更名该文件。 解决方案 对于 CD 中的受感染文件，请考虑不要使用该 CD，因为病毒可能会感染网络上的其他计算机。
	说明 2 受感染的文件位于客户端终端的 Temporary Internet Files 文件夹中。由于用户在浏览时终端会下载文件，因此 Web 浏览器可能已锁定受感染文件。Web 浏览器释放文件后，防毒墙网络版将隔离/更名文件。 解决方案：无
无法删除文件	说明 1

结果	描述
	受感染文件可能包含在压缩文件中，并且**客户端** > **全局客户端设置**中的**清除/删除压缩文件中的受感染文件**设置已禁用。 解决方案 启用**清除/删除压缩文件中的受感染文件**选项。启用时，防毒墙网络版会对压缩文件进行解压缩，清除/删除压缩文件中的受感染文件，然后重新压缩文件。 **注意** 启用此设置可能增加扫描期间的终端资源占用，扫描可能要用更长时间才能完成。
	说明 2 受感染的文件可能由另外一个应用程序锁定、正在执行或位于 CD 中。防毒墙网络版将在应用程序释放文件或文件执行完毕后再删除该文件。 解决方案 对于 CD 中的受感染文件，请考虑不要使用该 CD，因为病毒可能会感染网络上的其他计算机。
	说明 3 受感染的文件位于防毒墙网络版客户端终端的 Temporary Internet Files 文件夹中。由于用户在浏览时终端会下载文件，因此 Web 浏览器可能已锁定受感染文件。Web 浏览器释放文件后，防毒墙网络版将删除文件。 解决方案：无
无法将隔离文件发送到指定的隔离文件夹中	尽管防毒墙网络版成功将一个文件隔离在防毒墙网络版客户端终端上的 \Suspect 文件夹中，但它无法将该文件发送到指定的隔离目录。 解决方案 确定检测到该病毒/恶意软件的扫描类型（手动扫描、实时扫描、预设扫描或立即扫描），然后检查**客户端** > **客户端管理 > 设置** > **{扫描类型}** > **处理措施**选项卡中指定的隔离目录。 如果隔离目录在防毒墙网络版服务器计算机或另一台防毒墙网络版服务器计算机上：

结果	描述
	1. 检查客户端是否可以连接到该服务器。 2. 如果使用 URL 作为隔离目录格式： a. 确保您在 http:// 后指定的终端名称正确。 b. 检查受感染文件的大小。如果其大小超出**管理** > **设置** > **隔离管理器**中指定的最大文件大小，则调整设置以适应该文件。还可以执行其他处理措施，如删除文件。 c. 检查隔离目录文件夹的大小，并确定其是否超过了在**管理** > **设置** > **隔离管理器**中指定的文件夹容量。调整该文件夹容量，或手动删除隔离目录中的文件。 3. 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。还应检查隔离目录文件夹是否存在以及 UNC 路径是否正确。 如果隔离目录在网络上的另一台终端中（对于此情形只能使用 UNC 路径）： 1. 检查防毒墙网络版客户端是否可以连接到该终端。 2. 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。 3. 检查隔离目录文件夹是否存在。 4. 检查 UNC 路径是否正确。 如果隔离目录在防毒墙网络版客户端终端的其他目录中（对于此情形只能使用绝对路径），请检查隔离目录文件夹是否存在。
无法清除文件	说明 1 受感染文件可能包含在压缩文件中，并且**客户端** > **全局客户端设置**中的“清除/删除”压缩文件中的受感染文件设置已禁用。 解决方案 启用**清除/删除压缩文件中的受感染文件**选项。启用时，防毒墙网络版会对压缩文件进行解压缩，清除/删除压缩文件中的受感染文件，然后重新压缩文件。

结果	描述
	注意 启用此设置可能增加扫描期间的终端资源占用，扫描可能要用更长时间才能完成。
	说明 2 受感染的文件位于防毒墙网络版客户端终端的 Temporary Internet Files 文件夹中。由于用户在浏览时终端会下载文件，因此 Web 浏览器可能已锁定受感染文件。Web 浏览器释放文件后，防毒墙网络版将清除文件。 解决方案：无
	说明 3 文件可能无法清除。有关详细信息和解决方法，请参阅非可清除文件 第 E-15 页。
需要处理措施	在无用户干预的情况下，防毒墙网络版无法完成对受感染文件的配置处理措施。鼠标悬停在**需要处理措施**列以查看以下详细信息。 • “需要处理措施 - 有关如何使用防毒墙网络版工具箱中找到的防威胁工具包 "Clean Boot" 工具来删除此威胁的详细信息，请联系支持部门” • “需要处理措施 - 有关如何使用防毒墙网络版工具箱中找到的防威胁工具包“救援磁盘”工具来删除此威胁的详细信息，请联系支持部门” • “需要处理措施 - 有关如何使用防毒墙网络版工具箱中找到的防威胁工具包 "Rootkit Buster" 工具来删除此威胁的详细信息，请联系支持部门” • “需要处理措施 - 防毒墙网络版检测到受感染的客户端上存在一个威胁。请重新启动终端以完成安全威胁的清除” • “需要处理措施 - 执行完整系统扫描”

查看集中隔离恢复日志

清除恶意软件后，防毒墙网络版客户端会备份恶意软件数据。如果您认为某数据无害，请通知联机客户端恢复该备份数据。在日志中提供了有关哪些恶意软件备份数据已恢复、受感染的终端和恢复结果的信息。

过程

1. 转至**日志** > **客户端** > **集中隔离恢复**。
2. 检查**成功**、**未成功**和**挂起**列以查看防毒墙网络版是否已成功恢复隔离数据。
3. 单击每列的计数以查看有关每个受感染终端的详细信息。

   注意

   对于**未成功**恢复，可以尝试在**集中隔离恢复详细信息**窗口中通过单击**恢复全部**重新恢复文件。

4. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

查看间谍软件/灰色软件日志

防毒墙网络版客户端在检测到间谍软件和灰色软件时会生成日志，并将日志发送到服务器。

过程

1. 转到以下项之一：
   - **日志** > **客户端** > **安全风险**
   - **客户端** > **客户端管理**

2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **间谍软件/灰色软件日志**或**查看日志** > **间谍软件/灰色软件日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 查看日志。日志包含以下信息：
   - 间谍软件/灰色软件的检测日期和时间
   - 受感染的终端
   - 间谍软件/灰色软件名称
   - 检测到间谍软件/灰色软件的扫描类型
   - 有关间谍软件/灰色软件扫描结果的详细信息（是否成功执行了扫描处理措施）。请参阅间谍软件/灰色软件扫描结果 第 7-89 页以了解详细信息。
   - IP 地址
   - MAC 地址
   - 日志详细信息（单击**查看**可查看详细信息。）
6. 将您认为无害的间谍软件/灰色软件添加到间谍软件/灰色软件允许列表。
7. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

   CSV 文件包含以下信息：
   - 日志中的所有信息
   - 检测时登录到终端的用户名

间谍软件/灰色软件扫描结果

间谍软件/灰色软件日志中将显示以下扫描结果：

表 7-27. 第一级别间谍软件/灰色软件扫描结果

结果	描述
成功，无需采取任何处理措施	如果扫描处理措施成功，则这是第一级别结果。第二级别结果可能是以下任何状态： • 已清除 • 拒绝访问
需要进一步的处理措施	如果扫描处理措施未成功，这是第一级别结果。第二级别的结果将至少具有以下消息其中之一： • 已略过 • 清除间谍软件/灰色软件存在风险 • 间谍软件/灰色软件扫描已手动停止。请执行一次完全扫描 • 间谍软件/灰色软件已清除，需要重新启动。请重新启动计算机 • 无法清除间谍软件/灰色软件 • 无法识别间谍软件/灰色软件扫描结果。请联系趋势科技技术支持部门

表 7-28. 第二级别间谍软件/灰色软件扫描结果

结果	描述	解决方案
已清除	防毒墙网络版已终止进程或删除注册表、文件、cookie 和快捷方式。	无
拒绝访问	防毒墙网络版拒绝对检测到的间谍软件/灰色软件组件的访问（复制、打开）。	无
已略过	防毒墙网络版未执行任何处理措施，但记录了间谍软件/灰色软件的检测情况以进行评估。	将您认为安全的间谍软件/灰色软件添加到间谍软件/灰色软件允许列表。

结果	描述	解决方案
清除间谍软件/灰色软件存在风险	如果间谍软件扫描引擎尝试清除任何单个文件夹并满足以下条件，则将显示此消息： • 要清除的项超过 250MB。 • 操作系统将使用该文件夹中的文件。正常系统操作可能也需要该文件夹。 • 该文件夹为根目录（如 C: 或 F:）	请联系您的技术支持提供商以寻求帮助。
间谍软件/灰色软件扫描已手动停止。请执行一次完全扫描	用户在扫描完成前停止了扫描。	运行“手动扫描”并等待扫描完成。
间谍软件/灰色软件已清除，需要重新启动。请重新启动计算机	防毒墙网络版已清除间谍软件/灰色软件组件，但需要重新启动终端以完成该任务。	立即重新启动终端。
无法清除间谍软件/灰色软件	在 CD-ROM 或网络驱动器中检测到间谍软件/灰色软件。防毒墙网络版无法清除在这些位置检测到的间谍软件/灰色软件。	手动移除受感染文件。
无法识别间谍软件/灰色软件扫描结果。请联系趋势科技技术支持部门	新版本的间谍软件扫描引擎提供防毒墙网络版尚未配置为可处理的一种新扫描结果。	要获取确定新扫描结果的帮助，请联系技术支持提供商。

查看间谍软件/灰色软件恢复日志

清除间谍软件/灰色软件后，防毒墙网络版客户端备份间谍软件/灰色软件数据。如果您认为某数据无害，请通知联机客户端恢复该备份数据。在日志中提供了有关哪些间谍软件/灰色软件备份数据已恢复、受感染的终端和恢复结果的信息。

过程

1. 转至**日志** > **客户端** > **间谍软件/灰色软件恢复**。
2. 检查**结果**列，查看防毒墙网络版是否已成功恢复间谍软件/灰色软件数据。

3. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

查看可疑文件日志

防毒墙网络版客户端在检测到可疑文件时会生成日志，并将日志发送到服务器。

过程

1. 转到以下项之一：
   - **日志** > **客户端** > **安全风险**
   - **客户端** > **客户端管理**
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **可疑文件日志**或**查看日志** > **可疑文件日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 查看日志。日志包含以下信息：
   - 可疑文件的检测日期和时间
   - 终端
   - 域
   - 文件的感染源 SHA-1 哈希值
   - 文件路径
   - 检测到间可疑文件的扫描类型
   - 扫描结果

注意

有关扫描结果的详细信息，请参阅病毒/恶意软件扫描结果 第 7-83 页。

- IP 地址

查看扫描操作日志

运行手动扫描、预设扫描或立即扫描时，防毒墙网络版客户端会创建包含有关该扫描的信息的扫描日志。可以通过访问防毒墙网络版服务器或防毒墙网络版客户端控制台来查看扫描日志。

要查看防毒墙网络版服务器上的扫描操作日志，请转到以下一个位置：

- **日志** > **客户端** > **安全风险**并单击**查看日志** > **扫描操作日志**
- **客户端** > **客户端管理**并单击**日志** > **扫描操作日志**

扫描操作日志显示以下信息：

- 防毒墙网络版开始扫描的日期和时间
- 防毒墙网络版停止扫描的日期和时间
- 扫描状态
  - **已完成**：扫描已正常完成。
  - **已中断**：用户在扫描完成之前将其停止。
  - **意外停止**：扫描被用户、系统或意外事件中断。例如，防毒墙网络版实时扫描服务可能已意外终止，或用户强制重新启动了客户端。
- 扫描类型
- 已扫描对象数
- 检测出的病毒/恶意软件感染数

- 检测出的间谍软件/灰色软件总数
- 云安全客户端病毒码版本
- 病毒码版本
- 间谍软件特征码版本

安全风险爆发

当特定时间段检测到的病毒/恶意软件、间谍软件/灰色软件和共享文件夹会话超出某一阈值时，即发生安全风险爆发。在网络中响应和抑制爆发有几种方法，其中包括：

- 允许防毒墙网络版监控网络上是否有可疑活动
- 封闭关键客户端终端端口和文件夹
- 向客户端发送爆发警报消息
- 清理受感染终端

安全风险爆发条件和通知

将防毒墙网络版配置为在发生下列事件时向您和其他防毒墙网络版管理员发送通知：

表 7-29. 安全风险爆发通知的类型

类型	参考
• 病毒/恶意软件 • 间谍软件/灰色软件 • 共享文件夹会话	配置安全风险爆发条件和通知 第 7-95 页
防火墙违例	配置防火墙违例爆发条件和通知 第 12-28 页

类型	参考
C&C 回呼	配置 C&C 回呼爆发条件和通知 第 11-21 页

- 病毒/恶意软件爆发
- 间谍软件/灰色软件爆发
- 防火墙违例爆发
- 共享文件夹会话爆发

按照检测次数和检测期限定义爆发。在超过检测期限内的检测次数时，将触发爆发。

防毒墙网络版附带有一组缺省通知消息，用于通知您和其他防毒墙网络版管理员发生爆发。您可以根据需要修改通知和配置其他通知设置。

注意

防毒墙网络版可以通过电子邮件、SNMP 陷阱和 Windows NT 事件日志发送安全风险爆发通知。对于共享文件夹会话爆发，防毒墙网络版通过电子邮件发送通知。配置防毒墙网络版何时通过这些通道发送通知的设置。有关详细信息，请参阅管理员通知设置 第 13-32 页。

配置安全风险爆发条件和通知

过程

1. 转至**管理** > **通知** > **爆发**。
2. 在**条件**选项卡中：
   a. 转至**病毒/恶意软件**和**间谍软件/灰色软件**部分。
   b. 指定唯一检测源的数量。
   c. 指定每个安全风险的检测次数和检测期限。

提示

趋势科技建议接受此窗口中的缺省值。

防毒墙网络版会在 10 个不同类型的病毒/恶意软件检测在 5 小时内报告的安全风险总数达到 101 时发送通知。如果一个客户端在 5 小时内报告了 101 个任意类型的病毒/恶意软件检测，防毒墙网络版也会发送爆发通知。

3. 在**条件**选项卡中：

   a. 转至**共享文件夹会话**部分。

   b. 选择**监控网络上的共享文件夹会话**。

   c. 在**记录的共享文件夹会话**中，单击数字链接以查看含有共享文件夹的终端和访问共享文件夹的终端。

   d. 指定共享文件夹会话数和检测期限。

   防毒墙网络版将在超出指定的共享文件夹会话数时发送一个通知消息。

4. 在**电子邮件**选项卡中：

   a. 转至**病毒/恶意软件爆发**、**间谍软件/灰色软件爆发**和**共享文件夹会话爆发**部分。

   b. 选择**启用电子邮件通知**。

   c. 指定电子邮件收件人。

   d. 接受或修改缺省的电子邮件主题和消息。可以使用标记变量表示**主题**和**消息**文本框中的数据。

表 7-30. 安全风险爆发通知的标记变量

变量	描述
病毒/恶意软件爆发	
%CV	检测出的病毒/恶意软件的总数
%CC	感染了病毒/恶意软件的终端总数
间谍软件/灰色软件爆发	

变量	描述
%CV	检测出的间谍软件/灰色软件的总数
%CC	感染了间谍软件/灰色软件的终端总数
共享文件夹会话爆发	
%S	共享文件夹会话数
%T	共享文件夹会话的累计时长
%M	时间段，单位为分钟

e. 选择要包括在电子邮件中的其他病毒/恶意软件和间谍软件/灰色软件信息。可以包括客户端/域名称、安全风险名称、检测的日期和时间、路径和受感染文件以及扫描结果。

f. 接受或修改缺省通知消息。

5. 在 **SNMP 陷阱**选项卡中：

a. 转至**病毒/恶意软件爆发**和**间谍软件/灰色软件爆发**部分。

b. 选择**启用 SNMP 陷阱通知**。

c. 接受或修改缺省消息。可以使用标记变量表示**消息**文本框中的数据。请参阅表 7-30：安全风险爆发通知的标记变量 第 7-96 页以了解详细信息。

6. 在 **NT 事件日志**选项卡中：

a. 转至**病毒/恶意软件爆发**和**间谍软件/灰色软件爆发**部分。

b. 选择**启用 NT 事件日志通知**。

c. 接受或修改缺省消息。可以使用标记变量表示**消息**文本框中的数据。请参阅表 7-30：安全风险爆发通知的标记变量 第 7-96 页以了解详细信息。

7. 单击**保存**。

配置安全风险爆发阻止

发生爆发时，执行爆发阻止措施以响应和抑制爆发。配置阻止设置时需小心谨慎，因为不正确的配置可能导致不可预见的网络问题。

过程

1. 转至**客户端** > **爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**启动爆发阻止**。
4. 单击以下任一爆发阻止策略，然后配置该策略的设置：
   - 限制/拒绝访问共享文件夹 第 7-99 页
   - 封闭易受攻击的端口 第 7-100 页
   - 拒绝对文件和文件夹的写访问 第 7-102 页
   - 拒绝访问压缩可执行文件 第 7-104 页
   - 在恶意软件进程/文件上创建互相排斥处理 第 7-103 页
5. 选择要执行的策略。
6. 选择爆发阻止保持有效的小时数。缺省值为 48 小时。可以在爆发阻止到期前手动恢复网络设置。

   警告!

   不要允许爆发阻止无限期有效。要无限期阻止或拒绝对特定文件、文件夹或端口的访问，请直接修改终端和网络设置，而不要使用防毒墙网络版来处理。

7. 接受或修改缺省客户端通知消息。

注意

要配置防毒墙网络版以便使其在发生爆发时通知您，请转至**管理** > **通知** > **爆发**。

8. 单击**启动爆发阻止**。

   所选的爆发阻止措施将显示在一个新窗口中。

9. 返回到“爆发阻止”客户端树中，选中**爆发阻止**列。

   应用爆发阻止措施的终端上将显示一个复选标记。

防毒墙网络版在系统事件日志中记录以下事件：

- 服务器事件（启动爆发阻止及通知客户端启用爆发阻止）
- 防毒墙网络版客户端事件（启用爆发阻止）

爆发阻止策略

发生爆发时，执行以下任一策略：

- 限制/拒绝访问共享文件夹 第 7-99 页
- 封闭易受攻击的端口 第 7-100 页
- 拒绝对文件和文件夹的写访问 第 7-102 页
- 拒绝访问压缩可执行文件 第 7-104 页
- 在恶意软件进程/文件上创建互相排斥处理 第 7-103 页

限制/拒绝访问共享文件夹

在爆发期间，限制或拒绝对网络上共享文件夹的访问，以阻止安全风险通过共享文件夹传播。

此策略生效时，用户仍然可以共享文件夹，但是此策略将不会应用于新共享的文件夹。因此，通知用户不要在爆发期间共享文件夹，或者再次部署策略以便将策略应用于新共享的文件夹。

过程

1. 转至**客户端** > **爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**启动爆发阻止**。
4. 单击**限制/拒绝访问共享文件夹**。
5. 从以下选项中选择：
   - **只读访问权限**：限制访问共享文件夹
   - **拒绝完全访问**

   注意

   只读访问设置不会应用至已经配置为拒绝完全访问的共享文件夹。
6. 单击**保存**。

   将再次显示**爆发阻止设置**窗口。
7. 单击**启动爆发阻止**。

   所选的爆发阻止措施将显示在一个新窗口中。

封闭易受攻击的端口

在爆发期间，封闭易受攻击的端口，病毒/恶意软件可能使用这些端口来获取防毒墙网络版客户端计算机的访问权限。

警告!

仔细配置爆发阻止设置。封闭使用中的端口会导致基于这些端口的网络服务不可用。例如，如果封闭可信端口，防毒墙网络版将无法在爆发期间与客户端通信。

过程

1. 转至**客户端 > 爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**启动爆发阻止**。
4. 单击**封闭端口**。
5. 选择是否**封闭可信端口**。
6. 在**已封闭端口**列下选择要封闭的端口。
   a. 如果表中没有端口，则单击**添加**。在打开的窗口中，选择要封闭的端口，然后单击**保存**。
      - **所有端口（包括 ICMP）**：封闭除可信端口之外的所有端口。如果还想封闭可信端口，则选中上一窗口中的“封闭可信端口”复选框。
      - **常用端口**：至少选择一个端口号，以便防毒墙网络版可以保存端口封闭设置。
      - **特洛伊木马端口**：封闭特洛伊木马程序常用的端口。请参阅特洛伊木马端口 第 E-12 页以了解详细信息。
      - **端口号或端口范围**：可根据需要指定要阻止的网络通信方向和一些注释，例如，封闭指定端口的原因。
      - **Ping 协议（拒绝 ICMP）**：如果只想阻止 ICMP 数据包（例如，ping 请求），则单击。
   b. 要编辑已封闭端口的设置，请单击端口号。
   c. 在打开的窗口中，修改设置，然后单击**保存**。

d. 要从列表中移除端口，请选中端口号旁的复选框，然后单击**删除**。

7. 单击**保存**。

   将再次显示**爆发阻止设置**窗口。

8. 单击**启动爆发阻止**。

   所选的爆发阻止措施将显示在一个新窗口中。

拒绝对文件和文件夹的写访问

病毒/恶意软件可能会修改或删除宿主终端上的文件和文件夹。在爆发期间，配置防毒墙网络版，使其阻止病毒/恶意软件修改或删除防毒墙网络版客户端终端上的文件和文件夹。

警告!

防毒墙网络版不支持拒绝写访问映射网络驱动器。

过程

1. 转至**客户端** > **爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**启动爆发阻止**。
4. 单击**拒绝对文件和文件夹的写访问**。
5. 键入目录路径。键入要保护的目录路径后，单击**添加**。

   注意

   键入目录的绝对路径，而不是虚拟路径。

6. 指定要在受保护的目录中保护的文件。选择所有文件，或根据特定文件扩展名选择文件。对于文件扩展名，可以指定不在列表中的扩展名，在文本框中键入该扩展名，然后单击**添加**。

7. 要保护特定文件，在**要保护的文件**下，键入完整文件名，然后单击**添加**。
8. 单击**保存**。

   将再次显示**爆发阻止设置**窗口。
9. 单击**启动爆发阻止**。

   所选的爆发阻止措施将显示在一个新窗口中。

在恶意软件进程/文件上创建互相排斥处理

您可以通过覆盖威胁在系统中感染和传播所需的资源来配置爆发阻止以抵御利用互斥进程的安全威胁。爆发阻止在与已知恶意软件相关的文件和进程上创建互斥，阻止恶意软件访问这些资源。

提示

趋势科技建议维护这些互斥，直到可以实施该恶意软件威胁的解决方案。联系支持部门获取正确的互斥名称，以在爆发期间提供防护。

注意

互相排斥处理需要未授权更改阻止服务，且仅支持 32 位平台。

过程

1. 转至**客户端** > **爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**启动爆发阻止**。
4. 单击**在恶意软件进程/文件上创建互相排斥 (互斥) 处理**。
5. 在提供的文本框中键入要提供防护的互斥名称。

   使用 + 和 - 按钮从列表添加或移除互斥名称。

注意

爆发阻止最多可支持 6 个互斥威胁的互相排斥处理。

6. 单击**保存**。

   将再次显示**爆发阻止设置**窗口。

7. 单击**启动爆发阻止**。

   所选的爆发阻止措施将显示在一个新窗口中。

拒绝访问压缩可执行文件

在爆发期间，拒绝访问压缩可执行文件可阻止这些文件可能包含的安全风险在网络中传播。您可以选择允许访问由支持的可执行加壳程序创建的可信文件。

过程

1. 转至**客户端** > **爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**启动爆发阻止**。
4. 单击**拒绝访问压缩可执行文件**。
5. 从支持的可执行加壳程序列表中进行选择，然后单击**添加**以允许访问由这些加壳程序创建的可执行打包文件。

注意

您仅可允许使用由可执行加壳软件列表中的加壳程序创建的打包文件。爆发阻止拒绝访问所有其他的可执行打包文件格式。

6. 单击**保存**。

   将再次显示**爆发阻止设置**窗口。

7. 单击**启动爆发阻止**。

   所选的爆发阻止措施将显示在一个新窗口中。

禁用爆发阻止

确信已抑制爆发并且防毒墙网络版已清除或隔离所有受感染的文件时，通过禁用爆发阻止将网络设置恢复正常。

过程

1. 转至**客户端** > **爆发阻止**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**恢复设置**。
4. 要通知用户爆发已结束，请选择**恢复原始设置后通知用户**。
5. 接受或修改缺省客户端通知消息。
6. 单击**恢复设置**。

注意

如果未手动恢复网络设置，则防毒墙网络版将会在**爆发阻止设置**窗口上的 __ **小时后自动将网络设置恢复正常**中指定的小时数以后自动恢复这些设置。缺省设置为 48 小时。

防毒墙网络版在系统事件日志中记录以下事件：

- 服务器事件（启动爆发阻止及通知防毒墙网络版客户端启用爆发阻止）
- 防毒墙网络版客户端事件（启用爆发阻止）

7. 禁用爆发阻止后，请扫描联网终端上是否有安全风险以确保抑制了爆发。

第 8 章

使用行为监控

本章介绍如何使用行为监控功能保护计算机免受安全风险的危害。

主题包括：

- 行为监控 第 8-2 页
- 配置全局行为监控设置 第 8-7 页
- 行为监控权限 第 8-10 页
- 针对防毒墙网络版客户端用户的行为监控通知 第 8-11 页
- 行为监控日志 第 8-13 页

行为监控

行为监控会不断地监控终端上的操作系统或已安装软件是否发生了异常修改。行为监控通过**恶意软件行为阻止**和**事件监控**来保护终端。用户配置的**例外列表**和**安全软件认证服务**是对这两种功能的完善。

重要信息

- 行为监控不支持 Windows XP 或 Windows 2003 64 位平台。
- 行为监控支持带 SP1 或更高版本的 Windows Vista 64 位平台。
- 缺省情况下，行为监控在所有版本的 Windows Server 2003、Windows Server 2008 和 Windows Server 2012 上是禁用的。在这些服务器平台上启用行为监控之前，请先阅读防毒墙网络版客户端服务 第 14-6 页中所列的指导方针和最佳做法。

恶意软件行为阻止

恶意软件行为阻止提供了一个必需的额外威胁保护层以防御存在恶意行为的程序。它会观察一段时间内的系统事件。当程序执行不同的操作组合或操作序列时，恶意软件行为阻止将检测已知的恶意行为并阻止关联的程序。使用此功能可确保在较高级别上抵御新的、未知的、突发的威胁。

恶意软件行为监控提供以下威胁级的扫描选项：

- **已知威胁**：阻止与已知恶意软件威胁相关联的行为
- **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

如果阻止了某个程序且启用了通知，防毒墙网络版会在防毒墙网络版客户端终端上显示通知。有关通知的详细信息，请参阅针对防毒墙网络版客户端用户的行为监控通知 第 8-11 页。

勒索软件防护

勒索软件防护可防止“勒索软件”威胁对防毒墙网络版客户端上的文件进行未经授权的修改或加密。勒索软件是一种恶意软件，它会限制文件的访问权限，并且要求付款才能恢复受影响的文件。

您可以配置行为监控，以检测可能表示勒索软件攻击的一系列特定事件。行为监控符合以下所有条件后，防毒墙网络版将终止并隔离违例程序：

1. 在特定的时间间隔内，未识别为尝试对三个文件进行安全修改、删除或更名的进程。
2. 尝试修改受保护的文件扩展名类型的进程

警告!

防毒墙网络版无法恢复受勒索软件进程影响的第一个文件。

注意

为了减少防毒墙网络版将安全进程检测为恶意进程的可能性，请确保防毒墙网络版客户端可以访问 Internet，以便使用趋势科技服务器执行其他验证进程。

事件监控

事件监控提供了一种更为常规的方法来抵御未授权软件和恶意软件攻击。它监控系统区域中的某些事件，并允许管理员调整触发此类事件的程序。如果您的特定系统保护要求高于恶意软件行为阻止提供的要求，请使用事件监控。

下表提供了一列受监控的系统事件。

表 8-1. 监控的系统事件

事件	描述
重复的系统文件	许多恶意程序会以 Windows 系统文件使用的名称创建它们自身或其他恶意程序的副本。其目的通常是覆盖或替换系统文件，避开检测或阻挠用户删除恶意文件。

事件	描述
Hosts 文件修改	Hosts 文件用于将域名与 IP 地址匹配。许多恶意程序修改 Hosts 文件，以将 Web 浏览器重定向到受感染的、不存在的或假 Web 站点。
可疑行为	可疑行为是合法程序不常执行的特定操作或一系列操作。使用表现出可疑行为的程序时应小心谨慎。
新的 Internet Explorer 插件	间谍软件/灰色软件程序通常会安装用户不需要的 Internet Explorer 插件，其中包括工具栏和浏览器帮助程序对象。
Internet Explorer 设置修改	许多病毒/恶意软件更改 Internet Explorer 设置，包括主页、受信任的 Web 站点、代理服务器设置和菜单扩展。
安全策略修改	修改 Windows 安全策略会允许不需要的应用程序运行并更改系统设置。
程序库注入	许多恶意程序会对 Windows 进行配置，以便所有的应用程序自动加载程序库 (DLL)。这会在每次应用程序启动时允许 DLL 中的恶意例程运行。
Shell 修改	许多恶意程序都会对 Windows shell 设置进行修改，以将其自身与某些文件类型关联。如果用户在 Windows 资源管理器中打开关联的文件，此例程将会允许恶意程序自动启动。对 Windows shell 设置的更改还会允许恶意程序跟踪使用过的程序，并随合法的应用程序一同启动。
新服务	Windows 服务是具有特殊功能的进程，通常在后台以完全的管理权限持续运行。恶意程序有时会将其自身作为服务进行安装，以便处于隐藏状态。
系统文件修改	有些 Windows 系统文件可确定系统的行为，包括启动程序和窗口保护程序设置。许多恶意程序都会修改系统文件，以在启动时自动启动自身，并控制系统行为。
防火墙策略修改	Windows 防火墙策略可确定有权访问网络的应用程序、为通信打开的端口和与计算机进行通信的 IP 地址。许多恶意程序都会更改此策略，以允许它们自身访问网络和 Internet。
系统进程修改	许多恶意程序会在内置 Windows 进程中执行各种操作。这些操作可能包括终止或修改运行中的进程。
新的启动程序	恶意应用程序通常会在 Windows 注册表中添加或修改自启动条目，以在每次计算机启动时自动启动。

当事件监控检测到监控的系统事件时，它将执行针对此事件所配置的处理措施。

下表列出了管理员对受监控的系统事件可能采取的处理措施。

表 8-2. 监控的系统事件的处理措施

处理措施	描述
访问	防毒墙网络版 始终允许与事件相关联的程序，但会在日志中记录此处理措施以进行评估。 这是对所有监控的系统事件的缺省处理措施。 **注意** 64 位系统上的程序库注入不支持该选项。
允许	防毒墙网络版 始终允许与事件相关联的程序。
必要时询问	防毒墙网络版 提示用户允许或拒绝与事件相关联的程序并将相应程序添加到例外列表 如果用户在特定的时间段内未响应，防毒墙网络版 将自动允许此程序运行。缺省时间段为 30 秒。 要修改该时间段，请参阅配置全局行为监控设置 第 8-7 页。 **注意** 64 位系统上的程序库注入不支持该选项。
拒绝	防毒墙网络版 始终阻止与事件相关联的程序，并会在日志中记录此处理措施。 如果阻止了某个程序且启用了通知，防毒墙网络版 会在防毒墙网络版计算机上显示通知。 有关通知的详细信息，请参阅针对防毒墙网络版客户端用户的行为监控通知 第 8-11 页。

行为监控例外列表

行为监控例外列表包含不受行为监控所监控的程序。

- **允许的程序**：此列表中的程序可以运行。对于允许的程序，在最终允许其运行之前，其他防毒墙网络版功能（如基于文件的扫描）仍会对其进行检查。
- **阻止的程序**：此列表中的程序永远无法启动。要配置此列表，应启用事件监控。

从 Web 控制台配置例外列表。您也可以授予用户从防毒墙网络版客户端控制台配置他们各自的例外列表的权限。有关详细信息，请参阅行为监控权限 第 8-10 页。

配置恶意软件行为阻止、事件监控和例外列表

过程

1. 转至**客户端 > 客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置 > 行为监控设置**。
4. 启用恶意软件行为阻止：
   a. 选择**为已知的潜在威胁启用恶意软件行为阻止**，然后选择以下选项之一：
      - **已知威胁**：阻止与已知恶意软件威胁相关联的行为
      - **已知的潜在威胁**：阻止与已知威胁相关联的行为并对潜在恶意行为采取处理措施
   b. 选择要启用的勒索软件防护功能，以抵御勒索软件威胁。
      - **保护文档，使其免遭未授权的加密或修改**：阻止潜在的勒索软件威胁，防止其加密或修改文档内容
      - **阻止通常与勒索软件相关的进程**：阻止与已知勒索软件威胁相关的进程，防止其加密或修改文档

      有关详细信息，请参阅勒索软件防护 第 8-3 页。

5. 配置事件监控设置。

   a. 选择**启用事件监控**。

   b. 选择要监控的系统事件，并为每个所选事件选择一项处理措施。

      有关监控的系统事件和处理措施的信息，请参阅事件监控 第 8-3 页。

6. 配置例外列表。

   a. 在**键入完整的程序路径**下，键入要允许或阻止的程序的完整路径。使用半角分号 (;) 分隔多个条目。

   b. 单击**添加到允许列表**或**添加到阻止列表**。

   c. 要从列表中移除阻止的或允许的程序，请单击程序旁边的垃圾桶图标 ()。

   注意

   防毒墙网络版最多可接受 100 个允许的程序和 100 个阻止的程序。

7. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

配置全局行为监控设置

防毒墙网络版可将全局客户端设置应用于所有客户端，或者只应用于具有特定权限的客户端。

过程

1. 转至**客户端** > **全局客户端设置**。
2. 转至**行为监控设置**部分。
3. 根据需要配置以下设置：

选项	描述
如果用户在 __ 秒内未响应，则自动允许程序	仅当事件监控已启用，并且监控的系统事件的处理措施是“必要时询问”时，此设置才起作用。此处理措施提示用户允许或拒绝与事件关联的程序。如果用户在特定的时间段内未响应，防毒墙网络版将自动允许此程序运行。有关详细信息，请参阅事件监控 第 8-3 页。
在对通过 HTTP 或电子邮件应用程序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)	行为监控与 Web 信誉服务结合使用，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。检测到一个“最近遇到的”文件后，管理员可以选择在执行文件之前提醒用户。根据云安全智能防护网络确定的文件检测次数和文件的存在时间，趋势科技可确定是否将程序归类为最近遇到的程序。 行为监控扫描每个通道的以下文件类型： • HTTP：扫描 .exe 文件。 • 电子邮件应用程序：扫描 .exe 以及未加密的 .zip 和 .rar 文件中的已压缩 .exe 文件。 **注意** • 管理员必须在客户端上启用 Web 信誉服务，以允许防毒墙网络版能够在显示该提示前扫描 HTTP 通信。 • 对于 Windows 10/7/Vista/XP 系统，此提示仅支持端口 80、81 和 8080。 • 防毒墙网络版与在执行过程中通过电子邮件应用程序下载的文件名匹配。如果文件名已更改，则用户不会收到提示。

4. 转到**安全软件认证服务设置**部分，然后根据需要启用安全软件认证服务。

安全软件认证服务会查询趋势科技数据中心，以验证由恶意软件行为阻止、事件监控、防火墙或防病毒扫描检测到的程序的安全性。启用安全软件认证服务可降低误判检测的可能性。



注意

请先确保防毒墙网络版客户端的代理服务器设置正确（有关详细信息，请参阅防毒墙网络版客户端代理服务器设置 第 14-44 页），然后再启用安全软件认证服务。不正确的代理服务器设置和不稳定的 Internet 连接都会导致从趋势科技数据中心接收响应延迟或不成功，从而导致受监控程序看上去处于无响应状态。

另外，纯 IPv6 防毒墙网络版客户端无法直接从趋势科技数据中心进行查询。为允许防毒墙网络版客户端连接到趋势科技数据中心，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

5. 单击**保存**。

行为监控权限

如果客户端拥有行为监控权限，防毒墙网络版客户端控制台上的**设置**窗口中将显示“行为监控”选项。然后，用户可以管理他们各自的例外列表。



图 8-1. 防毒墙网络版客户端控制台上的“行为监控”选项

授予行为监控权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转至**行为监控权限**部分。
5. 选择**在防毒墙网络版客户端控制台上显示“行为监控”设置**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

针对防毒墙网络版客户端用户的行为监控通知

防毒墙网络版可以在行为监控阻止程序后，立即在防毒墙网络版客户端计算机上显示一条通知消息。请启用通知消息发送，然后便可根据需要修改消息的内容。

启用通知消息发送

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡，并转至**行为监控设置**部分。
5. 选择**阻止程序时显示通知**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改通知消息的内容

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择**行为监控策略违例**。
3. 在提供的文本框中修改缺省消息。
4. 单击**保存**。

行为监控日志

防毒墙网络版客户端记录未授权的程序访问实例，并将日志发送到服务器。持续运行的防毒墙网络版客户端聚集日志，并按指定的时间间隔（缺省情况下为每 60 分钟一次）发送日志。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看行为监控日志

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **行为监控日志**或**查看日志** > **行为监控日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 查看日志。日志包含以下信息：
   - 检测到未授权进程的日期/时间
   - 在其中检测到未授权进程的终端
   - 终端的域
   - 违例，即进程违反的事件监控规则
   - 检测到违例时执行的操作
   - 事件，即程序访问的对象的类型
   - 未授权程序的风险等级
   - 程序，即未授权程序

- 操作，即未授权程序执行的操作
- 目标，即访问的进程

6. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

配置行为监控日志发送时间表

过程

1. 访问 <服务器安装文件夹>\PCCSRV。
2. 使用文本编辑器（如记事本）打开 ofcscan.ini 文件。
3. 搜索 "SendBMLogPeriod" 字符串，然后查看它旁边的值。

   缺省值为 3600 秒，且该字符串显示为 SendBMLogPeriod=3600。
4. 指定该值，以秒为单位。

   例如，要将日志周期更改为 2 小时，请将该值更改为 7200。
5. 保存文件。
6. 转至**客户端** > **全局客户端设置**。
7. 单击**保存**，无需更改任何设置。
8. 重新启动客户端。

第 9 章

使用设备控制

本章介绍如何使用设备控制功能保护计算机免受安全风险的危害。

主题包括：

- 设备控制 第 9-2 页
- 存储设备的权限 第 9-4 页
- 非存储设备的权限 第 9-9 页
- 修改设备控制通知 第 9-16 页
- 设备控制日志 第 9-16 页

设备控制

设备控制能够控制对连接到计算机的外部存储设备与网络资源的访问。设备控制有助于防止数据丢失和泄露，与文件扫描组合使用时可帮助防御安全风险。

您可以为内部和外部客户端配置设备控制策略。防毒墙网络版 管理员通常会对外部客户端配置更严格的策略。

策略是防毒墙网络版客户端树中的粒度设置。您可对客户端组或各个客户端强制执行特定策略。也可对所有客户端强制执行一个策略。

部署策略之后，客户端会使用您在**计算机位置**窗口（请参阅终端位置 第 14-2 页）中已设置的位置条件来确定其位置和要应用的策略。客户端会在每次位置更改时切换策略。

重要信息

- 缺省情况下，设备控制在所有版本的 Windows Server 2003、Windows Server 2008 和 Windows Server 2012 上是禁用的。在这些服务器平台上启用设备控制之前，请先阅读防毒墙网络版客户端服务 第 14-6 页中所列的指导方针和最佳做法。
- 有关支持的设备型号的列表，请参阅“数据保护列表”文档，网址为：

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

防毒墙网络版可监控的设备类型取决于是否已激活数据保护使用授权。数据保护模块是另行授权的，必须先激活此模块才能使用它。有关数据保护使用授权的详细信息，请参阅数据保护使用授权 第 3-3 页。

表 9-1. 由未授权更改阻止服务监控的设备

设备类型	设备描述
存储设备	CD/DVD **重要信息** 设备控制只能限制对使用实时文件系统格式的 CD/DVD 录制设备的访问。即使启用了设备控制，部分使用母版格式的第三方应用程序也能执行读/写操作。可以通过数据丢失防护限制对使用任何格式类型的 CD/DVD 录制设备的访问。 有关详细信息，请参阅阻止访问数据记录器 (CD/DVD) 第 10-31 页。
	软盘
	网络驱动器
	USB 存储设备

表 9-2. 由数据丢失防护监控的设备

设备类型	设备描述
移动设备	移动设备
存储设备	CD/DVD
	软盘
	网络驱动器
	USB 存储设备

设备类型	设备描述
非存储设备	Bluetooth 无线收发器
	COM 和 LPT 端口
	IEEE 1394 接口
	图像处理设备
	红外设备
	调制解调器
	PCMCIA 卡
	打印屏幕键
	无线 NIC

存储设备的权限

当您执行下列操作时会使用存储设备的设备控制权限：

- 允许访问 USB 存储设备、CD/DVD、软盘和网络驱动器。您可以授予对这些设备的完全访问权限，或限制访问级别。
- 配置允许的 USB 存储设备的列表。设备控制可让您阻止对所有 USB 存储设备的访问，但对于已添加至允许设备列表的设备除外。您可以授予对这些允许设备的完全访问权限，或限制访问级别。

下表列出了存储设备的权限。

表 9-3. 存储设备的设备控制权限

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。

权限	设备上的文件	传入文件
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
仅列出设备内容	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
阻止 （安装数据保护后可用）	禁止的操作：所有操作 设备及其包含的文件对用户不可见（例如，在 Windows 资源管理器中对用户不可见）。	禁止的操作：保存、移动、复制

防毒墙网络版中基于文件的扫描功能对设备权限起补充作用，并有可能覆盖这些设备权限。例如，如果权限允许打开某文件，但是防毒墙网络版检测到该文件感染了恶意软件，则将对该文件执行特定的扫描处理措施，以清除恶意软件。如果扫描处理措施是“清除”，则文件将在清除恶意软件后打开。但是，如果扫描处理措施是“删除”，该文件将会被删除。

提示

数据保护的设备控制支持所有 64 位平台。对于防毒墙网络版不支持的系统中的“未授权更改阻止”监控，将设备权限设置为**阻止**，以限制对这些设备的访问。

存储设备的高级权限

高级权限适用于对大多数存储设备授予的权限受限时。权限可能是以下任一项：

- 修改
- 读取和执行
- 读取
- 仅列出设备内容

您可以保持权限受限，但对存储设备和本地终端上的特定程序授予高级权限。

要定义程序，请配置以下程序列表。

表 9-4. 程序列表

程序列表	描述	有效输入
对设备具有读写访问权限的程序	此列表包含本地应用程序和存储设备上对设备具有读写访问权限的程序。 Microsoft Word (winword.exe) 就是一个本地程序，该程序通常位于 C:\Program Files\Microsoft Office\Office 中。如果 USB 存储设备的权限为“仅列出设备内容”，但 C:\\Program Files\\Microsoft Office\\Office\\winword.exe\ 包含在此列表中： • 用户将对从 Microsoft Word 访问的 USB 存储设备上的任何文件具有读写访问权限。 • 用户可以将 Microsoft Word 文件保存、移动或复制到 USB 存储设备。	程序路径和名称 有关详细信息，请参阅指定程序路径和名称 第 9-8 页。
设备上允许执行的程序	此列表包含存储设备上用户或系统可以执行的程序。 例如，如果要允许用户从 CD 安装软件，请将安装程序路径和名称（如 E:.exe）添加到此列表。	程序路径和名称或数字签名提供程序 有关详细信息，请参阅指定程序路径和名称 第 9-8 页或指定数字签名提供程序 第 9-8 页。

存在需要将程序同时添加到这两个列表的情况。考虑 USB 存储设备中的数据锁定功能（如果已启用），该功能在解锁设备之前提示用户输入有效用户名和密码。数据锁定功能使用设备上称为 “Password.exe ”的程序，必须允许执行该程

序用户才可以成功解锁设备。"Password.exe”还必须对设备具有读写访问权限，以便用户可以更改用户名或密码。

用户界面上的每个程序列表最多可以包含 100 个程序。

如果要将更多程序添加到程序列表，您需要将程序添加到 ofcscan.ini 文件（最多可容纳 1,000 个程序）。有关将程序添加到 ofcscan.ini 文件的说明，请参阅使用 ofcscan.ini 将程序添加到设备控制列表 第 9-14 页。



警告!

添加到 ofcscan.ini 文件的程序将被部署到根域且将覆盖各个域和客户端上的程序。

指定数字签名提供程序

如果您信任提供程序发布的程序，则指定数字签名提供程序。例如，键入 Microsoft Corporation 或 趋势科技, Inc.。通过检查程序属性（例如，右键单击程序并选择**属性**）可以获取数字签名提供程序。

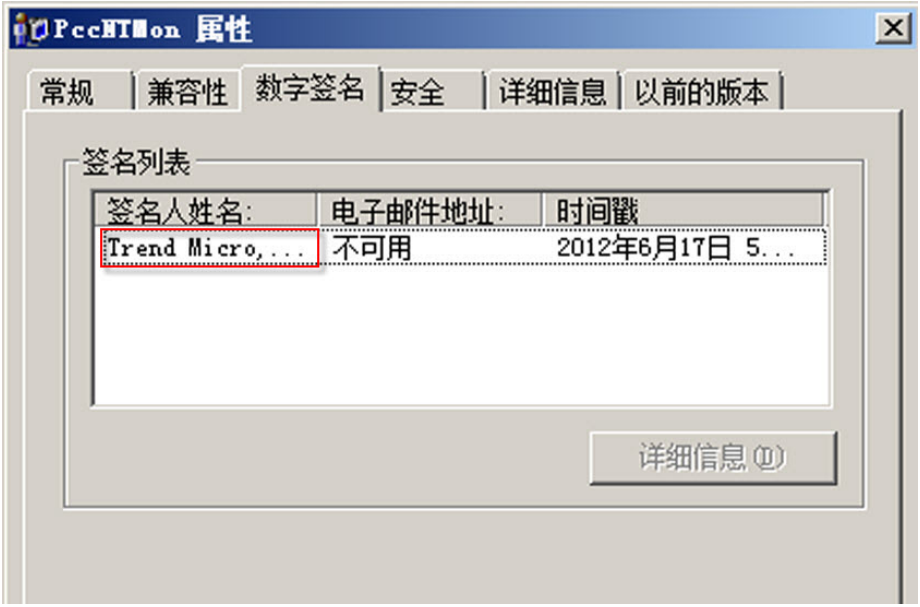


图 9-1. 防毒墙网络版客户端程序的数字签名提供程序 (PccNTMon.exe)

指定程序路径和名称

程序路径和名称最多具有 259 个字符，且必须只包含字母数字字符（A-Z、a-z、0-9）。不能仅指定程序名称。

您可以使用通配符来取代驱动器盘符和程序名称。使用问号 (?) 表示单个字符数据，如驱动器盘符。使用星号 (*) 表示多个字符数据，如程序名称。

注意

通配符不能用于表示文件夹名称。必须指定文件夹的准确名称。

在以下示例中通配符用法正确：

表 9-5. 通配符的正确用法

示例	匹配的数据
?:\Password.exe	位于任何驱动器根目录下的“Password.exe”文件
C:\Program Files\Microsoft *.exe	C:\Program Files 中带有文件扩展名的任意文件
C:\Program Files*.*	C:\Program Files 中带有文件扩展名的任意文件
C:\Program Files\a**?**c.exe	C:\Program Files 中带有 3 个字符（其中开头字母为“a”，结尾字母为“c”）的任何 .exe 文件
C:*	直接位于 C:\ 驱动器下带有或不带有文件扩展名的任意文件

在以下示例中通配符用法错误：

表 9-6. 通配符的错误用法

示例	原因
??:\Buffalo\Password.exe	?? 表示两个字符，但驱动器盘符只有一个字母字符。
*:\Buffalo\Password.exe	* 表示多字符数据，但驱动器盘符只有一个字母字符。
C:*\Password.exe	通配符不能用于表示文件夹名称。必须指定文件夹的准确名称。
C:**?**\Password.exe	

非存储设备的权限

您可以允许或阻止对非存储设备的访问。这些设备没有粒度或高级权限。

管理对外部设备的访问（数据保护已激活）

过程

1. 导航至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **设备控制设置**。
4. 单击**外部客户端**选项卡为外部客户端配置设置，或单击**内部客户端**选项卡为内部客户端配置设置。
5. 选择**启用设备控制**。
6. 如下所示应用设置：
   - 如果位于**外部客户端**选项卡中，则可以选择**将所有设置应用到内部客户端**以将设置应用到内部客户端。
   - 如果位于**内部客户端**选项卡中，则可以选择**将所有设置应用到外部客户端**以将设置应用到外部客户端。

   将显示确认消息。留出一些时间让部署命令传送到所有客户端。
7. 选择在 USB 存储设备上允许还是阻止自动运行功能 (autorun.inf)。
8. 配置存储设备的设置。
   a. 选择每个存储设备的权限。

      有关权限的详细信息，请参阅存储设备的权限 第 9-4 页。

   b. 如果 USB 存储设备的权限为**阻止**，请配置允许设备的列表。用户可以访问这些设备，您可以使用权限控制访问级别。

      请参阅配置 USB 设备的允许列表 第 9-12 页。
9. 对于每个非存储设备，选择**允许**或**阻止**。
10. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

- **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
- **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

配置高级权限

虽然您可以在用户界面上为特定存储设备配置高级权限和通知，但是权限和通知实际上应用于所有存储设备。这意味着单击 CD/DVD 的**高级权限和通知**时，实际上是定义所有存储设备的权限和通知。



注意

有关高级权限以及如何使用高级权限正确定义程序的详细信息，请参阅存储设备的高级权限 第 9-5 页。

过程

1. 单击**高级权限和通知**。

   此时打开一个新窗口。

2. 在**对存储设备具有读写访问权限的程序**下方，键入程序路径和文件名，然后单击**添加**。

   不接受数字签名提供程序。

3. 在**存储设备上允许执行的程序**下方，键入程序路径和名称或数字签名提供程序，然后单击**添加**。

4. 选择 **当防毒墙网络版检测到未授权的设备访问时，会在终端上显示通知消息**。

   - 未经授权的设备访问指的是禁止的设备操作。例如，如果设备权限为“读取”，用户将无法保存、移动、删除或执行设备上的文件。
   - 您可以修改通知消息。有关详细信息，请参阅修改设备控制通知 第 9-16 页。

5. 单击 **后退**。

配置 USB 设备的允许列表

USB 设备的允许列表支持使用星号 (*) 通配符。将任何文本框替换为星号 (*) 以包括满足其他文本框的所有设备。例如，[vendor]-[model]-* 会将指定供应商和指定型号类型的所有 USB 设备置于允许列表中，而不考虑序列号。

过程

1. 单击**允许的设备**。
2. 输入设备供应商。
3. 输入设备型号和序列号。

   提示

   可以使用设备列表工具查询连接至终端的设备。该工具可以提供每个设备的设备供应商、型号和序列号。

4. 选择设备的权限。

   有关权限的详细信息，请参阅存储设备的权限 第 9-4 页。

5. 要添加更多设备，请单击加号 (+) 图标。
6. 单击 **< 后退**。

设备列表工具

在每个终端上本地运行设备列表工具可查询连接到终端的外部设备。此工具会扫描终端是否连接外部设备，然后在浏览器窗口中显示设备信息。接着，您可以在配置数据丢失防护和设备控制的设备设置时使用这些信息。

运行设备列表工具

过程

1. 在防毒墙网络版服务器计算机上，转至 <服务器安装文件夹 第 xv 页> \PCCSRV\Admin\Utility\ListDeviceInfo。
2. 将 listDeviceInfo.exe 复制到目标终端。
3. 在终端上，运行 listDeviceInfo.exe。
4. 查看浏览器窗口中显示的设备信息。数据丢失防护和设备控制使用下列信息：
   - 供应商（必需）
   - 型号（可选）
   - 序列号（可选）

管理对外部设备的访问（数据保护未激活）

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **设备控制设置**。
4. 单击**外部客户端**选项卡为外部客户端配置设置，或单击**内部客户端**选项卡为内部客户端配置设置。
5. 选择**启用设备控制**。
6. 如下所示应用设置：

- 如果位于**外部客户端**选项卡中，则可以选择**将所有设置应用到内部客户端**以将设置应用到内部客户端。
- 如果位于**内部客户端**选项卡中，则可以选择**将所有设置应用到外部客户端**以将设置应用到外部客户端。

将显示确认消息。留出一些时间让部署命令传送到所有客户端。

7. 选择在 USB 存储设备上允许还是阻止自动运行功能 (autorun.inf)。
8. 选择每个存储设备的权限。
9. 如果存储设备权限为以下任意一项，则配置高级权限和通知：**修改**、**读取和执行**、**读取**或**仅列出设备内容**。

   请参阅配置高级权限 第 9-11 页。
10. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
    - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
    - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

使用 ofcscan.ini 将程序添加到设备控制列表

注意

有关程序列表以及如何正确定义可以添加到列表中的程序的详细信息，请参阅存储设备的高级权限 第 9-5 页。

过程

1. 在防毒墙网络版服务器计算机上，转至 <服务器安装文件夹>\PCCSRV。
2. 使用文本编辑器打开 ofcscan.ini 文件。
3. 添加对存储设备具有读写访问权限的程序：

a. 找到以下几行：

```
[DAC_APPROVED_LIST]
Count=x
```

b. 使用程序列表中的程序数替换“x”。

c. 在“Count=x”下，通过键入以下内容添加程序：

Item<**编号**>=<**程序路径和名称或数字签名提供程序**>

例如：

```
[DAC_APPROVED_LIST]
Count=3
Item0=C:\Program Files\program.exe
Item1=?:\password.exe
Item2=Microsoft Corporation
```

4. 添加在存储设备上允许执行的程序：

a. 找到以下几行：

```
[DAC_EXECUTABLE_LIST]
Count=x
```

b. 使用程序列表中的程序数替换“x”。

c. 在“Count=x”下，通过键入以下内容添加程序：

Item<**编号**>=<**程序路径和名称或数字签名提供程序**>

例如：

```
[DAC_EXECUTABLE_LIST]
Count=3
Item0=?:\Installer\Setup.exe
Item1=E:\*.exe
```

```
Item2=Trend Micro, Inc.
```

5. 保存并关闭 ofcscan.ini 文件。
6. 打开防毒墙网络版 Web 控制台，转至**客户端** > **全局客户端设置**。
7. 单击**保存**将程序列表部署到所有客户端。

修改设备控制通知

发生设备控制违例时，终端上会显示通知消息。如果需要，管理员可以修改缺省通知消息。

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择**设备控制违例**。
3. 在提供的文本框中修改缺省消息。
4. 单击**保存**。

设备控制日志

防毒墙网络版客户端记录未授权的设备访问实例，并将日志发送到服务器。持续运行的任何客户端聚集日志，并在 1 小时后发送这些日志。重新启动的任何客户端检查上次向服务器发送日志的时间。如果经过的时间超过 1 个小时，则客户端会立即发送日志。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看设备控制日志

注意

仅尝试访问**存储设备**生成的日志数据。防毒墙网络版客户端阻止或允许对配置的**非存储设备**的访问，但不记录处理措施。

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **设备控制日志**或**查看日志** > **设备控制日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 查看日志。日志包含以下信息：
   - 检测到未授权访问的日期/时间
   - 连接外部设备或映射网络资源的终端
   - 连接外部设备或映射网络资源的终端域
   - 访问的设备类型或网络资源
   - 目标，即访问的设备或网络资源中的项
   - 访问者，它指定发起访问的位置
   - 对目标设置的权限
6. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

第 10 章

使用数据丢失防护

本章讨论如何使用数据丢失防护功能。

主题包括：

- 关于数据丢失防护 (DLP) 第 10-2 页
- 数据丢失防护策略 第 10-3 页
- 数据标识符类型 第 10-4 页
- 数据丢失防护模板 第 10-18 页
- DLP 通道 第 10-22 页
- 数据丢失防护措施 第 10-35 页
- 数据丢失防护例外 第 10-38 页
- 数据丢失防护策略配置 第 10-43 页
- 数据丢失防护通知 第 10-48 页
- 数据丢失防护日志 第 10-52 页

关于数据丢失防护 (DLP)

传统的安全解决方案着重于防止外部安全威胁入侵网络。在当今的安全环境中，情况并非完全如此。数据外泄现在已司空见惯，将组织的机密和敏感数据（指的是数字资产）暴露给外部的非授权团体。数据外泄可能是因为内部员工出错或大意、数据外包、计算设备遭窃或放置不当或恶意攻击所造成的。

