TREND MICRO™

趋势科技™ 远程管理器™

版本：2018 年 1 月

管理员指南

Security Management

文档编号：APCMS8158/180130

发布日期：2018 年 1 月

受美国专利号保护： 正在申请专利。

本文档介绍服务的主要功能和/或提供针对生产环境的安装说明。在安装或使用服务之前，请详细阅读。

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

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

请在以下站点评估此文档：

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

目录

部分 III：管理趋势科技产品

第 4 章：远程管理器中的 Cloud App Security

第 5 章：远程管理器中的 Cloud Edge

第 6 章：远程管理器中的 Hosted Email Security

第 7 章：远程管理器中的 InterScan Web Security as a Service

第 8 章：远程管理器中的安全无忧软件

第 9 章：远程管理器中的安全无忧软件-云端版

部分 IV：集成第三方解决方案

第 10 章：AutoTask 支持

第 11 章：ConnectWise Manage 支持

第 12 章：ConnectWise Automate 支持

第 13 章：Kaseya 支持

部分 V：监控客户

第 14 章：了解控制台

第 19 章：技术支持

索引

部分 I

远程管理器简介

第 1 章

简介

本节包含以下主题：

趋势科技™远程管理器™

趋势科技™远程管理器™ 是一款与 Trend Micro Licensing Management Platform™ 平行的功能强大的控制台，为中小企业提供托管安全服务。

趋势科技远程管理器 使您可以通过多个托管产品和服务来监控多个托管网络的运行状况。趋势科技远程管理器允许经销商的管理员通过输入命令来管理网络安全的各个重要方面。

趋势科技远程管理器托管在当地的趋势科技数据中心服务器上，经销商需要从该服务器获取帐户。经销商可以使用趋势科技远程管理器来建立客户帐户，监控客户网络，并使用趋势科技远程管理器 Web 控制台来管理安全性。

远程管理器提供了客户网络的结构化视图，允许经销商输入命令并管理网络安全的以下方面：

- 组件更新和托管服务器的更新
- 漏洞检查
- 损害清除
- 自动爆发响应
- 防火墙和实时扫描设置
- 手动扫描

趋势科技远程管理器还支持全面的报告功能，允许经销商为个人订阅自动生成的报告。

新增功能

发行日期： 2018 年 1 月

下表概述趋势科技™远程管理器™中的新功能和增强功能。

功能	描述
ConnectWise Manage 集成增强功能	升级后的集成支持 RESTful API 和嵌入式远程管理器控制台。 有关更多信息，请参阅 ConnectWise Manage 支持 第 11-1 页。
适用于 ConnectWise Automate 的安全无忧软件-云端版插件的增强功能	升级后的插件支持自动部署安全客户端、重试脚本执行，以及针对不成功的命令提交票证。 有关更多信息，请参阅 ConnectWise Automate 支持 第 12-1 页。
适用于 Kaseya 的安全无忧软件-云端版插件的增强功能	升级后的插件支持模板分配、命令执行状态、自动部署安全客户端、重试脚本执行，以及针对不成功的命令提交票证。 有关更多信息，请参阅 Kaseya 支持 第 13-1 页。
远程管理器控制台配置选项	• 远程管理器控制台的可配置会话超时 • **通知中心**的新事件类型过滤器 • **客户**窗口会保存您的分类首选项，并在您下次访问该窗口时予以显示

功能

趋势科技远程管理器提供了以下功能。

表 1-1. 远程管理器功能

功能	描述
集成的平台	远程管理器是与 Trend Micro™ Licensing Management Platform 平行的产品，但是界面更加强大。您可以通过远程管理器门户执行以下操作： • 创建新帐户 • 为帐户续订使用授权 • 添加更多座席

功能	描述
	远程管理器还通过和在托管服务器上运行的远程管理器客户端通信，来从单个控制台监控和管理多个受保护的网络。此外，远程管理器还能提供基于关键安全指标的事件监控。
控制台小组件	定制控制台页面上的小组件。利用这些小组件，您可以知道自己是否需要续订使用授权、添加更多分配的座席，甚至了解哪些客户遇到的威胁最多。
可为新帐户自定义的设置	创建帐户时，您可以为新帐户自定义在缺省情况下使用的基本缺省设置，或从您已配置并保存的模板中选择。

安全状态	远程管理器 **事件**窗口提供了网络安全的以下方面的状态：
	• 安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版
	  • 反垃圾邮件
	  • 行为监控
	  • 设备控制（仅限版本 7.x、8.x 和 9.x）
	  • 网络病毒
	  • 爆发防御
	  • 间谍软件/灰色软件
	  • URL 过滤（仅版本 6.x 和更高版本）
	  • 病毒/恶意软件
	  • Web 信誉
	• 安全无忧软件-云端版
	  • 应用程序控制
	  • 行为监控
	  • 网络病毒
	  • 爆发防御
	  • 预测型机器学习
	  • 间谍软件/灰色软件
	  • URL 过滤

功能	描述
	• 病毒/恶意软件 • Web 信誉 • Hosted Email Security • 已接受的电子邮件大小 • 威胁摘要 • 收到垃圾邮件最多的收件人 • 收到病毒最多的收件人 • 电子邮件总流量 • Cloud App Security • 防病毒 • 文件阻止 • 沙盒平台 • Web 信誉 • Cloud Edge • 僵尸网络 • C&C 回调 • 入侵防御系统 (IPS) • 预测型机器学习 • 勒索软件 • 间谍软件/灰色软件 • 沙盒平台 • 病毒/恶意软件 • Web 信誉 • InterScan Web Security as a Service • 防间谍软件

功能	描述
	• 应用程序控制 • 防病毒 • URL 过滤 • Web 信誉 远程管理器提供了有关这些方面的详细信息，包括受感染计算机的数量和病毒/恶意软件事件的数量等统计数据。经销商管理员还可以查看受感染计算机名称或威胁名称等详细信息。
系统状态	经销商管理员可以通过远程管理器“事件”窗口查看网络安全与系统相关的以下方面： • 云安全智能防护服务 • 组件更新 • 磁盘空间不足 • 设备或客户端脱机 • 云电子邮件扫描可用性 • AD/LDAP 同步问题 • 固件更新 • 资源不足 • 帐户同步问题
使用授权状态	经销商管理员可以查看与使用授权相关的以下详细信息： • 已购买的座席总数 • 正在使用的座席数 • 使用授权已到期（包括到期日期） • 使用授权将到期（包括过期之前的天数）
网络管理	远程管理器提供了客户网络的结构化视图，允许经销商管理员输入命令并管理网络安全的以下重要方面： • 组件更新和托管服务器的更新 • 漏洞检查

功能	描述
	• 自动爆发响应 • 损害清除 • 防火墙和实时扫描设置 • 手动扫描
报告	除了提供有关安全事件的通知之外，远程管理器还可以定期自动生成并发送报告。您可以根据客户、产品、频率和内容来定义报告，并能以多种格式保存报告。
与第三方工具集成	通过第三方工具（包括 Autotask™、Kaseya™ 或 ConnectWise™）实现日志监控，规范您监控的任务和过程。
提交反馈	趋势科技希望为用户提供最好、最有用的平台。然而，趋势科技不知道哪些服务或功能对您最重要。因此，远程管理器欢迎您通过**提交反馈**按钮（可在横幅上找到和使用）提供反馈和建议。趋势科技随后会对反馈进行处理，并据此确定哪些功能对用户最有帮助。

