

趋势科技

防毒墙网络版 Officescan 10.5

产品安装标准程序 (SOP)



趋势科技技术支持部

唐寅如

Mac Tang

2010年10月

目 录

1	OFFICESCAN 10.5 是如何保护您的网络的?	5
1.1	OFFICESCAN 服务器的主要功能	5
1.2	OFFICESCAN 客户端的主要功能	6
1.3	什么是云安全智能防护解决方案?	7
1.3.1	云安全智能防护服务	7
1.3.2	云安全智能防护源	8
1.4	此版本的新功能	9
1.5	此版本增强的功能	10
2	OFFICESCAN 10.5 的系统需求	11
2.1	OFFICESCAN 服务器端	11
2.2	WEB 控制台	13
2.3	OFFICESCAN 客户端	14
3	安装 OFFICESCAN10.5 前注意事项	23
3.1	检查系统版本、硬件配置	23
3.2	检查操作系统配置是否正确	23
4	OFFICESCAN10.5 标准安装过程	26
4.1	安装前注意事项	26
4.1.1	不兼容的第三方安全软件	26
4.1.2	安装期间扫描方法部署	26
4.1.3	不兼容的第三方安全软件	27
4.2	安装 OFFICESCAN 10.5 服务器端	27
4.3	安装 OFFICESCAN 10.5 客户端	41
4.4	如何检查标准安装是否成功?	45
4.4.1	Officescan 服务器端	45
4.4.2	Officescan 客户端	48
5	升级安装过程	50
5.1	升级前的注意事项	50
5.2	升级前的备份	53
5.3	升级安装 OFFICESCAN 10.5	54
5.3.1	分批升级 Officescan 客户端	54
5.3.2	利用移动 Officescan 客户端的方式, 分批升级	56
5.3.3	Officescan 客户端全自动升级方式	57
5.4	如何检查升级安装是否成功	58
5.4.1	Officescan 服务器端	58
5.4.2	Officescan 客户端	58
6	其他设置及常见问题	58
6.1	OFFICESCAN 10.5 使用的网络通讯端口	58
6.2	如何恢复使用传统防病毒扫描?	59
6.3	针对 OSCE10.5 新功能的简单介绍和设定	60
6.3.1	客户端多层次分组	60

6.3.2	将 OSCE 服务端与 Active Directory 集成	61
6.3.3	趋势科技虚拟桌面支持	62
6.4	如何关闭 OFFICESCAN 10.5 客户端的 AEGIS 来解决机器运行缓慢的问题	62
6.5	安装 OFFICESCAN 10.5 客户端的防火墙后，原系统中的 VMWARE 客户机无法正常通讯.....	62
7	趋势科技厂商资源	64



今天，网络安全是一个所有IT管理员格外关注的问题，网络安全最主要的目的是阻止不被允许的链接进入网络以此来减少数据损坏，窃取数据，和对系统造成危险。

但是很不幸，很多时候不被允许的链接只是在一个威胁发布后才能被检测到。因而，在访问控制的机制之外，IT管理员必须用工具并且设定策略去监控活跃的网络资产，早早的检测网络威胁，并且能尽快的对潜在的威胁做出相应。

防毒墙网络版(Officescan) 10.5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。

1 Officescan 10.5 是如何保护您的网络的？

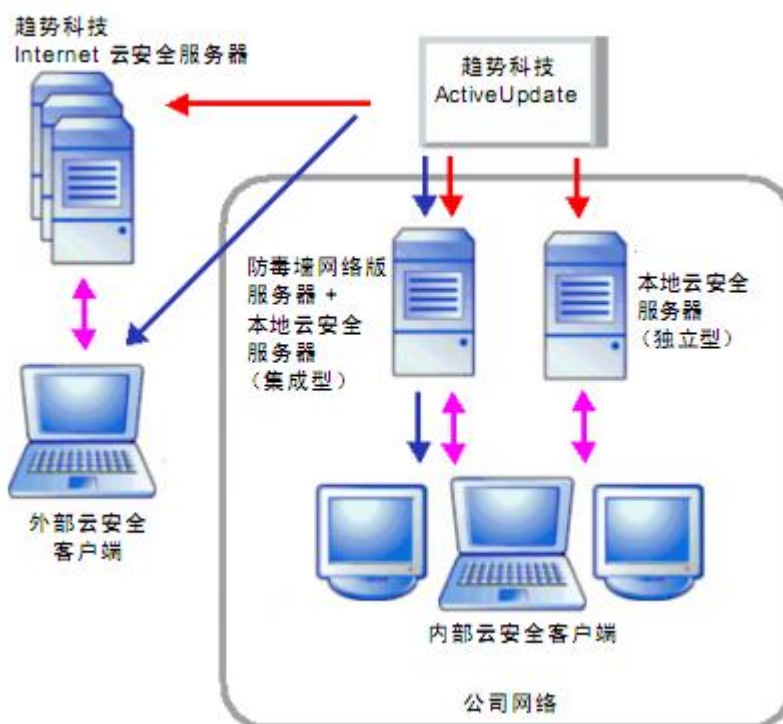
1.1 Officescan 服务器的主要功能

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服务器下载



防毒墙网络版服务器可提供服务器与客户端之间的实时、双向通信。从基于浏览器的 Web 控制台（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。

1.2 Officescan 客户端的主要功能

通过在每台计算机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。客户端提供三种扫描方法：实时扫描、预设扫描和手动扫描。

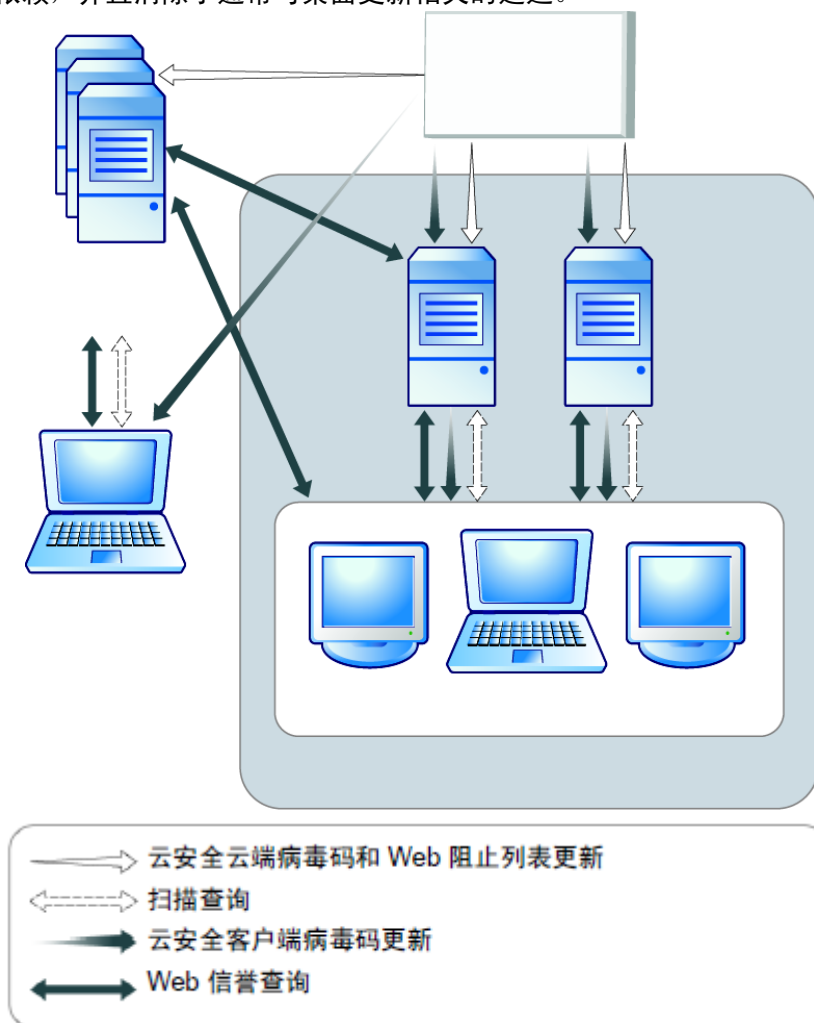
客户端会向作为其安装源的Officescan服务器报告。客户端将事件和状态信息实时发送到服务器。事件的示例包括病毒/恶意软件检测、客户端启动、客户端关闭、扫描启动和更新完成。

计算机上的可用防毒墙网络版客户端功能取决于计算机的操作系统。

功能					
	Win XP	Win 2003	win 2008	Win Vista	Win 7
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	是
Microsoft Outlook 邮件扫描	是 (32bit) 否 (64 bit)	是 (32bit) 否 (64 bit)	否	否	否
POP3 邮件扫描	是	是	是	是	是
防毒墙网络版防火墙	是	是 缺省情况下禁用	是 缺省情况下禁用	是	是
损害清除服务	是	是	是	是	是
Cisco NAC 支持	是	否	否	否	否
插件管理器	是	是	是	是	是
漫游模式	是	是	是	是	是
SecureClient 支持	是 (32bit) 否 (64 bit)	是 (32bit) 否 (64 bit)	否	否	否
行为监控	是 (32bit) 否 (64 bit)	是 (32bit) 否 (64 bit) 缺省情况下禁用	是 (32bit) 否 (64 bit) 缺省情况下禁用	是(32bit) 否 (64 bit)	是 (32bit) 否 (64 bit)
智能反馈	是	是	是	是	是
设备控制	是 (32bit) 否 (64 bit)	是 (32bit) 否 (64 bit) 缺省情况下禁用	是 (32bit) 否 (64 bit) 缺省情况下禁用	是(32bit) 否 (64 bit)	是 (32bit) 否 (64 bit)

1.3 什么是云安全智能防护解决方案？

通过结合云中信誉、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。



1.3.1 云安全智能防护服务

文件信誉

趋势科技的文件信誉技术将在允许用户访问每个文件之前，根据庞大的云中数据库检查这些文件的信誉。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，并且除了极大地减少总体客户端占用资源之外，还消除了特征码部署的负担。

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。

用户访问 URL 时，趋势科技将：

- 利用域信誉数据库验证 Web 站点和页面的可信度
- 为 Web 域和站点内的各个页面或链接指定信誉分值
- 允许或阻止用户访问站点

智能反馈

趋势科技智能反馈旨在从云安全智能防护服务器收集相关数据并将其传输到云安全智能防护网络，以便进行深入分析，从而能够发展高级解决方案并对其进行部署以保护客户端。

发送到趋势科技的一些信息示例：

- 文件校验和
- 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： 无需参与智能反馈便可为您的计算机提供防护。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。

1.3.2 云安全智能防护源

客户端连接到哪个云安全智能防护源取决于客户端所处的位置。客户端可连接到下列两个服务器中的任意一个：

- 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。
- 趋势科技云安全智能防护网络：基于 Internet 的全球范围的基础架构，用于将信誉服务提供给无法直接访问其公司网络的用户。

云安全智能防护源之间的比较

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。	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。
用途	设计用于将云安全智能防护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
服务器管理员	防毒墙网络版管理员安装和管理这些服务器	趋势科技维护此服务器
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

1.4 此版本的新功能

客户端默认为云安全扫描（全新安装）

云安全扫描将安全功能从端点移动到云端。云安全扫描是趋势科技云安全智能防护网络不可或缺的一部分，可以提供下列优点：

- 在云端提供快速、实时的安全状态查找功能。
- 减少针对新出现的威胁提供防护所需的总体时间。
- 减少在特征码更新期间占用的网络带宽。大多数特征码定义更新只需要传送到云端，而不是许多端点。
- 减少整个公司范围内特征码部署所涉及的成本和开销。
- 降低端点上的内核内存占用。内存占用随时间的推移以最低限度增加。

注意：从OSCE7.3/8.0/10.0升级至OSCE10.5版本则默认依旧保留传统扫描方式

云安全智能防护解决方案

云安全智能防护解决方案是基于云端的新一代端点保护解决方案。这些解决方案的核心是高级扫描体系结构，它利用防恶意软件签名和存储在云端的 Web 信誉数据

Active Directory 集成

防毒墙网络版利用 Microsoft™ Active Directory™ 服务在组织中强制执行安全合规。通过定期轮询 Active Directory，防毒墙网络版可以检测无安全软件的计算机，并将客户端安装到计算机。防毒墙网络版还允许您通过用户的 Active Directory 帐户，向其分配 Web 控制台的访问权限。

安全合规

确保防毒墙网络版客户端服务、设置、扫描和组件符合总体端点防护的安全设置。管理员可使用此功能执行以下操作：

- 生成有关非兼容客户端的报告
- 确定并确保网络中不受防毒墙网络版服务器管理的端点的合规

趋势科技虚拟桌面支持 (VDI)

调整构成服务器的一部分的虚拟机以限制同时执行更新或扫描的虚拟桌面的数量。这可以确保适当地管理带有防毒墙网络版客户端的虚拟机的资源。请单独获取此功能的许可证，然后从插件管理器管理虚拟桌面扫描和更新任务。

[详情可以参考本页第五章介绍](#)

基于角色的粒度管理

将 Web 控制台管理任务委派给其他管理员，并且允许非管理员查看 Web 控制台项。可以先创建具有防毒墙网络版 Web 控制台功能的特定访问权限的用户角色，然后将这些角色分配给用户。通过创建定制用户帐户或使用现有的 Active Directory 帐户来管理用户。

1.5 此版本增强的功能

更新代理

允许更新代理单独下载组件、域设置以及程序和 hotfix。另外，还可以下载更新代理分析报告，其中包括有关网络中的更新代理的更多详细信息。

例外列表

先前的防毒墙网络版版本将行为监控例外列表用于行为监控和设备控制。利用此版本的防毒墙网络版，用户现在可以单独配置行为监控和设备控制的例外列表。

防火墙

用户现在可以配置应用程序例外或安全软件认证列表以启用或禁用指定应用程序的网络连接。

日志

此功能确保防毒墙网络版服务器、客户端和趋势科技防毒墙控制管理中心之间的时间保持一致。防毒墙网络版发送日志时具有相同的时间戳，无需考虑时间因素，如夏令时（DST）或时区。

扫描设置

用户现在可以配置下列扫描设置：

注意： 这些设置仅适用于具有配置扫描例外的权限的客户端。

- 在客户端扫描例外列表中覆盖、添加或者移除文件或目录
- 配置 OLE 利用检测设置
- 针对可能的病毒/恶意软件配置设置和操作
- 清除压缩文件中的间谍软件/灰色软件
- **在例外列表中使用通配符**

粒度 Web 信誉设置

配置 Web 信誉策略，并将这些策略分配给一个、多个或所有防毒墙网络版客户端

插件程序更新

防毒墙网络版现在可以从“服务器更新源”窗口中的第一个更新源（包括趋势科技防毒墙控制管理中心）自动下载插件程序更新。

2 Officescan 10.5 的系统需求

2.1 Officescan 服务器端

资源	要求
操作系统	<p>Windows 2003</p> <ul style="list-style-type: none"> 带有 Service Pack 2 的 Windows Server 2003 (Standard、Enterprise 和 Datacenter 版), 32 位和 64 位版本 带有 Service Pack 2 的 Windows Server 2003 R2 (Standard、Enterprise 和 Datacenter 版), 32 位和 64 位版本 带有 Service Pack 2 的 Windows Storage Server 2003 (Basic、Standard、Enterprise 和 Workgroup 版), 32 位和 64 位版本 带有 Service Pack 2 的 Windows Storage Server 2003 R2 (Basic、Standard、Enterprise 和 Workgroup 版), 32 位和 64 位版本 Microsoft Windows Compute Cluster Server 2003 <p>Windows 2008</p> <ul style="list-style-type: none"> 带有 Service Pack 1 或 2 的 Windows Server 2008 (Standard、Enterprise、Datacenter 和 Web 版), 32 位和 64 位版本 Windows Server 2008 R2 (Standard、Enterprise、Datacenter 和 Web 版), 64 位版本 Windows Storage Server 2008 (Basic、Standard、Enterprise 和 Workgroup 版) 64 位版本 Windows Storage Server 2008 (Basic 版) 32 位和 64 位版本 Microsoft Windows HPC Server 2008 <p>注意: 如果 Windows 2008 在服务器核心环境中运行, 则无法安装防毒墙网络版。</p>
虚拟化	<p>防毒墙网络版支持在下列虚拟化应用程序中托管的来宾 Windows 2003 或 Windows 2008 操作系统中安装服务器:</p> <ul style="list-style-type: none"> 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 VMware ESX/ESXi Server 4 (Server 版) VMware Server 2 (Server 版) VMware Workstation 和 Workstation ACE 7.0 版 VMware vCenter™ 4 Citrix™ XenServer™ 5.5 Microsoft Windows Server 2008 64 位 Hyper-V™ Microsoft Windows Server 2008 R2 64 位 Hyper-V Microsoft Hyper-V Server 2008 R2 64 位

