TREND MICRO™

趋势科技™

防毒墙控制管理中心 6.0

集中式企业安全管理

安装指南

文档编号：CMEM65332/120203

发布日期：2012 年 5 月

受美国专利号 5,623,600、5,889,943、5,951,698、6,119,165 的保护

趋势科技控制管理中心的用户文档介绍该软件的主要功能组件以及针对贵组织生产环境的安装说明。在安装和使用该软件之前，请详细阅读。

有关如何使用软件中具体功能的详细信息，可在联机帮助文件和趋势科技 Web 站点上的在线知识库中获得。

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其他文档有任何问题、意见或建议，请通过 service@trendmicro.com.cn 与我们联系。我们始终欢迎您的反馈。

目录

前言

第 1 章：趋势科技防毒墙控制管理中心简介

第 2 章：规划和实施控制管理中心部署

第 3 章：初次安装趋势科技防毒墙控制管理中心

第 6 章：获取支持

附录 A：控制管理中心系统清单

前言

前言

此《安装指南》介绍趋势科技™防毒墙控制管理中心™ 6.0，并指导您完成安装规划和控制管理中心安装。

本前言包含以下主题：

本版本中的新增功能

趋势科技防毒墙控制管理中心 6.0 引入了用于将产品设置从单个控制台直接部署到端点的策略管理机制，在管理功能方面取得了巨大进步。

控制管理中心 6.0 功能和增强功能

版本 6.0 具有以下新功能和增强功能。

功能	描述
策略管理	• 使用策略将产品设置部署到被管理产品 • 灵活的策略类型 • 基于角色的管理 • 从 Web 控制台轻松地更新策略模板
策略状态控制台小组件	• 实时更新产品设置的部署状态 • 监控已部署和待定目标的数目 • 查看待定目标的详细状态
策略模板更新	有新模板或更新的模板时，管理员可以从 Web 控制台轻松执行更新。

功能	描述
数据丢失防护 (DLP) 集成	DLP 是数据保护模块的一项功能，用于监控数字资产的传输。DLP 功能可以将信息丢失风险降至最低，并且可以提高数据使用特征码和危险业务流程的可见性。 控制管理中心集成了以下 DLP 功能： • 可管理的 DLP 模板和数据标识符 • 使用策略管理、DLP 模板和数据标识符将 DLP 设置部署到被管理产品 • 收集 DLP 日志以用于报表和事件通知 • 22 个预定义的 DLP 报表模板 • 五种 DLP 事件通知 • 四个控制台小组件 • 产品支持：防毒墙网络版、IMSVA 和防毒墙群件版 for Microsoft Exchange
收藏夹	管理员可以将菜单快捷方式添加到“收藏夹”菜单以便快速访问。

控制管理中心文档

本文档假定您具备系统安全的基本知识。为了对那些熟悉该产品较早版本的系统管理员和人员有所帮助，引用了一些控制管理中心的以前版本。如果没有用过较早版本的控制管理中心，则引用信息可能有助于加强您对控制管理中心概念的理解。

表 1. 控制管理中心文档

文档	描述
联机帮助	可以从控制管理中心 Web 控制台访问的基于 Web 的文档。 联机帮助包含有关控制管理中心组件、功能以及配置控制管理中心所需步骤的解释说明。
趋势科技联机帮助中心 (http://docs.trendmicro.com/zh-cn/home.aspx)	趋势科技联机帮助中心提供了最新的产品文档。
自述文件	自述文件包含在联机或打印文档中未披露的最新的产品信息。主题包括新功能说明、已知问题和产品发布历史。
安装指南	PDF 文档，可以从 Trend Micro Enterprise DVD 中获取或者从趋势科技 Web 站点下载。 《安装指南》包含有关如何安装控制管理中心以及如何配置基本设置使其启动和运行的详细指导说明。
管理员指南	PDF 文档，可以从控制管理中心的 Trend Micro Solutions DVD 中获取或者从趋势科技的 Web 站点下载。 《管理员指南》包含有关如何配置和管理控制管理中心和被管理产品的详细指导说明以及有关控制管理中心概念和功能的解释说明。
教程	PDF 文档，可以从控制管理中心的 Trend Micro Solutions DVD 中获取或者从趋势科技的 Web 站点下载。 《教程》包含有关如何部署、安装、配置和管理控制管理中心以及注册到控制管理中心的被管理产品的实用说明。

文档约定

为了帮助您轻松地查找和解释信息，本文档使用以下约定。

约定/术语	描述
大写	首字母缩写词、缩写词、特定命令的名称和键盘上的按键。
粗体	菜单和菜单命令、命令按钮、选项卡、选项和任务。
斜体	对其他文档的引用。
等宽体	示例命令行、程序代码、Web URL、文件名和程序输出。
 **注意**	配置说明。
 **提示**	推荐或建议。
 **警告!**	重要的操作和配置选项。
导航 > **路径**	访问特定窗口的导航路径。例如，**扫描** > **手动扫描**表示，在界面上先单击**扫描**，然后单击**手动扫描**。

第 1 章

趋势科技防毒墙™控制管理中心™简介

趋势科技防毒墙控制管理中心是一个中心管理控制台，用于管理网关、邮件服务器、文件服务器和公司台式机级别的趋势科技产品和服务。管理员可以使用策略管理功能配置产品设置并将其部署到被管理产品和端点。基于 Web 的控制管理中心管理控制台为整个网络中的防病毒和内容安全产品以及服务提供单一监控点。

本章包含以下主题：

控制管理中心标准版和高级版

控制管理中心有两个版本：标准版和高级版。控制管理中心高级版包括标准版中没有的功能。例如，控制管理中心高级版支持层叠管理结构。这意味着可通过父级控制管理中心高级服务器管理控制管理中心网络，父级控制管理中心高级服务器包含多个向其报告的子级控制管理中心高级服务器。父级服务器充当整个网络的集线器。

注意

控制管理中心高级版支持将以下版本作为子级控制管理中心服务器：

- 控制管理中心 6.0 高级版
- 控制管理中心 5.5 高级版
- 控制管理中心 5.0 高级版

控制管理中心 5.0/5.5/6.0 标准版服务器不能作为子级服务器。

有关控制管理中心标准版和高级版中所有功能的完整列表，请参阅控制管理中心产品版本比较 第 A-8 页。

介绍控制管理中心特性

趋势科技将控制管理中心设计用于管理组织局域网和广域网中部署的防病毒和内容安全产品以及服务。

表 1-1. 控制管理中心特性

功能	描述
策略管理	系统管理员可以使用策略从单个管理控制台配置产品设置并将其部署到被管理产品和端点。

功能	描述
集中配置	使用产品目录和层叠管理结构，这些功能使您可从单个管理控制台协调病毒响应和内容安全方面的工作。 这些功能有助于确保实施公司的病毒/恶意软件和内容安全策略的一致性。
前瞻性爆发阻止	使用爆发阻止服务 (OPS)，可以采取前瞻性步骤来保护您的网络，以免其受害于迫近的病毒/恶意软件爆发。
安全通信基础架构	控制管理中心使用了构建在安全套接层 (SSL) 协议上的通信基础架构。 根据所使用的安全设置，控制管理中心可以加密消息或使用认证加密消息。
安全配置和组件下载	这些功能允许您配置安全的 Web 控制台访问和组件下载。
任务委派	系统管理员可以向控制管理中心 Web 控制台用户提供具有定制权限的个性化帐户。 用户帐户定义用户可以在控制管理中心网络中查看和操作的内容。通过用户日志跟踪帐户的使用情况。
命令跟踪	此功能使您可以使用控制管理中心 Web 控制台监控执行的所有命令。 命令跟踪对于确定控制管理中心是否成功执行了持续时间长的命令（如病毒码更新和部署）是很有用的。
按需产品控制	实时控制被管理产品。 控制管理中心将在 Web 控制台上所作的配置修改立即发送给被管理产品。系统管理员可从 Web 控制台运行手动扫描。这种命令系统在病毒/恶意软件爆发期间是不可缺少的。
集中更新控制	更新病毒码、反垃圾邮件规则、扫描引擎和其他防病毒或内容安全组件，有助于确保所有被管理产品都保持最新。
集中报表	使用全面的日志和报表总览防病毒和内容安全产品性能。 控制管理中心从其管理的所有产品收集日志，您不再需要检查每个单独产品的日志。

了解趋势科技管理通信协议

趋势科技管理通信协议 (MCP) 代理是趋势科技被管理产品的下一代代理。MCP 替换趋势科技管理基础架构 (TMI) 作为控制管理中心与被管理产品通信的方式。MCP 有若干特性：

- 网络负载减少，软件包变小
- 支持 NAT 和防火墙遍历
- 支持 HTTPS
- 支持单向和双向通信
- 支持单次登录 (SSO)

网络负载减少，软件包变小

TMI 使用基于 XML 的应用程序协议。即使 XML 在协议设计方面提供了一定程度的可扩展性和灵活性，将 XML 用作通信协议的数据格式标准还是有以下缺点：

- 与其他数据格式（如 CGI 名称－值对和二进制结构）相比，XML 解析需要更多系统资源（该程序在服务器或设备上会留下很大的覆盖区域）。
- 使用 XML 传输信息需要的代理覆盖区域比其他数据格式大得多。
- 由于数据覆盖区域更大，数据处理性能更低。
- 数据包传输需要更长时间，传输率低于其他数据格式。

MCP 的数据格式设计用于解决这些问题。MCP 的数据格式为 BLOB（二进制）流，每项包括名称标识、类型、长度和值。此 BLOB 格式具有以下优点：

- **与 XML 比较数据传输大小更小：**每个数据类型只需要有限数目的字节来存储该信息。这些数据类型为整型、无符号整型、布尔型和浮点型。
- **解析速度更快：**使用固定的二进制格式，可以很容易地逐个解析每个数据项。与 XML 比较，性能快好几倍。

- **设计灵活性提高：**还考虑到了设计灵活性，因为每个项都包括名称标识、类型、长度和值。没有严格的项顺序，只有需要的时候，才会在通信协议中显示问候项。

除了将二进制流格式应用于数据传输外，多种类型的数据都能打包在一个连接中，无论是否压缩。使用这种类型的数据传输战略，可以节省网络带宽，并提高可伸缩性。

支持 NAT 和防火墙遍历

由于 IPv4 网络上的可寻址 IP 地址有限，已广泛使用 NAT（网络地址转换）设备，以允许多个终端计算机连接到 Internet。NAT 设备是通过将连接到 NAT 设备的计算机组成一个专用虚拟网络而实现这点的。连接到 NAT 设备的每台计算机都将有一个专用的专用虚拟 IP 地址。在向 Internet 发送请求之前，NAT 设备将把此专有 IP 地址转换为一个真实的 IP 地址。这会产生一些问题，因为每台连接的计算机都使用一个虚拟 IP，并且许多网络应用程序不能识别这种行为。这通常会产生意外的程序故障和网络连接问题。

对于与控制管理中心 2.5/3.0 代理一起使用的产品，会假设一个先决条件。服务器所依赖的一个事实是，可以通过从服务器启动到代理的连接而联系到代理。这是一个所谓的双向通信产品，因为两端都可以启动到对方的连接。当代理处于 NAT 设备后面（或控制管理中心服务器处于 NAT 设备后面）时，这个假设就不成立了，因为该连接只能路由到 NAT 设备，而不是 NAT 设备后面的产品（或处于 NAT 设备后面的控制管理中心服务器）。一个常用的解决方法是，在 NAT 设备上建立特定的映射关系，以指示它将入站请求自动路由到相应的代理。但是，这种解决方法需要用户介入，并且当需要大规模产品部署时，这样做的效果不太好。

MCP 通过引入了一个单向通信模型而解决了这个问题。使用单向通信，只有代理会启动到服务器的网络连接。服务器不能启动到代理的连接。此单向通信对日志数据传输效果很好。但是，服务器分派命令是在被动模式下发生的。也就是说，命令的部署依赖于代理向服务器轮询可用的命令。

支持 HTTPS

MCP 集成协议应用业界标准通信协议 (HTTP/HTTPS)。HTTP/HTTPS 与 TMI 比较有几个优点：

- IT 中的大多数人都熟悉 HTTP/HTTPS，这使得容易确定通信问题和发现这些问题的解决方法
- 对于多数企业环境，不需要在防火墙中打开额外的端口以允许数据包通过
- 可以使用为 HTTP/HTTPS 构建的现有安全机制，如 SSL/TLS 和 HTTP 摘要认证

使用 MCP，控制管理中心有三个安全级别：

- **正常安全**：控制管理中心使用 HTTP 进行通信
- **中等安全**：如果支持 HTTPS，控制管理中心使用 HTTPS 进行通信，如果不支持 HTTPS，则使用 HTTP 进行通信
- **高度安全**：控制管理中心使用 HTTPS 进行通信

单向通信

在当今真实的网络环境中，NAT 遍历已经成为越来越突出的问题。为了解决此问题，MCP 使用单向通信。单向通信使 MCP 客户端启动到服务器的连接并轮询来自服务器的命令。每个请求都是一个类似于 CGI 的命令查询或日志传输。为了减少网络影响，连接保持活动状态并尽可能地开放。随后的请求会使用现有打开的连接。即使丢失了该连接，通过 SSL 对同一主机的所有连接都得益于会话标识缓存，它大大减少了重新连接的时间。

双向通信

双向通信是除单向通信之外的另一种选择。它仍基于单向通信，但是有一个额外的通道来接收服务器的通知。这个额外的通道也是基于 HTTP 协议的。双向通信可以通过 MCP 代理改进从服务器实时分派和处理命令。MCP 代理端需要

一个 Web 服务器或者 CGI 兼容程序（可以处理 CGI 式的请求），以便能接收来自控制管理中心服务器的通知。

支持单次登录 (SSO)

通过 MCP，控制管理中心支持趋势科技产品的单次登录 (SSO) 功能。该功能允许用户登录到控制管理中心并访问其他趋势科技产品的资源，而无需再登录到这些产品。

控制管理中心体系结构

趋势科技防毒墙控制管理中心提供了一种方式，可从一个中心位置控制趋势科技的产品和服务。此应用程序简化了公司中对病毒/恶意软件和内容安全策略的管理。下表列出了控制管理中心使用的组件。

表 1-2. 控制管理中心组件

组件	描述
控制管理中心服务器	充当从代理收集的所有数据的资源库。它可以是标准版或高级版服务器。控制管理中心服务器包括以下功能部件： • 存储被管理产品配置和日志的 SQL 数据库 控制管理中心使用 Microsoft SQL Server 数据库 (`db_ControlManager.mdf`) 存储包含在日志、通信器时间表、被管理产品和子级服务器信息、用户帐户、网络环境和通知设置中的数据。 • 托管控制管理中心 Web 控制台的 Web 服务器 • 通过电子邮件发送事件通知的邮件服务器 控制管理中心可以向个别收件人或成组的收件人发送关于在控制管理中心网络中发生的事件的通知。配置事件中心，通过电子邮件、Windows 事件日志、MSN Messenger、SNMP、Syslog、寻呼机或任何贵公司用于发送通知的内部/业界标准应用程序发送通知。 • 生成防病毒和内容安全产品报表的报表服务器（仅在高级版中） 控制管理中心报表是关于在控制管理中心网络上发生的安全威胁事件和内容安全事件的在线数字集合。
趋势科技管理通信协议	MCP 处理控制管理中心服务器与支持下一代代理的被管理产品的交互。 MCP 是控制管理中心系统的新主干。 MCP 代理将随被管理产品安装并使用单向/双向通信与控制管理中心通信。MCP 代理轮询控制管理中心以获取指令和更新。
趋势科技管理基础架构	处理控制管理中心服务器与较旧被管理产品的交互。 通信器（或消息路由框架）是较旧的控制管理中心系统的通信主干部分。它是趋势科技管理基础架构 (TMI) 的一个组件。通信器处理控制管理中心服务器与较旧被管理产品之间的所有通信。它们与控制管理中心 2.x 代理交互，以与较旧被管理产品通信。