浏览器要求

- 连接到 Internet
- 趋势科技提供的远程管理器帐户信息
- 支持的浏览器：
  - 最新版本的 Google™ Chrome™ 浏览器（推荐）
  - 最新的 Firefox™ 版本
  - Microsoft Edge
  - Internet Explorer™ 11

支持的产品

下表列出了趋势科技远程管理器可以监控的趋势科技产品和产品版本。

产品	支持的版本
Trend Micro Cloud App Security	最新版本 有关更多信息，请参阅远程管理器中的 Cloud App Security 第 4-1 页。
Trend Micro Cloud Edge	最新版本 有关更多信息，请参阅远程管理器中的 Cloud Edge 第 5-1 页。
Trend Micro Hosted Email Security™	最新版本 有关更多信息，请参阅远程管理器中的 Hosted Email Security 第 6-1 页。
Trend Micro InterScan Web Security as a Service™	最新版本 有关更多信息，请参阅远程管理器中的 InterScan Web Security as a Service 第 7-1 页。
安全无忧软件™-网络安全版（以前称为客户端服务器套件）	6.x、7.x、8.x、9.x 有关更多信息，请参阅远程管理器中的安全无忧软件 第 8-1 页。
安全无忧软件-邮件与网络安全版（以前称为客户端服务器邮件套件）	6.x、7.x、8.x、9.x 有关更多信息，请参阅远程管理器中的安全无忧软件 第 8-1 页。
安全无忧软件-云端版	最新版本 有关更多信息，请参阅远程管理器中的安全无忧软件-云端版 第 9-1 页。

趋势科技远程管理器还与以下第三方工具集成，提供管理您的趋势科技产品的其他方法：

第三方工具	参考
Autotask™	AutoTask 支持 第 10-1 页
ConnectWise Automate™	ConnectWise Automate 支持 第 12-1 页
ConnectWise Manage™	ConnectWise Manage 支持 第 11-1 页
Kaseya™	Kaseya 支持 第 13-1 页

整体基础架构

趋势科技远程管理器包含 3 个基本主题：

- 合作伙伴
- 趋势科技数据中心
- 客户网络

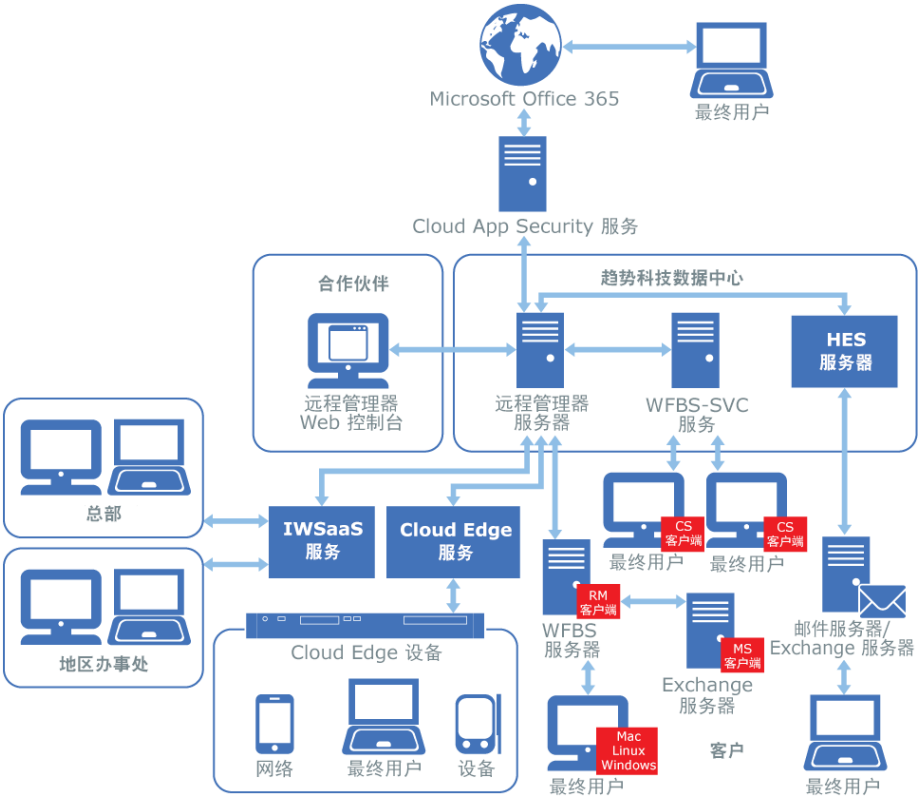


图 1-1. 远程管理器整体体系结构

合作伙伴使用远程管理器 Web 控制台通过 Internet 访问 趋势科技 数据中心（当前遍布于不同洲）。合作伙伴使用该产品不需要预先安装任何其他产品。合作伙伴必须在远程管理器 Web 控制台上添加每位客户并对其进行配置，然后才能管理客户帐户。

每个“安全无忧软件-网络安全版”和“安全无忧软件-邮件与网络安全版”托管服务器都安装了远程管理器客户端，可与远程管理器服务器相互往来通信。远程管理器客户端（可通过远程管理器 Web 控制台安装）在客户网络内的“安全无忧软件-网络安全版”和“安全无忧软件-邮件与网络安全版”托管服务器上运行。远程管理器客户端向远程管理器服务器发送信息，您可以通过 Internet 连接在该服务器中随时访问控制台的数据。

安全无忧软件-云端版 (WFBS-SVC) 和 Hosted Email Security (HES) 均托管在 趋势科技 数据中心。InterScan Web Security as a Service (IWSaaS)、Cloud App Security (CAS) 和 Cloud Edge (CE) 均托管在云中。WFBS-SVC、HES、IWSaaS、CAS 和 CE 均可将数据直接发送至远程管理器服务器。

关键术语

了解以下术语可帮助您更高效地使用远程管理器：

术语	定义
客户端	此程序安装在安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版服务器上，允许远程管理器监控和管理安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版。
检查	定期检查从客户网络收集的数据，以确定被监控网络的运行状况；这些检查使用一些称为“检查指标”的关键指标。
检查指标	安全检查的基础；经销商管理员可以分别定制这些指标，以控制检查间隔、范围和通知。
网络安全客户端 (CSA)	向安全无忧软件服务器进行报告的客户端。CSA 会实时发送事件状态信息。客户端报告威胁检测、客户端启动、客户端关闭、开始扫描以及更新完成等事件。CSA 提供三种扫描方法：实时扫描、预设扫描和手动扫描。您可以从 Web 控制台配置客户端扫描设置。
控制台	远程管理器中的控制台是主要屏幕（**主页**选项卡），其中显示 Web 控制台和小组件。
检测	发现威胁；检测到威胁并不意味着系统受到感染，只表示恶意软件已侵入计算机。如果在不同计算机上检测到同一威胁，则表示威胁已爆发。
事件	在监控域中发生的情况。
全局唯一标识符 (GUID) 或授权码	在计算机软件中用作标识符的唯一参考号。