硬件（适用于 Windows Server 2008）	<p>处理器</p> <ul style="list-style-type: none"> 至少 1.86GHz 的 Intel™ Core™2 Duo 处理器 AMD™64 和 Intel™ 64 处理器体系结构 <p>内存</p> <ul style="list-style-type: none"> 最低要求是 1GB，建议使用 2GB <p>可用磁盘空间</p> <ul style="list-style-type: none"> 最低要求是 3.1GB（如果本地安装防毒墙网络版服务器、防毒墙网络版客户端、策略服务器 for Cisco™ NAC 和集成型云安全智能防护服务器） 最低要求是 3.5GB（如果远程安装防毒墙网络版服务器、防毒墙网络版客户端和集成型云安全智能防护服务器） <p>其他</p> <ul style="list-style-type: none"> 千兆网络接口卡 (NIC) 在颜色为 256 或更高时，支持分辨率 1024 x 768 的显示器
硬件（适用于所有其他平台）	<p>处理器</p> <ul style="list-style-type: none"> 至少 1.86GHz 的 Intel™ Core™2 Duo 处理器 <p>内存</p> <ul style="list-style-type: none"> 最低要求是 1GB <p>可用磁盘空间</p> <ul style="list-style-type: none"> 最低要求是 3.1GB（如果本地安装防毒墙网络版服务器、防毒墙网络版客户端、策略服务器 for Cisco NAC 和集成型云安全智能防护服务器） 最低要求是 3.5GB（如果远程安装防毒墙网络版服务器、防毒墙网络版客户端和集成型云安全智能防护服务器） <p>其他</p> <ul style="list-style-type: none"> 千兆网络接口卡 (NIC) 在颜色为 256 或更高时，支持分辨率 1024 x 768 的显示器
Web 服务器	<ul style="list-style-type: none"> Microsoft Internet Information Server (IIS) <ul style="list-style-type: none"> 在 Windows Server 2003 上：版本 6.0 在 Windows Server 2008 上：版本 7.0 在 Windows Server 2008 R2 上：版本 7.5 Apache™ Web 服务器 2.0.x <p>如果计算机中安装了非 2.0.x 版的 Apache Web 服务器，防毒墙网络版将安装和使用 2.0.63 版。但不会移除现有的 Apache Web 服务器。</p>
其他	<ul style="list-style-type: none"> 可访问服务器计算机的管理员或域管理员权限 对于安装在服务器计算机上的 Microsoft 网络，允许“文件和打印机共享” 如果计划在安装防毒墙网络版服务器的同一台计算机上安装 Cisco Trust Agent (CTA)，则不要在 Windows Server 2003 x64 版上安装防毒墙网络版服务器。有关 CTA 需求的详细信息，请参阅《防毒墙网络版管理员指南》。

要升级的防毒墙网络版服务器

以下防毒墙网络版版本可以升级到此版本：

- 10 Service Pack 1
- 10
- 8.0 Service Pack 1
- 8.0
- 7.3

2.2 Web 控制台

资源	要求
硬件	<p>处理器</p> <p>300MHz Intel Pentium 处理器或同等处理器</p> <p>内存</p> <p>最低要求是 128MB</p> <p>可用磁盘空间</p> <p>最低要求是 30MB</p> <p>其他</p> <p>在颜色为 256 或更高时，支持分辨率 1024 x 768 的显示器</p>
浏览器	Microsoft Internet Explorer™ 7.0 或 8.0

2.3 Officescan 客户端

2.3.1 Windows XP/2003（32 位版本）上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> • 带有 Service Pack 3 的 Windows XP Home • 带有 Service Pack 3 的 Windows XP Professional • 适用于嵌入系统的 Windows XP Professional • Windows XP Tablet PC 版, Service Pack 3 • 带有 Service Pack 2 的 Windows Server™ 2003 (Standard、Enterprise、Datacenter 和 Web 版) • 带有 Service Pack 2 的 Windows Server 2003 R2 (Standard、Enterprise 和 Datacenter 版) • 带有 Service Pack 2 的 Windows Storage Server 2003 (Basic、Standard、Enterprise 和 Workgroup 版) • 带有 Service Pack 2 的 Windows Storage Server 2003 R2 (Basic、Standard、Enterprise 和 Workgroup 版) • Microsoft Windows Compute Cluster Server 2003 • 防毒墙网络版支持在以下虚拟化应用程序中托管的来宾 Windows XP/2003 操作系统中安装客户端： <ul style="list-style-type: none"> • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • VMware ESX/ESXi Server 4 (Server 版) • VMware Server 2 (Server 版) • VMware Workstation 和 Workstation ACE 7.0 版 • VMware vCenter 4 • Citrix XenServer 5.5 • Microsoft Windows Server 2008 64 位 Hyper-V • Microsoft Windows Server 2008 R2 64 位 Hyper-V • Microsoft Hyper-V Server 2008 R2 64 位 <p>注意：在服务器平台上防毒墙网络版会自动禁用某些功能。有关详细信息，请参考《防毒墙网络版管理员指南》。</p>
硬件	<p><i>处理器</i></p> <ul style="list-style-type: none"> • 300MHz Intel Pentium 或同等处理器 • AMD64 和 Intel™ 64 处理器体系结构 <p><i>内存</i></p> <p>最低要求是 256MB，建议使用 512MB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p>

	<p>其他</p> <p>颜色为 256 时支持分辨率为 1024 x 768 的监视器</p>
其他	<ul style="list-style-type: none">• 如果执行 Web 安装，则需要 Microsoft Internet Explorer 6.0、7.0 或 8.0• 禁用 Windows XP 计算机上的简单文件共享，以使用户成功安装防毒墙网络版客户端程序（请参阅 Windows 文档来获取指导信息）。

2.3.2 Windows XP/2003（64 位版本）上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> • 带有 Service Pack 2 的 Windows XP Professional • 带有 Service Pack 2 的 Windows Server 2003（Standard、Enterprise、Datacenter 和 Web 版） • 带有 Service Pack 2 的 Windows Server 2003 R2（Standard、Enterprise 和 Datacenter 版） • 带有 Service Pack 2 的 Windows Storage Server 2003（Basic、Standard、Enterprise 和 Workgroup 版） • 带有 Service Pack 2 的 Windows Storage Server 2003 R2（Basic、Standard、Enterprise 和 Workgroup 版） • Microsoft Windows Compute Cluster Server 2003 • 防毒墙网络版支持在以下虚拟化应用程序中托管的来宾 Windows XP/2003 操作系统中安装客户端： <ul style="list-style-type: none"> • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • VMware ESX/ESXi Server 4（Server 版） • VMware Server 2（Server 版） • VMware Workstation 和 Workstation ACE 7.0 版 • VMware vCenter 4 • Citrix XenServer 5.5 • Microsoft Windows Server 2008 64 位 Hyper-V • Microsoft Windows Server 2008 R2 64 位 Hyper-V • Microsoft Hyper-V Server 2008 R2 64 位 <p>注意：在服务器平台上防毒墙网络版会自动禁用某些功能。有关详细信息，请参考《防毒墙网络版管理员指南》。</p>
硬件	<p><i>处理器</i></p> <p>AMD64 和 Intel 64 处理器体系结构</p> <p><i>内存</i></p> <p>最低要求是 256MB，建议使用 512MB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 吋支持分辨率为 1024 x 768 的监视器</p>
其他	<ul style="list-style-type: none"> • 如果执行 Web 安装，则需要 Microsoft Internet Explorer 6.0、7.0 或 8.0 • 禁用 Windows XP 计算机上的简单文件共享，以便用户成功安装防毒墙网络版客户端程序（请参阅 Windows 文档来获取指导信息）。

2.3.3 Windows Vista（32 位和 64 位版本）中的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> • 带有 Service Pack 1 或 2 的 Windows Vista™（Business、Enterprise、Ultimate、Home Premium 和 Home Basic） • 适用于嵌入式系统的 Windows Vista Business/Ultimate • 防毒墙网络版支持在以下虚拟化应用程序中托管的来宾 Windows Vista 操作系统中安装客户端： <ul style="list-style-type: none"> • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • VMware ESX/ESXi Server 4（Server 版） • VMware Server 2（Server 版） • VMware Workstation 和 Workstation ACE 7.0 版 • VMware vCenter 4 • Citrix XenServer 5.5 • Microsoft Windows Server 2008 64 位 Hyper-V • Microsoft Windows Server 2008 R2 64 位 Hyper-V • Microsoft Hyper-V Server 2008 R2 64 位
硬件	<p><i>处理器</i></p> <ul style="list-style-type: none"> • 1GHz Intel Pentium 或同等处理器 • AMD64 和 Intel 64 处理器体系结构 <p><i>内存</i></p> <p>最低要求是 1GB，建议使用 1.5GB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 时支持分辨率为 1024 x 768 的监视器</p>
浏览器	如果执行 Web 安装，则需要 Windows Internet Explorer 7.0 或 8.0

2.3.4 Windows Server 2008（32 位版本）上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> 带有 Service Pack 1 或 2 的 Windows Server 2008（Standard、Enterprise Datacenter 和 Web 版） Microsoft Storage Server 2008（Basic 版） Microsoft Windows HPC Server 2008 防毒墙网络版客户端可以安装在以下虚拟化应用程序托管的来宾 Windows 2008 操作系统中： <ul style="list-style-type: none"> 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 VMware ESX/ESXi Server 4（Server 版） VMware Server 2（Server 版） VMware Workstation 和 Workstation ACE 7.0 版 VMware vCenter 4 Citrix XenServer 5.5 Microsoft Windows Server 2008 64 位 Hyper-V Microsoft Windows Server 2008 R2 64 位 Hyper-V Microsoft Hyper-V Server 2008 R2 64 位 <p>注意：</p> <ul style="list-style-type: none"> 如果 Windows 2008 在服务器核心环境中运行，则无法安装防毒墙网络版。 在服务器平台上防毒墙网络版会自动禁用某些功能。 有关详细信息，请参考《防毒墙网络版管理员指南》。
硬件	<p><i>处理器</i></p> <ul style="list-style-type: none"> 最低 1GHz Intel Pentium 或同等处理器，建议使用 2GHz AMD64 和 Intel 64 处理器体系结构 <p><i>内存</i></p> <p>最低要求是 512MB，建议使用 2GB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 吋支持分辨率为 1024 x 768 的监视器</p>
浏览器	如果执行 Web 安装，则需要 Windows Internet Explorer 7.0 或 8.0

2.3.5 Windows Server 2008 和 Windows Server 2008 R2 (64 位版本) 上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> 带有 Service Pack 1 或 2 的 Windows Server 2008 (Standard、Enterprise、Datacenter 和 Web 版) Windows Server 2008 R2 (Standard、Enterprise、Datacenter 和 Web 版) Microsoft Storage Server 2008 (Basic、Standard、Enterprise 和 Workgroup 版) Microsoft Windows HPC Server 2008 防毒墙网络版客户端可以安装在以下虚拟化应用程序托管的来宾 Windows 2008 操作系统中： <ul style="list-style-type: none"> 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 VMware ESX/ESXi Server 4 (Server 版) VMware Server 2 (Server 版) VMware Workstation 和 Workstation ACE 7.0 版 VMware vCenter 4 Citrix XenServer 5.5 Microsoft Windows Server 2008 64 位 Hyper-V Microsoft Windows Server 2008 R2 64 位 Hyper-V Microsoft Hyper-V Server 2008 R2 64 位 <p>注意：</p> <ul style="list-style-type: none"> 如果 Windows 2008 在服务器核心环境中运行，则无法安装防毒墙网络版。 在服务器平台上防毒墙网络版会自动禁用某些功能。有关详细信息，请参考《防毒墙网络版管理员指南》。
硬件	<p><i>处理器</i></p> <ul style="list-style-type: none"> 最低 1.4GHz Intel Pentium 或同等处理器，建议使用 2GHz AMD64 和 Intel 64 处理器体系结构 <p><i>内存</i></p> <p>最低要求是 512MB，建议使用 2GB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 时支持分辨率为 1024 x 768 的监视器</p>
浏览器	<p>如果执行 Web 安装：</p> <ul style="list-style-type: none"> 适用于 Windows Server 2008 的 Windows Internet Explorer 7.0 或 8.0 适用于 Windows Server 2008 R2 的 Windows Internet Explorer 8.0

2.3.6 Windows 7 (32 位版本) 上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> • Windows 7 (Home Basic、Home Premium、Ultimate、Professional 和 Enterprise) • 适用于嵌入系统的 Windows 7 Professional/Ultimate • 防毒墙网络版客户端可以安装在以下虚拟化应用程序托管的来宾 Windows 7 操作系统中： <ul style="list-style-type: none"> • VMware ESX/ESXi Server 4 (Server 版) • VMware Server 2 (Server 版) • VMware Workstation 和 Workstation ACE 7.0 版 • VMware vCenter 4 • Citrix XenServer 5.5 • Microsoft Windows Server 2008 64 位 Hyper-V • Microsoft Windows Server 2008 R2 64 位 Hyper-V • Microsoft Hyper-V Server 2008 R2 64 位
硬件	<p><i>处理器</i></p> <ul style="list-style-type: none"> • 最低 1GHz Intel Pentium 或同等处理器，建议使用 2GHz • AMD64 和 Intel 64 处理器体系结构 <p><i>内存</i></p> <p>最低要求是 1GB，建议使用 2GB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 时支持分辨率为 1024 x 768 的监视器</p>
浏览器	如果执行 Web 安装，则需要 Windows Internet Explorer 8.0

2.3.7 Windows 7（64 位版本）上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> • Windows 7（Home Basic、Home Premium、Ultimate、Professional 和 Enterprise） • 适用于嵌入系统的 Windows 7 Professional/Ultimate • 防毒墙网络版客户端可以安装在以下虚拟化应用程序托管的来宾 Windows 7 操作系统中： <ul style="list-style-type: none"> • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • VMware ESX/ESXi Server 4（Server 版） • VMware Server 2（Server 版） • VMware Workstation 和 Workstation ACE 7.0 版 • VMware vCenter 4 • Citrix XenServer 5.5 • Microsoft Windows Server 2008 64 位 Hyper-V • Microsoft Windows Server 2008 R2 64 位 Hyper-V • Microsoft Hyper-V Server 2008 R2 64 位
硬件	<p><i>处理器</i></p> <ul style="list-style-type: none"> • 最低要求是 2GHz Intel Pentium 或同等处理器 • AMD64 和 Intel 64 处理器体系结构 <p><i>内存</i></p> <p>最低要求是 1.5GB，建议使用 2GB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 时支持分辨率为 1024 x 768 的监视器</p>
浏览器	如果执行 Web 安装，则需要 Windows Internet Explorer 8.0

2.3.8 Windows Embedded POSReady 2009 (32 位版本) 上的防毒墙网络版客户端

资源	要求
操作系统	<ul style="list-style-type: none"> • Windows Embedded POSReady 2009 • 防毒墙网络版支持在以下虚拟化应用程序中托管的来宾 Windows Embedded POSReady 2009 操作系统中安装客户端： <ul style="list-style-type: none"> • 带有 Service Pack 1 的 Microsoft Virtual Server 2005 R2 • VMware ESX/ESXi Server 4 (Server 版) • VMware Server 2 (Server 版) • VMware Workstation 和 Workstation ACE 7.0 版 • VMware vCenter 4 • Citrix XenServer 5.5 • Microsoft Windows Server 2008 64 位 Hyper-V • Microsoft Windows Server 2008 R2 64 位 Hyper-V • Microsoft Hyper-V Server 2008 R2 64 位
硬件	<p><i>处理器</i></p> <p>最低要求是 300MHz Intel Pentium 或同等处理器</p> <p><i>内存</i></p> <p>最低要求是 256MB, 建议使用 512MB</p> <p><i>可用磁盘空间</i></p> <p>最低要求是 350MB</p> <p><i>其他</i></p> <p>颜色为 256 时支持分辨率为 1024 x 768 的监视器</p>
浏览器	如果执行 Web 安装, 则需要 Windows Internet Explorer 6.0、7.0 或 8.0

3 安装 Officescan10.5 前注意事项

3.1 检查系统版本、硬件配置

安装之前请检查您的服务器硬件配置和操作系统版本是否满足所需安装组件的最低配置。（详情请参考上一章节）

3.2 检查操作系统配置是否正确

安装之前请务必检查以下 3 项配置是否已经正常完成：

- 检查系统服务是否正确开启

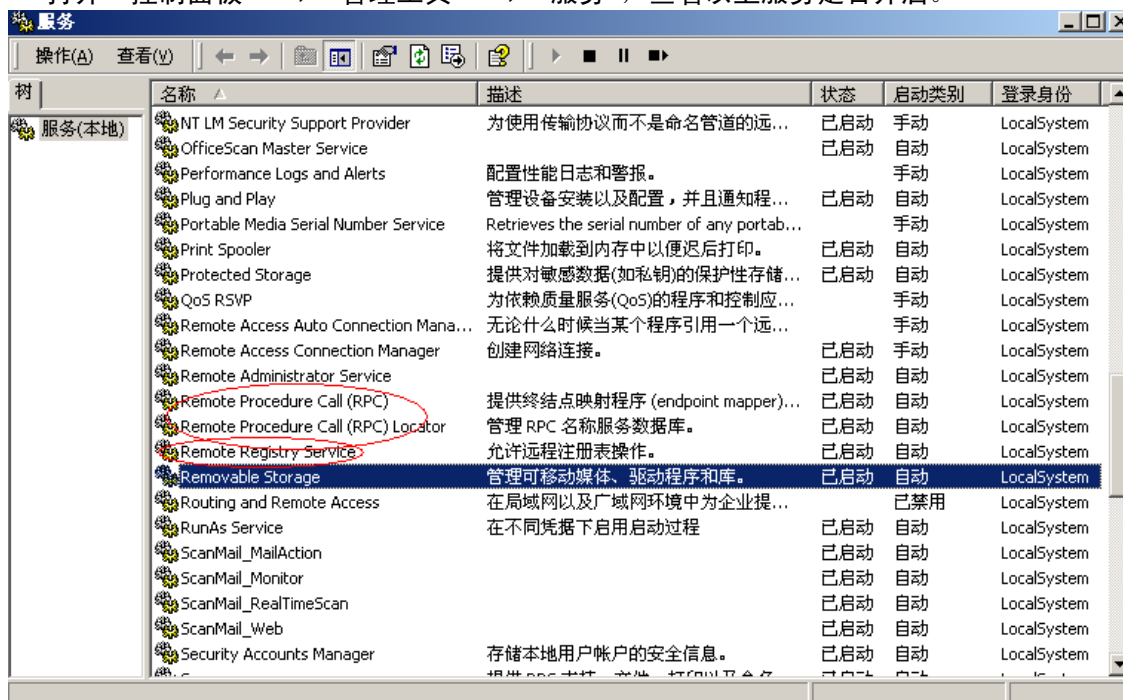
确保操作系统的一些应正常运行的系统服务开启

一些服务的存在保证了系统网络的完整性，需要特别强调的是：

- 1) Remote Procedure Call (RPC)
- 2) Remote Registry
- 3) Windows Installer.