组件	描述
控制管理中心 2.x 代理	接收来自控制管理中心服务器的命令，并向控制管理中心服务器发送状态信息和日志 控制管理中心代理是在被管理产品服务器上安装的一种应用程序，它允许控制管理中心管理产品。代理与被管理产品和通信器交互。代理充当被管理产品与通信器之间的桥梁。因此，必须将代理与被管理产品安装在同一计算机上。
基于 Web 的管理控制台	使管理员可从与 Internet 连接且安装有 Windows™ Internet Explorer™ 的几乎任何计算机上管理控制管理中心 控制管理中心管理控制台是一个基于 Web 的控制台，它通过 Microsoft Internet Information Server (IIS) 在 Internet 上发布，并由控制管理中心服务器托管。它允许您使用兼容的 Web 浏览器从任何计算机管理控制管理中心网络。
小组件框架	使管理员可创建定制的控制台以监控控制管理中心网络。

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。

电子邮件信誉

趋势科技电子邮件信誉技术可以验证 IP 地址，方法是对照已知垃圾邮件来源的信誉数据库对其进行检查并使用可以实时评估电子邮件发件人信誉的动态服务。信誉评估是通过对 IP 地址的“行为”、活动的范围以及优先级历史记录进行连续分析而改进的。电子邮件信誉根据发件人的 IP 地址阻止云中的恶意电子邮件，避免威胁侵害网络或用户的 PC。

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中，因此所有用户都可以即时使用。高性能内容交付网络和本地高速缓存服务器可确保检查过程中延迟最短。云客户端体系结构除了可以显著缩小客户端的整体覆盖区域外，还可以提供更即时的防护，并免除了特征码部署的负担。

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。随后，Web 信誉继续扫描站点并阻止用户访问受感染的站点。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。为了提高准确度并减少误判，趋势科技 Web 信誉技术为站点内的特定页面或链接指定信誉分数，而不是对整个站点进行分类或阻止，因为通常情况下，只有合法站点的某些部分被黑客改造且信誉会随时间而动态改变。

智能反馈

趋势科技智能反馈在趋势科技产品与其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。

第 2 章

规划和实施控制管理中心部署

管理员将控制管理中心部署到他们的网络之前，必须考虑几个因素。本章帮助您规划部署和管理控制管理中心测试部署。

本章包含以下主题：

确定部署体系结构和战略

部署是在您的网络环境中战略性分发控制管理中心服务器，以便于管理防病毒产品和内容安全产品并提供最佳管理的过程。

将企业级客户端-服务器软件（如控制管理中心）部署到网络中时需要仔细的规划和评估。

为了方便规划，趋势科技提出了两种体系结构部署建议：

- **单地点部署**：指从位于中心办事处的单个控制管理中心分发和管理子级服务器、被管理产品和端点。如果您的组织有多个办事处，但各地点之间存在快速而可靠的局域网连接和广域网连接，则单地点部署仍适用于您的环境。
- **多地点部署**：指针对在不同地理位置都有主办事处的组织分发和管理控制管理中心服务器。

提示

如果是第一次使用控制管理中心，趋势科技建议使用控制管理中心高级父级服务器来处理单地点部署和多地点部署。

了解单地点部署

单地点部署指从位于中心办事处的单个控制管理中心分发和管理子级服务器、被管理产品和端点。

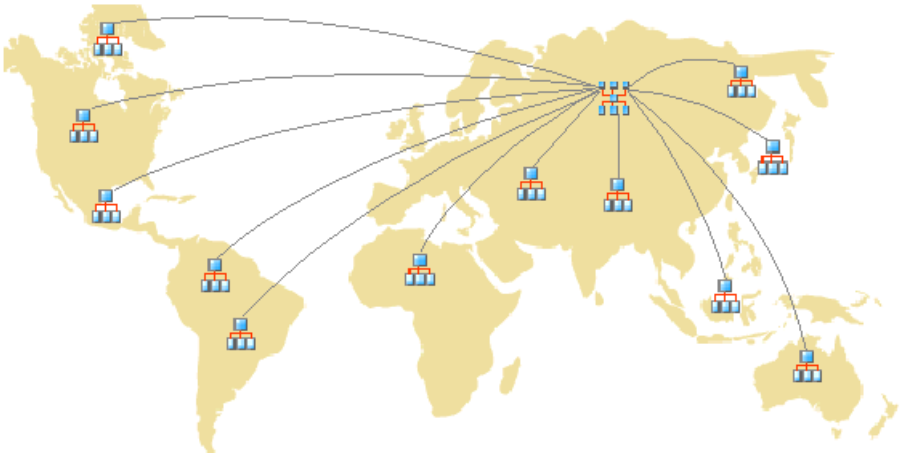


图 2-1. 使用高级版控制管理中心父级服务器和混合型子级服务器的单服务器部署

将控制管理中心部署到单地点之前，要完成以下任务：

1. 确定被管理产品、端点和层叠结构的数目
2. 规划下列各项的最佳比率：
   - 服务器管理产品与层叠结构
   - 服务器端点与层叠结构
3. 指定控制管理中心标准版服务器或控制管理中心高级版服务器

注意

控制管理中心 6.0 高级版支持将以下版本作为子级控制管理中心服务器：

- 控制管理中心 6.0 高级版
- 控制管理中心 5.5 高级版
- 控制管理中心 5.0 高级版

控制管理中心 5.0/5.5/6.0 标准版服务器不能作为子级服务器。

确定被管理产品、端点和层叠结构的数目

确定您计划使用控制管理中心管理多少个被管理产品、端点和层叠结构。您将需要这些信息来决定需要部署何种和多少控制管理中心服务器，以及将这些服务器放在网络中的什么位置来优化通信和管理。

规划服务器管理产品/服务器端点与层叠结构的最佳比率

确定单个控制管理中心服务器可以在本地网络上管理多少个被管理产品、端点和层叠结构的最关键因素是代理-服务器通信或父级服务器和子级服务器通信。

确定控制管理中心网络的 CPU 和内存要求时，请将建议的系统要求用作指南。

指定控制管理中心服务器

根据被管理产品、端点的数目和层叠结构要求，决定并指定控制管理中心服务器。决定是指定高级版服务器还是标准版服务器。

找到 Windows 服务器的位置，然后选择要指定为控制管理中心服务器的 Windows 服务器。还需要确定是否需要安装专用服务器。

选择将托管控制管理中心的服务器时，请考虑以下事项：

- CPU 负载
- 服务器执行的其他功能

如果您在具有其他用途的服务器（例如应用程序服务器）上安装控制管理中心，趋势科技建议您在未运行关键任务或耗费资源的应用程序的服务器上安装。

根据您的网络拓扑结构，可能需要执行其他特定于站点的任务。

了解多地点部署

与单地点部署相似，您需要收集相关网络信息并确定这些信息如何与将控制管理中心部署到多个地点相关。

因为每个网络都是独特的，所以请精确判断多少个控制管理中心服务器为最佳。

在多个不同的位置（包括非军事区 (DMZ) 或专用网络）部署控制管理中心服务器。将控制管理中心服务器置于公共网络上的 DMZ 中，以使用 Internet Explorer 通过 Internet 管理被管理产品、端点或子级服务器并访问控制管理中心 Web 控制台。

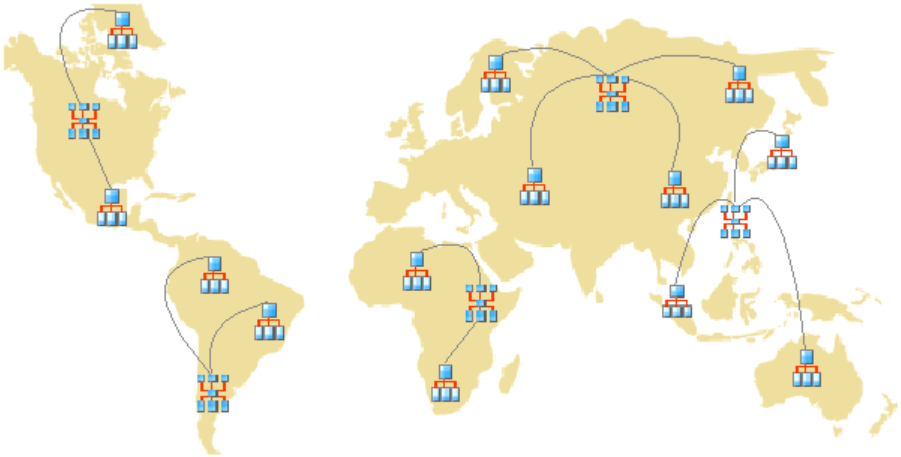


图 2-2. 使用多个控制管理中心高级父级服务器和混合型子级服务器的多地点部署

进行多地点部署时，请考虑以下事项：

- 对被管理产品、端点或子级服务器进行分组
- 确定地点的数目
- 确定被管理产品、端点和子级服务器的数目
- 规划网络流量
- 规划下列各项的最佳比率：
  - 服务器管理产品与层叠结构
  - 服务器端点与层叠结构
- 决定安装控制管理中心服务器的位置

对被管理产品、端点或子级服务器进行分组

当您对被管理产品和子级服务器进行分组时，请考虑以下事项：

表 2-1. 对被管理产品或子级服务器进行分组的注意事项

注意事项	描述
公司的网络策略和安全策略	如果有不同的访问权限和共享权适用于公司网络，则根据公司的网络策略和安全策略对被管理产品、端点和子级服务器进行分组。
组织结构和功能	根据公司的组织结构和功能划分对被管理产品、端点和子级服务器进行分组。例如，应有两个负责管理生产组和测试组的控制管理中心服务器。
地理位置	如果被管理产品、端点和子级服务器的位置影响到控制管理中心服务器与其被管理产品、端点或子级服务器之间的通信，则将地理位置用作分组条件。

注意事项	描述
管理责任	根据分配给被管理产品、端点和子级服务器的系统人员或安全人员对被管理产品、端点和子级服务器进行分组。这样就允许组配置。

确定地点的数目

确定您的控制管理中心部署将涉及到多少个地点。您需要这些信息来确定要安装的服务器的数目，以及要安装服务器的位置。

您可以从组织的 WAN 或 LAN 拓扑图中获取这些信息。

确定被管理产品、端点和子级服务器的数目

还需要了解控制管理中心服务器将要管理的被管理产品、端点和子级服务器的总数。趋势科技建议按地点收集被管理产品、端点和子级服务器数目的数据。如果您不能获取此信息，那么甚至粗略的估计值也将是有帮助的。您将需要这些信息来确定要安装的服务器的数目。

规划服务器管理产品/服务器端点与层叠结构的最佳比率

当在 WAN 中部署控制管理中心时，主办事处的控制管理中心服务器可管理远程办事处的被管理产品、端点和子级服务器。如果您打算让远程办事处的被管理产品、端点或子级服务器通过 WAN 向主办事处的服务器报告，则需要考虑 WAN 环境中网络带宽的变化。WAN 环境中不同的网络带宽对控制管理中心是有利的。如果让 LAN 和 WAN 上的被管理产品、端点或子级服务器向同一服务器报告，则报告会自然而然地错开时间；服务器会优先处理那些连接较快的被管理产品、端点或子级服务器（几乎在所有情况下都是 LAN 上的被管理产品、端点或子级服务器）。

确定控制管理中心网络的 CPU 和内存要求时，请将建议的系统要求用作指南。

指定控制管理中心服务器

根据被管理产品、端点的数目和层叠结构要求，决定并指定控制管理中心服务器。

找到 Windows 服务器的位置，然后选择要指定为控制管理中心服务器的 Windows 服务器。还需要确定是否需要安装专用服务器。

选择将托管控制管理中心的服务器时，请考虑以下事项：

- CPU 负载
- 服务器执行的其他功能

如果在具有其他用途的服务器（例如应用程序服务器）上安装控制管理中心，趋势科技建议您在未运行关键任务或耗费资源的应用程序的服务器上安装。

决定安装控制管理中心服务器的位置

一旦您了解了需要安装的客户端数目和服务器数目，则要决定安装控制管理中心服务器的位置。确定您是否需要在中心办事处安装所有服务器或是否需要将其中一些安装在远程办事处。

将这些服务器战略性地放在环境中的某些段中，可加快通信和优化被管理产品、端点和子级服务器的管理：

- **中心办事处**：中心办事处是组织中多数被管理产品、端点和子级服务器所处的场所。中心办事处有时被称为“总部”、“公司办公室”或“公司总部”。中心办事处可能在其他位置有其他的较小办事处或分部（在本指南中称为“远程办事处”）。

  提示

  趋势科技建议在中心办事处安装父级服务器。

- **远程办事处**：远程办事处定义为属于某个较大组织、并与中心办事处有 WAN 连接的任一小型专业办事处。如果您在远程办事处有被管理产品、端点和子级服务器向中心办事处的服务器报告，它们可能会在连接服务器时遇到困难。带宽限制可能会阻止出入控制管理中心服务器的正常通信。

中心办事处和远程办事处之间的网络带宽对于日常的客户机－服务器通信（例如更新配置设置和状态报表的通知）可能是足够的，但对于部署和其他任务则是不够的。

规划网络流量

服务器和被管理产品/端点/子级服务器通信时，控制管理中心会生成网络流量。规划控制管理中心网络流量，以将对组织网络的影响降至最低。

控制管理中心相关网络流量的来源有这些：

- 波动信号
- 日志
- 通信器时间表
- 被管理产品注册到控制管理中心服务器

  缺省情况下，控制管理中心服务器包含控制管理中心发布期间可用的所有产品概要文件。但是，如果将一个产品的新版本（不对应于任何现有的产品概要文件）注册到控制管理中心，新产品将把其概要文件上传到控制管理中心服务器。

  对于没有产品概要文件的全新趋势科技产品，趋势科技会提供更新以使控制管理中心可以识别这些产品。
- 子级服务器注册到控制管理中心父级服务器
- 下载和部署更新
- 策略部署

控制管理中心安装流程

安装控制管理中心系统是一个多步骤的过程，涉及以下事项：

1. 规划控制管理中心系统安装（服务器分布、网络流量、数据存储和 Web 服务器注意事项）。
2. 安装控制管理中心服务器。

注意

在控制管理中心服务器安装期间，提供备份和恢复文件的位置。

在一个位置测试控制管理中心

试验部署提供了确定功能如何工作和完全部署后可能需要的支持级别的反馈机会。

提示

趋势科技建议执行全面部署前先进行试验部署。

在一个位置试验控制管理中心可使您达到以下目的：

- 熟悉控制管理中心和被管理产品
- 制订或改进公司的网络策略

试验部署对于确定哪些配置需要改进是非常有用的。它使 IT 部门或安装团队有机会练习和改进部署过程，并验证部署计划是否符合组织的业务要求。

控制管理中心测试部署包括以下任务：

- 准备测试部署
- 选择测试地点
- 制订还原计划
- 开始测试部署
- 评估测试部署

准备测试部署

在准备阶段完成以下活动。

过程

1. 确定测试环境的控制管理中心服务器和代理配置。
   - 建立试用配置中所有系统之间的 TCP/IP 连接。
   - 通过从管理器系统向每个代理系统发送以及反向发送 ping 命令来验证双向 TCP/IP 通信。
2. 评估不同的部署方法，查看哪些方法适于您的特定环境。
3. 完成用于试验部署的系统清单。