术语	定义
感染	威胁能够在计算机中爆发的一种情形；防病毒扫描程序一旦检测到病毒/恶意软件，并且无法清除、删除或隔离该威胁，远程管理器即会视为已发生感染。如果计算机无法完全清除威胁（除非重新启动），则表明已经发生间谍软件/灰色软件感染。
受管产品/服务	远程管理器支持的任何趋势科技产品或服务
邮件安全客户端 (MSA)	位于 Microsoft Exchange Server 上的客户端，向中小企业网络与邮件安全版和安全无忧软件-邮件与网络安全版服务器报告。此客户端将防御病毒/恶意软件、特洛伊木马、蠕虫及其他电子邮件附带的威胁。还提供垃圾邮件阻止、内容过滤和附件阻止功能。
经销商	泛指那些在远程管理器中直接向客户提供安全监控和管理服务的组织。
经销商管理员	经销商方面的管理员，他们使用远程管理器执行与服务相关的任务。
趋势科技数据中心	趋势科技监控和管理中心，用于托管远程管理器（和 Hosted Email Security）并为经销商管理员提供支持。
安全管理服务器	安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版服务器计算机。
病毒警报	由 TrendLabs℠ 告知的一种警戒状态，告知客户网络做好应对病毒爆发的准备；TrendLabs 可针对各种趋势科技产品发出警报，并提供预防性解决方案，在特征码变为可用之前，IT 管理员可以实施这些解决方案作为第一道防线。
病毒爆发	病毒威胁快速传播到不同计算机和网络；根据威胁的蔓延程度，爆发可能是内部的、区域的或全局的。

部分 II

管理客户

第 2 章

远程管理器客户

本节包含以下主题：

客户概述

客户窗口可以提供您公司管理的所有先前配置的客户的列表。您可以使用此窗口查看基本客户联系信息，并确定客户是否需要我们立即处理明显的威胁、系统或许可事件。

提示

您可以使用列表右侧的搜索窗格过滤**客户**列表。

有关更多信息，请参阅过滤客户列表 第 2-5 页。

下表概述了**客户**窗口上的可用任务。

任务	描述	适用范围
添加新客户	单击**新客户**可设置公司配置文件和用户帐户，分配服务计划和配置缺省产品设置。 有关更多信息，请参阅添加客户 第 2-5 页。	• 客户许可门户帐户 • Licensing Management Platform 帐户
删除现有的客户	选择一个现有的客户，然后单击**删除**可从**客户**列表中删除客户帐户。 **注意** 必须先从选定客户中删除所有产品，才能删除客户。 **警告!** 一旦删除客户帐户，将无法恢复。	• 客户许可门户帐户

任务	描述	适用范围
向现有客户分配缺省产品模板	选择一个现有的客户，然后单击**分配模板**可从预先配置的产品设置中选择。 **注意** 远程管理器仅支持安全无忧软件-云端版和 Cloud Edge 的缺省产品模板。 有关更多信息，请参阅向现有客户分配缺省设置模板 第 2-9 页。	• Licensing Management Platform 帐户
将策略设置部署到多个客户	选择现有的客户，然后单击“策略设置”，从可应用到所有选定客户的可用安全无忧软件-云端版策略中选择。 有关更多信息，请参阅多个客户的批量策略更新 第 2-10 页。	• Licensing Management Platform 帐户
Cloud Edge 设备固件更新	选择现有的 Cloud Edge 客户，然后单击**更新固件**。远程管理器会通知需要更新固件的任何选定的 Cloud Edge 客户获取更新软件包。	• Licensing Management Platform 帐户
续订产品使用授权	选择现有的客户，然后单击**续订使用授权**。远程管理器可让您续订使用授权到期的任何客户。 有关更多信息，请参阅续订使用授权 第 3-14 页。	• Licensing Management Platform 帐户
导出客户信息	• 选择客户并单击**导出**将选定的客户信息保存为 CSV 文件 • 单击**全部导出**将显示的所有客户信息保存为 CSV 文件	• 客户许可门户帐户 • Licensing Management Platform 帐户
更改远程管理器**客户**视图设置	单击**设置**可更改远程管理器显示拥有 Licensing Management Platform 帐户的所有客户还是仅显示拥有远程管理器管理的产品的客户。	• Licensing Management Platform 帐户

客户数据

客户窗口可为您提供基本的客户信息，并显示影响客户的重要事件的摘要计数。

重要信息

要修改单个客户的信息，您必须使用 Licensing Management Platform 帐户登录，然后单击窗口右上角的 **Licensing Management Platform** 链接。您不能直接从远程管理器控制台修改客户信息。

表 2-1. 客户数据

项目	描述
公司	Licensing Management Platform 中配置的公司名称 单击**公司**名称可管理单独的客户和许可设置。 有关更多信息，请参阅单个客户设置 第 3-1 页。
联系人	Licensing Management Platform 中配置的公司联系人
电话	Licensing Management Platform 中配置的公司联系人电话号码
产品	公司许可的所有产品列表（以逗号分隔）
威胁和系统事件	当前影响客户的所有“需要采取处理措施”（红色）和“警告”（黄色）威胁或系统事件的摘要计数 单击计数可打开**<客户>**窗口并查看有关事件类型的特定信息。 有关更多信息，请参阅受管产品事件 第 15-3 页。
使用授权事件	当前影响客户的所有“需要采取处理措施”（红色）和“警告”（黄色）许可事件的摘要计数 单击计数可打开**<客户>**窗口并查看有关事件类型的特定信息。 有关更多信息，请参阅续订使用授权 第 3-14 页。
最后一次事务	客户发生的事件更改（例如使用授权事务或系统威胁）的最后日期和时间。

过滤客户列表

使用窗口右侧的搜索窗格过滤客户列表。

过程

1. 转至**客户**。
2. 在右侧，从搜索窗格中选择一个或多个选项。

   注意

   下拉菜单中的**威胁类别**、**系统事件**和**使用授权事件**选项不会根据您选择的**产品**而动态更新。如果您选择的产品没有所选的事件选项，系统将显示其他产品的结果。

   例如，选择**产品** > **Hosted Email Security (HES)** 和**系统事件** > **云电子邮件扫描**会返回任何产品的所有 Hosted Email Security (HES) 事件和所有“云电子邮件扫描”事件。

3. （可选）单击**导出**为过滤出的客户生成 CSV 文件。

添加客户

在创建客户帐户之前，您应该掌握基本的客户信息。要填写的文本框包括**姓氏和名字**（因为此信息会显示在报表和通知上）、**时区**（客户所属的时区）和**语言**（客户接收的报表和通知所使用的语言）。在托管服务器上添加客户和安装客户端之前，请确保您具有执行各项任务以访问、监控和管理客户资源的书面许可。