数据外泄会导致：

- 品牌信誉受损
- 客户对公司的信任度降低
- 为了进行补救措施而投入不必要的成本，以及因不遵守法规而需支付罚金
- 因知识产权被盗，错失商机和收益

随着数据外泄情况越来越普遍以及因此而带来的损害，许多公司现在都将数字资产保护视为安全措施的关键要素。

数据丢失防护可保护组织的敏感数据免遭意外或故意泄露。数据丢失防护允许您：

- 使用数据标识符标识需要保护的敏感信息。
- 创建用于限制或阻止通过常用传输通道（如电子邮件和外部设备）传输数字资产的策略
- 按照已建立的隐私标准强制执行合规

您必须首先回答以下问题，然后才能监控敏感信息以避免潜在丢失：

- 哪些数据需要保护，以使未经授权的用户无法访问？
- 敏感数据位于何处？
- 如何传送敏感数据？
- 哪些用户已被授权访问或传输敏感数据？
- 如果发生安全违例，应采取哪种处理措施？

此重要审核通常涉及熟悉组织中敏感信息的多个部门和人员。

如果您已定义敏感信息和安全策略，则可以开始定义数据标识符和公司策略。

数据丢失防护策略

防毒墙网络版会根据 DLP 策略中定义的规则集来评估文件或数据。策略确定哪些文件或数据需要受到保护以使其免遭未授权传输，以及防毒墙网络版检测到这种传输后所采取的措施。



注意

防毒墙网络版不监控服务器与防毒墙网络版客户端之间的数据传输。

防毒墙网络版允许管理员为内部和外部防毒墙网络版客户端配置策略。管理员通常会为外部客户端配置更为严格的策略。

管理员可对客户端组或各个客户端强制执行特定策略。

部署策略之后，客户端会使用在**终端位置**窗口（请参阅终端位置 第 14-2 页）中设置的位置条件来确定正确的位置设置和要应用的策略。客户端会在每次位置更改时切换策略。

策略配置

通过配置下列设置并将设置部署到选定客户端来定义 DLP 策略：

表 10-1. 定义 DLP 策略的设置

设置	描述
规则	DLP 规则可包含多个模板、通道和处理措施。每个规则是包含的 DLP 策略的子集。 **注意** 数据丢失防护按优先级处理规则和模板。如果规则设置为“不予处理”，数据丢失防护会处理列表中的下一个规则。如果规则设置为“阻止”或“用户原因”，数据丢失防护会阻止或接受用户处理措施，并且不会进一步处理该规则/模板。
模板	DLP 模板将数据标识符和逻辑运算符 (And、Or、Except) 结合使用以构成条件语句。只有满足特定条件语句的文件或数据才会受 DLP 规则的制约。 数据丢失防护附带一组预定义模板，而且允许管理员创建定制模板。 DLP 规则可包含一或多个模板。在检查模板时，数据丢失防护将使用第一个匹配规则。这意味着，如果文件或数据与一个模板中的数据标识符匹配，数据丢失防护将不再检查其他模板。
通道	通道是传输敏感信息的实体。数据丢失防护支持常见传输通道，如电子邮件、可移动存储设备和即时通讯应用程序。
处理措施	当数据丢失防护检测到尝试通过任一通道传输敏感信息的操作时，它会执行一种或多种处理措施。
例外	例外作为已配置 DLP 规则的覆盖。配置例外以管理不受监控的目标、受监控的目标和压缩文件扫描。
数据标识符	数据丢失防护使用数据标识符来识别敏感信息。数据标识符包含作为 DLP 模板构建块的表达式、文件属性和关键字。

数据标识符类型

数字资产是指企业必须对其加以保护以使其免遭未授权传输的文件和数据。管理员可以使用以下数据标识符定义数字资产：

- **表达式**：具有特定结构的数据。

  有关详细信息，请参阅表达式 第 10-5 页。

- **文件属性**：文件属性（如文件类型和文件大小）。

  有关详细信息，请参阅文件属性 第 10-10 页。

- **关键字列表**：特殊词或短语的列表。

  有关详细信息，请参阅关键字 第 10-12 页。

注意

管理员无法删除 DLP 模板使用的数据标识符。请先删除模板，然后再删除数据标识符。

表达式

表达式是具有特定结构的数据。例如，信用卡号通常有 16 位数字，而且其格式为 "nnnn-nnnn-nnnn-nnnn"，因此很适合通过表达式进行检测。

管理员可以使用预定义的表达式和定制的表达式。

有关详细信息，请参阅预定义的表达式 第 10-5 页和定制表达式 第 10-6 页。

预定义的表达式

数据丢失防护随附一组预定义的表达式。您无法修改或删除这些表达式。

数据丢失防护使用模式匹配和数学方程式验证这些表达式。数据丢失防护将可能的敏感数据与表达式匹配后，数据也可以进行其他验证检查。

有关预定义表达式的完整列表，请参阅“数据保护列表”文档，网址为 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

查看预定义表达式的设置

注意

您无法修改或删除预定义的表达式。

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。
2. 单击**表达式**选项卡。
3. 单击某个表达式名称。
4. 在打开的窗口中查看设置。

定制表达式

如果所有预定义表达式都不符合公司的要求，则可以创建定制表达式。

表达式是功能强大的字符串匹配工具。创建表达式之前，应熟悉表达式语法。设计不良的表达式会严重影响性能。

创建表达式时：

- 请参考预定义表达式，了解如何定义有效表达式的指导。例如，如果要创建包含日期的表达式，则可以参考前缀为“Date”的表达式。
- 请注意，数据丢失防护遵循 Perl Compatible Regular Expressions (PCRE) 中定义的表达式格式。有关 PCRE 的更多信息，请访问以下 Web 站点：

  http://www.pcre.org/
- 从简单表达式开始。如果表达式造成假警报，请予以修改；您也可以微调表达式以提高检测的准确性。

创建表达式时，有多种条件可供管理员选择。表达式必须符合选择的条件，数据丢失防护才能让它遵循 DLP 策略。有关不同条件选项的详细信息，请参阅定制表达式的条件 第 10-7 页。

定制表达式的条件

表 10-2. 定制表达式的条件选项

条件	规则	示例
无	无	所有 – 来自美国人口普查局的姓名 • 表达式：[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
特定字符	表达式必须包含您指定的字符。 此外，表达式中的字符数必须介于下限和上限之间。	美国 – ABA 路由号码 • 表达式：[^\d]([0123678]\d{8})[^\d] • 字符：0123456789 • 字符数下限：9 • 字符数上限：9
后缀	后缀是指表达式的最后部分。后缀必须包含您指定的字符并包含特定数量的字符。 此外，表达式中的字符数必须介于下限和上限之间。	所有 – 住宅地址 • 表达式：\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • 后缀字符：0123456789- • 字符数：5 • 表达式中的字符数下限：25 • 表达式中的字符数上限：80

条件	规则	示例
单字符分隔符	表达式必须包含两个部分，并用一个字符分隔。这个字符的长度必须是 1 个字节。 此外，分隔符左侧的字符数必须介于下限和上限之间。分隔符右侧的字符数不能超出上限。	所有 - 电子邮件地址 • 表达式：[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • 分隔符：@ • 左侧字符数下限：3 • 左侧字符数上限：15 • 右侧字符数上限：30

创建定制表达式

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。
2. 单击**表达式**选项卡。
3. 单击**添加**。

   将显示一个新窗口。
4. 键入表达式的名称。名称的长度不能超过 100 个字节，而且不能包含下列字符：

   • > < * ^ | & ? \ /
5. 键入长度不超过 256 个字节的描述。
6. 键入显示的数据。

   例如，如果要创建 ID 号的表达式，请键入示例 ID 号。此数据仅供参考，不会显示在产品的其他地方。
7. 选择下列条件之一，并为选择的条件配置其他设置（请参阅定制表达式的条件 第 10-7 页）：

- 无
- 特定字符
- 后缀
- 单字符分隔符

8. 针对实际数据测试表达式。

   例如，如果表达式用于表示国家 ID，请在**测试数据**文本框中键入有效的 ID 号，单击**测试**，然后检查结果。

9. 如果您对结果感到满意，则单击**保存**。



注意

仅当测试成功时才保存设置。检测不到任何数据的表达式会浪费系统资源，而且可能会影响性能。

10. 将显示一条消息，提醒您将设置部署到客户端。单击**关闭**。
11. 返回到 **DLP 数据标识符**窗口，单击**应用到全部客户端**。

导入定制表达式

如果您有包含表达式且格式正确的 .dat 文件，请使用此选项。您可以从当前正在访问的服务器或其他服务器导出表达式，以生成该文件。



注意

此数据丢失防护版本生成的 .dat 表达式文件与之前的版本不兼容。

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。
2. 单击**表达式**选项卡。
3. 单击**导入**，然后找到包含表达式的 .dat 文件。

4. 单击**打开**。

   将显示一条消息，通知您导入是否成功。如果要导入的表达式已存在，系统将跳过该表达式。

5. 单击**应用到全部客户端**。

文件属性

文件属性是文件的特定属性。定义数据标识符时，可以使用两个文件属性，即文件类型和文件大小。例如，某软件开发公司可能想只与研发部门（其成员负责开发和测试该软件）共享该公司的软件安装程序。在此情况下，防毒墙网络版管理员可以创建一个策略，阻止将大小为 10 到 40MB 的可执行文件传输到研发部门以外的所有部门。

对于敏感文件而言，单独使用文件属性不是很可靠。依然使用本主题中示例，最有可能阻止其他部门共享的第三方软件安装程序。因此，趋势科技建议将文件属性与其他 DLP 数据标识符结合使用，从而更有针对性地检测敏感文件。

有关支持的文件类型的完整列表，请参阅“数据保护列表”文档，网址为 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

预定义的文件属性列表

数据丢失防护随附预定义的文件属性列表。无法修改或删除该列表。该列表有自己的内置条件，用以确定模板是否应触发策略违例。

使用预定义的文件属性列表限制对数据记录器 (CD/DVD) 的访问。

有关详细信息，请参阅阻止访问数据记录器 (CD/DVD) 第 10-31 页。

创建文件属性列表

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。
2. 单击**文件属性**选项卡。
3. 单击**添加**。

   将显示一个新窗口。
4. 键入文件属性列表的名称。名称的长度不能超过 100 个字节，而且不能包含下列字符：

   - > < * ^ | & ? \ /
5. 键入长度不超过 256 个字节的描述。
6. 选择首选真实文件类型。
7. 如果要包含的文件类型未列出，请选择**文件扩展名**，然后键入文件类型的扩展名。数据丢失防护检查带有指定扩展名的文件，但不检查其真实文件类型。指定文件扩展名的准则：

   - 每个扩展名的开头必须是星号 (*)，接下来是英文句点 (.)，然后是扩展名。星号是通配符，表示文件的实际名称。例如，*.pol 与 12345.pol 和 test.pol 匹配。
   - 可以在扩展名中包含通配符。使用问号 (?) 表示单个字符；使用星号 (*) 表示两个或多个字符。请参阅以下示例：

     - *.*m 与以下文件匹配：ABC.dem、ABC.prm、ABC.sdcm

     - *.m*r 与以下文件匹配：ABC.mgdr、ABC.mtp2r、ABC.mdmr

     - *.fm? 与以下文件匹配：ABC.fme、ABC.fml、ABC.fmp
   - 请谨慎在扩展名的末尾添加星号，因为这可能会匹配部分文件名和不相关扩展名。例如：*.do* 与 abc.doctor_john.jpg 和 abc.donor12.pdf 匹配。
   - 使用半角分号 (;) 分隔文件扩展名。半角分号后面无需添加空格。

8. 键入最小文件大小和最大文件大小（以字节为单位）。这两个文件大小值必须是大于零的整数。
9. 单击**保存**。
10. 将显示一条消息，提醒您将设置部署到客户端。单击**关闭**。
11. 返回到 **DLP 数据标识符**窗口，单击**应用到全部客户端**。

导入文件属性列表

如果您有包含文件属性列表且格式正确的 .dat 文件，请使用此选项。您可以从当前正在访问的服务器或其他服务器导出文件属性列表，来生成该文件。

注意

此数据丢失防护版本生成的 .dat 属性文件与之前的版本不兼容。

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。
2. 单击**文件属性**选项卡。
3. 单击**导入**，然后找到包含文件属性列表的 .dat 文件。
4. 单击**打开**。

   将显示一条消息，通知您导入是否成功。如果要导入的文件属性列表已存在，系统将跳过该列表。
5. 单击**应用到全部客户端**。

关键字

关键字是特殊词或短语。可以将相关关键字添加到关键字列表，以识别特定类型的数据。例如，“预后”、“血型”、“接种”和“医师”是可能出现在诊

断书中的关键字。如果要防止传输诊断书文件，可以在 DLP 策略中使用这些关键字，然后将数据丢失防护配置为阻止包含这些关键字的文件。

可以将常用词结合在一起，以形成有意义的关键字。例如，您可以结合 "end"、"read"、"if" 和 "at"，以构成在源代码中找到的关键字（例如，"END-IF"、"END-READ" 和 "AT END"）。

可以使用预定义的关键字列表和定制的关键字列表。有关详细信息，请参阅预定义的关键字列表 第 10-13 页和定制的关键字列表 第 10-14 页。

预定义的关键字列表

数据丢失防护附带一组预定义的关键字列表。您无法修改或删除这些关键字列表。每个列表都有自己的内置条件，用以确定模板是否应触发策略违例。

有关数据丢失防护中预定义关键字列表的详细信息，请参阅“数据保护列表”文档，网址为 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

关键字列表的工作方式

关键字数量条件

每个关键字列表都包含一个条件，要求文档中存在一定数量的关键字，列表才会触发违例。

关键字数量条件包含以下值：

- **所有**：列表中的所有关键字都必须存在于文档中。
- **任何**：列表中的任一关键字必须存在于文档中。
- **特定数量**：文档中必须至少有指定数量的关键字。如果文档中关键字的数量超出指定数量，数据丢失防护将触发违例。

距离条件

有些列表中包含“距离”条件，用以确定是否有违例情况。“距离”指一个关键字的第一个字符与另一个关键字的第一个字符之间间隔的字符数。请考虑以下项：

First Name:_John_ **L**ast Name:_Smith_

表－名字、姓氏列表的“距离”条件为五十 (50)，并包含常用的表字段“名字”和“姓氏”。在上例中，由于“First Name”中的字符“F”与“Last Name”中的字符“L”之间的字符数等于十八 (18)，因此数据丢失防护将触发违例。

不触发违例的条目示例如下：

The **f**irst name of our new employee from Switzerland is John. His **l**ast name is Smith.

在本例中，“first name”中的字符“f”与“last name”中的字符“l”之间的字符数为六十一 (61)。该值超出了距离阈值，不触发违例。

定制的关键字列表

如果预定义的关键字列表都不符合您的要求，可以创建定制的关键字列表。

配置关键字列表时，有多种条件供您选择。关键字列表必须符合您选择的条件，数据丢失防护才能让它遵循策略。为每个关键字列表选择下列其中一个条件：

- **任何关键字**
- **所有关键字**
- **所有关键字不超过 <x> 个字符**
- **关键字的组合分值超过了阈值**

有关条件规则的详细信息，请参阅定制的关键字列表条件 第 10-15 页。

定制的关键字列表条件

表 10-3. 关键字列表的条件

条件	规则
任何关键字	文件至少必须包含关键字列表中的一个关键字。
所有关键字	文件必须包含关键字列表中的所有关键字。
所有关键字不超过 <x> 个字符	文件必须包含关键字列表中的所有关键字。此外，每个关键字对的字符数都必须算在各自的 <x> 个字符内。 例如，有 3 个关键字 WEB、DISK 和 USB，且指定的字符数为 20。 如果数据丢失防护按 DISK、WEB 和 USB 的顺序检测所有关键字，则从“D”（在 DISK 中）到“W”（在 WEB 中）和从“W”到“U”（在 USB 中）之间最多只能有 20 个字符。 以下数据符合该条件：DISK####WEB############USB 以下数据不符合该条件：DISK******************WEB****USB（在“D”和“W”之间有 23 个字符） 决定字符数时请记住，小数字（例如 10）的扫描时间通常比较短，但只涵盖相对小的区域。这可能会使得检测敏感数据的机率降低，特别是对于大型文件。当数字增加时，涵盖的区域也会增加，但是扫描时间会比较长。
关键字的组合分值超过了阈值	文件必须包含关键字列表中的一或多个关键字。如果只检测到一个关键字，其分值必须高于阈值。如果有多个关键字，其组合分值必须高于阈值。 请为每个关键字分配介于 1 到 10 之间的分值。高度机密的词或短语（例如，人力资源部门的“调薪”）应具有相对较高的分值。本身没有太高权重的字或短语可以具有较低的分值。 配置阈值时，请考虑为关键字分配的分值。例如，如果有五个关键字，而其中有三个关键字具有高优先级，则阈值可以等于或低于这三个高优先级关键字的组合分值。这表示检测到这三个关键字时就可以将该文件视为敏感文件。

创建关键字列表

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。
2. 单击**关键字**选项卡。
3. 单击**添加**。

   将显示一个新窗口。
4. 键入关键字列表的名称。名称的长度不能超过 100 个字节，而且不能包含下列字符：
   - > < * ^ | & ? \ /
5. 键入长度不超过 256 个字节的描述。
6. 选择下列条件之一，并为选择的条件配置其他设置：
   - **任何关键字**
   - **所有关键字**
   - **所有关键字不超过 <x> 个字符**
   - **关键字的组合分值超过了阈值**
7. 手动将关键字添加到列表中：
   a. 键入长度介于 3 到 40 个字节之间的关键字，并指定是否区分大小写。
   b. 单击**添加**。
8. 使用“导入”选项添加关键字：

注意

如果您有包含关键字且格式正确的 .csv 文件，请使用此选项。您可以从当前正在访问的服务器或其他服务器导出关键字来生成该文件。

a. 单击**导入**，然后找到包含关键字的 .csv 文件。

b. 单击**打开**。

将显示一条消息，通知您导入是否成功。如果要导入的关键字已存在于列表中，系统将跳过该关键字。

9. 要删除关键字，请选择关键字，然后单击**删除**。

10. 导出关键字：



注意

可以使用“导出”功能备份关键字，或将其导入到其他服务器。将导出关键字列表中的所有关键字。无法导出单个关键字。

a. 单击**导出**。

b. 将生成的 .csv 文件保存到首选位置。

11. 单击**保存**。

12. 将显示一条消息，提醒您将设置部署到客户端。单击**关闭**。

13. 返回到 **DLP 数据标识符**窗口，单击**应用到全部客户端**。

导入关键字列表

如果您有包含关键字列表且格式正确的 .dat 文件，请使用此选项。您可以从当前正在访问的服务器或其他服务器导出关键字列表来生成该文件。



注意

此版本数据丢失防护生成的 .dat 关键字列表文件与之前的版本不兼容。

过程

1. 转至**客户端** > **数据丢失防护** > **数据标识符**。

2. 单击**关键字**选项卡。
3. 单击**导入**，然后找到包含关键字列表的 .dat 文件。
4. 单击**打开**。

   将显示一条消息，通知您导入是否成功。如果要导入的关键字列表已存在，系统将跳过该列表。
5. 单击**应用到全部客户端**。

数据丢失防护模板

DLP 模板将 DLP 数据标识符和逻辑运算符 (And、Or、Except) 结合使用以构成条件语句。只有满足特定条件语句的文件或数据才会受 DLP 策略的制约。

例如，文件必须是 Microsoft Word 文件（文件属性）AND（且）必须包含特定法律术语（关键字）AND（且）必须包含 ID 号码（表达式），才能受到“雇佣合同”策略的制约。此策略允许人力资源部门的员工通过打印方式传输文件，以便将打印复本交由员工签署。但禁止通过其他可能的通道（例如，电子邮件）传输。

如果您已经配置 DLP 数据标识符，您也可以创建自己的模板。您也可以使用预定义的模板。有关详细信息，请参阅定制的 DLP 模板 第 10-19 页和预定义的 DLP 模板 第 10-18 页。

注意

无法删除 DLP 策略中正在使用的模板。删除模板之前，请先从策略中将其移除。

预定义的 DLP 模板

数据丢失防护附带以下一组预定义模板，供您视各种法规标准需求使用。您无法修改或删除这些模板。

- **GLBA**：《格雷姆-里奇-比利雷法案》
- **HIPAA**：《健康保险携带和责任法案》
- **PCI-DSS**：《支付卡行业数据安全标准》
- **SB-1386**：《美国参议院法案 1386》
- **US PII**：《美国个人可识别信息》

有关所有预定义模板的用途的详细列表以及要保护的数据的示例，请参阅“数据保护列表”文档，网址为 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

定制的 DLP 模板

如果您已经配置数据标识符，请创建自己的模板。模板将数据标识符和逻辑运算符 (And、Or、Except) 结合使用以构成条件语句。

有关条件语句和逻辑运算符工作方式的详细信息和示例，请参阅条件语句和逻辑运算符 第 10-19 页。

条件语句和逻辑运算符

数据丢失防护按照从左到右的顺序对条件语句求值。配置条件语句时，请谨慎使用逻辑运算符。使用不当会造成条件语句错误，从而有可能产生意想不到的后果。

请参阅下表中的示例。

表 10-4. 条件语句示例

条件语句	解译和示例
[数据标识符 1] **And** [数据标识符 2] **Except** [数据标识符 3]	文件必须满足 [数据标识符 1] 和 [数据标识符 2]，但不必满足 [数据标识符 3]。 例如： 文件必须是 [Adobe PDF 文档] 而且必须包含 [电子邮件地址]，但是不应包含 [关键字列表中的所有关键字]。
[数据标识符 1] **Or** [数据标识符 2]	文件必须满足 [数据标识符 1] 或 [数据标识符 2]。 例如： 文件必须是 [Adobe PDF 文档] 或 [Microsoft Word 文档]。
Except [数据标识符 1]	文件不得满足 [数据标识符 1]。 例如： 文件不得为 [多媒体文件]。

如表中最后一个示例所示，如果文件不得满足语句中的所有数据标识符，则条件语句中的第一个数据标识符可以有 "Except" 运算符。不过，在大部分情况下，第一个数据标识符没有运算符。

创建模板

过程

1. 转至**客户端** > **数据丢失防护** > **DLP 模板**。
2. 单击**添加**。

   将显示一个新窗口。
3. 键入模板的名称。名称的长度不能超过 100 个字节，而且不能包含下列字符：

   - > < * ^ | & ? \ /
4. 键入长度不超过 256 个字节的描述。

5. 选择数据标识符，然后单击“添加”图标。

   选择定义时：

   - 按住 CTRL 键的同时选择数据标识符，可以选择多个条目。
   - 如果想要使用特定定义，可以使用搜索功能。可以键入数据标识符的完整名称或部分名称。
   - 每个模板最多可以包含 40 个数据标识符。

6. 要创建新表达式，请单击 **表达式**，然后单击 **添加新表达式**。在显示的窗口中，配置表达式的设置。

7. 要创建新的文件属性列表，请单击 **文件属性**，然后单击 **添加新的文件属性**。在显示的窗口中，配置文件属性列表的设置。

8. 要创建新关键字列表，请单击 **关键字**，然后单击 **添加新关键字**。在显示的窗口中，配置关键字列表的设置。

9. 如果您选择表达式，请键入出现次数，该次数是指数据丢失防护让表达式遵循策略之前，表达式必须出现的次数。

10. 为每个定义选择一个逻辑运算符。



注意

配置条件语句时，请谨慎使用逻辑运算符。使用不当会造成条件语句错误，从而有可能产生意想不到的后果。有关正确用法示例，请参阅条件语句和逻辑运算符 第 10-19 页。

11. 要从选定标识符列表中移除数据标识符，请单击垃圾桶图标。

12. 在**预览**下，检查条件语句并进行更改（如果该语句不是预定语句）。

13. 单击**保存**。

14. 将显示一条消息，提醒您将设置部署到客户端。单击**关闭**。

15. 返回到 **DLP 模板**窗口，单击**应用到全部客户端**。

导入模板

如果您有包含模板且格式正确的 .dat 文件，请使用此选项。您可以从当前正在访问的服务器或其他服务器导出模板来生成该文件。

注意

要从防毒墙网络版 10.6 导入 DLP 模板，请先导入关联的数据标识符（以前称为“定义”）。数据丢失防护无法导入缺少关联数据标识符的模板。

过程

1. 转至**客户端** > **数据丢失防护** > **DLP 模板**。
2. 单击**导入**，然后找到包含表达式的 .dat 文件。
3. 单击**打开**。

   将显示一条消息，通知您导入是否成功。如果要导入的模板已存在，系统将跳过该模板。
4. 单击**应用到全部客户端**。

DLP 通道

用户可以通过各种通道传输敏感信息。防毒墙网络版可以监控下列通道：

- **网络通道**：敏感信息使用网络协议（如 HTTP 和 FTP）传输。
- **系统和应用程序通道**：敏感信息使用终端上的本地应用程序和外围设备传输。

网络通道

防毒墙网络版可以通过以下网络通道监控数据传输：

- 电子邮件客户端
- FTP
- HTTP 和 HTTPS
- IM 应用程序
- SMB 协议
- Webmail

要确定要监控的数据传输，防毒墙网络版将检查需要配置的传输范围。根据选择的范围，防毒墙网络版将监控所有数据传输或仅监控局域网 (LAN) 外部的传输。

有关传输范围的详细信息，请参阅网络通道的传输范围和目标 第 10-27 页。

电子邮件客户端

防毒墙网络版会监控通过各种电子邮件客户端传输的电子邮件。防毒墙网络版会检查电子邮件的主题、正文和附件是否包含数据标识符。有关支持的电子邮件客户端的列表，请参阅 *“数据保护列表”* 文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

当用户尝试发送电子邮件时，就会予以监控。如果电子邮件包含数据标识符，防毒墙网络版会允许或阻止该电子邮件。

可以定义不受监控的内部电子邮件域和受监控的子域。

- **不受监控的电子邮件域**：防毒墙网络版立即允许传输发送至不受监控的域的电子邮件。

注意

传输至不受监控的电子邮件域的数据与传输至受监控的电子邮件子域的数据（其中，处理措施是“监控”）的相似之处在于都允许传输。唯一的区别是对于不受监控的电子邮件域，防毒墙网络版不记录传输，但对于受监控的电子邮件子域，始终记录传输。

- **受监控的电子邮件子域**：当防毒墙网络版检测到传输至受监控子域的电子邮件时，将检查策略的处理措施。根据处理措施，将允许或阻止该传输。

注意

如果选择电子邮件客户端作为受监控通道，电子邮件必须匹配某个策略才能受到监控。相反，发送至受监控电子邮件子域的电子邮件会自动受到监控，即使其不匹配策略也会如此。

使用以下任一格式指定域，用逗号分隔多个域：

- X400 格式，如 /O=Trend/OU=USA, /O=Trend/OU=China
- 电子邮件域，如 example.com

对于通过 SMTP 协议发送的电子邮件，防毒墙网络版检查目标 SMTP 服务器是否位于以下列表上：

1. 受监控目标
2. 不受监控的目标

注意

有关受监控和不受监控的目标的详细信息，请参阅定义不受监控的目标和受监控的目标 第 10-38 页。

3. 不受监控的电子邮件域
4. 受监控的电子邮件子域

这意味着如果电子邮件发送至的 SMTP 服务器位于受监控目标列表上，则监控该电子邮件。如果 SMTP 服务器不在受监控目标列表上，则防毒墙网络版将检查其他列表。

对于通过其他协议发送的电子邮件，防毒墙网络版仅检查以下列表：

1. 不受监控的电子邮件域
2. 受监控的电子邮件子域

FTP

当防毒墙网络版检测到 FTP 客户端尝试将文件上传到 FTP 服务器时，它会检查文件中是否包含数据标识符。此时尚未上传任何文件。根据 DLP 策略，防毒墙网络版会允许或阻止上传。

当您配置阻止文件上传的策略时，请记住以下几点：

- 当防毒墙网络版阻止上传时，某些 FTP 客户端会尝试重新上传文件。在这种情况下，防毒墙网络版会终止该 FTP 客户端，以禁止重新上传。FTP 客户端终止后，用户不会收到通知。当您全面实施 DLP 策略时，请将此情况告知用户。
- 如果要上传的文件会覆盖 FTP 服务器上的文件，可能会删除 FTP 服务器上的文件。

有关支持的 FTP 客户端的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP 和 HTTPS

防毒墙网络版会监控要通过 HTTP 和 HTTPS 传输的数据。对于 HTTPS，在对数据进行加密并传输之前，防毒墙网络版会先进行检查。

有关支持的 Web 浏览器和应用程序的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

IM 应用程序

防毒墙网络版会监控用户通过即时通讯 (IM) 应用程序发送的消息和文件，但不会监控用户收到的消息和文件。

有关支持的 IM 应用程序的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

当防毒墙网络版阻止通过 AOL Instant Messenger、MSN、Windows Messenger 或 Windows Live Messenger 发送的消息或文件时，它也会终止相应的应用程序。如果防毒墙网络版不这样做，应用程序就会变成没有响应，用户仍会被迫终止应用程序。应用程序终止之后，用户不会收到通知。当您全面实施 DLP 策略时，请将此情况告知用户。

SMB 协议

防毒墙网络版会监控通过服务器消息块 (SMB) 协议（这种协议可用于共享文件访问）传输的数据。当另一位用户尝试复制或读取某一用户的共享文件时，防毒墙网络版会检查文件是否为数据标识符或包含数据标识符，然后允许或阻止该操作。

注意

设备控制处理措施的优先级高于 DLP 处理措施的优先级。例如，如果“设备控制”不允许移动映射网络驱动器上的文件，则即使 DLP 允许，也不会传输敏感数据。

有关“设备控制”处理措施的详细信息，请参阅存储设备的权限 第 9-4 页。

有关防毒墙网络版监控的、用于共享文件访问的应用程序的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Webmail

基于 Web 的电子邮件服务通过 HTTP 传输数据。如果防毒墙网络版检测到从支持的服务传出的数据，它会检查数据中是否包含数据标识符。

有关支持的基于 Web 的电子邮件服务的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

网络通道的传输范围和目标

传输范围和目标定义网络通道上防毒墙网络版必须监控的数据传输。对于应监控的传输，防毒墙网络版在允许或阻止传输之前检查是否存在数据标识符。对于不应监控的传输，防毒墙网络版将不检查是否存在数据标识符，立即允许传输。

传输范围：所有传输

防毒墙网络版会监控在主计算机之外传输的数据。

注意

趋势科技建议对外部客户端选择此作用域。

如果不想监控传输至宿主计算机之外特定目标的数据，请定义以下内容：

- **不受监控的目标**：防毒墙网络版不监控传输至这些目标的数据。

  注意

  传输至不受监控的目标的数据与传输至受监控目标的数据（其中，处理措施是“监控”）的相似之处在于都允许传输。唯一的区别是对于不受监控的目标，防毒墙网络版不记录传输，但对于受监控目标，始终记录传输。

- **受监控的目标**：这些是不受监控的目标内应该监控的特定目标。受监控目标是：
  - 如果定义了不受监控的目标，则可选。
  - 如果未定义不受监控的目标，则是不可配置的。

例如：

将以下 IP 地址分配给贵公司的法律部门：

- 10.201.168.1 至 10.201.168.25

您将创建一个策略，监控至除法律部门全职员工以外所有员工的就业证书的传输。要执行此操作，您将选择**所有传输**作为传输范围，然后：

选项	步骤
选项 1	1. **将** 10.201.168.1 **至** 10.201.168.25 **添加到不受监控目标。** 2. **将法律部门兼职员工的 IP 地址添加到受监控目标。假设有 3 个 IP 地址：** 10.201.168.21 **至** 10.201.168.23
选项 2	**将法律部门全职员工的 IP 地址添加到不受监控的目标：** • 10.201.168.1-10.201.168.20 • 10.201.168.24-10.201.168.25

有关如何定义受监控和不受监控的目标的准则，请参阅定义不受监控的目标和受监控的目标 第 10-38 页。

传输范围：仅局域网外部的传输

防毒墙网络版会监控传输到局域网 (LAN) 外部的任何目标的数据。

注意

趋势科技建议对内部客户端选择此作用域。

“网络”指的是公司或局部网络。这包括当前网络 (终端和网络掩码的 IP 地址) 以及下列标准专用 IP 地址：

- A 类：10.0.0.0 至 10.255.255.255
- B 类：172.16.0.0 至 172.31.255.255
- C 类：192.168.0.0 至 192.168.255.255

如果选择此传输范围，可以定义以下内容：

- **不受监控的目标**：定义 LAN 外部您认为安全而不应监控的目标。

注意

传输至不受监控的目标的数据与传输至受监控目标的数据（其中，处理措施是“监控”）的相似之处在于都允许传输。唯一的区别是对于不受监控的目标，防毒墙网络版不记录传输，但对于受监控目标，始终记录传输。

- **受监控的目标**：定义 LAN 内部要监控的目标。

有关如何定义受监控和不受监控的目标的准则，请参阅定义不受监控的目标和受监控的目标 第 10-38 页。

解决冲突

如果传输范围、受监控目标和不受监控的目标的设置存在冲突，防毒墙网络版将按照从高到低的顺序识别以下优先级：

- 受监控目标
- 不受监控的目标
- 传输范围

系统和应用程序通道

防毒墙网络版可以监控下列系统和应用程序通道：

- 云存储服务
- 数据记录器 (CD/DVD)
- 对等应用程序
- PGP 加密
- 打印机
- 可移动存储
- 同步软件 (ActiveSync)

- Windows 剪贴板

云存储服务

防毒墙网络版监控用户使用云存储服务访问的文件。有关支持的云存储服务列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

注意

如果在代理终端上安装了终端加密，则数据丢失防护支持在云存储服务中加密。

数据记录器 (CD/DVD)

防毒墙网络版会监记录到 CD 或 DVD 的数据。有关支持的数据记录设备和软件的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

当防毒墙网络版检测到支持的任何设备或软件发出“刻录”命令，而且处理措施是“不予处理”时，数据记录会继续。如果处理措施是“阻止”，防毒墙网络版会检查要记录的任意文件是否为数据标识符或包含数据标识符。如果防毒墙网络版至少检测到一个数据标识符，则不会记录所有文件（包括不属于数据标识符的文件和不包含数据标识符的文件）。防毒墙网络版还可能会阻止 CD 或 DVD 弹出。如果发生此问题，请指示用户重新启动软件进程或重置设备。

防毒墙网络版会执行其他 CD/DVD 记录规则：

- 为了减少误判的情况，防毒墙网络版不会监控下列文件：

.bud	.dll	.gif	.gpd	.htm	.ico	.ini
.jpg	.lnk	.sys	.ttf	.url	.xml	

- 为提高性能，系统不会监控 Roxio 数据记录器使用的两种文件类型（*.png 和 *.skn）。

- 防毒墙网络版不会监控下列目录中的文件：

*:\autoexec.bat	*:\Windows
..\Application Data	..\Cookies
..\Local Settings	..\ProgramData
..\Program Files	..\Users*\AppData
..\WINNT	

- 系统不会监控设备和软件创建的 ISO 镜像。

阻止访问数据记录器 (CD/DVD)

设备控制只能限制对使用实时文件系统格式的 CD/DVD 录制设备的访问。即使启用了设备控制，部分使用母版格式的第三方应用程序也能执行读/写操作。可以通过数据丢失防护限制对使用任何格式类型的 CD/DVD 录制设备的访问。

过程

1. 转至**客户端 > 客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置 > DLP 设置**。
4. 单击**外部客户端**选项卡为外部客户端配置策略，或单击**内部客户端**选项卡为内部客户端配置策略。

注意

配置客户端位置设置（如果尚未执行此操作）。客户端将使用这些位置设置来确定要应用的正确数据丢失防护策略。有关详细信息，请参阅终端位置 第 14-2 页。

5. 选择以下项之一：

- 如果您位于**外部客户端**选项卡，则可以选择**将所有设置应用到内部客户端**以将所有数据丢失防护设置应用到内部客户端。
- 如果您位于**内部客户端**选项卡，则可以选择**将所有设置应用到外部客户端**以将所有数据丢失防护设置应用到外部客户端。

6. 在**规则**选项卡上，单击**添加**。
7. 选择**启用此规则**。
8. 为该规则指定一个名称。
9. 单击**模板**选项卡。
10. 从列表中选择**所有文件扩展名**模板，然后单击**添加**。
11. 单击**通道**选项卡。
12. 在**系统和应用程序通道**部分中，选择**数据记录器 (CD/DVD)**。
13. 单击**处理措施**选项卡。
14. 选择**阻止**处理措施。
15. 单击**保存**。
16. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
    - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
    - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

对等应用程序

防毒墙网络版会监控用户通过对等应用程序共享的文件。

有关支持的对等应用程序的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

PGP 加密

防毒墙网络版会监控将由 PGP 加密软件加密的数据。数据加密之前，防毒墙网络版会先检查。

有关支持的 PGP 加密软件的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

打印机

防毒墙网络版会监控各种应用程序发出的打印机操作。

防毒墙网络版不会阻止尚未保存的新文件的打印机操作，因为打印信息此时只存储在内存中。

有关可发出打印机操作的受支持应用程序的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

可移动存储

防毒墙网络版监控至可移动存储设备或这些设备内的数据传输。与数据传输相关的活动包括：

- 在设备中创建文件
- 将文件从主机复制到设备
- 关闭设备中已修改的文件

- 修改设备中的文件信息（例如文件的扩展名）

当要传输的文件包含数据标识符时，防毒墙网络版会阻止或允许传输。

注意

- 设备控制处理措施的优先级高于 DLP 处理措施的优先级。例如，如果设备控制不允许将文件复制到可移动存储设备，则即使 DLP 允许，也不会传输敏感信息。
- 如果在代理终端上安装了终端加密，数据丢失防护支持在可移动存储设备中加密。

有关可简化数据传输活动的受支持可移动存储设备和应用程序的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

将文件传输至可移动存储设备的处理是一种直接的过程。例如，在 Microsoft Word 中创建文件的用户可能想要将文件保存至 SD 卡（与用户保存的文件类型无关）。如果文件包含不应该传输的数据标识符，防毒墙网络版会禁止保存该文件。

对于设备中的文件传输，防毒墙网络版会先将文件（如果文件大小未超过 75 MB）备份到 %WINDIR%\system32\dgagent\temp，然后再进行处理。如果防毒墙网络版允许传输文件，它就会移除备份文件。如果防毒墙网络版阻止传输，文件可能会在这个过程中被删除。在这种情况下，防毒墙网络版会将备份文件复制到包含原始文件的文件夹。

防毒墙网络版允许您定义例外。防毒墙网络版始终允许将数据传输到这些设备或在这些设备内进行数据传输。按照供应商识别设备并可选择提供设备型号和序列号。

提示

可以使用设备列表工具查询连接至终端的设备。该工具可以提供每个设备的设备供应商、型号和序列号。有关详细信息，请参阅设备列表工具 第 9-12 页。

同步软件 (ActiveSync)

防毒墙网络版会监控通过同步软件传输到移动设备的数据。

有关支持的同步软件的列表，请参阅“数据保护列表”文档，网址为：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

如果数据的源 IP 地址为 127.0.0.1，而且是通过端口 990 或 5678（用于同步的端口）发送的，则防毒墙网络版会检查数据是否为数据标识符，然后再允许或阻止其传输。

当防毒墙网络版阻止端口 990 上传输的文件时，可能仍会在移动设备上的目标文件夹中创建包含畸形字符的同名文件。这是因为在防毒墙网络版阻止传输之前，文件的某些部分已经复制到设备上。

Windows 剪贴板

防毒墙网络版会监控要传输到 Windows 剪贴板的数据，然后再允许或阻止传输。

防毒墙网络版也可以监控主机与 VMWare 或远程桌面之间的剪贴板活动。会对具有防毒墙网络版客户端的实体进行监控。例如，VMware 虚拟机上的防毒墙网络版客户端会禁止虚拟机上的剪贴板数据传输到主机。同样地，具有防毒墙网络版客户端的主机无法将剪贴板数据复制到通过远程桌面访问的终端。

数据丢失防护措施

当数据丢失防护检测到数据标识符的传输时，它会针对检测到的数据标识符检查 DLP 策略，并执行为该策略配置的处理措施。

下表列出了数据丢失防护处理措施。

表 10-5. 数据丢失防护措施

处理措施	描述
处理措施	
不予处理	数据丢失防护允许并记录传输。
阻止	数据丢失防护阻止并记录传输。
其他处理措施	
通知客户端用户	数据丢失防护会显示通知消息以通知传输数据的用户，并通知数据已传送还是已阻止。
记录数据	无论采取何种主要处理措施，数据丢失防护都会将敏感信息记录到 <客户端安装文件夹>\DLPLite\Forensic。选择此处理措施以评估数据丢失防护所标记的敏感信息。 记录的敏感信息可能会耗费过多的硬盘空间。因此，趋势科技强烈建议您仅为高度敏感的信息选择该选项。

处理措施	描述
使用指定的密钥/密码且支持加密的通道 (只在已安装终端加密时可用) **注意** 在选择**不予处理**处理措施的情况下，该选项仅适用于可移动存储和云存储服务通道。	如果随防毒墙网络版客户端一起安装了趋势科技终端加密，数据丢失防护将首先对文件自动加密，然后才允许用户将这些文件传送到其他位置。如果未安装终端加密，数据丢失防护将对文件执行“阻止”处理措施。 选择以下加密密钥或固定密码之一： • **用户密钥**：也称为**本地密钥**，该密钥对于每个用户而言是唯一的，它将加密文件的访问权限限制为创建了该文件的用户。 • **共享密钥**：该密钥是指**组密钥**或**企业密钥**，终端加密管理员使用 PolicyServer MMC 配置该类型。 • **固定密码**：用户使用窗口上的提示手动提供固定密码。终端加密将创建自解压缩软件包，用户在提供了解密密码后可在任何终端上访问它。 **重要信息** • 目标终端必须安装终端加密，用户必须登录终端加密才能加密数据。 • 用户尝试解密 USB 设备上的加密文件时，这些文件需要经过数据丢失防护扫描。解密 USB 设备上包含敏感数据的文件会触发 USB 加密协议，从而导致系统要求将这些敏感数据再次加密。为了防止防毒墙网络版尝试“重新加密”数据，请在尝试访问数据之前将加密文件移动到本地驱动器。 • 在使用 Web 客户端时，数据丢失防护阻止尝试将文件上传到云存储。在使用 Web 客户端上传之前手动对文件加密。

处理措施	描述
用户原因 **注意** 仅在选择**阻止**处理措施后，此选项才可用。	数据丢失防护会在执行“阻止”处理措施前提示用户。用户可以选择通过提供敏感数据可以安全传送的说明来覆盖“阻止”处理措施。可用的原因如下： • **这是已确定的业务流程的一部分。** • **我的经理允许数据传输。** • **此文件中的数据不是机密数据。** • **其他**：用户在提供的文本框中提供一个备用说明。

数据丢失防护例外

DLP 例外适用于整个策略，包括在策略中定义的所有规则。扫描数字资产之前，数据丢失防护会将例外设置应用到所有传输。如果某个传输与某个例外规则匹配，数据丢失防护会立即允许或扫描该传输，具体取决于例外类型。

定义不受监控的目标和受监控的目标

根据在**通道**选项卡上配置的传输范围定义不受监控的目标和受监控的目标。有关如何定义**所有传输**的受监控目标和不受监控的目标的详细信息，请参阅传输范围：所有传输 第 10-27 页。有关如何定义**仅局域网外部的传输**的受监控目标和不受监控的目标的详细信息，请参阅传输范围：仅局域网外部的传输 第 10-28 页。

定义受监控目标和不受监控的目标时，请遵循以下准则：

1. 按照以下内容定义每个目标：
   - IP 地址
   - 主机名
   - FQDN

- 网络地址和子网掩码，例如 10.1.1.1/32

注意

对于子网掩码，数据丢失防护仅支持无类域际路由选择 (CIDR) 类型端口。这表示您只能输入类似 32 的数字，而非 255.255.255.0。

2. 要定位特定通道，需要包含这些通道的缺省端口号或公司定义的端口号。例如，端口 21 通常用于 FTP 网络通信，端口 80 用于 HTTP，端口 443 用于 HTTPS。使用冒号分隔目标与端口号。
3. 也可以包含端口范围。要包含所有端口，请忽略端口范围。

   以下是带有端口号和端口范围的目标的一些示例：

   - 10.1.1.1:80
   - 主机:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. 使用逗号分隔各个目标。

解压缩规则

可以对压缩文件中包含的文件进行扫描以确定是否存在数字资产。要确定要扫描的文件，数据丢失防护要求压缩文件遵循以下规则：

- **解压缩文件大小超过：__ MB (1-512MB)**
- **压缩层数超过：__ (1-20)**
- **要扫描的文件数超过：__ (1-2000)**

规则 1：解压缩文件的最大大小

压缩文件在解压缩后必须符合指定限制。

示例：将限制设置为 20MB。

场景 1：如果 archive.zip 在解压缩后的大小为 30MB，archive.zip 中包含的任何文件都不会被扫描。将不再检查其他两个规则。

场景 2：如果 my_archive.zip 在解压缩后的大小为 10MB：

- 如果 my_archive.zip 不包含压缩文件，防毒墙网络版会跳过规则 2 并继续执行规则 3。
- 如果 my_archive.zip 包含压缩文件，所有解压缩文件的大小必须在限制范围内。例如，如果 my_archive.zip 包含 AAA.rar、BBB.zip 和 EEE.zip，并且 EEE.zip 包含 222.zip：

my_archive.zip			= 10MB（解压缩后）
	\AAA.rar		= 25MB（解压缩后）
	\BBB.zip		= 3MB（解压缩后）
	\EEE.zip		= 1MB（解压缩后）
		\222.zip	= 2MB（解压缩后）

将根据规则 2 检查 my_archive.zip、BBB.zip、EEE.zip 和 222.zip，因为这些文件的总大小在 20MB 的限制范围内。将跳过 AAA.rar 。

规则 2：最大压缩层数

在指定层数内的文件会被标记为进行扫描。

例如：

my_archive.zip			
	\BBB.zip	\CCC.xls	
	\DDD.txt		
	\EEE.zip	\111.pdf	
		\222.zip	\333.txt

如果将限制设置为两层：

- 防毒墙网络版将忽略 333.txt，因为它位于第三层。
- 防毒墙网络版将以下文件标记为进行扫描，然后检查规则 3：
  - DDD.txt（位于第一层）
  - CCC.xls（位于第二层）
  - 111.pdf（位于第二层）

规则 3：要扫描的最大文件数

防毒墙网络版最多可以扫描指定限制的文件。防毒墙网络版先按数字顺序，然后再按字母顺序扫描文件和文件夹。

继续使用规则 2 中的示例，防毒墙网络版已将突出显示的文件标记为进行扫描：

my_archive.zip			
	\BBB.zip	**\CCC.xls**	
	\DDD.txt		
	\EEE.zip	**\111.pdf**	
		\222.zip	\333.txt

此外，my_archive.zip 包含一个名为 7Folder 的文件夹，并不对照规则 2 检查该文件夹。该文件夹包含 FFF.doc 和 GGG.ppt。要扫描的文件数量就此达到 5，在下面所突出显示：

my_archive.zip		
	\7Folder	**\FFF.doc**
	\7Folder	**\GGG.ppt**
	\BBB.zip	**\CCC.xls**

	\DDD.txt		
	\EEE.zip	**\111.pdf**	
		\222.zip	\333.txt

如果将限制设置为 4 个文件，则将扫描以下文件：

- FFF.doc
- GGG.ppt
- CCC.xls
- DDD.txt

注意

对于包含嵌入式文件的文件，防毒墙网络版将提取嵌入式文件的内容。

如果提取的内容是文本，则将主机文件（如 123.doc）和嵌入式文件（如 abc.txt 和 xyz.xls）计数为 1。

如果提取的内容不是文本，则将分别对主机文件（如 123.doc）和嵌入式文件（如 abc.exe）计数。

触发解压缩规则的事件

以下事件会触发解压缩规则：

表 10-6. 触发解压缩规则的事件

要传输的压缩文件与策略匹配，且对压缩文件的处理措施为“不予处理（传输文件）”。	例如，为了监控用户正在传输的 .ZIP 文件，您定义了文件属性 (.ZIP)，将其添加到模板，在策略中使用该模板，然后将处理措施设置为**不予处理**。 **注意** 如果处理措施为“阻止”，将不会传输整个压缩文件，因此无需扫描其包含的文件。
要传输的压缩文件与策略不匹配。	在这种情况下，防毒墙网络版仍然会对该压缩文件应用解压缩规则以确定应对该文件中包含的哪些文件进行扫描以查看是否存在数字资产，并确定是否要传输整个压缩文件。

这两种事件具有相同的结果。当防毒墙网络版遇到压缩文件时：

- 如果不满足规则 1，防毒墙网络版将允许传输整个压缩文件。
- 如果满足规则 1，则将检查其他两个规则。如果出现以下情况，防毒墙网络版将允许传输整个压缩文件：
  - 所有扫描的文件与策略均不匹配。
  - 所有扫描的文件均与策略匹配，且处理措施为**不予处理**。

    如果至少有一个扫描的文件与策略匹配且处理措施为**阻止**，则将阻止传输整个压缩文件。

数据丢失防护策略配置

配置数据标识符并将它们分门别类放到各个模板之后，即可开始创建数据丢失防护策略。

除了数据标识符和模板之外，创建策略时，还需要配置通道和处理措施。有关策略的详细信息，请参阅数据丢失防护策略 第 10-3 页。

创建数据丢失防护策略

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **DLP 设置**。
4. 单击**外部客户端**选项卡为外部客户端配置策略，或单击**内部客户端**选项卡为内部客户端配置策略。

   注意

   配置客户端位置设置（如果尚未执行此操作）。客户端将使用这些位置设置来确定要应用的正确数据丢失防护策略。有关详细信息，请参阅终端位置 第 14-2 页。

5. 选择**启用数据丢失防护**。
6. 选择以下项之一：
   - 如果您位于**外部客户端**选项卡，则可以选择**将所有设置应用到内部客户端**以将所有数据丢失防护设置应用到内部客户端。
   - 如果您位于**内部客户端**选项卡，则可以选择**将所有设置应用到外部客户端**以将所有数据丢失防护设置应用到外部客户端。
7. 在**规则**选项卡上，单击**添加**。

   一个策略最多可以包含 40 个规则。
8. 配置规则设置。

有关创建 DLP 规则的详细信息，请参阅创建数据丢失防护规则 第 10-45 页。

9. 单击**例外**选项卡，然后配置任何必要的例外设置。

   有关可用的例外设置的详细信息，请参阅数据丢失防护例外 第 10-38 页。

10. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

    - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
    - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

创建数据丢失防护规则



注意

数据丢失防护按优先级处理规则和模板。如果规则设置为“不予处理”，数据丢失防护会处理列表中的下一个规则。如果规则设置为“阻止”或“用户原因”，数据丢失防护会阻止或接受用户处理措施，并且不会进一步处理该规则/模板。

过程

1. 选择**启用此规则**。
2. 为该规则指定一个名称。

   配置模板设置：

3. 单击**模板**选项卡。
4. 从**可用模板**列表中选择模板，然后单击**添加**。

   选择模板时：

   - 通过单击突出显示名称的模板名称来选择多个条目。

- 如果想要使用特定模板，可以使用搜索功能。您可以键入模板的完整名称或部分名称。

注意

每个规则最多可以包含 200 个模板。

5. 如果在**可用模板**列表中未找到首选模板：

   a. 单击 **添加新模板**。

      将显示**数据丢失防护模板**窗口。

      有关在**“数据防护模板”窗口**中添加模板的说明，请参阅数据丢失防护模板 第 10-18 页。

   b. 创建模板之后，请选择它，然后单击**添加**。

注意

在检查模板时，防毒墙网络版将使用第一个匹配规则。这意味着，如果文件或数据与一个模板中的定义匹配，防毒墙网络版将不再检查其他模板。优先级基于列表中模板的顺序。

配置通道设置：

6. 单击**通道**选项卡。
7. 请为此规则选择通道。

   有关通道的详细信息，请参阅网络通道 第 10-22 页和系统和应用程序通道 第 10-29 页。

8. 如果选择了任意网络通道，请选择传输范围：

   - **所有传输**
   - **仅局域网外部的传输**

   有关传输范围、目标的工作方式（取决于传输范围）以及如何正确定义目标的详细信息，请参阅网络通道的传输范围和目标 第 10-27 页。

9. 如果选择了**电子邮件客户端**：

a. 单击**例外**。

b. 指定受监控和不受监控的内部电子邮件域。

有关受监控和不受监控的电子邮件域的详细信息，请参阅电子邮件客户端 第 10-23 页。

10. 如果选择了**可移动存储**：

a. 单击**例外**。

b. 添加不受监控的可移动存储设备，使用其供应商进行识别。设备型号和序列号是可选的。

USB 设备的允许列表支持使用星号 (*) 通配符。将任何文本框替换为星号 (*) 以包括满足其他文本框的所有设备。

例如，[vendor]-[model]-* 会将指定供应商和指定型号类型的所有 USB 设备置于允许列表中，而不考虑序列号。

c. 要添加更多设备，请单击加号 (+) 图标。

提示

可以使用设备列表工具查询连接至终端的设备。该工具可以提供每个设备的设备供应商、型号和序列号。有关详细信息，请参阅设备列表工具 第 9-12 页。

配置处理措施设置：

11. 单击**处理措施**选项卡。

12. 选择一项主要处理措施和任意数量的其他处理措施。

有关处理措施的详细信息，请参阅数据丢失防护措施 第 10-35 页。

注意

数据丢失防护仅支持对可移动设备和云存储服务上的敏感数据进行加密。在不支持加密的所有通道上，数据丢失防护将执行“不予处理”处理措施而不进行加密。目标终端必须安装终端加密，用户必须登录终端加密才能加密数据。

13. 配置**模板**、**通道**和**处理措施**设置后，单击**保存**。

导入、导出和复制 DLP 规则

管理员可以导入先前定义的规则（包含在格式正确的 .dat 文件中）或导出已配置 DLP 规则的列表。复制 DLP 规则允许管理员修改先前定义的规则的内容以节省时间。

下表介绍了各功能的工作原理。

表 10-7. DLP 规则的导入、导出和复制功能

功能	描述
导入	导入规则列表会在现有的 DLP 规则列表中追加非现有规则。数据丢失防护会跳过目标列表中已存在的规则。数据丢失防护会保留每个规则的所有预先配置设置，包括启用或禁用状态。
导出	导出规则列表会将整个列表导出为 .dat 文件，然后，管理员可以导入该文件并将其部署到其他域或客户端。数据丢失防护会基于当前配置保存所有规则设置。 **注意** • 导出列表之前，管理员必须保存或应用所有新的或已修改的规则。 • 数据丢失防护只会导出为各个规则配置的设置，不会导出为策略配置的任何例外。
复制	复制规则将创建该规则当前配置设置的确切副本。管理员必须键入规则的新名称，且在必要时可对新规则进行任何配置修改。

数据丢失防护通知

防毒墙网络版具有一组缺省的通知消息，可在检测到数字资产传输时，通知防毒墙网络版管理员和客户端用户。

有关发送给管理员的通知的详细信息，请参阅管理员的数据丢失防护通知 第 10-49 页。

有关发送给客户端用户的通知的详细信息，请参阅客户端用户的数据丢失防护通知 第 10-52 页。

管理员的数据丢失防护通知

可以将防毒墙网络版配置为在检测到数字资产传输时或仅在阻止传输时，向管理员发送通知。

防毒墙网络版附带一组缺省的通知消息，可将数字资产传输通知给管理员。根据公司需要修改通知并配置其他通知设置。



注意

防毒墙网络版可以通过电子邮件、SNMP 陷阱和 Windows NT 事件日志来发送通知。配置防毒墙网络版何时通过这些通道发送通知的设置。有关详细信息，请参阅管理员通知设置 第 13-32 页。

配置管理员的数据丢失防护通知

过程

1. 转至**管理** > **通知** > **管理员**。
2. 在**条件**选项卡上：
   a. 转至**数字资产传输**部分。
   b. 指定是在检测到数字资产传输（处理措施可以是阻止或不予处理）时发送通知，还是仅当阻止传输时发送通知。
3. 在**电子邮件**选项卡上：
   a. 转至**数字资产传输**部分。
   b. 选择**启用电子邮件通知**。

c. 选择**向拥有客户端树域权限的用户发送通知**。

使用基于角色的管理授予用户客户端树域权限。如果属于特定域的任何客户端上发生传输，则会向具有域权限的用户的电子邮件地址发送电子邮件。有关示例，请参阅下表：

表 10-8. 客户端树域和权限

客户端树域	具有域权限的角色	具有该角色的用户帐户	用户帐户的电子邮件地址
域 A	Administrator (内置)	根	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
域 B	Administrator (内置)	根	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果属于域 A 的防毒墙网络版客户端检测到数字资产传输，则会向 mary@xyz.com、john@xyz.com 和 chris@xyz.com 发送电子邮件。