选择测试地点

选择最匹配生产环境的试验地点。尝试尽可能模拟足以表示生产环境的那种拓扑。

制订还原计划

制订灾难恢复或还原计划（例如，如何还原为控制管理中心 5.0/5.5），以防安装或升级时有困难。此过程应考虑到本地公司策略以及 IT 资源。

开始测试部署

完成准备步骤和系统清单后，通过安装控制管理中心服务器和代理来开始试验部署。

评估测试部署

创建整个试验过程中遇到的成功和失败的列表。确定潜在的*缺陷*并相应地规划成功的部署。

您可以将试验评估计划贯彻到整个生产安装和部署计划中。

服务器分布计划

计划服务器分布时，请考虑以下事项：

- 管理模型
- 控制管理中心服务器分布
- 单服务器拓扑
- 多服务器拓扑

了解管理模型

在早期的控制管理中心部署中，精确确定要向多少人授予对控制管理中心服务器的访问权限。用户数目取决于管理的集中化程度。指导原则是：集中化程度与用户数成反比。

遵循以下管理模型之一：

- **集中式管理**：此模型将控制管理中心访问权限提供给尽可能少的人。高度集中化的网络将仅有一个管理员，他管理网络上的所有防病毒服务器和内容安全服务器。

  集中式管理提供了对网络防病毒和内容安全策略的最严密控制。但是，随着网络复杂性的提高，管理负担对于一个管理员而言将变得过大。

- **分散式管理**：这正符合系统管理员已明确定义并建立责任区域的大型网络的情况。例如，邮件服务器管理员可能还负责电子邮件防护；地区办事处可能独立负责其当地区域。

一个控制管理中心主管理员仍是必要的，但他或她将与其他产品或区域管理员分担监督网络的责任。

将控制管理中心访问权限授予每个管理员，但将访问权限限制为仅查看和/或配置控制管理中心网络中其负责的网段。

初始化其中一个管理模型后，您就可以配置产品目录和必要的用户帐户来管理控制管理中心网络。

了解控制管理中心服务器的分布

控制管理中心可以管理产品，而不考虑其实际位置如何，所以使用单一的控制管理服务器管理所有防病毒和内容安全产品是可能的。

但是，按不同的服务器（包括高级版用户的父级服务器和子级服务器）划分控制管理中心网络的控制是有利的。基于网络的独特性，您可以决定控制管理中心服务器的最佳数目。

单服务器拓扑

单服务器拓扑适用于中小型的单站点企业。此拓扑因为单个管理员而方便了管理，但不排除按您的管理计划需要而创建其他管理员帐户。

然而，这种安排将网络流量（代理轮询、数据查询、更新部署等等）的负担集中到了单个服务器以及托管该服务器的 LAN 上。随着您的网络的发展，对性能的影响也会增加。

多服务器拓扑

对于具有多个地点的较大企业，可能有必要设置地区控制管理中心服务器来分担网络负载。

关于控制管理中心网络生成的流量的信息，请参阅了解控制管理中心网络流量 第 2-14 页。

网络流量计划

要制订计划将控制管理中心对您的网络的影响降到最低，了解控制管理中心生成的网络流量非常重要。

下节帮助您了解控制管理中心网络生成的流量，并制订一个计划来使流量对网络的影响降到最低。此外，流量频率的相关章节还描述了控制管理中心网络上哪些来源频繁生成流量。

了解控制管理中心网络流量

要制订计划将控制管理中心对您的网络的影响降到最低，了解控制管理中心生成的网络流量非常重要。

网络流量的来源

以下控制管理中心来源会生成网络流量：

- 日志流量
- 趋势科技管理基础架构和 MCP 策略
- 产品注册
- 下载和部署更新
- 部署策略设置

流量频率

以下来源频繁在控制管理中心网络上生成流量：

- 由被管理产品生成的日志
- MCP 轮询和命令

- 趋势科技管理基础架构策略

日志

被管理产品以不同时间间隔（取决于各自的日志设置）向控制管理中心发送日志。

被管理产品代理波动信号

缺省情况下，被管理产品代理每 60 分钟发送一次波动信号消息。管理员可将该值调整为 5 到 480 分钟（8 小时）之间。选择波动信号设置时，请在显示最新通信器状态信息的需要和管理系统资源的需要之间选择一个平衡点。

缺省设置会满足大多数情况，但如果您认为需要自定义这些设置，请考虑以下事项：

- **长时间间隔波动信号（60 分钟以上）**：波动信号之间的时间间隔越长，控制管理中心控制台显示它之前可能发生的事件就越多。

  例如，如果一个代理连接问题在波动信号之间得到解决，则它就有可能与代理通信 - 即使其状态显示为*非活动*或*异常*。

- **短时间间隔波动信号（低于 60 分钟）**：波动信号时间间隔比较短，可以在控制管理中心服务器上展示较新的网络状态。但是，短时间间隔波动信号会增加所使用的网络带宽量。

注意

将时间间隔调整为低于 15 分钟之前，请考虑现有的网络流量以了解增加网络带宽使用量的影响。

网络协议

控制管理中心使用 UDP 和 TCP 协议进行通信。

网络通信的来源

日志流量

在控制管理中心网络中网络流量的持续来源是“产品日志”— 被管理产品定期向控制管理中心服务器发送的日志。

表 2-2. 控制管理中心日志流量

日志	包含的信息涉及
病毒/间谍软件/灰色软件	检测到的病毒/恶意软件、间谍软件、灰色软件和其他安全威胁
安全	由内容安全产品报告的违例。
Web 安全性	由 Web 安全产品报告的违例。
事件	其他事件（例如，组件更新、一般安全性违例等）。
状态	被管理产品的环境。产品目录的“状态”选项卡显示此信息。
网络病毒	在网络数据包中检测到的病毒。
性能指标	用于较早版本的产品
URL 使用	由 Web 安全产品报告的违例。
安全性违例	由网络病毒墙产品报告的违例。
安全合规	由网络病毒墙产品报告的端点安全合规。
安全性统计	由网络病毒墙产品计算并报告的安全合规和安全性违例之间的差异。
端点	由 Web 安全产品报表的违例。

趋势科技管理通信协议策略

趋势科技管理通信协议 (MCP) 是控制管理中心最新的通信主干部分。MCP 实施以下策略：

- **MCP 波动信号**：控制管理中心的 MCP 波动信号可确保控制管理中心显示最新信息，并确保被管理产品与控制管理中心服务器之间的连接正常。
- **MCP 命令轮询**：当 MCP 代理启动对控制管理中心的命令轮询时，控制管理中心将通知代理发送被管理产品日志或对被管理产品发出一个命令。控制管理中心还将命令轮询解释为被动的波动信号以验证控制管理中心和被管理产品之间的连接。

趋势科技管理基础架构策略

趋势科技管理基础架构 (TMI) 是控制管理中心的通信主干部分，生成其自身的“常规”流量。TMI 实施两种策略：

- **通信器波动信号**：通信器（TMI 的消息路由框架）按固定的时间间隔轮询控制管理中心服务器。这就确保控制管理中心控制台显示最新信息，并确保被管理产品与控制管理中心服务器之间的连接在起作用。
- **工作时间策略**：工作时间策略定义通信器何时向控制管理中心服务器发送信息。使用通信预设程序可定义此策略；用户可以设置三个非活动期（也称为“非工作”期）。但有两种信息不服从通信器预设程序：
  - 紧急消息
  - 被禁止消息

  即使通信器处于非工作期，TMI 也会向控制管理中心服务器发送紧急消息。但是，即使通信器处于活动状态，TMI 也绝不会向控制管理中心发送被禁止消息。

产品注册流量

产品概要文件为控制管理中心提供关于如何管理特定产品的信息。被管理产品第一次向服务器注册时把概要文件上传到控制管理中心服务器。

每个产品都有相应的产品概要文件，并且在许多情况下，不同版本的产品都有其自身版本的特定概要文件。概要文件包含以下信息：

- 类别（例如，防病毒）
- 产品名
- 产品版本
- 菜单版本
- 日志格式
- 更新组件信息 — 产品支持的更新（例如，病毒码文件）
- 命令信息

缺省情况下，控制管理中心服务器包含在被管理产品发布时提供的所有产品概要文件。但是，如果新版本的产品向控制管理中心注册，则该新产品将向控制管理中心服务器上传其产品概要文件。

策略部署

将策略设置部署到被管理产品和端点时，控制管理中心会生成网络流量。流量源自下列来源：

- 定期策略强制

  控制管理中心每 60 分钟会在被管理产品和端点上强制一次策略设置。

- 部署的信息

  策略包含每个端点的全局唯一标识号 (GUID) 信息和设置信息。一个包含 50,000 个目标和一整套设置的策略最多可生成 1.8 MB 网络流量。

部署更新

更新控制管理中心网络的过程分为两个步骤：

1. 从趋势科技获取最新的更新组件。

   控制管理中心可以直接从趋势科技更新服务器下载组件，也可以从一个备用位置下载组件。

2. 将这些组件部署到被管理产品。

   控制管理中心向被管理产品部署更新组件，包括：

   - 病毒码/特征码文件/清除模板
   - 引擎（扫描引擎、损害清除引擎）
   - 反垃圾邮件规则
   - 防毒墙网络版插件管理器插件程序
   - 产品程序（因产品而异）

提示

趋势科技极力建议定期更新这些组件，以确保被管理产品可以保护网络免受最新的威胁。关于产品程序更新，请参阅特定程序的文档。

将更新部署到被管理产品是一种极占用带宽的操作。如果有可能，执行对网络影响最小的部署是非常重要的。

您可以使用部署计划错开组件更新的部署时间。

而且，检查控制管理中心服务器与被管理产品之间的网络连接可以方便这些更新。该连接在决定网络需要多少个控制管理中心服务器时将是一个要考虑的因素。

数据存储计划

控制管理中心数据必须存储在 SQL 数据库中。在没有自身数据库的服务器上安装控制管理中心时，安装程序会提供安装 Microsoft SQL Express 的选项。但是，由于 SQL Express 的局限性，大型网络要求安装 SQL Server。

注意

控制管理中心使用 SQL 和 Windows 认证来访问 SQL Server。

数据库建议事项

如果在同一计算机上安装控制管理中心及其 SQL Server，请配置 SQL Server 使用相当于服务器上总内存三分之二的固定内存大小。例如，如果服务器有 3GB 内存，则将 SQL Server 的固定内存大小设置为 1GB。

在控制管理中心服务器本身或在一台独立服务器（例如，专用 SQL Server）上安装控制管理中心 SQL 数据库。

如果控制管理中心管理 1,000 多个产品，趋势科技建议使用专用 SQL Server。

注意

关于如何管理 SQL 资源的指导信息以及其他估量建议，请参考 Microsoft SQL 文档。

ODBC 驱动程序

控制管理中心使用 ODBC 驱动程序与 SQL Server 通信。对于大多数实例，ODBC 版本 3.7 就足够了。

如果在控制管理中心计算机上安装 SQL Server，控制管理中心安装程序可验证 ODBC 驱动程序的版本。对于远程 SQL Server，必须手动验证驱动程序以确保控制管理中心可访问数据库。

认证

控制管理中心使用混合模式认证（而不是 Windows 认证）访问 SQL 数据库。

Web 服务器计划

控制管理中心安装程序中的 Web 服务器信息窗口显示与主机标识定义窗口类似的服务器标识选项：主机名、FQDN 或 IP 地址。Web 服务器名称的决策注意事项是相同的：

- 如果使用主机名或 FQDN，则便于更改控制管理中心服务器 IP 地址，但会使系统依赖 DNS 服务器
- IP 地址选项需要有固定的 IP

使用 Web 服务器地址标识组件更新的来源。`SystemConfiguration.xml` 文件存储此信息，并将其作为通知的一部分发送给代理，让这些代理可从控制管理中心服务器获取更新。与更新源相关的设置如下显示：

```
Value=http://Web server address>:port>/TvcsDownload/
ActiveUpdate/component>
```

其中：

- **Port**：连接更新源的端口。您也可以在 Web 服务器地址窗口上指定此值（缺省端口号为 80）
- **TvcsDownload/ActiveUpdate**：控制管理中心安装程序在 IIS 指定的 Web 站点中创建这个虚拟目录
- **Component**：这取决于更新的组件。例如，更新病毒码文件时，此处添加的值为：

  `Pattern/vsapi.zip`

  `Pattern` 对应于控制管理中心服务器上的 `\\.. . Control Manager \WebUI\download\activeupdate\pattern` 文件夹。`Vsapi.zip` 是压缩形式的病毒码。

第 3 章

初次安装趋势科技防毒墙控制管理中心

本章将指导您安装控制管理中心服务器。本章还包含安装后的配置信息，以及有关如何注册和激活软件的说明。

本章包含以下主题：

系统要求

各个公司的网络都像公司本身一样是不同的。因此，不同网络的要求因复杂程度而异。本节描述了最低系统要求和建议系统要求，包括综合建议和基于网络规模而提出的建议。

有关全新安装要求的完整列表，请访问以下链接：

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

注意

控制管理中心 6.0 高级版支持将以下版本作为子级控制管理中心服务器：

- 控制管理中心 6.0 高级版
- 控制管理中心 5.5 高级版
- 控制管理中心 5.0 高级版

控制管理中心 5.0/5.5/6.0 标准版服务器不能作为子级服务器。

关于详细的代理系统要求，请参考被管理产品的文档。

安装必备组件

下表列出了您在启动控制管理中心的安装程序之前需要安装的组件。没有这些组件，安装程序无法继续。

表 3-1. 必备组件

平台	组件
Windows 2003 Server	• .Net Framework 3.5 SP1* • Microsoft 消息队列 • Windows Installer 4.5*

平台	组件
Windows 2008 Server	• IIS 6 管理兼容性组件 • IIS Windows 认证模块 • IIS ASP.NET • .Net Framework 3.5 SP1* • Microsoft 消息队列

仅当管理员想要在服务器上使用 SQL 2008 Express 时，才需要安装标记有星号 (*) 的组件。

关于安装控制管理中心服务器

决定要用于网络的拓扑之后，您可以开始安装控制管理中心服务器。请参阅服务器地址清单 第 A-2 页帮助您记录安装的相关信息。

为进行安装，您需要以下信息：

- 相关目标服务器地址和端口信息
- 控制管理中心注册码
- 要用于“服务器-代理”通信的安全级别

以下内容是与数据库有关的注意事项：

- 决定您是否要将 SQL Server 与控制管理中心配合使用。如果 SQL Server 不在控制管理中心服务器上，则获取其 IP 地址、FQDN 或 NetBIOS 名。如果有 SQL Server 的多个实例，则确定要使用的一个实例
- 准备要用于控制管理中心的以下 SQL 数据库有关信息：
  - 数据库的用户名
  - 密码

注意

控制管理中心同时使用 Windows 认证和 SQL 认证来访问 SQL Server。

- 确定控制管理中心将处理的被管理产品的数目。如果未在服务器上检测到 SQL Server，控制管理中心将安装 SQL Server 2008 Express，后者只可处理有限数量的连接。