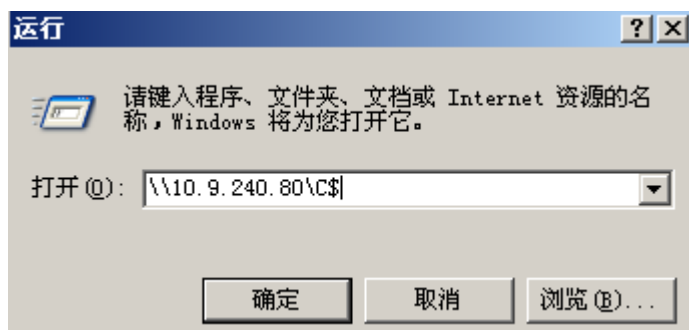
如何开启：

打开“控制面板”-->“管理工具”-->“服务”，查看以上服务是否开启。



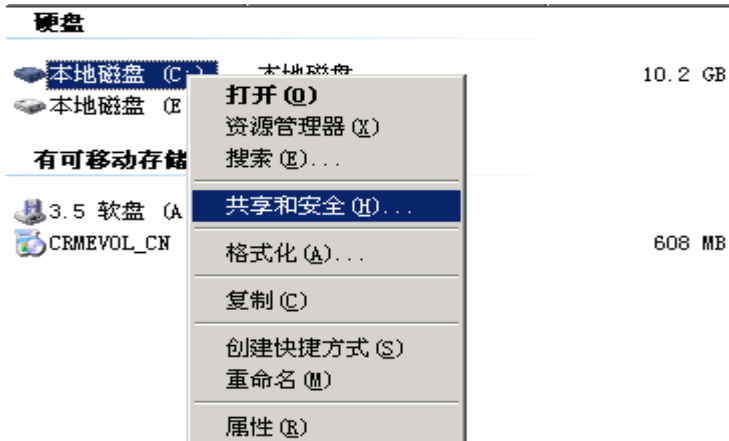
● **检查磁盘默认共享是否开启**

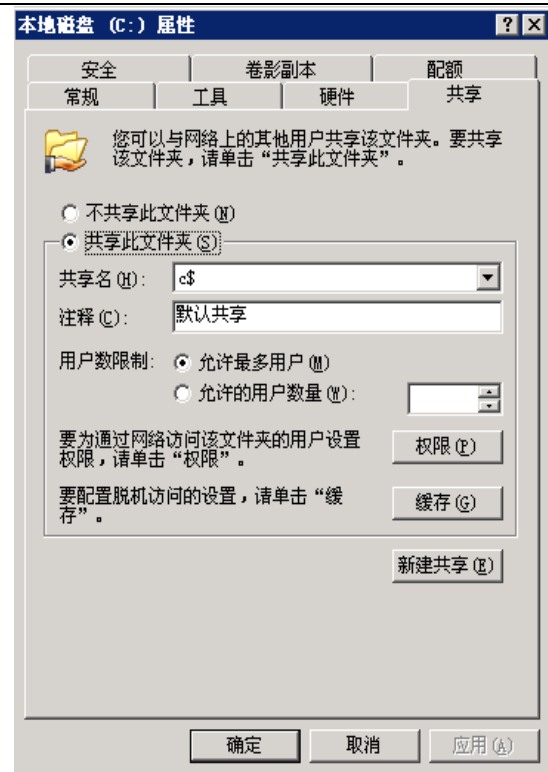
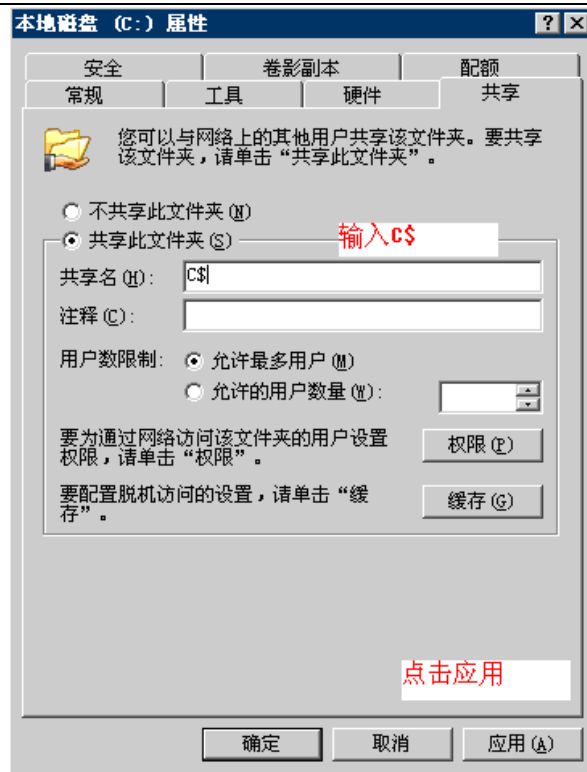
确认系统的默认\$共享存在且有权限可以访问, 比如, 在“开始菜单—>运行”里输入:
\\Server_IP\C\$, (Server_IP 指的是本机的 IP 地址), 按回车后可以进去, 并且可以新建文件。



如何开启默认共享:

打开 我的电脑——右键 C 盘——共享和安全——共享此文件夹
共享名: C\$——点击 应用。





4 Officescan10.5 标准安装过程

4.1 安装前注意事项

4.1.1 不兼容的第三方安全软件

提示： 趋势科技建议防毒墙网络版服务器至少有1.8GHz 的双处理器和大于 2GB 的内存

2. 单个防毒墙网络版服务器可以管理的联网计算机客户端的数量取决于多个因素。

防毒墙网络版服务器通常可以管理的客户端的数量如下所述：

- 带有 2GHz 双CPU和 2GB 内存的防毒墙网络版服务器通常可以管理 3000到 5000 个客户端
 - 带有 3GHz 双CPU和 4GB 内存的防毒墙网络版服务器通常可以管理 5000到 8000 个客户端
-

注意： 以上仅供参考，具体取决于实际情况

3. 可以使用 IIS Web 服务器或 Apache Web 服务器。

如果使用 IIS Web 服务器，请确保服务器计算机没有运行 IIS 锁定的应用程序。在安装期间，安装程序会自动停止再重新启动 IIS 服务。

如果使用 Apache Web 服务器，则管理员帐户是在 Apache Web 服务器上创建的唯一帐户。请创建一个新的系统帐户给Apache Web服务器使用，以防止如果黑客控制Web 服务器危及防毒墙网络版服务器的安全。

有关 Apache Web 服务器升级、Patch 和安全问题的最新信息，请参考 <http://www.apache.org>。

4.1.2 安装期间扫描方法部署

1. 传统扫描

传统扫描是所有早期防毒墙网络版版本使用的扫描方法。传统客户端将所有防毒墙网络版组件存储在客户端计算机上，并在本地扫描所有文件。

2. 云安全扫描

云安全扫描利用在云端存储的威胁签名。在云安全扫描模式中，防毒墙网络版客户端首先在

本地扫描安全风险。如果客户端在扫描期间无法确定文件的风险，它将连接到云安全智能防护服务器。

云安全扫描具有以下功能和优点：

- 在云端提供快速、实时的安全状态查找功能
- 减少针对新出现的威胁提供防护所需的总体时间
- 减少在特征码更新期间占用的网络带宽大多数特征码定义更新只需要传送到云端，而不是许多端点

- 减少整个公司范围内特征码部署所涉及的成本和开销
- 降低端点上的内核内存占用。内存占用随时间的推移以最低限度增加。

3. 扫描方法部署

客户端全新安装的缺省扫描方法是云安全扫描方法。防毒墙网络版还允许您在安装服务器后为每个域定制扫描方法。请考虑下列事项：

- 如果在安装服务器后未更改扫描方法，则安装的所有客户端都将使用云安全扫描。
- 如果希望在所有客户端上使用传统扫描，请在安装服务器后将根级扫描方法更改为传统扫描。
- 如果希望同时使用传统扫描和云安全扫描，趋势科技建议将云安全扫描保留为根级扫描方法，然后更改要应用传统扫描的域上的扫描方法。

4.1.3 不兼容的第三方安全软件

请从将安装防毒墙网络版服务器的计算机删除第三方端点安全软件。第三方安全软件可能会阻止防毒墙网络版服务器的成功安装或影响其性能。在删除第三方安全软件后立即安装防毒墙网络版服务器和客户端，以保护计算机免受安全风险的侵扰。

注意：如在Officescan 服务器上**安装360安全卫士工具**，请务必关闭其实时防护功能以确保Officescan 服务器和客户端的正常使用

4.2 安装 Officescan 10.5 服务器端

准备工作：从趋势科技网站获得最新的 Officescan 10.5 安装程序
简体中文版：

<http://www.trendmicro.com/download/zh-cn/product.asp?productid=5>

英文版：

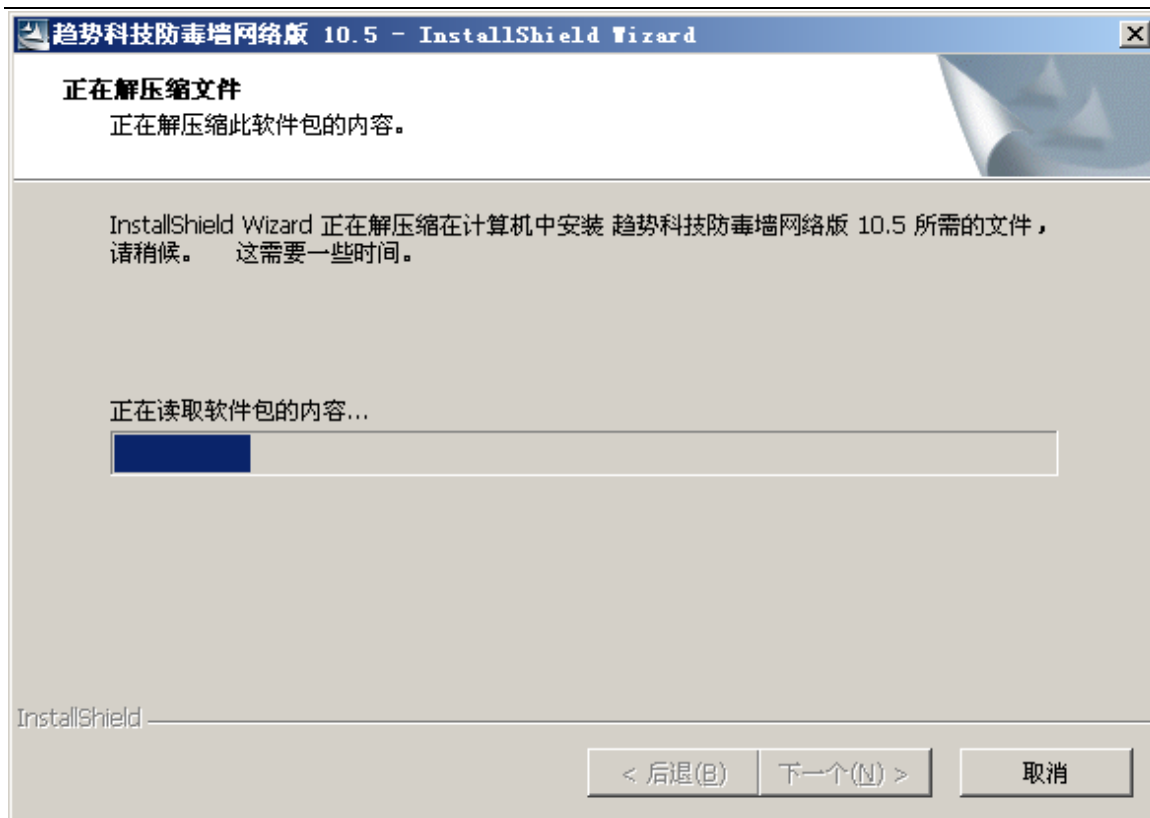
<http://www.trendmicro.com/download/product.asp?productid=5>

注意：下载完毕后，请使用 MD5 工具进行校验，确保下载的文件完整（非常重要！）。

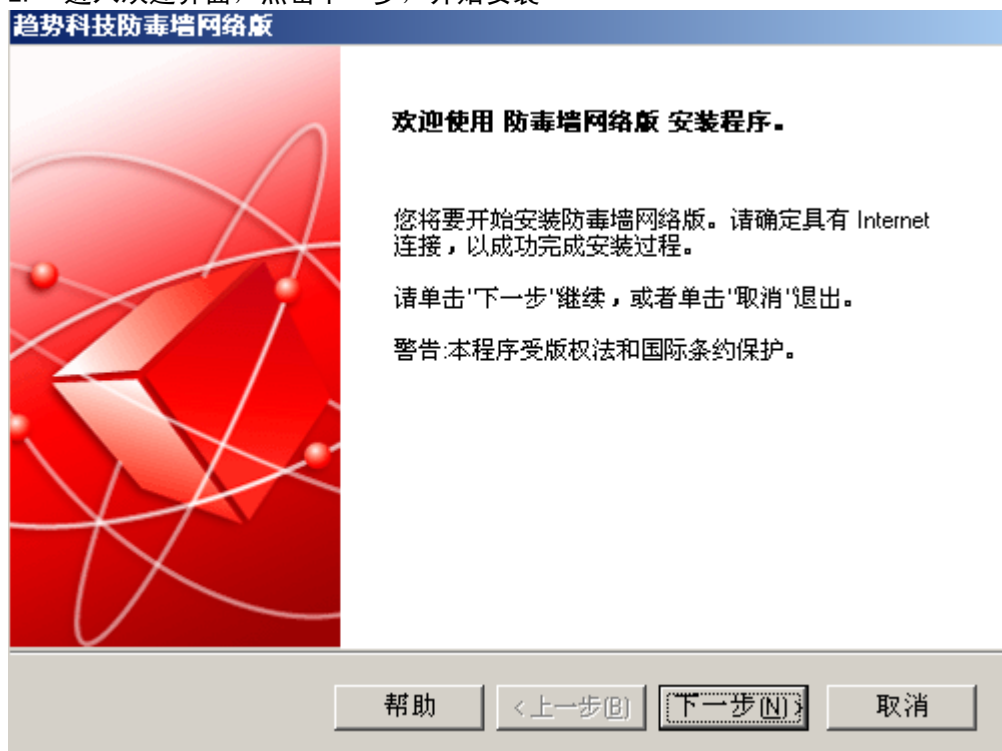
提醒：

本文档采用 Officescan 10.5 简体中文版作为安装举例。

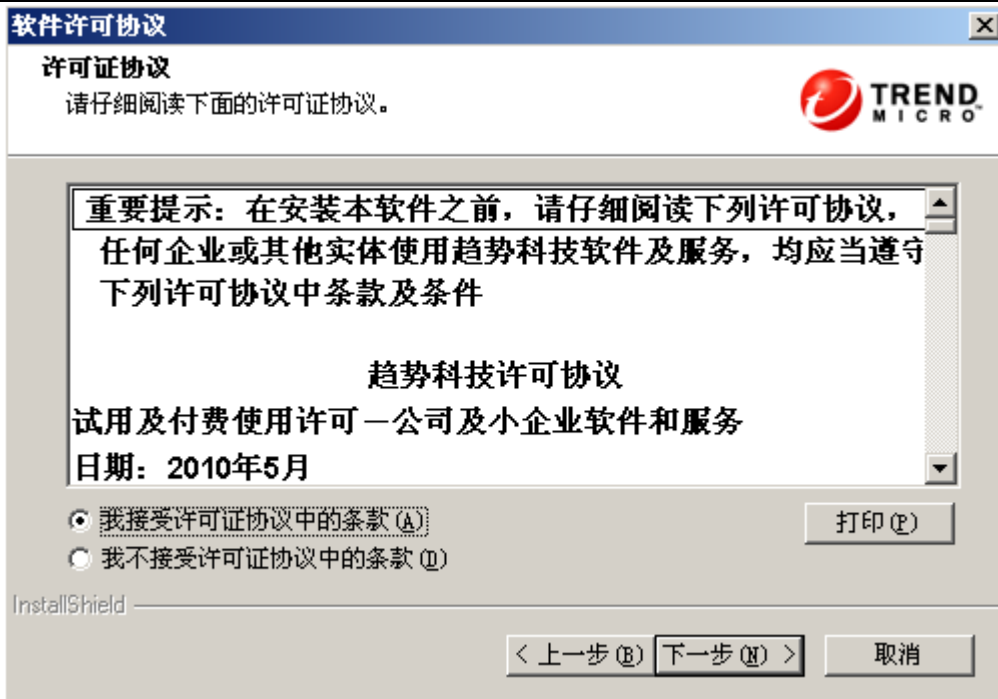
1. 在服务器端双击执行安装程序，自解压完成后进入安装程序



2. 进入欢迎界面，点击下一步，开始安装



3. 进入产品许可证界面，选择接受许可协议条款后 下一步按钮变为黑色，点击下一步



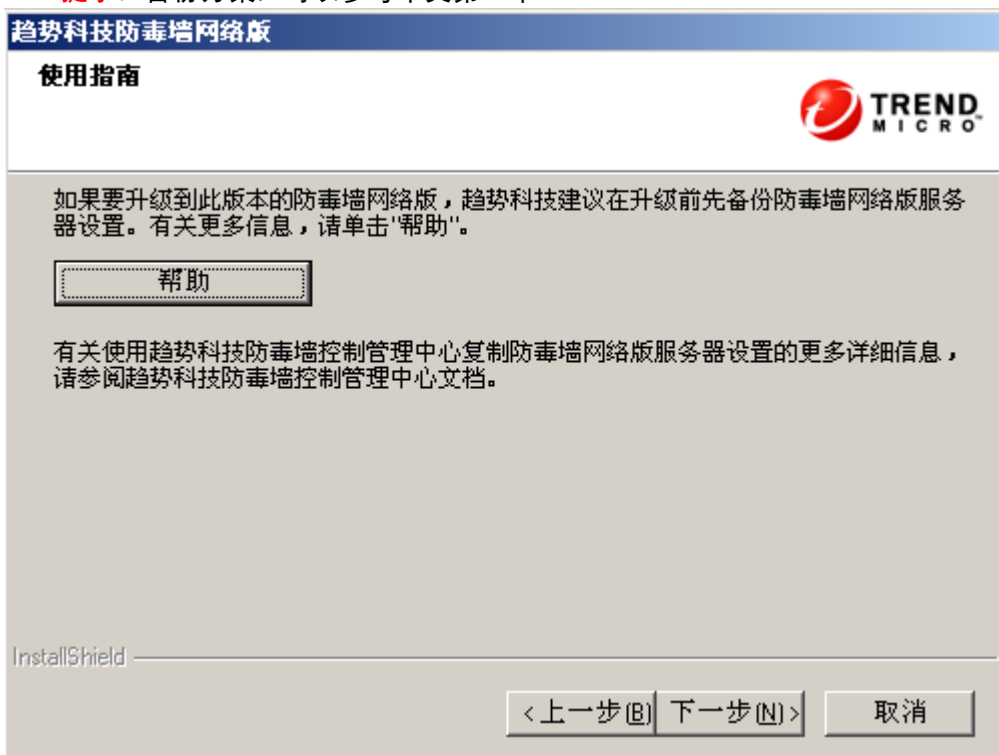
4. 提示此版本进行客户端部署估计占用网络带宽参考值

注意: Officescan10.5 版本默认将采用云安全扫描方式 (云客户端)