如果属于域 B 的防毒墙网络版客户端检测到传输，则会向 mary@xyz.com 和 jane@xyz.com 发送电子邮件。

注意

如果启用此选项，具有域权限的所有用户都必须具有相应的电子邮件地址。不会向没有电子邮件地址的用户发送电子邮件通知。用户和电子邮件地址是从**管理** > **帐户管理** > **用户帐户**进行配置的。

d. 选择**向以下电子邮件地址发送通知**，然后键入电子邮件地址。

e. 接受或修改缺省的主题和消息。使用标记变量表示**主题**和**消息**文本框中的数据。

表 10-9. 数据丢失防护通知的标记变量

变量	描述
%USER%	检测到传输时已登录到终端的用户
%COMPUTER%	检测到传输的终端
%DOMAIN%	终端的域
%DATETIME%	检测到传输的日期和时间
%CHANNEL%	检测到传输的通道
%TEMPLATE%	触发检测的数字资产模板
%RULE%	触发检测的规则名称

4. 在 **SNMP Trap** 选项卡上：
   a. 转至**数字资产传输**部分。
   b. 选择**启用 SNMP 陷阱通知**。
   c. 接受或修改缺省消息。使用标记变量表示**消息**文本框中的数据。请参阅表 10-9：数据丢失防护通知的标记变量 第 10-51 页以了解详细信息。
5. 在 **NT 事件日志**选项卡上：
   a. 转至**数字资产传输**部分。
   b. 选择**启用 NT 事件日志通知**。
   c. 接受或修改缺省消息。可以使用标记变量表示**消息**文本框中的数据。请参阅表 10-9：数据丢失防护通知的标记变量 第 10-51 页以了解详细信息。
6. 单击**保存**。

客户端用户的数据丢失防护通知

防毒墙网络版可以在允许或阻止数字资产传输之后，立即在客户端计算机上显示通知消息。

要在阻止或允许数字资产传输时通知用户，请在创建数据丢失防护策略时选择**通知客户端用户**选项。有关创建策略的说明，请参阅数据丢失防护策略配置 第 10-43 页。

配置客户端的数据丢失防护通知

过程

1. 转至**管理** > **通知** > **客户端**。
2. 在**类型**下拉列表中，选择**数字资产传输**。
3. 接受或修改缺省消息。
4. 单击**保存**。

数据丢失防护日志

客户端会记录数字资产传输（阻止和允许的传输），并立即将日志发送给服务器。如果客户端无法发送日志，它会在 5 分钟后重试。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看数据丢失防护日志

过程

1. 转至**客户端** > **客户端管理**或**日志** > **客户端** > **安全风险**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **数据丢失防护日志**或**查看日志** > **DLP 日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 查看日志。

   日志包含以下信息：

表 10-10. 数据丢失防护日志信息

列	描述
日期/时间	数据丢失防护记录事件的日期和时间
用户	登录到终端的用户名
终端	数据丢失防护检测到传输的终端名称
域	终端的域
IP	终端的 IP 地址
规则名称	触发事件的规则名称 **注意** 先前版本的防毒墙网络版中创建的策略显示缺省名称为 LEGACY_DLP_Policy。
通道	发生传输的通道
进程	促进传输数字资产的进程（进程视通道而有所不同） 有关详细信息，请参阅与通道有关的进程 第 10-54 页。

列	描述
源	包含数字资产的文件源或通道（若无可用源）
目标	包含数字资产的文件的预期目标或通道（若无任何可用源）
处理措施	对传输采取的操作
详细信息	包括传输的其他详细信息的链接 有关详细信息，请参阅数据丢失防护日志详细信息 第 10-56 页。

6. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

与通道有关的进程

下表列出了数据丢失防护日志中**进程**列下显示的进程。

表 10-11. 与通道有关的进程

通道	进程
同步软件 (ActiveSync)	同步软件的完整路径和进程名称 示例： C:\Windows\system32\WUDFHost.exe
数据记录器 (CD/DVD)	数据记录器的完整路径和进程名称 示例： C:\Windows\Explorer.exe
Windows 剪贴板	不适用
电子邮件客户端 – Lotus Notes	Lotus Notes 的完整路径和进程名称 示例： C:\Program Files\IBM\Lotus\Notes\nlnotes.exe

通道	进程
电子邮件客户端 – Microsoft Outlook	Microsoft Outlook 的完整路径和进程名称 **示例：** C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE
电子邮件客户端 – 使用 SMTP 协议的所有客户端	电子邮件客户端的完整路径和进程名称 **示例：** C:\Program Files\Mozilla Thunderbird\thunderbird.exe
可移动存储	将数据传输至存储设备或在存储设备内部传输数据的应用程序的进程名称 **示例：** explorer.exe
FTP	FTP 客户端的完整路径和进程名称 **示例：** D:\Program Files\FileZilla FTP Client\filezilla.exe
HTTP	“HTTP 应用程序”
HTTPS	浏览器或应用程序的完整路径和进程名称 **示例：** C:\Program Files\Internet Explorer\iexplore.exe
IM 应用程序	IM 应用程序的完整路径和进程名称 **示例：** C:\Program Files\Skype\Phone\Skype.exe
IM 应用程序 – MSN	• MSN 的完整路径和进程名称 **示例：** C:\Program Files\Windows Live\Messenger\ msnmsgr.exe • “HTTP 应用程序”（如果从聊天窗口传输数据）

通道	进程
对等应用程序	对等应用程序的完整路径和进程名称 **示例：** D:\Program Files\BitTorrent\bittorrent.exe
PGP 加密	PGP 加密软件的完整路径和进程名称 **示例：** C:\Program Files\PGP Corporation\PGP Desktop\ PGPmnApp.exe
打印机	启动打印机操作的应用程序的完整路径和进程名称 **示例：** C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE
SMB 协议	从中执行共享文件访问（复制或创建新文件）的应用程序的完整路径和进程名称 **示例：** C:\Windows\Explorer.exe
Webmail（HTTP 模式）	“HTTP 应用程序”
Webmail（HTTPS 模式）	浏览器或应用程序的完整路径和进程名称 **示例：** C:\Program Files\Mozilla Firefox\firefox.exe

数据丢失防护日志详细信息

数据丢失防护日志详细信息窗口显示了有关数字资产传输的其他详细信息。传输的详细信息因防毒墙网络版检测事件的通道和过程的不同而有所差异。

下表列出了显示的详细信息。

表 10-12. 数据丢失防护日志详细信息

详细信息	描述
日期/时间	数据丢失防护记录事件的日期和时间
违例 ID	事件的唯一 ID
用户	登录到终端的用户名
终端	数据丢失防护检测到传输的终端名称
域	终端的域
IP	终端的 IP 地址
通道	发生传输的通道
进程	促进传输数字资产的进程（进程视通道而有所不同） 有关详细信息，请参阅与通道有关的进程 第 10-54 页。
源	包含数字资产的文件源或通道（若无可用源）
电子邮件发件人	发生传输的电子邮件地址
电子邮件主题	包含数字资产的电子邮件的主题行
电子邮件收件人	电子邮件的目标电子邮件地址
URL	Web 站点或网页的 URL
FTP 用户	用来登录 FTP 服务器的用户名
文件类	数据丢失防护检测到数字资产的文件类型
规则/模板	触发检测的准确规则名称和模板列表 **注意** 每个规则可能包含多个触发事件的模板。多个模板名称以逗号分隔。
处理措施	对传输采取的操作
用户原因	用户提供的用于继续传输敏感数据的原因

启用数据保护模块的调试日志记录

过程

1. 从技术支持提供商处获取 logger.cfg 文件。
2. 在 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`（对于 32 位系统）或 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite`（对于 64 位系统）中添加以下数据：
   - **类型**：字符串
   - **名称**：`debugcfg`
   - **值**：`C:\Log\logger.cfg`
3. 在 C:\ directory 中，创建名为“Log”的文件夹。
4. 将 logger.cfg 复制到 “Log” 文件夹。
5. 从 Web 控制台部署数据丢失防护和设备控制设置，以开始收集日志。

注意

通过删除注册表项中的 `debugcfg` 并重新启动终端，来禁用数据保护模块的调试日志记录。

第 11 章

保护计算机免受基于 Web 的威胁

本章介绍基于 Web 的威胁和使用防毒墙网络版保护您的网络和计算机免遭基于 Web 的威胁的攻击。

主题包括：

- 关于 Web 威胁 第 11-2 页
- 命令与控制联系人警报服务 第 11-2 页
- Web 信誉 第 11-4 页
- Web 信誉策略 第 11-4 页
- 可疑连接服务 第 11-12 页
- 客户端用户的 Web 威胁通知 第 11-15 页
- 适用于管理员的 C&C 回调通知 第 11-17 页
- C&C 回呼爆发 第 11-21 页
- Web 威胁日志 第 11-23 页

关于 Web 威胁

Web 威胁包括一系列广泛源自于 Internet 的威胁。Web 威胁的方式非常复杂，使用了各种文件和技术的组合，而非单一的文件或方法。例如，Web 威胁创建者不断更改使用的版本或变种。由于 Web 威胁处于 Web 站点的固定位置，而非在受感染终端上，因此 Web 威胁创建者会不断修改其代码以免被检测到。

近年来，曾经作为黑客、病毒编写者、垃圾邮件制造者和间谍软件制作者出现的个人统称为网络罪犯。Web 威胁可帮助这些人实现以下两个目标之一。一个目标是窃取信息以便后续销售。由此引起的后果是以身份丢失的形式泄漏机密信息。受感染终端还可能成为传递网络钓鱼攻击或其他信息捕捉活动的带毒站点。除了以上影响之外，此威胁还可能腐蚀对 Web 商务的信心，从而破坏 Internet 事务所需的信任。第二个目标是劫持用户的 CPU，并将其用作开展牟利活动的工具。这些活动包括发送垃圾邮件或者以分布式拒绝服务攻击或点击付费活动的形式进行敲诈勒索。

命令与控制联系人警报服务

趋势科技命令与控制 (C&C) 联系人警报服务提供了增强的检测和警报功能，可以减少由高级持续性威胁和针对性攻击导致的损害。C&C 联系人警报服务会与 Web 信誉服务集成，该 Web 信誉服务可根据 Web 信誉安全级别确定对检测到的回呼地址采取的处理措施。

C&C IP 列表可使用网络内容检查引擎通过任何网络通道识别 C&C 联系人，从而进一步增强 C&C 回呼检测。

有关配置 Web 信誉服务安全级别的详细信息，请参阅配置 Web 信誉策略 第 11-5 页。

表 11-1. C&C 联系人警报服务功能

功能	描述
全局情报列表	趋势科技云安全智能防护网络可搜集来自世界各地的全局情报列表，测试并评估每个 C&C 回呼地址的风险等级。Web 信誉服务可将全局情报列表与恶意 Web 站点的信誉分值结合使用，从而提供抵御高级威胁的增强安全性。Web 信誉安全级别可根据分配的风险等级确定对恶意 Web 站点或 C&C 服务器采取的处理措施。
沙盒虚拟平台列表	云安全智能防护服务器可与沙盒虚拟平台集成，以获取沙盒虚拟平台 C&C 服务器列表。沙盒虚拟平台会评估安全环境中的潜在风险，并通过使用高级启发式和行为测试方法向经过分析的威胁分配风险等级。沙盒虚拟平台使用任何尝试连接到可能的 C&C 服务器的威胁来填充沙盒虚拟平台列表。沙盒虚拟平台列表是专门针对公司的，提供了更加个性化的防御，以防止受到针对性攻击的威胁。 防毒墙网络版可从沙盒虚拟平台检索列表，并根据全局情报和本地沙盒虚拟平台列表评估所有可能的 C&C 威胁。 有关连接沙盒虚拟平台可疑对象列表的详细信息，请参阅配置可疑对象列表设置 第 13-29 页。
可疑连接服务	可疑连接服务管理用户定义的全局 IP C&C 列表，并监控终端与可能的 C&C 服务器建立的连接的行为。 有关详细信息，请参阅可疑连接服务 第 11-12 页。
管理员通知	管理员可以选择在检测到 C&C 回呼之后接收详细的可定制通知。 有关详细信息，请参阅为管理员配置 C&C 回呼通知 第 11-17 页。
客户端通知	管理员可以选择在终端上检测到 C&C 回呼之后向最终用户发送详细的可定制通知。 有关详细信息，请参阅针对客户端用户的 C&C 联系人警报通知 第 11-19 页。
爆发通知	管理员可以定制特定于 C&C 回呼事件的爆发通知，并指定是在单个终端上还是整个网络中发生爆发。 有关详细信息，请参阅 C&C 回呼爆发 第 11-21 页。
C&C 回呼日志	日志可以提供有关所有 C&C 回呼事件的详细信息。 有关详细信息，请参阅查看 C&C 回呼日志 第 11-24 页。

Web 信誉

Web 信誉技术跟踪 Web 域的可信度，方法是根据 Web 站点的年龄、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，此技术将继续扫描站点并阻止用户访问受感染站点。

防毒墙网络版客户端向云安全智能防护源发送查询来确定用户尝试访问的 Web 站点的信誉。Web 站点的信誉与终端上实施的特定 Web 信誉策略有关。根据正在使用的策略，防毒墙网络版客户端将阻止或者允许对 Web 站点的访问。

注意

有关云安全智能防护源的详细信息，请参阅云安全智能防护源列表 第 4-21 页。

将认为安全或危险的 Web 站点添加到允许列表或阻止列表。防毒墙网络版客户端检测到对这些 Web 站点的访问时，会自动允许或阻止访问，且不再向云安全智能防护源发送查询。

Web 信誉策略

Web 信誉策略控制防毒墙网络版是阻止还是允许对 Web 站点的访问。

您可以为内部和外部客户端配置策略。防毒墙网络版管理员通常会对外部客户端配置更严格的策略。

策略是防毒墙网络版客户端树中的粒度设置。您可对客户端组或各个客户端强制执行特定策略。也可对所有客户端强制执行一个策略。

部署策略之后，客户端会使用您在**终端位置**窗口（请参阅终端位置 第 14-2 页）中已设置的位置条件来确定其位置和要应用的策略。客户端会在每次位置更改时切换策略。

配置 Web 信誉策略

如果已将代理服务器设置为处理贵组织中的 HTTP 通信，并且在允许 Web 访问之前需要进行认证，请指定代理服务器认证凭证。

有关配置代理服务器设置的说明，请参阅 防毒墙网络版客户端的外部代理服务器 第 14-46 页。

过程

1. 转至**客户端 > 客户端管理**。
2. 在客户端树中选择目标。
   - 要为运行 Windows XP、Vista、7、8、8.1 或 10 的客户端配置策略，请选择根域图标 ()、特定域或客户端。

     注意

     当选择根域或特定域时，设置将仅应用于运行 Windows XP、Vista、7、8、8.1 或 10 的客户端。设置不会应用于运行 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 的客户端，即便它们属于这些域。
   - 要为运行 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 的客户端配置策略，请选择特定客户端。
3. 单击**设置 > Web 信誉设置**。
4. 单击**外部客户端**选项卡为外部客户端配置策略，或单击**内部客户端**选项卡为内部客户端配置策略。

   提示

   配置客户端位置设置（如果尚未执行此操作）。客户端将使用这些设置确定自己的位置，然后应用正确的 Web 信誉策略。有关详细信息，请参阅终端位置 第 14-2 页。
5. 选择**在下列操作系统上启用 Web 信誉策略**。

   窗口中列出的操作系统取决于您在步骤 1 中选定的目标。

提示

如果已将趋势科技产品与 Web 信誉功能（如趋势科技 Web 安全网关）一起使用，趋势科技建议对内部客户端禁用 Web 信誉。

启用 Web 信誉策略时：

- 外部客户端向云安全智能防护网络发送 Web 信誉查询。
- 内部客户端将发送 Web 信誉查询至：
  - 云安全智能防护服务器，如果已启用**向云安全智能防护服务器发送查询**选项。有关此选项的详细信息，请参阅步骤 7。
  - 云安全智能防护网络，如果已禁用**向云安全智能防护服务器发送查询**选项。

6. 选择**启用评估**。

注意

在评估模式下，客户端将允许访问所有 Web 站点，但会记录禁用评估时应阻止的对 Web 站点的访问。趋势科技提供评估模式以允许您评估 Web 站点，然后根据您的评估采取适当的处理措施。例如，可将您认为安全的 Web 站点添加到允许列表。

7. 选择**检查 HTTPS URL**。

HTTPS 通信使用证书来识别 Web 服务器。它对数据进行加密以防止盗窃和窃听。尽管使用 HTTPS 访问 Web 站点更为安全，但仍存在风险。遭受危害的站点即使具有有效证书，仍可以寄存恶意软件并窃取个人信息。另外，证书相对易于获取，因此构建使用 HTTPS 的恶意 Web 服务器变得很容易。

启用检查 HTTPS URL 以减少受到使用 HTTPS 的遭受危害的站点和恶意站点的感染。防毒墙网络版可以在以下浏览器中监控 HTTPS 流量：

表 11-2. 支持 HTTPS 流量的浏览器

浏览器	版本
Microsoft Internet Explorer	• 6（带 SP2）或更高版本 • 7.x • 8.x • 9.x • 10.x • 11.x
Microsoft Edge	无
Mozilla Firefox	3.5 或更高版本
Chrome	无

重要信息

- HTTPS 扫描仅支持在桌面模式下运行的 Windows 8、Windows 8.1、Windows 10 或 Windows 2012 平台。
- 在防毒墙网络版客户端上首次启用 HTTPS 扫描之后，用户必须先在浏览器中启用所需的附加软件，然后才能运行 HTTPS 扫描。
  - Firefox

    对于运行 Windows 7、8、8.1、10、Server 2008 R2 或 Server 2012 的防毒墙网络版客户端，用户必须在浏览器弹出窗口中（或在**附加组件** > **扩展**窗口中）启用 Trend Micro Osprey Firefox Extension 2.0.0.1077 附加组件。

    对于运行 Windows XP、Vista、Server 2003 或 Server 2008 的防毒墙网络版客户端，用户必须在浏览器弹出窗口中（或在**附加组件** > **扩展**窗口中）启用 Trend Micro NSC Firefox Extension 5.82.0.1092 附加组件。
  - Internet Explorer 9、10 和 11

    对于运行 Windows 7、8、8.1、10、Server 2008 R2 或 Server 2012 的防毒墙网络版客户端，用户必须在浏览器弹出窗口中启用 Trend Micro Osprey Plugin Class 附加组件。

    对于运行 Windows XP、Vista、Server 2003 或 Server 2008 的防毒墙网络版客户端，用户必须在浏览器弹出窗口中启用 TmIEPlugInBHO Class 附加组件。

  有关配置 Internet Explorer 中 Web 信誉设置的详细信息，请参阅以下知识库文章：

  - http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionID=72275
  - http://esupport.trendmicro.com/solution/en-us/1095350.aspx

8. 选择**仅扫描通用 HTTP 端口**，可将 Web 信誉扫描限制为通过端口 80、81 和 8080 的网络通信。缺省情况下，防毒墙网络版会扫描通过所有端口的所有网络通信。

注意

在 Windows 7、8、8.1、10 或 Windows Server 2008 R2、2012 或更高版本的平台上不受支持。

9. 如果希望内部客户端向云安全智能防护服务器发送 Web 信誉查询，请选择**向云安全智能防护服务器发送查询**。

- 如果您启用此选项：
  - 客户端参考云安全智能防护源列表，以确定要向其发送查询的云安全智能防护服务器。

    有关云安全智能防护源列表的详细信息，请参阅云安全智能防护源列表 第 4-21 页。
  - 请确保云安全智能防护服务器可用。如果所有云安全智能防护服务器均不可用，则客户端不会向云安全智能防护网络发送查询。适用于客户端的仅有的 Web 信誉数据源是（在步骤 10 中配置的）允许和阻止的 URL 列表。
  - 如果要使用代理服务器将客户端连接到云安全智能防护服务器，请在**管理 > 设置 > 代理服务器 > 内部代理服务器**选项卡中指定代理服务器设置。
  - 请务必定期更新云安全智能防护服务器，以便防护保持最新状态。
  - 客户端将不阻止未经测试的 Web 站点。云安全智能防护服务器不会存储这些 Web 站点的 Web 信誉数据。
- 如果您禁用此选项：
  - 客户端将向云安全智能防护网络发送 Web 信誉查询。客户端计算机必须连接到 Internet 才能成功发送查询。
  - 如果连接到云安全智能防护网络需要代理服务器认证，请在**管理 > 设置 > 代理服务器 > 外部代理服务器（选项卡） > 防毒墙网络版客户端与趋势科技服务器之间的连接**中指定认证凭证。
  - 如果在步骤 11 中选择**阻止尚未经过趋势科技测试的页面**，客户端将阻止未经测试的 Web 站点。

10. 从以下可用的 Web 信誉安全级别中选择：**高**、**中**或**低**

注意

安全级别确定防毒墙网络版是允许还是阻止访问 URL。例如，如果安全级别设置为“低”，则防毒墙网络版将仅阻止已知是 Web 威胁的 URL。随着安全级别设置的增高，Web 威胁检测率会提高，但误报的可能性也会增加。

11. 如果您在步骤 9 中禁用了**向云安全智能防护服务器发送查询**选项，您可以选择**阻止尚未经过趋势科技测试的页面**。

注意

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。

12. 选择**阻止包含恶意脚本的页面**来识别 Web 浏览器漏洞和恶意脚本，并防止使用这些威胁危害 Web 浏览器。

防毒墙网络版利用浏览器漏洞防护特征码和脚本分析器特征码来识别和阻止网页，然后再暴露系统。

表 11-3. 支持浏览器安全漏洞防御的浏览器

浏览器	版本
Microsoft Internet Explorer	• 7.x • 8.x • 9.x • 10.x • 11.x

重要信息

浏览器安全漏洞防御功能要求您启用高级保护服务。

要启用高级保护服务，请转至**客户端** > **客户端管理**，单击**设置** > **其他服务设置**。

首次在防毒墙网络版客户端上启用浏览器安全漏洞防御功能后，用户必须在浏览器中启用所需附加组件，方可运行浏览器安全漏洞防御。对于运行 Internet Explorer 9、10 或 11 的防毒墙网络版客户端，用户必须在浏览器弹出窗口中启用 Trend Micro IE Protection 附加组件。

13. 配置允许列表和阻止列表。

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，客户端始终允许访问它。

a. 选择**启用允许/阻止列表**。

b. 键入 URL。

可以在 URL 中的任意位置添加通配符 (*)。

例如：

- 键入 www.trendmicro.com/* 意味着将允许趋势科技 Web 站点中的所有页面。
- 键入 *.trendmicro.com/* 意味着将允许 trendmicro.com 的任何子域中的所有页面。

可以键入包含 IP 地址的 URL。如果 URL 包含 IPv6 地址，则使用括号将地址括起来。

c. 单击**添加到允许列表**或**添加到阻止列表**。

d. 要将列表导出到 .dat 文件，请单击**导出**，然后单击**保存**。

e. 如果已从其他服务器导出列表，并希望将该列表导入到此窗口，请单击**导入**并找到该 .dat 文件。该列表将加载到窗口中。

重要信息

Web 信誉不对允许和阻止列表中的地址执行任何扫描。

14. 要提交 Web 信誉反馈，请单击**重新评估 URL** 下提供的 URL。将在浏览器窗口中打开趋势科技 Web 信誉查询系统。

15. 选择是否允许防毒墙网络版客户端向服务器发送 Web 信誉日志。如果要分析防毒墙网络版正在阻止的 URL 并要对您认为可以安全访问的 URL 采取相应的处理措施，则允许客户端发送日志。

16. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

    - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
    - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

可疑连接服务

可疑连接服务管理用户定义的全局 IP C&C 列表，并监控终端与可能的 C&C 服务器建立的连接的行为。

- 用户定义的允许和阻止 IP 列表允许进一步控制终端是否可访问特定 IP 地址。想要允许访问全局 C&C IP 列表阻止的地址或阻止访问可能会造成安全风险的地址时，对这些列表进行配置。

  有关详细信息，请参阅配置用户定义的全局 IP 列表设置 第 11-13 页。

- 全局 C&C IP 列表与网络内容检查引擎 (NCIE) 结合使用，以检测与趋势科技确认的 C&C 服务器的网络连接。NCIE 通过任何网络通道检测 C&C 服务器联系人。可疑连接服务在全局 C&C IP 列表中记录服务器的所有连接信息，以用于评估。

  有关启用全局 C&C IP 列表的详细信息，请参阅配置可疑连接设置 第 11-14 页。

- 通过网络数据包的关联规则特征码匹配在终端上检测到恶意软件后，可疑连接服务可以进一步调查连接行为，以确定是否发生了 C&C 回呼。检测 C&C 回呼后，可疑连接服务可以尝试阻止和清除使用 GeneriClean 技术的连接源。

  有关配置可疑连接服务的详细信息，请参阅配置可疑连接设置 第 11-14 页。

  有关 GeneriClean 的详细信息，请参阅 GeneriClean 第 E-4 页。

在**其他服务设置**窗口中启用可疑连接服务，来保护客户端抵御 C&C 服务器回呼。有关详细信息，请参阅从 Web 控制台启用或禁用客户端服务 第 14-7 页。

配置用户定义的全局 IP 列表设置

管理员可以将防毒墙网络版配置为允许、阻止或记录客户端与用户定义的 C&C IP 地址之间的所有连接。

注意

用户定义的 IP 列表仅支持 IPv4 地址。

过程

1. 转至**客户端 > 全局客户端设置**。
2. 转到**可疑连接设置**部分。
3. 单击**编辑用户定义的 IP 列表**。
4. 在**允许列表**或**阻止列表**选项卡上，添加要监控的 IP 地址。

提示

可以将防毒墙网络版配置为仅记录与用户定义的阻止 IP 列表中的地址建立的连接。要仅记录与用户定义的阻止 IP 列表中的地址建立的连接，请参阅配置可疑连接设置 第 11-14 页。

a. 单击**添加**。

b. 在显示的新窗口上，键入要让防毒墙网络版监控的 IP 地址、IP 地址范围或 IPv4 地址和子网掩码。

c. 单击**保存**。

5. 要从列表中移除 IP 地址，请选中地址旁的复选框，然后单击**删除**。

6. 配置列表后，单击**关闭**返回到**全局客户端设置**窗口。

配置可疑连接设置

防毒墙网络版可以记录客户端与全局 C&C IP 列表中地址之间的所有连接。**可疑连接设置**窗口允许您记录和访问在用户定义的阻止 IP 列表中配置的 IP 地址。

防毒墙网络版还可以监控可能引起 BotNet 或其他恶意软件威胁的连接。检测到恶意软件威胁后，防毒墙网络版可以尝试清除感染。

过程

1. 转至**客户端** > **客户端管理**。

2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。

3. 单击**设置** > **可疑连接设置**。

   将显示**可疑连接设置**窗口。

4. 启用**记录全局 C&C IP 列表中地址的网络连接**设置以监控与趋势科技确认的 C&C 服务器建立的连接。

   - 要允许客户端连接到用户定义的阻止 IP 列表中的地址，请启用**记录并允许访问用户定义的阻止 IP 列表地址**设置。

注意

必须先启用网络连接日志记录，防毒墙网络版才能允许访问用户定义的阻止 IP 列表中的地址。

有关全局 C&C IP 列表的详细信息，请参阅可疑连接服务 第 11-12 页。

5. 启用**使用恶意软件网络指纹验证的日志连接**设置以对数据包头执行特征码匹配。防毒墙网络版会使用关联规则特征码来记录数据包头与已知恶意软件威胁匹配的数据包所建立的所有连接。

   - 要允许防毒墙网络版尝试清除与 C&C 服务器建立的连接，请启用**检测到 C&C 回呼时清除可疑连接**设置。防毒墙网络版会使用 GeneriClean 来清除恶意软件威胁，并终止与 C&C 服务器的连接。

注意

必须先启用**使用恶意软件网络指纹验证的日志连接**，防毒墙网络版才能尝试清除与数据包结构匹配所检测到的 C&C 服务器建立的连接。

6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

客户端用户的 Web 威胁通知

防毒墙网络版在阻止违反 Web 信誉策略的 URL 后，可以立即在防毒墙网络版客户端终端上显示一条通知消息。需要启用通知消息并可选择修改通知消息的内容。

启用 Web 威胁通知消息

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡。
5. 在 **Web 信誉设置**部分中，选择**阻止 Web 站点时显示通知**。
6. 在 **C&C 回呼设置**部分中，选择**检测到 C&C 回呼时显示通知**。
7. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改 Web 威胁通知

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择要修改的 Web 威胁通知类型：
   - **Web 信誉违例**
   - **C&C 回呼**

3. 在提供的文本框中修改缺省消息。
4. 单击**保存**。

适用于管理员的 C&C 回调通知

防毒墙网络版附带有一组缺省通知消息，用于通知您和其他防毒墙网络版管理员 C&C 回调检测。您可以根据需要修改通知和配置其他通知设置。

为管理员配置 C&C 回呼通知

过程

1. 转至**管理** > **通知** > **管理员**。
2. 在**条件**选项卡上：
   a. 转至 **C&C 回呼**部分。
   b. 指定是在防毒墙网络版检测到 C&C 回呼（处理措施可以是阻止或记录）时发送通知，还是仅在回呼地址的风险等级为“高”时才发送通知。
3. 在**电子邮件**选项卡上：
   a. 转至 **C&C 回呼**部分。
   b. 选择**启用电子邮件通知**。
   c. 选择**向拥有客户端树域权限的用户发送通知**。

      使用基于角色的管理授予用户客户端树域权限。如果属于特定域的任何客户端上发生传输，则会向具有域权限的用户的电子邮件地址发送电子邮件。有关示例，请参阅下表：

表 11-4. 客户端树域和权限

客户端树域	具有域权限的角色	具有该角色的用户帐户	用户帐户的电子邮件地址
域 A	Administrator (内置)	根	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
域 B	Administrator (内置)	根	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果属于域 A 的任何防毒墙网络版客户端检测到 C&C 回呼，则会向 mary@xyz.com、john@xyz.com 和 chris@xyz.com 发送电子邮件。

如果属于域 B 的任何防毒墙网络版客户端检测到 C&C 回呼，则会向 mary@xyz.com 和 jane@xyz.com 发送电子邮件。

注意

如果启用此选项，具有域权限的所有用户都必须具有相应的电子邮件地址。不会向没有电子邮件地址的用户发送电子邮件通知。用户和电子邮件地址是从**管理** > **帐户管理** > **用户帐户**进行配置的。

d. 选择**向以下电子邮件地址发送通知**，然后键入电子邮件地址。

e. 接受或修改缺省的主题和消息。使用标记变量表示**主题**和**消息**文本框中的数据。

表 11-5. C&C 回呼通知的标记变量

变量	描述
%CLIENTCOMPUTER%	发送回呼的目标终端
%IP%	目标终端的 IP 地址
%DOMAIN%	计算机的域

变量	描述
%DATETIME%	检测到传输的日期和时间
%CALLBACKADDRESS%	C&C 服务器的回呼地址
%CNCRISKLEVEL%	C&C 服务器的风险等级
%CNCLISTSOURCE%	表示 C&C 源列表
%ACTION%	采取的措施

4. 在 **SNMP Trap** 选项卡上：
   a. 转至 **C&C 回呼**部分。
   b. 选择**启用 SNMP 陷阱通知**。
   c. 接受或修改缺省消息。使用标记变量表示**消息**文本框中的数据。请参阅 表 11-5：C&C 回呼通知的标记变量 第 11-18 页 以了解详细信息。
5. 在 **NT 事件日志**选项卡上：
   a. 转至 **C&C 回呼**部分。
   b. 选择**启用 NT 事件日志通知**。
   c. 接受或修改缺省消息。可以使用标记变量表示**消息**文本框中的数据。请参阅 表 11-5：C&C 回呼通知的标记变量 第 11-18 页 以了解详细信息。
6. 单击**保存**。

针对客户端用户的 C&C 联系人警报通知

防毒墙网络版可以在阻止 C&C 服务器 URL 后，立即在防毒墙网络版客户端计算机上显示一条通知消息。需要启用通知消息并可选择修改通知消息的内容

启用 C&C 回调通知消息

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡。
5. 在 **C&C 回调设置**部分中，选择**检测到 C&C 回调时显示通知**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改 C&C 回呼通知

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择 **C&C 回呼**。
3. 在提供的文本框中修改缺省消息。
4. 单击**保存**。

C&C 回呼爆发

按回呼的数量、源和风险等级定义 C&C 回呼爆发。

防毒墙网络版具有缺省通知消息，可在检测到爆发时，通知您和其他防毒墙网络版管理员。您可以根据需要修改通知消息。

注意

防毒墙网络版可以通过电子邮件发送 C&C 回呼爆发通知。配置电子邮件设置，让防毒墙网络版可以成功地发送电子邮件。有关详细信息，请参阅管理员通知设置 第 13-32 页。

配置 C&C 回呼爆发条件和通知

过程

1. 转至**管理** > **通知** > **爆发**。
2. 在**条件**选项卡上，配置以下选项：

选项	说明
同一台遭受危害的主机	选择该选项**以根据每个**终端的回呼检测**次数来定**义**爆**发
C&C 风险等级	**指定是**对**所有** C&C **回呼触**发**爆**发还**是**仅对**高**风险**源触**发**爆**发
处**理措施**	**从任何处理措施、记录或阻止**中进行选择
检测	**表示定**义**爆**发**所需的**检测**次数**
时间**段**	**表示必**须发**生**检测**的小**时**数**

提示

趋势科技建议接受此窗口中的缺省值。

3. 在**电子邮件**选项卡中：

   a. 转至 **C&C 回呼**部分。

   b. 选择**启用电子邮件通知**。

   c. 指定电子邮件收件人。

   d. 接受或修改缺省的电子邮件主题和消息。可以使用标记变量表示**主题**和**消息**文本框中的数据。

   表 11-6. C&C 回呼爆发通知的标记变量

变量	描述
%C	C&C 回呼日志的数量
%T	C&C 回呼日志的累计时长

   e. 选择要包括在电子邮件中的其他可用 C&C 回呼信息。

4. 在 **SNMP 陷阱**选项卡中：

   a. 转至 **C&C 回呼**部分。

   b. 选择**启用 SNMP 陷阱通知**。

   c. 接受或修改缺省消息。可以使用标记变量表示**消息**文本框中的数据。请参阅表 11-6：C&C 回呼爆发通知的标记变量 第 11-22 页以了解详细信息。

5. 在 **NT 事件日志**选项卡中：

   a. 转至 **C&C 回呼**部分。

   b. 选择**启用 NT 事件日志通知**。

   c. 接受或修改缺省消息。可以使用标记变量表示**消息**文本框中的数据。请参阅表 11-6：C&C 回呼爆发通知的标记变量 第 11-22 页以了解详细信息。

6. 单击**保存**。

Web 威胁日志

配置内部和外部客户端，以将 Web 信誉日志发送给服务器。如果想要分析防毒墙网络版阻止的 URL 并对您认为可以安全访问的 URL 采取适当处理措施，请执行此操作。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看 Web 信誉日志

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。
3. 单击**查看日志** > **Web 信誉日志**或单击**日志** > **Web 信誉日志**。
4. 指定日志条件，然后单击**显示日志**。
5. 查看日志。日志包含以下信息：

项	描述
日期/时间	发生检测的时间
终端	发生检测的终端
域	发生检测的终端的域
URL	Web 信誉服务阻止的 URL
风险等级	URL 的风险等级
描述	安全威胁的描述
进程	尝试进行联系所利用的进程（路径\应用程序名称）

项	描述
处理措施	对检测采取的处理措施

6. 如果存在不应阻止的 URL，单击**添加到允许列表**按钮可将 Web 站点添加到允许的 URL 列表。

7. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**将所有内容导出为 CSV 格式**。打开文件或将其保存到特定位置。

查看 C&C 回呼日志

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。

2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。

3. 单击**查看日志** > **C&C 回呼日志**或**日志** > **C&C 回呼日志**。

4. 指定日志条件，然后单击**显示日志**。

5. 查看日志。日志包含以下信息：

项	描述
日期/时间	发生检测的时间
用户	检测时登录的用户
遭受危害的主机	最初发生回呼的终端
IP 地址	遭受危害的主机的 IP 地址
域	发生检测的终端的域
回呼地址	终端将回呼发送到的地址

项	描述
C&C 列表来源	识别 C&C 服务器的 C&C 列表来源
C&C 风险等级	C&C 服务器的风险等级
协议	用于传输的 Internet 协议
进程	启动传输的进程（路径\应用程序名称）
处理措施	对回呼采取的处理措施

6. 如果 Web 信誉阻止了您不想阻止的 URL，可单击**添加到 Web 信誉允许列表**按钮将该地址添加到 Web 信誉允许列表。

注意

防毒墙网络版只能将 URL 添加到 Web 信誉允许列表。对于按全局 C&C IP 列表或沙盒虚拟平台 (IP) C&C 列表进行的检测，请手动将这些 IP 地址添加到用户定义的允许 C&C IP 列表。

有关详细信息，请参阅配置用户定义的全局 IP 列表设置 第 11-13 页。

7. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**将所有内容导出为 CSV 格式**。打开文件或将其保存到特定位置。

查看可疑连接日志

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。
3. 单击**查看日志** > **可疑连接日志**或**日志** > **可疑连接日志**。
4. 指定日志条件，然后单击**显示日志**。

5. 查看日志。日志包含以下信息：

项	描述
日期/时间	发生检测的时间
终端	发生检测的终端
域	发生检测的终端的域
进程	启动传输的进程（路径\应用程序名称）
本地 IP 和端口	源终端的 IP 地址和端口号
远程 IP 和端口	目标终端的 IP 地址和端口号
结果	所采取处理措施的结果
检测者	识别 C&C 服务器的 C&C 列表来源
网络通信方向	传输的方向

6. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**将所有内容导出为 CSV 格式**。打开文件或将其保存到特定位置。

第 12 章

使用防毒墙网络版防火墙

本章介绍防毒墙网络版防火墙功能和配置。

主题包括：

- 关于防毒墙网络版防火墙 第 12-2 页
- 启用或禁用防毒墙网络版防火墙 第 12-6 页
- 防火墙策略和概要文件 第 12-7 页
- 防火墙权限 第 12-21 页
- 全局防火墙设置 第 12-23 页
- 向防毒墙网络版客户端用户发送的防火墙违例通知 第 12-25 页
- 防火墙日志 第 12-26 页
- 防火墙违例爆发 第 12-28 页
- 测试防毒墙网络版防火墙 第 12-29 页

关于防毒墙网络版防火墙

防毒墙网络版防火墙使用基于状态的检查和高性能的网络病毒扫描来保护网络上的客户端和服务器。通过中央管理控制台，可以创建按应用程序、IP 地址、端口号或协议过滤连接的规则，然后将这些规则应用到不同的用户组中。



注意

可以在启用 Windows 防火墙的 Windows XP 终端上启用、配置和使用防毒墙网络版防火墙。但是，必须仔细管理策略以避免创建有冲突的防火墙策略和产生意外结果。有关 Windows 防火墙的详细信息，请参阅 Microsoft 文档。

防毒墙网络版防火墙包括以下主要功能和优点：

- 网络通信过滤 第 12-2 页
- 应用程序过滤 第 12-3 页
- 安全软件认证列表 第 12-3 页
- 扫描网络病毒 第 12-4 页
- 可定制的概要文件和策略 第 12-4 页
- 基于状态的检查 第 12-4 页
- 入侵检测系统 第 12-4 页
- 防火墙违例爆发监控 第 12-5 页
- 防毒墙网络版客户端防火墙权限 第 12-6 页

网络通信过滤

防毒墙网络版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
- 源和目标终端

应用程序过滤

防毒墙网络版防火墙对特定应用程序中的传入和传出流量进行过滤，以允许这些应用程序访问网络。但是，网络连接将取决于管理员设置的策略。

注意

防毒墙网络版不支持 Windows 8、Windows 8.1、Windows 10 和 Windows Server 2012 平台上的特定应用程序例外。防毒墙网络版允许或拒绝具有这些平台的终端上的所有应用程序通信。

安全软件认证列表

安全软件认证列表提供可绕开防火墙策略安全级别的应用程序的列表。如果将安全级别设置为“中”或“高”，则防毒墙网络版仍将允许应用程序运行并访问网络。

对提供更完整列表的全局安全软件认证列表启用查询。这是一个由趋势科技动态更新的列表。

注意

此功能可与行为监控配合使用。请确保先启用未授权更改阻止服务和安全软件认证服务，然后再启用全局安全软件认证列表。

扫描网络病毒

防毒墙网络版防火墙还会在每个数据包中查找是否有网络病毒。有关详细信息，请参阅病毒和恶意软件 第 7-2 页。

可定制的概要文件和策略

防毒墙网络版防火墙让您可以配置策略以阻止或允许指定类型的网络通信。将策略分配到一个或多个概要文件，然后可将这些概要文件部署到指定的防毒墙网络版客户端。这提供了一种高度定制的为客户端组织和配置防火墙设置的方法。

基于状态的检查

防毒墙网络版防火墙是基于状态进行检查的防火墙；它会监控与防毒墙网络版客户端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。

入侵检测系统

防毒墙网络版 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防毒墙网络版客户端的攻击的特征码。防毒墙网络版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 数据包定向到目标终端。这会导致终端缓存溢出，从而使终端死机或重新启动。
Ping of Death	拒绝服务攻击，黑客将特大的 ICMP/ICMPv6 数据包定向到目标终端。这会导致终端缓存溢出，从而使终端死机或重新启动。

入侵	描述
Conflicted ARP	一种攻击类型，黑客会向目标终端发送带有相同源和目标 IP 地址的地址解析协议 (ARP) 请求。目标终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) 数据包发送到终端，从而导致终端持续发送同步应答 (SYN/ACK) 响应。这可能会耗尽终端内存并最终使终端崩溃。
Overlapping Fragment	与 Teardrop 攻击相似，这种拒绝服务攻击会向终端发送重叠的 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，到达目标终端。
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终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，向目标终端发送被分割的 IGMP 数据包，导致无法正确处理 IGMP 数据包。这会使终端死机或运行速度减慢。
LAND Attack	一种攻击类型，向终端发送带有相同源地址和目标地址的 IP 同步 (SYN) 数据包，导致终端向自身发送同步应答 (SYN/ACK) 响应。这会使终端死机或运行速度减慢。

防火墙违例爆发监控

防火墙违例超出特定阈值（可能意味着发生攻击）时，防毒墙网络版防火墙会向指定收件人发送定制的通知消息。

防毒墙网络版客户端防火墙权限

授予防毒墙网络版客户端用户在防毒墙网络版客户端控制台上查看其防火墙设置的权限。还授予用户启用或禁用防火墙、入侵检测系统和防火墙违例通知消息的权限。

启用或禁用防毒墙网络版防火墙

在安装防毒墙网络版服务器期间，系统会提示您启用或禁用防毒墙网络版防火墙。

如果在安装期间已启用防火墙，并发现性能受到影响（特别是在 Windows Server 2003、Windows Server 2008 和 Windows Server 2012 服务器平台上），请考虑禁用防火墙。

如果已在安装期间禁用防火墙，但想要启用防火墙以保护客户端免于遭受入侵，请先阅读防毒墙网络版客户端服务 第 14-6 页中的指导方针和说明。

可以启用或禁用所有或选定防毒墙网络版客户端终端上的防火墙。

启用或禁用选定终端上的防毒墙网络版防火墙

在 Web 控制台上使用以下方法之一启用或禁用防火墙。

方法	过程
创建一项新策略，并将它应用于防毒墙网络版客户端	1. 创建可启用/禁用防火墙的新策略。有关创建新策略的步骤，请参阅添加或修改防火墙策略 第 12-10 页。 2. 将该策略应用于防毒墙网络版客户端。

方法	过程
从 Web 控制台启用/禁用防火墙服务。	有关详细步骤，请参阅防毒墙网络版客户端服务 第 14-6 页。 **注意** 禁用防火墙服务会自动禁用选定客户端上的所有防火墙策略。

在选定的终端上使用以下方法之一启用或禁用防火墙。

方法	过程
启用/禁用防火墙驱动程序	1. 打开 **Windows 网络连接属性**。 2. 从网卡中选择或清除**趋势科技通用防火墙驱动程序**复选框。
启用/禁用防火墙服务	1. 打开命令提示符，然后键入 `services.msc`。 2. 从 Microsoft 管理控制台 (MMC) 启动或停止**防毒墙网络版 NT 防火墙**。

启用或禁用所有终端上的防毒墙网络版防火墙

过程

1. 转至**管理** > **设置** > **产品使用授权**。
2. 转至**其他服务**部分。
3. 在**其他服务**部分，在**终端的防火墙**行旁边，单击**启用**或**禁用**。

防火墙策略和概要文件

防毒墙网络版防火墙使用策略和概要文件来组织和定制保护联网终端的方法。

借助 Active Directory 集成和基于角色的管理，每个用户角色均可根据权限来创建、配置或删除特定域的策略和概要文件。

提示

在同一个终端上安装多个防火墙可能会产生意外的结果。请考虑在部署和启用防毒墙网络版防火墙前先卸载防毒墙网络版客户端上其他基于软件的防火墙应用程序。

下列步骤是成功使用防毒墙网络版防火墙所必需的步骤：

1. 创建策略。该策略允许您选择一个安全级别，该级别可阻止或允许联网终端上的网络通信和启用防火墙功能。
2. 将例外添加到该策略。例外允许防毒墙网络版客户端背离策略。使用例外可以指定客户端以及允许或阻止特定类型的网络通信，而不管策略中的安全级别设置。例如，在一个策略中阻止一组客户端的所有网络通信，但是创建一个允许 HTTP 网络通信的例外以便客户端可以访问 Web 服务器。
3. 创建概要文件并将其分配到防毒墙网络版客户端。防火墙概要文件包括一组客户端属性且与策略关联。当客户端与在概要文件中指定的属性相匹配时，将触发关联的策略。

防火墙策略

通过防火墙策略，您可以阻止或允许在策略例外中未指定的某些网络通信类型。策略还定义启用或禁用哪些防火墙功能。将策略分配到一个或多个防火墙概要文件。

防毒墙网络版附带有一组缺省策略，可以修改或删除这些策略。

借助 Active Directory 集成和基于角色的管理，每个用户角色均可根据权限来创建、配置或删除特定域的策略。

下表列出了缺省防火墙策略。

表 12-1. 缺省防火墙策略

策略名称	安全级别	客户端设置	例外	建议使用
所有访问	低	启用防火墙	无	用于允许客户端无限制访问网络
适用于趋势科技防毒墙控制管理中心的通信端口	低	启用防火墙	允许通过端口 80 和 10319 的所有传入和传出 TCP/UDP 网络通信	客户端安装有 MCP 代理时使用
防毒墙群件版 for Microsoft Exchange 控制台	低	启用防火墙	允许通过端口 16372 的所有传入和传出 TCP 网络通信	客户端需要访问防毒墙群件版控制台时使用
趋势科技防毒墙邮件安全版控制台	低	启用防火墙	允许通过端口 80 的所有传入和传出 TCP 网络通信	客户端需要访问 IMSS 控制台时使用

如果具有所有缺省策略都未包括的要求，则另外创建新策略。

所有缺省的和用户创建的防火墙策略都显示在 Web 控制台上的防火墙策略列表中。

配置防火墙策略列表

过程

1. 转至**客户端** > **防火墙** > **策略**。
2. 要添加新策略，请单击**添加**。

   如果要创建的新策略具有与现有策略类似的设置，请选择现有策略，然后单击**复制**。要编辑现有策略，请单击策略名称。

   将显示策略配置窗口。请参阅添加或修改防火墙策略 第 12-10 页以获取详细信息。
3. 要删除现有策略，请选中策略旁的复选框，然后单击**删除**。

4. 要编辑防火墙例外模板，请单击**编辑例外模板**。

   请参阅编辑防火墙例外模板 第 12-12 页以获取详细信息。

   将显示“例外模板编辑器”。

添加或修改防火墙策略

为每项策略配置以下内容：

- **安全级别**：一种常规设置，阻止或允许防毒墙网络版客户端 终端上的所有入站和/或所有出站网络通信。
- **防火墙功能**：指定启用还是禁用防毒墙网络版防火墙、入侵检测系统 (IDS) 和防火墙违例通知消息。有关 IDS 的详细信息，请参阅入侵检测系统 第 12-4 页。
- **安全软件认证列表**：指定是否允许经过认证的安全应用程序连接到网络。有关安全软件认证列表的详细信息，请参阅安全软件认证列表 第 12-3 页。
- **策略例外列表**：用于阻止或允许各种类型的网络通信的可配置例外列表。

添加防火墙策略

过程

1. 转至**客户端** > **防火墙** > **策略**。
2. 要添加新策略，请单击**添加**。

   如果要创建的新策略具有与现有策略类似的设置，请选择现有策略，然后单击**复制**。
3. 键入策略的名称。
4. 选择安全级别。

   选定的安全级别将不会应用到符合防火墙策略例外条件的网络通信。

5. 选择要用于策略的防火墙功能。

   - 防火墙阻止传出数据包时，将显示防火墙违例通知消息。要修改该消息，请参阅修改防火墙通知消息的内容 第 12-26 页。
   - 如果管理员启用了所有防火墙功能并授予防毒墙网络版客户端用户配置防火墙设置的权限，那么用户就可以在防毒墙网络版客户端控制台中启用/禁用功能并修改防火墙设置。

     警告!