控制管理中心安装流程

安装控制管理中心需要执行以下步骤：

1. 安装所需的所有组件
2. 指定安装位置
3. 注册并激活产品和服务
4. 指定控制管理中心安全设置和 Web 服务器设置
5. 指定备份设置
6. 配置通知设置
7. 配置数据库信息
8. 设置 root 帐户

提示

趋势科技建议升级到版本 6.0，而不是进行全新安装。

安装所有必备的组件

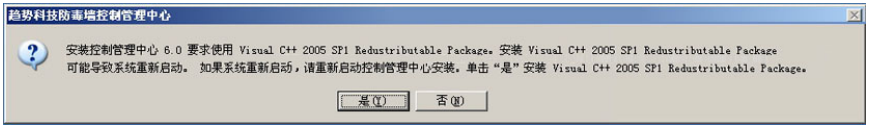
过程

1. 在 Windows 任务栏上，单击**开始** > **运行**，然后找到控制管理中心安装程序 (`Setup.exe`)。如果从趋势科技企业 DVD 安装，则转至 DVD 中的 Control

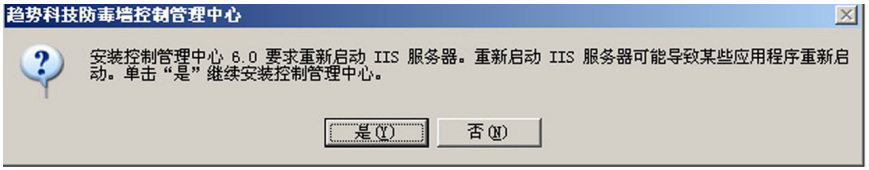
Manager 文件夹。如果您从趋势科技 Web 站点上下载了软件，则导航至计算机上的相关文件夹。安装程序检查您系统中的所需组件。如果安装程序没有在服务器上检测到以下组件，会出现对话框提示您安装缺少的组件：

- **Visual C++ 2005 SP1 Redistributable Package**：此组件包含在控制管理中心安装软件包中
- **PHP 5.3.5**：如果服务器使用早期的 PHP，那么在启动安装之前移除该早期版本。随后，控制管理中心会在安装期间安装 PHP 5.3.5。

2. 安装所有缺少的组件。显示确认对话框。



3. 单击**是**继续安装。将显示另一个确认对话框。



4. 单击**是**继续安装。

将显示**欢迎**窗口。

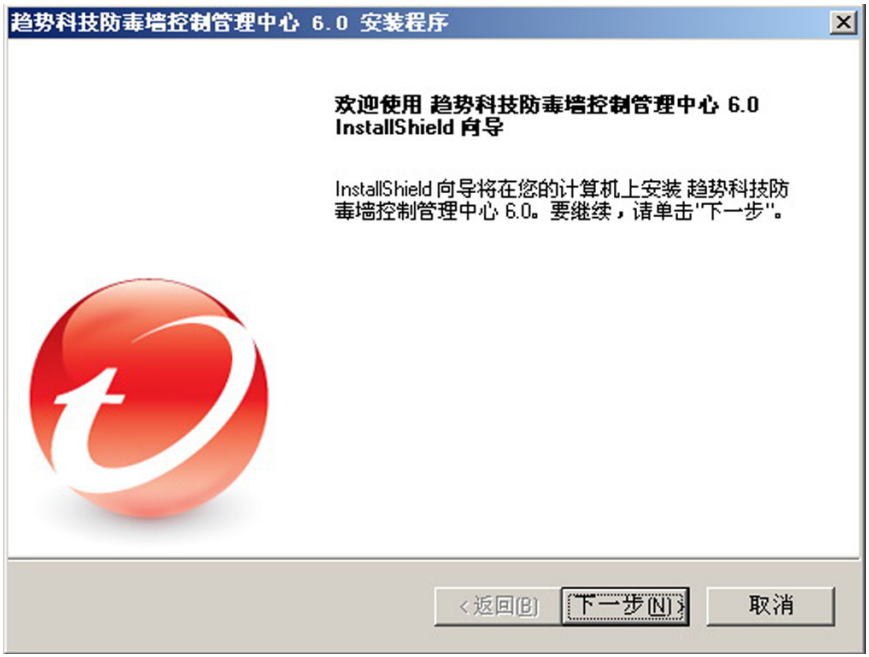


图 3-1. 欢迎窗口

安装程序检查您系统中的现有组件。关闭 Microsoft 管理控制台的所有实例，然后继续安装。有关迁移的更多信息，请参阅控制管理中心 2.x 代理的迁移方案 第 4-12 页。

5. 单击**下一步**。

将显示**软件许可协议**窗口。

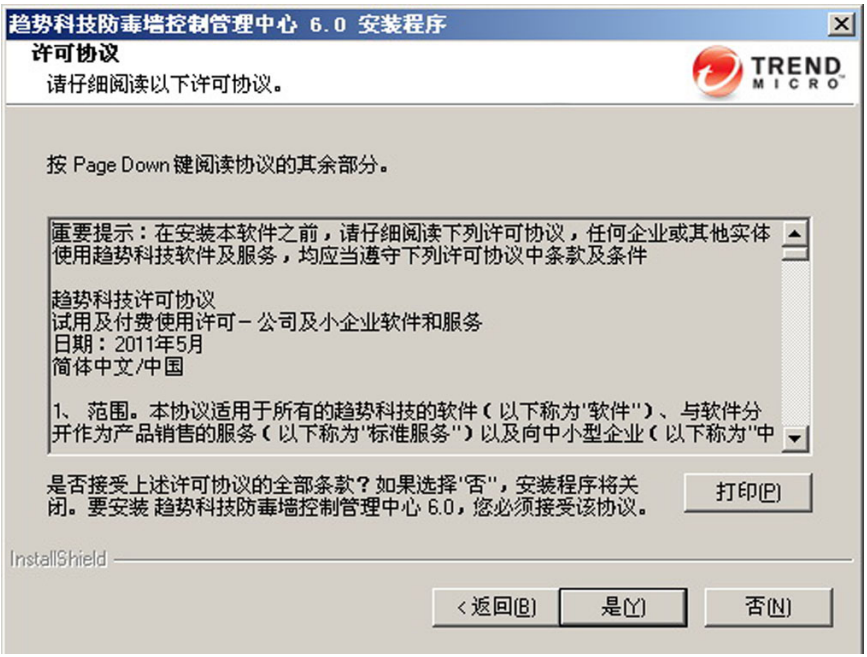


图 3-2. 同意许可协议

6. 如果不同意许可协议的条款，则单击**否**；安装随即停止。否则单击**是**。

7. （对于 Windows 2003，仅 64 位安装）将显示确认对话框。单击**是**将 Microsoft IIS 切换为 32 位模式。单击**否**停止安装。

8. 出现检测到的组件的摘要信息。

图 3-3. 显示本地系统环境信息

指定安装位置

过程

1. 单击**下一步**。

将显示**选择目标文件夹**窗口。

图 3-4. 选择目标文件夹

2. 指定控制管理中心文件的位置。缺省位置为 `C:\Program Files\Trend Micro`。要更改此位置，则单击**浏览**，然后指定一个替代位置。

注意

安装程序会在 `Program Files` 文件夹中预定的文件夹中安装与控制管理中心通信相关的文件（趋势科技管理基础架构和 MCP）。

注册和激活产品和服务

过程

1. 单击**下一步**。

   将显示**产品激活**窗口。

图 3-5. 提供激活码以激活控制管理中心和服务

2. 输入控制管理中心和任何其他已购买服务的激活代码（您还可从控制管理中心控制台激活可选的服务）。要使用控制管理中心的完整功能和其他服务（爆发阻止服务），需要获取激活码并激活该软件或这些服务。该软件中包含一个用于在趋势科技在线注册 Web 站点上在线注册软件并获取激活码的注册码。

3. 单击**下一步**。

将显示**趋势科技智能反馈**窗口。

图 3-6. 云安全智能防护网络设置

4. 选择**启用趋势科技智能反馈**即可参与云安全智能防护网络计划。选择参与后，控制管理中心将会向趋势科技云安全智能防护网络服务器发送匿名威胁信息。此举允许对网络进行前瞻性防护。您可以通过控制管理中心 Web 控制台随时停止参与。

指定控制管理中心安全设置和 Web 服务器设置

过程

1. 单击**下一步**。

将显示**选择安全级别和主机地址**窗口。

图 3-7. 选择一个安全级别

2. 从安全级别列表中，选择控制管理中心与代理进行通信的安全级别。这些选项如下：

   - **高**：控制管理中心与被管理产品之间的所有通信都使用 128 位加密以及认证。这确保在控制管理中心和被管理产品之间有最安全的通信。
   - **中**：控制管理中心与被管理产品之间的所有通信都使用 128 位加密（如果支持）。这是安装控制管理中心时的缺省设置。
   - **低**：控制管理中心与被管理产品之间的所有通信都使用 40 位加密。这是控制管理中心与其他产品之间通信的最不安全的通信方法。

3. 选择一个使代理可以与控制管理中心通信的主机地址：

   - FQDN/主机名

a. 选择**全限定域名 (FQDN) 或主机名**。

b. 在后面的文本框中选择或输入一个 FQDN 或主机名。

- IP 地址

a. 选择 **IP 地址**。

缺省情况下，IP 地址文本框显示 IPv4 地址。当用户在纯 IPv6 服务器上安装控制管理中心时，IP 地址文本框显示本地 IPv4 地址 (127.0.0.1)。

4. 单击**下一步**。

将显示**指定 Web 服务器信息**窗口。

指定 Web 服务器信息窗口中的设置定义了通信安全和控制管理中心网络识别您的服务器的方式。

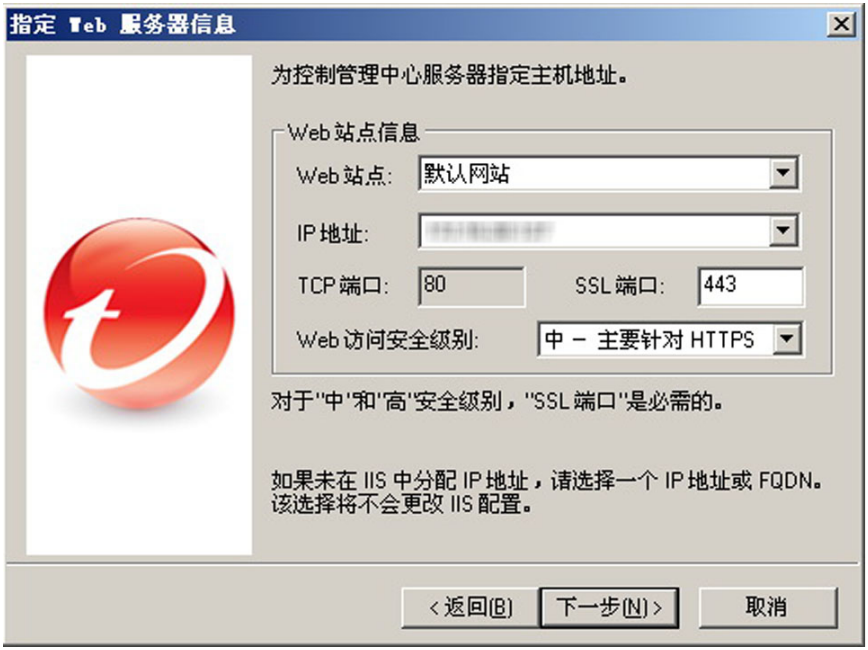


图 3-8. 指定 Web 服务器信息

5. 从 **Web 站点**列表中，选择用于访问控制管理中心的 Web 站点。

6. 从 IP 地址列表中选择您要用于控制管理中心管理控制台的 FQDN/主机名、IPv4 或 IPv6 地址。该项设置定义了控制管理中心的通信系统识别控制管理中心服务器的方式。安装程序尝试同时检测服务器的全限定域名 (FQDN) 和 IP 地址，并在相应的文本框中显示它们。

   如果您的服务器有多个网络接口卡，或如果您将多个 FQDN 分配给您的服务器，则在此处显示名称和 IP 地址。通过在列表中选择相应的选项或项来选择最适当的地址或名称。

   如果使用主机名或 FQDN 来标识您的服务器，则要确保该名称可在产品计算机上解析，否则这些产品无法与控制管理中心服务器通信。

7. 从 Web 访问安全性级别列表中，选择控制管理中心通信的安全级别。这些选项如下：

   - **高 - 仅 HTTPS**：所有的控制管理中心通信都使用 HTTPS 协议。这确保在控制管理中心和其他产品之间有最安全的通信。
   - **中 - HTTPS 为主**：如果支持 HTTPS，所有的控制管理中心通信都使用 HTTPS 协议。如果 HTTPS 不可用，代理将使用 HTTP。这是安装控制管理中心时的缺省设置。
   - **低 - 基于 HTTP**：所有的控制管理中心通信都使用 HTTP 协议。这是控制管理中心与其他产品之间通信的最不安全的通信方法。

8. 如果您选择**低 — 基于 HTTP**，并且尚未在 IIS 管理控制台中指定 SSL 端口值，请在 **SSL 端口**文本框中为控制管理中心通信指定访问端口。

指定备份设置

过程

1. 单击**下一步**。

将显示**选择目标位置**窗口。

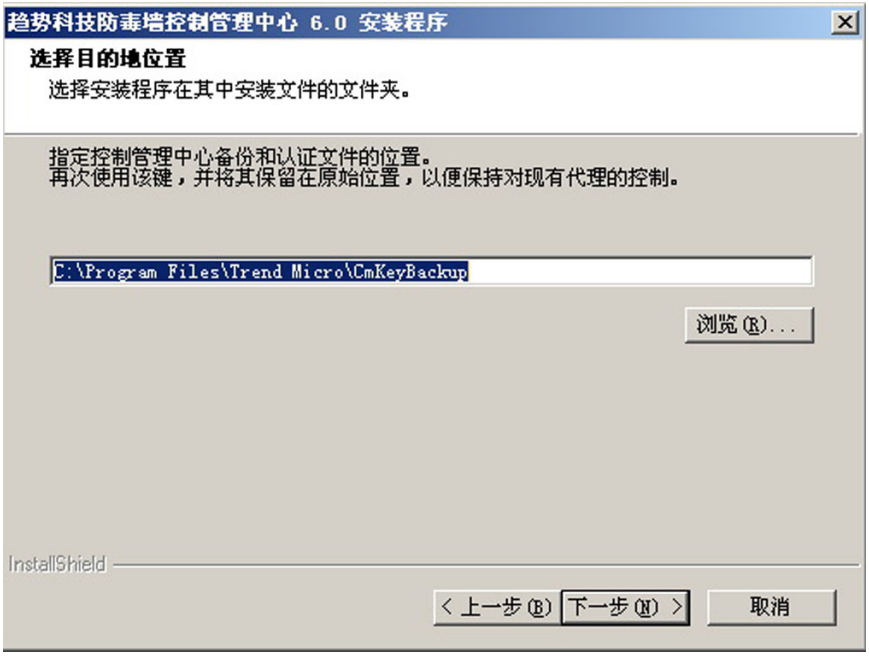


图 3-9. 为备份和认证文件选择一个目标位置

2. 指定控制管理中心备份和认证文件的位置（有关更多信息，请参阅第 4 章, 表 4-2：应备份的控制管理中心文件 第 4-6 页）。单击**浏览**指定一个替换位置。