过程

1. 在远程管理器 Web 控制台横幅上，单击**新客户**。

注意

您可以从横幅上或从**客户**选项卡上单击**新客户**。

2. 提供客户信息。

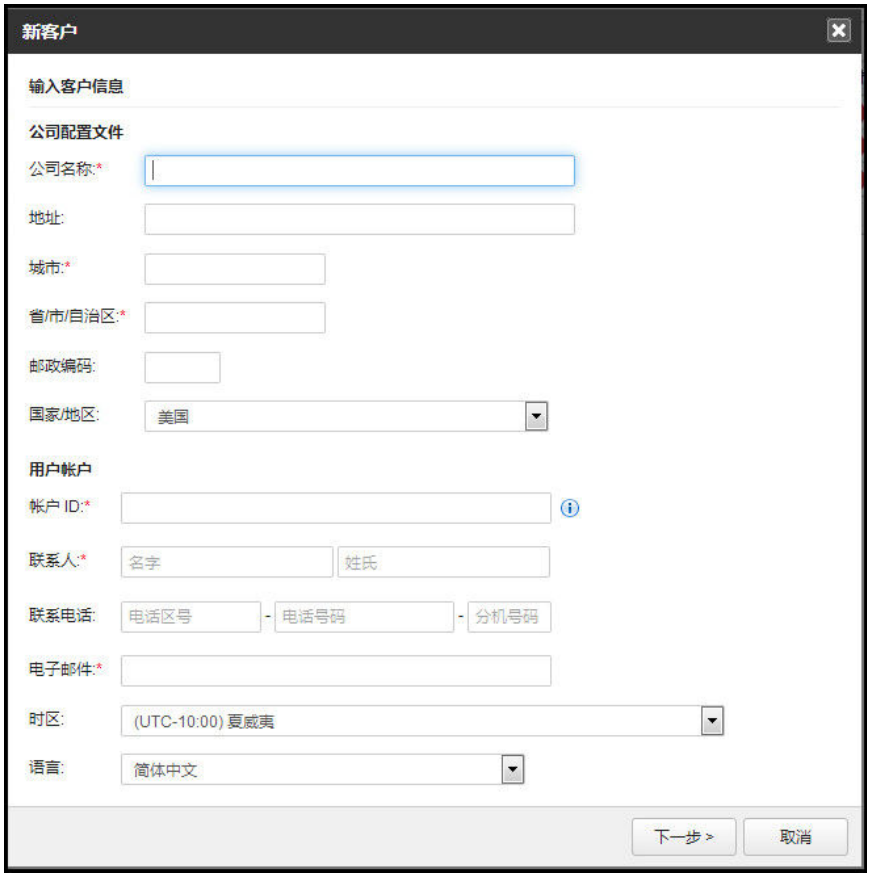
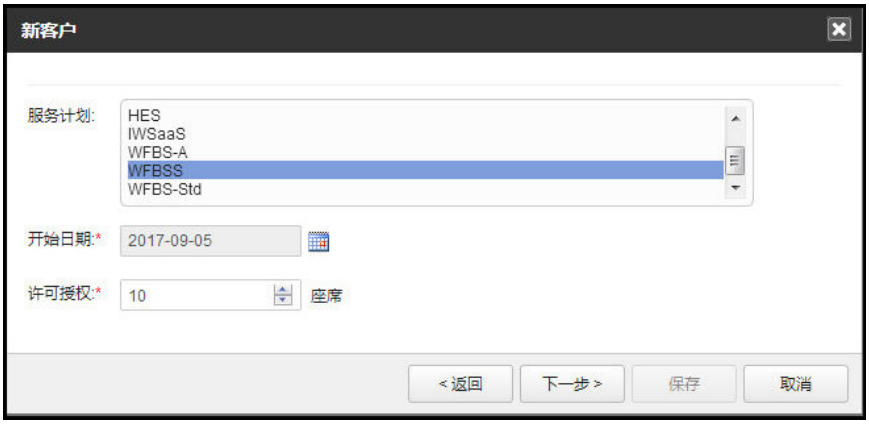


图 2-1. “客户信息”窗口

3. 单击**下一步>**。

4. 指定服务计划、授权开始日期，以及每个使用授权的部门数。



5. 设置此帐户的产品缺省设置。它们是：

注意

此功能仅适用于安全无忧软件-云端版和 Cloud Edge。

- **基本**：仅在此窗口中配置新客户帐户将会使用的设置。

图 2-2. 基本产品设置

- **模板**：使用此选项选择缺省设置模板。从**管理** > **配置缺省设置模板**中配置这些设置。

6. 验证所有信息，然后单击**保存**。

注意

添加客户后，只能从 Trend Micro Licensing Management Platform 中更改配置文件。

向现有客户分配缺省设置模板

仅当趋势科技远程管理器与 Licensing Management Platform 集成后，才可使用缺省设置模板。

您可以通过分配已启用行为监控的缺省模板向现有客户分配缺省设置模板，从而启用勒索软件防护。

有关可配置的设置的更多信息，请参阅产品文档。

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

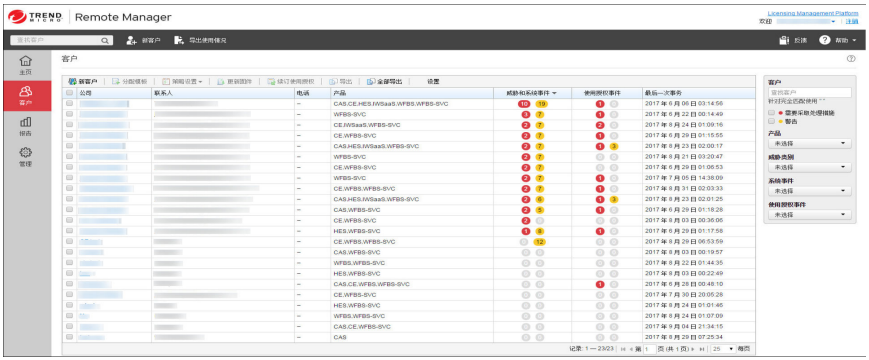
注意

只能将模板分配给使用安全无忧软件-云端版的公司。

过程

1. 转至**客户**。

   此时会显示**客户**窗口。



2. 从**公司**列表中选择一个或多个客户。
3. 单击**分配模板**选项卡。

   此时会显示**分配模板**窗口。

4. 从列表中选择模板。
5. 单击**下一步>**。

   此时会显示确认窗口，其中仅列出了具有受支持产品的公司。

6. 单击**分配**。

   模板成功分配给选定的客户。

多个客户的批量策略更新

远程管理器可让您配置单个安全无忧软件-云端版策略，并通过一次批量部署将设置部署到多个客户。您可以将策略部署到每个客户的特定设备组或更新客户的全局设置供以后使用，具体取决于策略类型。将策略部署到多个客户和客户设备组可以减少基于每个客户手动配置列表的开销。