     无法使用防毒墙网络版 Web 控制台来覆盖用户配置的防毒墙网络版客户端控制台设置。

   - 如果不启用上述功能，则从防毒墙网络版 Web 控制台中配置的防火墙设置将显示在防毒墙网络版客户端控制台上的**网卡列表**下面。
   - 防毒墙网络版客户端控制台**防火墙**选项卡**设置**下的信息始终反映从防毒墙网络版客户端控制台配置的设置，而不反映从服务器 Web 控制台配置的设置。

6. 启用本地或全局安全软件认证列表。

   注意

   请确保先启用未授权更改阻止服务和安全软件认证服务，然后再启用此服务。

7. 在例外下，选择防火墙策略例外。这里所包含的策略例外是基于防火墙例外模板创建的。请参阅编辑防火墙例外模板 第 12-12 页以了解详细信息。

   - 通过单击策略例外名称并更改所打开的页面中的设置来修改现有策略例外。

     注意

     修改后的策略例外将仅适用于要创建的策略。如果希望该策略例外修改成为永久性的，则需要对防火墙例外模板中的策略例外做同样的修改。

   - 单击**添加**以创建新的策略例外。在打开的页面中指定设置。

注意

该策略例外同样仅适用于要创建的策略。要将此策略例外应用到其他策略，您需要先将其添加到防火墙例外模板中的策略例外列表。

8. 单击**保存**。

修改现有防火墙策略

过程

1. 转至**客户端** > **防火墙** > **策略**。
2. 单击某个策略。
3. 修改以下内容：
   - 策略名称
   - 安全级别
   - 用于策略的防火墙功能
   - 安全软件认证服务列表状态
   - 要包含在策略中的防火墙策略例外
     - 编辑现有策略例外（单击策略例外名称和更改打开的页面中的设置）。
     - 单击**添加**以创建新的策略例外。在打开的页面中指定设置。
4. 单击**保存**将修改应用到现有策略。

编辑防火墙例外模板

防火墙例外模板包含可根据防毒墙网络版客户端终端的端口号和 IP 地址配置以允许或阻止不同类型网络通信的策略例外。创建策略例外后，编辑策略例外要应用的策略。

确定要使用的策略例外类型。有两种类型：

- **限定**

  仅阻止指定类型的网络通信，适用于允许所有网络通信的策略。使用限定策略例外的一个示例是阻止易受攻击的防毒墙网络版客户端端口，如特洛伊木马经常使用的端口。

- **许可**

  仅允许指定类型的网络通信，适用于阻止所有网络通信的策略。例如，您可能要允许防毒墙网络版客户端仅访问防毒墙网络版服务器和 Web 服务器。要执行此操作，请允许来自于可信端口（用以与防毒墙网络版服务器通信的端口）和防毒墙网络版客户端用于 HTTP 通信的端口的网络通信。

  防毒墙网络版客户端侦听端口：**客户端** > **客户端管理** > **状态**。端口号在**基本信息**下。

  服务器侦听端口：**管理** > **设置** > **客户端连接**。端口号在**客户端连接设置**下。

  防毒墙网络版附带有一组缺省防火墙策略例外，可以修改或删除这些例外。

表 12-2. 缺省防火墙策略例外

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

例外名称	处理措施	协议	端口	方向
POP3	允许	TCP	110	传入和传出
LDAP	允许	TCP/UDP	389	传入和传出

注意

缺省例外适用于所有客户端。如果希望缺省例外仅适用于某些客户端，请编辑该例外并指定客户端的 IP 地址。

如果从先前的防毒墙网络版版本升级，则 LDAP 例外不可用。如果在例外列表上没有看到此例外，请手动添加。

添加防火墙策略例外

过程

1. 转至**客户端** > **防火墙** > **策略**。
2. 单击**编辑例外模板**。
3. 单击**添加**。
4. 键入策略例外的名称。
5. 选择应用程序类型。您可以选择所有应用程序，也可以指定应用程序路径或注册表项。

   注意

   请验证输入的名称和完整路径。应用程序例外不支持通配符。

6. 选择防毒墙网络版将对网络通信执行的操作（阻止或允许满足例外条件的网络通信）和网络通信方向（防毒墙网络版客户端 终端上的入站或出站网络通信）。
7. 选择网络协议的类型：TCP、UDP、ICMP 或 ICMPv6。

8. 指定防毒墙网络版客户端 终端上用于执行操作的端口。

9. 选择要包括在例外中的防毒墙网络版客户端终端 IP 地址。例如，如果您选择拒绝所有网络通信（入站和出站）并键入网络中的单个终端的 IP 地址，则在策略中包含有此例外的任一防毒墙网络版客户端都将无法向该 IP 地址发送数据或从该 IP 地址接收数据。

   - **所有 IP 地址**：包括所有 IP 地址
   - **单个 IP 地址**：键入 IPv4 或 IPv6 地址，或键入主机名。
   - **范围（对于 IPv4 或 IPv6）**：键入 IPv4 或 IPv6 地址范围。
   - **范围（对于 IPv6）**：键入 IPv6 地址前缀和长度。
   - **子网掩码**：键入 IPv4 地址和其子网掩码。

10. 单击**保存**。

修改防火墙策略例外

过程

1. 转至**客户端** > **防火墙** > **策略**。
2. 单击**编辑例外模板**。
3. 单击某个策略例外。
4. 修改以下内容：
   - 策略例外名称
   - 应用程序类型、名称或路径
   - 防毒墙网络版将对网络通信执行的操作和网络通信方向
   - 网络协议的类型
   - 策略例外的端口号

- 防毒墙网络版客户端终端 IP 地址

5. 单击**保存**。

保存策略例外列表设置

过程

1. 转至**客户端** > **防火墙** > **策略**。
2. 单击**编辑例外模板**。
3. 单击以下保存选项之一：
   - **保存模板更改**：保存带有当前策略例外和设置的例外模板。此选项仅将该模板应用于在将来创建的策略，而不是现有的策略。
   - **保存并应用到现有策略上**：保存带有当前策略例外和设置的例外模板。此选项将该模板应用于现有和将来的策略。

防火墙概要文件

防火墙概要文件具有灵活性，允许您在应用策略前选择一个客户端或一组客户端必须具有的属性。创建可以创建、配置或删除特定域的概要文件的用户角色。

使用内置管理员帐户的用户或具有完全管理权限的用户还可以启用**覆盖客户端安全级别/例外列表**选项以使用服务器设置替换防毒墙网络版客户端概要文件设置。

概要文件包括以下内容：

- **关联的策略**：每个概要文件都使用一个策略
- **客户端属性**：带有一个或多个以下属性的防毒墙网络版客户端应用关联的策略：

- **IP 地址**：具有特定 IP 地址，其 IP 地址在某个 IP 地址范围内，或者其 IP 地址属于特定子网的任何防毒墙网络版客户端
- **域**：属于特定防毒墙网络版域的任何防毒墙网络版客户端
- **终端**：带有特定终端名的防毒墙网络版客户端
- **平台**：运行特定平台的任何防毒墙网络版客户端
- **登录名**：指定的用户已登录到的防毒墙网络版客户端终端
- **NIC 描述**：包含匹配的 NIC 描述的任何防毒墙网络版客户端终端
- **客户端连接状态**：防毒墙网络版客户端是联机还是脱机



注意

如果防毒墙网络版客户端可以连接到防毒墙网络版或任一参考服务器，则防毒墙网络版客户端处于联机状态；如果防毒墙网络版客户端无法连接到任何服务器，则防毒墙网络版客户端处于脱机状态。

防毒墙网络版附带有一个名为?所有客户端概要文件?的缺省概要文件，此概要文件使用?所有访问?策略。可以修改或删除此缺省概要文件。也可以创建新的概要文件。所有缺省的和用户创建的防火墙概要文件（包括与每个概要文件关联的策略和当前概要文件状态）都显示在 Web 控制台上的防火墙概要文件列表中。管理概要文件列表并将所有概要文件部署到防毒墙网络版客户端。防毒墙网络版客户端将所有防火墙概要文件存储在客户端 终端中。

配置防火墙概要文件列表

过程

1. 转至**客户端** > **防火墙** > **概要文件**。
2. 对于使用内置管理员帐户的用户或具有完全管理权限的用户，也可以启用**覆盖客户端安全级别/例外列表**选项以使用服务器设置替换防毒墙网络版客户端概要文件设置。
3. 要添加新的概要文件，请单击**添加**。要编辑现有概要文件，请选择概要文件名称。

将显示概要文件配置窗口。请参阅添加和编辑防火墙概要文件 第 12-19 页获取详细信息。

4. 要删除现有策略，请选中策略旁的复选框，然后单击**删除**。

5. 要更改概要文件在列表中的顺序，请选中要移动的概要文件旁的复选框，然后单击**上移**或**下移**。

   防毒墙网络版会按照概要文件在列表中显示的顺序将防火墙概要文件应用到防毒墙网络版客户端。例如，如果客户端与第一个概要文件匹配，则防毒墙网络版会将为该概要文件配置的处理措施应用到该客户端。防毒墙网络版将忽略为该客户端配置的其他概要文件。

   提示

   将排他性最强的策略放在列表顶部，这样效果最好。例如，将为单个客户端创建的策略移动到顶部，接下来才是为一系列客户端、网络域和所有客户端创建的策略。

6. 要管理参考服务器，请单击**编辑参考服务器列表**。参考服务器是在防毒墙网络版服务器应用防火墙概要文件时作为其替换服务器的终端。参考服务器可以是网络上的任何终端（请参阅参考服务器 第 13-30 页获取详细信息）。当启用参考服务器时，防毒墙网络版做以下假设：

   - 即使客户端无法与防毒墙网络版服务器通信，连接到参考服务器的防毒墙网络版客户端也处于联机状态。
   - 应用到联机防毒墙网络版客户端的防火墙概要文件也适用于连接到参考服务器的防毒墙网络版客户端。

   注意

   只有使用内置管理员帐户的用户或那些具有完全管理权限的用户可以查看和配置参考服务器列表。

7. 保存当前设置并将概要文件分配给防毒墙网络版客户端：

   a. 选择是否要**覆盖客户端安全等级/例外列表**。此选项将覆盖所有用户配置的防火墙设置。

   b. 单击**向客户端分配概要文件**。防毒墙网络版会将概要文件列表中的所有概要文件分配给所有防毒墙网络版客户端。

8. 验证是否将概要文件成功分配给防毒墙网络版客户端：

   a. 转至**客户端** > **客户端管理**。在客户端树视图下拉框中，选择**防火墙视图**。

   b. 请确保在客户端树中的**防火墙**列下有绿色复选标记。如果与概要文件关联的策略启用入侵检测系统，则在 **IDS** 列下还存在绿色复选标记。

   c. 验证客户端是否应用了正确的防火墙策略。该策略在客户端树中的**防火墙策略**列下显示。

添加和编辑防火墙概要文件

防毒墙网络版客户端终端可能需要不同级别的防护。防火墙概要文件允许您指定关联策略应用到的客户端 终端。通常，每个正在使用的策略都需要一个概要文件。

添加防火墙概要文件

过程

1. 转至**客户端** > **防火墙** > **概要文件**。
2. 单击**添加**。
3. 单击**启用该概要文件**以允许防毒墙网络版将该概要文件部署到防毒墙网络版客户端。
4. 键入名称以识别该概要文件和可选描述。
5. 选择此概要文件的策略。
6. 指定防毒墙网络版要应用该策略的客户端 终端。根据以下条件选择终端：
   - IP 地址
   - 单击按钮打开客户端树，并从中选择域。

注意

只有具有完全域权限的用户可以选择域。

- 终端名称：单击按钮打开客户端树，并从中选择防毒墙网络版客户端终端。
- 平台
- 登录名
- NIC 描述：键入完整或部分描述，不使用通配符。

提示

趋势科技建议键入 NIC 卡制造商，因为 NIC 描述通常以制造商的名称开头。例如，如果您键入的是 "Intel"，则所有 Intel 制造的 NIC 都将符合条件。如果您键入的是特殊的 NIC 型号，如 "Intel(R) Pro/100"，则只有以 "Intel(R) Pro/100" 开头的 NIC 描述才符合条件。

- 客户端连接状态

7. 单击**保存**。

修改防火墙概要文件

过程

1. 转至**客户端** > **防火墙** > **概要文件**。
2. 单击某个概要文件。
3. 单击**启用该概要文件**以允许防毒墙网络版将该概要文件部署到防毒墙网络版客户端。修改以下内容：
   - 概要文件名称和描述
   - 分配给概要文件的策略
   - 防毒墙网络版客户端根据以下条件选择终端：

- IP 地址
- 域：单击按钮打开客户端树，并从中选择域。
- 终端名称：单击按钮打开客户端树，并从中选择客户端终端。
- 平台
- 登录名
- NIC 描述：键入完整或部分描述，不使用通配符。



提示

趋势科技建议键入 NIC 卡制造商，因为 NIC 描述通常以制造商的名称开头。例如，如果您键入的是 "Intel"，则所有 Intel 制造的 NIC 都将符合条件。如果您键入的是特殊的 NIC 型号，如 "Intel(R) Pro/100"，则只有以 "Intel(R) Pro/100" 开头的 NIC 描述才符合条件。

- 客户端连接状态

4. 单击**保存**。

防火墙权限

允许用户配置自己的防火墙设置。所有用户配置的设置都不能被从防毒墙网络版服务器部署的设置所覆盖。例如，如果用户禁用了“入侵检测系统 (IDS)”，而您在防毒墙网络版服务器上启用了 IDS，则 IDS 在防毒墙网络版客户端终端上仍然是禁用的。

启用下列设置以允许用户配置防火墙。

表 12-3. 防火墙权限

权限	描述
在防毒墙网络版客户端控制台上显示防火墙设置	**防火墙**选项显示防毒墙网络版客户端上的所有防火墙设置。
允许用户启用/禁用防火墙、入侵检测系统及防火墙违例通知消息	防毒墙网络版防火墙使用基于状态的检查、高性能的网络病毒扫描和清除来保护网络上的客户端和服务器。如果授予用户启用或禁用该防火墙及其功能的权限，则警告他们不要长时间禁用该防火墙以避免终端遭到入侵和黑客的攻击。 如果不授予用户这些权限，则从防毒墙网络版服务器 Web 控制台配置的防火墙设置将显示在防毒墙网络版客户端控制台上的网卡列表下。
允许客户端向防毒墙网络版服务器发送防火墙日志	选择此选项分析防毒墙网络版防火墙阻止和允许的网络通信。 有关防火墙日志的详细信息，请参阅防火墙日志 第 12-26 页。 如果选择了此选项，则在**客户端** > **全局客户端设置**中配置日志发送时间表。转至**防火墙设置**部分。该时间表仅适用于具有防火墙日志发送权限的客户端。有关说明，请参阅全局防火墙设置 第 12-23 页。

授予防火墙权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转至**防火墙权限**部分。
5. 选择下列选项：
   - 在防毒墙网络版客户端控制台上显示“防火墙”选项卡 第 12-22 页

- 允许用户启用/禁用防火墙、入侵检测系统及防火墙违例通知消息 第 12-22 页
- 允许防毒墙网络版客户端向防毒墙网络版服务器发送防火墙日志 第 12-22 页

6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

全局防火墙设置

有许多种方法可以将全局防火墙设置应用于防毒墙网络版客户端。

- 可将特定防火墙设置应用于服务器所管理的所有客户端。
- 可将设置只应用于具有特定防火墙权限的防毒墙网络版客户端。例如，您可以只将防火墙日志发送时间表应用于具有将日志发送到服务器的权限的防毒墙网络版客户端。

根据需要启用下列全局设置：

- **将防火墙日志发送到服务器**

  可以授予某些防毒墙网络版客户端向防毒墙网络版服务器发送防火墙日志的权限。在此部分中配置日志发送时间表。只有具有发送防火墙日志权限的客户端可使用此时间表。

  有关可用于所选客户端的防火墙权限的信息，请参阅防火墙权限 第 12-21 页。

- **仅在系统重新启动后更新防毒墙网络版防火墙驱动程序**

  仅允许防毒墙网络版客户端客户端在防毒墙网络版客户端终端重新启动后更新通用防火墙驱动程序。当通用防火墙驱动程序在客户端升级期间更新

时，启用此选项避免出现潜在客户端终端中断（例如，暂时断开网络连接）。

- **每小时向防毒墙网络版服务器发送一次防火墙日志信息，以确定防火墙爆发的可能性**

  启用此选项后，防毒墙网络版客户端每小时向防毒墙网络版服务器发送一次防火墙日志计数。有关防火墙日志的详细信息，请参阅 防火墙日志 第 12-26 页。

  防毒墙网络版会使用日志数和防火墙违例爆发条件确定防火墙违例爆发的可能性。发生爆发情况时，防毒墙网络版会给防毒墙网络版 管理员发送电子邮件通知。

- 转到**安全软件认证服务设置**部分，然后根据需要启用安全软件认证服务。

  安全软件认证服务会查询趋势科技数据中心，以验证由恶意软件行为阻止、事件监控、防火墙或防病毒扫描检测到的程序的安全性。启用安全软件认证服务可降低误判检测的可能性。

  注意

  请先确保防毒墙网络版客户端的代理服务器设置正确（有关详细信息，请参阅防毒墙网络版客户端代理服务器设置 第 14-44 页），然后再启用安全软件认证服务。不正确的代理服务器设置和不稳定的 Internet 连接都会导致从趋势科技数据中心接收响应延迟或不成功，从而导致受监控程序看上去处于无响应状态。

  另外，纯 IPv6 防毒墙网络版客户端无法直接从趋势科技数据中心进行查询。为允许防毒墙网络版客户端连接到趋势科技数据中心，需要可转换 IP 地址的双栈代理服务器（如 DeleGate）。

配置全局防火墙设置

过程

1. 转至**客户端** > **全局客户端设置**。
2. 转至下列部分并配置设置：

表 12-4. 全局防火墙设置

部分	设置
防火墙设置	• 将防火墙日志发送到服务器 第 12-23 页 • 仅在系统重新启动后更新防毒墙网络版防火墙驱动程序 第 12-23 页
防火墙日志计数	每小时向防毒墙网络版服务器发送一次防火墙日志信息，以确定防火墙爆发的可能性 第 12-24 页
安全软件认证设置	为行为监控、防火墙和防病毒扫描启用安全软件认证服务 第 12-24 页

3. 单击**保存**。

向防毒墙网络版客户端用户发送的防火墙违例通知

在防毒墙网络版防火墙阻止违反防火墙策略的出站网络通信后，防毒墙网络版可以在客户端上立即显示通知消息。授予用户启用/禁用通知消息的权限。

注意

配置特定防火墙策略时，您也可以启用通知。要配置防火墙策略，请参阅添加或修改防火墙策略 第 12-10 页。

授予用户启用/禁用通知消息的权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。

3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转至**防火墙权限**部分。
5. 选择**允许用户启用/禁用防火墙、入侵检测系统及防火墙违例通知消息**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

修改防火墙通知消息的内容

过程

1. 转至**管理** > **通知** > **客户端**。
2. 从**类型**下拉列表中，选择**防火墙违例**。
3. 在提供的文本框中修改缺省消息。
4. 单击**保存**。

防火墙日志

服务器上可用的防火墙日志由具有发送防火墙日志权限的防毒墙网络版客户端发送。将此权限授予特定客户端，以监控和分析防毒墙网络版防火墙阻止的终端上的网络通信。

有关防火墙权限的信息，请参阅防火墙权限 第 12-21 页。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看防火墙日志

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**日志** > **防火墙日志**或**查看日志** > **防火墙日志**。
4. 要确保为您提供最新的日志，请单击**通知客户端**。在继续执行下一步之前，留出一些时间供客户端发送防火墙日志。
5. 指定日志条件，然后单击**显示日志**。
6. 查看日志。日志包含以下信息：
   - 防火墙违例的检测日期和时间
   - 发生防火墙违例的终端
   - 发生防火墙违例的终端域
   - 远程主机 IP 地址
   - 本地主机 IP 地址
   - 协议
   - 端口号
   - 方向：是入站（接收）还是出站（发送）网络通信违反了防火墙策略
   - 进程：正在终端上运行的导致防火墙违例的可执行程序或服务
   - 描述：指出实际安全风险（例如，网络病毒或 IDS 攻击）或防火墙策略违例

7. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

防火墙违例爆发

依防火墙违例数量和检测期间定义防火墙违例爆发。

防毒墙网络版具有缺省通知消息，可在检测到爆发时，通知您和其他防毒墙网络版管理员。您可以根据需要修改通知消息。

注意

防毒墙网络版可以通过电子邮件发送防火墙爆发通知。配置电子邮件设置，让防毒墙网络版可以成功地发送电子邮件。有关详细信息，请参阅管理员通知设置 第 13-32 页。

配置防火墙违例爆发条件和通知

过程

1. 转至**管理** > **通知** > **爆发**。
2. 在**条件**选项卡中：
   a. 转至**防火墙违例**部分。
   b. 选择**监控防毒墙网络版客户端上的防火墙违例**。
   c. 指定 IDS 日志、防火墙日志和网络病毒日志的数量。
   d. 指定检测期间。

提示

趋势科技建议接受此窗口中的缺省值。

防毒墙网络版将在超出指定的日志数量时发送一个通知消息。例如，如果您指定 100 个 IDS 日志、100 个防火墙日志和 100 个网络病毒日志，并指定 3 小时的期间，当服务器在 3 个小时内收到 301 个日志时，防毒墙网络版会发送通知。

3. 在**电子邮件**选项卡中：

   a. 转至**防火墙违例爆发**部分。

   b. 选择**启用电子邮件通知**。

   c. 指定电子邮件收件人。

   d. 接受或修改缺省的电子邮件主题和消息。可以使用标记变量表示**主题**和**消息**文本框中的数据。

表 12-5. 防火墙违例病毒爆发通知的标记变量

变量	描述
%A	超出的日志类型
%C	防火墙违例日志数
%T	防火墙违例日志的累计时长

4. 单击**保存**。

测试防毒墙网络版防火墙

要确保防毒墙网络版防火墙正常工作，请在一个防毒墙网络版客户端或一组防毒墙网络版客户端上执行测试。

警告!

请仅在受控的环境中测试防毒墙网络版客户端程序设置。请勿在已连接到网络或 Internet 的终端上执行测试。执行此操作可能会将防毒墙网络版客户端终端暴露在病毒、黑客攻击和其他风险中。

过程

1. 创建并保存测试策略。配置设置以阻止要测试的网络通信的类型。例如，要阻止防毒墙网络版客户端访问 Internet，请执行以下操作：

   a. 将安全级别设置为**低**（允许所有入站/出站网络通信）。

   b. 选择**启用防火墙和发生防火墙违例时通知用户**。

   c. 创建阻止 HTTP 网络通信的例外。

2. 通过选择将测试防火墙功能的客户端，创建并保存测试概要文件。将测试策略与测试概要文件关联。

3. 单击**向客户端分配概要文件**。

4. 验证部署。

   a. 单击**客户端** > **客户端管理**。

   b. 选择客户端属于的域。

   c. 从客户端树视图中选择**防火墙视图**。

   d. 检查在客户端树的**防火墙**列下是否有绿色复选标记。如果已为该客户端启用了入侵检测系统，则请检查在 **IDS** 列下是否还有绿色复选标记。

   e. 验证客户端是否应用了正确的防火墙策略。该策略在客户端树中的**防火墙策略**列下显示。

5. 通过尝试发送或接收在策略中配置的网络通信类型来测试客户端终端上的防火墙。

6. 要测试配置为阻止客户端访问 Internet 的策略，请在客户端终端上打开 Web 浏览器。如果已将防毒墙网络版配置为发生防火墙违例时显示通知消息，则在发生出站网络通信违例时，会在客户端终端上显示该消息。

部分 III

管理防毒墙网络版服务器和客户端

第 13 章

管理防毒墙网络版服务器

本章介绍防毒墙网络版服务器管理和配置。

主题包括：

- 基于角色的管理 第 13-3 页
- 趋势科技防毒墙控制管理中心 第 13-22 页
- 可疑对象列表设置 第 13-28 页
- 参考服务器 第 13-30 页
- 管理员通知设置 第 13-32 页
- 系统事件日志 第 13-34 页
- 日志管理 第 13-35 页
- 使用授权 第 13-38 页
- 防毒墙网络版数据库备份 第 13-41 页
- SQL Server 迁移工具 第 13-43 页
- 防毒墙网络版 Web 服务器/客户端连接设置 第 13-47 页
- 服务器-客户端通信 第 13-48 页

- Web 控制台密码 第 13-53 页
- Web 控制台设置 第 13-53 页
- 隔离管理器 第 13-54 页
- 服务器调节程序 第 13-55 页
- 云安全智能反馈 第 13-58 页

基于角色的管理

使用基于角色的管理授予和控制访问防毒墙网络版 Web 控制台的权限。如果贵组织中有多个防毒墙网络版管理员，可以使用此功能将特定的 Web 控制台权限分配给各个管理员，并仅向管理员提供执行特定任务所必需的工具和权限。通过向管理员分配一个或多个要管理的域，还可以控制对客户端树的访问权限。此外，还可授予除管理员之外的人对 Web 控制台的“仅查看”权限。

每个用户（管理员或非管理员）均分配有特定角色。角色定义了对 Web 控制台的访问级别。用户使用定制用户帐户或 Active Directory 帐户登录到 Web 控制台。

基于角色的管理涉及下列任务：

1. 定义用户角色。有关详细信息，请参阅用户角色 第 13-3 页。
2. 配置用户帐户并为每个用户帐户分配特定角色。有关详细信息，请参阅用户帐户 第 13-12 页。

查看系统事件日志中所有用户的 Web 控制台活动。记录以下活动：

- 登录到控制台
- 修改密码
- 从控制台注销
- 会话超时（用户被自动注销）

用户角色

用户角色确定用户可访问的 Web 控制台菜单项。角色分配有对每个菜单项的权限。

为下列项目分配权限：

- 菜单项权限 第 13-4 页
- 菜单项类型 第 13-4 页

- 服务器和客户端的菜单项 第 13-4 页
- 受管理域的菜单项 第 13-7 页

菜单项权限

权限确定了对每个菜单项的访问级别。菜单项权限可以是：

- **配置**：允许完全访问菜单项。用户可以配置所有设置，执行所有任务并查看菜单项中的数据。
- **查看**：仅允许用户查看菜单项中的设置、任务和数据。
- **不能访问**：隐藏菜单项，无法查看。

菜单项类型

防毒墙网络版用户角色共有两种可配置的菜单项类型。

表 13-1. 菜单项类型

类型	作用域
服务器/客户端的菜单项	• 服务器设置、任务和数据 • 全局客户端设置、任务和数据 有关可用的菜单项的完整列表，请参阅服务器和客户端的菜单项 第 13-4 页。
受管理域的菜单项	在客户端树外可用的粒度客户端设置、任务和数据 有关可用的菜单项的完整列表，请参阅受管理域的菜单项 第 13-7 页。

服务器和客户端的菜单项

下表列出了服务器/客户端的可用菜单项：

注意

菜单项仅在各自的插件程序激活之后显示。例如，如果数据丢失防护模块未激活，则任何数据丢失防护菜单项均不会显示在列表中。任何其他插件程序显示在插件菜单项下。

只有分配了 “Administrator (内置)” 角色的用户才拥有对插件菜单项的访问权限。

表 13-2. 客户端菜单项

顶层菜单项	菜单项
客户端	• 客户端管理 • 客户端分组 • 全局客户端设置 • 终端位置 • 数据丢失防护 • 连接验证 • 爆发阻止

表 13-3. 日志菜单项

顶层菜单项	菜单项
日志	• 客户端 • 安全风险 • 客户端组件更新 • 服务器更新 • 系统事件 • 日志维护

表 13-4. 更新菜单项

顶层菜单项	菜单项	子菜单项
更新	服务器	• 预设更新 • 手动更新 • 更新源
	客户端	• 自动更新 • 更新源
	还原	无

表 13-5. 管理菜单项

顶层菜单项	菜单项	子菜单项
管理	帐户管理	• 用户帐户 • 用户角色 **注意** 只有使用内置管理员帐户的用户可以访问用户帐户和用户角色。
	云安全智能防护	• 云安全智能防护源 • 集成型服务器 • 云安全智能反馈
	Active Directory	• Active Directory 集成 • 预设同步
	通知	• 常规设置 • 爆发 • 客户端
	设置	• 代理服务器

顶层菜单项	菜单项	子菜单项
		• 客户端连接 • 非活动客户端 • 隔离管理器 • 产品使用授权 • 控制管理中心 • Web 控制台 • 数据库备份 • 可疑对象列表

受管理域的菜单项

下表列出了受管理域的可用菜单项。

表 13-6. 控制台菜单项

主菜单项	菜单项
控制台 **注意** 无论权限如何，任何用户都可以访问此页面。	无

表 13-7. 评估菜单项

顶层菜单项	菜单项	子菜单项
评估	安全合规	• 手动报告 • 预设报告
	不受管理的终端	无

表 13-8. 客户端菜单项

顶层菜单项	菜单项	子菜单项
客户端	防火墙	• 策略 • 概要文件
	客户端安装	• 基于浏览器 • 远程

表 13-9. 日志菜单项

顶层菜单项	菜单项	子菜单项
日志	客户端	• 连接验证 • 集中隔离恢复 • 间谍软件/灰色软件恢复

表 13-10. 更新菜单项

顶层菜单项	菜单项	子菜单项
更新	摘要	无
	客户端	手动更新

表 13-11. 管理菜单项

顶层菜单项	菜单项	子菜单项
管理	通知	管理员

内置用户角色

防毒墙网络版附带了一组内置用户角色，您无法修改或删除这些角色。内置角色如下：

表 13-12. 内置用户角色

角色名称	描述
管理员	可以将此角色委派给其他防毒墙网络版管理员或具有丰富的防毒墙网络版知识的用户。 具有此角色的用户拥有对所有菜单项的“配置”权限。 **注意** 只有分配了 “Administrator (内置)” 角色的用户才拥有对插件菜单项的访问权限。
Guest User	将此角色委派给希望查看 Web 控制台以供参考的用户。 • 具有此角色的用户无权访问以下菜单项： • 插件 • **管理** > **帐户管理** > **用户角色** • **管理** > **帐户管理** > **用户帐户** • 用户拥有对所有其他菜单项的“查看”权限。
Trend Power User （“仅升级”角色）	此角色仅在从防毒墙网络版 10 升级时可用。 此角色继承了防毒墙网络版 10 中 Power User 角色的权限。具有此角色的用户拥有对所有客户端树域的“配置”权限，但无权访问此发行版中的新增功能。

定制角色

如果内置角色都不符合要求，可以创建定制角色。

只有具有内置管理员角色的用户和使用在防毒墙网络版安装期间创建的 root 帐户的用户才可以创建定制用户角色，并将这些角色分配给用户帐户。

添加定制角色

过程

1. 转至**管理** > **帐户管理** > **用户角色**。
2. 单击**添加**。如果要创建的角色具有与现有角色类似的设置，请选择现有角色，然后单击**复制**。

   将显示一个新窗口。
3. 为角色键入名称并可选择提供描述。
4. 单击**服务器/客户端的菜单项**并指定对每个可用菜单项的权限。有关可用菜单项的列表，请参阅服务器和客户端的菜单项 第 13-4 页。
5. 单击**受管理域的菜单项**并指定对每个可用菜单项的权限。有关可用菜单项的列表，请参阅受管理域的菜单项 第 13-7 页。
6. 单击**保存**。

   新角色显示在“用户角色”列表上。

修改定制角色

过程

1. 转至**管理** > **帐户管理** > **用户角色**。
2. 单击角色名称。

   将显示一个新窗口。
3. 修改以下任意内容：
   - 描述
   - 角色权限

- **服务器/客户端的菜单项**
- **受管理域的菜单项**

4. 单击**保存**。

删除定制角色

过程

1. 转至**管理** > **帐户管理** > **用户角色**。
2. 选中角色旁的复选框。
3. 单击**删除**。

注意

如果角色至少分配给一个用户帐户，则无法删除该角色。

导入或导出定制角色

过程

1. 转至**管理** > **帐户管理** > **用户角色**。
2. 将定制角色导出到 .dat 文件：
   a. 选择角色，然后单击**导出**。
   b. 保存 .dat 文件。如果要管理另一个防毒墙网络版服务器，请使用该 .dat 文件将定制角色导入到该服务器。

注意

导出角色操作只能在相同版本的服务器之间完成。

3. 将定制角色导出到 .dat 文件：

   a. 选择角色，然后单击**导出角色设置**。

   b. 保存 .csv 文件。使用此文件可以检查选定角色的信息和权限。

4. 如果已保存另一台防毒墙网络版服务器上的定制角色，且希望将这些角色导入到当前防毒墙网络版服务器中，则单击**导入**并找到包含这些定制角色的 .dat 文件。

   - 如果导入与“用户角色”窗口上的角色具有相同名称的角色，则将覆盖“用户角色”窗口上的角色。
   - 导入角色操作只能在相同版本的服务器之间完成。
   - 从其他防毒墙网络版服务器导入的角色：
     - 保留服务器/客户端菜单项以及受管理域菜单项的权限。
     - 应用客户端管理菜单项的缺省权限。在另一台服务器上，记录角色对客户端管理菜单项的权限，然后将这些权限重新应用到导入的角色。

用户帐户

设置用户帐户并为每个用户分配特定角色。用户角色确定用户可查看或配置的 Web 控制台菜单项。

在防毒墙网络版服务器安装期间，安装程序会自动创建称为“root”的内置帐户。使用 root 帐户登录的用户可以访问所有菜单项。您无法删除 root 帐户，但是可以修改帐户详细信息，如密码和全名或帐户描述。如果忘记 root 帐户密码，请与技术支持提供商联系，以帮助您重置密码。

添加定制帐户或 Active Directory 帐户。所有用户帐户都显示在 Web 控制台上的“用户帐户”列表上。

为用户帐户分配权限，使其能够查看或配置客户端树中可用的粒度客户端设置、任务和数据。有关可用的客户端树菜单项的完整列表，请参阅客户端管理菜单项 第 13-13 页。

注意

在升级防毒墙网络版服务器后，必须编辑定制帐户并在**步骤 3 定义客户端树菜单**屏幕上为以前添加的定制帐户手动启用所有新功能。有关权限的详细信息，请参阅定义域权限 第 13-17 页。

防毒墙网络版用户帐户可用于执行“单点登录”。单次登录允许用户从趋势科技防毒墙控制管理中心控制台访问防毒墙网络版 Web 控制台。有关详细信息，请参阅以下过程。

客户端管理菜单项

下表列出了可用的客户端管理菜单项。

注意

菜单项仅在各自的插件程序激活之后显示。例如，如果数据丢失防护模块未激活，则任何数据丢失防护菜单项均不会显示在列表中。

表 13-13. 客户端管理菜单项

主菜单项	子菜单
状态	无
任务	• 立即扫描 • 客户端卸载 • 集中隔离恢复 • 间谍软件/灰色软件恢复

主菜单项	子菜单
设置	• 扫描设置 • 扫描方法 • 手动扫描设置 • 实时扫描设置 • 预设扫描设置 • 立即扫描设置 • Web 信誉设置 • 可疑连接设置 • 行为监控设置 • 设备控制设置 • DLP 设置 • 更新代理设置 • 权限和其他设置 • 其他服务设置 • 间谍软件/灰色软件允许列表 • 可信程序列表 • 导出设置 • 导入设置

主菜单项	子菜单
日志	• 病毒/恶意软件日志 • 间谍软件/灰色软件日志 • 防火墙日志 • Web 信誉日志 • 可疑连接日志 • 可疑文件日志 • C&C 回呼日志 • 行为监控日志 • 设备控制日志 • 数据丢失防护日志 • 扫描操作日志 • 删除日志
管理客户端树	• 添加域 • 更名域 • 移动客户端 • 移除域/客户端
导出	无

添加定制帐户

过程

1. 转至**管理** > **帐户管理** > **用户帐户**。
2. 单击**添加**。

   此时将显示**步骤 1 用户信息**窗口。

3. 选择**启用此帐户**。

4. 在**选择角色**下拉列表中选择先前配置的角色。

   有关创建用户角色的详细信息，请参阅定制角色 第 13-9 页。

5. 键入用户名、描述和密码，并确认密码。

   重要信息

   不能将用户名用作帐户密码。请提供一个非用户名的密码。

6. 键入帐户的电子邮件地址。

   注意

   防毒墙网络版向此电子邮件地址发送通知。这些通知会通知收件人安全风险检测和数字资产传输。有关通知的详细信息，请参阅针对管理员的安全风险通知 第 7-72 页。

7. 单击**下一步**。

   此时将显示**步骤 2 客户端域控制**窗口。

8. 选择根域或客户端树中的一个或多个域来定义客户端树作用域。

   此时仅定义了域。对选定域的访问级别将在步骤 10 中定义。

9. 单击**下一步**。

   此时将显示**步骤 3 定义客户端树菜单**窗口。

10. 单击**可用菜单项**控件，然后指定对每个可用菜单项的权限。有关可用菜单项的列表，请参阅客户端管理菜单项 第 13-13 页。

    在步骤 8 中配置的客户端树作用域确定了对菜单项的权限级别，并定义了权限的目标。客户端树作用域可以是根域（所有客户端）或特定客户端树域。

表 13-14. 客户端管理菜单项和客户端树作用域

条件	客户端树作用域	
	根域	特定域
菜单项权限	配置、查看或不能访问	配置、查看或不能访问
目标	根域（所有客户端）或特定域 例如，可以向某个角色授予对客户端树中“任务”菜单项的“配置”权限。如果目标为根域，用户可在所有客户端上启动任务。如果目标为域 A 和 B，仅可在域 A 和 B 中的客户端上启动任务。	仅选定域 例如，可以向某个角色授予对客户端树中“设置”菜单项的“配置”权限。这意味着用户仅可将设置部署到选定域中的客户端。
	仅当对“服务器/客户端的菜单项”中“客户端管理”菜单项的权限为“查看”时，才显示客户端树。	

- 如果选中**配置**下的复选框，则会自动选中**查看**下的复选框。
- 如果未选中任何复选框，则权限为“不能访问”。
- 如果为特定域配置权限，可通过单击**将选定域的设置复制到其他域**将权限复制到其他域。

11. 单击**完成**。
12. 将帐户详细信息发送给用户。

定义域权限

定义域权限时，防毒墙网络版自动将父域的权限应用至该父域管理的所有子域。子域的权限不能少于其父域的权限。例如，如果系统管理员具有查看和配置防毒墙网络版管理的所有客户端（“防毒墙网络版服务器”域）的权限，子域的权限必须允许系统管理员访问这些配置功能。删除子域的权限意味着，系统管理员不具有针对所有客户端的完全配置权限。

下列过程的域树如下：



例如，要为用户帐户 “Chris” 授予查看和配置子域“员工”中特定菜单项的权限，同时仅授予查看父域“经理”中日志的权限，请执行下列过程。

表 13-15. 针对用户帐户 “Chris” 的权限

域	所需权限
防毒墙网络版服务器	无特殊权限
经理	查看**日志**
员工	查看和配置**任务** 查看和配置**日志** 查看**设置**
销售	无特殊权限

过程

1. 转至**用户帐户: 步骤 3 定义客户端树菜单**窗口。
2. 单击“防毒墙网络版服务器”域。
3. 清除所有**查看**和**配置**复选框。

> **注意**
>
> “防毒墙网络版服务器”域仅当您在**用户帐户: 步骤 2 客户端域控制**窗口中选择了其所有子域后才可用。

4. 单击“销售”域。
5. 清除所有**查看**和**配置**复选框。

注意

“销售”域只有在**用户帐户: 步骤 2 客户端域控制**窗口中选定后才显示。

6. 单击“经理”域。
7. 选择“查看日志”并清除所有其他**查看**和**配置**复选框。
8. 单击“员工”域。
9. 为 Chris 选择下列菜单项：
   - **任务**：查看和配置
   - **日志**：查看和配置
   - **设置**：查看

   Chris 现在可查看和配置“员工”域中的选定菜单项，同时只能查看“经理”域中的**日志**。

如果 Chris 具有查看和配置“经理”域的权限，防毒墙网络版将自动为“员工”子域授予相同的权限。这是因为“经理”域管理其所有子域。

修改定制帐户

注意

在升级防毒墙网络版服务器后，必须编辑定制帐户并在**步骤 3 定义客户端树菜单**屏幕上为以前添加的定制帐户手动启用所有新功能。有关权限的详细信息，请参阅定义域权限 第 13-17 页。

过程

1. 转至**管理** > **帐户管理** > **用户帐户**。

2. 单击用户帐户。
3. 使用提供的复选框启用或禁用帐户。
4. 修改以下内容：
   - 角色
   - 描述
   - 密码

   注意

   在编辑帐户时，不能重新键入以前配置的密码。不要修改**密码**字段以继续使用以前配置的密码。

   - 电子邮件地址
5. 单击**下一步**。
6. 定义客户端树作用域。
7. 单击**下一步**。
8. 单击**可用菜单项**控件，然后指定对每个可用菜单项的权限。

   有关可用菜单项的列表，请参阅客户端管理菜单项 第 13-13 页。
9. 单击**完成**。
10. 将新帐户详细信息发送给用户。

添加 Active Directory 帐户或组

过程

1. 转至**管理** > **帐户管理** > **用户帐户**。
2. 单击**添加**。

   此时将显示**步骤 1 用户信息**窗口。

3. 选择**启用此帐户**。
4. 在**选择角色**下拉列表中选择先前配置的角色。

   有关创建用户角色的详细信息，请参阅定制角色 第 13-9 页。
5. 选择 **Active Directory 用户或组**。
6. 通过指定用户名和帐户所属的域来搜索帐户（用户名或组）。

   注意

   使用字符 (*) 可搜索多个帐户。如果不指定通配符，则包括完整帐户名。对于不完整的帐户名，或者如果使用了缺省组“域用户”，防毒墙网络版将不返回结果。
7. 当防毒墙网络版找到有效帐户时，它在**用户和组**下显示帐户名。单击向前图标 (>) 移动**所选用户和组**下的帐户。

   如果指定 Active Directory 组，则属于同一个组的所有成员都会得到相同的角色。如果某个特定帐户至少属于两个组，并且其在两个组中具有不同的角色：

   - 两个角色的权限会合并起来。如果用户配置了特定设置，但该设置的权限之间存在冲突，则应用较高的权限。
   - 所有用户角色都会显示在系统事件日志中。例如，“用户 JohnDoe 使用下列角色登录：Administrator、Power User”。
8. 单击**下一步**。

   此时将显示**步骤 2 客户端域控制**窗口。
9. 定义客户端树作用域。
10. 单击**下一步**。

    此时将显示**步骤 3 定义客户端树菜单**窗口。
11. 单击**可用菜单项**控件，然后指定对每个可用菜单项的权限。

    有关可用菜单项的列表，请参阅客户端管理菜单项 第 13-13 页。

12. 单击**完成**。

13. 通知用户使用其域帐户和密码登录到 Web 控制台。

趋势科技防毒墙控制管理中心

趋势科技™ 防毒墙控制管理中心™ 是管理网关、邮件服务器、文件服务器和企业桌面级别的趋势科技产品和服务的中央管理控制台。控制管理中心基于 Web 的管理控制台为整个网络内被管理产品和服务提供单个监控点。

控制管理中心允许系统管理员监控和报告活动，例如感染、安全性违例或病毒入口点。系统管理员可以下载组件并在整个网络内部署，以帮助确保防护的一致性和及时性。控制管理中心既允许手动更新又允许预设更新，还允许作为组或作为个体来配置和管理产品，以增加灵活性。

在此防毒墙网络版版本中集成控制管理中心

此防毒墙网络版版本在从控制管理中心管理防毒墙网络版服务器时包括下列功能和能力：

- 为防毒墙网络版防病毒、数据丢失防护和设备控制创建、管理和部署策略，并从控制管理中心控制台直接为防毒墙网络版客户端分配权限。

  下表列出了控制管理中心 6.0 中可用的策略配置。

表 13-16. 控制管理中心中的防毒墙网络版策略管理类型

策略类型	功能
防毒墙网络版防病毒和客户端设置	• 其他服务设置 • 行为监控设置 • 设备控制设置 • 手动扫描设置 • 权限和其他设置 • 实时扫描设置 • 间谍软件/灰色软件允许列表 • 扫描方法 • 立即扫描设置 • 预设扫描设置 • 可疑连接设置 • 更新代理设置 • Web 信誉设置
数据保护	数据丢失防护策略设置 **注意** 在防毒墙网络版客户端策略中管理设备控制权限以进行数据保护。

- 在控制管理中心控制台中，将以下设置从一台防毒墙网络版服务器复制到另一台：
  - 数据标识符类型 第 10-4 页
  - 数据丢失防护模板 第 10-18 页

注意

如果将这些设置复制到尚未激活数据保护使用授权的防毒墙网络版服务器，则只有在激活该使用授权时这些设置才能生效。

支持的控制管理中心版本

此版本防毒墙网络版支持以下控制管理中心版本。

表 13-17. 支持的控制管理中心版本

防毒墙网络版服务器	控制管理中心版本	
	6.0 或更高版本	5.5 SP1
双栈	是	是
纯 IPv4	是	是
纯 IPv6	是	否

注意

控制管理中心自版本 5.5 Service Pack 1 起开始支持 IPv6。

有关防毒墙网络版服务器和防毒墙网络版客户端向控制管理中心报告的 IP 地址的详细信息，请参阅显示 IP 地址的窗口 第 A-6 页。

对这些控制管理中心版本应用最新的 Patch 和重要的 Hotfix，使控制管理中心能够对防毒墙网络版进行管理。要获取最新的 Patch 和 Hot Fix，请与技术支持提供商联系或者访问趋势科技更新中心：

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

在安装防毒墙网络版之后，将其注册到控制管理中心，然后在控制管理中心管理控制台上配置防毒墙网络版的设置。有关管理防毒墙网络版服务器的信息，请参阅*控制管理中心文档*。

将防毒墙网络版注册到控制管理中心

过程

1. 转至**管理** > **设置** > **控制管理中心**。
2. 指定实体显示名称，该名称就是将在控制管理中心显示的防毒墙网络版服务器的名称。

   缺省情况下，实体显示名称包括服务器计算机的主机名和此产品的名称（例如，Server01_OSCE）。

   注意

   在控制管理中心，由控制管理中心管理的防毒墙网络版服务器及其他产品都称为“实体”。
3. 指定控制管理中心服务器 FQDN 或 IP 地址以及用于连接到该服务器的端口号。可选择是否以更高的安全性（使用 HTTPS）来连接。
   - 对于双栈防毒墙网络版服务器，请键入控制管理中心 FQDN 或 IP 地址（IPv4 或 IPv6，如果可用）。
   - 对于纯 IPv4 防毒墙网络版服务器，请键入控制管理中心 FQDN 或 IPv4 地址。
   - 对于纯 IPv6 防毒墙网络版服务器，请键入控制管理中心 FQDN 或 IPv6 地址。

   注意

   只有控制管理中心 5.5 SP1 和更高版本支持 IPv6。
4. 如果控制管理中心的 IIS Web 服务器需要认证，请键入用户名和密码。
5. 如果要使用代理服务器连接到控制管理中心服务器，请指定以下代理服务器设置：
   - 代理服务器协议

- 服务器 FQDN 或 IPv4/IPv6 地址和端口
- 代理服务器认证的用户 ID 和密码

6. 确定是使用单向通信还是双向通信端口转发，然后指定 IPv4/IPv6 地址和端口。

7. 要检查防毒墙网络版是否可以根据您指定的设置连接到控制管理中心服务器，请单击**测试连接**。

   如果成功建立连接，则单击**注册**。

8. 如果控制管理中心服务器为 6.0 SP1 或更高版本，则会显示一条消息，提示您将控制管理中心服务器用作防毒墙网络版集成型云安全智能防护服务器的更新源。单击**确定**可将控制管理中心服务器用作集成型云安全智能防护服务器更新源，单击**取消**则会继续使用当前更新源（缺省情况下为 ActiveUpdate 服务器）。

9. 如果在注册后更改了此窗口上的任何设置，请在更改设置后单击**更新设置**，以向控制管理中心服务器通知这些更改。

注意

如果控制管理中心服务器已连接到 Deep Discovery，则在完成注册后将启动自动订阅过程。有关详细信息，请参阅可疑对象列表设置 第 13-28 页。

10. 如果不再希望控制管理中心服务器管理防毒墙网络版，则单击**取消注册**。

在控制管理中心管理控制台上查看防毒墙网络版的状态

过程

1. 打开控制管理中心管理控制台。

   要打开控制管理中心控制台，请在网络上的任意终端上打开一个 Web 浏览器，然后键入以下内容：

   https://<控制管理中心服务器名称>/Webapp/login.aspx

其中 <控制管理中心服务器名称> 是控制管理中心服务器的 IP 地址或主机名

2. 在主菜单上，单击**目录** > **产品**。
3. 在显示的树中，转至 **[控制管理中心服务器]** > **本地文件夹** > **新建实体**文件夹。
4. 检查防毒墙网络版服务器图标是否显示。

策略导出工具

趋势科技防毒墙网络版服务器策略导出工具帮助管理员导出控制管理中心 6.0 或更高版本支持的防毒墙网络版策略设置。管理员还需要控制管理中心导入工具，以便导入策略。策略导出工具支持防毒墙网络版 10.6 Service Pack 1 或更高版本。

- 实时扫**描**设**置**
- 预设扫**描**设**置**
- **手**动扫**描**设**置**
- **立即**扫**描**设**置**
- **更新代理**设**置**
- Web **信誉**设**置**
- 扫**描方法**
- **行**为监**控**设**置**
- 设备**控制**设**置**
- **数据**丢**失防**护设**置**
- 权**限和其他**设**置**
- **其他服**务设**置**
- 间谍软**件/灰色**软**件允**许**列表**
- **可疑**连**接**设**置**

使用策略导出工具

过程

1. 在防毒墙网络版服务器计算机上，导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\PolicyExportTool。
2. 双击 PolicyExportTool.exe 启动策略导出工具。

命令行界面窗口打开，策略导出工具开始导出设置。此工具创建两个文件夹（PolicyClient 和 PolicyDLP），位于包含导出设置的 PolicyExportTool 文件夹中。

3. 将这两个文件夹复制到控制管理中心的安装文件夹。

4. 在控制管理中心服务器上执行策略导入工具。

   有关策略导入工具的详细信息，请参阅控制管理中心服务器上的《策略导入工具自述文件》(TMCM_installation folder\WebUI\WebApp\widget\common\tool\PolicyImport\)。

注意

策略导出工具不导出定制的数据标识符或定制的 DLP 模板。对于需要导出定制的数据标识符和 DLP 模板的管理员，请从防毒墙网络版控制台手动导出,然后使用控制管理中心控制台手动导入文件。

可疑对象列表设置

可疑对象是指经 Trend Micro Deep Discovery 产品分析而得出的或从其他来源获取的数字项目。防毒墙网络版可与控制管理中心 6.0 SP3 或更高版本服务器（已连接到 Deep Discovery）同步可疑对象，并对这些对象采取处理措施。

订阅控制管理中心后，可以选择可疑对象的类型以监控 C&C 回调或客户端在网络上识别到的潜在针对性攻击。可疑对象包括：

- 可疑 URL 列表
- 可疑 IP 列表
- 可疑文件列表

注意

在防毒墙网络版 10.6 到 11.0 中，主要可疑对象来源为 Deep Discovery 分析器。从防毒墙网络版 11.0 SP1 开始，主要可疑对象来源为控制管理中心 6.0 SP3，它可以提供更强大的可疑对象管理和处理过程。

如果防毒墙网络版已订阅 Deep Discovery Analyzer，则只有可疑 URL 列表可用。防毒墙网络版取消订阅 Deep Discovery Analyzer 后，将无法重新订阅。防毒墙网络版必须订阅与 Deep Discovery 连接的控制管理中心才能同步可疑对象。

有关控制管理中心如何管理可疑对象的更多信息，请参阅《联动威胁治理手册》，网址为：

http://docs.trendmicro.com/all/ent/tmcm/v6.0-sp3/zh-cn/tmcm_6.0_sp3_ctd_primer/ctd_primer.pdf.

配置可疑对象列表设置

在向控制管理中心注册防毒墙网络版期间，控制管理中心会向防毒墙网络版部署一个 API 密钥，用于启动订阅过程。要启用此自动订阅过程，请咨询控制管理中心的管理员，以确保控制管理中心已连接到 Deep Discovery 并已配置所需的设置。

有关向控制管理中心服务器注册的详细信息，请参阅将防毒墙网络版注册到控制管理中心 第 13-25 页。

过程

1. 转至**管理** > **设置** > **可疑对象列表**。
2. 选择要在客户端上启用的列表。
   - 可疑 URL 列表
   - 可疑 IP 列表（仅在订阅已注册的控制管理中心服务器后才可用）
   - 可疑文件列表（仅在订阅已注册的控制管理中心服务器后才可用）

   管理员可以通过单击**立即同步**按钮随时手动同步可疑对象列表。

3. 在**客户端更新设置**部分中，指定客户端更新可疑对象列表的时间。
   - **基于客户端组件更新时间表通知防毒墙网络版客户端**：防毒墙网络版客户端基于当前更新时间表更新可疑对象列表。
   - **更新服务器上的可疑对象列表后自动通知防毒墙网络版客户端**：在防毒墙网络版服务器收到已更新的列表后，防毒墙网络版客户端会自动更新可疑对象列表。
4. 单击**保存**。

参考服务器

防毒墙网络版客户端确定要使用哪一策略或概要文件的方式之一是，通过检查其与防毒墙网络版服务器的连接状态。如果某个内部防毒墙网络版客户端（或公司网络中的任何客户端）无法连接到服务器，则该客户端的状态将变为脱机。然后，该客户端会应用用于外部客户端的策略或概要文件。参考服务器可解决此问题。

与防毒墙网络版服务器失去连接的任何防毒墙网络版客户端将尝试连接到参考服务器。如果客户端与参考服务器成功建立连接，其将应用用于内部客户端的策略或概要文件。

由参考服务器管理的策略和概要文件包括：

- 防火墙概要文件
- Web 信誉策略
- 数据保护策略
- 设备控制策略

请注意以下事项：

- 将具有服务器功能的计算机（如 Web 服务器、SQL 服务器或 FTP 服务器）指定为参考服务器。最多可以指定 320 个参考服务器。
- 防毒墙网络版客户端将连接到参考服务器列表中的第一个参考服务器。如果无法建立连接，则客户端将尝试连接到列表中的下一个服务器。

- 在确定要使用的防病毒（行为监控、设备控制、防火墙概要文件、Web 信誉策略）或数据保护设置时，防毒墙网络版客户端会使用参考服务器。参考服务器不管理客户端或部署更新和客户端设置。防毒墙网络版服务器执行这些任务。
- 防毒墙网络版客户端不能将日志发送到参考服务器，也不能将参考服务器用作更新源

管理参考服务器列表

过程

1. 转至**客户端** > **防火墙** > **概要文件**或**客户端** > **终端位置**。
2. 根据显示的窗口，执行以下操作：
   - 如果在**客户端的防火墙概要文件**窗口中，则单击**编辑参考服务器列表**。
   - 如果在**终端位置**窗口中，则单击**参考服务器列表**。
3. 选择**启用参考服务器列表**。
4. 要将任何终端添加到该列表，请单击**添加**。
   a. 指定终端的 IPv4/IPv6 地址、名称或完全限定域名 (FQDN)，例如：
      - computer.networkname
      - 12.10.10.10
      - mycomputer.domain.com
   b. 键入客户端与此终端通信时通过的端口。指定参考服务器上的任一开放联系端口（如端口 20、23 或 80）。



注意

要指定同一参考服务器的其他端口号，请重复步骤 2a 和 2b。防毒墙网络版客户端将使用列表中的第一个端口号，如果连接未成功，则将使用下一个端口号。

c. 单击**保存**。

5. 要编辑列表中任何终端的设置，请单击终端名称。修改终端名称或端口，然后单击**保存**。

6. 要从列表中删除任何终端，请选择终端名称，然后单击**删除**。

7. 要使终端充当参考服务器，请单击**分配到客户端**。

管理员通知设置

配置管理员通知设置，以允许防毒墙网络版通过电子邮件和 SNMP 陷阱成功发送通知。防毒墙网络版还可以通过 Windows NT 事件日志发送通知，但未针对此通信通道配置任何设置。

检测到以下情况时，防毒墙网络版会向您和其他防毒墙网络版管理员发送通知：

表 13-18. 触发管理员通知的检测

检测	通信通道		
	电子邮件	SNMP 陷阱	Windows NT 时间日志
病毒和恶意软件	是	是	是
间谍软件和灰色软件	是	是	是
数字资产传输	是	是	是
C&C 回呼	是	是	是
病毒和恶意软件爆发	是	是	是
间谍软件和灰色软件爆发	是	是	是
防火墙违例爆发	是	否	否
共享文件夹会话爆发	是	否	否

配置常规通知设置

过程

1. 转至**管理** > **通知** > **常规设置**。
2. 配置电子邮件通知设置。
   a. 在 **SMTP 服务器**文本框中指定 IPv4/IPv6 地址或终端名称。
   b. 指定一个 1 到 65535 之间的端口号。
   c. 指定电子邮件地址。

      如果要在下一步中启用 ESMTP，请指定一个有效的电子邮件地址。
   d. （可选）启用 **ESMTP**。
   e. 指定在**发件人**文本框中指定的电子邮件地址的用户名和密码。
   f. 选择用于向服务器验证客户端的方法：
      - **登录**：登录是旧版本的邮件用户客户端。服务器和客户端均使用 BASE64 来认证用户名和密码。
      - **纯文本**：纯文本最易于使用，但安全性较低，因为用户名和密码作为一个字符串进行发送，在通过 Internet 发送之前进行 BASE64 编码。
      - **CRAM-MD5**:CRAM-MD5 使用请求-响应验证机制和 Message Digest 5 加密算法组合来交换和认证信息。
3. 配置 SNMP 陷阱通知设置。
   a. 在**服务器 IP 地址**文本框中指定 IPv4/IPv6 地址或终端名称。
   b. 请指定一个难以推测的团体名称。
4. 单击**保存**。

系统事件日志

防毒墙网络版记录与服务器程序相关的事件，如关闭和启动。使用这些日志来验证防毒墙网络版服务器及服务是否工作正常。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看系统事件日志

过程

1. 转至**日志 > 系统事件**。
2. 在**事件**下查看是否有需要采取进一步处理措施的日志。防毒墙网络版将记录以下事件：

表 13-19. 系统事件日志

日志类型	事件
防毒墙网络版主服务和数据库服务器	• 主服务已启动 • 主服务停止成功 • 主服务停止未成功
爆发阻止	• 爆发阻止已启用 • 爆发阻止已禁用 • 最近 <分钟数> 内的共享文件夹会话数
数据库备份	• 数据库备份成功 • 数据库备份未成功

日志类型	事件
基于角色的 Web 控制台访问	• 登录到控制台 • 修改密码 • 从控制台注销 • 会话超时（用户被自动注销）
服务器认证	• 防毒墙网络版客户端从服务器收到无效命令 • 认证证书无效或过期

3. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

日志管理

防毒墙网络版保留有关安全风险检测、事件和更新的全面日志。使用这些日志来评估贵组织的防护策略并识别处于较高感染风险或攻击风险的防毒墙网络版客户端。还使用这些日志来检查客户端-服务器连接并验证组件更新是否成功。

防毒墙网络版还使用中央标准时间验证机制确保防毒墙网络版服务器和客户端之间的时间保持一致。这可以防止日志分析期间时区、夏令时和时差造成的日志不一致性，日志不一致性可能会产生混淆。

注意

防毒墙网络版对所有日志（服务器更新日志和系统事件日志除外）执行时间验证。

防毒墙网络版服务器从防毒墙网络版客户端接收以下日志：

- 查看病毒/恶意软件日志 第 7-81 页
- 查看间谍软件/灰色软件日志 第 7-88 页
- 查看间谍软件/灰色软件恢复日志 第 7-91 页

- 查看防火墙日志 第 12-27 页
- 查看 Web 信誉日志 第 11-23 页
- 查看可疑连接日志 第 11-25 页
- 查看可疑文件日志 第 7-92 页
- 查看 C&C 回呼日志 第 11-24 页
- 查看行为监控日志 第 8-13 页
- 查看设备控制日志 第 9-17 页
- 查看扫描操作日志 第 7-93 页
- 查看数据丢失防护日志 第 10-53 页
- 查看防毒墙网络版客户端更新日志 第 6-46 页
- 查看连接验证日志 第 14-40 页

防毒墙网络版服务器生成以下日志：

- 防毒墙网络版服务器更新日志 第 6-26 页
- 系统事件日志 第 13-34 页

以下日志也可在防毒墙网络版服务器和防毒墙网络版客户端上找到：

- Windows 事件日志 第 16-24 页
- 防毒墙网络版服务器日志 第 16-2 页
- 防毒墙网络版客户端日志 第 16-15 页

日志维护

要防止日志大小占用过多的硬盘空间，请从 Web 控制台手动删除日志或者配置日志删除时间表。

根据时间表删除日志

过程

1. 转至**日志** > **日志维护**。
2. 选择**启用预设日志删除**。
3. 选择要删除的日志类型。基于时间表，可以删除除调试日志外的所有防毒墙网络版生成的日志。对于调试日志，禁用调试日志记录以停止收集日志。

   注意

   对于病毒/恶意软件日志，可以删除某些扫描类型和损害清除服务生成的日志。对于间谍软件/灰色软件日志，可以删除某些扫描类型生成的日志。有关扫描类型的详细信息，请参阅扫描类型 第 7-12 页。

4. 选择是删除所有选定日志类型的日志，还是仅删除特定天数前的日志。
5. 指定日志删除的频率和时间。
6. 单击**保存**。

手动删除日志

过程

1. 转至**日志** > **客户端** > **安全风险**或**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。
3. 执行以下步骤之一：
   - 如果要访问**安全风险日志**窗口，请单击**删除日志**。
   - 如果要访问**客户端管理**窗口，请单击**日志** > **删除日志**。

4. 选择要删除的日志类型。只能手动删除以下日志：
   - 行为监控日志
   - C&C 回呼日志
   - 数据丢失防护日志
   - 设备控制日志
   - 防火墙日志
   - 间谍软件/灰色软件日志
   - 扫描操作日志
   - 可疑连接日志
   - 可疑文件日志
   - 病毒/恶意软件日志
   - Web 信誉日志

   注意

   对于病毒/恶意软件日志，可以删除某些扫描类型和损害清除服务生成的日志。对于间谍软件/灰色软件日志，可以删除某些扫描类型生成的日志。有关扫描类型的详细信息，请参阅扫描类型 第 7-12 页。

5. 选择是删除所有选定日志类型的日志，还是仅删除特定天数前的日志。
6. 单击**删除**。

使用授权

在 Web 控制台上可以查看、激活和续订防毒墙网络版使用授权服务，以及启用/禁用防毒墙网络版防火墙。防毒墙网络版防火墙是防病毒服务的一部分，防病毒服务还包括爆发阻止的技术支持。

注意

某些本机防毒墙网络版功能（例如数据保护和虚拟桌面支持）具有单独的使用授权。这些功能的使用授权是从插件管理器激活和管理的。有关这些功能的授权的详细信息，请参阅数据保护使用授权 第 3-3 页和虚拟桌面支持使用授权 第 14-69 页。

纯 IPv6 防毒墙网络版服务器无法连接到趋势科技在线注册服务器来激活/续订使用授权。需要使用可以转换 IP 地址的双栈代理服务器（例如 DeleGate）才能将防毒墙网络版服务器连接到注册服务器。

查看产品使用授权信息

过程

1. 转至**管理** > **设置** > **产品使用授权**。
2. 查看使用授权状态摘要，该摘要显示在窗口的顶部。以下实例中将显示关于使用授权的提醒信息：

表 13-20. 使用授权提醒

使用授权类型	提醒
完全版	• 在产品的宽限期内。宽限期的持续时间因地区而异。请通过趋势科技代表验证宽限期。 • 当使用授权到期且宽限期已过时。在此期间，您将无法获得技术支持或无法执行组件更新。扫描引擎将仍然扫描终端，但将使用过期组件。这些过期组件可能不能完全保护您不受最新安全风险的侵扰。
试用版	当使用授权过期时。在此期间，防毒墙网络版将禁用组件更新。扫描引擎将仍然扫描终端，但将使用过期组件。这些过期组件可能不能完全保护您不受最新安全风险的侵扰。

3. 查看使用授权信息。**使用授权信息**部分将提供以下信息：
   - **服务**：包括所有防毒墙网络版使用授权服务

- **状态**：显示“已激活”、“尚未激活”、“已过期”或“在宽限期”。如果服务有多个使用授权，且至少一个使用授权仍然处于活动状态，则显示的状态为“已激活”。
- **版本**：显示“完全版”或“试用版”。如果同时具有完全版和试用版，则显示的版本为“完全版”。
- **过期时间**：如果一个服务有多个使用授权，则将显示最晚过期时间。例如，如果使用授权到期时间为 12/31/2007 和 06/30/2008，则将显示 06/30/2008。

注意

尚未激活的使用授权服务的版本和到期日期为“无”。

4. 通过防毒墙网络版可以激活一个使用授权服务的多个使用授权。单击服务名称可以查看该服务的所有使用授权（不论处于活动状态还是已过期状态）。

激活或续订使用授权

过程

1. 转至**管理** > **设置** > **产品使用授权**。
2. 单击使用授权服务的名称。
3. 在打开的**产品使用授权详细信息**窗口中，单击**新激活码**。
4. 在打开的窗口中，键入激活码并单击**保存**。

注意

在激活服务前先注册服务。有关注册表项和激活码的详细信息，请与趋势科技代表联系。

5. 返回到**产品使用授权详细信息**窗口，单击 **更新信息**以使用新使用授权的详细信息和服务状态来刷新该窗口。此窗口还提供一个到趋势科技 Web 站点的链接，您可以利用该链接来查看关于您的使用授权的详细信息。

防毒墙网络版数据库备份

防毒墙网络版服务器数据库包含所有防毒墙网络版设置，包括扫描设置和权限。服务器数据库损坏时，如果具有备份，则可以将其恢复。随时手动备份数据库或者配置备份时间表。

备份数据库时，防毒墙网络版帮助您自动整理数据库碎片并修复所有可能的索引文件损坏。

检查系统事件日志以确定备份状态。有关详细信息，请参阅系统事件日志 第 13-34 页。

提示

趋势科技建议您为自动备份配置时间表。在服务器网络通信较低的非高峰时段期间备份数据库。

警告!