配置通知设置

过程

1. 单击**下一步**。

将显示**指定消息路由路径**窗口。该窗口仅当主机服务器没有安装 TMI 时才会出现。

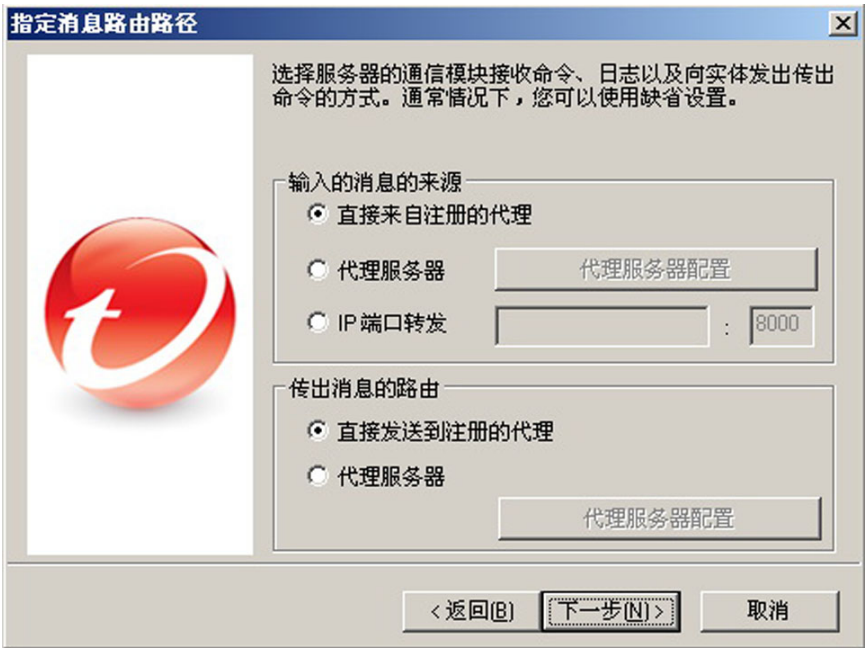


图 3-10. 定义消息或请求的路由

2. 定义传入和传出消息或请求的路由。这些设置允许您使控制管理中心适应您所在公司的现有安全系统。选择适当的路由。

注意

消息路由设置仅在安装过程中设置。此处所做的代理服务器配置与用于 Internet 连接的代理服务器设置无关 — 尽管缺省情况下使用的代理服务器设置相同。

- 输入的消息的来源
  - **直接从已注册的代理**：代理可直接接收传入的消息。

- **代理服务器**：在接收消息时使用代理服务器。
- **IP 端口转发**：此功能配置使得控制管理中心与您所在公司防火墙的 IP 端口转发功能配合工作。提供防火墙服务器的 FQDN、IP 地址或 NetBIOS 名称，然后键入控制管理中心为通信而打开的端口号。

- 传出消息的路由
  - **直接到已注册的代理**：控制管理中心将传出消息直接发送到代理。
  - **代理服务器**：控制管理中心通过代理服务器发送传出的消息。

配置数据库信息

过程

1. 单击**下一步**。

将显示**安装控制管理中心数据库**窗口。

图 3-11. 选择控制管理中心数据库

2. 选择用于控制管理中心的数据库。

   - **安装 Microsoft SQL Express：**如果此计算机上未安装 SQL Server，则安装程序自动选择此选项。不要忘记在提供的文本框中为此数据库指定一个密码。

     提示

     Microsoft SQL Server Express 只适合少量的连接。趋势科技建议对大型控制管理中心网络使用 SQL Server。

   - **SQL Server：**如果安装程序在服务器上检测到 SQL Server，则自动选择此选项。提供以下信息：

- **SQL 服务器 (\实例)**：该服务器将托管要用于控制管理中心的 SQL server。如果 SQL Server 存在于您的服务器上，则安装程序自动选择它。

  要指定一个备用服务器，请使用 FQDN、IPv4 地址或 NetBIOS 名称来标识它。

  如果在主机服务器上存在 SQL Server 的多个实例（这可以是您正在安装控制管理中心的同一服务器，或其他服务器），则您必须指定实例。例如：`your_sql_server.com\instance`

  注意

  如果用户选择使用远程 SQL server，则请勿在 SQL Server 文本框中指定 IPv6 地址。控制管理中心无法通过 IPv6 地址标识远程数据库。

- **SQL server 认证**：提供用于访问 SQL 服务器的凭证。缺省情况下，用户名为 sa。

  当使用 Windows 帐户连接到 SQL server 时，请使用下面的格式键入用户名：**域名\用户名**。

警告!

考虑到安全性，不要使用没有密码保护的 SQL 数据库。

3. 在**趋势科技防毒墙控制管理中心数据库**下，提供控制管理中心数据库的名称。缺省名称为 db_ControlManager。
4. 单击**下一步**创建必需的数据库。如果安装程序检测到现有的控制管理中心数据库，则您有以下选择：

   - **向现有数据库追加新的记录**：您安装的控制管理中心保持与以前服务器相同的设置、帐户和产品目录实体。此外，控制管理中心还保留以前安装的 root 帐户。您不能创建新的 root 帐户。

     注意

     如果安装的是控制管理中心 6.0，则无法为先前的控制管理中心数据库版本选择“向现有数据库追加新的记录”。

- **删除现有记录并创建新数据库**：删除现有数据库，创建另一个使用相同名称的数据库。
- **创建具有新名称的新数据库**：您将返回到上一个窗口，以允许更改控制管理中心数据库名称。

注意

如果将记录追加到当前数据库中，则无法更改 root 帐户。

设置 Root 帐户

过程

1. 单击**下一步**。

将显示**创建 Root 帐户**窗口。

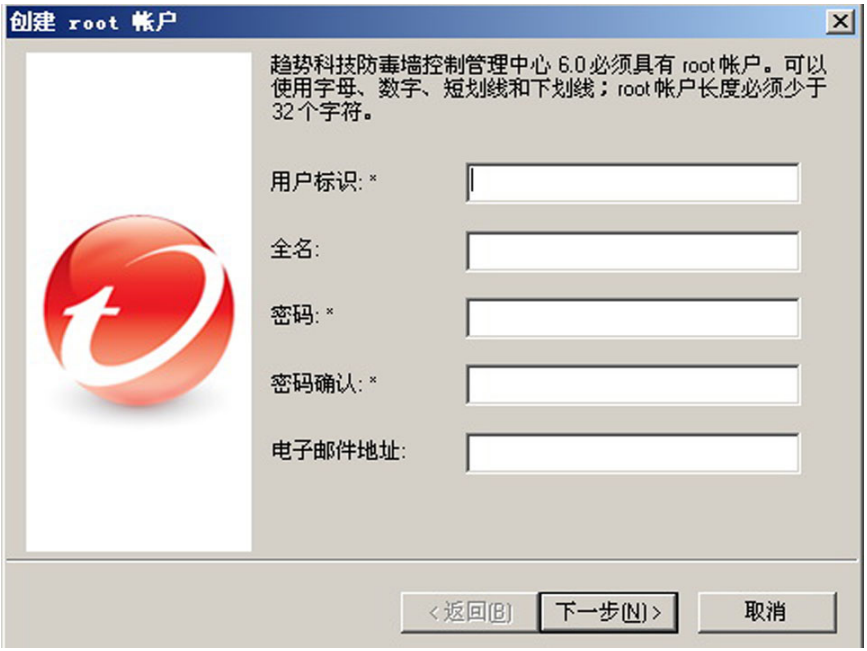


图 3-12. 提供控制管理中心 root 帐户的信息

2. 请提供以下必需帐户信息：
   - 用户标识
   - 全名
   - 密码
   - 密码确认
   - 电子邮件地址
3. 单击**下一步**。
4. 单击**完成**，完成安装。

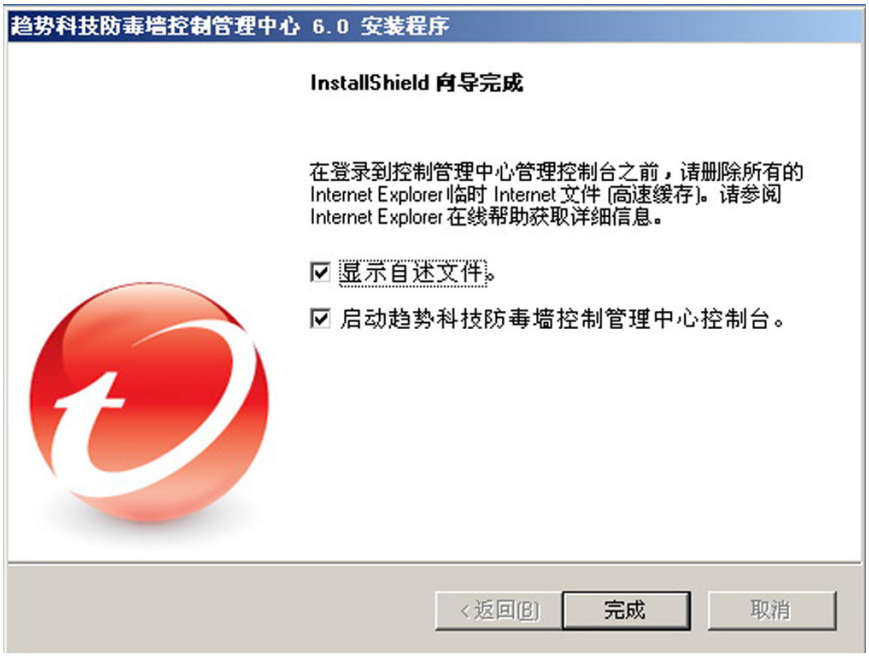


图 3-13. 安装完毕

验证控制管理中心服务器安装成功

要确认控制管理中心服务器已安装成功，请检查下表中的事项。

项	描述
控制面板 > **添加/删除程序**对话框	“添加/删除程序”中显示以下程序： • Trend Micro Common CGI • 趋势科技防毒墙控制管理中心 • Trend Micro Management Infrastructure • Microsoft Visual C++ 2005 Redistributable（最新版本） • PHP 5.3.5 • Crystal Report 2008 Runtime SP4 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 R2 Native Client • Microsoft SQL Server 2008 R2 安装程序 • Microsoft SQL Server 2008 安装支持文件 • Microsoft SQL Server 浏览器 • Microsoft SQL Server VSS 编写器 • FastCGI（仅在 Windows Server 2003 中显示）

项	描述
C:\Program Files	目录下显示以下文件夹： • Trend Micro\Common\TMI • Trend Micro\Common\CCGI • Trend Micro\Control Manager • PHP **注意** PHP 文件夹应在控制管理中心安装期间创建
控制管理中心数据库文件	• db_ControlManager.mdf • db_ControlManager_Log.LDF
安装程序创建以下服务和进程	
Control Manager Services	• Trend Micro Control Manager • Trend Micro Common CGI • Trend Micro Management Infrastructure • Trend Micro Network Time Protocol
CCGI 进程	• Jk_nt_service.exe • Java.exe
IIS 进程	Inetinfo.exe (Internet Information Services)
ISAPI 过滤器	• CCGIRedirect • ReverseProxy • TmcmRedirect

项	描述
TMI 进程	• CM.exe (TMI-CM) • MRF.exe（消息路由框架模块） • DMServer.exe（TMI-DM 完全功能）
控制管理中心进程	• ProcessManager.exe • LogReceiver.exe • MsgReceiver.exe • LogRetriever.exe • CmdProcessor.exe • UIProcessor.exe • ReportServer.exe • NTPD.exe（安全期间用户选择打开趋势科技 NTP 服务器时显示） • DCSProcessor.exe • CasProcessor.exe
消息队列进程	LogProcessor.exe

安装之后的配置

安装控制管理中心成功之后，趋势科技建议您执行以下安装后配置任务。

1. 注册并激活控制管理中心
2. 配置用户帐户和用户角色
3. 下载最新组件
4. 设置通知

注册并激活控制管理中心

成功安装控制管理中心之后，请在 Web 控制台上检查使用授权的状态和到期日期，方法是选择**管理** > **使用授权管理** > **控制管理中心**。如果该状态不是*已激活*或是已过期，则获取一个激活码并激活您的软件（在 Web 控制台上，选择**管理** > **使用授权管理** > **控制管理中心** > **指定新的激活码**）。如果您的激活码有问题，请联系技术支持。有关更多信息，请参阅注册和激活软件 第 3-27 页。

配置用户帐户

根据需要创建控制管理中心用户帐户。创建帐户时，请考虑以下事项：

- 不同用户角色（Administrator、Power User 和 Operator）的数目
- 将适当的许可和权限分配给每个用户角色
- 用户要利用层叠管理结构，则需要具有 Power User 或以上权限

下载最新组件

安装之后，从趋势科技 ActiveUpdate 服务器手动下载最新组件（病毒码文件\清除模板和引擎更新），以协助维持最高的安全防护。如果在趋势科技服务器和 Internet 之间存在代理服务器，请配置代理服务器设置（在 Web 控制台上，选择**管理** > **设置** > **代理服务器设置**）。

设置通知

安装之后，配置将触发通知的事件，以监控重大的病毒/恶意软件攻击和相关的安全活动。除了指定通知收件人之外，还要选择通知通道并进行测试以确保它们按照预期目标工作（在 Web 控制台上，选择**管理** > **事件中心**）。

注册和激活软件

激活控制管理中心服务器，可使安全和产品更新保持最新。要激活您的产品，请使用注册码在线注册并获取一个激活码。

如果您是第一次安装控制管理中心：

- 您已从趋势科技经销商处购买了完全版，注册码就包括在产品软件包中

  联机注册并获取一个激活码以激活该产品。

- 您在使用评估版

  从经销商处获取一个完全版注册码，然后按照完全版指导信息激活该产品。

关于激活控制管理中心

激活控制管理中心后，您可以使用产品的所有功能，包括下载更新的程序组件。您可以先从产品软件包或通过向趋势科技经销商购买获得激活码，然后激活控制管理中心。

注意

激活控制管理中心之后，注销并登录到控制管理中心 Web 控制台以使更改生效。

激活控制管理中心

过程

1. 导航到**管理** > **使用授权管理** > **控制管理中心**。

   将显示**使用授权信息**窗口。


使用授权信息

状态

控制管理中心的维护将于 2012-11-1 到期。
维护到期之前剩余 97 天。

爆发阻止服务的维护将于 2012-11-1 到期。
维护到期之前剩余 97 天。

控制管理中心使用授权信息	
产品:	控制管理中心（高级）
版本:	完全
状态:	已激活
激活码:	（指定新的激活码）
到期日期:	2012-11-1
检查状态	在线查看使用授权信息

爆发阻止服务使用授权信息	
产品:	爆发阻止服务
版本:	完全
状态:	已激活
激活码:	（指定新的激活码）

2. 单击**指定新的激活码**链接。
3. 在**新的**框中输入您的激活码。如果您没有激活码，则单击**在线注册**链接并按照在线注册 Web 站点上的指导信息获取一个激活码。
4. 单击**激活**，然后单击**确定**。

转换为完全版

激活控制管理中心以在评估期之后继续使用它。要使用包括下载更新的程序组件在内的控制管理中心的完整功能，请激活控制管理中心。

过程

1. 从趋势科技经销商处购买完全版注册码。

2. 在线注册软件。
3. 获取激活码。
4. 按照上述过程中的指导信息激活控制管理中心。

续订产品维护

请使用以下方法之一续订控制管理中心或其相关集成产品和服务（爆发阻止服务）的维护期。

要续订产品或服务的维护期，首先要获取更新的注册码。注册码使您可以获得新的激活码。续订产品维护期的过程根据您使用评估版还是完全版而变化。

使用“在线检查状态”续订产品维护

过程

1. 导航到**管理** > **使用授权管理** > **控制管理中心**。

   将显示**使用授权信息**窗口。
2. 在工作区中的**控制管理中心使用授权信息**下，单击**在线检查状态**，然后单击**确定**。
3. 注销然后再登录至 Web 控制台以使更改生效。

通过手动输入更新的激活码续订维护

过程

1. 导航到**管理** > **使用授权管理** > **控制管理中心**。

   将显示**使用授权信息**窗口。
2. 在工作区中的**控制管理中心使用授权信息**下，单击**激活产品**链接。

3. 单击**指定新的激活码**链接，并遵循在线注册 Web 站点上的指导信息。
4. 在**新的**框中输入您的激活码。
5. 单击**激活**。
6. 单击**确定**。

第 4 章

升级服务器或将代理迁移至控制管理中心

将现有的控制管理中心 5.0/5.5 服务器升级到控制管理中心 6.0 需要仔细考虑和详细规划。类似地，将 MCP 和较旧的控制管理中心代理迁移到控制管理中心 6.0 服务器时也同样如此。

本章包含以下主题：

升级到控制管理中心 6.0

下表列出了升级为标准版或高级版时的注意事项：

表 4-1. 升级到控制管理中心 6.0 时的注意事项

功能	标准版	高级版
保留报表功能	否	是
将标准版升级到高级版 要从标准版升级到高级版，请获取高级版激活码 (AC)，然后从**使用授权管理**窗口更改 AC。	是	N/A
将企业版/高级版转换为标准版	N/A	是

升级控制管理中心 5.0/5.5 服务器

趋势科技建议在先前安装的控制管理中心之上安装控制管理中心 6.0。这样做就可以使得以前的所有设置、日志、报表以及产品目录保持不变。不过，在升级之前，请验证安装控制管理中心的服务器是否有足够的系统资源。

支持的升级版本

控制管理中心支持从 IIS 缺省 Web 站点上安装的下列版本进行升级：

- 控制管理中心 5.5 SP1
- 控制管理中心 5.5
- 控制管理中心 5.0

警告!