5. 提示如果从旧版本升级，建议升级前进行备份

提示：备份方案，可以参考本文第 5 章

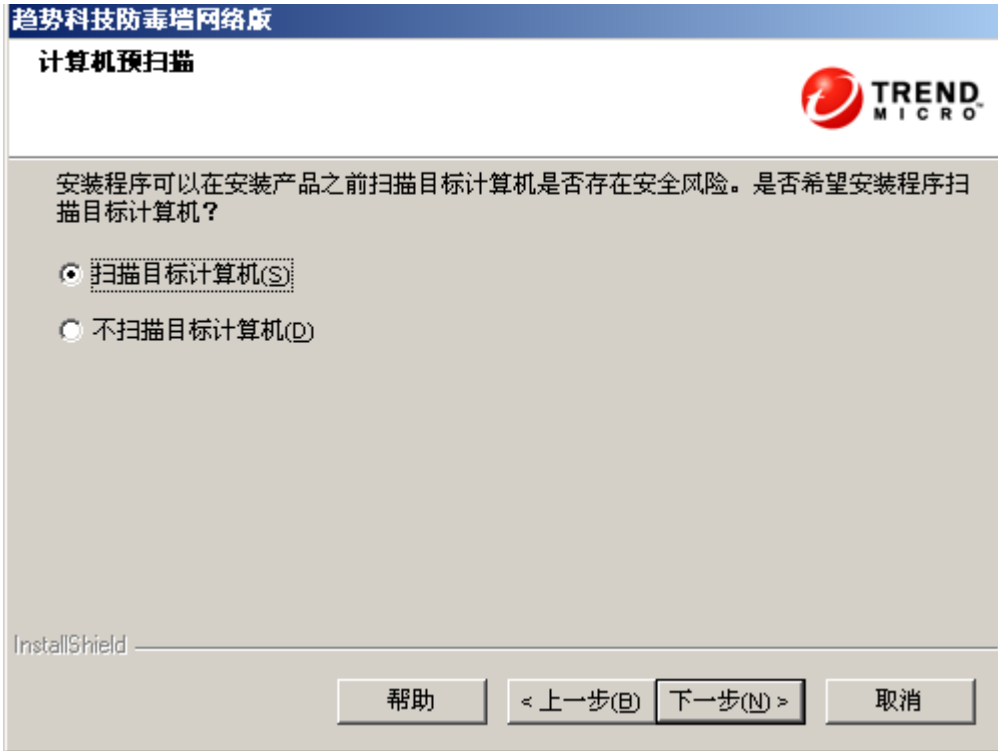


6. 选择安装目标，Officescan 10.5 支持远程安装一台或同时安装多台计算机，选择完成后点击下一步



7. 选择是否在安装前对服务器进行扫描，推荐在安装 Officescan 服务器前进行扫描，选择完

成后点下一步

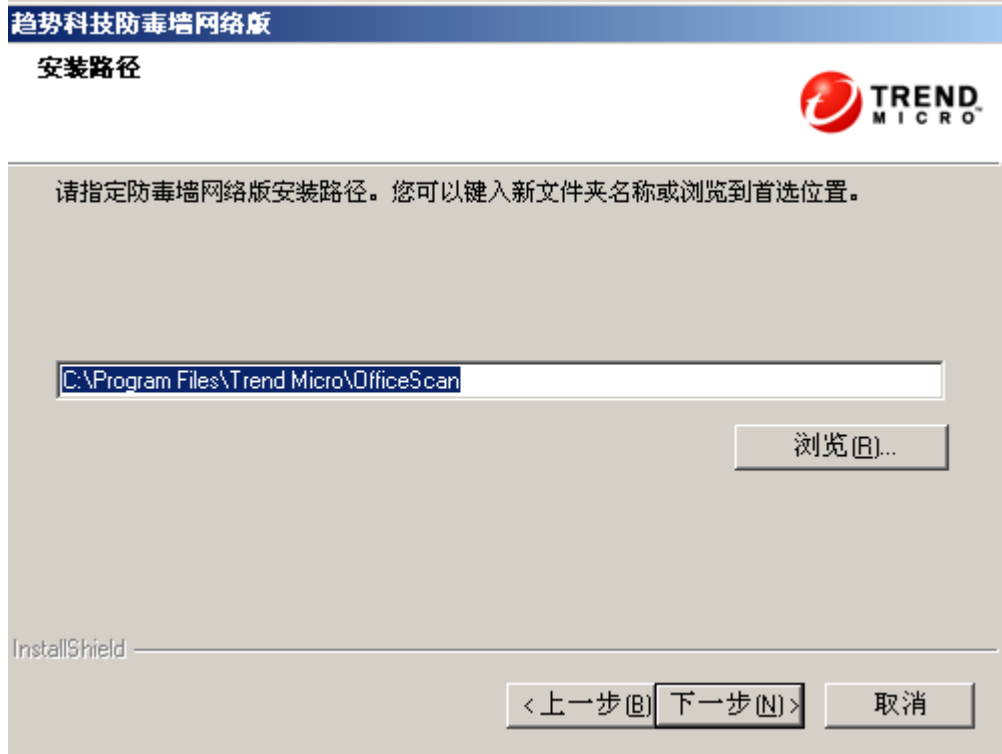


8. 扫描完成后/或不进行扫描 进入资源评估页面, 如果您的服务器被检测有不符合安装需求的配置, 安装程序将自动终止并退出



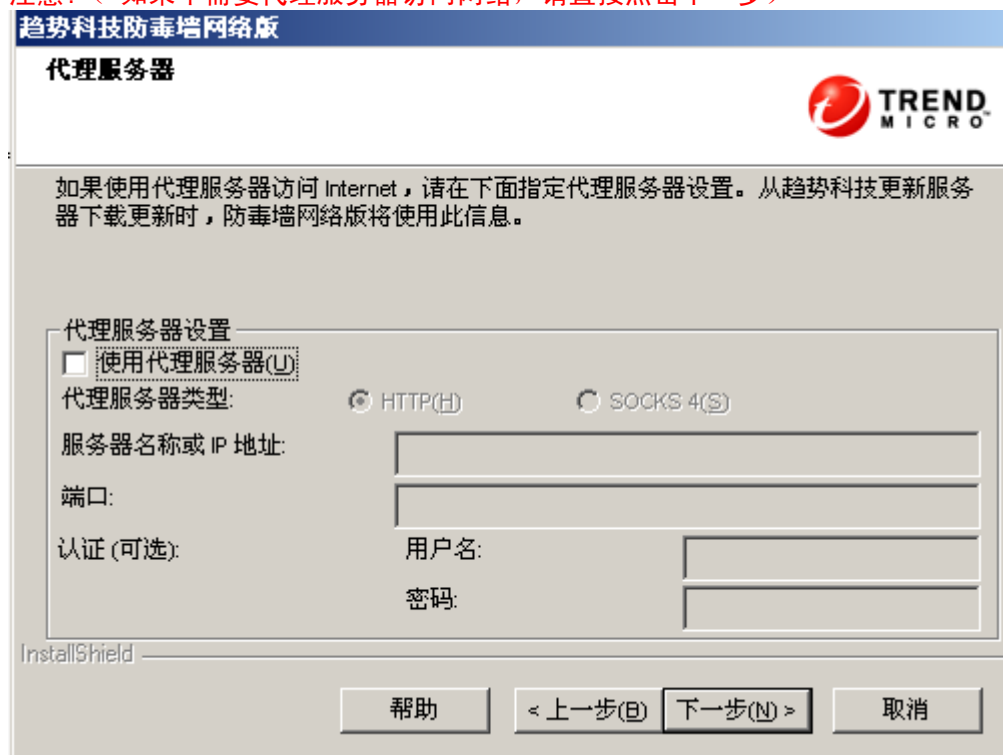
9. 选择 Officescan 服务器安装路径

注意: 由于 Officescan10.5 服务器端需存放大量客户端信息以及病毒日志, 病毒码等文件, 强烈建议将它安装在非系统盘路径下, 以避免磁盘空间不足而引起的系统问题。



10. 代理服务器设置，如果您的服务器需要通过代理访问 internet，请在此处设置代理服务器信息。使得 Officescan 10.5 服务器在安装完成后可以正常从趋势更新服务器获得最新病毒码以及更新程序，设置完成后点击下一步

注意：（ 如果不需要代理服务器访问网络，请直接点击下一步）

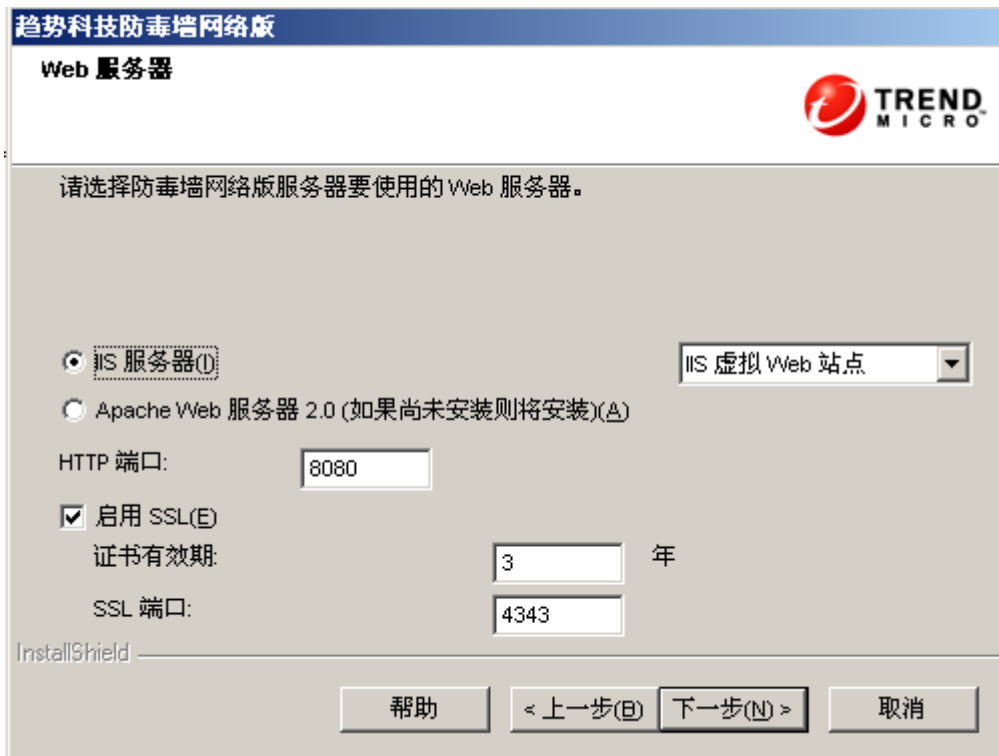


11. 选择安装的 Web 服务器，如果机器未安装 IIS，Officescan 将帮您安装最新的 Apache Web 服务器。设置完成后点击下一步

注意： 1、如果您的服务器上已存在其他的 web 站点应用建立在虚拟站点上，请注意避免选

择与该站点相同的端口，否则会引起端口冲突导致网站无法访问。

2、Apache Web 服务器 2.0.x 如果计算机中安装了非 2.0.x 版的 Apache Web 服务器，防毒墙网络版将安装和使用 2.0.63 版。但不会移除现有的 Apache Web 服务器。



趋势科技防毒墙网络版

Web 服务器

请选择防毒墙网络版服务器要使用的 Web 服务器。

IIS 服务器(I) IIS 虚拟 Web 站点

Apache Web 服务器 2.0 (如果尚未安装则将安装)(A)

HTTP 端口:

启用 SSL(E)

证书有效期: 年

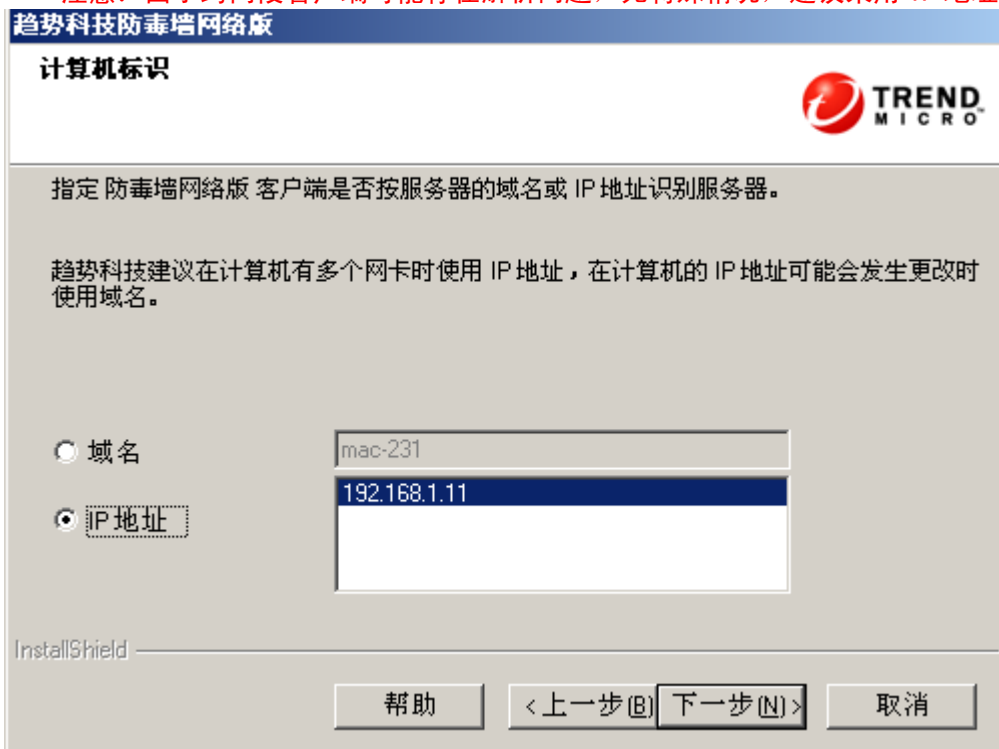
SSL 端口:

InstallShield

帮助 < 上一步(B) 下一步(N) > 取消

12. 选择 Officescan 10.5 服务器与客户端通讯所使用的标志，可以使用 IP 地址或电脑名称，可根据实际情况任意选择，选择完成后点击下一步

注意：由于跨网段客户端可能存在解析问题，无特殊情况，建议采用 IP 地址进行安装。



趋势科技防毒墙网络版

计算机标识

指定 防毒墙网络版 客户端是否按服务器的域名或 IP 地址识别服务器。

趋势科技建议在计算机有多个网卡时使用 IP 地址，在计算机的 IP 地址可能会发生更改时使用域名。

域名 IP 地址

InstallShield

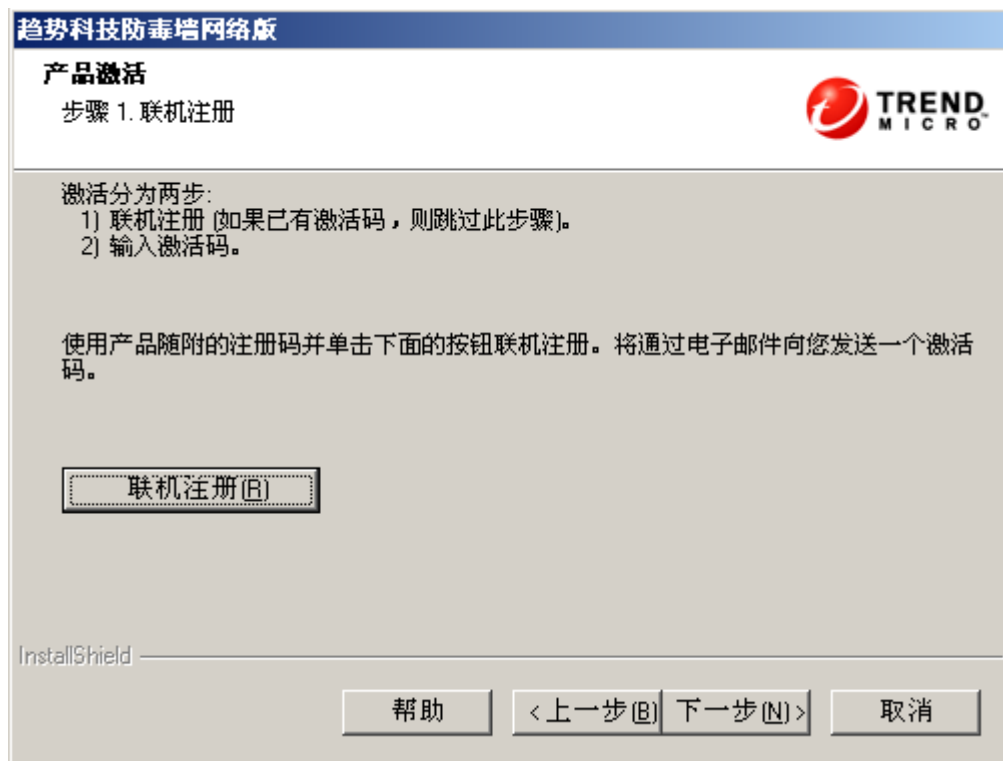
帮助 < 上一步(B) 下一步(N) > 取消

13. 进入产品激活页面

注意：如果您是试用此产品的用户，请访问以下站点进行试用注册：

http://www.trendmicro.com.cn/corporate/techsupport/online_registration/cd.asp

如果您是正式购买用户，已获得激活码请直接点击下一步

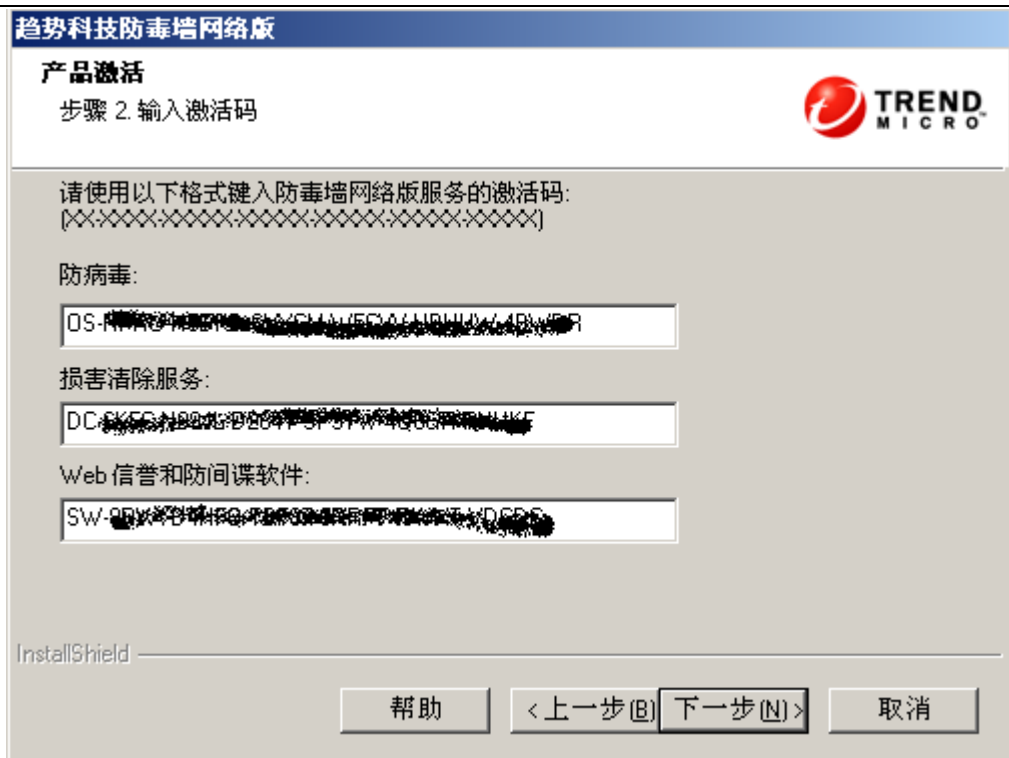


14. 输入已获得的激活码

注意： 在防病毒栏填入以 OS-XXXX 开头的激活码

在损害清除服务栏填入以 DC-XXXX 开头的激活码

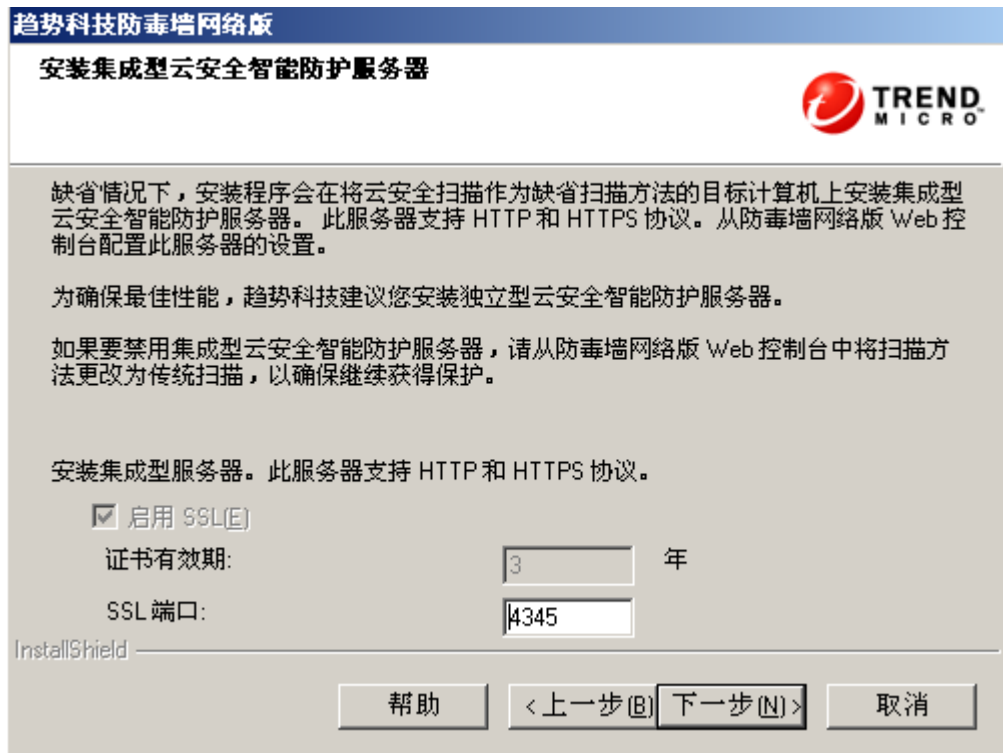
在 Web 信誉和防间谍软件栏填入以 SW-XXXX 开头的激活码。



15. 选择是否安装集成型云安全服务器

注意: Officescan10.5 默认即需启用集成性云安全智能防护服务器。

如果选择安装云安全服务器，将默认使用 web 站点的 4345 端口，可根据具体情况设置端口，以避免与其他网站应用产生端口冲突

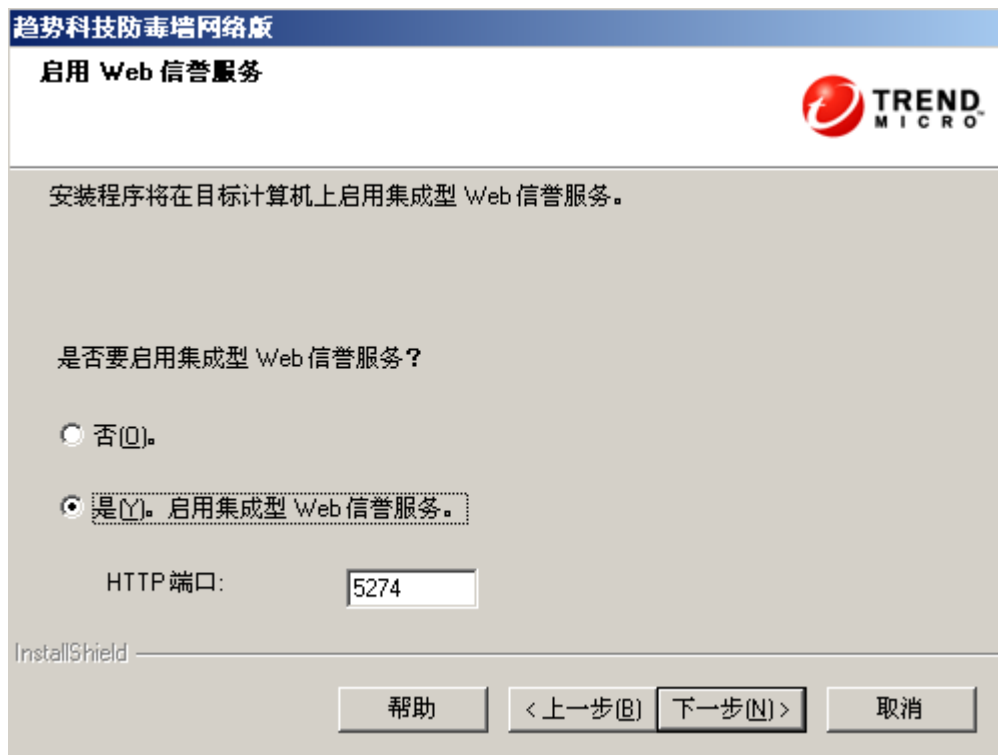


16. 启用集成性 Web 信誉服务

注意: 如果您的 Officescan 服务端与客户端都是独立内网（与 Internet 物理隔离），则可

以取消启用，否则建议启用

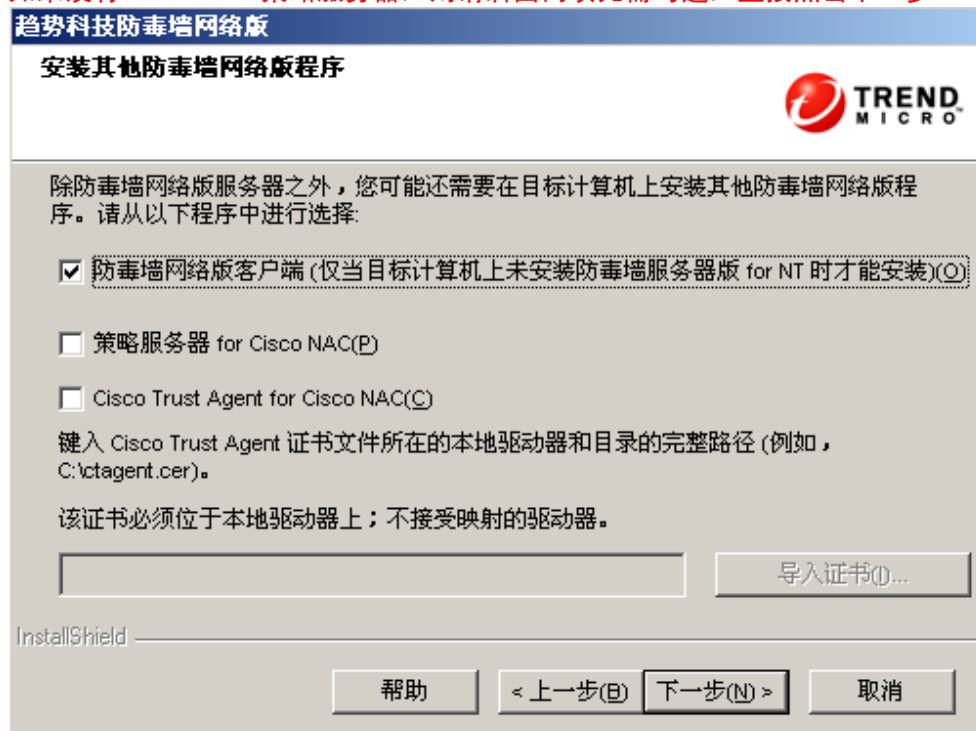
如果选择启用 Web 信誉服务，将默认使用 web 站点的 5274 端口，可根据具体情况设置端口，以避免与其他网站应用产生端口冲突



17. 选择是否在此机器上安装防病毒网络版客户端，以及 NAC 策略服务器，选择完成后点击下一步

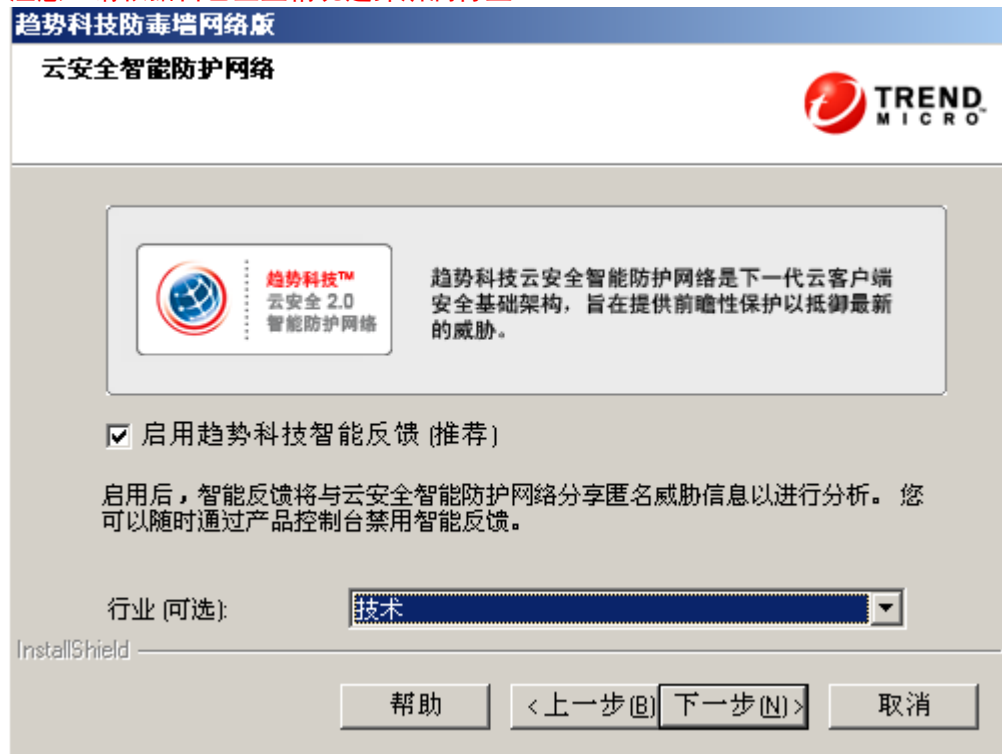
注意：Officescan 10.5 服务器并不具备防病毒功能，如果此安装服务器上并未安装其他防病毒产品，请务必选择安装防病毒网络版客户端。

如果没有 Cisco NAC 策略服务器，则请后面两项无需勾选，直接点击下一步




18. 选择是否启用云安全智能反馈


注意：请根据自己企业情况选择所属行业



趋势科技防毒墙网络版

云安全智能防护网络





趋势科技™
云安全 2.0
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安全基础架构，旨在提供前瞻性保护以抵御最新的威胁。

启用趋势科技智能反馈 (推荐)

启用后，智能反馈将与云安全智能防护网络分享匿名威胁信息以进行分析。您可以随时通过产品控制台禁用智能反馈。

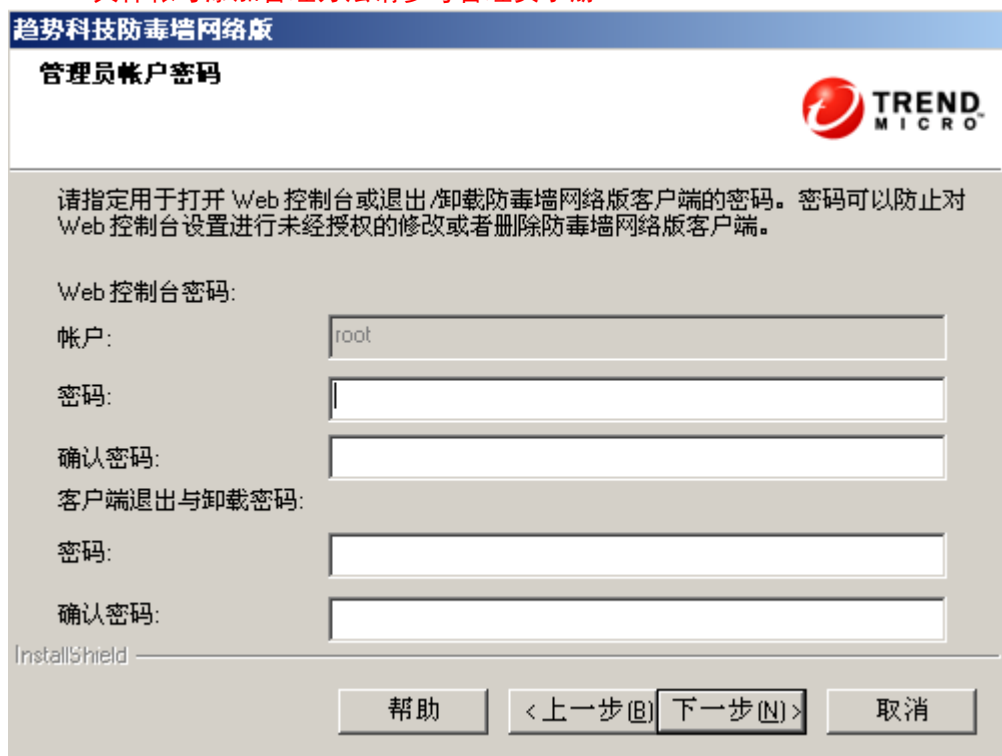
行业 (可选):