不要使用任何其他工具或软件来执行备份。仅从防毒墙网络版 Web 控制台中配置数据库备份。

备份防毒墙网络版数据库

过程

1. 转至**管理** > **设置** > **数据库备份**。
2. 键入要保存数据库的位置。如果文件夹尚不存在，请选择**不存在时创建文件夹**。包括驱动器和完整目录路径，例如 C:\OfficeScan\DatabaseBackup。

缺省情况下，防毒墙网络版将备份保存在以下目录中：<服务器安装文件夹>\DBBackup

注意

防毒墙网络版会在备份路径下创建一个子文件夹。文件夹名称表示备份的时间并且格式如下：YYYYMMDD_HHMMSS。防毒墙网络版保存 7 个最近的备份文件夹，自动删除较旧的文件夹。

3. 如果备份路径位于远程计算机（使用 UNC 路径），则键入合适的帐户名称和相应的密码。确保该帐户在上述远程计算机上具有写权限。
4. 配置备份时间表：
   a. 选择**启用预设数据库备份**。
   b. 指定备份频率和时间。
   c. 要备份数据库并保存所做的更改，请单击**立即备份**。要仅保存而不备份数据库，请单击**保存**。

恢复数据库备份文件

过程

1. 停止防毒墙网络版主服务。
2. 使用备份文件覆盖 <服务器安装文件夹>\PCCSRV\HTTPDB 中的数据库文件。
3. 重新启动防毒墙网络版主服务。

SQL Server 迁移工具

管理员可以使用 SQL Server 迁移工具将现有防毒墙网络版数据库从其本机 CodeBase 样式迁移到 SQL Server 数据库。SQL Server 迁移工具支持以下数据库迁移：

- 防毒墙网络版 CodeBase 数据库到新的 SQL Server Express 数据库
- 防毒墙网络版 CodeBase 数据库到先前存在的 SQL Server 数据库
- 已移动到其他位置的防毒墙网络版 SQL 数据库（先前进行了迁移）

使用 SQL Server 迁移工具

SQL Server 迁移工具使用 SQL Server 2008 R2 SP2 Express 将现有的 CodeBase 数据库迁移至 SQL 数据库。

提示

迁移防毒墙网络版数据库之后，可以将新迁移的 SQL 数据库迁移至其他 SQL Server。再次运行 SQL Server 迁移工具，并选择**切换至现有防毒墙网络版 SQL 数据库**，以使用其他 SQL Server。

重要信息

在使用域用户 Windows 认证凭证在 Windows Server 2008 或更高版本上运行 SQL Server 迁移工具之前：

- 需要关闭**用户访问控制**
- 不能使用用于登录 SQL Server 的域用户帐户运行防毒墙网络版主服务

过程

1. 在防毒墙网络版服务器计算机上，导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\SQL。

2. 双击 SQLTxfr.exe 运行该工具。

   此时将打开 **SQL Server 迁移工具**控制台。

3. 选择迁移类型：

选项	说明
安装新的 SQL Server 2008 R2 SP2 Express 并迁移防毒墙网络版数据库	自动安装 SQL Server 2008 R2 SP2 Express 并将现有防毒墙网络版数据库迁移到新的 SQL 数据库 **注意** 防毒墙网络版会自动将端口 1433 分配给 SQL Server。
将防毒墙网络版数据库迁移到现有的 SQL Server	将现有防毒墙网络版数据库迁移到现有 SQL Server 上新的 SQL 数据库
切换到现有的防毒墙网络版 SQL 数据库	将防毒墙网络版配置设置更改为指向现有 SQL Server 上现有的防毒墙网络版 SQL 数据库

4. 按照如下方式指定**服务器名称**：

   - 对于新 SQL 安装：<SQL Server 的主机名或 IP 地址>\<实例名称>
   - 对于 SQL Server 迁移：<SQL Server 的主机名或 IP 地址>、<端口号>\<实例名称>
   - 切换到现有的防毒墙网络版 SQL 数据库时：<SQL Server 的主机名或 IP 地址>、<端口号>\<实例名称>

   重要信息

   安装 SQL Server 时，防毒墙网络版会自动为防毒墙网络版数据库创建一个实例。迁移到现有 SQL Server 或数据库时，请为 SQL Server 上的防毒墙网络版实例键入先前存在的实例名称。

5. 为 SQL Server 数据库提供认证凭证。

重要信息

使用 **Windows 帐户**登录服务器时：

- 对于缺省域管理员帐户：
  - **用户名**格式：domain_name\administrator
  - 帐户需要下列要素：
    - 组：“管理员组”
    - 用户角色：“作为服务登录”和“作为批处理作业登录”
    - 数据库角色：“dbcreator”、“bulkadmin” 和 “db_owner”
- 对于域用户帐户：
  - **用户名**格式：domain_name\user_name
  - 帐户需要下列要素：
    - 组：“管理员组”和“域管理员”
    - 用户角色：“作为服务登录”和“作为批处理作业登录”
    - 数据库角色：“dbcreator”、“bulkadmin” 和 “db_owner”

6. 对于新的 SQL Server 安装，请键入并确认新密码。

注意

密码必须符合以下最低强度要求：

a. 最小长度：6 个字符

b. 必须至少包含以下三种字符：

- 大写字母：A - Z
- 小写字母：a - z
- 数字：0 - 9
- 特殊字符：!@#$^*?_~-();.+:

7. 指定 SQL Server 上的防毒墙网络版**数据库名称**。

将防毒墙网络版 CodeBase 数据库迁移到新的 SQL 数据库时，防毒墙网络版会自动使用所提供的名称创建新数据库。

8. 此外也可以执行以下任务：
   - 单击**测试连接**以验证现有 SQL Server 或数据库的认证凭证。
   - 单击 **SQL 数据库不可用警报…** 以配置 SQL 数据库通知设置。

     有关详细信息，请参阅配置 SQL 数据库不可用警报 第 13-46 页。
9. 单击**开始**以应用配置更改。

配置 SQL 数据库不可用警报

每当 SQL 数据库变为不可用时，防毒墙网络版会自动发送此警报。

警告!

当数据库变为不可用时，防毒墙网络版会自动停止所有服务。当数据库不可用时，防毒墙网络版将无法记录客户端或事件信息，也无法执行更新或配置客户端。

过程

1. 在防毒墙网络版服务器计算机上，导航到 <服务器安装文件夹>\PCCSRV\Admin\Utility\SQL。
2. 双击 SQLTxfr.exe 运行该工具。

   此时将打开 **SQL Server 迁移工具**控制台。
3. 单击 **SQL 数据库不可用警报…**。

   此时将打开 **SQL Server 不可用警报**窗口。
4. 键入警报收件人的电子邮件地址。

   使用半角分号 (;) 分隔多个条目。

5. 根据需要修改**主题**和**消息**。

   防毒墙网络版提供以下标记变量：

   表 13-21. SQL 数据库不可用警报标记

变量	描述
%x	防毒墙网络版 SQL Server 实例的名称
%s	受影响的防毒墙网络版服务器的名称

6. 单击**确定**。

防毒墙网络版 Web 服务器/客户端连接设置

在防毒墙网络版服务器安装过程中，安装程序会自动设置一个 Web 服务器（IIS 或 Apache Web 服务器），以使联网计算机能够连接到防毒墙网络版服务器。请配置联网终端客户端将要连接到的 Web 服务器。

如果从外部修改了 Web 服务器设置（例如，从 IIS 管理控制台），请复制这些更改以应用于防毒墙网络版。例如，如果手动更改了联网计算机的服务器的 IP 地址或如果为其分配了一个动态 IP 地址，则需要重新配置防毒墙网络版的服务器设置。

警告!

更改连接设置可能导致服务器与客户端之间的连接永久丢失，并且可能需要重新部署防毒墙网络版客户端。

配置连接设置

过程

1. 转至**管理** > **设置** > **客户端连接**。

2. 键入 Web 服务器的域名或 IPv4/IPv6 地址和端口号。

   注意

   端口号是防毒墙网络版服务器用于和防毒墙网络版客户端通信的可信端口。

3. 单击**保存**。

服务器-客户端通信

可以对防毒墙网络版进行配置，以确保服务器和客户端之间的所有通信是有效的。防毒墙网络版提供公共密钥密码系统和增强的加密功能来保护服务器和客户端之间的所有通信。

有关通信保护功能的详细信息，请参考以下部分：

- 服务器启动的通信的认证 第 13-48 页
- 增强服务器-客户端通信加密 第 13-52 页

服务器启动的通信的认证

防毒墙网络版使用公共密钥密码系统来认证防毒墙网络版服务器在客户端上启动的通信。使用公共密钥密码系统时，服务器会保留私有密钥并将公共密钥部署到所有客户端。客户端会使用该公共密钥来验证传入通信是否由服务器启动以及是否有效。如果验证成功，客户端会作出响应。

注意

防毒墙网络版不会认证客户端在服务器上启动的通信。

公共密钥和私有密钥与趋势科技证书关联。安装防毒墙网络版服务器期间，安装程序会将证书存储在主机的证书存储区上。使用认证证书管理器工具可管理趋势科技证书和密钥。

决定是否跨所有防毒墙网络版服务器使用单个认证密钥时，注意以下事项：

- 实施单个证书密钥是获得标准级别安全的常用措施。此方法可平衡组织的安全级别，并降低维护多个密钥的相关费用。
- 跨防毒墙网络版服务器实施多个证书密钥可确保最高级别的安全。在证书密钥过期并需要为服务器重新分发密钥时，这种方法会增加需要执行的维护工作。

重要信息

重新安装防毒墙网络版服务器之前，请确保已备份现有证书。新安装完成后，请导入备份的证书，以使防毒墙网络版服务器与防毒墙网络版客户端之间的通信认证保持不中断。如果在服务器安装期间创建新证书，防毒墙网络版客户端将因仍旧使用旧证书（此证书不再存在）而无法认证服务器通信。

有关备份、还原、导出和导入证书的详细信息，请参阅使用认证证书管理器 第 13-50 页。

配置服务器启动的通信的认证

过程

1. 在防毒墙网络版服务器上，转到 <服务器安装文件夹>\PCCSRV 并使用文本编辑器打开 ofcscan.ini。
2. 在 `[Global Settings]` 部分中添加或修改 `SGNF` 文本字符串。

   启用认证：`SGNF=1`

   禁用认证：`SGNF=0`

   注意

   缺省情况下，防毒墙网络版已启用认证。仅当希望禁用此功能时才将 `SGNF` 项添加到 ofcscan.ini 文件。

3. 在 Web 控制台上，转至**客户端** > **全局客户端设置**，然后单击**保存**将设置部署到客户端。

使用认证证书管理器

防毒墙网络版服务器会为公共密钥已过期的客户端保留过期的证书。例如，长时间未连接到服务器的客户端的公共密钥已过期。当客户端重新连接时，它们会将过期的公共密钥与过期的证书关联，从而能够识别服务器启动的通信。然后，服务器会将最新公共密钥部署到这些客户端。

配置证书时，请注意以下事项：

- 对于证书路径，可接受映射的驱动器和 UNC 路径。
- 选择强密码，并记录下来供将来参考。

重要信息

使用认证证书管理器工具时，请注意下列要求：

- 用户必须具有管理员权限
- 该工具只能管理位于本地终端上的证书

过程

1. 在防毒墙网络版服务器上，打开命令提示符并将目录更改为 <服务器安装文件夹>\PCCSRV\Admin\Utility\CertificateManager。
2. 发布以下任一命令：

命令	示例	描述
`CertificateManager.exe -c [Backup_Password]`	`CertificateManager.exe -c strongpassword`	生成新的趋势科技证书并替换现有证书 如果现有证书已过期或已泄露给非授权团体，可执行此操作。

命令	示例	描述
CertificateManager.exe -b [密码] [证书路径] **注意** 证书采用 ZIP 格式。	CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip	备份当前防毒墙网络版服务器产生的所有趋势科技证书 执行此操作可备份防毒墙网络版服务器上的证书。 **注意** 备份防毒墙网络版服务器证书允许您在需要重新安装防毒墙网络版服务器时使用这些证书。
CertificateManager.exe -r [密码] [证书路径] **注意** 证书采用 ZIP 格式。	CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip	在服务器上还原所有趋势科技证书 执行此操作可在重新安装的防毒墙网络版服务器上还原证书。
CertificateManager.exe -e [证书路径]	CertificateManager.exe -e <客户端安装文件夹>\OfcNTCer.dat	导出与当前所使用的证书关联的防毒墙网络版客户端公共密钥 如果客户端所使用的公共密钥损坏，可执行此操作。将 .dat 文件复制到客户端的根文件夹，以覆盖现有文件。 **重要信息** 防毒墙网络版客户端上的证书文件路径必须为： <客户端安装文件夹>\OfcNTCer.dat

命令	示例	描述
CertificateManager.exe -i [密码] [证书路径] **注意** 证书的缺省文件名为： OfcNTCer.pfx	CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx	将趋势科技证书导入到证书存储区
CertificateManager.exe -l [CSV路径]	CertificateManager.exe -l D:\Test\MismatchedAgentList.csv	（以 CSV 格式）列出当前使用不匹配证书的客户端

增强服务器-客户端通信加密

防毒墙网络版使用高级加密标准 (AES) 256 为服务器和客户端之间的通信提供增强的加密，以符合政府合规标准。

重要信息

防毒墙网络版仅支持在运行防毒墙网络版 11.0 SP1 或更高版本及插件管理器 2.2 或更高版本的服务器和客户端上进行 AES-256 加密。

警告!

启用 AES-256 加密之前，确保将服务器管理的所有防毒墙网络版客户端升级到版本 11.0 SP1。旧版的防毒墙网络版客户端可能无法解密 AES-256 加密通信。如果使用代理服务器，在旧版的防毒墙网络版客户端上启用 AES-256 加密可能会导致与防毒墙网络版服务器的通信完全丢失。

过程

1. 转至**客户端** > **全局客户端设置**。
2. 转至**服务器-客户端通信**部分。
3. 单击**对防毒墙网络版服务器和防毒墙网络版客户端之间的通信使用 AES-256 加密**旁边的**更改**按钮。

   此时将显示一条消息。
4. 单击**验证版本**以确认您已将所有客户端更新到防毒墙网络版 11.0 SP1 或更高版本。
5. 单击**确定**。

Web 控制台密码

仅当服务器计算机不具有使用基于角色的管理所需的资源时，才可以访问用于管理 Web 控制台密码（或在防毒墙网络版服务器安装期间创建的 root 帐户的密码）的窗口。例如，如果服务器计算机运行 Windows Server 2003，但没有安装 Authorization Manager Runtime，则可以访问该窗口。如果资源满足需要，则此窗口不显示，这时可以通过在**用户帐户**窗口中修改 root 帐户来管理密码。

如果没有将防毒墙网络版注册到控制管理中心，请与技术支持提供商联系以获取如何访问 Web 控制台的说明。

Web 控制台设置

使用 **Web 控制台设置**窗口可执行下列操作：

- 配置防毒墙网络版服务器以定期刷新“摘要”控制台。缺省情况下，服务器将每隔 30 秒刷新控制台。间隔时间可以是 10 到 300 秒。

- 指定 Web 控制台超时设置。缺省情况下，如果用户在 30 分钟内不进行任何操作，会自动从 Web 控制台注销。无操作时间可以是 10 到 60 分钟。

配置 Web 控制台设置

过程

1. 转至**管理** > **设置** > **Web 控制台**。
2. 选择**启用自动刷新**，然后选择刷新间隔。
3. 选择**启用自动从 Web 控制台注销**，然后选择超时间隔。
4. 单击**保存**。

隔离管理器

只要防毒墙网络版客户端检测到安全风险且扫描处理措施为隔离，它就会加密受感染文件并将其移动到位于 <客户端安装文件夹>\SUSPECT 中的本地隔离文件夹。

将文件移动到本地隔离目录之后，防毒墙网络版客户端会将其发送到指定的隔离目录中。在**客户端** > **客户端管理** > **设置** > **{扫描类型} 设置** > **处理措施**选项卡中指定该目录。指定隔离目录中的文件会被加密，以防止其感染其他文件。请参阅隔离目录 第 7-34 页以获取详细信息。

如果指定的隔离目录位于防毒墙网络版服务器计算机上，则从 Web 控制台修改服务器的隔离目录设置。服务器将隔离文件存储到 <服务器安装文件夹>\PCCSRV\Virus 中。

注意

如果防毒墙网络版客户端由于任何原因（如，网络连接问题）无法将加密的文件发送到防毒墙网络版服务器，则加密的文件将仍然保留在防毒墙网络版客户端隔离文件夹中。连接到防毒墙网络版服务器时，防毒墙网络版客户端将尝试重新发送该文件。

配置隔离目录设置

过程

1. 转至**管理** > **设置** > **隔离管理器**。
2. 接受或修改隔离文件夹的缺省容量以及防毒墙网络版可以存储在隔离文件夹内的最大受感染文件大小。

   缺省值将显示在此窗口上。
3. 单击**保存隔离设置**。
4. 要移除隔离文件夹中的所有现有文件，请单击**删除所有隔离文件**。

服务器调节程序

使用服务器调节程序来优化使用参数的防毒墙网络版服务器的性能，以解决以下与服务器相关的性能问题：

- **下载**

  当请求从防毒墙网络版服务器更新的防毒墙网络版客户端（包括更新代理）数量超过服务器的可用资源时，服务器会将客户端的更新请求移动到队列中并在资源可用时处理请求。成功从防毒墙网络版服务器更新组件后，客户端会通知服务器更新完成。设置防毒墙网络版服务器等待接收来自客户端的更新通知的最长时间（分钟）。另请设置服务器尝试通知客户端执行更新以及通知客户端应用新配置设置的最大次数。仅当未收到客户端通知时，服务器才会不断尝试。

- **缓存**

  防毒墙网络版服务器收到来自防毒墙网络版客户端客户端的多个请求（例如，执行更新的请求）时，服务器会尽其所能处理请求并将剩余的请求放入缓存中。服务器然后在资源可用时每次处理一个保存在缓存中的请求。为事件（例如客户端更新请求）和客户端日志报告指定缓存大小。

- **网络通信**

  网络通信量在一天中不断变化。要控制到防毒墙网络版服务器以及到其他更新源的网络通信流，请指定在一天中任何给定时间可以同时更新的防毒墙网络版客户端数。

服务器调节程序需要以下文件：SvrTune.exe

服务器调节程序

过程

1. 在防毒墙网络版服务器计算机上，转到 <服务器安装文件夹>\PCCSRV\Admin\Utility\SvrTune。
2. 双击 SvrTune.exe 启动服务器调节程序。

   将打开服务器调节程序控制台。
3. 在**下载**下，修改以下设置：
   - **客户端超时**：键入防毒墙网络版服务器等待从客户端接收更新响应的时间（分钟）。如果客户端在上述指定时间内没有响应，则防毒墙网络版服务器认为该客户端不具有当前组件。如果通知的客户端超时，则为另一个正在等待通知的客户端提供一个位置。
   - **更新代理超时**：键入防毒墙网络版服务器等待从更新代理接收更新响应的时间（分钟）。如果通知的客户端超时，则为另一个正在等待通知的客户端提供一个位置。
   - **重试次数**：键入防毒墙网络版服务器尝试通知客户端执行更新或通知客户端应用新配置设置的最大次数。

- **重试间隔**：键入防毒墙网络版服务器在两次通知尝试之间等待的时间（分钟）。

4. 在**网络通信**下，修改以下设置：
   - **正常时间**：单击表示您认为一天中网络通信正常的时间的单选按钮。
   - **离峰时间**：单击表示您认为一天中网络通信最低的时间的单选按钮。
   - **高峰时间**：单击表示您认为一天中网络通信为高峰的时间的单选按钮。
   - **最大客户端连接数量**：键入既可以从?其他更新源?也可以从防毒墙网络版服务器同时更新组件的最大客户端数量。键入各个时间段的最大客户端数量。达到最大连接数量时，防毒墙网络版客户端仅能在当前客户端连接关闭后再更新组件（可能是因为更新的完成或因为客户端响应时间达到了您在**客户端超时**或**更新代理超时**文本框中指定的值）。
5. 单击**确定**。将显示一个提示，询问您是否要重新启动防毒墙网络版主服务。

注意

仅重新启动服务，而非计算机。

6. 从以下重新启动选项中选择：
   - 单击**是**保存服务器调节程序设置并重新启动服务。重新启动后，设置立即生效。
   - 单击**否**保存服务器调节程序设置但不重新启动服务。重新启动防毒墙网络版主服务或重新启动防毒墙网络版服务器计算机以使设置生效。

云安全智能反馈

趋势科技云安全智能反馈将与云安全智能防护网络分享匿名威胁信息，从而使趋势科技可以快速地对新威胁进行识别和处理。可以随时通过此控制台禁用云安全智能反馈。

参与云安全智能反馈计划

过程

1. 转至**管理** > **云安全智能防护** > **云安全智能反馈**。
2. 单击**启用趋势科技云安全智能反馈**。
3. 要帮助趋势科技了解贵组织，请选择**行业**类型。
4. 要发送防毒墙网络版客户端上的文件中潜在安全威胁的相关信息，请选中**启用可疑程序文件的反馈**复选框。

   注意

   发送到云安全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。

5. 要配置发送反馈的条件，请选择在特定时间长度内触发反馈的检测次数。
6. 指定发送反馈时防毒墙网络版可以使用的最大带宽，以尽可能减少网络中断。
7. 单击**保存**。

第 14 章

管理防毒墙网络版客户端

本章介绍防毒墙网络版客户端的管理和配置。

主题包括：

- 终端位置 第 14-2 页
- 防毒墙网络版客户端程序管理 第 14-5 页
- 客户端-服务器连接 第 14-25 页
- 防毒墙网络版客户端代理服务器设置 第 14-44 页
- 查看防毒墙网络版客户端信息 第 14-49 页
- 导入和导出客户端设置 第 14-49 页
- 安全合规 第 14-51 页
- 趋势科技虚拟桌面支持 第 14-67 页
- 全局客户端设置 第 14-80 页
- 配置客户端权限和其他设置 第 14-81 页

终端位置

防毒墙网络版提供位置感知功能，可判断防毒墙网络版客户端的位置位于内部或外部。在以下防毒墙网络版功能和服务中利用了位置感知：

表 14-1. 利用位置感知的功能和服务

功能/服务	描述
Web 信誉服务	防毒墙网络版客户端的位置决定防毒墙网络版客户端将应用的 Web 信誉策略。管理员通常会为外部客户端执行更为严格的策略。 有关 Web 信誉策略的详细信息，请参阅 Web 信誉策略 第 11-4 页。
文件信誉服务	对于使用云安全扫描的客户端，防毒墙网络版客户端的位置决定客户端向其发送扫描查询的云安全智能防护源。 外部防毒墙网络版客户端向云安全智能防护网络发送扫描查询，而内部客户端向在云安全智能防护源列表中定义的源发送查询。 有关云安全智能防护源的详细信息，请参阅云安全智能防护源 第 4-5 页。
数据丢失防护	防毒墙网络版客户端的位置决定客户端将应用的数据丢失防护策略。管理员通常会为外部客户端执行更为严格的策略。 有关数据丢失防护策略的详细信息，请参阅数据丢失防护策略 第 10-3 页。
设备控制	防毒墙网络版客户端的位置决定客户端将应用的设备控制策略。管理员通常会为外部客户端执行更为严格的策略。 有关设备控制策略的详细信息，请参阅设备控制 第 9-2 页。

位置条件

指定该位置是基于防毒墙网络版客户端终端的网关 IP 地址，还是基于防毒墙网络版客户端与防毒墙网络版服务器或任何参考服务器的连接状态。

- **客户端连接状态**：如果防毒墙网络版客户端可以连接到防毒墙网络版服务器或 Intranet 中任何指定参考服务器，则终端位置位于内部。此外，如果

公司网络之外的任何终端可与防毒墙网络版服务器/参考服务器建立连接，则其位置也位于内部。如果不符合以上任何条件，则终端位置位于外部。

- **网关 IP 和 MAC 地址**：如果防毒墙网络版客户端 终端的网关 IP 地址与您在**终端位置**窗口上指定的任何网关 IP 地址相匹配，则终端位置位于内部。否则，终端位置位于外部。

配置位置设置

过程

1. 转至**客户端 > 终端位置**。
2. 选择位置是基于**客户端连接状态**还是**网关 IP 和 MAC 地址**。
3. 如果选择**客户端连接状态**，请决定是否要使用参考服务器。

   请参阅参考服务器 第 13-30 页以了解详细信息。

   a. 如果未指定参考服务器，当发生以下事件时，防毒墙网络版客户端将检查与防毒墙网络版服务器的连接状态：

      - 防毒墙网络版客户端从漫游模式切换到普通（联机或脱机）模式。
      - 防毒墙网络版客户端从一种扫描方法切换到另一种扫描方法。请参阅扫描方法类型 第 7-7 页以了解详细信息。
      - 防毒墙网络版客户端检测到终端中发生 IP 地址变更。
      - 防毒墙网络版客户端重新启动。
      - 服务器启动连接验证。请参阅防毒墙网络版客户端图标 第 14-26 页以了解详细信息。
      - 应用全局设置时 Web 信誉位置条件发生变化。
      - 不再执行爆发阻止策略，并且已恢复爆发前设置。

b. 如果指定了参考服务器，防毒墙网络版客户端将首先检查其与防毒墙网络版服务器的连接状态，当与防毒墙网络版服务器的连接不成功时，将检查其与参考服务器的连接状态。防毒墙网络版客户端每小时检查连接状态一次，发生上述任一事件时也会进行检查。

4. 如果选择**网关 IP 和 MAC 地址**：

   a. 在提供的文本框中键入网关 IPv4/IPv6 地址。

   b. 键入 MAC 地址。

   c. 单击**添加**。

      如果没有键入 MAC 地址，防毒墙网络版将包括所有属于指定 IP 地址范围的 MAC 地址。

   d. 重复步骤 a 到 c 直到获得所有要添加的网关 IP 地址。

   e. 使用网关设置导入程序工具导入网关设置列表。

      请参阅网关设置导入程序 第 14-4 页以了解详细信息。

5. 单击**保存**。

网关设置导入程序

防毒墙网络版会检查终端的位置，以确定要使用的 Web 信誉策略以及要连接到的云安全智能防护源。防毒墙网络版识别位置的一种方法是通过检查终端的网关 IP 地址和 MAC 地址。

可以在**终端位置**窗口上配置网关设置，或者使用网关设置导入程序工具将网关设置列表导入到**终端位置**窗口。

使用网关设置导入程序

过程

1. 准备包含网关设置列表的文本文件 (.txt)。在每一个行上，键入 IPv4 或 IPv6 地址，也可根据需要键入 MAC 地址。

使用半角逗号分隔 IP 地址和 MAC 地址。最大条目数为 4096。

例如：

```
10.1.111.222,00:17:31:06:e6:e7

2001:0db7:85a3:0000:0000:8a2e:0370:7334

10.1.111.224,00:17:31:06:e6:e7
```

2. 在服务器计算机上，转至 <服务器安装文件夹>\PCCSRV\Admin\Utility\GatewaySettingsImporter，然后双击 GSImporter.exe。

注意

不能通过终端服务运行网关设置导入程序工具。

3. 在**网关设置导入程序**窗口上，浏览到步骤 1 中创建的文件，然后单击**导入**。
4. 单击**确定**。

   网关设置显示在**终端位置**窗口上，防毒墙网络版服务器会将设置部署到防毒墙网络版客户端客户端。
5. 要删除所有条目，请单击**全部清除**。

   如果仅需要删除特定条目，则从**终端位置**窗口中将其移除。
6. 要将设置导出到文件，请单击**全部导出**，然后指定文件名和类型。

防毒墙网络版客户端程序管理

下列主题讨论管理和保护防毒墙网络版客户端程序的方法：

- 防毒墙网络版客户端服务 第 14-6 页
- 重新启动防毒墙网络版客户端服务 第 14-11 页
- 防毒墙网络版客户端自我保护 第 14-12 页

- 防毒墙网络版客户端安全 第 14-16 页
- 防毒墙网络版客户端控制台访问限制 第 14-17 页
- 防毒墙网络版客户端退出和解锁 第 14-18 页
- 防毒墙网络版客户端漫游权限 第 14-19 页
- 客户端迁移程序 第 14-22 页
- 非活动防毒墙网络版客户端 第 14-25 页

防毒墙网络版客户端服务

防毒墙网络版客户端会运行下表中所列的服务。您可以从 Microsoft 管理控制台中查看这些服务的状态。

表 14-2. 防毒墙网络版客户端服务

服务	受控的功能
趋势科技未授权更改阻止服务 (TMBMSRV.exe)	• 行为监控 • 设备控制 • 安全软件认证服务
防毒墙网络版 NT 防火墙 (TmPfw.exe)	防毒墙网络版防火墙
防毒墙网络版数据保护服务 (dsagent.exe)	• 数据丢失防护 • 设备控制
防毒墙网络版 NT Listener (tmlisten.exe)	防毒墙网络版客户端与防毒墙网络版服务器之间的通信
防毒墙网络版 NT 代理服务 (TmProxy.exe)	• Web 信誉 • POP3 邮件扫描

服务	受控的功能
防毒墙网络版 NT 实时扫描 (ntrtscan.exe)	• 实时扫描 • 预设扫描 • 手动扫描/立即扫描
防毒墙网络版通用客户端解决方案框架 (TmCCSF.exe)	高级保护服务 • 浏览器安全漏洞防御 • 内存扫描

下列服务提供强大的防护，但它们的监控机制会加剧系统资源的使用，特别是在运行耗费大量系统资源的应用程序的服务器上。

- 趋势科技未授权更改阻止服务 (TMBMSRV.exe)
- 防毒墙网络版 NT 防火墙 (TmPfw.exe)
- 防毒墙网络版数据保护服务 (dsagent.exe)

因此，在服务器平台（Windows Server 2003、Windows Server 2008 和 Windows Server 2012）上会缺省禁用这些服务。如果要启用这些服务，请执行以下操作：

- 持续监控系统性能，并在发现性能下降时采取必要的处理措施。
- 对于 TMBMSRV.exe，如果您将耗用大量系统资源的应用程序从行为监控策略排除，则可以启用该服务。您可以使用性能调整工具来标识耗费大量系统资源的应用程序。有关详细信息，请参阅使用趋势科技性能调整工具 第 14-9 页。

对于桌面平台，仅在发现性能严重下降时才禁用这些服务。

从 Web 控制台启用或禁用客户端服务

过程

1. 转至**客户端** > **客户端管理**。

2. 对于运行 Windows XP、Vista、7、8、8.1 或 10 的防毒墙网络版客户端：

   a. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。

   注意

   选择根域或特定域时，设置只会应用到运行 Windows XP、Vista、7、8、8.1 或 10 的客户端。即使运行任何 Windows Server 平台的客户端属于这些域，设置也不会应用到这些客户端。

   b. 单击**设置** > **其他服务设置**。

   c. 选中或清除以下部分中的复选框：

      - **未授权更改阻止服务**
      - **防火墙服务**
      - **可疑连接服务**
      - **数据保护服务**
      - **高级保护服务**

   d. 单击**保存**以将设置应用于域。如果选择了根域图标，则从下列选项进行选择：

      - **应用到全部客户端**：将设置应用到所有现有 Windows XP/Vista/7/8/8.1/10 客户端以及已添加到现有/将来域的任何新客户端。将来域是在您配置设置时还未创建的域。
      - **仅应用到将来的域**：仅将设置应用到添加到将来域的 Windows XP/Vista/7/8/8.1/10 客户端。此选项不会将设置应用到添加到现有域的新客户端。

3. 对于运行 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 的防毒墙网络版客户端：

   a. 在客户端树中选择单个客户端。

   b. 单击**设置** > **其他服务设置**。

c. 选中或清除以下部分中的复选框：

- **未授权更改阻止服务**
- **防火墙服务**
- **可疑连接服务**
- **数据保护服务**
- **高级保护服务**

d. 单击**保存**。

使用趋势科技性能调整工具

过程

1. 从以下位置下载趋势科技性能调整工具：

   http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionID=69719

2. 解压缩 TMPerfTool.zip 以提取 TMPerfTool.exe。
3. 将 TMPerfTool.exe 放在 <客户端安装文件夹> 或 TMBMCLI.dll 所在的文件夹中。
4. 右键单击 TMPerfTool.exe，然后选择**以管理员身份运行**。
5. 阅读并接受最终用户协议，然后单击**确定**。
6. 单击**分析**。

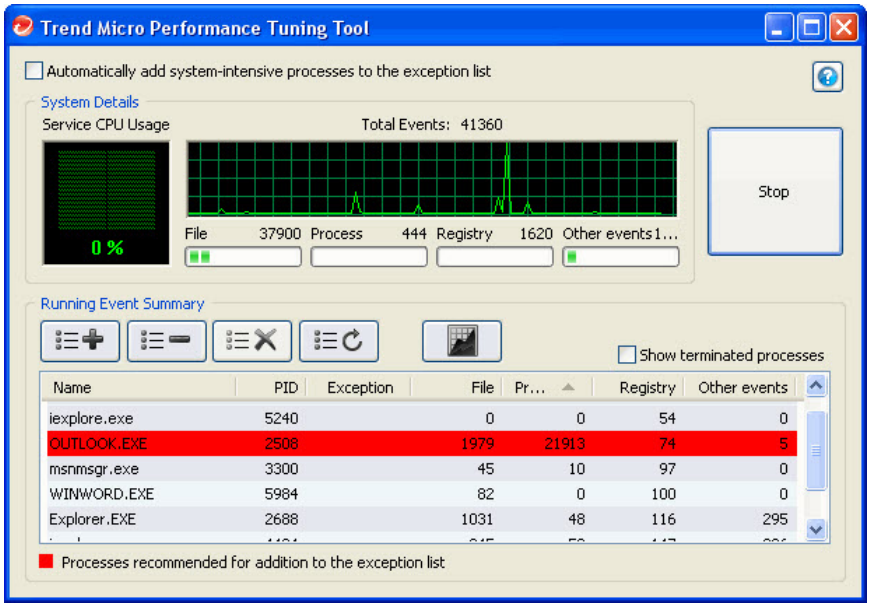


图 14-1. 突出显示耗费大量系统资源的进程

工具开始监控 CPU 使用情况和事件加载。耗费大量系统资源的进程会以红色突出显示。

7. 选择耗费大量系统资源的进程，然后单击**添加至例外列表 (允许)** 按钮 ( )。

8. 检查系统或应用程序性能是否有所提升。

9. 如果性能有所提升，再次选择该进程，然后单击**从例外列表移除**按钮 ( )。

10. 如果性能再次下降，则执行下列步骤：

    a. 记录应用程序的名称。

    b. 单击**停止**。

    c. 单击**生成报告**按钮（ ），然后保存该 .xml 文件。

d. 检查已确定为发生冲突的应用程序，并将它们添加到“行为监控”例外列表中。

有关详细信息，请参阅行为监控例外列表 第 8-5 页。

重新启动防毒墙网络版客户端服务

防毒墙网络版会重新启动意外停止响应（而不是由正常系统进程停止）的防毒墙网络版客户端服务。有关客户端服务的详细信息，请参阅防毒墙网络版客户端服务 第 14-6 页。

需要配置必需的设置，以使防毒墙网络版客户端服务重新启动。

配置服务重新启动设置

过程

1. 转至**客户端 > 全局客户端设置**。
2. 转至**重新启动防毒墙网络版服务**部分。
3. 选择**防毒墙网络版客户端服务意外终止后，自动重新启动该服务**。
4. 配置以下信息：
   - **__ 分钟后重新启动服务**：指定防毒墙网络版重新启动服务之前的等候时间（以分钟为单位）。
   - **如果首次尝试重新启动服务不成功，请重试 __ 次**：指定重新启动服务的最大重试次数。如果服务在最大重试次数后仍然停止，则手动重新启动服务。
   - **_ 小时后重置重新启动失败计数**：如果服务在用尽最大重试次数后仍然停止，则防毒墙网络版会等待若干小时，然后重置失败计数。如果这些小时过后服务仍然停止，则防毒墙网络版会重新启动服务。

防毒墙网络版客户端自我保护

防毒墙网络版客户端自我保护为防毒墙网络版客户端提供保护其正常运行所需的进程及其他资源的方式。防毒墙网络版客户端自我保护可帮助阻止程序或实际用户尝试禁用防恶意软件防护。

防毒墙网络版客户端自我保护可提供下列选项：

- 保护防毒墙网络版客户端服务 第 14-13 页
- 保护防毒墙网络版客户端安装文件夹中的文件 第 14-13 页
- 保护防毒墙网络版客户端注册表项 第 14-15 页
- 保护防毒墙网络版客户端进程 第 14-15 页

配置防毒墙网络版客户端自我保护设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡，然后转到**防毒墙网络版客户端自我保护**部分。
5. 启用以下选项：
   - 保护防毒墙网络版客户端服务 第 14-13 页
   - 保护防毒墙网络版客户端安装文件夹中的文件 第 14-13 页
   - 保护防毒墙网络版客户端注册表项 第 14-15 页
   - 保护防毒墙网络版客户端进程 第 14-15 页
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

- **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
- **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

保护防毒墙网络版客户端服务

防毒墙网络版会阻止终止下列防毒墙网络版客户端服务的所有尝试：

- 防毒墙网络版 NT Listener (TmListen.exe)
- 防毒墙网络版 NT 实时扫描 (NTRtScan.exe)
- 防毒墙网络版 NT 代理服务 (TmProxy.exe)
- 防毒墙网络版 NT 防火墙 (TmPfw.exe)
- 防毒墙网络版数据保护服务 (dsagent.exe)
- 趋势科技未授权更改阻止服务 (TMBMSRV.exe)

注意

如果启用此选项，防毒墙网络版可能阻止您在终端上成功安装第三方产品。如果遇到此问题，您可以先暂时禁用此选项，然后在安装完第三方产品之后重新启用此选项。

- 趋势科技通用客户端解决方案框架 (TmCCSF.exe)

保护防毒墙网络版客户端安装文件夹中的文件

为防止其他程序（甚至用户）修改或删除防毒墙网络版客户端文件，防毒墙网络版提供了多种增强的保护功能。

启用**保护防毒墙网络版客户端安装文件夹中的文件**之后，防毒墙网络版会在根文件夹 <客户端安装文件夹> 中锁定以下文件：

- 扩展名为 .exe、.dll 和 .sys 的所有数字签名的文件
- 某些不具有数字签名的文件包括：
  - bspatch.exe
  - bzip2.exe
  - INETWH32.dll
  - libcurl.dll
  - libeay32.dll
  - libMsgUtilExt.mt.dll
  - msvcm80.dll
  - MSVCP60.DLL
  - msvcp80.dll
  - msvcr80.dll
  - OfceSCV.dll
  - OFCESCVPack.exe
  - patchbld.dll
  - patchw32.dll
  - patchw64.dll
  - PiReg.exe
  - ssleay32.dll
  - Tmeng.dll
  - TMNotify.dll
  - zlibwapi.dll

启用**保护防毒墙网络版客户端安装文件夹中的文件**以及实时扫描以查找病毒/恶意软件威胁之后，防毒墙网络版将执行以下处理措施：

- 启动安装文件夹中的 .exe 文件之间进行文件完整性检查

  在 ActiveUpdate 更新期间，防毒墙网络版会验证触发更新的文件发起方是否为趋势科技。如果识别到发起方不是趋势科技，并且 ActiveUpdate 无法替换不正确的文件，防毒墙网络版会将该事件记录在 Windows 事件日志中并阻止更新。

- 防止 DLL 劫持

  某些恶意软件编写者将动态链接库文件复制到防毒墙网络版客户端安装文件夹或行为监控文件夹中，试图在客户端加载之前加载这些文件。这些文件企图中断防毒墙网络版提供的保护。为了防止将劫持文件复制到防毒墙网络版客户端文件夹，防毒墙网络版可阻止将这些文件复制到安装文件夹和行为监控文件夹。

- 使用 Windows 中的 “SHARE:NONE” 设置防止锁定文件

保护防毒墙网络版客户端注册表项

防毒墙网络版阻止修改、删除下列注册码和子键下的条目或者向其中添加新条目的所有尝试：

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

保护防毒墙网络版客户端进程

防毒墙网络版阻止终止下表中进程的所有尝试。

进程	描述
TmListen.exe	接收来自防毒墙网络版服务器的命令和通知，并简化防毒墙网络版客户端到服务器的通信
NTRtScan.exe	对防毒墙网络版客户端执行实时扫描、预设扫描和手动扫描
TmProxy.exe	在将网络通信传递给目标应用程序之前，先对其进行扫描。
TmPfw.exe	提供数据包级防火墙、网络病毒扫描和入侵检测功能
TMBMSRV.exe	控制对外部存储设备的访问并阻止对注册表项和进程的未授权更改
DSAgent.exe	监控敏感数据的传输并控制对设备的访问
PccNTMon.exe	此进程负责启动防毒墙网络版客户端控制台
TmCCSF.exe	执行浏览器安全漏洞防御和内存扫描

防毒墙网络版还可以防止在 Microsoft 软件限制策略 (SRP) 中添加进程。软件限制策略可防止列出的应用程序在终端上运行。防止在软件限制策略列表中添加防毒墙网络版进程：

1. 启用**保护防毒墙网络版客户端进程**。

2. 启用**未授权更改阻止服务**。

   有关详细信息，请参阅从 Web 控制台启用或禁用客户端服务 第 14-7 页。

防毒墙网络版客户端安全

通过从两个安全设置中选择想要的选项，控制用户对防毒墙网络版客户端安装目录和注册表设置的访问。

控制对防毒墙网络版客户端安装目录和注册表项的访问

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡，然后转到**客户端安全设置**部分。
5. 从以下访问权限进行选择：
   - **高**：防毒墙网络版客户端安装目录从 Program Files 文件夹继承权限，防毒墙网络版客户端注册表项从 `HKLM\Software` 注册表项继承权限。对于大多数 Active Directory 配置，此级别会自动将“普通”用户（即，无管理员权限的那些用户）限制为只读访问权限。
   - **正常**：此权限授予所有用户（用户组“Everyone”）对防毒墙网络版客户端程序目录和防毒墙网络版客户端注册表项的完全访问权限。

注意

防毒墙网络版客户端自我保护设置的优先级高于**防毒墙网络版客户端安全设置**。配置了这两种设置的防毒墙网络版客户端首先应用**防毒墙网络版客户端自我保护**设置。

例如，如果将**防毒墙网络版客户端安全设置**配置为**正常**，并启用**防毒墙网络版客户端自我保护**设置中的文件保护，则**防毒墙网络版客户端自我保护**设置将阻止用户修改扩展名为 .exe、.dll、.ptn 或 .sys 的防毒墙网络版客户端文件。

6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

防毒墙网络版客户端控制台访问限制

此设置不允许从系统托盘或 Windows“开始”菜单访问防毒墙网络版客户端控制台。用户访问防毒墙网络版客户端控制台的唯一方法是双击<客户端安装文件夹>中的 PccNTMon.exe。配置此设置后，请重新加载防毒墙网络版客户端，以使该设置生效。

此设置不禁用防毒墙网络版客户端。该防毒墙网络版客户端会在后台运行并继续提供抵御安全风险的防护。

限制对防毒墙网络版客户端控制台的访问

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。

3. 单击**设置** > **权限和其他设置**。
4. 单击**其他设置**选项卡，然后转到**防毒墙网络版客户端访问限制**部分。
5. 选择**不允许用户从系统托盘或 Windows“开始”菜单访问防毒墙网络版客户端控制台**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

防毒墙网络版客户端退出和解锁

防毒墙网络版客户端的退出和解锁权限允许用户（使用密码或无需密码）临时停止防毒墙网络版客户端，或者获取对高级 Web 控制台功能的访问权限。

授予客户端退出和解锁权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转到**退出和解锁**部分。
5. 要允许无需密码就可退出防毒墙网络版客户端，请选择**不需要输入密码**。
   - 如果要求输入密码，则选择**需要输入密码**，然后键入并确认密码。

6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

防毒墙网络版客户端漫游权限

如果客户端与服务器之间的事件干扰用户的任务，可以授予特定用户防毒墙网络版客户端漫游权限。例如，经常进行演示的用户可在开始演示之前启用漫游模式，以阻止防毒墙网络版服务器部署防毒墙网络版客户端设置和在防毒墙网络版客户端上启动扫描。

防毒墙网络版客户端处于漫游模式时：

- 防毒墙网络版客户端不向防毒墙网络版服务器发送日志，即使服务器与客户端之间存在可用连接。
- 防毒墙网络版服务器不会启动任务，也不会将防毒墙网络版客户端设置部署到客户端，即使服务器与客户端之间存在可用连接。
- 如果防毒墙网络版客户端客户端可以连接到任一更新源，则会更新组件。源包括防毒墙网络版服务器、更新代理或定制更新源。

  下列事件会触发漫游客户端上的更新：

  - 用户执行手动更新。
  - 自动客户端更新运行。您可以禁用漫游客户端上的自动客户端更新。

    有关详细信息，请参阅禁用漫游客户端上的自动客户端更新 第 14-20 页。

  - 预设更新运行。仅具有所需权限的客户端可以运行预设更新。您可以随时撤销此权限。

有关详细信息，请参阅撤销漫游防毒墙网络版客户端上的预设更新权限 第 14-21 页。

授予客户端漫游权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转到**漫游**部分。
5. 选择**启用漫游模式**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

禁用漫游客户端上的自动客户端更新

过程

1. 转至**更新** > **客户端** > **自动更新**。
2. 转至**事件触发更新**部分。
3. 禁用**包括漫游客户端和脱机客户端**。

注意

如果禁用**防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新**，系统会自动禁用此选项。

撤销漫游防毒墙网络版客户端上的预设更新权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 或选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转至**组件更新**部分。
5. 清除**启用/禁用基于时间表的更新**选项。
6. 单击**保存**。

防毒墙网络版客户端语言配置

您可以将所有防毒墙网络版客户端配置为使用防毒墙网络版服务器语言设置或本地登录用户的语言设置进行显示。安装或升级防毒墙网络版客户端程序之后，客户端将应用在**全局设置**窗口中配置的语言设置。

缺省情况下，如果防毒墙网络版客户端不支持已登录用户的语言设置，语言设置将缺省为防毒墙网络版服务器语言，然后是英文。

配置防毒墙网络版客户端语言设置

过程

1. 转至**客户端** > **全局客户端设置**。
2. 转至**客户端语言配置**部分。
3. 指定防毒墙网络版客户端如何应用语言设置：
   - **终端上的本地语言设置**：防毒墙网络版客户端使用已登录用户的语言设置显示。

     注意

     如果防毒墙网络版客户端不支持已登录用户的语言设置，客户端会应用防毒墙网络版服务器语言。如果终端不支持防毒墙网络版服务器语言，则显示英文。
   - **防毒墙网络版服务器语言**：防毒墙网络版客户端使用防毒墙网络版服务器语言显示。

     注意

     如果终端不支持防毒墙网络版服务器语言，则显示英文。
4. 单击**保存**。

客户端迁移程序

如果网络上存在多个防毒墙网络版服务器，则使用客户端迁移程序工具将防毒墙网络版客户端从一台防毒墙网络版服务器转移到另一台。将新的防毒墙网络版服务器添加到网络后，如果希望将现有防毒墙网络版客户端客户端转移到新服务器，则此程序非常有用。

注意

这两台服务器必须具有相同的语言版本。如果使用客户端迁移程序将任何运行早期版本的防毒墙网络版客户端移动到当前版本的服务器，则防毒墙网络版客户端会自动升级。

在使用此工具之前，请确保您使用的帐户具有管理员权限。

运行客户端迁移程序

过程

1. 在防毒墙网络版服务器上，转至 <服务器安装文件夹>\PCCSRV\Admin\Utility\IpXfer。
2. 将 IpXfer.exe 复制到防毒墙网络版客户端终端。如果防毒墙网络版客户端终端运行 x64 类型平台，则复制 IpXfer_x64.exe。
3. 在防毒墙网络版客户端终端上打开命令提示符，然后转到将该可执行文件复制到的文件夹。
4. 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> -d <域或域层次结构> -e <证书位置和文件名>

表 14-3. 客户端迁移程序参数

参数	说明
<可执行文件名>	IpXfer.exe 或 IpXfer_x64.exe
-s <服务器名称>	目标防毒墙网络版服务器（防毒墙网络版客户端要转移到的服务器）的名称
-p <服务器侦听端口>	目标防毒墙网络版服务器的侦听端口（或可信端口）。要查看防毒墙网络版 Web 控制台上的侦听端口，请在主菜单中单击**管理** > **设置** > **客户端连接**。
-c <客户端侦听端口>	防毒墙网络版客户端终端用于与服务器通信的端口号

参数	说明
-d <域或域层次结构>	将客户端分组到的客户端树域或子域。域层次结构应指明该子域。
-e <证书位置和文件名>	在迁移过程中导入防毒墙网络版客户端的新认证证书。如果不使用此参数，防毒墙网络版客户端将自动从新管理服务器检索当前认证证书。 **注意** 防毒墙网络版服务器上的缺省证书位置为： <服务器安装文件夹>\PCCSRV\Pccnt\Common\OfcNTCer.dat。 使用来自非防毒墙网络版的源的证书时，确保证书采用可区别编码规则 (DER) 格式。