请始终在执行升级之前备份现有服务器。

升级和迁移方案

控制管理中心支持三种升级和迁移方案：

方案 1：将控制管理中心 5.0/5.5 服务器升级为控制管理中心 6.0

如果是将控制管理中心 5.0/5.5 直接升级为控制管理中心 6.0，管理员可以选择备份控制管理中心或备份安装控制管理中心的服务器的整个操作系统。备份操作系统需要更大的工作量，但防止数据丢失的安全性更好。

通过备份先前的控制管理中心服务器和数据库来进行升级

过程

1. 备份现有控制管理中心 5.0/5.5 数据库。
2. 备份 `\Trend Micro\CmKeyBackup\*.*` 下的所有文件。
3. 备份当前控制管理中心 5.0/5.5 服务器的所有文件夹。
4. 备份当前控制管理中心 5.0/5.5 服务器的注册表。

注意

有关步骤 2 到步骤 4 的信息，请参阅表 4-2：应备份的控制管理中心文件 第 4-6 页。

5. 在控制管理中心 5.0/5.5 之上安装控制管理中心 6.0。

通过备份服务器的整个操作系统和控制管理中心数据库来进行升级

过程

1. 备份现有控制管理中心 5.0/5.5 服务器的操作系统。
2. 备份现有控制管理中心 5.0/5.5 数据库。
3. 在控制管理中心 5.0/5.5 之上安装控制管理中心 6.0。

升级流程

要将控制管理中心 5.0/5.5 升级到控制管理中心 6.0，请按安装所有必备的组件 第 3-4 页的步骤 1 所述运行安装程序 (`Setup.exe`)。按步骤升级控制管理中心。升级过程与全新安装非常类似，只有以下区别：

- 该安装程序会升级 Visual C++ 2005 SP1 Redistribution 软件包
- （仅限从控制管理中心 5.5 升级时）该安装程序会升级服务器的现有 PHP
- 该安装程序会将现有数据库迁移到控制管理中心 6.0。

方案 2：使用代理迁移工具迁移至全新安装的控制管理中心 6.0

此方案涉及在独立于现有控制管理中心服务器的服务器上安装控制管理中心 6.0。此方法使您可以慢慢地淘汰先前的服务器。有关迁移代理的详细信息，请参阅规划控制管理中心代理迁移 第 4-10 页。

将控制管理中心 5.0/5.5 服务器迁移到全新安装的控制管理中心 6.0

过程

1. 备份现有控制管理中心 5.0/5.5 数据库。
2. 在其他计算机上执行控制管理中心 6.0 的全新安装。
3. 使用代理迁移工具将实体从控制管理中心 5.0/5.5 服务器迁移到控制管理中心 6.0 服务器。

注意

代理迁移工具仅支持迁移被管理产品及其日志。代理迁移工具不支持从先前服务器迁移报表或产品目录结构。

方案 3：升级或迁移层叠环境

控制管理中心支持升级层叠环境。要升级层叠环境，请取消注册然后重新注册子级控制管理中心服务器。

过程

1. 取消所有子级控制管理中心在父级控制管理服务器上的注册。
2. 备份父级控制管理中心服务器。
3. 备份所有子级控制管理中心服务器。

4. 升级父级控制管理中心服务器。
5. 升级所有子级控制管理中心服务器。
6. 将所有子级控制管理中心服务器注册到父级控制管理中心服务器。

表 4-2. 应备份的控制管理中心文件

控制管理中心 5.0/5.5/6.0 信息	位置
数据库	使用 SQL 企业管理器或 osql 备份控制管理中心数据库。请参考控制管理中心的“使用 SQL 企业管理器/osql 备份 db_ControlManager”联机帮助主题，以获得详细的步骤。
认证信息 （确保如果控制管理中心恢复了，向控制管理中心服务器报告的被管理产品将向同一服务器报告）	`\Program Files\Trend Micro \CmKeyBackup\*.*`
GUID 信息	`\Program files\Trend Micro\COMMON \TMI\TMI.cfg` 中的 GUID 值
被管理产品信息	`\Program Files\Trend Micro\common \tmi\mrf_entity.dat` `\Program Files\Trend Micro\common \tmi\mrf_entity.bak`
ActiveUpdate 文件	`\Program Files\Trend Micro \Control Manager\webui\download \Activeupdate`

控制管理中心 5.0/5.5/6.0 信息	位置
控制管理中心注册表	**对于 32 位操作系统：** HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\ HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI\ HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM

控制管理中心 5.0/5.5/6.0 信息	位置
控制管理中心注册表	**对于 64 位操作系统：** HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TVCS HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TMI\ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\CommonCGI HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TMCM HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM
控制管理中心注册表	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQL$SQLEXPRESS

还原至控制管理中心 5.0/5.5 服务器

如果升级至控制管理中心 6.0 不成功，则执行以下步骤来还原至控制管理中心 5.0/5.5 系统。

方案 1：将控制管理中心 6.0 服务器还原至控制管理中心 5.0/5.5

使用以下方法之一还原控制管理中心 5.0/5.5 系统：

- 从控制管理中心服务器和数据库备份进行还原
- 从服务器的整个操作系统和控制管理中心数据库备份进行还原

从控制管理中心服务器和数据库备份进行还原

过程

1. 移除控制管理中心 6.0 服务器。
2. 安装控制管理中心 5.0/5.5 服务器。
3. 应用所需的控制管理中心 5.0/5.5 Service Pack 和 Hot Fix。

警告!

仅应用原始的控制管理中心 5.0/5.5 服务器已安装的 Service Pack 和 Hot Fix。

4. 使用备份的数据库恢复控制管理中心 5.0/5.5 数据库。
5. 使用备份的文件夹恢复所有控制管理中心 5.0/5.5 文件夹。
6. 使用备份的注册项恢复控制管理中心 5.0/5.5 注册项。
7. 恢复 `\Trend Micro\CmKeyBackup\*.*` 下的所有文件。

8. 导入旧证书。

从服务器的整个操作系统和控制管理中心数据库备份进行还原

过程

1. 使用备份的数据库恢复控制管理中心 5.0/5.5 数据库。
2. 使用备份的操作系统恢复服务器的操作系统。

方案 2：还原层叠环境

过程

1. 取消所有子级控制管理中心在父级控制管理服务器上的注册。
2. 还原父级控制管理中心服务器。
3. 还原所有的子级控制管理中心服务器。
4. 应用控制管理中心的 Service Pack 和 Hot Fix。
5. 将所有子级控制管理中心服务器注册到父级控制管理中心服务器。

规划控制管理中心代理迁移

将代理迁移至控制管理中心 6.0 服务器的方法有两种：

- 快速升级
- 分阶段升级

快速升级

快速升级使用下表中显示的方式运行。

表 4-3. 快速升级

原始服务器/代理	处理措施
控制管理中心 5.0/5.5 与 MCP 代理	将 MCP 代理注册到控制管理中心 6.0 服务器，然后重新组织产品目录结构
控制管理中心 5.0/5.5 与混合代理	将 MCP 代理注册到控制管理中心 6.0 服务器，然后重新组织产品目录结构

趋势科技建议在实验室环境中或在较小的网络中（测试部署期间尤佳）使用快速升级来迁移代理（请参阅在一个位置测试控制管理中心 第 2-10 页）。但由于在迁移启动之后无法停止，此方法最适合小型部署。难度会随着网络规模的扩大而增加。

分阶段升级

趋势科技建议对大型的单服务器控制管理中心 5.0/5.5 网络进行分阶段升级。对于多服务器网络，这种方法是必需的。此方法提供一种更结构化的系统迁移方法，并遵循以下准则：

- 在对现有网络影响最小的系统上开始迁移，然后再继续迁移影响较大的系统
- 按合理规划的多个阶段来升级旧网络，而不是一下子全部升级

  如果需要排除故障，这种方式可以简化排除故障的过程。

分阶段升级涉及以下步骤：

1. 在没有安装过控制管理中心以前的任何版本的服务器（没有任何被管理产品尤佳）上安装控制管理中心 6.0。
2. 在控制管理中心 6.0 服务器上运行 `AgentMigrateTool.exe` 工具

将控制管理中心代理安装与代理迁移工具配合使用，以规划在现有控制管理中心网络上的代理升级。代理迁移工具可以生成装有控制管理中心代理的服务器的列表。这样就不必再手动选择代理服务器了。

控制管理中心 2.x 代理的迁移方案

以下是代理迁移的可能情况：

- 单服务器迁移
- 不同服务器/代理的合并

单服务器迁移

图 4-1. 迁移属于单个服务器的代理

在这种情况下，快速迁移和分阶段迁移都可以使用。请参阅升级和迁移方案 第 4-3 页。

不同服务器/代理的合并

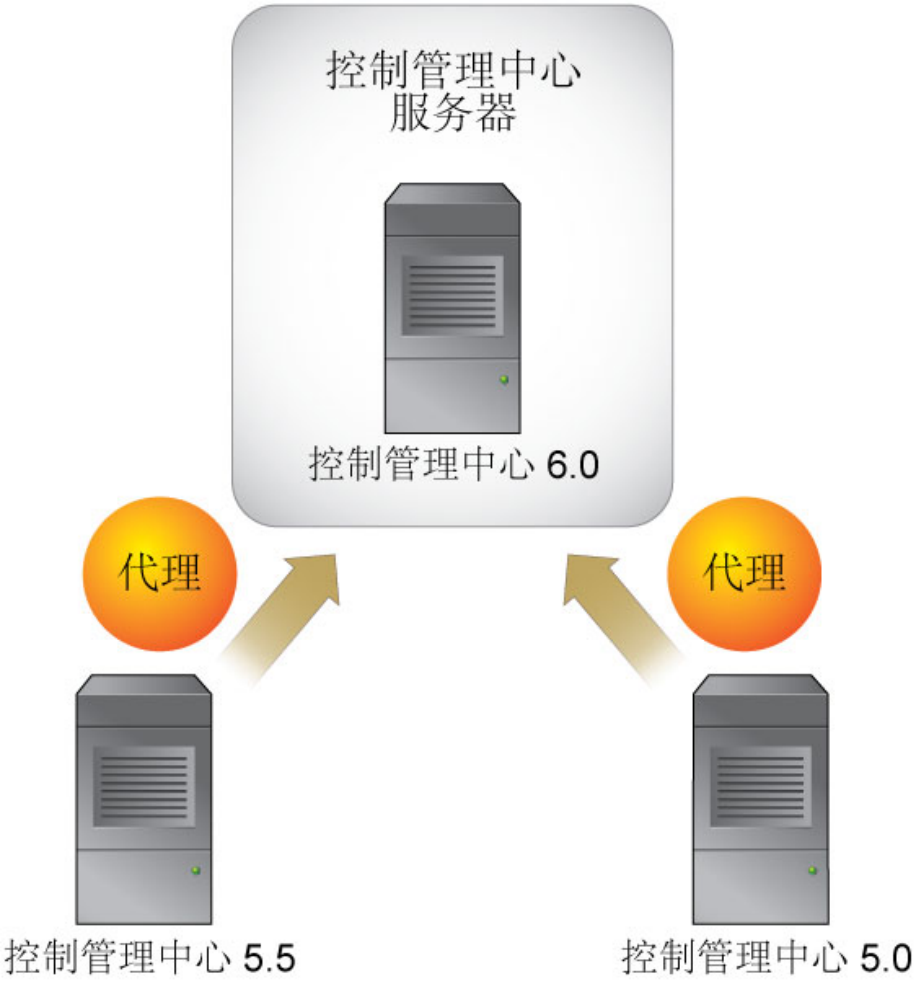


图 4-2. 迁移属于多个服务器的代理

由于新的控制管理中心访问控制功能，先前由各自的控制管理中心服务器处理的功能（将用户访问限制在防病毒网络的特定网段）现在可以合并到一台控制管理中心服务器。

控制管理中心 2.5x 代理迁移流程

在控制管理中心 2.5x 代理迁移期间，代理迁移工具执行以下操作：

1. 停止趋势科技管理基础架构服务
2. 从控制管理中心 5.0/5.5 服务器获取产品目录信息
3. 从控制管理中心 5.0/5.5 数据库和 `TMI.cfg` 中删除代理信息
4. 保留控制管理中心 2.5x 代理版本（不进行升级）
5. 将代理信息写入控制管理中心 6.0 数据库和 `TMI.cfg`
6. 重新启动趋势科技管理基础架构服务

如果 `AgentMigrationTool.exe` 无法完成控制管理中心 2.5x 代理迁移，它会从控制管理中心 6.0 数据库和 `TMI.cfg` 中移除代理信息，然后将信息写回控制管理中心 5.0/5.5 数据库中。

MCP 代理迁移流程

在 MCP 迁移期间，代理迁移工具执行以下操作：

1. 停止目标服务器的趋势科技管理基础架构服务。
2. 从控制管理中心服务器获取产品目录信息。
3. 保留控制管理中心代理版本（不进行升级）。
4. 将代理信息写至目标服务器的数据库中。
5. 重新启动目标服务器的趋势科技管理基础架构服务。
6. 停止然后重新启动目标服务器的趋势科技防毒墙控制管理中心服务。