远程管理器可以提供以下批量策略部署选项：

配置允许/阻止的 URL 列表

您可以为安全无忧软件-云端版客户配置允许/阻止的 URL 列表，并将列表部署到多个客户、设备组或在全局设置级别中部署。

注意

将允许/阻止的 URL 列表策略设置部署到特定设备组会在安全客户端上自动启用自定义允许/阻止的 URL 列表。

有关更多信息，请参阅*安全无忧软件-云端版联机帮助*。

注意

- 允许的 URL 列表的策略配置设置同时适用于 Web 信誉和 URL 过滤功能。
- 阻止的 URL 列表的策略配置设置仅适用于 URL 过滤功能。

过程

1. 转至**客户**。
2. 从公司列表中选择一个或多个客户。
3. 单击**策略设置**并选择**允许/阻止的 URL 列表**。

   此时会显示**允许/阻止的 URL 列表**窗口。

4. 选择策略设置的**目标**。

   - **客户 (全局设置)**：仅将更改应用到列表中选定客户的全局设置中

     重要信息

     对全局设置所做的任何更改均不适用于预先存在的设备组。您必须选择**设备组**才能立即将更改应用到现有的设备组。

   - **设备组**：将更改应用到列表中选定的设备组

     注意

     要选择特定类型的设备组，请使用**选择组**下拉按钮以选择或删除策略设置中的设备组。缺省情况下，远程管理器会选择所有客户的所有设备组。

5. 单击**配置策略 >**。

6. 为允许列表和阻止列表配置策略设置。

   a. 使用下拉框中指定更改如何影响每个列表。

      - **选择操作**：未应用当前策略设置任何更改的缺省设置
      - **附加**：远程管理器将指定的项目添加到现有列表中
      - **删除**：远程管理器删除现有列表中指定的项目

        注意

        如果远程管理器在现有列表中找不到指定的项目，远程管理器不会对列表执行任何操作。

      - **覆盖**：远程管理器删除现有列表中的所有项目并使用指定项目替换列表

        警告!

        此操作无法撤消。如果您选择替换整个列表，则无法恢复先前的列表项目。

b. 键入适用于策略的 URL。

注意

如果允许/阻止的 URL 列表中添加的条目数导致列表超出允许的最大值，列表部署将会失败。

使用空格符号、逗号 (,)、分号 (;) 或 ENTER 键指定多个条目。

URL 可以使用星号 (*) 作为通配符（星号匹配零个或更多个字符）。

7. 单击**部署策略设置**。

远程管理器可将所做更改部署到指定客户或设备组。您可以从**管理日志**监控策略部署的状态。

有关更多信息，请参阅查看管理日志 第 17-20 页。

针对实时扫描配置防病毒例外

您可以为安全无忧软件-云端版客户配置防病毒例外列表，并将列表部署到多个客户或设备组。

注意

启用防病毒例外会在受影响的安全客户端上自动启用实时防病毒和防间谍软件扫描。

过程

1. 转至**客户**。
2. 从公司列表中选择一个或多个客户。
3. 单击**策略设置**并选择**防病毒例外**。

此时会显示**防病毒例外**窗口。

4. 选择您想要配置的客户或特定的设备组。

> **注意**
>
> 要选择特定类型的设备组，请使用**选择组**下拉按钮以选择或删除策略设置中的设备组。缺省情况下，远程管理器会选择所有客户的所有设备组。

5. 单击**配置策略 >**。

6. 使用下拉框中指定更改如何影响每个列表。

   - **选择操作**：未应用当前策略设置任何更改的缺省设置
   - **启用防病毒例外**：远程管理器为选定设备组启用防病毒例外。

     此时会显示 **Windows 例外**和 **Mac 例外**部分。
   - **禁用防病毒例外**：远程管理器为选定设备组禁用防病毒例外。

7. 在 **Windows 例外**和 **Mac 例外**部分中：

   a. 使用下拉框中指定更改如何影响每个列表。

      - **选择操作**：未应用当前策略设置任何更改的缺省设置
      - **附加**：远程管理器将指定的项目添加到现有列表中
      - **删除**：远程管理器删除现有列表中指定的项目

> **注意**
>
> 如果远程管理器在现有列表中找不到指定的项目，远程管理器不会对列表执行任何操作。

      - **覆盖**：远程管理器删除现有列表中的所有项目并使用指定项目替换列表

> **警告!**
>
> 此操作无法撤消。如果您选择替换整个列表，则无法恢复先前的列表项目。

b. 在以下字段中键入必要的例外：

- **目录路径**：排除指定的目录和所有子目录

重要信息

Mac 设备不支持目录路径列表。

注意

可以在目录路径条目中使用星号 (*) 作为通配符。

- **文件名或带有完整路径的文件名**：根据文件名或带有完整路径的文件名排除指定的文件

注意

文件名和带有完整路径的文件名可以使用星号 (*) 作为通配符。

- **文件扩展名**：排除带有指定扩展名的所有文件

注意

字段中输入的文件扩展名不带句点，例如 txt（而非 .txt）。

使用分号 (;) 或 ENTER 键指定多个条目。

8. 单击**部署策略设置**。

远程管理器可将所做更改部署到指定客户或设备组。您可以从**管理日志**监控策略部署的状态。

有关更多信息，请参阅查看管理日志 第 17-20 页。

配置行为监控例外列表

您可以为安全无忧软件-云端版客户配置行为监控例外列表，并将列表部署到多个客户或设备组。

重要信息

部署行为监控例外列表设置时，请注意以下事项：

- 对于“设备 (缺省)”组，安全客户端会自动启用行为监控。
- 对于“服务器 (缺省)”组，安全客户端会自动启用行为监控和未授权更改阻止服务。
- 对于手动组：
  - 安装在桌面平台的安全客户端会自动启用行为监控。
  - 安装在服务器平台的安全客户端会自动启用行为监控，但您必须使用安全无忧软件-云端版控制台手动启用未授权更改阻止服务。

有关更多信息，请参阅*安全无忧软件-云端版联机帮助*。

过程

1. 转至**客户**。
2. 从公司列表中选择一个或多个客户。
3. 单击**策略设置**并选择**行为监控例外列表**。

   此时会显示**行为监控例外列表**窗口。
4. 选择您想要配置的客户或特定的设备组。

   注意

   要选择特定类型的设备组，请使用**选择组**下拉按钮以选择或删除策略设置中的设备组。缺省情况下，远程管理器会选择所有客户的所有设备组。
5. 单击**配置策略 >**。
6. 为**允许的程序列表**和/或**阻止的程序列表**配置策略设置。
   a. 使用下拉框中指定更改如何影响每个列表。
      - **选择操作**：未应用当前策略设置任何更改的缺省设置
      - **附加**：远程管理器将指定的项目添加到现有列表中

- **删除**：远程管理器删除现有列表中指定的项目

  注意

  如果远程管理器在现有列表中找不到指定的项目，远程管理器不会对列表执行任何操作。

- **覆盖**：远程管理器删除现有列表中的所有项目并使用指定项目替换列表

  警告!