示例：

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

ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01
```

5. 要确定防毒墙网络版客户端现在是否向其他服务器报告，请执行以下操作：

   a. 在防毒墙网络版客户端终端上，右键单击系统托盘中的防毒墙网络版客户端程序图标。

   b. 选择**组件版本**。

   c. 在**服务器名称/端口**文本框中检查作为防毒墙网络版客户端报告对象的防毒墙网络版服务器。

   注意

   如果该防毒墙网络版客户端未显示在管理它的新防毒墙网络版服务器的客户端树中，请重新启动新服务器的主服务 (ofservice.exe)。

非活动防毒墙网络版客户端

当使用防毒墙网络版客户端卸载程序从终端删除防毒墙网络版客户端程序时，该程序将自动通知服务器。当服务器收到此通知时，它将在客户端树中删除防毒墙网络版客户端图标以显示该客户端已不再存在。

但是，如果使用其他方法删除防毒墙网络版客户端，如重新格式化终端硬盘驱动器或手动删除防毒墙网络版客户端文件，则防毒墙网络版将不会注意到它的删除，而只会将防毒墙网络版客户端显示为非活动。如果用户长时间退出或禁用防毒墙网络版客户端，服务器也会将该防毒墙网络版客户端显示为非活动。

要使客户端树仅显示活动客户端，请将防毒墙网络版配置为自动从客户端树中删除非活动客户端。

自动移除非活动客户端

过程

1. 转至**管理** > **设置** > **非活动客户端**。
2. 选择**允许自动删除非活动客户端**。
3. 选择防毒墙网络版认为防毒墙网络版客户端处于非活动期超过 __ 天后自动将其删除。
4. 单击**保存**。

客户端-服务器连接

防毒墙网络版客户端必须与其父级服务器之间保持持续连接，才能及时更新组件、接收通知，以及应用配置更改。下列主题讨论如何检查防毒墙网络版客户端的连接状态和解决连接问题：

- 客户端 IP 地址 第 5-8 页

- 防毒墙网络版客户端图标 第 14-26 页
- 客户端-服务器连接验证 第 14-39 页
- 连接验证日志 第 14-40 页
- 无法访问客户端 第 14-40 页

防毒墙网络版客户端图标

系统托盘中的防毒墙网络版客户端图标会提供视觉提示，指出防毒墙网络版客户端的当前状态，并提示用户执行某些操作。该图标在任意给定的时间均会显示下列视觉提示的组合。

表 14-4. 防毒墙网络版客户端图标中指出的防毒墙网络版客户端状态

客户端状态	描述	视觉提示
客户端与防毒墙网络版服务器之间的连接	联机客户端已连接到防毒墙网络版服务器。服务器可以启动任务并将设置部署到这些客户端	图标包含一个类似波动信号的符号。  背景颜色是蓝色或红色的阴影，具体取决于实时扫描服务的状态。
	脱机客户端与防毒墙网络版服务器断开连接。服务器无法管理这些客户端。	图标包含一个类似中断波动信号的符号。  背景颜色是蓝色或红色的阴影，具体取决于实时扫描服务的状态。 客户端即使已连接到网络，也可能变成脱机状态。有关此问题的详细信息，请参阅 防毒墙网络版客户端图标中所指出问题的解决方案 第 14-36 页。
	漫游客户端也许能够与防毒墙网络版服务器通信，也许不能。	图标包含桌面和信号符号。  背景颜色是蓝色或红色的阴影，具体取决于实时扫描服务的状态。 有关漫游客户端的详细信息，请参阅防毒墙网络版客户端漫游权限 第 14-19 页。

客户端状态	描述	视觉提示
云安全智能防护源的可用性	云安全智能防护源包括云安全智能防护服务器和趋势科技云安全智能防护网络。 传统扫描客户端会连接到云安全智能防护源进行 Web 信誉查询。 云安全扫描客户端会连接到云安全智能防护源进行扫描和 Web 信誉查询。	如果云安全智能防护源可用，则图标会包含一个复选标记。 
		如果没有可用的云安全智能防护源并且客户端正在尝试与源建立连接，则图标会包含一个进度条。  有关此问题的详细信息，请参阅 防毒墙网络版客户端图标中所指出问题的解决方案 第 14-36 页。
		对于传统扫描客户端，如果在该客户端上禁用了 Web 信誉，则不会显示复选标记或进度条。

客户端状态	描述	视觉提示
实时扫描服务状态	防毒墙网络版不仅将实时扫描服务用于实时扫描，还用于手动扫描和预设扫描。 服务必须正常运行，否则客户端会变得易受安全风险的攻击。	如果实时扫描服务正常运行，整个图标为蓝色阴影。使用两种蓝色阴影来指示客户端的扫描方法。 • 对于传统扫描：  • 对于云安全扫描： 
		如果实时扫描服务已禁用或未正常运行，整个图标为红色阴影。 使用两种红色阴影来指示客户端的扫描方法。 • 对于传统扫描：  • 对于云安全扫描：  有关此问题的详细信息，请参阅 防毒墙网络版客户端图标中所指出问题的解决方案 第 14-36 页。
实时扫描状态	实时扫描通过在创建、修改或检索文件时进行扫描以查看是否存在安全风险，来提供前瞻性保护。	如果启用实时扫描，没有视觉提示。
		如果禁用实时扫描，整个图标将被一个红色圆圈围绕并内含一条红色对角线。  有关此问题的详细信息，请参阅 防毒墙网络版客户端图标中所指出问题的解决方案 第 14-36 页。

客户端状态	描述	视觉提示
特征码更新状态	客户端必须定期更新特征码，以保护客户端不受最新威胁的攻击。	如果特征码为最新或仅稍微过期，则不会有视觉提示。
		如果特征码严重过期，则图标会包含一个叹号。这表示特征码已有一段时间未更新。  有关如何更新客户端的详细信息，请参阅防毒墙网络版客户端更新 第 6-26 页。
防毒墙网络版服务器试用期使用授权状态	联机客户端已连接到使用过期的试用版使用授权的防毒墙网络版服务器。	此图标表示防毒墙网络版服务器试用版使用授权已过期。 

云安全扫描图标

当防毒墙网络版客户端使用云安全扫描时，会显示下列任一图标。

表 14-5. 云安全扫描图标

图标	与防毒墙网络版服务器连接	云安全智能防护源的可用性	实时扫描服务	实时扫描
	联机	可用	正常运行	已启用
	联机	可用	正常运行	已禁用
	联机	可用	已禁用或未正常运行	已禁用或未正常运行
	联机	不可用，正在重新连接到源	正常运行	已启用

图标	与防毒墙网络版服务器连接	云安全智能防护源的可用性	实时扫描服务	实时扫描
	联机	不可用，正在重新连接到源	正常运行	已禁用
	联机	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行
	脱机	可用	正常运行	已启用
	脱机	可用	正常运行	已禁用
	脱机	可用	已禁用或未正常运行	已禁用或未正常运行
	脱机	不可用，正在重新连接到源	正常运行	已启用
	脱机	不可用，正在重新连接到源	正常运行	已禁用
	脱机	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行
	漫游	可用	正常运行	已启用
	漫游	可用	正常运行	已禁用
	漫游	可用	已禁用或未正常运行	已禁用或未正常运行
	漫游	不可用，正在重新连接到源	正常运行	已启用
	漫游	不可用，正在重新连接到源	正常运行	已禁用
	漫游	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行

传统扫描图标

当防毒墙网络版客户端使用传统扫描时，会显示下列任一图标。

表 14-6. 传统扫描图标

图标	与防毒墙网络版服务器连接	由云安全智能防护源提供的 Web 信誉服务	实时扫描服务	实时扫描	病毒码
	联机	可用	正常运行	已启用	最新或稍微过期
	联机	不可用，正在重新连接到源	正常运行	已启用	最新或稍微过期
	联机	可用	正常运行	已启用	严重过期
	联机	不可用，正在重新连接到源	正常运行	已启用	严重过期
	联机	可用	正常运行	已禁用	最新或稍微过期
	联机	不可用，正在重新连接到源	正常运行	已禁用	最新或稍微过期
	联机	可用	正常运行	已禁用	严重过期
	联机	不可用，正在重新连接到源	正常运行	已禁用	严重过期
	联机	可用	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	联机	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	联机	可用	已禁用或未正常运行	已禁用或未正常运行	严重过期

图标	与防毒墙网络版服务器连接	由云安全智能防护源提供的 Web 信誉服务	实时扫描服务	实时扫描	病毒码
	联机	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行	严重过期
	脱机	可用	正常运行	已启用	最新或稍微过期
	脱机	不可用，正在重新连接到源	正常运行	已启用	最新或稍微过期
	脱机	可用	正常运行	已启用	严重过期
	脱机	不可用，正在重新连接到源	正常运行	已启用	严重过期
	脱机	可用	正常运行	已禁用	最新或稍微过期
	脱机	不可用，正在重新连接到源	正常运行	已禁用	最新或稍微过期
	脱机	可用	正常运行	已禁用	严重过期
	脱机	不可用，正在重新连接到源	正常运行	已禁用	严重过期
	脱机	可用	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	脱机	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	脱机	可用	已禁用或未正常运行	已禁用或未正常运行	严重过期
	脱机	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行	严重过期
	漫游	可用	正常运行	已启用	最新或稍微过期

图标	与防毒墙网络版服务器连接	由云安全智能防护源提供的 Web 信誉服务	实时扫描服务	实时扫描	病毒码
	漫游	不可用，正在重新连接到源	正常运行	已启用	最新或稍微过期
	漫游	可用	正常运行	已启用	严重过期
	漫游	不可用，正在重新连接到源	正常运行	已启用	严重过期
	漫游	可用	正正常运行	已禁用	最新或稍微过期
	漫游	不可用，正在重新连接到源	正常运行	已禁用	最新或稍微过期
	漫游	可用	正常运行	已禁用	严重过期
	漫游	不可用，正在重新连接到源	正常运行	已禁用	严重过期
	漫游	可用	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	漫游	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	漫游	可用	已禁用或未正常运行	已禁用或未正常运行	严重过期
	漫游	不可用，正在重新连接到源	已禁用或未正常运行	已禁用或未正常运行	严重过期
	联机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已启用	最新或稍微过期
	联机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已启用	严重过期

图标	与防毒墙网络版服务器连接	由云安全智能防护源提供的 Web 信誉服务	实时扫描服务	实时扫描	病毒码
	联机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已禁用	最新或稍微过期
	联机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已禁用	严重过期
	联机	不适用（客户端上已禁用 Web 信誉功能）	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	联机	不适用（客户端上已禁用 Web 信誉功能）	已禁用或未正常运行	已禁用或未正常运行	严重过期
	脱机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已启用	最新或稍微过期
	脱机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已启用	严重过期
	脱机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已禁用	最新或稍微过期
	脱机	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已禁用	严重过期
	脱机	不适用（客户端上已禁用 Web 信誉功能）	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	脱机	不适用（客户端上已禁用 Web 信誉功能）	已禁用或未正常运行	已禁用或未正常运行	严重过期

图标	与防毒墙网络版服务器连接	由云安全智能防护源提供的 Web 信誉服务	实时扫描服务	实时扫描	病毒码
	漫游	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已启用	最新或稍微过期
	漫游	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已启用	严重过期
	漫游	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已禁用	最新或稍微过期
	漫游	不适用（客户端上已禁用 Web 信誉功能）	正常运行	已禁用	严重过期
	漫游	不适用（客户端上已禁用 Web 信誉功能）	已禁用或未正常运行	已禁用或未正常运行	最新或稍微过期
	漫游	不适用（客户端上已禁用 Web 信誉功能）	已禁用或未正常运行	已禁用或未正常运行	严重过期

防毒墙网络版客户端图标中所指出问题的解决方案

如果防毒墙网络版客户端图标指出以下情况中的任意一种，则请执行必要的操作：

情况	描述
暂时尚未更新特征码文件	防毒墙网络版客户端用户需要更新组件。从 Web 控制台上，在**更新** > **客户端** > **自动更新**中配置组件更新设置，或者在**客户端** > **客户端管理** > **设置** > **权限和其他设置** > **权限选项卡** > **组件更新**中为用户授予更新权限。

情况	描述
实时扫描服务已禁用或未正常运行	如果实时扫描服务 (OfficeScan NT RealTime Scan) 已禁用或变为未正常运行，用户必须从 Microsoft 管理控制台手动启动该服务。
实时扫描已禁用	从 Web 控制台（**客户端** > **客户端管理** > **设置** > **扫描设置** > **实时扫描设置**）启用实时扫描。
实时扫描已禁用且防毒墙网络版客户端处于漫游模式	用户需要先禁用漫游模式。禁用漫游模式后，从 Web 控制台中启用实时扫描。
防毒墙网络版客户端已连接到网络但显示为脱机	从 Web 控制台（**客户端** > **连接验证**）验证连接，然后查看连接验证日志（**日志** > **客户端** > **连接验证日志**）。 如果验证后防毒墙网络版客户端仍处于脱机状态： 1. 如果服务器和防毒墙网络版客户端的连接状态均为脱机，请检查网络连接。 2. 如果防毒墙网络版客户端的连接状态为脱机但服务器的连接状态为联机，则服务器域名可能已更改，而防毒墙网络版客户端使用该域名连接到服务器（如果在服务器安装过程中选择了域名）。将防毒墙网络版服务器的域名注册到 DNS 或 WINS 服务器，或将该域名和 IP 信息添加到客户端终端的 <Windows 文件夹>\system32\drivers\etc 文件夹中的 "hosts" 文件中。 3. 如果防毒墙网络版客户端的连接状态为联机但服务器的连接状态为脱机，请检查防毒墙网络版防火墙设置。防火墙可能会阻止服务器到客户端的通信，但会允许客户端到服务器的通信。 4. 如果防毒墙网络版客户端的连接状态为联机但服务器的连接状态为脱机，则防毒墙网络版客户端的 IP 地址可能已更改，但其状态未反映在服务器上（例如，重新加载客户端时）。请尝试重新部署防毒墙网络版客户端。
云安全智能防护源不可用	如果客户端与云安全智能防护源之间的连接中断，请执行以下任务： 1. 在 Web 控制台上，转至**终端位置**窗口（**客户端** > **终端位置**），然后检查下列终端位置设置是否配置正确： • 参考服务器和端口号 • 网关 IP 地址

情况	描述
	2. 在 Web 控制台上，转至“云安全智能防护源”窗口（**管理** > **云安全智能防护** > **云安全智能防护源**），然后执行下列任务： a. 检查源的标准或自定义列表上的云安全智能防护服务器设置是否正确。 b. 测试是否可以建立与服务器的连接。 c. 配置源列表之后，单击**通知所有客户端**。 3. 检查云安全智能防护服务器和防毒墙网络版客户端上的下列配置文件是否同步： • sscfg.ini • ssnotify.ini 4. 打开注册表编辑器，然后检查客户端是否已连接到公司网络。 注册表项： `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • 如果 LocationProfile=1，则防毒墙网络版客户端已连接到网络，并且应当能够连接到云安全智能防护服务器。 • 如果 LocationProfile=2，则防毒墙网络版客户端未连接到网络，并且应该连接到云安全智能防护网络。在 Internet Explorer 中，检查防毒墙网络版客户端终端是否可以浏览 Internet 网页。 5. 检查用于连接到云安全智能防护网络和云安全智能防护服务器的内部和外部代理服务器设置。有关详细信息，请参阅防毒墙网络版客户端的内部代理服务器 第 14-44 页和防毒墙网络版客户端的外部代理服务器 第 14-46 页。 6. 对于运行 Windows XP、Vista、Server 2003 和 Server 2008 的传统扫描客户端，请验证防毒墙网络版 NT 代理服务 (TmProxy.exe) 是否正在运行。如果此服务已停止，客户端将无法连接到云安全智能防护源以验证 Web 信誉。 对于运行 Windows 7、Server 2012 及更高版本的传统扫描客户端，请验证 tmusa 驱动程序是否正在运行。如果此驱动程序已停止，客户端将无法连接到云安全智能防护源以验证 Web 信誉。

客户端-服务器连接验证

防毒墙网络版 Web 控制台的客户端树上显示客户端与防毒墙网络版服务器的连接状态。

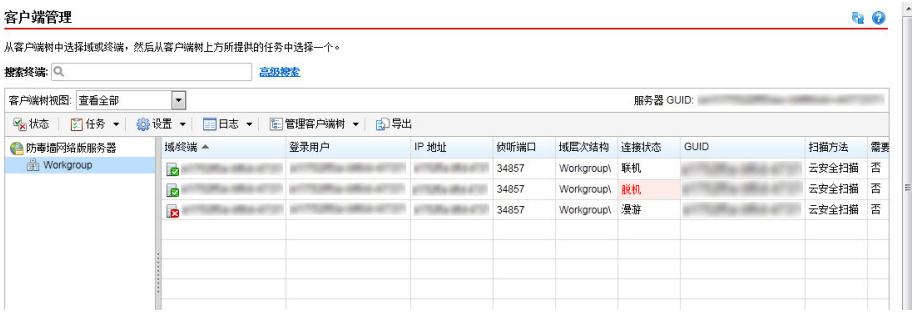


图 14-2. 显示客户端与防毒墙网络版服务器的连接状态的客户端树

特定情况可能会导致客户端树无法正确显示客户端连接状态。例如，如果意外拔下了客户端终端的网络电缆，则客户端将不能通知服务器其已脱机。此客户端在客户端树中将仍显示为联机。

手动验证客户端-服务器连接，或者允许防毒墙网络版执行预设验证。不能先选择特定域或客户端，然后再验证其连接状态。防毒墙网络版会验证所有已注册客户端的连接状态。

验证客户端-服务器连接

过程

1. 转至**客户端** > **连接验证**。
2. 要手动验证客户端-服务器连接，请转至**手动验证**选项卡，然后单击**立即验证**。
3. 要自动验证客户端-服务器连接，请转至**预设验证**选项卡。

a. 选择**启用预设验证**。

b. 选择验证频率以及开始时间。

c. 单击**保存**保存验证时间表。

4. 检查客户端树以验证其状态或查看连接验证日志。

连接验证日志

防毒墙网络版会保留连接验证日志，以使您可以确定防毒墙网络版服务器是否能够与其所有已注册客户端通信。每次从 Web 控制台验证客户端-服务器连接时，防毒墙网络版都会创建一个日志条目。

要防止日志大小占用太多的硬盘空间，请手动删除日志或者配置日志删除时间表。有关管理日志的详细信息，请参阅日志管理 第 13-35 页。

查看连接验证日志

过程

1. 转至**日志** > **客户端** > **连接验证日志**。
2. 通过检查**状态**列查看连接验证结果。
3. 要将日志保存到一个逗号分隔值 (CSV) 文件，请单击**导出为 CSV 格式**。打开文件或将其保存到特定位置。

无法访问客户端

无法访问的网络上的防毒墙网络版客户端（如位于 NAT 网关之后的网段上的防毒墙网络版客户端）几乎始终处于脱机状态，因为服务器无法与这些客户端建立直接连接。因此，服务器无法通知客户端执行以下操作：

- 下载最新的组件。
- 应用从 Web 控制台配置的客户端设置。例如，当从 Web 控制台更改预设扫描频率时，服务器会立即通知客户端应用新设置。

因此，无法访问的客户端无法及时执行这些任务。它们仅在启动与服务器的连接时才执行这些任务，启动连接在下列情况下发生：

- 客户端在安装后向服务器注册时。
- 客户端重新启动或重新加载时。该事件不经常发生且通常需要用户干预。
- 在客户端上触发手动或预设更新时。该事件也不经常发生。

只有在注册、重新启动或重新加载时，服务器才能“感知”客户端的连接并将它们视为联机。但是，由于服务器仍无法与客户端建立连接，因此服务器会立即将其状态更改为脱机。

防毒墙网络版提供“波动信号”和服务器轮询功能来解决无法访问的客户端的有关问题。有了这些功能之后，服务器不再通知客户端有关组件更新和设置更改的信息。相反，服务器处于被动的角色，始终等待客户端发送波动信号或启动轮询。当服务器检测到任何这些事件时，会将客户端视为联机。

注意

与波动信号和服务器轮询无关的客户端启动事件（如手动客户端更新和日志发送）不会触发服务器更新无法访问的客户端的状态。

波动信号

防毒墙网络版客户端会发送波动信号消息以通知服务器来自客户端的连接仍然有效。服务器收到波动信号消息之后，会将客户端视为联机。在客户端树中，客户端可以为以下任一状态：

- **联机**：针对常规联机客户端
- **无法访问/联机**：针对位于无法访问的网络中的联机客户端

注意

防毒墙网络版客户端不会在发送波动信号消息时更新组件或应用新设置。常规客户端会在定期更新期间执行这些任务（请参阅防毒墙网络版客户端更新 第 6-26 页）。位于无法访问的网络中的客户端会在服务器轮询期间执行这些任务。

波动信号功能解决了位于无法访问的网络中的防毒墙网络版客户端即使可以连接到服务器仍显示为脱机的问题。

Web 控制台中的一个设置控制客户端发送波动信号消息的频率。如果服务器未收到波动信号，它不会立即将客户端视为脱机。另外一个设置控制服务器多长时间未收到波动信号才将客户端的状态更改为：

- **脱机**：针对常规脱机防毒墙网络版客户端
- **无法访问/脱机**：针对位于无法访问的网络中的脱机防毒墙网络版客户端

选择波动信号设置时，请在显示最新客户端状态信息的需要和管理系统资源的需要之间保持平衡。缺省设置可以满足大多数情况。但是，当您定制波动信号设置时，请考虑以下几点：

表 14-7. 波动信号建议

波动信号频率	建议
长时间间隔波动信号（60 分钟以上）	波动信号的时间间隔越长，服务器在 Web 控制台上反映客户端状态之前可能发生事件的数量就越多。
短时间间隔波动信号（60 分钟以下）	短时间间隔会提供更新的客户端状态，但可能占用大量的带宽。

服务器轮询

服务器轮询功能解决了无法访问的防毒墙网络版客户端无法及时接收有关组件更新和客户端设置更改的通知的问题。该功能独立于波动信号功能。

通过服务器轮询功能：

- 防毒墙网络版客户端可以按固定时间间隔自动启动与防毒墙网络版服务器的连接。服务器检测到轮询发生时，它会将客户端视为“无法访问/联机”。

- 防毒墙网络版客户端可以连接到一个或多个更新源来下载所有更新的组件并应用新的客户端设置。如果防毒墙网络版服务器或更新代理是主要更新源，则客户端会同时获取组件和新设置。如果更新源不是防毒墙网络版服务器或更新代理，则客户端仅可以获取更新的组件，然后再连接到防毒墙网络版服务器或更新代理以获取新的设置。

配置波动信号和服务器轮询功能

过程

1. 转至**客户端** > **全局客户端设置**，
2. 转至**无法访问的网络**部分。
3. 配置服务器轮询设置。

   有关服务器轮询的详细信息，请参阅服务器轮询 第 14-42 页。

   a. 如果防毒墙网络版服务器同时具有 IPv4 和 IPv6 地址，可以键入 IPv4 地址范围及 IPv6 前缀和长度。

      如果服务器只有 IPv4 地址，请键入 IPv4 地址范围；如果服务器只有 IPv6 地址，请键入 IPv6 前缀和长度。

      当客户端的 IP 地址与范围中的某个 IP 地址匹配时，客户端会应用波动信号和服务器轮询设置，服务器会将该客户端视为处于无法访问的网络中。

      注意

      具有 IPv4 地址的客户端可连接到纯 IPv4 或双栈防毒墙网络版服务器。

      具有 IPv6 地址的客户端可连接到纯 IPv6 或双栈防毒墙网络版服务器。

      双栈客户端可连接到双栈、纯 IPv4 或纯 IPv6 防毒墙网络版服务器。

   b. 在**客户端每隔 __ 分钟轮询一次服务器以确定是否有更新的组件和设置**中，指定服务器轮询频率。请键入一个介于 1 到 129600 分钟之间的值。

提示

趋势科技建议服务器轮询频率应至少为波动信号发送频率的三倍。

4. 配置波动信号设置。

   有关波动信号功能的详细信息，请参阅波动信号 第 14-41 页。

   a. 选择**允许客户端向服务器发送波动信号**。

   b. 选择**所有客户端**或**仅无法访问的网络中的客户端**。

   c. 在**客户端每隔 __ 分钟发送波动信号**中，指定客户端发送波动信号的频率。请键入一个介于 1 到 129600 分钟之间的值。

   d. 在**如果超过 __ 分钟仍未收到客户端发送的波动信号，则将其视为脱机**中，指定防毒墙网络版服务器多长时间未收到波动信号后才将客户端视为脱机。请键入一个介于 1 到 129600 分钟之间的值。

5. 单击**保存**。

防毒墙网络版客户端代理服务器设置

连接到内部和外部服务器时，将防毒墙网络版客户端配置为使用代理服务器设置。

防毒墙网络版客户端的内部代理服务器

防毒墙网络版客户端可以使用内部代理服务器设置连接到网络中的下列服务器：

- 防毒墙网络版服务器

  服务器计算机托管防毒墙网络版服务器和集成型云安全智能防护服务器。防毒墙网络版客户端连接到防毒墙网络版服务器以更新组件、获取配置设置和发送日志。防毒墙网络版客户端连接到集成型云安全智能防护服务器以发送扫描查询。

- 云安全智能防护服务器

  云安全智能防护服务器包括所有独立型云安全智能防护服务器及其他防毒墙网络版服务器的集成型云安全智能防护服务器。防毒墙网络版客户端连接到服务器以发送扫描和 Web 信誉查询。

配置内部代理服务器设置

过程

1. 转至**管理** > **设置** > **代理服务器**。
2. 单击**内部代理服务器**选项卡。
3. 转到**客户端与防毒墙网络版服务器之间的连接**部分。
   a. 选择**当客户端连接到防毒墙网络版服务器时，使用以下代理服务器设置**。
   b. 指定代理服务器名称或 IPv4/IPv6 地址，以及端口号。

   注意

   如果有 IPv4 和 IPv6 客户端，请指定通过主机名标识的双栈代理服务器。这是因为内部代理服务器设置是全局设置。如果指定 IPv4 地址，IPv6 客户端将无法连接到代理服务器。同样的道理也适用于 IPv4 客户端。

   c. 如果代理服务器需要认证，请键入用户名和密码，然后确认密码。
4. 转到**客户端与独立型云安全智能防护服务器之间的连接**部分。
   a. 选择**当客户端连接到独立型云安全智能防护服务器时，使用以下代理服务器设置**。
   b. 指定代理服务器名称或 IPv4/IPv6 地址，以及端口号。
   c. 如果代理服务器需要认证，请键入用户名和密码，然后确认密码。
5. 单击**保存**。

防毒墙网络版客户端的外部代理服务器

防毒墙网络版服务器和防毒墙网络版客户端在连接到趋势科技托管的服务器时，可以使用外部代理服务器设置。本主题讨论客户端的外部代理服务器设置。有关服务器的外部代理服务器设置，请参阅用于防毒墙网络版服务器更新的代理服务器 第 6-19 页。

防毒墙网络版客户端可使用在 Internet Explorer 或 Chrome 中配置的代理服务器设置连接到趋势科技云安全智能防护网络。如果需要代理服务器认证，则客户端将使用代理服务器认证凭证（用户 ID 和密码）。

配置代理服务器认证凭证

过程

1. 转至**管理** > **设置** > **代理服务器**。
2. 单击**外部代理服务器**选项卡。
3. 转到**防毒墙网络版客户端与趋势科技服务器之间的连接**部分。
4. 键入代理服务器认证需要的用户标识和密码。下列代理服务器认证协议受支持：
   - 基本访问认证
   - 摘要访问认证
   - 集成 Windows 认证
5. 单击**保存**。

客户端的代理服务器配置权限

可以授予客户端用户配置代理服务器设置的权限。防毒墙网络版客户端仅在以下情况下才使用用户配置的代理服务器设置：

- 防毒墙网络版客户端执行“立即更新”时。
- 用户禁用自动代理服务器设置，或防毒墙网络版客户端无法检测到自动代理服务器设置时。

  请参阅防毒墙网络版客户端的自动代理服务器设置 第 14-48 页以获取详细信息。

警告!

如果用户配置的代理服务器设置错误，会导致发生更新问题。当允许用户配置自己的代理服务器设置时请多加谨慎。

授予代理服务器配置权限

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 ( ) 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，转至**代理服务器设置**部分。
5. 选择**允许用户配置代理服务器设置**。
6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：
   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

防毒墙网络版客户端的自动代理服务器设置

手动配置代理服务器设置对于许多终端用户而言是个复杂的任务。使用自动代理服务器设置可以确保在不需要任何用户干预的情况下应用正确的代理服务器设置。

如果启用，则防毒墙网络版客户端通过自动更新或“立即更新”更新组件时，自动代理服务器设置将用作主代理服务器设置。有关自动更新和立即更新的信息，请参阅防毒墙网络版客户端更新方法 第 6-35 页。

如果防毒墙网络版客户端无法使用自动代理服务器设置进行连接，则具有配置代理服务器设置权限的客户端用户可以使用用户配置的代理服务器设置。否则，使用自动代理服务器设置的连接将不成功。

注意

代理服务器认证不受支持。

配置自动代理服务器设置

过程

1. 转至**客户端** > **全局客户端设置**，
2. 转至**代理服务器配置**部分。
3. 如果您希望防毒墙网络版按 DHCP 或 DNS 自动检测管理员配置的代理服务器设置，则选择**自动检测设置**。
4. 如果希望防毒墙网络版使用网络管理员设置的代理服务器自动配置 (PAC) 脚本来检测相应的代理服务器，则执行以下操作：
   a. 选择**使用自动配置脚本**。
   b. 键入 PAC 脚本的地址。
5. 单击**保存**。

查看防毒墙网络版客户端信息

“查看状态”窗口显示有关防毒墙网络版客户端的重要信息，其中包括权限、客户端软件详细信息和系统事件。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**状态**。
4. 展开客户端终端的名称以查看状态信息。如果您选择了多个客户端，请单击**全部展开**查看所有选定客户端的状态信息。
5. （可选）使用**重置**按钮将安全风险计数重置为零。

导入和导出客户端设置

防毒墙网络版允许将特定防毒墙网络版客户端或域所应用的客户端树设置导出到文件。接着，便可以导入该文件以将设置应用到其他客户端和域，或应用到相同版本的其他防毒墙网络版服务器。

除更新代理设置之外，所有客户端树设置均可导出。

导出客户端设置

过程

1. 转至**客户端** > **客户端管理**。

2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **导出设置**。
4. 单击任一链接以查看选定防毒墙网络版客户端或域的设置。
5. 单击**导出**保存设置。

   设置保存为 .dat 文件。
6. 单击**保存**，然后指定要保存 .dat 文件的位置。
7. 单击**保存**。

导入客户端设置

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **导入设置**。
4. 单击**浏览**在终端上找到 .dat 文件，然后单击**导入**。

   将显示**导入设置**窗口，显示设置的摘要。
5. 单击任一链接以查看要导入的扫描设置或权限的详细信息。
6. 导入设置。
   - 如果单击的是根域图标，请选择**应用到所有域**，然后单击**应用到目标计算机**。
   - 如果选择了域，请选择**应用到属于选定的域的所有计算机**，然后单击**应用到目标计算机**。

- 如果选择了多个客户端，请单击**应用到目标计算机**。

安全合规

使用安全合规可以确定漏洞、部署解决方案和维护安全基础架构。此功能可帮助减少保护网络环境所需的时间，并有助于平衡组织在安全性和功能方面的要求。

执行下列两类终端的安全合规：

- **受管理**：防毒墙网络版客户端受防毒墙网络版服务器所管理的终端。有关详细信息，请参阅受管理客户端的安全合规 第 14-51 页。
- **不受管理**：包括以下内容：
  - 不受防毒墙网络版服务器管理的防毒墙网络版客户端
  - 未安装防毒墙网络版客户端的终端
  - 防毒墙网络版服务器无法与其连接的终端
  - 无法验证其安全状态的终端

    有关详细信息，请参阅不受管理的终端的安全合规 第 14-62 页。

受管理客户端的安全合规

安全合规会生成合规报告，以帮助评估受防毒墙网络版服务器管理的防毒墙网络版客户端的安全状态。安全合规按需或根据时间表生成报告。

手动评估窗口显示下列选项卡：

- **服务**：使用此选项卡检查客户端服务是否正常运行。有关详细信息，请参阅服务 第 14-52 页。
- **组件**：使用此选项卡检查防毒墙网络版客户端的组件是否已为最新。有关详细信息，请参阅组件 第 14-54 页。

- **手动/预设扫描**：使用此选项卡检查防毒墙网络版客户端是否定期运行扫描。有关详细信息，请参阅手动/预设扫描 第 14-55 页。
- **设置**：使用此选项卡检查客户端设置是否与服务器设置一致。有关详细信息，请参阅设置 第 14-57 页。



注意

组件选项卡可显示运行当前版本和早期版本产品的防毒墙网络版客户端。而其他选项卡只显示运行 10.5、10.6 的防毒墙网络版客户端或运行更高版本的防毒墙网络版客户端。

合规报告的注意事项

- 安全合规在生成合规报告之前先查询防毒墙网络版客户端的连接状态。它在报告中包含联机和脱机客户端，但不包含漫游客户端。
- 对于基于角色的用户帐户：
  - 每个 Web 控制台用户帐户都有一组完全独立的合规报告设置。对某个用户帐户的合规报告设置的任何更改都不会影响其他用户帐户的设置。
  - 报告的范围取决于用户帐户的客户端域权限。例如，如果授予某个用户帐户管理域 A 和 B 的权限，则该用户帐户的报告将仅显示来自属于域 A 和 B 的客户端的数据。

    有关用户帐户的详细信息，请参阅基于角色的管理 第 13-3 页。

服务

安全合规会检查下列防毒墙网络版客户端服务是否正常运行：

- 防病毒
- 防间谍软件
- 防火墙
- Web 信誉

- 行为监控/设备控制（亦称为“趋势科技未授权更改阻止服务”）
- 数据保护
- 可疑连接

状态异常的客户端在合规报告中至少会被计数两次。



图 14-3. “合规报告”－“服务”选项卡

- 在**服务状态异常的终端**类别中
- 在防毒墙网络版客户端异常状态对应的类别中。例如，如果防毒墙网络版客户端的“防病毒”服务未正常运行，则会将该客户端计入**防病毒**类别中。如果多个服务未正常运行，则会将该客户端分别计入每种异常状态对应的类别中。

从 Web 控制台或防毒墙网络版客户端重新启动未正常运行的服务。如果这些服务在重新启动后运行正常，则在下次评估期间，客户端将不再显示为状态异常。

组件

安全合规可确定防毒墙网络版服务器和防毒墙网络版客户端之间不一致的组件。客户端无法连接到服务器以更新组件时，通常会发生不一致。如果客户端是从其他来源（如趋势科技 ActiveUpdate 服务器）获取更新，该客户端的组件版本可能比服务器上的版本更新。

安全合规会检查下列组件：

- 云安全客户端病毒码
- 病毒码
- IntelliTrap 特征码
- IntelliTrap 例外特征码
- 病毒扫描引擎
- 间谍软件特征码
- 间谍软件主动监控特征码
- 间谍软件扫描引擎
- 病毒清除模板
- 病毒清除引擎
- 通用防火墙特征码
- 通用防火墙驱动程序
- 行为监控驱动程序
- 行为监控核心服务
- 行为监控配置特征码
- 数字签名特征码
- 策略强制特征码
- 行为监控检测特征码
- 全局 C&C IP 列表
- 关联规则特征码
- 预启动的清除驱动程序
- 内存扫描触发特征码
- 内存检查特征码
- 浏览器漏洞防护特征码
- 脚本分析器特征码
- 程序版本

状态异常的客户端在合规报告中至少会被计数两次。



图 14-4. “合规报告”－“组件”选项卡

- 在**组件需要更新的终端**类别中
- 在客户端异常状态对应的类别中。例如，如果客户端的云安全扫描客户端特征码版本与服务器上的版本不一致，则会将该客户端计入**云安全客户端病毒码**类别中。如果多个组件版本不一致，则会将该客户端分别计入每种异常状态对应的类别中。

要解决组件版本不一致问题，请更新客户端或服务器上的已过期组件。

手动/预设扫描

安全合规检查立即扫描或预设扫描是否定期运行，以及这些扫描是否在合理的时间长度内完成。

注意

如果客户端上已启用预设扫描，安全合规只能报告预设扫描状态。

安全合规使用下列手动/预设扫描条件：

- **距离上次执行立即扫描或预设扫描已有 (x) 天**：如果防毒墙网络版客户端在指定天数内未运行过“立即扫描”或“预设扫描”，则会被判定为状态异常。
- **立即扫描或预设扫描已超过 (x) 个小时**：如果防毒墙网络版客户端上次执行“立即扫描”或“预设扫描”的持续时间超过指定的小时数，则会被判定为状态异常。

状态异常的客户端在合规报告中至少会被计数两次。



图 14-5. “合规报告”－“手动/预设扫描”选项卡

- 在**带有过期扫描的终端**类别中
- 在客户端异常状态对应的类别中。例如，如果上次执行预设扫描的时间超出指定的时数，则会将该客户端计入**立即扫描或预设扫描已超过 <x> 个小时**类别中。如果该客户端符合多个手动/预设扫描条件，则会将它分别计入每种异常状态对应的类别中。

在尚未执行扫描任务或无法完成扫描的客户端上运行“立即扫描”或“预设扫描”。

设置

安全合规会确定客户端树中的客户端与其父域是否具有相同的设置。如果将任何客户端移动到应用一组不同设置的其他域，或者如果具有特定权限的客户端用户在防毒墙网络版客户端控制台上手动配置了这些设置，则设置可能不一致。

防毒墙网络版将验证下列设置：

- 扫描方法
- 手动扫描设置
- 实时扫描设置
- 预设扫描设置
- 立即扫描设置
- 权限和其他设置
- 其他服务设置
- Web 信誉
- 行为监控
- 设备控制
- 间谍软件/灰色软件允许列表
- 数据丢失防护设置
- 可疑连接
- 可信程序列表

状态异常的客户端在合规报告中至少会被计数两次。



图 14-6. “合规报告”－“设置”选项卡

- 在**配置策略违规的终端**类别中
- 在客户端异常状态对应的类别中。例如，如果客户端中的扫描方法设置与其父域不一致，则会将该客户端计入**扫描方法**类别中。如果多组设置不一致，则会将该客户端分别计入每种异常状态对应的类别中。

要解决设置不一致问题，请将域设置应用到客户端。

按需合规报告

安全合规可以按需生成合规报告。报告有助于您评估受防毒墙网络版服务器管理的防毒墙网络版客户端的安全状态。

有关合规报告的详细信息，请参阅受管理客户端的安全合规 第 14-51 页。

生成按需合规报告

过程

1. 转至**评估** > **安全合规** > **手动报告**。
2. 转到**客户端树作用域**部分。
3. 选择根域或某个域，然后单击**评估**。
4. 查看客户端服务的合规报告。

   有关客户端服务的详细信息，请参阅服务 第 14-52 页。

   a. 单击**服务**选项卡。

   b. 在**服务状态异常的终端**下，检查服务状态异常的客户端的数量。

   c. 单击数字链接以显示客户端树中所有受影响的客户端。

   d. 从查询结果中选择客户端。

   e. 单击**重新启动防毒墙网络版客户端**以重新启动该服务。

   注意

   再次执行评估后，如果客户端仍显示为异常，请在客户端终端上手动重新启动该服务。

   f. 要将客户端列表保存到文件，请单击**导出**。

5. 查看客户端组件的合规报告。

   有关客户端组件的详细信息，请参阅组件 第 14-54 页。

   a. 单击**组件**选项卡。

   b. 在**组件需要更新的终端**下，检查其组件版本与服务器上的版本不一致的客户端的数量。

   c. 单击数字链接以显示客户端树中所有受影响的客户端。

注意

如果至少一个客户端拥有比防毒墙网络版服务器更新的组件，请手动更新防毒墙网络版服务器。

d. 从查询结果中选择客户端。

e. 单击**立即更新**强制客户端下载组件。

注意

- 为确保客户端可升级客户端程序，请禁用**客户端 > 客户端管理 > 设置 > 权限和其他设置**中的**防毒墙网络版客户端可以更新组件，但不能升级客户端程序，也不能部署 hotfix** 选项。
- 请重新启动终端（而不是单击**立即更新**）来更新通用防火墙驱动程序。

f. 要将客户端列表保存到文件，请单击**导出**。

6. 查看扫描的合规报告。

有关扫描的详细信息，请参阅手动/预设扫描 第 14-55 页。

a. 单击**手动/预设扫描**选项卡。

b. 在**带有过期扫描的终端**下，配置下列选项：

- 客户端未执行“立即扫描”或“预设扫描”的天数
- 立即扫描或预设扫描的运行小时数

注意

如果超出此天数或小时数，则客户端将被视为状态异常。

c. 单击**客户端树作用域**旁边的**评估**。

d. 在**带有过期扫描的终端**下，检查符合扫描条件的客户端的数量。

e. 单击数字链接以显示客户端树中所有受影响的客户端。

f. 从查询结果中选择客户端。

g. 单击**立即扫描**以在客户端上启动“立即扫描”。



注意

为避免重复扫描，如果立即扫描的持续时间超过指定小时数，将禁用**立即扫描**选项。

h. 要将客户端列表保存到文件，请单击**导出**。

7. 查看设置的合规报告。

有关设置的详细信息，请参阅设置 第 14-57 页。

a. 单击**设置**选项卡。

b. 在**配置策略违规的客户端**下，检查其设置与客户端树域设置不一致的客户端的数量。

c. 单击数字链接以显示客户端树中所有受影响的客户端。

d. 从查询结果中选择客户端。

e. 单击**应用域设置**。

f. 要将客户端列表保存到文件，请单击**导出**。

预设合规报告

安全合规可以根据时间表生成合规报告。报告有助于您评估受防毒墙网络版服务器管理的防毒墙网络版客户端的安全状态。

有关合规报告的详细信息，请参阅受管理客户端的安全合规 第 14-51 页。

配置预设合规报告的设置

过程

1. 转至**评估** > **安全合规** > **预设报告**。

2. 选择**启用预设报告**。
3. 指定报告的标题。
4. 选择以下一个或所有项：
   - 服务 第 14-52 页
   - 组件 第 14-54 页
   - 手动/预设扫描 第 14-55 页
   - 设置 第 14-57 页
5. 指定将接收预设合规报告相关通知的电子邮件地址。

注意

配置电子邮件通知设置以确保可成功发送电子邮件通知。有关详细信息，请参阅管理员通知设置 第 13-32 页。

6. 指定时间表。
7. 单击**保存**。

不受管理的终端的安全合规

安全合规可查询防毒墙网络版服务器所属的网络中不受管理的终端。使用 Active Directory 和 IP 地址来查询终端。

不受管理的终端的安全状态可以是下列任一种：

表 14-8. 不受管理的终端的安全状态

状态	描述
由另一个防毒墙网络版服务器管理	计算机上安装的防毒墙网络版客户端受另一个防毒墙网络版服务器管理。防毒墙网络版客户端为联机状态，并且运行此防毒墙网络版版本或早期版本。

状态	描述
未安装防毒墙网络版客户端	防毒墙网络版客户端未安装在终端上。
无法访问	防毒墙网络版服务器无法连接到终端并确定其安全状态。
未解析的 Active Directory 评估	该终端属于 Active Directory 域，但防毒墙网络版服务器无法确定其安全状态。 **注意** 防毒墙网络版服务器数据库包含服务器管理的客户端的列表。服务器查询 Active Directory 中的计算机 GUID，然后与数据库中存储的 GUID 比较。如果 GUID 不在数据库中，则终端将属于“未解析的 Active Directory 评估”类别。

要运行安全性评估，请执行以下任务：

1. 定义查询作用域。有关详细信息，请参阅定义 Active Directory/IP 地址作用域和查询 第 14-63 页。
2. 检查查询结果中不受保护的计算机。有关详细信息，请参阅查看查询结果 第 14-66 页。
3. 安装防毒墙网络版客户端。有关详细信息，请参阅使用安全合规安装 第 5-54 页。
4. 配置预设查询。有关详细信息，请参阅配置预设查询评估 第 14-67 页。

定义 Active Directory/IP 地址作用域和查询

首次查询时，需要定义 Active Directory/IP 地址作用域，包括防毒墙网络版服务器将按需或定期查询的 Active Directory 对象和 IP 地址。在定义作用域之后，启动查询进程。

注意

要定义 Active Directory 作用域，防毒墙网络版必须首先与 Active Directory 集成。有关集成的详细信息，请参阅Active Directory 集成 第 2-34 页。

过程

1. 转至**评估** > **不受管理的终端**。
2. 在 **Active Directory/IP 地址作用域**部分中，单击**定义**。此时打开一个新窗口。
3. 定义 Active Directory 作用域：
   a. 转到 **Active Directory 作用域**部分。
   b. 选择**使用按需评估**以执行实时查询并获得更准确的结果。禁用此选项将导致防毒墙网络版查询数据库，而非查询每个防毒墙网络版客户端。只查询数据库的速度比较快，但查询结果不太准确。
   c. 选择要查询的对象。首次进行查询时，选择少于 1,000 个帐户的对象，然后记录需要使用多少时间才能完成这次查询。将此数据用作性能基准。
4. 定义 IP 地址作用域：
   a. 转至 **IP 地址作用域**部分。
   b. 选择**启用 IP 地址作用域**。
   c. 指定 IP 地址范围。单击“加”或“减”按钮添加或删除 IP 地址范围。
   - 对于纯 IPv4 防毒墙网络版服务器，请键入 IPv4 地址范围。
   - 对于纯 IPv6 防毒墙网络版服务器，请键入 IPv6 前缀和长度。
   - 对于双栈防毒墙网络版服务器，请键入 IPv4 地址范围和/或 IPv6 前缀和长度。

     IPv6 地址范围限制为 16 位，这与 IPv4 地址范围的限制类似。因此，前缀长度应该介于 112 到 128 之间。

表 14-9. IPv6 地址的前缀长度和数量

长度	IPv6 地址的数量
128	2

长度	IPv6 地址的数量
124	16
120	256
116	4,096
112	65,536

5. 在“高级设置”下，指定防毒墙网络版服务器与客户端通信时使用的端口。在防毒墙网络版服务器安装期间，安装程序随机生成端口号。

   要查看防毒墙网络版服务器使用的通信端口，请转至**客户端 > 客户端管理**并选择域。端口将显示在“IP 地址”列旁边。趋势科技建议保留端口号记录作为参考。

   a. 单击**指定端口**。

   b. 键入端口号并单击**添加**。重复此步骤，直到获得要添加的所有端口号。

   c. 单击**保存**。

6. 要使用特定端口号检查终端的连接，请选择**检查端口 <x> 后声明某终端无法访问**。未建立连接时，防毒墙网络版会立即将终端视为无法访问。缺省端口号为 135。

   启用此设置可加速查询。无法建立与终端的连接时，在将终端视为无法访问之前，防毒墙网络版服务器不再需要执行所有其他连接验证任务。

7. 要保存作用域并启动查询，请单击**保存并重新评估**。要仅保存设置，请单击**仅保存**。“外部服务器管理”窗口将显示查询结果。



注意

查询可能需要很长时间才能完成，尤其是当查询作用域较大时。在“外部服务器管理”窗口显示结果之前，不要执行其他查询。否则，当前查询会话将终止，并且查询进程重新启动。

查看查询结果

查询结果会显示在**安全状态**部分下。不受管理的终端将具有下列一种状态：

- 由另一个防毒墙网络版服务器管理
- 未安装防毒墙网络版客户端
- 无法访问
- 未解析的 Active Directory 评估

过程

1. 在**安全状态**部分中，单击数字链接可显示所有受影响的计算机。
2. 使用搜索和高级搜索功能仅搜索和显示满足搜索条件的计算机。

   如果使用高级搜索功能，则指定下列项：

   - IPv4 地址范围
   - IPv6 前缀和长度（前缀应该介于 112 到 128 之间）
   - 终端名称
   - 防毒墙网络版服务器
   - Active Directory 树
   - 安全状态

   如果名称不完整，则防毒墙网络版将不会返回结果。如果不知道确切的完整名称，请使用通配符 (*)。
3. 要将计算机列表保存到文件，请单击**导出**。
4. 对于由其他防毒墙网络版服务器管理的防毒墙网络版客户端，使用客户端迁移程序工具让当前的防毒墙网络版服务器来管理这些防毒墙网络版客户端。有关此工具的详细信息，请参阅客户端迁移程序 第 14-22 页。

配置预设查询评估

配置防毒墙网络版服务器以定期查询 Active Directory 和 IP 地址，从而确保实施安全准则。

过程

1. 转至**评估** > **不受管理的终端**。
2. 单击客户端树顶部的**设置**。
3. 启用预设查询。
4. 指定时间表。
5. 单击**保存**。

趋势科技虚拟桌面支持

通过使用趋势科技虚拟桌面支持优化虚拟桌面保护。这种功能可控制驻留在单个虚拟服务器上的防毒墙网络版客户端中的任务。

在单个服务器上运行多个桌面和执行按需扫描或组件更新将消耗大量的系统资源。使用此功能可以禁止客户端同时运行扫描和更新组件。

例如，如果 VMware vCenter Server 包含三个运行防毒墙网络版客户端的虚拟桌面，则防毒墙网络版可以启动立即扫描和同时对所有这三个客户端部署更新。虚拟桌面支持将客户端识别为位于同一物理服务器上。虚拟桌面支持允许任务在第一个客户端上运行，并将其他两个客户端上的相同任务推迟到第一个客户端完成该任务时。

可以在下列平台上使用虚拟桌面支持：

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

对于使用其他虚拟化应用程序的管理员，防毒墙网络版服务器也可以充当模仿的虚拟机监控程序以管理虚拟客户端。

有关这些平台的更多详细信息，请参考 VMware View、Citrix XenDesktop 或 Microsoft Hyper-V Web 站点。

使用防毒墙网络版 VDI 预扫描模板生成工具优化按需扫描，或者从基本镜像或黄金镜像中移除 GUID。

虚拟桌面支持安装

虚拟桌面支持是一种本机防毒墙网络版功能，但该功能必须单独授权。安装防毒墙网络版服务器之后，此功能即可用，但未正常运行。安装此功能会从 ActiveUpdate 服务器或自定义更新源（如果已设置）下载文件。将该文件并入防毒墙网络版服务器之后，您就可以激活虚拟桌面支持以启用其完整功能。从插件管理器执行安装和激活操作。

注意

纯 IPv6 环境不完全支持虚拟桌面支持。有关详细信息，请参阅纯 IPv6 服务器限制 第 A-3 页。

安装虚拟桌面支持

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口上，转到**趋势科技虚拟桌面支持**部分，然后单击**下载**。

   软件包的大小显示在**下载**按钮旁边。

   插件管理器会将下载的软件包存储到 <服务器安装文件夹>\PCCSRV\Download\Product。

注意

如果插件管理器无法下载文件，它会在 24 小时后自动重新下载。要手动触发插件管理器下载该软件包，请从 Microsoft 管理控制台重新启动防毒墙网络版插件管理器服务。

3. 监控下载进度。在下载过程中可以离开该窗口。

   如果在下载软件包时遇到问题，请检查防毒墙网络版产品控制台上的服务器更新日志。在主菜单上，单击**日志** > **服务器更新**。

   插件管理器下载该文件之后，虚拟桌面支持会显示在新窗口中。

注意

如果未显示“虚拟桌面支持”，请参阅插件管理器故障排除 第 15-11 页中的原因和解决方案。

4. 要立即安装虚拟桌面支持，请单击 **立即安装**。要稍后安装：

   a. 单击**稍后安装**。

   b. 打开**插件管理器**窗口。

   c. 转至**趋势科技虚拟桌面支持**部分，然后单击**安装**。

5. 阅读许可协议，然后单击**同意**以接受其中的条款。

   安装即开始。

6. 监控安装进度。安装完成后，会显示虚拟桌面支持的版本。

虚拟桌面支持使用授权

您可以从插件管理器查看、激活和续订虚拟桌面支持使用授权。

请从趋势科技获取激活码，然后用它来启用虚拟桌面支持的完整功能。

激活或续订虚拟桌面支持

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口上，转到**趋势科技虚拟桌面支持**部分，然后单击**管理程序**。
3. 单击**查看使用授权信息**。
4. 在打开的**产品使用授权详细信息**窗口中，单击**新激活码**。
5. 在打开的窗口上，键入激活码并单击**保存**。
6. 返回到“产品使用授权详细信息”窗口，单击**更新信息**以使用新使用授权的详细信息和功能状态来刷新该窗口。此窗口还提供一个到趋势科技 Web 站点的链接，您可以利用该链接来查看关于您的使用授权的详细信息。

查看虚拟桌面支持的使用授权信息

过程

1. Open the 防毒墙网络版 web console and click **插件** > **[趋势科技虚拟桌面支持] 管理程序** in the main menu.
2. 单击**查看使用授权信息**。
3. 在打开的窗口中查看使用授权详细信息。

   “虚拟桌面支持使用授权详细信息”部分提供了以下信息：

   - **状态**：显示“已激活”、“尚未激活”或“已过期”。
   - **版本**：显示“完全版”或“试用版”。如果同时具有完全版和试用版，则显示的版本为“完全版”。
   - **过期时间**：如果“虚拟桌面支持”有多个使用授权，则将显示最晚到期日期。例如，如果使用授权到期日期为 12/31/2010 和 06/30/2010，则将显示 12/31/2010。

- **座席数**：显示可使用虚拟桌面支持的防毒墙网络版客户端的数量
- **激活码**：显示激活码

以下实例中将显示关于使用授权的提醒信息：

如果您具有完全版使用授权：

- 在功能的宽限期内。宽限期的持续时间因地区而异。请通过趋势科技代表验证宽限期。
- 当使用授权到期且宽限期已过时。在此期间，您将不能获得技术支持。

如果您具有试用版使用授权

- 当使用授权过期时。在此期间，您将不能获得技术支持。

4. 单击**联机查看使用授权详细信息**，在趋势科技 Web 站点上查看您的使用授权的相关信息。
5. 要更新窗口以显示最新的使用授权信息，请单击**更新信息**。

虚拟服务器连接

过添加 VMware vCenter 4 (VMware View 4)、Citrix XenServer 5.5 (Citrix XenDesktop 4) 或 Microsoft Hyper-V Server 优化按需扫描或组件更新。防毒墙网络版 服务器与指定的虚拟服务器进行通信来确定位于同一物理服务器上的防毒墙网络版客户端。

对于其他 VDI 服务器，防毒墙网络版服务器会提供模仿的虚拟机监控程序以管理其他平台上的虚拟客户端。防毒墙网络版虚拟机监控程序会按照服务器收到请求的顺序处理虚拟客户端的请求。防毒墙网络版服务器一次处理一个请求，并将其他请求放入队列中。

添加服务器连接

过程

1. Open the 防毒墙网络版 web console and click **插件** > **[趋势科技虚拟桌面支持] 管理程序** in the main menu.
2. 选择 **VMware vCenter Server**、**Citrix XenServer**、**Microsoft Hyper-V** 或**其他虚拟化应用程序**。

   注意

   选择**其他虚拟化应用程序**时，不需要提供更多信息。防毒墙网络版服务器会按照服务器收到请求的顺序对虚拟客户端的请求作出响应。
3. 启用与服务器的连接。
4. 指定以下信息：
   - 对于 VMware vCenter 和 Citrix XenServer 服务器：
     - IP 地址
     - 端口
     - 连接协议（HTTP 或 HTTPS）
     - 用户名
     - 密码
   - 对于 Microsoft Hyper-V 服务器：
     - 主机名或 IP 地址
     - 域\用户名

     注意

     登录帐户必须为 Administrators 组中的域帐户

- 密码

5. （可选）启用 VMware vCenter 或 Citrix XenServer 的代理服务器连接。
   a. 指定代理服务器名称或 IP 地址和端口。
   b. 如果代理服务器要求认证，则指定用户名和密码。
6. 单击**测试连接**验证防毒墙网络版服务器可以成功连接到服务器。

注意

有关 Microsoft Hyper-V 连接故障排除的详细信息，请参阅 Microsoft Hyper-V 连接故障排除 第 14-75 页。

7. 单击**保存**。

添加其他服务器连接

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件** > **[趋势科技虚拟桌面支持] 管理程序**。
2. 单击**添加新的 vCenter 连接**、**添加新的 XenServer 连接**或**添加新的 Hyper-V 连接**。
3. 重复上述步骤以提供正确的服务器信息。
4. 单击**保存**。

删除连接设置

过程

1. 打开防毒墙网络版 Web 控制台，然后转到主菜单中的**插件** > **[趋势科技虚拟桌面支持] 管理程序**。

2. 单击**删除此连接**。
3. 单击**确定**确认要删除此设置。
4. 单击**保存**。

更改 VDI 扫描容量

管理员可通过修改 vdi.ini 文件来增加运行并发扫描的 VDI 终端的数量。趋势科技建议严格监控更改 VDI 容量的影响，以确保系统资源可以处理增加的任何扫描。

过程

1. 在防毒墙网络版服务器计算机上，转至 <服务器安装文件夹>PCCSRV\Private\vdi.ini。
2. 查找 `[TaskController]` 设置。

   缺省的 TaskController 设置如下：

   - 对于防毒墙网络版 10.5 客户端：

     ```
     [TaskController]

     Controller_00_MaxConcurrentGuests=1

     Controller_01_MaxConcurrentGuests=3
     ```

     其中：

     - `Controller_00_MaxConcurrentGuests=1` 等于可并发执行扫描的最大客户端数。
     - `Controller_01_MaxConcurrentGuests=3` 等于可并发执行更新的最大客户端数。

   - 对于防毒墙网络版 10.6 客户端和防毒墙网络版 11.0 客户端：

     ```
     [TaskController]
     ```

```
Controller_02_MaxConcurrentGuests=1

Controller_03_MaxConcurrentGuests=3
```

其中：

- `Controller_02_MaxConcurrentGuests=1` 等于可并发执行扫描的最大客户端数。
- `Controller_03_MaxConcurrentGuests=3` 等于可并发执行更新的最大客户端数。

3. 根据需要增加或减少每个控制器的计数。

   所有设置的最小值均为 1。

   所有设置的最大值均为 65536。

4. 保存并关闭 vdi.ini 文件。
5. 重新启动防毒墙网络版主服务。
6. 监控 VDI 终端的 CPU、内存和磁盘使用资源。通过重复步骤 1 到步骤 5 修改控制器设置，进一步增加/减少并发扫描数以最适合 VDI 环境。

Microsoft Hyper-V 连接故障排除

Microsoft Hyper-V 连接使用 Windows Management Instrumentation (WMI) 和 DCOM 进行客户端-服务器通信。防火墙策略可能会阻止此通信，导致无法成功连接到 Hyper-V 服务器。

Hyper-V 服务器的侦听端口缺省为端口 135，然后会选择随机配置的端口进行进一步通信。如果防火墙阻止 WMI 网络通信或者这两个端口中的任意一个，将无法与服务器成功通信。管理员可以修改防火墙策略，以允许与 Hyper-V 服务器成功通信。

在执行下列防火墙修改之前，请验证所有连接设置（包括 IP 地址、域\用户名和密码）是否正确。

允许 WMI 通信通过 Windows 防火墙

过程

1. 在 Hyper-V 服务器上，打开 **Windows 防火墙允许的程序**窗口。

   在 Windows 2008 R2 系统上，转至**控制面板** > **系统和安全性** > **Windows 防火墙** > **允许程序或功能通过 Windows 防火墙**。

2. 选择 **Windows Management Instrumentation (WMI)**。

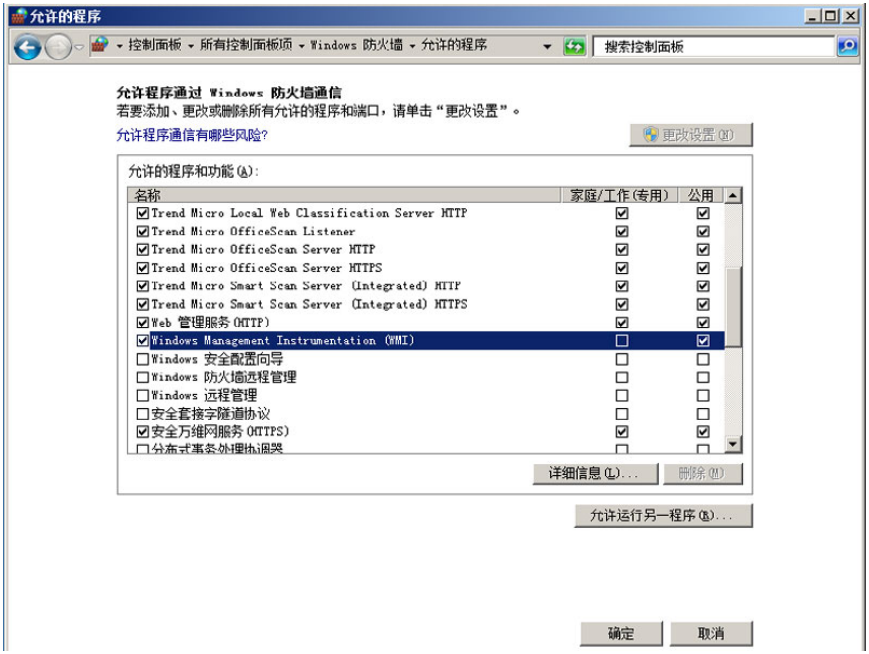


图 14-7. “Windows 防火墙允许的程序”窗口

3. 单击**保存**。

4. 再次测试 Hyper-V 连接。

允许端口通信通过 Windows 防火墙或第三方防火墙

过程

1. 在 Hyper-V 服务器上，确保防火墙允许通过端口 135 进行通信，然后再次测试 Hyper-V 连接。

   有关打开端口的详细信息，请参阅防火墙文档。

2. 如果无法成功连接到 Hyper-V 服务器，请将 WMI 配置为使用固定端口。

   有关*为 WMI 设置固定端口*的详细信息，请参阅：

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. 打开端口 135 和新创建的固定端口 (24158)，以便通信可以通过防火墙。

4. 再次测试 Hyper-V 连接。

VDI 预扫描模板生成工具

使用防毒墙网络版 VDI 预扫描模板生成工具优化按需扫描，或者从基本镜像或黄金镜像中移除 GUID。此工具扫描基本镜像或黄金镜像并证实镜像。扫描此镜像的副本时，防毒墙网络版仅检查已更改的部分。这可以确保缩短扫描时间。

提示

趋势科技建议在应用 Windows 更新或安装新的应用程序后生成预扫描模板。

创建预扫描模板

过程

1. 在防毒墙网络版服务器计算机上，浏览到 <服务器安装文件夹>\PCCSRV\Admin\Utility\TCacheGen。
2. 选择某个版本的 VDI 预扫描模板生成工具。以下版本可用：

表 14-10. VDI 预扫描模板生成工具版本

文件名	指导信息
TCacheGen.exe	如果要在 32 位平台上直接运行该工具，请选择此文件。
TCacheGen_x64.exe	如果要在 64 位平台上直接运行该工具，请选择此文件。
TCacheGenCli.exe	如果要从 32 位平台的命令行界面运行该工具，请选择此文件。
TCacheGenCli_x64.exe	如果要从 64 位平台的命令行界面运行该工具，请选择此文件。

3. 将在上一步中选择的工具版本复制到终端。
4. 运行该工具。
   - 直接运行该工具：
     a. 双击 TCacheGen.exe 或 TCacheGen_x64.exe。
     b. 选择**生成预扫描模板**，然后单击**下一步**。
   - 从命令行界面运行该工具：
     a. 打开命令提示符并将目录更改为 <客户端安装文件夹>。
     b. 键入以下命令：