7. 请求源服务器发出一个 Change Server 的命令，并且等待 MCP 代理的轮询。

迁移控制管理中心 2.5x 代理和 MCP 代理

使用 `AgentMigrateTool.exe` 来迁移原来由控制管理中心 5.0/5.5 服务器管理的基于 Windows 的代理。当迁移代理时，首先迁移 2.5x 代理，然后是 MCP 代理。

如果代理迁移不成功，将会发生以下的事情：

- 代理继续由源服务器管理
- 代理日志同时位于源服务器和目标服务器上

迁移的日志只有在代理注册到目标服务器后才显示。当触发清除时，目标控制管理中心服务器将会清除迁移的日志。

注意

在目标服务器（您会将这些代理迁移到的控制管理中心 6.0 服务器）中直接运行 `AgentMigrateTool.exe`。

过程

1. 使用 Windows 资源管理器，打开控制管理中心 6.0 root 目录。例如：
   `<root>\Program Files\Trend Micro\Control Manager\`
2. 双击 `AgentMigrateTool.exe`。

   注意

   记住启动目标控制管理中心服务器的远程注册服务，否则代理迁移将不能成功。
3. 单击主菜单上的**配置来源服务器设置**。
4. 在**源服务器**下的“配置”窗口中，键入托管要迁移代理的来源服务器的 **IP 地址**。

5. 在**系统管理员帐户**下，指定将用于访问来源服务器的管理员**用户名**和**密码**，然后单击**连接**。

6. 在主窗口上，单击**添加 >** 或**全部添加 >>** 将代理从**来源**迁移到**目标**列表。

7. 选择以下的所有选项或其中一个选项：

   - **保留树型结构**：`AgentMigrateTool.exe` 指示目标服务器（控制管理中心 6.0 服务器）保留选定的被管理产品的原产品目录结构
   - **迁移日志**：`AgentMigrateTool.exe` 将选定的被管理产品的日志从源服务器复制到目标服务器
   - **启用 HTTPS**：`AgentMigrateTool.exe` 通知迁移代理使用 HTTPS 注册到控制管理中心。如果不选择此选项，代理会使用 HTTP 注册到控制管理中心

     这些选项适用于“目标”列表中列出的代理。

   注意

   趋势科技建议从来源服务器迁移所有代理时启用**保留树结构**和**迁移日志**选项。

8. 单击**迁移**。`AgentMigrateTool.exe` 会迁移“目标”列表中列出的代理。

迁移控制管理中心数据库

迁移控制管理中心 5.0/5.5 数据库的方式有两种：

- 在控制管理中心 5.0/5.5 服务器之上安装控制管理中心 6.0。这是建议的方法。

  控制管理中心 6.0 安装程序会自动将数据库升级到版本 6.0。

- 将控制管理中心 5.0/5.5 数据库手动传送到控制管理中心 6.0 服务器。

将控制管理中心 SQL 2005 数据库迁移到其他 SQL Server 2005

修改 TMI.cfg 中的一些参数，可将控制管理中心数据库从一个 SQL Server 2005 服务器移到另一个 SQL Server 2005 服务器。

过程

1. 使用 Windows 服务，停止以下控制管理中心服务：
   - Trend Micro Management Infrastructure
   - Trend Micro Common CCGI
   - Trend Micro Control Manager
2. 将控制管理中心数据库从旧的 SQL Server 2005 服务器复制到新的 SQL Server 2005 服务器。

   注意

   控制管理中心加密用户名和密码的值。趋势科技建议使用用于访问 db_ControlManager 的同一认证帐户配置目标 SQL server，并保留同一标识和密码组合。

3. 使用文本编辑器打开 `<root>\Program Files\Trend Micro\COMMON\TMI\TMI.cfg`。

   注意

   备份 TMI.cfg 以还原为原设置。

4. 用目标 SQL server 的名称替换 `CFG_DM_DB_DSN=DSN=ControlManager_DataBase` 参数值。
5. 保留旧的标识和密码，或者更新以下参数的值：

   `CFG_DM_DB_ID`

   `CFG_DM_DB_PWD`

6. 保存并关闭 `TMI.cfg`。
7. 单击**开始** > **程序** > **管理工具** > **数据源 (ODBC)** 来打开 ODBC 数据源管理器。
8. 激活**系统 DSN** 选项卡，然后配置 **ControlManager_DataBase** 数据源。
9. 在 Microsoft SQL Server DSN 配置中，选择**目标服务器**以修改**您要连接哪个 SQL Server?** 的值，然后单击**下一步**。如果列表中没有该目标服务器，则输入**服务器名称**。
10. 在下一个窗口中，选择**使用由用户输入的登录标识和密码的 SQL Server 认证**和**连接到 SQL Server 来获取其他配置的缺省设置**选项。
11. 输入 `TMI.cfg` 中提供的同一**标识**和**密码**，然后单击**下一步**。
12. 单击**完成**保存新的配置，并关闭 Microsoft SQL Server DSN 配置。
13. 单击**确定**来关闭 ODBC 数据源管理器。
14. 使用 Windows 服务，重新启动所有控制管理中心服务。
15. 登录到 Web 控制台并访问产品目录，检查是否所有被管理产品均已注册。如果都已注册，那么您已经成功地将数据库移到目标 SQL Server 上。

第 5 章

删除趋势科技防毒墙控制管理中心

本章包含关于如何从网络中删除控制管理中心代理组件（包括控制管理中心服务器、控制管理中心代理和其他相关文件）的信息。

本章包含以下小节：

删除控制管理中心服务器

有两种方法来自动删除控制管理中心（以下指导信息适用于 Windows 2003 环境，细节之处会有所不同，这要取决于您使用的 Microsoft Windows 平台）：

过程

- 从“开始”菜单中，单击**开始** > **程序** > **趋势科技防毒墙控制管理中心** > **卸载趋势科技控制管理中心**。
- 使用“添加/删除程序”：
  a. 单击**开始** > **设置** > **控制面板** > **添加/删除程序**。
  b. 选择**趋势科技防毒墙控制管理中心**，然后单击**删除**。该操作将自动移除其他相关服务，例如趋势科技管理基础架构和通用 CGI 服务，以及控制管理中心数据库。
  c. 单击**是**保留数据库，或单击**否**将数据库删除。

  注意
  保留数据库使您可以在服务器上重新安装控制管理中心，并保留所有系统信息，如代理注册和用户帐户数据。

  如果您重新安装了控制管理中心服务器，并删除了原始数据库，而未删除原本向先前安装的控制管理中心服务器报告的代理，这些代理将在以下情况下重新注册到服务器：
  - 被管理产品服务器重新启动代理服务
  - 控制管理中心代理在 8 小时时间过后验证它们的连接

手动删除控制管理中心

本节描述如何手动删除控制管理中心。仅在 Windows 的“添加/删除”功能或控制管理中心卸载程序不成功时，才使用下面的步骤。

注意

特定于 Windows 的指导信息可能会因操作系统版本的不同而异。以下步骤是针对 **Windows Server 2003** 编写的。

删除控制管理中心实际上包括删除几个不同的组件。这些组件可按任意顺序删除，甚至可以一起删除。但为了明确起见，每个模块的卸载都分别在各自的章节中讨论。这些组件有：

- 控制管理中心应用程序
- Trend Micro Management Infrastructure
- Common CGI Modules
- Control Manager Database（可选）
- PHP
- FastCGI

其他趋势科技产品也使用趋势科技管理基础架构和通用 CGI 模块，所以如果您在同一计算机上装有其他趋势科技产品，趋势科技建议不删除这两个组件。

注意

删除所有组件后，必须重新启动服务器。只有在完成移除后才必须执行一次该操作。

移除控制管理中心应用程序

手动删除控制管理中心的应用程序包括以下步骤：

1. 停止控制管理中心服务 第 5-4 页
2. 删除控制管理中心 IIS 设置 第 5-5 页
3. 删除 Crystal Report、PHP、FastCGI、TMI 和 CCGI 第 5-6 页
4. 删除控制管理中心文件/目录和注册表键 第 5-7 页

5. 移除数据库组件 第 5-8 页
6. 删除控制管理中心和 NTP 服务 第 5-10 页

停止控制管理中心服务

使用 Windows“服务”窗口可停止以下所有控制管理中心服务：

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager
- Trend Micro NTP

注意

这些服务运行在 Windows 操作系统后台，不是需要激活码的趋势科技服务（例如，爆发阻止服务）。

从 Windows“服务”窗口停止控制管理中心服务

过程

1. 单击**开始** > **程序** > **管理工具** > **服务**，打开**服务**窗口。
2. 右键单击 **<Control Manager service>**，然后单击**停止**。

从命令提示符处停止 IIS 和控制管理中心服务

过程

- 在命令提示符下运行以下命令：

```
net stop w3svc
```

```
net stop tmcm
```

删除控制管理中心 IIS 设置

在停止控制管理中心服务后删除 Internet Information Services 设置。

过程

1. 从控制管理中心服务器，单击**开始** > **运行**。

   将显示**运行**对话框。

2. 在**打开**文本框中键入以下内容：

   ```
   %SystemRoot%\System32\Inetsrv\iis.msc
   ```

3. 在左侧菜单中，双击服务器名称来展开控制台树。

4. 双击**缺省 Web 站点**。

5. 删除以下虚拟目录：

   - ControlManager
   - TVCSDownload
   - crystalreportviewers12
   - TVCS
   - Jakarta
   - WebApp

6. 仅在 IIS 6 上：

   a. 右键单击您在安装期间设置的 IIS Web 站点。

   b. 单击**属性**。

7. 选择 **ISAPI 过滤器**选项卡。

8. 删除以下 ISAPI 过滤器：
   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy
9. 仅在 IIS 6 上，删除以下 Web 服务扩展：
   - Trend Micro Common CGI Redirect Filter（如果删除 CCGI）
   - 趋势科技防毒墙控制管理中心 CGI 扩展

删除 Crystal Report、PHP、FastCGI、TMI 和 CCGI

可选择删除 PHP、FastCGI、TMI 和 CCGI。使用“添加/删除程序”卸载 Crystal Report、PHP 和 FastCGI。

删除 Crystal Report

过程

1. 在控制管理中心服务器上，单击**开始** > **设置** > **控制面板** > **添加/删除程序**。
2. 向下滚动至 Crystal Report 运行时文件，然后单击**删除**以自动移除 Crystal Report 相关文件。

删除 PHP 和 FastCGI

过程

1. 在控制管理中心服务器上，单击**开始** > **设置** > **控制面板** > **添加/删除程序**。
2. 向下滚动至 PHP，然后单击**删除**以自动删除 PHP 相关文件。

3. 向下滚动至 FastCGI，然后单击**删除**以自动删除 FastCGI 相关文件。

删除 TMI 和 CCGI

过程

1. 将 Microsoft 服务工具 `Sc.exe` 下载到控制管理中心服务器：

   http://support.microsoft.com/kb/251192/zh-cn

2. 运行 `Sc.exe` 并输入以下命令：

   ```
   sc delete "TrendCGI"
   ```

   ```
   sc delete "TrendMicro Infrastructure"
   ```

删除控制管理中心文件/目录和注册表键

过程

1. 删除以下目录：

   - `.Trend Micro\Control Manager`
   - `.Trend Micro\COMMON\ccgi`
   - `.Trend Micro\COMMON\TMI`
   - `.PHP`
   - `C:\Documents and Settings\All Users\Start Menu\Programs\PHP 5`
   - `C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro Control Manager`

2. 删除以下控制管理中心注册表键：

   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI`

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DamageCleanupService
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPPTrustPort
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\VulnerabilityAssessmentServices
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP

移除数据库组件

本节介绍如何从控制管理中心服务器移除以下数据库组件：

- 移除控制管理中心 ODBC 设置
- 移除控制管理中心 SQL Server 2008 Express 数据库

移除控制管理中心 ODBC 设置

过程

1. 在控制管理中心服务器上，单击**开始** > **运行**。

   将显示**运行**对话框。

2. 在“打开”文本框中键入以下内容：

   ```
   odbcad32.exe
   ```

3. 在 **ODBC 数据源管理器**窗口上，单击**系统 DSN** 选项卡。

4. 在**名称**下，选择 **ControlManager_Database**。

5. 单击**删除**，并单击**是**确认。

移除控制管理中心 SQL Server 2008 Express 数据库

过程

1. 在控制管理中心服务器上，单击**开始** > **控制面板** > **添加/删除程序**。

2. 向下滚动至 **SQL Server 2008 Express**，然后单击**删除**自动移除相关文件。

提示

如有任何卸载问题，趋势科技建议访问 Microsoft Web 站点获取有关移除 SQL Server 2008 Express 的说明：

http://support.microsoft.com/kb/909967

删除控制管理中心和 NTP 服务

过程

1. 将 Microsoft 服务工具 `Sc.exe` 下载到控制管理中心服务器：http://support.microsoft.com/kb/251192/zh-cn
2. 运行 `Sc.exe` 并输入以下命令：

```
sc delete "TMCM"

sc delete "TrendMicro_NTP"
```

删除基于 Windows 的控制管理中心 2.x 代理

要删除一个或多个代理，必须运行控制管理中心代理安装程序的卸载组件。

要远程卸载代理，可从控制管理中心服务器或其他服务器运行程序，要本地卸载代理，可在代理计算机上运行设置程序。

过程

1. 导航至**管理** > **设置** > **产品代理设置**。

   将显示**产品代理设置**窗口。
2. 单击 **RemoteInstall.exe** 链接下载应用程序。
3. 使用 Microsoft 资源管理器，转至您保存代理安装程序的位置。
4. 双击 `RemoteInstall.exe` 文件。

将显示**趋势科技防毒墙控制管理中心代理安装程序**窗口。

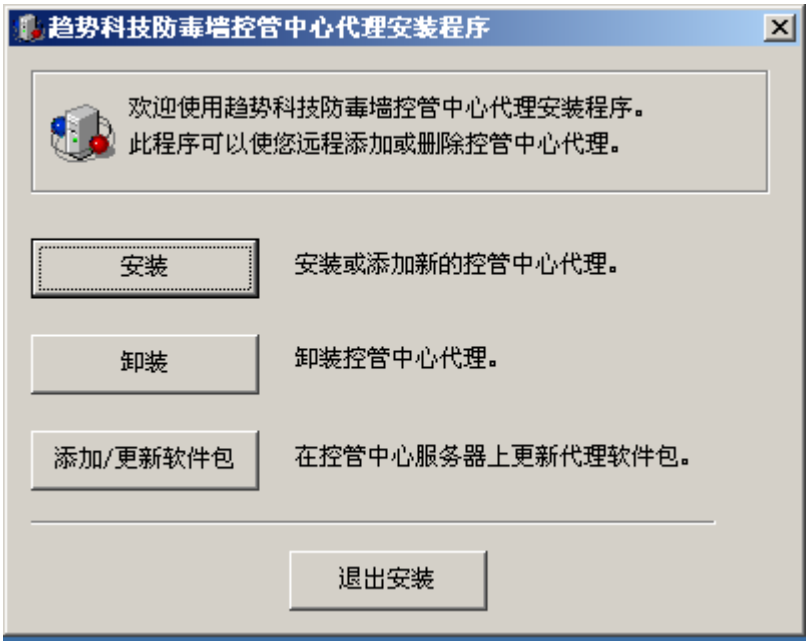


图 5-1. 趋势科技防毒墙控制管理中心代理安装程序

5. 单击**卸载**。

   将显示**欢迎**窗口。

6. 单击**下一步**。

将显示**控制管理中心来源服务器登录**窗口。

图 5-2. 控制管理中心来源服务器登录

7. 指定并提供控制管理中心服务器的管理员级登录凭证。输入以下信息：
   - 主机名
   - 用户名
   - 密码
8. 单击**下一步**。选择要从中删除代理的产品。
9. 单击**下一步**。选择要从中删除代理的服务器。有两种方法来选择那些服务器：
   - 从列表中选择：

   a. 在左侧的列表框中，双击防病毒服务器所处的域，该域将展开以显示其中所有的服务器。

b. 从左侧的列表框中选择目标服务器，然后单击**添加**。选择的服务器出现在右侧的列表框中。单击**全部添加**，将代理添加到选定域中的所有服务器上。或者，您也可以双击某个服务器将其添加到左侧列表中。