  此操作无法撤消。如果您选择替换整个列表，则无法恢复先前的列表项目。

b. 键入适用于策略的程序的完整路径。

使用分号 (;) 或 ENTER 键指定多个条目。

7. 单击**部署策略设置**。

远程管理器可将所做更改部署到指定客户或设备组。您可以从**管理日志**监控策略部署的状态。

有关更多信息，请参阅查看管理日志 第 17-20 页。

配置预测型机器学习例外列表

您可以为安全无忧软件-云端版客户配置预测型机器学习例外列表，并在全局设置级别中将列表部署到多个客户。

重要信息

对全局设置所做的任何更改均不适用于预先存在的设备组。

过程

1. 转至**客户**。
2. 从公司列表中选择一个或多个客户。
3. 单击**策略设置**并选择**预测型机器学习例外列表**。

   此时会显示**预测型机器学习例外列表**窗口。
4. 选择您想要配置的客户。
5. 单击**配置策略 >**。
6. 为预测型机器学习例外列表配置策略设置。

   a. 使用下拉框指定更改如何影响列表。

   - **选择操作**：未应用当前策略设置任何更改的缺省设置
   - **附加**：远程管理器将指定的项目添加到现有列表中
   - **删除**：远程管理器删除现有列表中指定的项目

   注意

   如果远程管理器在现有列表中找不到指定的项目，远程管理器不会对列表执行任何操作。

   - **覆盖**：远程管理器删除现有列表中的所有项目并使用指定项目替换列表

   警告!

   此操作无法撤消。如果您选择替换整个列表，则无法恢复先前的列表项目。

   b. 键入适用于策略的 SHA-1 文件哈希。

   使用分号 (;) 或 ENTER 键指定多个条目。
7. 单击**部署策略设置**。

远程管理器可将所做的更改部署到指定的客户。您可以从**管理日志**监控策略部署的状态。

有关更多信息，请参阅查看管理日志 第 17-20 页。

配置预测型机器学习设置

您可以为安全无忧软件-云端版客户配置预测型机器学习设置列表，并将列表部署到多个客户或设备组。

注意

预测型机器学习需要连接到 Internet 以访问云安全智能防护网络。

过程

1. 转至**客户**。
2. 从公司列表中选择一个或多个客户。
3. 单击**策略设置**并选择**预测型机器学习设置**。

   此时会显示**预测型机器学习设置**窗口。
4. 选择您想要配置的客户或特定的设备组。

   注意

   要选择特定类型的设备组，请使用**选择组**下拉按钮以选择或删除策略设置中的设备组。缺省情况下，远程管理器会选择所有客户的所有设备组。
5. 单击**配置策略 >**。
6. 选择**操作**即可应用到策略。
   - **选择操作：**未应用当前策略设置任何更改的缺省设置
   - **启用预测型机器学习：**在选定的设备组上启用预测型机器学习

     此时会显示**检测设置**部分。

- **禁用预测型机器学习**：在选定的设备组上禁用预测型机器学习

7. 在**检测设置**下，选择预测机器学习采取的检测类型和相关处理措施。

检测类型	处理措施
文件	• **隔离**：选择此选项可自动隔离预测型机器学习分析结果指示存在恶意软件相关特征的文件 • **仅记录**：选择此选项可扫描未知文件，并记录预测型机器学习分析结果，以进行进一步的内部威胁调查
进程	• **终止**：选中可根据预测机器学习分析自动终止表现出恶意软件相关行为的进程或脚本 **重要信息** 预测机器学习将尝试清除已执行恶意进程的文件。如果清除处理措施不成功，受管产品将隔离受影响的文件。 • **仅记录日志**：选中可扫描未知进程或脚本并记录预测机器学习分析，进一步对威胁开展内部调查

8. 单击**部署策略设置**。

   远程管理器可将所做更改部署到指定客户或设备组。您可以从**管理日志**监控策略部署的状态。

   有关更多信息，请参阅查看管理日志 第 17-20 页。

配置勒索软件设置

您可以为安全无忧软件-云端版客户配置勒索软件设置，并将设置部署到多个客户或设备组。

重要信息

部署勒索软件设置时，请注意以下事项：

- 对于“设备 (缺省)”组，安全客户端会自动启用行为监控。
- 对于“服务器 (缺省)”组，安全客户端会自动启用行为监控和未授权更改阻止服务。
- 对于手动组：
  - 安装在桌面平台的安全客户端会自动启用行为监控。
  - 安装在服务器平台的安全客户端会自动启用行为监控，但您必须使用安全无忧软件-云端版控制台手动启用未授权更改阻止服务。

有关更多信息，请参阅*安全无忧软件-云端版联机帮助*。

过程

1. 转至**客户**。
2. 从公司列表中选择一个或多个客户。
3. 单击**策略设置**并选择**勒索软件设置**。

   此时会显示**勒索软件设置**窗口。
4. 选择您想要配置的客户或特定的设备组。

   注意

   要选择特定类型的设备组，请使用**选择组**下拉按钮以选择或删除策略设置中的设备组。缺省情况下，远程管理器会选择所有客户的所有设备组。
5. 单击**配置策略 >**。
6. 选择**操作**即可应用到策略。
   - **选择操作**：未应用当前策略设置任何更改的缺省设置
   - **启用勒索软件防护**：在选定的设备组上启用勒索软件防护功能

     此时会显示**设置**部分。

- **禁用勒索软件防护**：在选定的设备组上禁用勒索软件防护功能

7. 如果启用勒索软件防护功能，请选择您要应用的勒索软件防护功能。

   - **启用文档保护，使其免遭未授权的加密或修改**：阻止由加密或修改文档内容造成的潜在恶意软件威胁

     - **自动备份和恢复被可疑程序修改的文件**：创建终端上加密的文件备份，防止在受管产品检测到勒索软件威胁时丢失任何数据

     注意

     自动文件备份要求客户端终端上至少有 100 MB 磁盘空间，且仅备份那些小于 10 MB 的文件。

   - **针对通常与勒索软件关联的进程启用阻止**：在任何加密或修改文档事件发生之前阻止与已知勒索软件威胁相关的进程

   - **启用程序检查以检测并阻止遭受危害的可执行文件**：程序检查可监控进程并执行 API 挂接，确定程序的行为方式是否异常。虽然此过程可提高遭受危害的可执行文件的总体检测比率，但系统性能可能会降低。

8. 单击**部署策略设置**。

   远程管理器可将所做更改部署到指定客户或设备组。您可以从**管理日志**监控策略部署的状态。

   有关更多信息，请参阅查看管理日志 第 17-20 页。

在 Licensing Management Platform 中合并多个远程管理器帐户

如果您管理的其他趋势科技远程管理器帐户尚未迁移至新的 Licensing Management Platform，那么您可以将这些帐户与目前的帐户合并。

过程

1. 登录某个已迁移至 Licensing Management Platform 的远程管理器帐户。

   将显示**控制台**窗口。

2. 单击登录名称旁边的箭头，然后单击**合并其他帐户** > **是**。

警告!