InstallShield

帮助 < 上一步(B) 下一步(N) > 取消


19. 设置登陆 Officescan 10.5 服务器控制台的帐号密码，以及客户机退出卸载密码

注意：Officescan 10.5 控制台登陆默认帐号为 root，登陆后可以添加其他管理帐号
具体帐号添加管理方法请参考管理员手册



趋势科技防毒墙网络版

管理员帐户密码



请指定用于打开 Web 控制台或退出/卸载防毒墙网络版客户端的密码。密码可以防止对 Web 控制台设置进行未经授权的修改或者删除防毒墙网络版客户端。

Web 控制台密码:

帐户:

密码:

确认密码:

客户端退出与卸载密码:

密码:

确认密码:

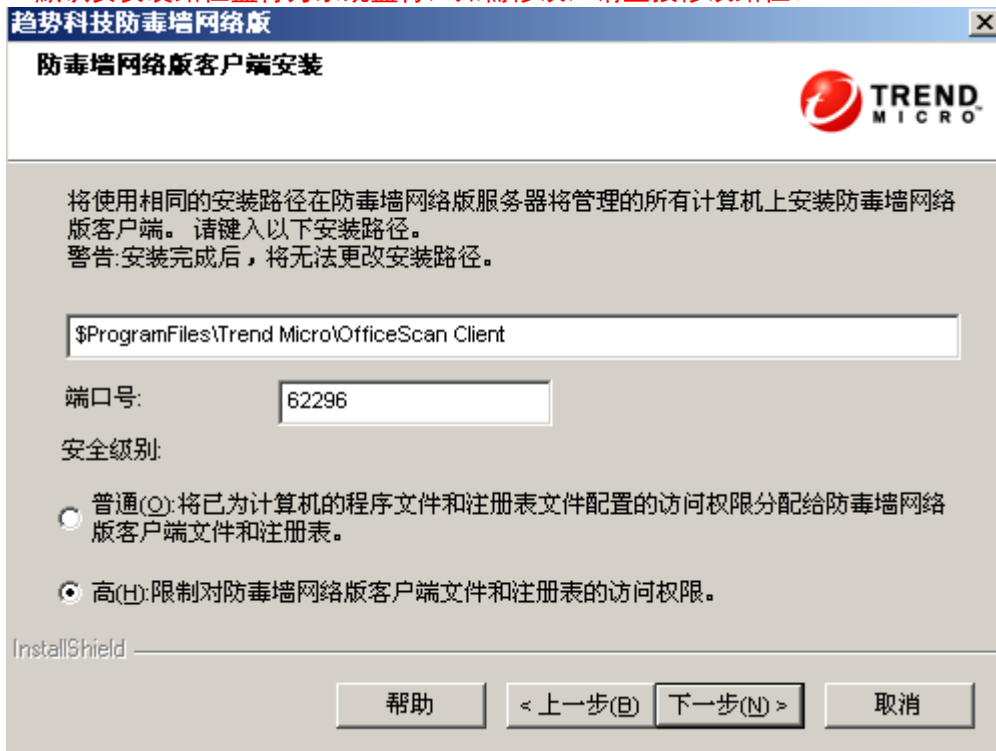
InstallShield

帮助 < 上一步(B) 下一步(N) > 取消

20. 选择 Officescan 客户端安装路径，以及与服务器进行通讯的 5 位端口，选择完成后点击下一步

注意：此通信端口为随机产生，请牢记此 5 位高位端口，以便下次重新安装 Officescan 服务端时改为此时的 5 位端口

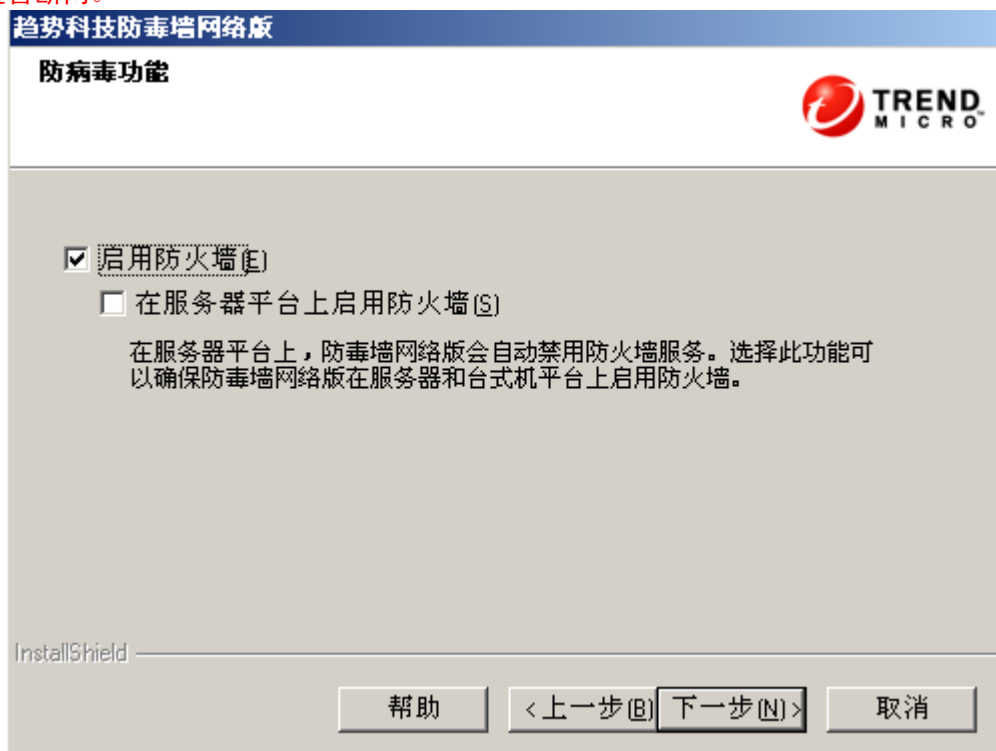
默认安装路径盘符为系统盘符，如需修改，请直接修改路径。



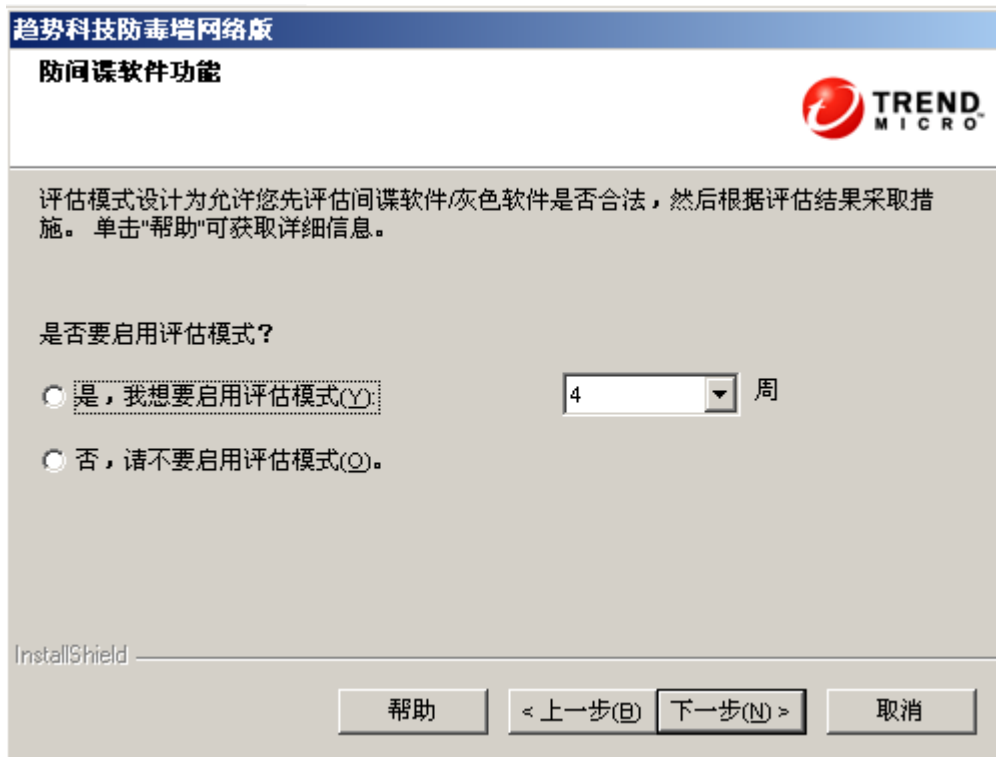
21. 选择是否启用防火墙功能（选择前请阅读以下提示！）

注意：为了确保企业服务器运行稳定，Officescan10.5 在默认情况下，不会在 Windows Server 操作系统平台上安装的客户端上启用防火墙（防病毒功能不影响）。

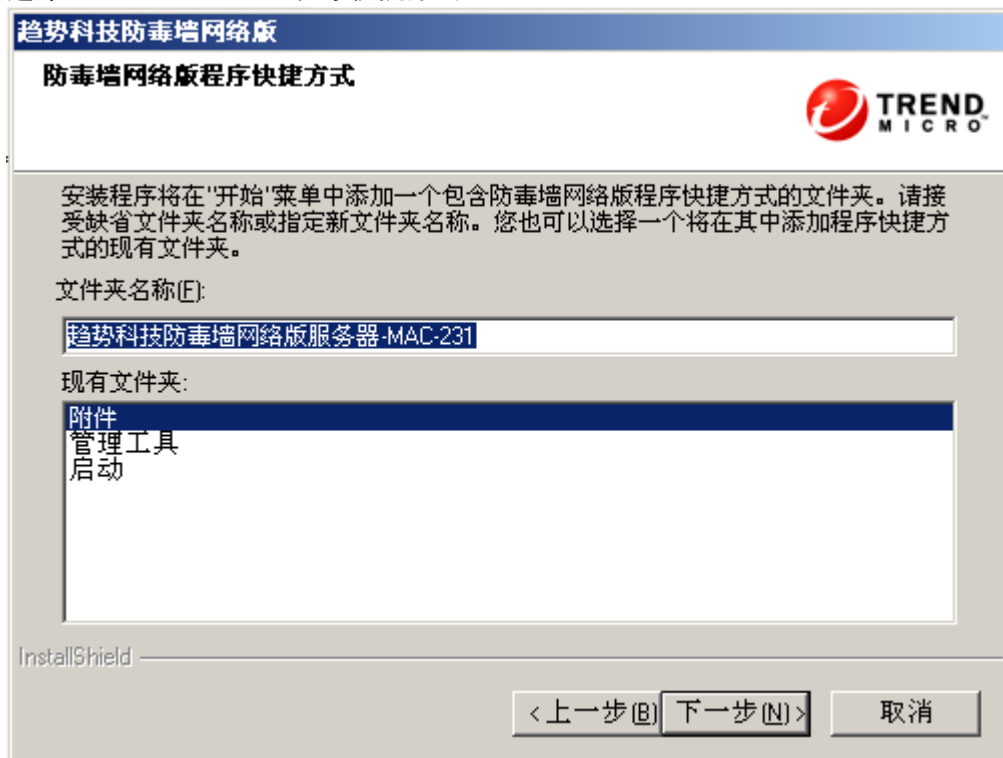
如需启用则可以勾选。启用后，在之后安装补丁等需要更新防火墙驱动，则可能会使得客户端出现短暂断网。