- 直接指定服务器名称：

a. 在**服务器名称**文本框中输入服务器的 FQDN 或 IP 地址。

b. 单击**添加**。该服务器出现在右侧的列表框中。要从列表中删除服务器，则从右侧列表框中选择一个服务器，然后单击**删除**。要删除所有服务器，请单击**全部删除**。

10. 单击**上一步**返回到前一窗口，单击**退出**中止操作，或单击**下一步**继续操作。

11. 为选定的服务器提供管理员级登录凭证。在相应的文本框中输入所需的用户名和密码。

12. 单击**确定**。**分析选择的服务器**窗口提供有关目标服务器的以下详细信息：服务器名称、域和检测到的代理类型。

13. 单击**下一步**继续。此窗口上的表格显示有关目标服务器的以下信息：服务器名称、操作系统版本、IP 地址、域名和要移除代理的版本。单击**上一步**返回至前一窗口，单击**退出**中止操作，或单击**卸载**删除代理。卸载开始。

14. 单击**确定**，然后在**删除代理**窗口中单击**退出**。

第 6 章

获取支持

趋势科技致力于提供超出用户预期的服务和支持。本章包含关于如何获取技术支持的信息。记住，您必须注册产品才有资格获取支持。

本章包含以下主题：

联系技术支持之前

在联系技术支持之前，您可以快速通过两项操作尝试找到问题的解决方法：

- **查看文档**：手册和联机帮助提供关于控制管理中心的全面信息。查找这两种文档以确定是否包含所需要的解决方案。
- **访问技术支持 Web 站点**：我们的技术支持 Web 站点包含有关所有趋势科技产品的最新信息。技术支持 Web 站点具有以前用户所提问题的答案。

  要搜索知识库，请访问

  http://cn.trendmicro.com/cn/support/techsupport/index.html

联系技术支持

趋势科技向所有已注册用户（必须在购买续订维护后）提供一年的技术支持、病毒码下载和程序更新。如果您需要帮助或只是有疑问，请随时联系我们。我们也欢迎您提出意见。

- 请登录 http://cn.trendmicro.com/cn/support/techsupport/index.html 获取全球技术支持办事处的列表
- 请登录 http://docs.trendmicro.com/zh-cn/home.aspx 获取最新趋势科技产品文档

在中国，您可以通过电话、传真或电子邮件与趋势科技销售代表取得联系。

上海市淮海中路 398 号世纪巴士大厦 8 楼，
趋势科技（中国）有限公司
免费咨询电话：800-820-8876(021-63848622)
技术支持热线：800-820-8839(021-6100-6656)
传真：86-21-6384 1899
网址：http:// www.trendmicro.com.cn
电子邮件：service@trendmicro.com.cn

加快解决问题的速度

为了加快解决问题的速度，当您联系我们的员工时，请尽可能多地提供以下信息：

- 产品序列号
- 控制管理中心 Build 版本
- 操作系统版本、Internet 连接类型和数据库版本（例如，SQL 2005 或 SQL 2008）
- 错误消息原文（如果有）
- 重现该问题的步骤

TrendLabs

趋势科技 TrendLabsSM 是一个全球性的防毒研究和产品支持中心网络，向全世界的趋势科技客户提供不间断的全天候服务。

全球 TrendLabs 专用服务中心拥有超过 250 名工程师和资深支持人员组成的团队，确保可快速响应世界上任何地方爆发的任何病毒或紧急客户支持问题。

TrendLabs 现代化总部的质量管理体系在 2000 年通过了 ISO 9002 认证。TrendLabs 是世界上首家获得该认证的防病毒研究和技术支持公司之一。趋势科技相信，TrendLabs 是防病毒业界领先的服务和技术支持团队。

关于 TrendLabs 的更多信息，请访问：

http://cn.trendmicro.com/cn/about/company/trendlabs/index.html

其他有用资源

趋势科技通过其 Web 站点 http:// www.trendmicro.com.cn 提供大量服务。

基于 Internet 的工具和服务包括：

- **趋势科技™云安全智能防护网络™**：监控全球范围内的安全威胁事件
- **HouseCall™**：趋势科技联机病毒扫描程序

附录 A

控制管理中心系统清单

使用本附录中的清单来记录相关系统信息作为参考。

本附录包含以下小节：

服务器地址清单

在安装期间以及配置控制管理中心服务器以用于您的网络期间，必须提供以下服务器地址信息。在此处记录信息以便于参考。

表 A-1. 服务器地址清单

所需信息	样本	您的值
控制管理中心服务器信息		
IP 地址	10.1.104.255	
全限定域名 (FQDN)	server.company.com	
NetBIOS（主机）名称	yourserver	
Web 服务器信息		
IP 地址	10.1.104.225	
全限定域名 (FQDN)	server.company.com	
NetBIOS（主机）名称	yourserver	
基于 SQL 的控制管理中心数据库信息		
IP 地址	10.1.104.225	
全限定域名 (FQDN)	server.company.com	
NetBIOS（主机）名称	sqlserver	
用于组件下载的代理服务器		
IP 地址	10.1.174.225	
全限定域名 (FQDN)	proxy.company.com	
NetBIOS（主机）名称	proxyserver	
SMTP 服务器信息（可选；用于电子邮件通知）		
IP 地址	10.1.123.225	

所需信息	样本	您的值
全限定域名 (FQDN)	mail.company.com	
NetBIOS（主机）名称	mailserver	
SNMP 陷阱信息（可选，用于 SNMP 陷阱通知）		
团体名称	trendmicro	
IP 地址	10.1.194.225	

端口清单

控制管理中心有针对性地使用以下端口。

端口	样本	您的值
SMTP	25	
代理服务器	8088	
寻呼机 COM	COM1	
用于 Trend VCS 代理的代理服务器（可选）	223	
Web 控制台和更新/部署组件	80	
防火墙，“转发”端口（可选；在控制管理中心代理安装期间使用）	224	
趋势科技管理基础架构 (TMI) 内部进程通信（用于远程产品）	10198	
TMI 外部进程通信	10319	
实体模拟程序	10329	

注意

控制管理中心要求独占使用端口 10319 和 10198。

控制管理中心 2.x 代理安装清单

代理安装过程中使用以下信息。

所需信息	样本	您的值
控制管理中心服务器管理员帐户用户名	root	
密钥位置	C:\MyDocuments\E2EPulic.dat	

注意

您可以使用任何用户名代替 root 帐户。但是，趋势科技建议使用 root 帐户，因为如果删除了代理安装过程中指定的用户名，管理代理将会非常困难。

产品名	管理员级别的帐户	IP 地址	主机名
样本	Admin	10.225.225.225	PH-antivirus

控制管理中心约定

有关控制管理中心安装或 Web 控制台配置，请参考下面的适用约定。

- 用户名

最大长度	32 个字符
允许	A-Z、a-z、0-9、-、_

- 文件夹名称

最大长度	40 个字符
不允许	/ > & "

注意

对于控制管理中心服务器主机名，安装程序支持将下划线 ("_") 作为服务器名称组成部分的服务器。

核心进程和配置文件

控制管理中心以 XML 格式保存系统配置设置和临时文件。

以下各表描述控制管理中心所用的配置文件和进程。

表 A-2. 控制管理中心配置文件

配置文件	描述
AuthInfo.ini	包含关于私有密钥文件名、公共密钥文件名、证书文件名和私有密钥的加密密码以及主机标识和端口的配置文件。
aucfg.ini	ActiveUpdate 配置文件
TVCS_Cert.pem	由 SSL 认证使用的证书
TVCS_Pri.pem	SSL 使用的私有密钥
TVCS_Pub.pem	SSL 使用的公共密钥
ProcessManager.xml	由 ProcessManager.exe 使用
CmdProcessorEventHandler.xml	由 CmdProcessor.exe 使用

配置文件	描述
UIProcessorEventHandler.xml	由 UIProcessor.exe 使用
DMRegisterinfo.xml	由 CasProcessor.exe 使用
DataSource.xml	它存储控制管理中心进程的连接参数
SystemConfiguration.xml	控制管理中心系统配置文件
CascadingLogConfiguration.xml	用于子级服务器的日志上传配置文件
agent.ini	MCP 代理文件
TMI.cfg	趋势科技管理基础架构配置文件

表 A-3. 控制管理中心进程

进程	描述
ProcessManager.exe	启动和停止其他控制管理中心核心进程。
CmdProcessor.exe	将其他进程形成的 XML 指令发送到被管理产品、处理产品注册信息、发送警报、执行预设任务并应用爆发阻止策略。
UIProcessor.exe	处理控制管理中心 Web 控制台中的用户输入信息，并将其转换为实际命令。
LogReceiver.exe	接收被管理产品日志和消息。
LogProcessor.exe	接收来自被管理产品的新消息，并接收来自子级控制管理中心服务器的实体信息。
LogRetriever.exe	在控制管理中心数据库中检索和保存日志。
ReportServer.exe	生成控制管理中心报表。
MsgReceiver.exe	接收来自控制管理中心服务器、被管理产品和子级服务器的消息。
EntityEmulator.exe	允许控制管理中心使用 Trend VCS 代理。
CasProcessor.exe	允许控制管理中心服务器（父级服务器）管理其他控制管理中心服务器（子级服务器）。

进程	描述
DCSProcessor.exe	执行损害清除服务功能。
Ntpd.exe	网络时间协议服务。
inetinfo.exe	Microsoft Internet Information Service 进程。
jk_nt_service.exe java.exe	用于通过定义接口而不是使用大量独立 CGI 程序来构建基于 Web 的用户界面的 Java 服务器端扩展。
cm.exe	管理 dmserver.exe 和 mrf.exe。
mrf.exe	通信器进程。
dmserver.exe	提供控制管理中心 Web 控制台登录页面并管理产品目录（控制管理中心端）。
sCloudProcessor.NET.exe	管理与策略管理相关的任务。

通信和侦听端口

这些是缺省的控制管理中心通信和侦听端口。

类型	通信端口
内部通信	10198
外部通信	10319

服务	服务端口
ProcessManager.exe	20501
CmdProcessor.exe	20101
UIProcessor.exe	20701
LogReceiver.exe	20201

服务	服务端口
LogProcessor.exe	21001
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
CasProcessor.exe	20801
DcsProcessor.exe	20903

控制管理中心产品版本比较

下表提供了控制管理中心版本之间的功能比较。

表 A-4. 产品版本比较

功能	控制管理中心版本					
	5.0 高级版	5.0 标准版	5.5 高级版	5.5 标准版	6.0 高级版	6.0 标准版
2.x 和 MCP 代理与被管理产品相互作用	●	●	●	●	●	●
条件查询	●	●	●	●	●	●
自动组件（例如，病毒码/规则）更新	●	●	●	●	●	●
层叠管理结构	●		●		●	
用于所有病毒日志和系统事件的中心数据库	●	●	●	●	●	●
基于 Web 的集中式企业病毒管理解决方案	●	●	●	●	●	●

功能	控制管理中心版本					
	5.0 高级版	5.0 标准版	5.5 高级版	5.5 标准版	6.0 高级版	6.0 标准版
子级服务器监控	●		●		●	
发出子级服务器任务	●		●		●	
命令跟踪	●	●	●	●	●	●
通信器波动信号	●	●	●	●	●	●
通信器预设程序	●	●	●	●	●	●
组件下载间隔	●	●	●	●	●	●
按组配置	●	●	●	●	●	●
配置多个下载源	●	●	●	●	●	●
被管理产品和控制管理中心用户界面一致	●	●	●	●	●	●
控制管理中心 MIB 文件（之前称为 HP OpenView MIB）	●	●	●	●	●	●
自定义用户类型	●	●	●	●	●	●
部署计划	●	●	●	●	●	●
目录管理器	●	●	●	●	●	●
增强的通信安全性	●	●	●	●	●	●
事件中心	●	●	●	●	●	●
改进的导航	●	●	●	●	●	●
改进的用户界面	●	●	●	●	●	●
InterScan Web Security Service 集成	●	●	●	●	●	●

功能	控制管理中心版本					
	5.0 高级版	5.0 标准版	5.5 高级版	5.5 标准版	6.0 高级版	6.0 标准版
日志增强功能	●	●	●	●	●	●
日志处理速度增强功能			●	●	●	●
管理防病毒产品和内容安全产品	●	●	●	●	●	●
管理服务	●	●	●	●	●	●
被管理产品使用授权管理中心	●		●		●	
被管理产品报表	●		●		●	
Web 控制台渲染增强功能			●	●	●	●
Microsoft SQL Express 或 Microsoft SQL 2005	●	●	●	●		
Microsoft SQL Express 或 Microsoft SQL 2008					●	●
MSDE 或 Microsoft SQL 7/2000	●	●				
MSN Messenger 通知	●	●	●	●	●	●
通知和爆发警报	●	●	●	●	●	●
防毒墙网络版集成增强功能			●	●	●	●
爆发指挥中心/爆发阻止服务 (OPS) • 自动下载和部署 OPP • 手动下载和部署 OPP	●	●	●	●	●	●
对第三方产品的默许支持	●		●		●	
策略管理					●	●

功能	控制管理中心版本					
	5.0 高级版	5.0 标准版	5.5 高级版	5.5 标准版	6.0 高级版	6.0 标准版
远程代理安装和本地代理安装	●	●	●	●	●	●
远程管理	●	●	●	●	●	●
报表	●		●		●	
服务器和代理之间的安全通信	●	●	●	●	●	●
对于支持单次登录 (SSO) 的被管理产品使用 SSO	●	●	●	●	●	●
云安全智能防护网络集成			●	●	●	●
SNMP 陷阱通知	●		●		●	
对 ActiveUpdate 的 SSL 支持	●	●	●	●	●	●
对 Web 控制台的 SSL 支持	●	●	●	●	●	●
支持控制管理中心 2.x 代理	●	●	●	●	●	●
支持服务器、代理和被管理产品之间的 HTTPS 通信	●	●	●	●	●	●
支持 MCP 代理	●	●	●	●	●	●
Syslog 通知	●		●		●	
智能化的威胁控制台			●	●	●	●
趋势科技防毒墙网关版 for Cisco 内容安全和控制安全服务模块 (ISC CSC SSM) 集成	●	●	●	●	●	●
趋势科技网络病毒墙 1200 集成	●	●	●	●	●	●
趋势科技网络病毒墙 2500 集成	●	●	●	●	●	●

功能	控制管理中心版本					
	5.0 高级版	5.0 标准版	5.5 高级版	5.5 标准版	6.0 高级版	6.0 标准版
趋势科技产品注册服务器集成	●	●	●	●	●	●
TrendLabs 消息公告牌	●	●				
用户帐户管理	●	●	●	●	●	●
漏洞检查	●	●	●	●	●	●
Windows 认证	●	●	●	●	●	●
工作时间控制	●	●	●	●	●	●