如果您将某帐户合并到当前帐户，那么合并进来的帐户的所有数据都将被移动。例如，如果您目前登录的是 admin1，并将 admin2 合并到了 admin1 帐户，则 admin2 帐户中的所有数据都将从 admin2 帐户删除。这些数据合并到了 admin1 帐户。您仍然可以打开 admin2 帐户，但是其中的所有数据现在都转移到了 admin1 帐户。

3. 输入您要与当前帐户合并的帐户的用户名和密码。
4. 单击**合并**。

   等几分钟，让数据完成合并。

后续步骤

迁移帐户后，添加新客户时将会始终看到以下内容：

- **具有一个活动的 Licensing Management Platform 帐户**：如果新客户在 Licensing Management Platform 中已经有一个帐户。
- **使用需要连接到此帐户的现有产品服务器**：如果新客户已有产品/服务，但是帐户尚未集成到 Licensing Management Platform。

第 3 章

单个客户设置

本节包含以下主题：

客户信息

<客户>窗口包含多个选项卡，您可以使用这些选项卡查看关联产品、使用授权、公司数据、通知和 ConnectWise 设置相关的各个客户信息。

表 3-1. 客户选项卡

选项卡	描述
产品	提供与客户帐户关联的所有产品的列表，并显示可能需要紧急处理的所有产品相关事件的列表 您可以使用**产品**选项卡配置各个产品设置。 **注意** 如果任何产品具有“需要采取处理措施”（红色）或“警告”（黄色）事件，远程管理器会直接在选项卡上显示摘要计数。 有关更多信息，请参阅客户产品 第 3-3 页。
使用授权	提供与客户帐户关联的所有产品和服务计划列表 **注意** 如果任何产品具有“已到期”（红色）或“即将到期”（黄色）事件，远程管理器会直接在选项卡上显示摘要计数。 有关更多信息，请参阅客户使用授权 第 3-13 页。
公司配置文件	显示 Licensing Management Platform 中配置的客户公司的常规信息 有关更多信息，请参阅公司配置文件 第 3-15 页。
联系信息	显示 Licensing Management Platform 中配置的客户的联系信息 有关更多信息，请参阅联系信息 第 3-16 页。
通知	显示客户的所有通知配置设置 有关更多信息，请参阅客户通知 第 3-17 页。

选项卡	描述
ConnectWise	显示客户的 ConnectWise 集成设置 有关更多信息，请参阅各个客户的 ConnectWise 设置 第 3-18 页。

客户产品

客户**产品**选项卡可以显示当前与客户帐户关联的所有产品，并列出所有相关事件通知。

提示

您可以使用表格上方的**查看方式**下拉框过滤**通知事件**列表。

下表概述了**产品**选项卡上的可用任务。

任务	描述
添加新产品	单击**添加**按钮可向客户分配新的产品和服务计划。 有关更多信息，请参阅使用 Licensing Management Platform 帐户添加新产品 第 3-8 页或使用客户许可门户帐户添加新产品 第 3-11 页。

任务	描述
管理产品设置	选择产品树中的产品可显示产品特定的事件通知和配置设置 有关更多信息，请参阅以下产品的特定产品设置信息： • Cloud App Security 第 4-2 页 • Cloud Edge 第 5-2 页 • Hosted Email Security 第 6-2 页 • InterScan Web Security as a Service 第 7-2 页 • 安全无忧软件 第 8-2 页 • 安全无忧软件-云端版 第 9-2 页 有关产品树中显示的图标的详细信息，请参阅网络树状态图标 第 3-12 页。
查看威胁和系统事件通知	缺省情况下，远程管理器可以显示与客户帐户关联的所有产品的所有事件通知。要查看特定产品的事件通知，请从产品树中选择相应的产品。 有关更多信息，请参阅受管产品事件 第 15-3 页。 要查看特定事件的相关详情，请单击**出现次数**计数。

产品/服务信息

该控制台仅列出需要注意的客户。要获取任何产品（包括控制台上未列出的产品）的详细信息，请转到**客户**选项卡，然后访问客户树上的产品。

单击**客户** > **{客户}** > **{产品}**可显示其他信息。

注意

显示的选项因产品/服务而异。

产品	选项
Cloud App Security	• **事件**：显示系统事件和威胁事件 • **用户**：可让您创建或删除 Cloud App Security 用户，以及重置用户的密码

Cloud Edge	• 对于服务计划：
	  • **事件**：在服务计划中显示所有 Cloud Edge 设备的事件摘要
	  • **固件更新**：显示每个设备的当前固件版本以及最新版本；提供用来手动更新固件的选项
	  • **设备**：显示每个注册设备的名称和序列号
	• 对于注册设备：
	  • **事件**：显示系统事件和威胁事件
	  • **组件**：显示每个组件的当前版本、最新版本和上次更新日期
	  • **网络**：显示通过 Cloud Edge 设备连接到网络的端点的用户名、远程 IP 地址和 MAC 地址
	  • **VPN**：显示通过虚拟专用网络和 Cloud Edge 设备连接到网络的端点的用户名、远程 IP 地址和虚拟 IP 地址
	  **注意**
	要进行更细化的更改，请访问 Cloud Edge 控制台。

Hosted Email Security	• **实时状态**：显示最新的 Hosted Email Security 信息。 • **策略设置**：列出所有可用策略。 • **允许的发件人**：列出所有不受基于 IP 信誉、垃圾邮件、网络钓鱼或营销邮件过滤的发件人。 • **被阻止的发件人**：列出所有被阻止发送邮件的地址或域。  **注意** 要进行更细化的更改，请访问 Hosted Email Security 控制台。

产品	选项
InterScan Web Security as a Service	显示最新的 InterScan Web Security as a Service 威胁和系统信息。 **注意** 要进行更细化的更改，请访问 InterScan Web Security as a Service 控制台。

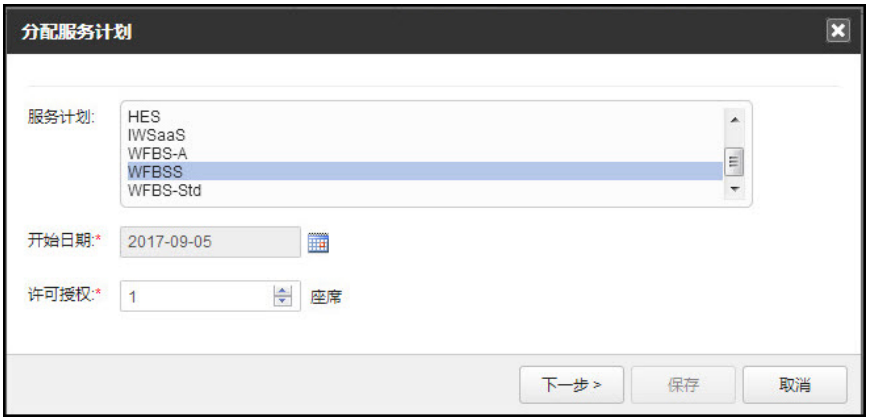
产品	选项
安全无忧软件	• **事件**：列出可能需要或不需要执行操作的系统事件和威胁事件。 • **组**：列出服务器上配置的不同组。您可以在此处请求启动或停止扫描。 • **域设置**：配置整个域的设置。 请参阅趋势科技安全无忧软件文档，了解详细信息： http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security.aspx. **注意** 各个组的安全设置不能从此处配置。您需要访问安全无忧软件控制台才能做这些更改。 • **托管服务器**：显示服务器的所有详细信息。您可以在此处请求更新服务器和更新客户端。 • **TMRM 客户端**：包含有关趋势科技远程管理器客户端的一般信息，如可用性、全局唯一标识符 (GUID) 或授权码以及 IP 地址等。 • **设备**：列出扫描引擎的名称、IP 地址、在线/离线状态和详细信息，以及特征码文件和平台。 **注意** 当您展开产品并单击**服务器**或**台式机**后，您就会看到**设备**和**安全设置**。 • **安全设置**：配置特定组的安全设置（仅适用于安全无忧软件 6.0 和更高版本）。请参阅趋势科技安全无忧软件文档，了解详细信息。