```
TCacheGenCli Generate_Template
```

或者

```
TcacheGenCli_x64 Generate_Template
```

注意

此工具会在生成预扫描模板并移除 GUID 前扫描镜像是否存在安全威胁。

在生成预扫描模板后，该工具将退出防毒墙网络版客户端。不要重新加载防毒墙网络版客户端。如果防毒墙网络版客户端重新加载，您将需要再次创建预扫描模板。

从模板中移除 GUID

过程

1. 在防毒墙网络版服务器计算机上，浏览到 <服务器安装文件夹>\PCCSRV\Admin\Utility\TCacheGen。
2. 选择某个版本的 VDI 预扫描模板生成工具。以下版本可用：

表 14-11. VDI 预扫描模板生成工具版本

文件名	指导信息
TCacheGen.exe	如果要在 32 位平台上直接运行该工具，请选择此文件。
TCacheGen_x64.exe	如果要在 64 位平台上直接运行该工具，请选择此文件。
TCacheGenCli.exe	如果要从 32 位平台的命令行界面运行该工具，请选择此文件。
TCacheGenCli_x64.exe	如果要从 64 位平台的命令行界面运行该工具，请选择此文件。

3. 将在上一步中选择的工具版本复制到终端。
4. 运行该工具。
   - 直接运行该工具：
     a. 双击 TCacheGen.exe 或 TCacheGen_x64.exe。
     b. 选择**从模板中移除 GUID**，然后单击**下一步**。

- 从命令行界面运行该工具：

  a. 打开命令提示符并将目录更改为 <客户端安装文件夹>。

  b. 键入以下命令：

  ```
  TCacheGenCli Remove GUID
  ```

  或者

  ```
  TcacheGenCli_x64 Remove GUID
  ```

全局客户端设置

防毒墙网络版可将全局客户端设置应用于所有客户端，或者只应用于具有特定权限的客户端。

过程

1. 转至**客户端** > **全局客户端设置**。
2. 配置下列设置：

表 14-12. 全局客户端设置

设置	参考
扫描设置	全局扫描设置 第 7-62 页
预设扫描设置	全局扫描设置 第 7-62 页
病毒/恶意软件日志带宽设置	全局扫描设置 第 7-62 页
防火墙设置	全局防火墙设置 第 12-23 页
行为监控设置	行为监控 第 8-2 页
安全软件认证服务设置	为行为监控、防火墙和防病毒扫描启用安全软件认证服务 第 7-71 页

设置	参考
可疑连接设置	配置用户定义的全局 IP 列表设置 第 11-13 页
更新	作为防毒墙网络版客户端更新源的 ActiveUpdate 服务器 第 6-34 页
保留的磁盘空间	配置为防毒墙网络版客户端更新保留的磁盘空间 第 6-44 页
无法访问的网络	无法访问客户端 第 14-40 页
警报设置	配置防毒墙网络版客户端更新通知 第 6-45 页
客户端语言配置	防毒墙网络版客户端语言配置 第 14-21 页
服务器-客户端通信	增强服务器-客户端通信加密 第 13-52 页
重新启动防毒墙网络版服务	重新启动防毒墙网络版客户端服务 第 14-11 页
代理服务器配置	防毒墙网络版客户端的自动代理服务器设置 第 14-48 页
首选 IP 地址	客户端 IP 地址 第 5-8 页

3. 单击**保存**。

配置客户端权限和其他设置

授予用户在防毒墙网络版客户端上修改特定设置和执行高级别任务的权限。

注意

只有在激活防毒墙网络版防病毒功能后，才会显示防病毒设置。

提示

要在整个组织内执行统一的设置和策略，请授予用户有限的权限。

过程

1. 转至**客户端** > **客户端管理**。
2. 在客户端树中，单击根域图标 () 以包含所有客户端，或者选择特定域或客户端。
3. 单击**设置** > **权限和其他设置**。
4. 在**权限**选项卡上，配置以下用户权限：

表 14-13. 客户端权限

客户端权限	参考
漫游权限	防毒墙网络版客户端漫游权限 第 14-19 页
扫描权限	扫描类型权限 第 7-48 页
预设扫描权限	预设扫描权限和其他设置 第 7-50 页
防火墙权限	防火墙权限 第 12-21 页
行为监控权限	行为监控权限 第 8-10 页
可信程序列表	可信程序列表权限 第 7-61 页
邮件扫描权限	邮件扫描权限和其他设置 第 7-56 页
代理服务器设置权限	客户端的代理服务器配置权限 第 14-46 页
组件更新权限	配置更新权限和其他设置 第 6-42 页
退出和解锁	授予客户端退出和解锁权限 第 14-18 页
卸载	授予防毒墙网络版客户端卸载权限 第 5-65 页

5. 单击**其他设置**选项卡，然后配置下列设置：

表 14-14. 其他客户端设置

设置	参考
更新设置	配置更新权限和其他设置 第 6-42 页

设置	参考
Web 信誉设置	客户端用户的 Web 威胁通知 第 11-15 页
行为监控设置	行为监控权限 第 8-10 页
C&C 联系人警报设置	针对客户端用户的 C&C 联系人警报通知 第 11-19 页
集中隔离恢复警报设置	恢复隔离文件后在终端上显示通知消息
防毒墙网络版客户端自我保护	防毒墙网络版客户端自我保护 第 14-12 页
预设扫描设置	授予预设扫描权限和显示权限通知 第 7-51 页
扫描的缓存设置	扫描的缓存设置 第 7-58 页
POP3 电子邮件扫描设置	授予邮件扫描权限和启用 POP3 邮件扫描 第 7-57 页
防毒墙网络版客户端访问限制	防毒墙网络版客户端控制台访问限制 第 14-17 页
防毒墙网络版客户端安全	防毒墙网络版客户端安全 第 14-16 页
重新启动通知	针对防毒墙网络版客户端用户的安全风险通知 第 7-78 页

6. 如果在客户端树中选择了域或客户端，请单击**保存**。如果单击根域图标，请从下列选项进行选择：

   - **应用到全部客户端**：将设置应用到所有现有客户端以及已添加到现有/将来域的任何新客户端。将来域是在配置设置时尚未创建的域。
   - **仅应用到将来的域**：仅将设置应用到添加到将来域的客户端。此选项不会将设置应用到添加到现有域的新客户端。

部分 IV

提供其他防护

第 15 章

使用插件管理器

本章讨论如何设置插件管理器，并概述了通过插件管理器提供的插件解决方案。

主题包括：

- 关于插件管理器 第 15-2 页
- 插件管理器安装 第 15-3 页
- 本机防毒墙网络版功能管理 第 15-4 页
- 管理插件程序 第 15-4 页
- 卸载插件管理器 第 15-10 页
- 插件管理器故障排除 第 15-11 页

关于插件管理器

防毒墙网络版包括一个将新的解决方案集成到现有防毒墙网络版环境的框架，称为插件管理器。为帮助简化这些解决方案的管理，插件管理器以小组件的形式为解决方案提供了概览数据。

注意

当前没有任何插件解决方案支持 IPv6。服务器可下载这些解决方案，但无法将其部署到纯 IPv6 防毒墙网络版客户端或纯 IPv6 主机。

插件管理器提供了两种类型的解决方案：

- **本机产品功能**

  一些本机防毒墙网络版功能单独授权，并通过插件管理器激活。在本版本中，有两种功能属于此类别，分别为**趋势科技虚拟桌面支持**和**防毒墙网络版数据保护**。

- **插件程序**

  插件程序不属于防毒墙网络版程序。插件程序具有各自的使用授权和管理控制台。可以从防毒墙网络版 Web 控制台访问这些管理控制台。插件程序的示例包括**入侵防御防火墙**和**趋势科技安全（适用于 Mac）**。

本文档提供了插件程序安装和管理的一般概述，并讨论了小组件中可用的插件程序数据。有关配置和管理程序的详细信息，请参考特定插件程序的文档。

终端上的插件程序客户端

一些插件程序（如入侵防御防火墙）具有安装在终端的 Windows 操作系统中的客户端。以进程名称 CNTAoSMgr.exe 运行的防毒墙网络版客户端插件管理器负责管理这些客户端。

防毒墙网络版会随防毒墙网络版客户端一起安装 CNTAoSMgr.exe。CNTAoSMgr.exe 仅有的额外系统要求是使用 Microsoft XML Parser (MSXML) 版本 3.0 或更高版本。

注意

客户端未安装在 Windows 操作系统中的其他插件程序无法通过防毒墙网络版客户端插件管理器进行管理。趋势科技安全（适用于 Mac）客户端就是这些客户端的一个示例。

小组件

使用小组件可以查看已部署的插件解决方案的概览数据。防毒墙网络版服务器的**控制台**窗口上提供了小组件。一个名为**防毒墙网络版与插件混合 Web 应用程序**的特殊小组件将防毒墙网络版客户端和插件解决方案中的数据结合起来，然后将数据显示在客户端树中。

本《管理员指南》概述了小组件以及支持小组件的解决方案。

插件管理器安装

在先前的插件管理器版本中，插件管理器安装包是从趋势科技 ActiveUpdate 服务器中下载的，然后安装在托管防毒墙网络版服务器的终端上。在此版本中，安装包包含在防毒墙网络版服务器安装包中。

防毒墙网络版的新用户在完成防毒墙网络版安装之后，会同时安装了防毒墙网络版服务器和插件管理器。将要升级至此防毒墙网络版版本且之前已使用插件管理器的用户需要先停止插件管理器服务，然后再运行安装包。

执行安装后任务

安装插件管理器之后执行以下操作：

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。

2. 管理插件解决方案。

3. 访问防毒墙网络版 Web 控制台上的**控制台**控制台以管理用于插件解决方案的小组件。

本机防毒墙网络版功能管理

本机防毒墙网络版功能随防毒墙网络版一起安装，管理员可从插件管理器激活各个功能。某些功能（如趋势科技虚拟桌面支持）通过插件管理器进行管理，而其他功能（如防毒墙网络版数据保护）则通过防毒墙网络版 Web 控制台进行管理。

管理插件程序

独立于防毒墙网络版安装并激活插件程序。每个插件都具有单独的产品管理控制台。可以从防毒墙网络版 Web 控制台访问这些管理控制台。

插件程序安装

插件程序会显示在**插件管理器**控制台上。使用控制台可下载、安装和管理这些程序。插件管理器会从趋势科技 ActiveUpdate 服务器或定制更新源（如果已正确设置）下载插件程序的安装包。要从 ActiveUpdate 服务器下载软件包，必须连接到 Internet。

当插件管理器下载安装软件包或开始安装时，插件管理器会暂时禁用其他插件程序功能（如下载、安装和升级）。

插件管理器不支持利用趋势科技防毒墙控制管理中心的单次登录功能安装或管理插件程序。

安装插件程序

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**下载**。

   插件程序软件包的大小将显示在**下载**按钮旁边。 插件管理器会将下载的软件包存储到 <服务器安装文件夹>\PCCSRV\Download\Product。

   插件管理器会将下载的软件包存储到<服务器安装文件夹>\PCCSRV\Download\Product。

   在下载过程中可以监控进度，也可以离开该窗口。

   注意

   如果防毒墙网络版在下载或安装软件包时遇到问题，请检查防毒墙网络版 Web 控制台上的服务器更新日志。在主菜单上，单击**日志** > **服务器更新**。

3. 单击**立即安装**或**稍后安装**。
   - 单击**立即安装**后，安装将会开始，并且会显示安装进度窗口。
   - 单击**稍后安装**后，将显示**插件管理器**窗口。

     单击**安装**按钮（位于**插件管理器**窗口上的“插件程序”部分中）以安装插件程序。

   此时将显示**趋势科技最终用户许可协议**窗口。

   注意

   并非所有插件程序都需要访问此窗口。如果未显示此窗口，插件程序安装将会开始。

4. 单击**同意**安装插件程序。

   在安装过程中可以监控进度，也可以离开该窗口。

注意

如果防毒墙网络版在下载或安装软件包时遇到问题，请检查防毒墙网络版 Web 控制台上的服务器更新日志。在主菜单上，单击**日志** > **服务器更新**。

安装后，当前插件程序版本会显示在**插件管理器**窗口上。

激活插件程序许可证

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**管理程序**。

   此时将显示**产品使用授权新激活码**窗口。
3. 在文本框中键入或复制并粘贴激活码。
4. 单击**保存**。

   此时将显示插件控制台。

查看和续订使用授权信息

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**管理程序**。
3. 在插件控制台中导航到**查看使用授权信息**超链接。

   并非所有插件程序都在同一个位置显示**查看使用授权信息**超链接。有关详细信息，请参考插件程序的用户文档。
4. 在打开的窗口中查看以下使用授权详细信息。

选项	说明
状态	显示“已激活”、“尚未激活”或“已过期”
版本	显示“完全版”或“试用版” **注意** 同时激活完全版和试用版时，只显示为“完全版”。
座席数	显示插件程序能够管理的终端数量
使用授权过期日期	如果插件程序有多个使用授权，则将显示最晚过期日期。 例如，如果使用授权到期日期为 12/31/2011 和 06/30/2011，则将显示 12/31/2011。
激活码	显示激活码
提醒	根据当前的使用授权版本，插件会在宽限期内（仅限完全版）或使用授权到期时显示关于使用授权到期日期的提醒

注意

宽限期的持续时间因地区而异。请与趋势科技代表核实插件程序宽限期。

插件程序使用授权到期后，插件可继续工作，但无法再获取更新和技术支持。

5. 单击**联机查看使用授权详细信息**，在趋势科技 Web 站点上查看当前使用授权的相关信息。
6. 要更新窗口以显示最新的使用授权信息，请单击**更新信息**。
7. 单击**新激活码**以打开**产品使用授权新激活码**窗口。

   有关详细信息，请参阅激活插件程序许可证 第 3-4 页。

插件程序管理

从插件程序的管理控制台（可从防毒墙网络版 Web 控制台访问）配置设置并执行程序相关任务。任务包括激活程序，也可能包括将插件程序客户端部署到终端。有关配置和管理程序的详细信息，请查阅特定插件程序的文档。

管理插件程序

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**管理程序**。



图 15-1. “管理程序”按钮

首次管理插件程序时，插件程序可能需要激活。有关详细信息，请参阅激活插件程序许可证 第 3-4 页。

插件程序升级

安装的插件程序的新版本会显示在插件管理器控制台上。在控制台上下载软件包并升级插件程序。插件管理器会从趋势科技 ActiveUpdate 服务器或定制更新源（如果已正确设置）下载软件包。要从 ActiveUpdate 服务器下载软件包，必须连接到 Internet。

当插件管理器下载安装软件包或开始升级时，插件管理器会暂时禁用其他插件程序功能（如下载、安装和升级）。

插件管理器不支持利用趋势科技防毒墙控制管理中心的单次登录功能进行插件程序升级。

升级插件程序

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**下载**。

   升级包的大小显示在**下载**按钮旁边。

   在下载过程中可以监控进度，也可以离开该窗口。

   注意

   如果防毒墙网络版在下载或安装软件包时遇到问题，请检查防毒墙网络版 Web 控制台上的服务器更新日志。在主菜单上，单击**日志** > **服务器更新**。
3. 插件管理器下载软件包后，会显示一个新窗口。
4. 单击**立即升级**或**稍后升级**。
   - 单击**立即升级**后，升级将会开始，并且会显示升级进度窗口。
   - 单击**稍后升级**后，将显示**插件管理器**窗口。

     单击**升级**按钮（位于**插件管理器**窗口上的“插件程序”部分中）以升级插件程序。

升级后，插件管理器服务可能需要重新启动，这会导致**插件管理器**窗口暂时不可用。该窗口可用时，会显示当前插件程序版本。

插件程序卸载

通过以下方法卸载插件程序：

- 从插件管理器控制台卸载插件程序。
- 卸载防毒墙网络版服务器，这会同时卸载插件管理器和已安装的所有插件程序。有关卸载防毒墙网络版服务器的说明，请参阅*防毒墙网络版安装和升级指南*。

对于终端上存在客户端的插件程序：

- 请查阅插件程序的文档了解卸载插件程序是否也将卸载插件客户端。
- 对于与防毒墙网络版客户端安装在同一个终端上的插件客户端，卸载防毒墙网络版客户端也将卸载插件客户端和防毒墙网络版客户端插件管理器 (CNTAoSMgr.exe)。

从插件管理器控制台卸载插件程序

过程

1. 打开防毒墙网络版 Web 控制台，然后单击主菜单中的**插件**。
2. 在**插件管理器**窗口中，转至“插件程序”部分，然后单击**卸载**。



3. 在卸载过程中可以监控卸载进度，也可以离开该窗口。
4. 卸载之后，请刷新**插件管理器**窗口。

   插件程序将再次变为可供安装。

卸载插件管理器

卸载防毒墙网络版服务器会同时卸载插件管理器和安装的所有插件程序。有关卸载防毒墙网络版服务器的说明，请参阅*防毒墙网络版安装和升级指南*。

插件管理器故障排除

查看防毒墙网络版服务器和防毒墙网络版客户端的调试日志，以了解插件管理器和插件程序的调试信息。

插件程序不显示在插件管理器控制台上

可供下载和安装的任何插件程序可能会因以下原因而无法显示在插件管理器控制台上：

过程

1. 插件管理器仍在下载插件程序，如果程序软件包太大，这可能需要一些时间。请不时检查屏幕以查看插件程序是否已显示。

   注意

   如果插件管理器无法下载插件程序，它会在 24 小时后自动重新下载。要手动触发插件管理器下载插件程序，请重新启动防毒墙网络版插件管理器服务。

2. 服务器计算机无法连接到 Internet。如果服务器通过代理服务器连接到 Internet，请确保可以使用代理服务器设置建立 Internet 连接。

3. 防毒墙网络版更新源不是 ActiveUpdate 服务器。在防毒墙网络版 Web 控制台上，转至**更新** > **服务器** > **更新源**，并检查更新源。如果更新源不是 ActiveUpdate 服务器，您有以下选项：

   - 选择 ActiveUpdate 服务器作为更新源。
   - 如果选择**其他更新源**，请选择**其他更新源**列表中的第一项作为更新源，并验证它是否可以成功连接到 ActiveUpdate 服务器。插件管理器仅支持列表中的第一项。
   - 如果选择**包含当前文件副本的 Intranet 位置**，请确保 Intranet 中的终端也可以连接到 ActiveUpdate 服务器。

终端上的插件客户端安装和显示问题

由于以下原因，在终端上安装插件程序的客户端可能会不成功，或者客户端可能无法显示在防毒墙网络版客户端控制台中：

过程

1. 终端上的插件管理器 (CNTAosMgr.exe) 未运行。在防毒墙网络版客户端终端上，打开“Windows 任务管理器”并运行 CNTAosMgr.exe 进程。
2. 未将插件客户端的安装包下载到位于 <客户端安装文件夹>\AU_Data\AU_Temp\{xxx}AU_Down\Product 中的防毒墙网络版客户端终端文件夹中。请检查位于\AU_Data\AU_Log\中的 Tmudump.txt 以了解下载不成功原因。

   注意

   如果成功安装客户端，则客户端信息会出现在 <客户端安装文件夹>\AOSSvcInfo.xml 中。

3. 客户端安装不成功或需要进一步操作。可从插件程序的管理控制台检查安装状态，并执行操作，如在安装后重新启动防毒墙网络版客户端终端或在安装前安装必需的操作系统 Patch。

Apache Web 服务器版本不受支持

插件管理器使用 Internet 服务器应用程序编程接口 (ISAPI) 处理某些 Web 请求。ISAPI 与 Apache Web 服务器版本 2.0.56 到 2.0.59 以及 2.2.3 到 2.2.4 不兼容。

如果运行的 Apache Web 服务器版本不兼容，可以将其替换为版本 2.2.25，该版本是防毒墙网络版和插件管理器正在使用的版本。该版本也与 ISAPI 相兼容。

过程

1. 将防毒墙网络版服务器升级至当前版本。

2. 在 <服务器安装文件夹> 中的 Apache2 文件夹中备份以下文件：
   - httpd.conf
   - httpd.conf.tmbackup
   - httpd.default.conf
3. 从“添加/删除程序”窗口卸载不兼容的服务器版本。
4. 安装 Apache Web 服务器 2.2.25。
   a. 从 <服务器安装文件夹>\Admin\Utility\Apache 启动 apache.msi。
   b. 在“服务器信息”窗口中，键入所需信息。
   c. 在“目标文件夹”窗口中，单击**更改**并浏览到 <服务器安装文件夹> 更改目标文件夹。
   d. 完成安装。
5. 将备份文件复制回 Apache2 文件夹。
6. 重新启动 Apache Web 服务器服务。

Internet Explorer 上的自动配置脚本设置重定向到代理服务器时，无法启动终端上的客户端

由于客户端启动命令重定向到代理服务器，因此防毒墙网络版客户端插件管理器 (CNTAosMgr.exe) 无法启动终端上的客户端。仅当代理服务器设置将用户的 HTTP 通信重定向为 127.0.0.1 时，才会发生这种问题。

要解决该问题，请使用定义明确的代理服务器策略。例如，不要将 HTTP 通信重新路由到 127.0.0.1。

如果需要使用控制 127.0.0.1 HTTP 请求的代理服务器配置，请执行以下任务：

过程

1. 在防毒墙网络版 Web 控制台上配置防毒墙网络版防火墙设置。

   注意

   如果在防毒墙网络版客户端上启用了防毒墙网络版防火墙，则执行此步骤。

   a. 在 Web 控制台上，转至**客户端** > **防火墙** > **策略**，然后单击**编辑例外模板**。

   b. 在“编辑例外模板”窗口中，单击**添加**。

   c. 使用以下信息：

      - **名称**：您的首选名称
      - **操作**：允许网络通信
      - **方向**：入站
      - **协议**：TCP
      - **端口**：5000 到 49151 之间的任意端口号

   d. **IP 地址**：选择**单个 IP 地址**，然后指定代理服务器的 IP 地址（建议），或者选择**所有 IP 地址**。

   e. 单击**保存**。

   f. 返回到“编辑例外模板”窗口，单击**保存并应用到现有策略上**。

   g. 转至**客户端** > **防火墙** > **概要文件**，然后单击**向客户端分配概要文件**。

      如果没有防火墙概要文件，则通过单击**添加**创建一个概要文件。请使用以下设置：

      - **名称**：您的首选名称
      - **描述**：首选描述
      - **策略**：所有访问策略

保存新概要文件后，单击**向客户端分配概要文件**。

2. 修改 ofcscan.ini 文件。

   a. 使用文本编辑器打开 <服务器安装文件夹> 中的 ofcscan.ini 文件。

   b. 搜索 **[Global Setting]**，然后将 `FWPortNum=21212` 添加到下一行。将 "21212" 更改为您在上述 c 中指定的端口号。

      例如：

      ```
      [Global Setting]

      FWPortNum=5000
      ```

   c. 保存文件。

3. 在 Web 控制台上，转至**客户端** > **全局客户端设置**，然后单击**保存**。

系统、更新模块或插件管理器程序中发生错误，并且错误消息提供了特定的错误代码

插件管理器会在错误消息中显示以下任一错误代码。如果参考下表中提供的解决方案后仍无法解决问题，请与您的技术支持提供商联系。

表 15-1. 插件管理器错误代码

错误代码	消息、原因和解决方案
001	**插件管理器程序中**发**生**错误。 查询**更新任务的**进**度**时，**插件管理器更新模**块**未响**应。**模**块**或命令**处**理程序可能尚未初始化。** 请**重新启**动**防毒墙网络版插件管理器服**务，**然后重新**执**行**该**任**务。

错误代码	消息、原因和解决方案
002	发生系统错误。 插件管理器更新模块无法打开注册表项 SOFTWARE\TrendMicro\OfficeScan \service\AoS，因为可能已将其删除。 执行下列步骤： 1. 打开注册表编辑器，然后转到 HKEY_LOCAL_MACHINE\SOFTWARE \TrendMicro\OfficeScan\ service\AoS \OSCE_Addon_Service_CompList_Version。将值重置为 1.0.1000。 2. 重新启动防毒墙网络版插件管理器服务。 3. 下载/卸载插件程序。
028	发生更新错误。 可能的原因： • 插件管理器更新模块无法下载插件程序。请验证网络连接是否有效，然后重试。 • 由于 AU Patch 代理已返回错误，因此插件管理器更新模块无法安装插件程序。AU Patch 代理是用于启动新插件程序安装的程序。有关错误的确切原因，请检查 \PCCSRV\Web\Service\AU_Data\AU_Log 中的 ActiveUpdate 模块调试日志“TmuDump.txt”。 执行下列步骤： 1. 打开注册表编辑器，然后导航到 HKEY_LOCAL_MACHINE\SOFTWARE \TrendMicro\OfficeScan\ service\AoS \OSCE_Addon_Service_CompList_Version。将值重置为 1.0.1000。 2. 删除插件程序注册表键 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \OfficeScan\ service\AoS\OSCE_ADDON_xxxx。 3. 重新启动防毒墙网络版插件管理器服务。 4. 下载和安装插件程序。
170	发生系统错误。 由于当前插件管理器更新模块正在处理其他操作，因此它无法处理传入操作。 稍后执行此任务。

错误代码	消息、原因和解决方案
202	插件管理器程序中发生错误。 插件管理器程序无法处理正在 Web 控制台上执行的任务。 如果有程序升级可用，请刷新 Web 控制台或升级插件管理器。
203	插件管理器程序中发生错误。 尝试与插件管理器后端服务通信时，插件管理器程序遇到进程间通信 (IPC) 错误。 请重新启动防毒墙网络版插件管理器服务，然后重新执行该任务。
其他错误代码	发生系统错误。 下载新的插件程序时，插件管理器将检查 ActiveUpdate 服务器中的插件程序列表。插件管理器无法获取列表。 执行下列步骤： 1. 打开注册表编辑器，然后导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`。将值重置为 `1.0.1000`。 2. 重新启动防毒墙网络版插件管理器服务。 3. 下载和安装插件程序。

第 16 章

资源故障排除

本章提供可以用于解决防毒墙网络版服务器和防毒墙网络版客户端问题的资源列表。

主题包括：

- 支持情报系统 第 16-2 页
- 案例诊断工具 第 16-2 页
- 趋势科技性能调整工具 第 16-2 页
- 防毒墙网络版服务器日志 第 16-2 页
- 防毒墙网络版客户端日志 第 16-15 页

支持情报系统

支持情报系统是您可以在其中轻松将文件发送到趋势科技进行分析的页面。此系统可确定防毒墙网络版服务器 GUID 并将该信息与所发送的文件一起发送。提供防毒墙网络版服务器 GUID 可确保趋势科技能够提供有关文件发送的反馈以进行评估。

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。

在防毒墙网络版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。

趋势科技性能调整工具

趋势科技提供了一个独立的性能调整工具，该工具可识别可能导致性能问题的应用程序。趋势科技性能调整工具（可以通过趋势科技知识库获得）应首先在标准的工作站镜像和/或几个目标工作站上试运行，以尽早发现并解决在实际部署行为监控和设备控制时出现的性能问题。

有关详细信息，请访问 http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionID=69719。

防毒墙网络版服务器日志

除可在 Web 控制台上访问的日志之外，您还可以使用其他类型的日志（例如调试日志）解决产品问题。

警告!

调试日志可能会影响服务器性能并消耗大量的磁盘空间。仅在需要时才启用调试日志记录，并且如果不再需要调试数据时立即禁用它。如果需要节省磁盘空间，请删除日志文件。

服务器调试日志（使用 LogServer.exe）

使用 LogServer.exe 为以下项目收集调试日志：

- 防毒墙网络版服务器基本日志
- 趋势科技漏洞扫描程序
- Active Directory 集成日志
- 客户端分组日志
- 安全合规日志
- 基于角色的管理
- 云安全扫描

启用调试日志记录

过程

1. 登录到 Web 控制台。
2. 在 Web 控制台的旗标中，单击 "OfficeScan" 中的第一个 "O"。
3. 选择**启用调试日志**。
4. 指定调试日志设置。
5. 单击**保存**。

6. 检查以下缺省位置中的日志文件 (ofcdebug.log)：服务器安装文件夹>\PCCSRV\Log。

禁用调试日志记录

过程

1. 登录到 Web 控制台。
2. 在 Web 控制台的旗标中，单击 "OfficeScan" 中的第一个 "O"。
3. 清除**启用调试日志**。
4. 单击**保存**。

启用服务器安装和升级的调试日志记录

在执行以下任务前启用调试日志记录：

- 卸载，然后再次安装服务器。
- 将防毒墙网络版升级到新版本。
- 执行远程安装/升级（调试日志记录在启动安装程序的终端上启用，而不在远程终端上启用）。

过程

1. 将位于 <服务器安装文件夹>\PCCSRV\Private 中的 LogServer 文件夹复制到 C:\。
2. 使用以下内容创建名为 cdebug.ini 的文件：

```
[debug]

debuglevel=9

debuglog=c:\LogServer\ofcdebug.log
```

```
debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. 将 ofcdebug.ini 保存到 C:\LogServer。
4. 执行适当的任务（即，卸载/重新安装服务器、升级到新服务器版本或执行远程安装/升级）。
5. 检查 C:\LogServer 中的 ofcdebug.log。

安装日志

- 本地安装/升级日志

  文件名：OFCMAS.LOG

  位置：%windir%

- 远程安装/升级日志
  - 在启动安装程序的终端上：

    文件名：ofcmasr.log

    位置：%windir%
  - 在目标终端上：

    文件名：OFCMAS.LOG

    位置：%windir%

Active Directory 日志

- 文件名：ofcdebug.log
- 文件名：ofcserver.ini

  位置：<服务器安装文件夹>\PCCSRV\Private\
- 文件名：
  - dbADScope.cdx
  - dbADScope.dbf
  - dbADPredefinedScope.cdx
  - dbADPredefinedScope.dbf
  - dbCredential.cdx
  - dbCredential.dbf

  位置：<服务器安装文件夹>\PCCSRV\HTTPDB\

基于角色的管理日志

要获取详细的基于角色的管理信息，请执行以下操作之一：

- 运行趋势科技情况诊断工具。有关信息，请参阅案例诊断工具 第 16-2 页。
- 收集下列日志：
  - <服务器安装文件夹>\PCCSRV\Private\AuthorStore 文件夹中的所有文件。
  - 防毒墙网络版服务器日志 第 16-2 页

防毒墙网络版客户端分组日志

- 文件名：ofcdebug.log
- 文件名：ofcserver.ini

  位置：<服务器安装文件夹>\PCCSRV\Private\
- 文件名：SortingRule.xml

  位置：<服务器安装文件夹>\PCCSRV\Private\SortingRuleStore\
- 文件名：
  - dbADScope.cdx
  - dbADScope.dbf

  位置：<服务器安装文件夹>\HTTPDB\

组件更新日志

文件名：TmuDump.txt

位置：<服务器安装文件夹>\PCCSRV\Web\Service\AU_Data\AU_Log

获取详细的服务器更新信息

过程

1. 使用以下内容创建名为 aucfg.ini 的文件：

```
[Debug]
level=-1
[Downloader]
ProxyCache=0
```

2. 将该文件保存到 <服务器安装文件夹>\PCCSRV\Web\Service。
3. 重新启动防毒墙网络版主服务。

停止收集详细的服务器更新信息

过程

1. 删除 aucfg.ini。
2. 重新启动防毒墙网络版主服务。

Apache 服务器日志

文件名：

- install.log
- error.log
- access.log

位置：<服务器安装文件夹>\PCCSRV\Apache2

客户端打包程序日志

启用客户端打包程序创建过程的日志记录

过程

1. 修改 <服务器安装文件夹>\PCCSRV\Admin\Utility\ClientPackager 中的 ClnExtor.ini，如下所示：

```
[Common]
```

```
DebugMode=1
```

2. 检查 C:\ 中的 ClnPack.log。

禁用客户端打包程序创建过程的日志记录

过程

1. 打开 ClnExtor.ini。
2. 将“DebugMode”的值从 1 更改为 0。

安全合规报告日志

要获取详细的安全合规信息，请收集以下各项：

- 文件名：RBAUserProfile.ini

  位置：<服务器安装文件夹>\PCCSRV\Private\AuthorStore\

- <服务器安装文件夹>\PCCSRV\Log\Security Compliance Report 文件夹中的所有文件。
- 防毒墙网络版服务器日志 第 16-2 页

外部服务器管理日志

- 文件名：ofcdebug.log
- 文件名：ofcserver.ini

  位置：<服务器安装文件夹>\PCCSRV\Private\

- <服务器安装文件夹>\PCCSRV\Log\Outside Server Management Report\ 文件夹中的所有文件。

- 文件名：
  - dbADScope.cdx
  - dbADScope.dbf
  - dbClientInfo.cdx
  - dbclientInfo.dbf

  位置：<服务器安装文件夹>\HTTPDB\

设备控制例外日志

要获取详细的设备控制例外信息，请收集以下各项：

- 文件名：ofcscan.ini

  位置：<服务器安装文件夹>\
- 文件名：dbClientExtra.dbf

  位置：<服务器安装文件夹>\HTTPDB\
- 防毒墙网络版 Web 控制台中的设备控制例外列表。

Web 信誉日志

文件名：diagnostic.log

位置：<服务器安装文件夹>\PCCSRV\LWCS\

ServerProtect 标准服务器迁移工具日志

启用 ServerProtect 标准服务器迁移工具的调试日志：

过程

1. 使用以下内容创建名为 ofcdebug.ini 的文件：

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. 将该文件保存到 C:\。

3. 检查 C:\ 中的 ofcdebug.log。



注意

要禁用调试日志记录，请删除 ofcdebug.ini 文件。

VSEncrypt 日志

防毒墙网络版自动在用户帐户的临时文件夹中创建该调试日志 (VSEncrypt.log)。例如，C:\Documents and Settings\<用户名>\Local Settings\Temp。

控制管理中心 MCP 代理日志

<服务器安装文件夹>\PCCSRV\CMAgent 文件夹中的调试文件

- Agent.ini
- Product.ini
- 控制管理中心“设置”页面的屏幕截图
- ProductUI.zip

启用 MCP 代理的调试日志记录

过程

1. 修改 <服务器安装文件夹>\PCCSRV\CmAgent 中的 product.ini，如下所示：

```
[Debug]
debugmode = 3
debuglevel= 3
debugtype = 0
debugsize = 10000
debuglog = C:\CMAgent_debug.log
```

2. 从 Microsoft 管理控制台重新启动防毒墙网络版控制管理中心代理服务。
3. 检查 C:\ 中的 CMAgent_debug.log。

禁用 MCP 代理的调试日志记录

过程

1. 打开 product.ini 并删除以下内容：

```
debugmode = 3
debuglevel= 3
debugtype = 0
debugsize = 10000
debuglog = C:\CMAgent_debug.log
```

2. 重新启动防毒墙网络版控制管理中心服务。

病毒扫描引擎日志

启用病毒扫描引擎的调试日志：

过程

1. 打开注册表编辑器 (regedit.exe)。
2. 转到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`。
3. 将 "`DebugLogFlags`" 的值更改为 "`00003eff`"。
4. 执行导致您所遇到的扫描问题的步骤。
5. 检查 %windir% 中的 TMFilter.log。



注意

通过将 "`DebugLogFlags`" 的值恢复为 "`00000000`" 来禁用调试日志记录。

病毒/恶意软件日志

文件名：

- dbVirusLog.dbf
- dbVirusLog.cdx

位置：<服务器安装文件夹>\PCCSRV\HTTPDB\

间谍软件/灰色软件日志

文件名：

- dbSpywareLog.dbf

- dbSpywareLog.cdx

位置：<服务器安装文件夹>\PCCSRV\HTTPDB\

爆发日志

日志类型	文件
当前防火墙违例爆发日志	文件名：Cfw_Outbreak_Current.log 位置：<服务器安装文件夹>\PCCSRV\Log\
上次防火墙违例爆发日志	文件名：Cfw_Outbreak_Last.log 位置：<服务器安装文件夹>\PCCSRV\Log\
当前病毒/恶意软件爆发日志	文件名：Outbreak_Current.log 位置：<服务器安装文件夹>\PCCSRV\Log\
上次病毒/恶意软件爆发日志	文件名：Outbreak_Last.log 位置：<服务器安装文件夹>\PCCSRV\Log\
当前间谍软件/灰色软件爆发日志	文件名：Spyware_Outbreak_Current.log 位置：<服务器安装文件夹>\PCCSRV\Log\
上次间谍软件/灰色软件爆发日志	文件名：Spyware_Outbreak_Last.log 位置：<服务器安装文件夹>\PCCSRV\Log\

虚拟桌面支持日志

- 文件名：vdi_list.ini

  位置：<服务器安装文件夹>\PCCSRV\TEMP\

- 文件名：vdi.ini

  位置：<服务器安装文件夹>\PCCSRV\Private\

- 文件名：ofcdebug.txt

  位置：<服务器安装文件夹>\PCCSRV\

要生成 ofcdebug.txt，请启用调试日志记录。有关启用调试日志记录的说明，请参阅启用调试日志记录 第 16-3 页。

防毒墙网络版客户端日志

使用防毒墙网络版客户端日志（如调试日志）来解决防毒墙网络版客户端问题。

警告!

调试日志可能会影响客户端性能并消耗大量的磁盘空间。仅在需要时才启用调试日志记录，并且如果不再需要调试数据时立即禁用它。如果日志文件变得很大，则删除日志文件。

防毒墙网络版客户端调试日志（使用 LogServer.exe）

启用防毒墙网络版客户端的调试日志记录：

过程

1. 使用以下内容创建名为 ofcdebug.ini 的文件：

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760
```

```
debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. 将 ofcdebug.ini 发送给用户，指示他们将该文件保存到 C:\。

注意

LogServer.exe 在防毒墙网络版客户端终端每次启动时自动运行。指示用户不要关闭在终端启动时打开的 LogServer.exe 命令窗口，因为这会指示防毒墙网络版停止调试日志记录。如果用户关闭了该命令窗口，他们可以通过运行位于 <客户端安装文件夹> 中的 LogServer.exe 再次启动调试日志记录。

3. 对于每个防毒墙网络版客户端终端，检查 C:\ 中的 ofcdebug.log。

注意

通过删除 ofcdebug.ini，禁用防毒墙网络版客户端的调试日志记录。

全新安装日志

对于 MSI 软件包安装：

- 文件名：OFCNT.LOG
- 位置：<客户端安装文件夹>

对于 Web 安装：

- 文件名：WebInstall.log
- 位置：C:\

对于远程安装：

- 文件名：OFCNT.LOG
- 位置：C:\

对于 Autopcc 和 EXE 软件包安装：

- 文件名：OFCNT.LOG
- 位置：<客户端安装文件夹>%windir%\

升级/Hot Fix 日志

文件名：upgrade_yyyymmddhhmmss.log

位置：<客户端安装文件夹>\Temp

损害清除服务日志

启用损害清除服务的调试日志记录

过程

1. 打开 <客户端安装文件夹> 中的 TSC.ini。
2. 如下所示修改下行：

   ```
   DebugInfoLevel=5
   ```

3. 检查 <客户端安装文件夹>\debug 中的 TSCDebug.log。

禁用损害清除服务的调试日志记录

打开 TSC.ini，然后将 "`DebugInfoLevel`" 的值从 5 更改为 0。

清除日志

文件名：yyyymmdd.log

位置：<客户端安装文件夹>\report\

邮件扫描日志

文件名：SmolDbg.txt

位置：<客户端安装文件夹>

防毒墙网络版客户端连接日志

文件名：Conn_YYYYMMDD.log

位置：<客户端安装文件夹>\ConnLog

防毒墙网络版客户端更新日志

文件名：Tmudump.txt

位置：<客户端安装文件夹>\AU_Data\AU_Log

获取详细的防毒墙网络版客户端更新信息

过程

1. 使用以下内容创建名为 aucfg.ini 的文件：

```
[Debug]
level=-1
[Downloader]
ProxyCache=0
```

2. 将该文件保存到 <客户端安装文件夹>。
3. 重新加载防毒墙网络版客户端。

注意

通过删除 aucfg.ini 文件并重新加载防毒墙网络版客户端，停止收集详细的客户端更新信息。

爆发阻止日志

文件名：OPPLogs.log

位置：<客户端安装文件夹>\OppLog

爆发阻止恢复日志

文件名：

- TmOPP.ini
- TmOPPRestore.ini

位置：<客户端安装文件夹>\

防毒墙网络版防火墙日志

在 Windows Vista/Server 2008/7/Server 2012/8/8.1/10 计算机上启用通用防火墙驱动程序的调试日志记录

过程

1. 修改下列注册表值：

注册表项	值
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	类型：DWORD 值 (REG_DWORD) 名称：DebugCtrl 值：0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	类型：DWORD 值 (REG_DWORD) 名称：DebugCtrl 值：0x00001111

2. 重新启动终端。
3. 检查 C:\ 中的 wfp_log.txt 和 lwf_log.txt。

启用 Windows XP 和 Windows Server 2003 计算机上的通用防火墙驱动程序的调试日志记录

过程

1. 将以下数据添加到 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters 中：

- 类型：DWORD 值 (REG_DWORD)
- 名称：DebugCtrl
- 值：0x00001111

2. 重新启动终端。
3. 检查 C:\ 中的 cfw_log.txt。

禁用通用防火墙驱动程序的调试日志记录（所有操作系统）

过程

1. 删除注册表项中的 "DebugCtrl"。
2. 重新启动终端。

启用防毒墙网络版 NT 防火墙服务的调试日志记录

过程

1. 编辑位于 <客户端安装文件夹> 中的 TmPfw.ini，如下所示：

```
[ServiceSession]
Enable=1
```

2. 重新加载客户端。
3. 检查 C:\temp 中的 ddmmyyyy_NSC_TmPfw.log。

禁用防毒墙网络版 NT 防火墙服务的调试日志记录

过程

1. 打开 TmPfw.ini，然后将 "Enable" 值从 1 更改为 0。
2. 重新加载防毒墙网络版客户端。

Web 信誉和 POP3 邮件扫描日志

启用 Web 信誉和 POP3 邮件扫描功能的调试日志记录

过程

1. 编辑位于 <客户端安装文件夹> 中的 TmProxy.ini，如下所示：

```
[ServiceSession]
Enable=1
LogFolder=C:\temp
```

2. 重新加载防毒墙网络版客户端。
3. 检查 C:\temp 中的 ddmmyyyy_NSC_TmProxy.log。

禁用 Web 信誉和 POP3 邮件扫描功能的调试日志记录

过程

1. 打开 TmProxy.ini，然后将 "Enable" 值从 1 更改为 0。
2. 重新加载防毒墙网络版客户端。

设备控制例外列表日志

文件名：DAC_ELIST

位置：<客户端安装文件夹>\

数据保护调试日志

启用数据保护调试日志：

过程

1. 从技术支持提供商处获取 logger.cfg 文件。
2. 将下列数据添加至 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`：
   - 类型：**字符串**
   - 名称：`debugcfg`
   - 值：`C:\Log\logger.cfg`
3. 在 C:\ directory 中，创建名为“Log”的文件夹。
4. 将 logger.cfg 复制到 Log 文件夹。
5. 从 Web 控制台部署数据丢失防护和设备控制设置，以开始收集日志。

注意

通过删除注册表项中的 `debugcfg` 并重新启动终端，来禁用数据保护模块的调试日志记录。

Windows 事件日志

Windows 事件查看器记录成功应用程序事件，如“登录”或“更改帐户设置”。

过程

1. 执行以下操作之一：
   - 依次单击**开始** > **控制面板** > **性能和维护** > **管理工具** > **计算机管理**。
   - 打开包含事件查看器管理单元的 MMC。
2. 单击**事件查看器**。

传输驱动接口 (TDI) 日志

启用传输驱动接口 (TDI) 日志：

过程

1. 将以下数据添加到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters` 中：

参数	值
键 1	类型：`DWORD 值 (REG_DWORD)` **名称**：`Debug` 值：`1111`（十六进制）
键 2	类型：**字符串值** `(REG_SZ)` **名称**：`LogFile` 值：`C:\tmtdi.log`

2. 重新启动终端。

3. 检查 C:\ 中的 tmtdi.log。

注意

通过删除注册表项中的 `Debug` 和 `LogFile` 并重新启动终端，禁用 TDI 的调试日志记录。

第 17 章

技术支持

本章介绍如何联机查找解决方案、使用技术支持门户以及联系趋势科技。

主题包括：

- 资源故障排除 第 17-2 页
- 与趋势科技联系 第 17-4 页
- 将可疑内容发送给趋势科技 第 17-5 页
- 其他资源 第 17-6 页

资源故障排除

联系技术支持之前，请考虑访问以下趋势科技联机资源。

Trend Community

要获取帮助、分享经验、提问题以及与其他用户、爱好者和安全专家讨论安全问题，请访问以下网址：

http://community.trendmicro.com/

使用技术支持门户

趋势科技技术支持门户是一个 24x7 联机资源，包含有关常见问题和罕见问题的最新信息。

过程

1. 访问 http://esupport.trendmicro.com/zh-cn/default.aspx。
2. 选择产品或服务，或者单击按钮查找更多产品或服务。
3. 使用**搜索支持**文本框搜索可用解决方案。
4. 如果找不到任何解决方案，请单击**联系支持部门**，或者从以下网址提交支持案例：

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

   趋势科技技术支持工程师会对案例进行调查，并在 24 小时内作出响应。

安全情报社区

趋势科技网络安全专家是一个安全情报精英团队，他们专门从事威胁检测和分析、云计算和虚拟化安全以及数据加密。

请访问 http://www.trendmicro.com/us/security-intelligence/index.html 了解更多信息：

- 趋势科技博客、Twitter、Facebook、YouTube 及其他社交媒体
- 威胁报告、研究论文和重点文章
- 来自全球安全业内人士的解决方案、播客和简报
- 免费工具、应用和小组件

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

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://www.trendmicro.com/us/about-us/contact/index.html
- 趋势科技产品文档：

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

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://intkb.trendmicro.com/solution/zh-CN/1055473.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。

其他资源

除解决方案和技术支持之外，趋势科技还提供许多有用的联机资源，旨在帮助您及时掌握最新信息、了解创新技术并获知最新安全趋势。

TrendEdge

查找有关不支持的创新技术、工具以及趋势科技产品和服务的最佳实践的信息。TrendEdge 数据库包含许多文档，涵盖大量面向趋势科技合作伙伴、员工及其他感兴趣的团体的主题。

要查看添加到 TrendEdge 的最新信息，请访问以下网址：

http://trendedge.trendmicro.com/

下载专区

趋势科技可能会不定期发布针对报告的已知问题的 Patch 或适用于特定产品或服务的升级。要查找是否有任何 Patch 可用，请访问以下网址：

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

如果未应用某个 Patch（Patch 已过时），请打开自述文件确定该 Patch 是否与您的环境相关。自述文件还包含安装说明。

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

附录

附录

附录 A

防毒墙网络版中的 IPv6 支持

本附录的适用对象是打算在支持 IPv6 寻址的环境中部署防毒墙网络版的用户。本附录包含有关防毒墙网络版中 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。

防毒墙网络版服务器和客户端的 IPv6 支持

从版本 10.6 的防毒墙网络版起开始支持 IPv6。早期的防毒墙网络版版本不支持 IPv6 寻址。安装或升级满足 IPv6 要求的防毒墙网络版服务器和防毒墙网络版客户端之后，将自动启用 IPv6 支持。

防毒墙网络版服务器要求

防毒墙网络版服务器包括以下 IPv6 要求：

- 服务器必须安装在 Windows Server 2008 或 Windows Server 2012 上。不能将其安装在 Windows Server 2003 上，因为该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 服务器不支持 IPv6 寻址。
- 如果服务器将管理 IPv4 和 IPv6 防毒墙网络版客户端，则必须同时具有 IPv4 和 IPv6 地址，且必须用其主机名进行标识。如果服务器用其 IPv4 地址进行标识，则 IPv6 防毒墙网络版客户端无法连接到该服务器。如果纯 IPv4 客户端连接到用 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。

注意

只有在执行服务器的本地安装时，才能指定 FQDN。远程安装不支持此功能。

防毒墙网络版客户端要求

防毒墙网络版客户端必须安装在以下系统上：

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows 10

不能将其安装在 Windows Server 2003 和 Windows XP 上，因为这些操作系统不完全支持 IPv6 寻址。

防毒墙网络版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

下表列出了防毒墙网络版服务器仅具有 IPv6 地址时的限制。

表 A-1. 纯 IPv6 服务器限制

项	限制
客户端管理	纯 IPv6 服务器无法执行以下操作： • 将防毒墙网络版客户端部署到纯 IPv4 终端。 • 管理纯 IPv4 防毒墙网络版客户端。
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。

项	限制
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，但无法将任何插件解决方案部署到： • 纯 IPv4 防毒墙网络版客户端或纯 IPv4 主机（由于没有直接连接） • 纯 IPv6 防毒墙网络版客户端或纯 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防毒墙网络版服务器与它连接的实体或服务的实体之间。

纯 IPv6 防毒墙网络版客户端限制

下表列出了防毒墙网络版客户端仅具有 IPv6 地址时的限制。

表 A-2. 纯 IPv6 防毒墙网络版客户端限制

项目	限制
父级防毒墙网络版服务器	纯 IPv6 防毒墙网络版客户端不能由纯 IPv4 防毒墙网络版服务器管理。
更新	纯 IPv6 防毒墙网络版客户端无法从纯 IPv4 更新源进行更新，例如： • 趋势科技 ActiveUpdate 服务器 • 纯 IPv4 防毒墙网络版服务器 • 纯 IPv4 更新代理 • 任何纯 IPv4 定制更新源

项目	限制
扫描查询、Web 信誉查询以及智能反馈	纯 IPv6 防毒墙网络版客户端无法向云安全智能防护源发送查询，例如： • 云安全智能防护服务器 2.0（集成型或独立型） **注意** 云安全智能防护服务器自版本 2.5 开始支持 IPv6。 • 趋势科技云安全智能防护网络（也用于智能反馈）
软件安全	纯 IPv6 防毒墙网络版客户端无法连接到趋势科技托管的安全软件认证服务。
插件解决方案	纯 IPv6 防毒墙网络版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 防毒墙网络版客户端无法通过纯 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防毒墙网络版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。