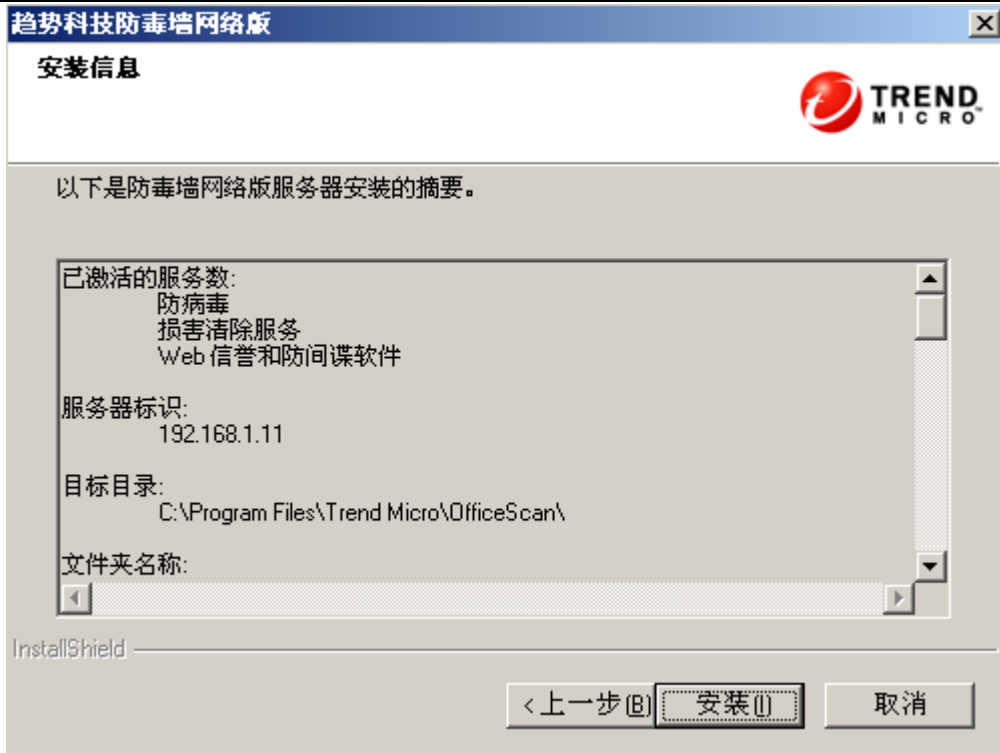
22. 进行防间谍软件功能的设置



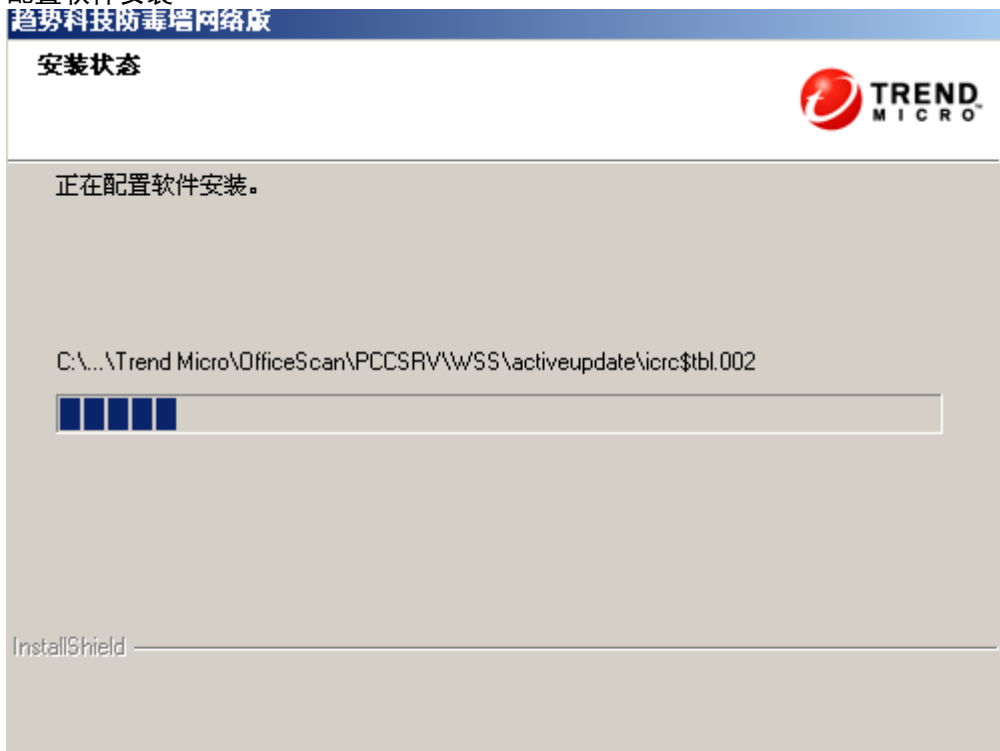
23. 选择 Officescan 10.5 程序快捷方式



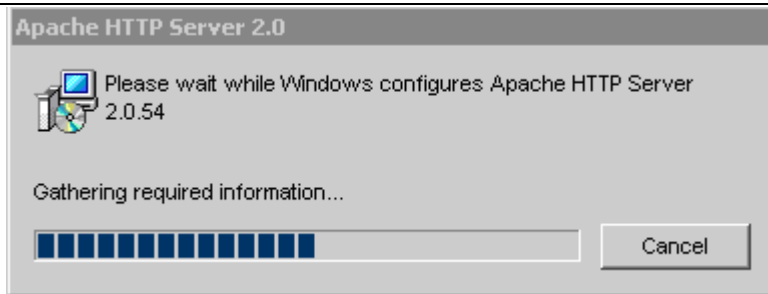
24. 显示 Officescan 10.5 安装摘要



25. 配置软件安装



26. 如果选择将 Officescan 10.5 安装在 Apache Web 服务器上，将会进行 Apache 的安装



27. 安装完成



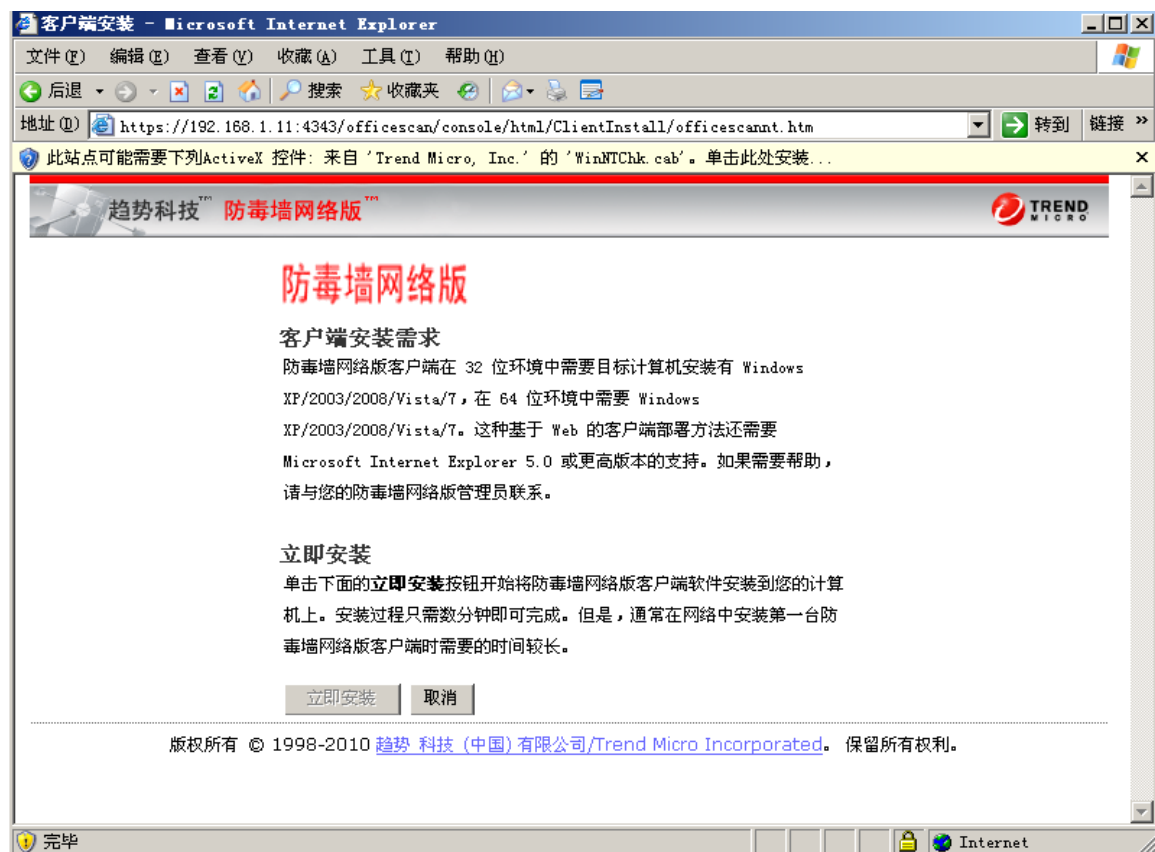
4.3 安装 Officescan 10.5 客户端

Officescan 10.5 支持多种方法安装客户端程序，一般我们使用网页安装方式进行安装。关于其他安装方式的具体操作，请参考管理员手册。

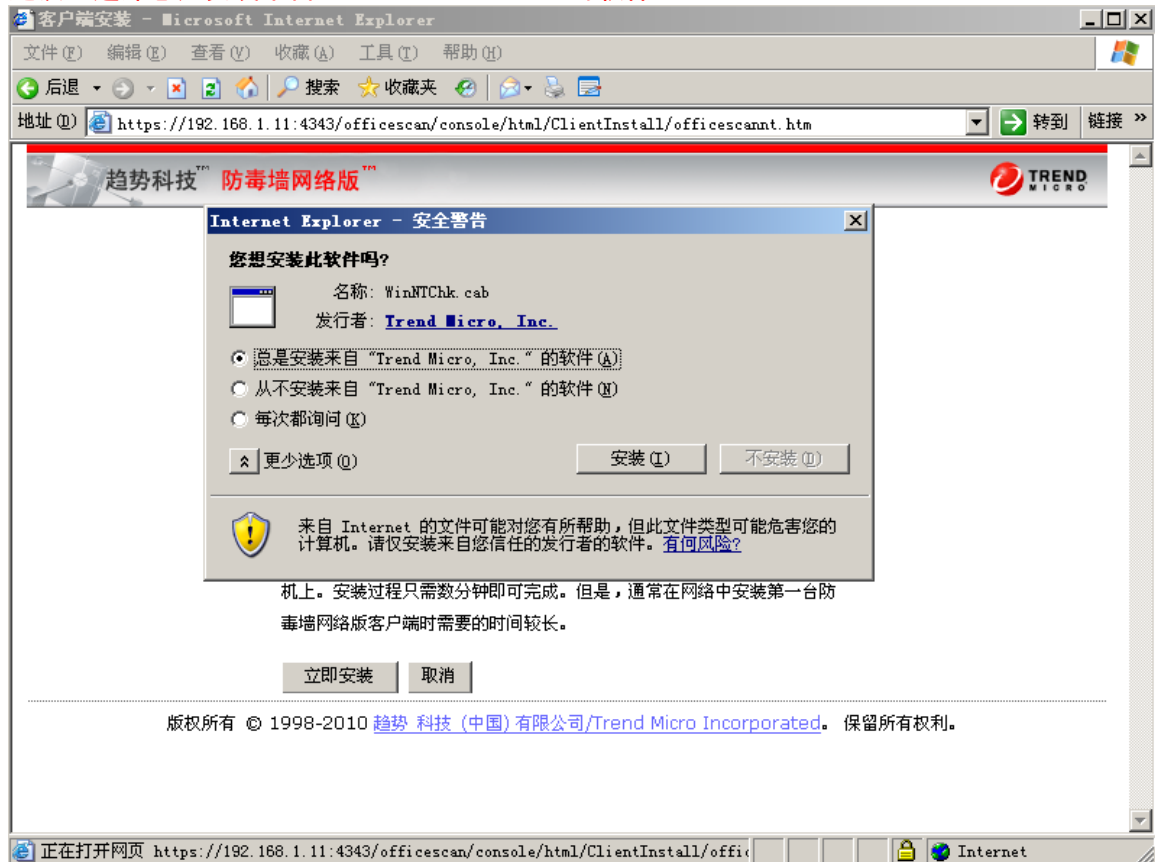
1. 打开 Officescan 10.5 服务器控制台，并点击控制台登陆窗口下方“可向用户提供以下客户端安装程序连接”下的超连接（也可将此连接直接复制到需安装客户端计算机的 IE 浏览器中打开）。



2. IE 浏览器会出现需要安装 Activex 控件的提示，请点击提示条进行安装（如浏览器无法出现提示，请检查 IE 浏览器中关于 Activex 的安全设置）



3. 进行 ActiveX 控件安装时弹出安全警告，请点击安装
建议：选择总是安装来自“Trendmicro Inc”的软件



4. 控件安装后，出现客户端安装画面，请点击立即安装



5. 安装程序开始进行



8. 安装结束，请关闭安装窗口页面

4.4 如何检查标准安装是否成功？

4.4.1 Officescan 服务器端

1. 防毒墙网络版服务器快捷方式：

服务器计算机的 Windows 开始菜单中将出现趋势科技防毒墙网络版服务器的快捷方式。



2. 程序列表：

趋势科技防毒墙网络版服务器在服务器计算机控制面板的添加/删除程序列表中列出。



3. 防毒墙网络版 Web 控制台:

在 Internet Explorer 浏览器上键入以下 URL:

- HTTP 连接: `http://<Officescan 服务器名称/IP>:<端口号>/Officescan`
- HTTPS 连接: `https://<Officescan 服务器名称/IP>:<端口号>/Officescan`

将出现 Officescan 10.5 服务器控制台登陆页面



4. 防毒墙网络版服务器服务:

在 Microsoft 管理控制台上将显示以下防毒墙网络版服务器服务:

- 防毒墙网络版主服务 (Officescan Masterservice / 应该正在运行)
- 趋势科技云安全服务器 (Trend Micro Smart Server / 如果已安装集成型云安全服务器, 启动类型为“手动”)
- 趋势科技策略服务器 for Cisco NAC (如果之前选择安装)
- 防毒墙网络版 Active Directory 集成服务 (Officescan Active Directory Intergration service / 如果基于角色的管理功能正常工作)
- Officescan 控管中心代理 (Officescan Control Manager Agent)
- 防毒墙网络版客户端提供本地 Web 分类扫描功能 (Trend Micro Local Web Classification Server/应该正在运行)。
- 防毒墙网络版客户端提供云安全扫描功能。(Trend Micro Smart Scan Server)

可从 开始- 运行 输入 `services.msc` 命令, 打开服务管理器查看

Name	Description	Status
Network Provisioning Service	Manages XML configuration files on a do...	
NT LM Security Support Provider	Provides security to remote procedure c...	
Office Source Engine	可保存用于更新和修复的安装文件，...	
OfficeScan Active Directory Integration Service	为防毒墙网络版主服务提供 Active Dir...	Started
OfficeScan Control Manager Agent	允许管理员从控制管理中心控制台管...	
OfficeScan Master Service	接受并响应防毒墙网络版客户端、We...	Started
OfficeScan NT Firewall	提供数据包级防火墙、网络病毒扫描...	
OfficeScan NT Listener	接收来自防毒墙网络版服务器的命令...	
OfficeScan NT Proxy Service	在将网络通信传递给目标应用程序之...	
OfficeScanNT RealTime Scan	对防毒墙网络版客户端执行实时扫描...	
Performance Logs and Alerts	Collects performance data from local or r...	
Plug and Play	Enables a computer to recognize and ad...	Started
Trend Micro Local Web Classification Server	为... 已启动 手动 本地系统	
Trend Micro Smart Scan Server	为... 已启动 手动 本地系统	

5. 防毒墙网络版服务器进程：

打开 Windows 任务管理器时，以下防毒墙网络版进程正在运行：

OfcService.exe

DBServer.exe

iCRCSservice.exe （如果已安装集成型云安全服务器）

OfcCMAgent.exe （如果防毒墙网络版服务器已注册到控制管理中心）

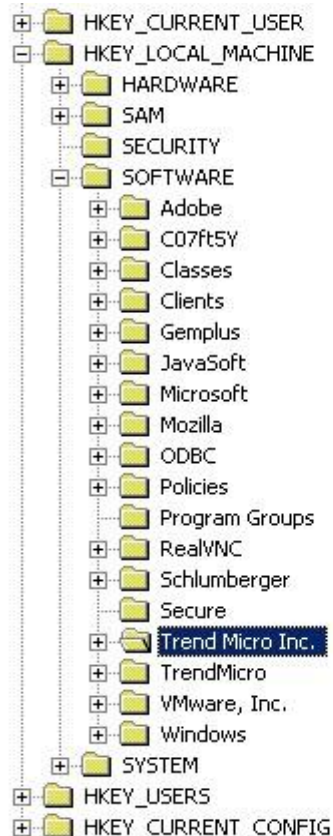
LWCSService.exe （如果已启用Web信誉服务）

6. 注册表：

存在以下注册表：

HKEY_LOCAL_MACHINE\Software\TrendMicro\Officescan

可从开始-运行 输入 regedit 命令查看：



4.4.2 Officescan 客户端

1. 客户端图标



注意：云客户端与之前传统客户端图标略有不同

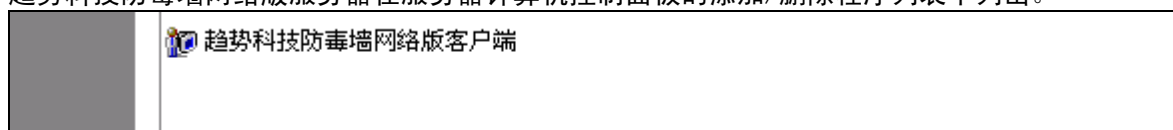
如果从OSCE7.3/8.0/10.0版本升级至OSCE10.5，则默认还是保留原有的扫描方式。

2. 防毒墙网络版客户端快捷方式：



3. 程序列表：

趋势科技防毒墙网络版服务器在服务器计算机控制面板的添加/删除程序列表中列出。



4. 防毒墙网络版客户端服务：

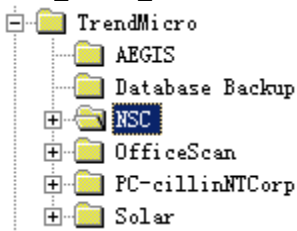
可在安装客户端的计算机上，通过 开始-运行 输入 services.msc 查看

Performance Logs and Alerts	Collects performance data from local or r...	
OfficeScanNT RealTime Scan	对防毒墙网络版客户端执行实时扫描...	Started
OfficeScan NT Proxy Service	在将网络通信传递给目标应用程序之...	
OfficeScan NT Listener	接收来自防毒墙网络版服务器的命令...	Started
OfficeScan NT Firewall	提供数据包级防火墙、网络病毒扫描...	Started
OfficeScan Master Service	接受并响应防毒墙网络版客户端、We...	Started
OfficeScan Control Manager Agent	允许管理员从控制管理中心控制台管...	
OfficeScan Active Directory Integration Service	为防毒墙网络版主服务提供 Active Dir...	Started
Uninterruptible Power Supply	Manages an uninterruptible power suppl...	
Trend Micro Unauthorized Change Prevention Service	Manages the Trend Micro unauthorized c...	

5. 防毒墙网络版客户端注册表:

可在安装客户端的计算机上，通过 开始-运行 输入 regedit 查看

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro



5. 客户端进程:

Ntrtscan.exe

Pccntmon.exe

Tmpfw.exe (如果启用防火墙)

Tmlisten.exe

TMBMSRV.exe

5 升级安装过程

5.1 升级前的注意事项

不支持的客户端操作系统

防毒墙网络版10.5 不再支持 Windows 95、98、Me、NT、Itanium以及**Windows2000** 体系结构平台。如果打算从防毒墙网络版 7.x 升级到此版本，并具有运行这些操作系统的防毒墙网络版 7.x 客户端，请参考以下建议：

1. 不要将所有的防毒墙网络版 7.x 服务器都升级到此版本的防毒墙网络版。
2. 至少指定一个防毒墙网络版 7.x 服务器(父服务器)来管理运行不支持的操作系统的客户端。
3. 在升级其他服务器之前：
 - a. 打开每个Officescan 服务器的Web 控制台，并单击主菜单上的客户端。
 - b. 从客户端树，选择要移动的客户端，然后单击移动。
 - c. 在将选定的客户端移动到另一个防毒墙网络版服务器下指定父服务器的计算机名/IP 地址和服务器侦听端口。
 - d. 单击移动。

升级期间的扫描方法部署

在此版本的防毒墙网络版中，可以将客户端配置为使用云安全扫描或传统扫描。

如果从早期版本升级防毒墙网络版服务器，并且已启用自动客户端升级，则服务器管理的所有客户端在升级后自动使用传统扫描。

在升级后，可以将所有或一定数量的客户端配置为使用云安全扫描。

有关详细信息，请参考管理员手册

语言版本升级限制：

Officescan 10.5 只支持相同语言版本的升级，例如支持从Officescan 8.0 简体中文版，升级至Officescan 10.5 简体中文版，但不支持从Officescan 8.0 英文版，升级至Officescan 10.5 简体中文版

确认Officescan 服务器版本以及配置需求

此版本的防毒墙网络版支持从以下版本升级：

- Officescan 10.X 或者10.0 SP1 简体中文版
- Officescan 8.0 With Patch 5 简体中文版 版本号3510
- Officescan 7.3 with Patch 4 简体中文版 版本号1343

- Officescan 8.0 With Patch 5 英文版 版本号3510
- Officescan 7.3 with Patch 6 英文版 版本号1405
- Officescan 7.0 with Patch 6 英文版 版本号1340

如果您的产品低于上述版本信息，请先从趋势科技网站下载并安装最新补丁，并全部部署到客户端后再进行升级。

补丁程序下载地址：

简体中文版：

<http://www.trendmicro.com/download/zh-cn/product.asp?productid=5>

英文版：

<http://www.trendmicro.com/download/product.asp?productid=5>

备注：

OSCE7.3因为已经停止提供技术支持，故OSCE7.3的补丁请从以下地址连接下载：

Officescan 7.3 英文版：

最新补丁程序：

Trend Micro OfficeScan 7.3 Corporate Edition Patch 6 - Build 1405

http://www.trendmicro.com/ftp/products/patches/OSCE_73_WIN_EN_PATCH6.exe

http://www.trendmicro.com/ftp/documentation/readme/Readme_OSCE_73_WIN_EN_PATCH6.txt

如何校验，补丁已成功部署至Officescan客户端？

补丁成功部署后，Officescan客户端程序Ntrtscan.exe的版本号为7.3.0.1405 或更新

Officescan 7.3 简体中文版：

最新补丁程序：

趋势科技防毒墙网络版 7.3 版 Patch 4

http://www.trendmicro.com/ftp/china/officescan/OSCE_73_WIN_SC_PATCH4.exe

http://www.trendmicro.com/ftp/china/officescan/OSCE_73_WIN_SC_PATCH4_Readme.txt

如何校验，补丁已成功部署至Officescan客户端？

补丁成功部署后，Officescan客户端程序Ntrtscan.exe的版本号为7.3.0.1343 或更新

关于各补丁安装方法以及注意事项请参考readme文档，或咨询趋势科技技术支持部门

此外，服务器和客户端均须满足 OFFICESCAN 10.5 服务器以及客户端系统以及配置需求，具体请参考

[Officescan 10.5 的系统需求](#)



5.2 升级前的备份

备份和恢复防毒墙网络版数据库和配置文件：

1. 打开Officescan 服务器控制台 管理-数据库备份，从Officescan 8. x/7. x 控制台备份数据库

选择备份数据库径 点击立即备份

警告！ 不要使用任何类型的备份工具或应用程序。



The screenshot shows the 'Database Backup' configuration window in the OfficeScan server console. On the left is a navigation menu with options like '立即扫描', '立即更新', '立即清除', and '管理'. The main area is titled '数据库备份' and contains the following fields and options:

- 上次数据库备份时间** (Last Database Backup Time): A table with columns for '开始时间' (Start Time), '完成时间' (End Time), '路径' (Path), and '结果' (Result).
- 备份路径:** (Please use the complete path of the OfficeScan network edition server or UNC path.)
- 帐户:**
- 密码:**
- 在不存在时创建该文件夹
- 预设数据库备份** (Predefined Database Backup):
 - 启用预设数据库备份
 - 每天一次
 - 每周一次，在
 - 每月一次，在每月的
- 开始时间:** :
- Buttons:

2. 从开始-运行 执行 services.msc 命令打开 服务管理器
将 Officescan master service 停止
3. 手动备份在<服务器安装文件夹>\PCGSRV 下找到的以下文件和文件夹：
 - ofcscan.ini: 全局客户端设置
 - ous.ini: 包括防病毒组件部署的更新源表
 - Private 文件夹: 包括防火墙和更新源设置
 - Web\tmOPP 文件夹: 包括爆发阻止设置
 - Pccnt\Common\OfcPfw2.dat: 包括防火墙设置
 - Download\OfcPfw2.dat: 包括防火墙部署设置
 - Log 文件夹: 包括系统事件和连接验证日志
 - Virus 文件夹: 包括隔离的文件
 - HTTPDB 文件夹: 包括防毒墙网络版数据库

5.3 升级安装 Officescan 10.5

5.3.1 分批升级 Officescan 客户端

通过禁用自动客户端升级，可以先升级服务器，然后升级组中的客户端。

此方法优点在于可分批升级客户机，以避免升级过程中产生的更新包流量问题，主要适用于大批量客户机升级。

升级步骤：

第一步：在防毒墙网络版10.x、8.x 或 7.x 服务器上配置更新设置和权限

对于防毒墙网络版 10.x/8.x：

1. 打开Officescan 服务器控制台 点击 **更新 > 联网计算机 > 自动更新**。
2. 不勾选以下选项：
 - 防毒墙网络版服务器下载完新组件后立即在客户机上启动组件更新。
 - 使客户机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（漫游客户机除外）。
3. 点击 **联网计算机 > 客户机管理**。
4. 点击 右侧窗口的客户端树状结构根目录 “**防毒墙网络版服务器**”
5. 单击 **设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
6. 启用 **客户机可以更新组件，但不能升级客户端程序也不能部署 Hotfix**。
7. 点击 **应用到全部客户机**。

对于防毒墙网络版 7.x：

1. 打开 Officescan 控制台 点击 **更新 > 客户机部署 > 自动部署**。
2. 不勾选以下选项：
 - 防毒墙网络版服务器下载完新组件后立即部署到客户端。
 - 重新启动客户端时部署到客户端（仅适用于防毒墙网络版客户端，漫游客户端除外）。
3. 点击控制台左侧的 **客户机**
4. 从右侧窗口的客户端树状结构，选择根目录 “**防毒墙网络版服务器**”
5. 单击 **客户机权限/设置**。
6. 在“更新设置”下，启用 **禁止程序升级和 hotfix 部署**。
7. 单击 **全部应用**。

注意： 如果网络环境复杂，并且有大量的客户端，则将设置部署到联机客户端可能需要一段时间。在升级之前，请分配足够的时间以便将设置部署到所有客户端。不应用设置的客户端将自动升级。

第二步：升级防毒墙网络版服务器

有关升级防毒墙网络版服务器具体步骤请参考本文以下章节

[4.2 安装 Officescan 10.5 服务器端](#)

注意： 在 Windows 2008 Standard 64 位服务器上升级防毒墙网络版服务器之前，请先退出防毒墙网络版客户端，以确保减少更新时间。

第三步：升级防毒墙网络版客户端

1. 转至 **联网计算机 > 客户机管理**。
2. 在客户端树上，选择要升级的客户端。通过选择域 或 域中的特定客户端 错开升级。
提示： 首先升级更新代理。通过充当其他客户端的更新源，更新代理可帮助减少定向到防毒墙网络版服务器的流量。
3. 单击 **设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
4. 取消选中 **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**。
5. 转至 **更新 > 联网计算机 > 自动更新**。
6. 启用 以下选项：
 - 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。
 - 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）。
6. 自动升级
当发生以下任一事件时联机客户端将开始升级：
 - 防毒墙网络版服务器下载新组件并通知客户端进行更新。
 - 客户端重新加载。
 - 客户端重新启动，然后连接到防毒墙网络版服务器。
 - 运行 Windows2003 和 XP Professional 的客户端计算机登录到使用登录脚本安装程序 (AutoPcc.exe) 修改其登录脚本的服务器。
 - 预设更新运行在客户端计算机上（仅适用于具有预设更新权限的客户端）。
7. 手动升级
如果上述事件都未发生，则执行以下任一任务立即升级客户端：
 - 创建并部署 EXE 或 MSI 客户端软件包。
 - 指示客户端用户在客户端计算机上运行立即更新。
 - 如果客户端计算机运行 Windows 2003、XP Professional、2008、Vista™（除 Vista Home 外的所有版本）或 7™（除 7 Home 外的所有版本），请指示用户执行下列步骤：
 - 连接到服务器计算机。
 - 导航到 \\<服务器计算机名称>\ofcscan。
 - 启动 AutoPcc.exe。
 - 如果客户端计算机运行 Windows XP Home、Vista Home 或 7 Home，请指示用户右键单击 AutoPcc.exe，然后选择以管理员身份运行。

5.3.2 利用移动 Officescan 客户端的方式,分批升级

执行防毒墙网络版 10.5 服务器的全新安装,然后将Officescan客户端移动到此服务器。移动客户端时,它们将自动升级到防毒墙网络版 10.5。

此方法优点在于,可较灵活的控制客户端的升级时间,并避免未接受到不更新补丁命令的客户端在联网后自动更新,适用于有多台服务器资源的用户

升级步骤:

第一步: 执行防毒墙网络版服务器的全新安装, 然后配置服务器设置

1. 在新计算机上执行防毒墙网络版 10.5 服务器的全新安装。有关步骤请参考 [3.2 安装 Officescan 10.5 服务器端](#)

安装防毒墙网络版后请进行如下操作:

由于 Officescan 10.5 将不再在 Windows 服务器操作系统上加载有 Officescan 防火墙的驱动程序, 请安装防毒墙网络版的服务器端后, 立刻运行以下工具以确保 Windows 服务器操作系统上的防火墙得以正常的卸载, 以确保保障服务器的网络稳定性。

<http://support.trendmicro.com.cn/TM-Product/Product/OSCE/CN/10.5/tool.zip>

2. 打开防毒墙网络版 10.5 Web 控制台, 并转至更新 > 联网计算机 > 自动更新。
3. 启用以下选项:
 - 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。
 - 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)
4. 点击 联网计算机 > 客户端管理。
5. 从右侧窗口点击 客户端树状结构 根目录
6. 单击 设置 > 权限和其他设置, 然后转至其他设置选项卡。
7. 禁用 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
8. 单击应用到全部客户端。
9. 记录Officescan 10.5 服务器控制台登陆的 URL:
HTTP 连接: <http://<Officescan 服务器名称/IP>:<端口号>/Officescan>
HTTPS 连接: <https://<Officescan 服务器名称/IP>:<端口号>/Officescan>

第二步: 升级防毒墙网络版客户端

对于防毒墙网络版 8.x:

1. 打开Officescan控制台, 转至更新 > 摘要。
2. 点击取消通知。(此步作用为 清除服务器通知队列, 这将防止将客户端移动到Officescan 10.5时出现问题)

注意: 立即执行后续步骤。

如果在移动客户端之前更新了服务器通知队列, 则客户端可能无法成功移动。

3. 点击 联网计算机 > 客户端管理。
4. 从右边窗口 客户端树状结构中 选择要升级的客户端。

提示: 首先升级更新代理。通过更新代理充当其他客户端的更新源, 可帮助减少更新病毒码

时定向到防毒墙网络版服务器的流量。

5. 单击 窗口上方 **管理客户机** 树
6. 选择“**将选定的客户机移动到另一个防毒墙网络版服务器**”
在指定服务器处填写Officescan10.5 服务器名称，端口号处填写端口号
注意：根据之前记录的url填写服务器名称/IP 以及端口号
7. 单击 **移动**。

对于防毒墙网络版 7.x:

1. 打开Officescan 控制台，单击**客户机**。
2. 从右边窗口客户机树状结构中选择要升级的客户机。
提示：首先升级更新代理。通过更新代理充当其他客户端的更新源，可帮助减少更新病毒码

时定向到防毒墙网络版服务器的流量。

3. 单击 **移动**。
4. 选择“**将选定的客户机移动到另一个防毒墙网络版服务器**”
在指定服务器处填写Officescan10.5服务器名称，端口号处填写端口号
注意：根据之前记录的url填写服务器名称/IP 以及端口号
5. 单击 **移动**。

5.3.3 Officescan 客户端全自动升级方式

在将防毒墙网络版服务器升级到此版本后，服务器将立即通知它管理的所有客户端进行升级。

优点在于，操作方便不需要做任何复杂的设置，适用于服务器管理的客户端数量很少的用户

操作步骤：

第一步：在防毒墙网络版 8.x 或 7.x 服务器上配置设置

对于防毒墙网络版 8.x:

1. 打开Officescan 控制台 转至 **更新 > 联网计算机 > 自动更新**。
2. 启用 以下选项：
 - 防毒墙网络版服务器下载完新组件后立即在客户机上启动组件更新。
 - 使客户机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(漫游客户机除外)。
3. 单击 **联网计算机 > 客户机管理**。
4. 从右侧窗口客户机树状结构中选择根目录“**防毒墙网络版服务器**”
5. 单击 **设置 > 权限和其他设置**，然后转至**其他设置**选项卡。
6. 不勾选“**客户机可以更新组件，但不能升级客户机程序也不能部署 Hotfix**”
7. 单击 **应用到全部客户机**。

对于防毒墙网络版 7.x:

1. 打开Officescan 服务器 **更新 > 客户机部署 > 自动部署**。
2. 启用 以下选项：
 - 防毒墙网络版服务器下载完新组件后立即部署到客户机。

- 重新启动客户机时部署到客户机（仅适用于防毒墙网络版客户机，漫游客户机除外）。
3. 点击控制台 **客户机** 选项
 4. 从右侧客户机树状结构选择根根目录防毒墙网络版服务器
 5. 点击客户端权限/设置。
 6. 在“更新设置”下，不勾选 **禁止程序升级和 hotfix 部署**。
 7. 点击全部应用。

第二步：升级防毒墙网络版服务器

在新计算机上执行防毒墙网络版 10.5 服务器的全新安装。有关步骤请参考 [4.2 安装 Officescan 10.5 服务器端](#)

第三步：升级客户端

在服务器升级完成后，联机客户端会立即升级。

脱机客户端变为联机状态时将升级。

漫游客户端变为联机状态时，或者运行预设更新时（如果客户端具有预设更新权限将升级

5.4 如何检查升级安装是否成功

5.4.1 Officescan 服务器端

请参考 [4.4.1 Officescan 服务器端](#)

5.4.2 Officescan 客户端

请参考 [4.4.2 Officescan 客户端](#)

6 其他设置及常见问题

6.1 Officescan 10.5 使用的网络通讯端口

防毒墙网络版使用 HTTP 端口（缺省情况下，8080）作为服务器上的通讯端口

在安装过程中，可输入不同的服务器通讯端口号。

在安装过程中，主安装程序随机生成客户端可信端口。

确定通讯端口：

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=80，这表示服务器上的端口为 80
如果使用HTTPS，搜索字符串“Master_SSLPort=”，然后检查与该字符串相邻的值
例如，如果字符串显示为“Master_SSLPort=443”，这表示服务器上的https端口为443
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，这表示客户端上通讯端口为41375
5. 如果启用集成的云安全服务器，客户端默认与云安全服务器连接端口为
http: 8082
https: 4345（此端口根据Officescan 服务器端口设置）

6.2 如何恢复使用传统防病毒扫描？

1. 登录到 Officescan10.5 控制台。
2. 单击联网计算机-客户端管理。
3. 在右边窗口选择要启用云安全扫描模式的客户机或者客户机组
4. 窗口上方单击 设置-扫描方法
5. 选择 传统扫描

6.3 针对 OSCE10.5 新功能的简单介绍和设定

6.3.1 客户端多层次分组

分组介绍

OSCE10.5支持两层模式的客户端分组。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。

客户端分组方法：

方法	客户端分组	描述
手动	NetBIOS 域 ActiveDirectory 域 DNS 域	防毒墙网络版仅在客户端全新安装时使用此设置。 安装后，手动管理分组在其下的域和客户端。
自动	定制客户端组	定期检查目标计算机的域并将其映射到防毒墙网络版域。发生特定事件时，防毒墙网络版可自动将客户端移动到相应的防毒墙网络版域。

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。安装程序检查目标计算机所属的网络域。

1. 如果客户端树上已存在该域名：

防毒墙网络版会将目标计算机上的客户端分组到该域下，并应用为该域配置的设置。

2. 如果该域名不存在：

则防毒墙网络版将该域添加到该客户端树上，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。

手动客户端分组

配置手动客户端分组

1、打开OSCE的Web控制台不，登录

2、“联网计算机” > “客户端分组”

指定客户端分组方法：

NetBIOS 域

Active Directory 域

DNS 域

3、单击保存。

自动客户端分组

在防毒墙网络版OSCE上设定连接的Active Directory 域或 IP 地址。防毒墙网络版定期检查计算机的 Active Directory 域或 IP 地址并将客户端映射到防毒墙网络版域。

要简化防毒墙网络版域管理，可以执行下列操作之一：

- 创建自动客户端分组时复制 Active Directory 结构
- 使用 Active Directory 对象或 IP 地址创建全新的结构

创建自动客户端分组后，您可以手动排序客户端。

要自动分组客户端，请执行以下操作：

- 1、打开OSCE的Web控制台，登录
- 2、“联网计算机” > “客户端分组”
- 3、选择定制客户端组
添加 Active Directory 组
添加 IP 地址组
- 4、通过选择一个客户端组并单击箭头在列表中上下移动组来定义客户端分组优先级。客户端组的 ID 号将更改以反映新位置。执行此操作，以便如果一个客户端属于两个客户端组，防毒墙网络版将该客户端移动到等级较高的客户端组。
通过选择一个客户端组并单击箭头在列表中上下移动组来定义客户端分组优先级。当如果一个客户端属于两个客户端组，防毒墙网络版将该客户端移动到等级较高的客户端组。

例如，客户端分组有两条规则：

- 分组 1 将所有管理员都映射到“管理员”域。
- 分组 2 将 IP 地址介于 192.1.1.1 到 200.1.1.1 之间的所有计算机都映射到“待定”。

由于分组 1 比分组 2 具有更高的优先级，因此，防毒墙网络版将 IP 地址为 192.123.123.123 的客户端计算机 US 管理员映射到“管理员”域而不是“待定”域。

6.3.2 将 OSCE 服务端与 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，并确定哪些端点未安装安全软件。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：

- 1、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
- 2、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
- 3、外部服务器管理：确保不受防毒墙网络版服务器管理的网络中的计算机符合贵公司的安全准则
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。

将 Active Directory 与防毒墙网络版集成

- 1、打开OSCE的Web控制台，登录
- 2、转到管理 > ACTIVE DIRECTORY > ACTIVE DIRECTORY 集成
- 3、在 Active Directory 域下，指定 Active Directory 域名。
- 4、如果防毒墙网络版服务器不是网络的一部分，则单击输入域凭证，然后键入域凭证和加密密钥。
- 5、在打开的窗口中，键入防毒墙网络版将用于查询 Active Directory 域的用户名和密码
注意：请确保域凭证未过期
- 6、（可选）单击“加”按钮（）输入多个 Active Directory 域或“减”按钮（）删除 Active Directory 域。分别指定各个域凭证。
- 7、为了获得额外的安全性，请指定一个加密密钥和文件，供防毒墙网络版在防毒墙网络版数据库中存储域凭证时用来将纯文本转换成密码文本。此加密密钥支持所有文件格式。
- 8、单击下列操作之一：
 - 保存：仅保存信息。在重要营业时间更改设置后选择此选项。

• 保存并同步 Active Directory: 保存并同步 Active Directory。在非重要营业时间更改设置后选择此选项。

9、 (可选) 预设 Active Directory 域与防毒墙网络版数据库的定期同步。

6.3.3 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。这种分离的使用授权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

注意: 此功能需要单独授权

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 服务器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。

趋势科技虚拟桌面支持下列平台:

- VMware vCenter™ 4 (VMware View™ 4)
- Citrix™ XenServer™5.5 (Citrix XenDesktop™ 4)

关于设定, 详情可以参考管理手册

6.4 如何关闭 Officescan 10.5 客户端的 AEGIS 来解决机器运行缓慢的问题

- 1, 打开 ofcscacn.ini 文件, C:\Program Files\Trend Micro\Officescan\PCGSRV 下面
- 2, 找到 EnableBM, 设置成为 0
- 3, 找到 EnableAEGIS=1, 设置成 0
- 4, 进入 Officescan 控制台, 进入全局客户端设置, 保存

6.5 安装 Officescan 10.5 客户端的防火墙后, 原系统中的 Vmware 客户机无法正常通讯

1. 在客户端计算机上, 打开注册表编辑器。
2. 添加以下注册表值:
[HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\PFW
对于 x64 计算机:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\TrendMicro\PC-cillinNTCorp\CurrentVersion\PFW
名称: EnableBypassRule
类型: REG_DWORD

值： 1

3. 重新加载客户端，以使设置生效。

7 趋势科技厂商资源

800 免费技术支持热线

800-820-8839

800 免费商务热线

800-820-8876

售后电子邮件地址

service@trendmicro.com.cn

趋势科技中文网站

<http://cn.trendmicro.com/cn/home/>

病毒查询

www.trendmicro.com.cn/vinfo

趋势科技英文网站

<http://us.trendmicro.com/us/home/>

趋势科技病毒递交信箱

virus_doctor@trendmicro.com.cn