- 防毒墙网络版接受标准 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
  ```

- 防毒墙网络版也接受链接-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，因为即使防毒墙网络版可以接受该地址，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，则防毒墙网络版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防毒墙网络版客户端，但是防毒墙网络版客户端会忽略它们。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 防毒墙网络版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。

- 客户端树

  每次显示客户端树时，纯 IPv6 防毒墙网络版客户端的 IPv6 地址都会显示在 **IP 地址**列下。对于双栈防毒墙网络版客户端，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

  双栈防毒墙网络版客户端向服务器注册时使用的 IP 地址可通过**客户端** > **全局客户端设置** > **首选 IP 地址**进行控制。

将客户端树设置导出到文件时，IPv6 地址也将显示在导出的文件中。

- 客户端状态

  转至**客户端 > 客户端管理 > 状态**可获得详细的客户端信息。在该窗口中，将会看到纯 IPv6 防毒墙网络版客户端的 IPv6 地址以及使用自身的 IPv6 地址向服务器注册的双栈防毒墙网络版客户端的 IPv6 地址。

- 日志

  双栈和纯 IPv6 防毒墙网络版客户端的 IPv6 地址将显示在以下日志中：

  - 病毒/恶意软件日志
  - 间谍软件/灰色软件日志
  - 防火墙日志
  - 连接验证日志

- 控制管理中心控制台

  下表列出了哪些防毒墙网络版服务器和防毒墙网络版客户端的 IP 地址显示在控制管理中心控制台上。

表 A-3. 显示在控制管理中心控制台上的防毒墙网络版服务器和防毒墙网络版客户端 IP 地址

防毒墙网络版	控制管理中心版本	
	6.0 或更高版本	5.5 SP1
双栈服务器	IPv4 和 IPv6	IPv4 和 IPv6
纯 IPv4 服务器	IPv4	IPv4
纯 IPv6 服务器	IPv6	IPv6
双栈防毒墙网络版客户端	防毒墙网络版客户端向防毒墙网络版服务器注册所使用的 IP 地址	防毒墙网络版客户端向防毒墙网络版服务器注册所使用的 IP 地址
纯 IPv4 防毒墙网络版客户端	IPv4	IPv4

防毒墙网络版	控制管理中心版本	
	6.0 或更高版本	5.5 SP1
纯 IPv6 防毒墙网络版客户端	IPv6	IPv6

附录 B

Windows Server Core 2008/2012 支持

本附录讨论防毒墙网络版对 Windows Server Core 2008/2012 的支持。

Windows Server Core 2008/2012 支持

Windows Server Core 2008/2012 是 Windows Server 2008/2012 的“最小”安装。在 Server Core 中：

- 删除了许多 Windows Server 2008/2012 选项和功能。
- 服务器运行极为精简的核心操作系统。
- 大部分任务都从命令行界面执行。
- 操作系统只运行少数服务，而且在启动期间只需要少量资源。

防毒墙网络版客户端支持 Server Core。本部分包含有关 Server Core 支持的信息。

防毒墙网络版服务器不支持 Server Core。

Windows Server Core 安装方法

不支持或只部分支持下列安装方法：

- Web 安装页面：不支持这种方法，因为 Server Core 没有 Internet Explorer。
- 趋势科技漏洞扫描程序：漏洞扫描程序工具无法在 Server Core 上本地运行。请从防毒墙网络版服务器或另一个终端运行此工具。

支持以下安装方法：

- 远程安装。有关详细信息，请参阅从防毒墙网络版 Web 控制台远程安装 第 5-17 页。
- 登录脚本安装
- 客户端打包程序

使用“登录脚本安装”安装防毒墙网络版客户端

过程

1. 打开命令提示符。
2. 键入以下命令以映射 AutoPcc.exe 文件的位置：

   ```
   net use <映射的驱动器盘符> \\<防毒墙网络版服务器主机名或 IP 地址>\ofcscan
   ```

   例如：

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

   此时将显示一条消息，通知您 AutoPcc.exe 的位置是否映射成功。
3. 键入映射的驱动器盘符和冒号以更改为 AutoPcc.exe 的位置。例如：

   ```
   P:
   ```
4. 键入以下命令以启动安装：

   ```
   AutoPcc.exe
   ```

以下镜像将在命令提示符上显示命令和结果。

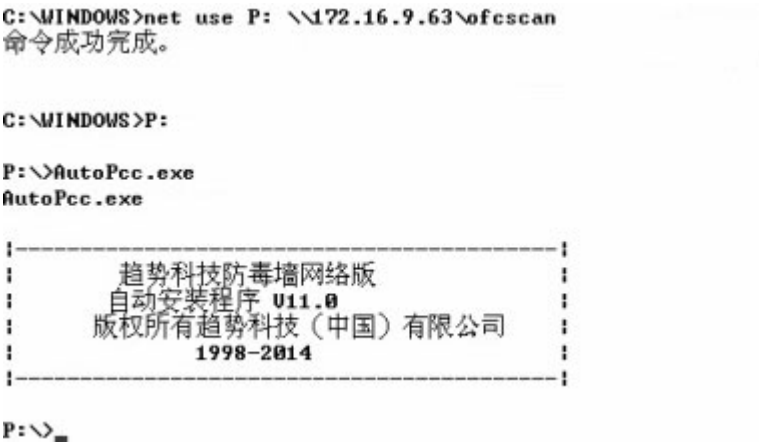


图 B-1. 命令提示符显示了如何使用“登录脚本安装”安装防毒墙网络版客户端

使用防毒墙网络版客户端软件包安装防毒墙网络版客户端

过程

1. 创建软件包。

   有关详细信息，请参阅使用客户端打包程序安装 第 5-22 页。

2. 打开命令提示符。

3. 键入以下命令以映射防毒墙网络版客户端软件包的位置：

   ```
   net use <映射的驱动器盘符> \\<客户端软件包的位置>
   ```

   例如：

   ```
   net use P: \\10.1.1.1\Package
   ```

此时将显示一条消息，通知您防毒墙网络版客户端软件包的位置是否映射成功。

4. 键入映射的驱动器盘符和冒号以更改为防毒墙网络版客户端软件包的位置。例如：

   ```
   P:
   ```

5. 键入以下命令以将防毒墙网络版客户端软件包复制到 Server Core 终端上的本地目录：

   ```
   copy <软件包文件名> <要将软件包复制到的 Server Core 终端上的目录>
   ```

   例如：

   ```
   copy officescan.msi C:\Client Package
   ```

   此时将显示一条消息，通知您防毒墙网络版客户端软件包是否复制成功。

6. 更改为本地目录。例如：

   ```
   C:
   ```

   ```
   cd C:\Client Package
   ```

7. 键入软件包文件名以启动安装。例如：

   ```
   officescan.msi
   ```

以下镜像将在命令提示符上显示命令和结果。



图 B-2. 命令提示符显示了如何使用客户端软件包安装防毒墙网络版客户端

Windows Server Core 上的防毒墙网络版客户端功能

Windows Server 2008/2012 上可用的大部分防毒墙网络版客户端功能在 Server Core 上都可用。唯一不支持的功能是漫游模式。

有关 Windows Server 2008/2012 上可用功能的列表，请参阅防毒墙网络版客户端功能 第 5-3 页。

只能从命令行界面访问防毒墙网络版客户端控制台。

注意

某些防毒墙网络版客户端控制台窗口包含“帮助”按钮，单击此按钮时，将打开上下文相关且基于 HTML 的帮助。由于 Windows Server Core 2008/2012 缺少浏览器，因此“帮助”将无法供用户使用。要查看“帮助”，用户必须安装浏览器。

Windows Server Core 命令

通过从命令行界面发出命令来执行防毒墙网络版客户端任务。

要运行命令，请转到 PccNTMon.exe 的位置。此进程负责启动防毒墙网络版客户端控制台。可在 <客户端安装文件夹> 下找到此进程。

下表列出了可用的命令。

表 B-1. Windows Server Core 命令

命令	处理措施
pccnt <drive or folder path>	扫描指定的驱动器或文件夹中是否存在安全风险 准则： • 如果文件夹路径中包含空格，则使用引号将整个路径括起来。 • 不支持扫描单个文件。 正确的命令： • pccnt C:\ • pccnt D:\Files • pccnt "C:\Documents and Settings" 不正确的命令： • pccnt C:\Documents and Settings • pccnt D:\Files\example.doc
pccntmon -r	打开实时监控程序
pccntmon -v	列出客户端组件及其版本
pccntmon -u	更新防毒墙网络版客户端组件
pccntmon -n <unload_password>	退出防毒墙网络版客户端 要重新加载防毒墙网络版客户端，请键入以下命令： pccntmon

命令	处理措施
`pccntmon -m <uninstall_password>`	卸载防毒墙网络版客户端
`pccntmon -c`	在命令行中显示以下信息： • 扫描方法 • 云安全扫描 • 传统扫描 • 特征码状态 • 已更新 • 已过期 • 实时扫描服务 • 正常运行 • 已禁用或未正常运行 • 客户端连接状态 • 联机 • 漫游 • 脱机 • Web 信誉服务 • 可用 • 正在重新连接 • 文件信誉服务 • 可用 • 正在重新连接
`pccntmon -h`	显示所有可用命令

附录 C

Windows 8/8.1/10 和 Windows Server 2012 支持

本附录讨论防毒墙网络版对 Windows 8/8.1/10 和 Windows Server 2012 的支持。

关于 Windows 8/8.1/10 和 Windows Server 2012

Windows 8/8.1 和 Windows Server 2012 可向用户提供两种类型的运行模式：桌面模式和 Windows UI 模式。用户可以选择在桌面模式或平板电脑模式下运行 Windows 10。桌面模式类似于传统 Windows **开始**窗口。

Windows UI 模式可为用户提供全新的用户界面体验，使用起来与 Windows Phone 类似。新增功能包括滚动触摸屏界面、磁贴和 Toast 通知。

表 C-1. 磁贴和 Toast 通知

控制	描述
磁贴	磁贴类似于先前 Windows 版本中使用的桌面图标。用户单击或轻按磁贴可启动与该磁贴相关联的应用程序。 动态磁贴可向用户提供动态更新的特定于应用程序的信息。即使应用程序未运行，应用程序也可将信息发布到磁贴
Toast 通知	Toast 通知类似于弹出消息。这些通知提供关于应用程序运行时发生的事件的时效性信息。不管 Windows 当前处于桌面模式、显示锁定窗口，还是正在运行其他应用程序，Toast 通知均在前台显示。 **注意** 根据应用程序的不同，toast 通知可能不会在所有窗口或每种模式下均显示。

防毒墙网络版对磁贴和 Toast 通知的支持

下表介绍了防毒墙网络版如何在 Windows UI 模式下支持磁贴和 Toast 通知。

表 C-2. 防毒墙网络版对磁贴和 Toast 通知的支持

控制	防毒墙网络版技术支持
磁贴	防毒墙网络版向用户提供可链接到防毒墙网络版客户端程序的磁贴。当用户单击该磁贴时，Windows 会切换到桌面模式，并显示防毒墙网络版客户端程序。 **注意** 防毒墙网络版不支持动态磁贴。
Toast 通知	防毒墙网络版提供以下 Toast 通知： • 检测到可疑程序 • 预设扫描 • 已解决威胁 • 需要重新启动计算机 • 检测到 USB 存储设备 • 检测到爆发 **注意** 防毒墙网络版仅在 Windows UI 模式下显示 Toast 通知。

在 Windows 8/8.1 和 Windows Server 2012 中启用 Toast 通知

用户可以选择通过在防毒墙网络版客户端终端上修改 **PC 设置**来接收 toast 通知。防毒墙网络版要求用户启用 toast 通知。

过程

1. 将鼠标指针移至窗口右下方以显示**超级按钮**栏。
2. 单击**设置** > **更改电脑设置**。

将显示“**PC 设置**”窗口。

3. 单击**通知**。
4. 在**通知**部分下，将以下设置设置为**启用**：
   - **显示应用程序通知**
   - **在锁定窗口上显示应用程序通知**（可选）
   - **播放通知声音**（可选）

在 Windows 10 中启用 Toast 通知

用户可以选择通过在防毒墙网络版客户端终端上访问 **Active Center** 来接收 Toast 通知。防毒墙网络版要求用户启用 Toast 通知。

过程

1. 在系统托盘中，单击通知图标和**所有设置**。
2. 在“设置”窗口中，单击**系统**和**通知和操作**。
3. 在**通知**部分下，将**显示应用程序通知**设置为**开**。

处于 UI 模式的防毒墙网络版功能支持

用户运行 Windows 8/8.1 或 Windows Server 2012 所使用的模式会影响使用的 Internet Explorer 10 及更高版本，因此也会影响不同防毒墙网络版功能提供的支持级别。下表列出了处于桌面模式和 Windows UI 模式的不同防毒墙网络版功能的支持级别。

注意

未列出的功能可在两种 Windows 运行模式下提供完全支持。

表 C-3. 处于 UI 模式的防毒墙网络版功能支持

功能	桌面模式	WINDOWS UI
Web 服务器控制台	完全支持	不支持
Web 信誉	完全支持	有限支持 • HTTPS 扫描已禁用
防火墙	完全支持	有限支持 • 应用程序过滤已禁用

Internet Explorer 10/11 和 Microsoft Edge

Internet Explorer (IE) 10 是 Windows 8/8.1 和 Windows Server 2012 中的缺省浏览器。Internet Explorer 10 及更高版本有两个不同版本：一个适用于 Windows UI，另一个适用于桌面模式。

Microsoft Edge 是 Windows 10 中的缺省浏览器。

注意

在 Microsoft Edge 中已禁用 HTTPS 扫描，因为 Microsoft Edge 不支持插件扩展。

适用于 Windows UI 的 Internet Explorer 10 及更高版本可提供无需插件的浏览体验。用于 web 浏览的插件程序之前未遵循设定的标准，因此，这些插件程序采用的代码的质量时常变化。插件还要求使用更多系统资源，从而增加感染恶意软件的风险。

Microsoft 开发了适用于 Windows UI 的 Internet Explorer 10 及更高版本，以采用基于标准的新技术替换先前使用的插件解决方案。下表列出了 Internet Explorer 10 及更高版本使用的技术，用于替换较旧的插件技术。

表 C-4. 基于标准的技术与插件程序的比较

功能	万维网 (W3C) 标准技术	同等插件示例
视频和音频	HTML5 视频和音频	• Flash • Apple QuickTime • Silverlight
图形	• HTML5 画布 • 可缩放的向量图形 (SVG) • 级联样式表（级别 3）(CSS3) 过渡和动画 • CSS 转换	• Flash • Apple QuickTime • Silverlight • Java applet
脱机存储	• Web 存储 • 文件 API • IndexedDB • 应用程序缓存 API	• Flash • Java applet • Google Gears
网络通信、资源共享、文件上传	• HTML Web 消息传递 • 跨源资源共享 (CORS)	• Flash • Java applet

Microsoft 还开发了仅适用于桌面模式的可兼容插件的 Internet Explorer 10 及更高版本。如果使用 Windows UI 模式的用户遇到要求使用其他插件程序的 Web 站点，则 Internet Explorer 10 及更高版本中会显示一条通知，提示用户切换到桌面模式。一旦进入桌面模式，用户可以查看要求使用或安装第三方插件程序的 Web 站点。

附录 D

防毒墙网络版还原

本附录讨论了防毒墙网络版服务器和防毒墙网络版客户端还原支持。

还原防毒墙网络版服务器和防毒墙网络版客户端

防毒墙网络版还原过程涉及依次还原防毒墙网络版客户端和防毒墙网络版服务器。

重要信息

- 如果管理员之前在安装过程中选择了备份防毒墙网络版服务器，则管理员仅可使用以下步骤来还原防毒墙网络版服务器和防毒墙网络版客户端。如果服务器备份文件不可用，请参考防毒墙网络版 11.0 的《安装和升级指南》，以了解手动还原过程。
- 此版本的防毒墙网络版仅支持还原到以下防毒墙网络版版本：
  - 防毒墙网络版 11.0

还原防毒墙网络版客户端

过程

1. 请确保防毒墙网络版客户端可升级客户端程序。
   a. 在防毒墙网络版 11.0 SP1 Web 控制台上，导航到**客户端** > **客户端管理**。
   b. 选择要还原的防毒墙网络版客户端。
   c. 单击**设置** > **权限和其他设置** > **其他设置**选项卡。
   d. 启用**客户端可以更新组件，但不能升级防毒墙网络版客户端程序，也不能部署 hotfix** 选项。
2. 在防毒墙网络版 11.0 SP1 Web 控制台上，导航到**更新** > **客户端** > **更新源**。
3. 选择**定制的更新源**。

4. 在**定制的更新源列表**上，单击**添加**。

   此时打开一个新窗口。

5. 键入要还原的防毒墙网络版客户端的 IP 地址。

6. 键入更新源 URL。

   例如，键入：

   `http://<防毒墙网络版服务器的 IP 地址>:<端口>/OfficeScan/download/Rollback`

7. 单击**保存**。

8. 单击**通知所有客户端**。

   当要还原的防毒墙网络版客户端从该更新源进行更新时，会先卸载该防毒墙网络版客户端，然后再安装先前版本的防毒墙网络版客户端。



提示

管理员可通过对客户端启动手动更新来加快还原过程的速度。有关详细信息，请参阅手动更新防毒墙网络版客户端 第 6-41 页。

9. 安装先前版本的防毒墙网络版客户端后，通知用户重新启动计算机。

   完成还原过程后，防毒墙网络版客户端会继续向同一台防毒墙网络版服务器报告。



注意

还原防毒墙网络版客户端后，所有组件（包括病毒码）也会还原到先前版本。如果管理员未还原防毒墙网络版服务器，则已还原的防毒墙网络版客户端将无法更新组件。管理员必须将已还原的防毒墙网络版客户端的更新源更改为标准更新源，以便接收进一步的组件更新。

还原防毒墙网络版服务器

防毒墙网络版服务器的还原过程要求管理员手动停止 Windows 服务、更新系统注册表并在防毒墙网络版安装目录中替换防毒墙网络版服务器文件。

过程

1. 在防毒墙网络版服务器计算机上，停止以下服务：
   - 入侵防御防火墙（如果已安装）
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - 防毒墙网络版控制管理中心代理
   - 防毒墙网络版插件管理器
   - 防毒墙网络版主服务
   - Apache 2（如果使用 Apache Web 服务器）
   - World Wide Web Publishing 服务（如果使用 IIS Web 服务器）
2. 复制 <服务器安装文件夹>\PCCSRV\Backup\ServicePack1_<build_number>\ 目录中的所有文件，并将其放回到 <服务器安装文件夹>\PCCSRV\ 目录。
3. 单击**启动**，键入 `regedit`，然后按 ENTER 键。

   此时将显示**注册表编辑器**窗口。
4. 在左侧导航窗格中，选择以下注册表项之一：
   - 对于 32 位系统：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
   - 对于 64 位系统：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

5. 转到**文件** > **导入...**。

6. 选择位于 <服务器安装文件夹>\PCCSRV\Backup\ 目录中的 RegBak_ServicePack1_<build_number>.reg 文件。

7. 单击**是**以恢复所有先前的防毒墙网络版版本密钥。

8. 打开命令行编辑器（单击**启动**并键入 `cmd.exe`），然后键入以下命令，以便重置本地 Web 分类服务器性能计数器：

   ```
   cd <服务器安装文件夹>\PCCSRV\LWCS

   regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

   regsvr32.exe /s perfLWCSPerfMonMgr.dll
   ```

9. 重新启动以下服务：

   - 入侵防御防火墙（如果已安装）
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - 防毒墙网络版控制管理中心代理
   - 防毒墙网络版插件管理器
   - 防毒墙网络版主服务
   - Apache 2（如果使用 Apache Web 服务器）
   - World Wide Web Publishing 服务（如果使用 IIS Web 服务器）

10. 清除 Internet Explorer 缓存并手动移除 ActiveX 控件。有关移除 Internet Explorer 9 中的 ActiveX 控件的详细信息，请参阅 http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9。

    防毒墙网络版服务器已恢复为先前安装的版本。

提示

管理员可以通过在**关于**窗口（**帮助** > **关于**）上检查防毒墙网络版版本号来确认成功还原。

11. 确认防毒墙网络版已成功还原后，删除 <服务器安装文件夹>\PCCSRV\Backup\ 目录中的以下文件：

    - 文件夹：ServicePack1_<SP1_build_number>
    - 文件：RegBak_ServicePack1_<SP1_build_number>.reg

附录 E

词汇表

本词汇表中包含的术语提供了有关常用终端术语以及趋势科技产品和技术的详细信息。

ActiveUpdate

ActiveUpdate 是许多趋势科技产品的通用功能。在连接到趋势科技更新 Web 站点后，可使用 ActiveUpdate 通过 Internet 下载最新的病毒码文件、扫描引擎、程序及其他趋势科技组件文件。

压缩文件

单个文件，它包含一个或多个单独的文件以及用于由合适的程序（如 WinZip）提取的信息。

Cookie

一种存储有关 Internet 用户的信息（如名称、首选项和兴趣）的机制，Cookie 存储在 Web 浏览器中以供日后使用。当您下次访问浏览器具有其 Cookie 的 Web 站点时，浏览器会将该 Cookie 发送到 Web 服务器，然后 Web 服务器可以使用它向您显示定制的 Web 页。例如，您可能进入一个名称吸引您的 Web 站点。

拒绝服务攻击

拒绝服务 (DoS) 攻击是指终端或网络上导致“服务”（即网络连接）丢失的攻击。通常，DoS 攻击会对网络带宽产生负面影响或使系统资源（如终端的内存）超载。

DHCP

动态主机控制协议 (Dynamic Host Control Protocol, DHCP) 是一种将动态 IP 地址分配给网络中设备的协议。通过动态寻址，设备每次连接到网络时，可以使用

不同的 IP 地址。在一些系统中，设备的 IP 地址甚至可以在它仍处于连接状态时发生更改。DHCP 还支持混合使用静态和动态 IP 地址。

DNS

域名系统 (DNS) 是一种主要在 Internet 中使用的通用数据查询服务，用于将主机名转换为 IP 地址。

当 DNS 客户端从 DNS 服务器请求主机名和地址数据时，此过程称为解析。基本的 DNS 配置可导致服务器执行缺省解析。例如，一个远程服务器向另一个服务器查询当前区域中计算机上的数据。远程服务器中的客户端软件会查询解析程序，而解析程序将答复来自其数据库文件的请求。

域名

系统的完整名称，由其本地主机名和其域名组成，例如 tellsitall.com。域名应该足以确定 Internet 上任何主机的唯一 Internet 地址。此过程（称为“名称解析”）使用域名系统 (DNS)。

动态 IP 地址

动态 IP 地址是由 DHCP 服务器分配的 IP 地址。终端的 MAC 地址将保持不变，但是，DHCP 服务器可以根据可用性为终端分配新的 IP 地址。

ESMTP

增强的简单邮件传输协议 (ESMTP) 包括安全、认证和其他设备，从而节省带宽并保护服务器。

最终用户许可协议

最终用户许可协议或 EULA 是软件出版商和软件用户之间的合法合同。它通常概括出了对用户方的限制，用户可以通过在安装过程中不单击?我接受?而拒绝签订协议。当然，单击?我不接受?将终止软件产品的安装。

在安装某个免费软件过程中显示的 EULA 提示消息上单击?我接受?时，许多用户会不经意地同意在其计算机上安装间谍软件和其他类型的灰色软件。

误报

当安全软件错误地将某个文件检测为受到感染时，即发生误报。

FTP

文件传输协议 (FTP) 是用于将文件通过 Internet 从服务器传输到客户端的标准协议。有关详细信息，请参考“Network Working Group RFC 959”。

GeneriClean

GeneriClean，也称为参照性清除，是一种即使没有病毒清除组件可用也能清除病毒/恶意软件的新技术。GeneriClean 使用检测到的文件作为基础，确定检测到的文件是否在内存和注册表项中具有相应的进程/服务，然后将其一起移除。

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）。

缺省情况下，防毒墙网络版客户端可以安装 Hotfix。如果不希望防毒墙网络版客户端安装 Hotfix，请在 Web 控制台中更改客户端更新设置，方法如下：转至**客户端** > **客户端管理**，然后单击**设置** > **权限和其他设置** > **其他设置**选项卡。

如果您尝试在防毒墙网络版服务器上部署 Hot Fix 未成功，请使用“触探工具”更改该 Hot Fix 的时间戳。这将使防毒墙网络版将该 Hot Fix 文件解释为新文件，从而使服务器再次尝试自动部署此 Hot Fix。关于此工具的详细信息，请参阅运行防毒墙网络版客户端 Hot Fix 的触探工具 第 6-48 页。

HTTP

超文本传输协议 (HTTP) 是用于将 Web 页面（包括图形和多媒体内容）通过 Internet 从服务器传输到客户端的标准协议。

HTTPS

使用安全套接层 (SSL) 的超文本传输协议。HTTPS 是 HTTP 的变种，用于处理安全事务。

ICMP

网关或目标主机偶尔会使用 Internet 控制消息协议 (ICMP) 与源主机进行通信，例如，报告数据报处理过程中出现的错误。ICMP 将把 IP 基础支持用作更高级别的协议，但是，ICMP 实际上是 IP 的组成部分，由每个 IP 模块实施。在以下几个情况下会发送 ICMP 消息：例如，当数据报不能达到其目标时，当网关没有转发数据报的缓冲能力时，以及当网关可以将主机定向为在较短的路由上发送网络通信时。因特网协议的设计不是绝对可靠。这些控制消息的目的是在通信环境中提供有关问题的反馈，而不是使 IP 可靠。

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

病毒编写者经常通过使用实时压缩算法来尝试绕开病毒过滤。IntelliTrap 通过阻止实时压缩可执行文件和将其与其他恶意软件特征配对来帮助减少此类病毒进入网络的风险。由于 IntelliTrap 将这样的文件识别为安全风险，可能错误地阻止安全文件，因此，启用 IntelliTrap 后，请考虑隔离（不要删除或者清除）文件。如果用户经常交换实时压缩可执行文件，请禁用 IntelliTrap。

IntelliTrap 使用以下组件：

- 病毒扫描引擎
- IntelliTrap 特征码
- IntelliTrap 例外特征码

IP

“因特网协议 (IP) 规定了将数据块（称为数据报）从源到目标的传输，其中源和目标是由固定长度的地址识别的主机。”(RFC 791)

Java 文件

Java 是 Sun Microsystems 开发的通用编程语言。Java 文件包含 Java 代码。Java 支持以独立于平台的 Java "applets"applet 是用 Java 编程语言编写的程序，可以包括在 HTML 页中。当使用支持 Java 技术的浏览器查看包含 applet 的页面时，applet 会将其代码传输到终端，浏览器的 Java 虚拟机会执行 applet。

LDAP

轻型目录访问协议 (LDAP) 是一种应用程序协议，用于查询和修改通过 TCP/IP 运行的目录服务。

侦听端口

侦听端口用于客户端连接的数据交换请求。

MCP 代理

趋势科技管理通信协议 (MCP) 是趋势科技用于被管理产品的下一代客户端。MCP 替换了趋势科技管理基础架构 (TMI)，作为控制管理中心与防毒墙网络版通信的方法。MCP 具有一些新功能：

- 减少网络负荷和软件包大小
- 支持 NAT 和防火墙遍历
- HTTPS 支持
- 单向和双向通信支持
- 支持单次登录 (SSO)

- 集群节点支持

混合威胁攻击

混合威胁攻击利用企业网络中的多个入口点和漏洞，例如“Nimda”或“Code Red”威胁。

NAT

网络地址转换 (NAT) 是将地址池中的安全 IP 地址转换为临时的、外部的、已注册的 IP 地址的标准。这样，具有分配的专用 IP 地址的可信网络就可以访问 Internet。这还意味着您不必获取网络中每个计算机的已注册 IP 地址。

NetBIOS

网络基本输入输出系统 (NetBIOS) 是一个将诸如网络能力之类的功能添加到磁盘操作系统 (DOS) 基本输入/输出系统 (BIOS) 的应用程序接口 (API)。

单向通信

NAT 穿越在真实网络环境里已经日益成为一个重大问题。为处理此问题，MCP 使用了单向通信。单向通信使用 MCP 代理启动到服务器的连接，并轮询来自服务器的命令。每个请求是一条类似 CGI 命令的查询或日志传输。为减少网络的影响，MCP 代理保持连接活动，并打开尽可能多的连接。后继请求使用现有打开的连接。如果连接中断，所有到同一主机的 SSL 连接将受益于会话 ID 缓存，该缓存能极大地降低重新连接时间。

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。

Phish Attack（网络钓鱼攻击）

网络钓鱼（Phish 或 Phishing）是一种正在迅速发展的欺诈形式，它通过伪造合法的 Web 站点来试图欺骗 Web 用户以盗取私人信息。

通常情况下，没有疑心的用户会收到一封听上去很紧急的（并且看起来真实的）电子邮件，告诉他们现在他们的帐户出现了问题，必须要立即解决以免帐户中止。电子邮件中将包括一个 URL，指向一个外观跟实际站点一模一样的 Web 站点。复制合法的电子邮件与 Web 站点很容易，但是随后会更改所谓的后台，也就是接收被收集的数据的目标系统。

该电子邮件提示用户登录到站点并确认一些帐户信息。黑客会接收用户提供的数据，如登录名、密码、信用卡号或社会保险号。

网络钓鱼欺诈快速、便宜且易于维持。它对于从事犯罪活动的那些罪犯也有相当大的潜在利润。甚至是了解计算机的用户都难以察觉网络钓鱼。执法部门也难以跟踪。更糟的是无法对其起诉。

请向趋势科技报告怀疑是网络钓鱼站点的任一 Web 站点。

Ping

Ping 是向 IP 地址发送 ICMP 回显请求并等待响应的实用工具。Ping 实用工具可以确定使用指定 IP 地址的终端是否联机。

POP3

邮局协议 3 (POP3) 是存储电子邮件以及将其从服务器传输到客户端电子邮件应用程序的标准协议。

代理服务器

代理服务器是接受带有特殊前缀的 URL 的 World Wide Web 服务器，用于从本地缓存或远程服务器提取文档，然后将 URL 返回给请求方。

RPC

远程过程调用 (RPC) 是一种网络协议，允许在一个主机上运行的程序促使代码在另一个主机上执行。

安全 Patch

安全 Patch 关注的重点是适合部署到所有客户的安全问题。Windows 安全 Patch 包括一个安装程序，而非 Windows Patch 通常有一个安装脚本。

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。

SMTP

简单邮件传输协议 (SMTP) 是一种标准协议，用于通过 Internet 在服务器之间以及客户端与服务器之间传输电子邮件。

SNMP

简单网络管理协议 (SNMP) 是一种支持监控连接到网络的设备是否出现应进行管理的情况的协议。

SNMP 陷阱

简单网络管理协议 (SNMP) 陷阱是向网络管理员发送通知的方法，网络管理员使用的管理控制台应支持此协议。

防毒墙网络版可以将通知存储在管理信息库 (MIB) 中。可以使用 MIB 浏览器来查看 SNMP 陷阱通知。

SOCKS 4

SOCKS 4 是一种 TCP 协议，由代理服务器用来在内部网络上的客户端之间或在 LAN 及其外部的终端或服务器之间建立连接。SOCKS 4 协议提出连接请求，设置代理服务器线路并在 OSI 模型的应用程序层中继数据。

SSL

安全套接层 (SSL) 是由 Netscape 设计的一个协议，用于为在应用程序协议（例如 HTTP、Telnet 或 FTP）和 TCP/IP 之间分层的数据提供安全。此安全协议为

TCP/IP 连接提供了数据加密、服务器认证、消息完整性和可选的客户端认证。

SSL 证书

此数字证书建立安全的 HTTPS 通信。

TCP

传输控制协议 (Transmission Control Protocol, TCP) 是面向连接的且端对端的可靠协议，设计用来适应支持多网应用程序的分层协议层次结构。TCP 根据 IP 数据报来进行地址解析。有关信息，请参考“DARPA Internet Program RFC 793”。

Telnet

Telnet 是一种借助创建“网络虚拟终端”来进行终端设备交互（通过 TCP）的标准方法。有关详细信息，请参考“Network Working Group RFC 854”。

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终端。在爆发期间，防毒墙网络版 会封闭特洛伊木马程序可能使用的以下端口号。

表 E-1. 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

端口号	特洛伊木马程序	端口号	特洛伊木马程序
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
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

可信端口

服务器与防毒墙网络版客户端使用可信端口进行通信。

如果在爆发后封闭可信端口然后将网络设置恢复正常，则防毒墙网络版客户端将不会立即恢复与服务器的通信。仅经过了您在“爆发阻止设置”窗口中指定的时间（小时）后，才恢复客户端与服务器的通信。

防毒墙网络版使用 HTTP 端口（缺省情况下，8080）作为服务器上的可信端口。在安装过程中，可输入不同的端口号。要封闭此可信端口和防毒墙网络版客户端上的可信端口，请选中“端口封闭”窗口上的“封闭可信端口”复选框。

在安装过程中，主安装程序会随机生成防毒墙网络版客户端可信端口。

确定可信端口

过程

1. 访问 <服务器安装文件夹>\PCCSRV。
2. 使用文本编辑器（如记事本）打开 ofcscan.ini 文件。
3. 对于服务器可信端口，搜索字符串“Master_DomainPort”，然后检查与该字符串相邻的值。

   例如，如果字符串显示为 `Master_DomainPort`，这表示服务器上的可信端口是端口 80。
4. 对于客户端可信端口，搜索字符串“Client_LocalServer_Port”，然后检查邻近该字符串的值。

   例如，如果字符串显示为 `Client_LocalServer_Port=41375`，这表示客户端上的可信端口是端口 41375。

双向通信

除单向通信外，还可以选择双向通信。双向通信基于单向通信，但附加了一个基于 HTTP 的通道以接收服务器通知，从而提高通过 MCP 代理实时分发和处理来自服务器命令的能力。

UDP

用户数据报协议 (User Datagram Protocol, UDP) 是一种用于 IP 的无连接通信协议，使应用程序可以向其他程序发送消息。有关信息，请参考“DARPA Internet Program RFC 768”。

非可清除文件

病毒扫描引擎无法清除以下文件：

表 E-2. 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终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。如果终端运行正常，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终端。
	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 模式下重新启动终端。
	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，因为终端正在使用它们。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终端。
	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 终端，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 终端，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. 检查文件是否已被删除。

非可清除文件	说明和解决方案

	针对运行其他操作系统（或不使用 NTFS）的解决方案：
	1. 在 MS-DOS 模式下重新启动终端。
	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 终端，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终端。
	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 终端，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终端。

用不支持的压缩格式压缩过的文件	解决方案：解压缩文件。
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。

非可清除文件	说明和解决方案
遭破坏的文件	**解决方案**：删除文件。

受特洛伊木马感染的文件

特洛伊木马是执行意外或未授权操作（通常是恶意操作，例如显示消息、删除文件或格式化磁盘）的程序。特洛伊木马不感染文件，因此不需要清除。

解决方案：防毒墙网络版使用病毒清除引擎和病毒清除模板来移除特洛伊木马。

受蠕虫病毒感染的文件

蠕虫病毒是一种自包含程序（或程序集），能够将自身的功能性副本或段传播到其他终端系统。传播通常通过网络连接或电子邮件附件进行。由于文件是自包含程序，因此蠕虫病毒无法清除。

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：去掉写保护以允许防毒墙网络版清除该文件。

受密码保护的文件

包括受密码保护的压缩文件或受密码保护的 Microsoft Office 文件。

解决方案：去掉密码保护以允许防毒墙网络版清除这些文件。

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。防毒墙网络版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：如果防毒墙网络版成功清除受感染文件，则不需要保留备份副本。如果终端正常运行，则可以删除备份文件。

索引

A

ActiveAction, 7-32
Active Directory, 2-34-2-36, 2-50, 2-54, 5-12, 5-27
  定制客户端组, 2-34
  复制结构, 2-54
  基于角色的管理, 2-34
  集成, 2-34
  客户端分组, 2-50
  凭证, 2-35
  同步, 2-36
  外部服务器管理, 2-34
  作用域和查询, 14-63
ActiveSync, 10-35
ActiveX 恶意代码, 7-3
AutoPcc.exe, 5-10, 5-11, 5-19, 5-20

C

C&C 回呼
  全局设置
    用户定义的 IP 列表, 11-13
  小组件, 2-25
COM 文件感染源, 7-3
Conflicted ARP, 12-5
Cookie 扫描, 7-68
CPU 使用率, 7-25

D

DHCP 设置, 5-41
DSP, 9-8

E

EICAR 测试脚本, 5-62, 7-2
EXE 文件感染源, 7-3

F

FakeAV, 7-36
Fragmented IGMP, 12-5
FTP, 10-25

H

Hotfix, 6-10, 6-48
HTML 病毒, 7-3
HTTP 和 HTTPS, 10-25

I

IDS, 12-4
IM 应用程序, 10-25
IntelliScan, 7-23
IntelliTrap 例外特征码, 6-5
IntelliTrap 特征码, 6-5
intranet, 4-11
IPv6, 4-21
  支持, 4-21
IPv6 支持, A-2
  显示 IPv6 地址, A-6
  限制, A-3, A-4
IpXfer.exe, 14-22

J

JavaScript 病毒, 7-3
Java 恶意代码, 7-3

L

LAND Attack, 12-5
LogServer.exe, 16-3, 16-15

M

MAC 地址, 14-3
Microsoft Exchange 服务器扫描, 7-64
Microsoft SMS, 5-11, 5-28
MSI 软件包, 5-11, 5-12, 5-27, 5-28

N

NetBIOS, 2-50

O

Overlapping Fragment, 12-5

P

Patch, 6-10
PCRE, 10-6
Perle Compatible Regular Expressions, 10-6
Ping of Death, 12-4
ptngrowth.ini, 4-16, 4-17

R

rootkit, 7-2
Rootkit 检测, 6-9

S

ServerProtect, 5-57
SMB 协议, 10-26
SQL Server 迁移工具, 13-43, 13-46
  警报通知, 13-46
  配置, 13-43
SYN Flood, 12-5

T

Teardrop, 12-5
Tiny Fragment Attack, 12-5
TMPerftool, 16-2
TMTouch.exe, 6-48
Too Big Fragment, 12-4
TrendLabs, 17-6

U

URL 过滤引擎, 6-8
USB 设备
  允许列表, 9-12
    配置, 9-12

V

VBScript 病毒, 7-3
VDI, 14-67
  日志, 16-14
VDI 预扫描模板生成工具, 14-77

W

webmail, 10-26
Web 安装页面, 5-10, 5-13
Web 服务器信息, 13-47
Web 控制台, 1-10, 2-2-2-4
  URL, 2-3
  登录帐户, 2-3
  关于, 2-2
  密码, 2-3
  旗标, 2-4
  要求, 2-2
Web 威胁, 11-2
Web 信誉, 1-11, 5-3, 5-5, 11-4
  策略, 11-4
  日志, 16-10
Web 信誉服务, 4-3, 4-4
Web 阻止列表, 4-8, 4-19
Windows Server Core, B-2
  可用的客户端功能, B-6
  命令, B-7
  支持的安装方法, B-2
Windows 剪贴板, 10-35

A

安全 Patch, 6-10
安全风险, 7-2, 7-4-7-6
  防护, 1-10
  间谍软件/灰色软件, 7-4-7-6
  网络钓鱼攻击, E-9
安全合规, 14-51
  安装, 5-54

服务, 14-52
日志, 16-9
扫描, 14-55
设置, 14-57
外部服务器管理, 2-34, 14-62
预设评估, 14-61
执行, 14-63
执行更新, 6-47
组件, 14-54
安全软件认证服务, 7-71, 8-9, 12-24
安全软件认证列表, 12-3
安装, 5-2
安全合规, 5-54
插件程序, 15-4
插件管理器, 15-3
客户端, 5-2
数据保护, 3-2
安装前的任务, 5-14, 5-17, 5-54
按需扫描缓存, 7-59
案例诊断工具, 16-2

B

爆发条件, 7-94, 11-21, 12-28
爆发阻止, 2-18
策略, 7-99
禁用, 7-105
爆发阻止策略
封闭端口, 7-100
互斥处理, 7-103
拒绝访问压缩文件, 7-104
拒绝写访问, 7-102
限制/拒绝访问共享文件夹, 7-99
相互排斥, 7-103
压缩可执行文件, 7-104
表达式, 10-5
定制, 10-6, 10-9
条件, 10-7, 10-8
预定义的, 10-5, 10-6
病毒/恶意软件, 7-2-7-4
ActiveX 恶意代码, 7-3
COM 和 EXE 文件感染源, 7-3
Java 恶意代码, 7-3
rootkit, 7-2
VBScript、JavaScript 或 HTML 病毒, 7-3
测试病毒, 7-2
恶作剧程序, 7-2
宏病毒, 7-3
加壳软件, 7-2
类型, 7-2-7-4
潜在病毒/恶意软件, 7-4
蠕虫病毒, 7-3
特洛伊木马程序, 7-3
引导扇区病毒 (boot sector virus), 7-3
病毒/恶意软件扫描
结果, 7-83
全局设置, 7-62
病毒百科全书, 7-4
病毒码, 6-3, 6-46, 6-47
病毒码文件
Web 阻止列表, 4-8
云安全客户端病毒码, 4-7
云安全云端病毒码, 4-8
云安全智能防护, 4-7
病毒清除模板, 6-6
病毒清除引擎, 6-6
病毒扫描驱动程序, 6-4
病毒扫描引擎, 6-3
不受监控的电子邮件域, 10-23
不受监控的目标, 10-27, 10-28

C

参考服务器, 13-30
策略, 10-3

Web 信誉, 11-4
防火墙, 12-4, 12-8
数据丢失防护, 10-43
策略强制特征码, 6-9
测试病毒, 7-2
测试扫描, 5-62
插件程序
安装, 15-4
激活, 3-4, 15-6
卸载, 15-10
插件管理器, 1-10, 5-4, 5-7, 15-2
安装, 15-3
故障排除, 15-11
管理本机产品功能, 15-4
卸载, 15-10
程序, 2-20, 6-2

H

触探工具, 6-48

C

处理措施
数据丢失防护, 10-35
传统扫描, 7-8, 7-9
切换到云安全扫描, 7-9
存储设备
高级权限, 9-5, 9-6
权限, 9-4

D

代理服务器设置, 4-28
对于内部连接, 14-44
对于外部连接, 14-46
客户端, 4-28
权限, 14-46
用于服务器组件更新, 6-19
自动代理服务器设置, 14-48
导出设置, 14-49
导入设置, 14-49
登录脚本安装, 5-10, 5-11, 5-19, 5-20
第三方安全软件, 5-55
电子邮件域, 10-23
调试日志
服务器, 16-2
客户端, 16-15
定制表达式, 10-6–10-9
导入, 10-9
条件, 10-7, 10-8
定制的模板, 10-19
创建, 10-20
导入, 10-22
定制客户端组, 2-34, 2-50
独立型服务器, 4-6
独立型云安全智能防护服务器, 4-16
ptngrowth.ini, 4-16
端口封闭, 7-100

E

恶意软件行为阻止, 8-2
恶作剧程序, 7-2

F

防毒墙网络版
Web 服务器, 13-47
Web 控制台, 2-2
程序, 2-20
关键功能和优点, 1-9
关于, 1-2
客户端, 1-13
客户端服务, 14-11
日志, 13-35
使用授权, 13-38
数据库备份, 13-41
数据库扫描, 7-64

文档, xii
组件, 2-20, 6-2
组件更新, 5-62
防毒墙网络版服务器, 1-12
功能, 1-12
防毒墙网络版更新, 6-13
防毒墙网络版客户端
安装方法, 5-10
保留的磁盘空间, 6-44
导入和导出设置, 14-49
非活动客户端, 14-25
个文件, 14-13
进程, 14-15
客户端详细信息, 14-49
卸载, 5-63
与防毒墙网络版服务器连接, 14-26, 14-37
与云安全智能防护服务器的连接, 14-37
注册表项, 14-15
防护的持续性, 4-10
防火墙, 5-3, 5-5, 12-2
爆发监控, 12-5
策略, 12-8
策略例外, 12-12
测试, 12-29
概要文件, 12-4, 12-16
禁用, 12-6
权限, 12-6, 12-21
缺省策略例外, 12-13, 12-14
任务, 12-8
优点, 12-2
防火墙日志计数, 12-23
非存储设备
权限, 9-9
非活动客户端, 14-25
服务器调节程序, 13-55
服务器更新
代理服务器设置, 6-19
更新方法, 6-24
日志, 6-26
手动更新, 6-25
预设更新, 6-25
组件复制, 6-20
服务器日志
Active Directory 日志, 16-6
Apache 服务器日志, 16-8
ServerProtect 迁移工具调试日志, 16-11
VSEncrypt 调试日志, 16-11
Web 信誉日志, 16-10
安全合规日志, 16-9
本地安装/升级日志, 16-5
病毒扫描引擎调试日志, 16-13
调试日志, 16-3
基于角色的管理日志, 16-6
客户端打包程序日志, 16-8
客户端分组日志, 16-7
控制管理中心 MCP 代理日志, 16-11
设备控制日志, 16-10
外部服务器管理日志, 16-9
虚拟桌面支持日志, 16-14
远程安装/升级日志, 16-5
组件更新日志, 16-7
服务重新启动, 14-11

G

高级权限
存储设备, 9-5, 9-6
配置, 9-11
隔离管理器, 13-54
隔离目录, 7-34, 7-38
更新, 4-17, 4-19

防毒墙网络版服务器, 6-15
更新代理, 6-49
集成型云安全智能防护服务器, 4-17, 4-19
客户端, 6-26
云安全智能防护服务器, 6-14, 6-26
执行, 6-47
更新代理, 5-3, 5-5, 6-49
标准更新源, 6-52
分析报告, 6-56
更新方法, 6-55
系统要求, 6-49
指定, 6-50
组件复制, 6-54
更新方法
防毒墙网络版服务器, 6-24
更新代理, 6-55
客户端, 6-35
更新源
防毒墙网络版服务器, 6-18
更新代理, 6-51
客户端, 6-29
故障排除
插件管理器, 15-11
关键字, 10-5, 10-12
定制, 10-14, 10-15, 10-17
预定义的, 10-13, 10-14

H

合规报告, 14-51
宏病毒, 7-3

J

基于角色的管理, 2-34, 13-3
用户角色, 13-3
用户帐户, 13-12
集成服务器, 4-6
集成型云安全智能防护服务器, 4-17
ptngrowth.ini, 4-17
Web 阻止列表, 4-19
更新, 4-17, 4-19
组件, 4-19
加壳软件, 7-2
加密的文件, 7-38
监控的系统事件, 8-3
监控的系统事件的处理措施, 8-5
间谍软件/灰色软件, 7-4-7-6
拨号程序, 7-4
恶作剧程序, 7-5
防御, 7-6
广告程序, 7-4
黑客工具, 7-5
恢复, 7-45
间谍软件, 7-4
密码破解程序, 7-5
潜在威胁, 7-5
远程访问工具, 7-5
间谍软件/灰色软件扫描
处理措施, 7-41
结果, 7-89
允许列表, 7-43
间谍软件扫描引擎, 6-7
间谍软件特征码, 6-7
间谍软件主动监控特征码, 6-7
解压缩规则, 10-39

K

可能的病毒/恶意软件, 7-84
客户端, 2-50, 2-57, 2-58, 4-28, 5-2
安装, 5-2
代理服务器设置, 4-28
分组, 2-50
功能, 5-3
连接, 4-28

删除, 2-57
位置, 4-28
移动, 2-58
客户端安全级别, 14-16
客户端安装, 5-2, 5-20
安装后, 5-60
从 Web 安装页面, 5-13
从 Web 控制台, 5-17
登录脚本安装, 5-19
基于浏览器, 5-15
客户端打包程序, 5-22
使用“安全合规”, 5-54
使用客户端磁盘镜像, 5-32
使用漏洞扫描程序, 5-33
系统要求, 5-2
客户端磁盘镜像, 5-12, 5-32
客户端打包程序, 5-11, 5-22, 5-25, 5-27, 5-28
部署, 5-22
设置, 5-24
客户端分组, 2-50-2-54, 2-56-2-58
Active Directory, 2-50, 2-53
DNS, 2-50
IP 地址, 2-54
NetBIOS, 2-50
定制组, 2-50
方法, 2-50
更名域, 2-57
任务, 2-56
删除域或客户端, 2-57
手动, 2-50, 2-51
添加域, 2-56
移动客户端, 2-58
自动, 2-50, 2-52
客户端更新
标准源, 6-29
从 ActiveUpdate 服务器, 6-42
定制源, 6-31
禁用, 6-43
权限, 6-42
使用 NAT 的预设更新, 6-38
事件触发, 6-36
手动, 6-40
预设更新, 6-37
自动, 6-35
客户端控制台
访问限制, 14-17
客户端迁移程序, 14-22
客户端日志
TDI 调试日志, 16-24
Web 信誉调试日志, 16-22
爆发阻止调试日志, 16-19
调试日志, 16-15
防毒墙网络版防火墙调试日志, 16-20
客户端更新日志, 16-18
客户端连接日志, 16-18
全新安装日志, 16-16
升级/Hot Fix 日志, 16-17
数据保护调试日志, 10-58, 16-23
损害清除服务日志, 16-17
邮件扫描日志, 16-18
客户端树, 2-38-2-42, 2-45-2-48
查看, 2-40
常规任务, 2-39
高级搜索, 2-40, 2-41
关于, 2-38
过滤器, 2-40
特定任务, 2-41, 2-42, 2-45-2-48
安全风险日志, 2-48
爆发阻止, 2-45
还原组件更新, 2-47
客户端管理, 2-42
手动组件更新, 2-46

客户端卸载, 5-63
客户端自我保护, 14-12
控制管理中心
    MCP 代理日志, 16-11
    与防毒墙网络版集成, 13-22
控制台, 2-5
    用户帐户, 2-5
    摘要, 2-5, 2-7, 2-10

L

例外列表, 8-5
    行为监控, 8-5
立即更新, 6-43
立即扫描, 7-19
联机
    社区, 17-2
连接验证, 14-39
漏洞扫描程序, 5-12, 5-33
    DHCP 设置, 5-41
    ping 设置, 5-52
    产品查询, 5-46
    效力, 5-34
    支持的协议, 5-48
    终端描述检索, 5-49
逻辑运算符, 10-19

M

漫游客户端, 5-4, 5-7
密码, 13-53
命令与控制联系人警报服务, 11-2
    全局情报列表, 11-3
    沙盒虚拟平台, 11-3
    沙盒虚拟平台列表, 11-3
    云安全智能防护服务器, 11-3
模板, 10-18-10-20, 10-22
    定制, 10-19, 10-20, 10-22
    逻辑运算符, 10-19
    条件语句, 10-19
    预定义的, 10-18

P

评估模式, 7-68

Q

其他服务设置, 14-5, 14-6
迁移
    从 ServerProtect 标准服务器, 5-57
    从第三方安全软件, 5-56
前 10 项安全风险统计, 2-19
潜在病毒/恶意软件, 7-4
权限
    程序路径和名称, 9-8
    存储设备, 9-4
    代理服务器设置权限, 14-46
    防火墙权限, 12-21, 12-23
    非存储设备, 9-9
    高级, 9-11
    漫游权限, 14-19
    扫描权限, 7-48
    退出权限, 14-18
    邮件扫描权限, 7-56
    预设扫描权限, 7-50

R

日志, 13-35
    Web 信誉日志, 11-23
    安全风险日志, 7-81
    病毒/恶意软件日志, 7-71, 7-81
    防火墙日志, 12-22, 12-23, 12-26
    集中隔离恢复日志, 7-88
    间谍软件/灰色软件恢复日志, 7-91
    间谍软件/灰色软件日志, 7-88
    可疑文件日志, 7-92
    客户端更新日志, 6-46

连接验证日志, 14-40
扫描日志, 7-93
设备控制日志, 9-16
系统事件日志, 13-34
行为监控, 8-13
有关, 13-35
蠕虫病毒, 7-3
入侵检测系统, 12-4

S

扫描处理措施, 7-30
病毒/恶意软件, 7-66
间谍软件/灰色软件, 7-41
扫描的缓存设置, 7-58
扫描方法, 5-23
缺省, 7-7
扫描缓存, 7-58
扫描类型, 5-3, 5-5, 7-12
扫描例外, 7-26, 7-27
目录, 7-27
文件, 7-29
文件扩展名, 7-29
扫描权限, 7-47
扫描条件
CPU 使用率, 7-25
文件压缩, 7-24
要扫描的文件, 7-23
用户对文件执行的活动, 7-22
预设, 7-25
社区, 17-2
设备控制, 1-11, 9-2, 9-4-9-6, 9-8-9-13
USB 设备, 9-12
存储设备, 9-4-9-6
非存储设备, 9-9
高级权限, 9-11
配置, 9-11
管理访问权限, 9-10, 9-13
权限, 9-4-9-6, 9-8, 9-9
程序路径和名称, 9-8
日志, 9-16, 16-10
数字签名提供程序, 9-8
通配符, 9-9
通知, 9-16
外部设备, 9-10, 9-13
要求, 9-2
允许列表, 9-12
设备控制;设备控制列表;设备控制列表:
添加程序, 9-14
设备列表工具, 9-12
实时扫描, 7-12
实时扫描服务, 14-36
使用授权, 13-38
数据保护, 3-3
状态, 2-5
事件监控, 8-3
试用版, 13-38
手动客户端分组, 2-50, 2-51
手动扫描, 7-15
快捷方式, 7-63
受监控的电子邮件子域, 10-24
受监控的目标, 10-27, 10-29

Z

术语, xiii

S

数据保护, 10-2
安装, 3-2
部署, 3-5
使用授权, 3-3
卸载, 3-13
状态, 3-7
数据标识符, 10-4
表达式, 10-5

关键字, 10-5
文件属性, 10-5
数据丢失防护, 10-2-10-4
表达式, 10-5-10-9
策略, 10-3, 10-43
处理措施, 10-35
关键字, 10-12-10-15, 10-17
解压缩规则, 10-39
模板, 10-18-10-20, 10-22
数据标识符, 10-4
通道, 10-22
网络通道, 10-22, 10-23, 10-25-10-29, 10-38
文件属性, 10-10-10-12
系统和应用程序通道, 10-29, 10-30, 10-32, 10-33, 10-35
小组件, 2-22, 2-24
数据库备份, 13-41
数据库扫描, 7-64
数字签名缓存, 7-58
数字签名特征码, 6-9, 7-58
数字签名提供程序, 9-8
指定, 9-8
损害清除服务, 1-11, 5-3, 5-5

T

特洛伊木马程序, 1-11, 6-6, 7-3
条件
定制表达式, 10-7, 10-8
关键字, 10-15
条件语句, 10-19
通配符, 10-11
设备控制, 9-9
文件属性, 10-11
通用防火墙驱动程序, 6-7, 6-8, 16-20
通知
C&C 回呼检测, 11-19
Web 威胁检测, 11-15
爆发, 7-94, 11-21, 12-28
病毒/恶意软件检测, 7-36, 7-37
防火墙违例, 12-25
管理员, 10-49, 13-32
过期病毒码, 6-46
间谍软件/灰色软件检测, 7-42
客户端更新, 6-45
设备控制, 9-16
针对客户端用户, 7-78, 10-52
重新启动终端, 6-46

W

外部服务器管理, 2-34, 14-62
查询结果, 14-66
日志, 16-9
预设查询, 14-67
外部设备
管理访问权限, 9-10, 9-13
外部设备防护, 6-9
网关 IP 地址, 14-3
网关设置导入程序, 14-4
网络病毒, 7-3, 12-4
网络病毒墙, 4-28
网络钓鱼, E-9
网络通道, 10-22, 10-23, 10-25-10-29, 10-38
FTP, 10-25
HTTP 和 HTTPS, 10-25
IM 应用程序, 10-25
SMB 协议, 10-26
webmail, 10-26
不受监控的目标, 10-29, 10-38
传输范围, 10-29
冲突, 10-29
所有传输, 10-27
外部传输, 10-28
传输作用域和目标, 10-27
电子邮件客户端, 10-23

受监控目标, 10-29, 10-38
位置, 4-28
感知, 4-28
位置感知, 14-2
文档, xii
文件属性, 10-5, 10-10-10-12
创建, 10-11
导入, 10-12
通配符, 10-11
预定义的, 10-10
文件信誉, 4-3
文件信誉服务, 4-3
无法访问的客户端, 14-40

X

系统和应用程序通道, 10-22, 10-29, 10-30, 10-32, 10-33, 10-35
CD/DVD, 10-30
PGP 加密, 10-33
Windows 剪贴板, 10-35
打印机, 10-33
对等 (P2P), 10-32
可移动存储, 10-33
同步软件, 10-35
云存储服务, 10-30
系统要求
更新代理, 6-49
小组件, 2-7, 2-10, 2-13, 2-14, 2-18, 2-20-2-22, 2-24, 2-25, 2-28-2-30, 15-3
C&C 回呼事件, 2-25
Web 信誉排名居前的受威胁用户, 2-29
Web 信誉排名居前的威胁源, 2-28
安全风险检测, 2-18
爆发, 2-18
防病毒客户端连接, 2-14
防毒墙网络版与插件混合 Web 应用程序, 2-21
可用, 2-10
客户端-服务器连接, 2-13
客户端更新, 2-20
数据丢失防护 - 一段时间内的检测, 2-24
数据丢失防护 - 最匹配的检测, 2-22
文件信誉威胁地图, 2-30
卸载, 5-63
插件程序, 15-10
插件管理器, 15-10
从 Web 控制台, 5-64
使用卸载程序, 5-64
数据保护, 3-13
新增功能, 1-2
行为监控, 8-13
例外列表, 8-5
日志, 8-13
系统事件的处理措施, 8-5
行为监控核心服务, 6-9
行为监控检测特征码, 6-8
行为监控配置特征码, 6-9
行为监控驱动程序, 6-9
性能调整工具, 16-2
性能控制, 7-25
虚拟桌面支持, 14-67
选项卡, 2-7

Y

压缩文件, 7-24, 7-66
解压缩规则, 10-39
引导扇区病毒 (boot sector virus), 7-3
应用程序过滤, 12-3
用户角色
guest user, 13-9
Trend Power User, 13-9

管理员, 13-9
用户帐户, 2-5
控制台, 2-5
邮件扫描, 7-56
域, 2-50, 2-56, 2-57
客户端分组, 2-50
删除, 2-57
添加, 2-56
已更名, 2-57
预定义的表达式, 10-5
查看, 10-6
预定义的关键字
关键字数量, 10-13
距离, 10-14
预定义的模板, 10-18
预定义的小组件, 2-10
预定义的选项卡, 2-10
预启动的清除驱动程序, 6-6
预设评估, 14-61
预设扫描, 7-17
继续, 7-70
提醒, 7-69
跳过并停止, 7-51, 7-70
推迟, 7-69
自动停止, 7-69
远程安装, 5-11
云安全客户端病毒码, 4-7, 6-3
云安全扫描, 6-3, 7-8, 7-9
从传统扫描切换, 7-9
云安全云端病毒码, 4-8, 6-3
云安全智能反馈, 4-3
云安全智能防护, 4-2-4-9, 4-11, 4-21, 4-22
Web 信誉服务, 4-3, 4-4
病毒码文件, 4-7-4-9
Web 阻止列表, 4-8
更新过程, 4-9
云安全客户端病毒码, 4-7
云安全云端病毒码, 4-8
环境, 4-11
威胁数量, 4-2
文件信誉服务, 4-3
源, 4-6, 4-7, 4-21, 4-22
IPv6 支持, 4-21
比较, 4-6
位置, 4-22
协议, 4-7
云安全智能防护服务器, 4-6
云安全智能防护网络, 4-5
云安全智能防护服务器, 4-6, 4-12, 4-16, 4-17, 4-19
安装, 4-12
独立型, 4-6, 4-16
更新, 6-14, 6-26
集成型, 4-6, 4-17, 4-19
最佳实践, 4-16
云安全智能防护网络, 1-2, 4-5
允许的程序列表, 8-6
允许列表, 7-43

Z

增量特征码, 6-20
摘要
更新, 6-57
控制台, 2-5, 2-7, 2-10
摘要控制台, 2-5, 2-7, 2-10
产品使用授权状态, 2-5
小组件, 2-7
选项卡, 2-7
预定义的小组件, 2-10
预定义的选项卡, 2-10
组件和程序, 2-20
支持
TrendLabs, 17-6

更快解决问题, 17-4
知识库, 17-2
支持情报系统, 2-4, 16-2
资源故障排除, 16-1
自定义关键字, 10-14
导入, 10-17
条件, 10-15
自动客户端分组, 2-50, 2-52
阻止的程序列表, 8-6
组件, 2-20, 5-62, 6-2
更新权限和设置, 6-42
更新摘要, 6-57
在防毒墙网络版服务器上, 6-15
在更新代理上, 6-49
在客户端上, 6-26
组件复制, 6-20, 6-54
最终用户许可协议 (End User License Agreement, EULA), E-4

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: OSCM117089/150730