产品	选项
安全无忧软件-云端版	• **事件**：列出可能需要或不需要执行操作的系统事件和威胁事件。 • **组**：列出配置的组和类型。 • **设备**：列出扫描引擎的名称、IP 地址、在线/离线状态和详细信息，以及特征码文件和平台。 **注意** 当您展开产品并单击**服务器**或**台式机**后，您就会看到**设备**和**安全设置**。 • **安全设置**：配置安全无忧软件-云端版的安全设置。请参阅趋势科技安全无忧软件-云端版文档，了解详细信息： http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security-services.aspx **注意** 要进行更细化的更改，请访问安全无忧软件-云端版控制台。

使用 Licensing Management Platform 帐户添加新产品

过程

1. 转至**客户** > **{客户名称}** > **产品** > **添加**。



2. 指定服务计划、开始日期，以及每个使用授权的单位数。
3. 单击**下一步>**或**保存**。
4. 配置产品缺省设置。您选择以下其中一个选项：

注意

仅当您已选择安全无忧软件-云端版时，才会显示此功能。

- **基本**：只配置显示的设置。
  - 用于 Web 信誉和 URL 过滤的允许列表

> **注意**
>
> 如果要向“允许的”列表中添加 URL，请确保它没有被加入到“阻止的”列表中列表中，反之亦然。

- 针对 URL 过滤的已阻止列表
- 针对服务器和设备的预设扫描

- **模板**：转至**管理** > **配置缺省设置模板**即可使用类似于安全无忧软件的控制台进行更多设置。

5. 单击**保存**。

   即已添加该产品/服务，系统会显示该添加的详细信息。

注意

如果添加的是安全无忧软件产品，请记下安全无忧软件的激活码，然后在 Licensing Management Platform 控制台中完成安装过程。

6. 单击**连接**，以取得有关如何将产品/服务连接到控制台的信息。

使用客户许可门户帐户添加新产品

您仅可以使用 CLP 帐户添加以下产品：

- Hosted Email Security
- 安全无忧软件
- 安全无忧软件-云端版

过程

1. 在远程管理器控制台上，转至**客户** > **[客户]** > **产品** > **添加**。

   此时会显示**添加产品**窗口。

2. 在**产品类型**下拉列表中，选择您要注册到该客户的产品。
3. 键入**产品描述**。
4. 单击**保存**。

此时会显示包含详细说明的确认窗口。

5. 复制用于将受管产品注册到远程管理器的“授权密钥”或“GUID”。
6. 在受管产品控制台上，转至**管理** > **趋势科技远程管理器**。
7. 在可用字段中提供“授权密钥”或“GUID”。
8. 单击**连接**。

   受管产品连接到远程管理器，并注册到先前选择的客户帐户。

   打开远程管理器控制台并查看客户产品列表，验证受管产品是否成功注册。

网络树状态图标

在**产品**选项卡的左侧，窗口会显示客户产品的树视图。

表 3-2. 网络树对象

图标	网络对象	描述
	产品/服务	此产品/服务未连接到远程管理器。
	产品/服务	此产品/服务已连接到远程管理器。
	设备	该设备处于脱机状态。
	设备	该设备处于联机状态。
	组	台式机组
	组	安全无忧软件-云端版设备组由不同的设备类型组成。
	Exchange Server	Exchange Server 计算机；此计算机运行邮件安全客户端 (MSA)。
	组	服务器组；此组管理众多网络安全客户端 (CSA)。

客户使用授权

客户**使用授权**选项卡可以显示当前授权客户帐户使用的所有产品以及每个使用授权当前的状态。

下表概述了**使用授权**选项卡上的可用任务。

任务	描述
续订使用授权	选择产品，然后单击**续订使用授权**按钮可延长选定产品的许可期限。 有关更多信息，请参阅续订使用授权 第 3-14 页。
修改座席分配	选择产品，然后单击**修改座席分配**按钮可更改与每个服务计划关联的座席数。 有关更多信息，请参阅修改座席分配 第 3-15 页。

下表概述了**使用授权**表上显示的信息。

项目	描述
状态图标	状态图标可以提供识别使用授权问题的快速方式。 •  ：正常 •  ：即将到期 •  ：已到期 •  ：分配已超限
产品	指出产品名称 单击可用的链接可单次登录产品控制台。
服务计划	指出与产品关联的服务计划
已提供	指出分配给产品的座席数
已使用	指出客户已激活的座席数
到期日期	指出使用授权的到期日期

项目	描述
自动续订	指出使用授权是否自动延长许可期限

续订使用授权

为您管理的客户续订使用授权。

注意

此功能仅在您使用与 Trend Micro Licensing Management Platform 集成的帐户时才能使用。

过程

1. 打开**续订使用授权**窗口的方法有多种：
   - 在远程管理器 Web 控制台中：
     a. 单击**客户**。
     b. 选择使用授权已过期或即将过期的客户。
     c. 单击**使用授权**选项卡。
     d. 点击**续订使用授权**。
   - 在**使用授权管理**小组件中：
     a. 单击**已过期**或**即将到期**计数。
     b. 选择使用授权已过期或即将过期的客户。
     c. 单击**使用授权**选项卡。
     d. 单击**续订使用授权**。
   - 在电子邮件通知中，单击**续订**链接。
2. 指定使用授权期限的变动。

3. 单击**提交**。

修改座席分配

每个经销商都可以指定为每个客户分配多少个座席。如果超过分配的座席数，经销商可以为每个客户分配更多座席。

注意

此功能仅在您使用与 Trend Micro Licensing Management Platform 集成的帐户时才能使用。

过程

1. 转至**客户** > **{客户名称}** > **使用授权**。

提示

您还可以单击“通知”小组件中请求更多坐席的客户的数目，来查看需要额外坐席的客户的较短列表。

2. 选择您要修改的产品。
3. 单击**修改座席分配**。

   修改座席分配屏幕随即显示。
4. 指定要在**新坐席**列下为每个产品添加的新坐席的数目。
5. 单击**提交**。

公司配置文件

客户**公司配置文件**选项卡可以显示 Licensing Management Platform 中存储的客户公司的常规信息。

下表概述了**公司配置文件**选项卡上的可用信息。

项目	描述
公司名称	客户公司的名称
地址	客户公司的街道地址
城市	客户公司所在的城市
省/市/自治区	客户公司所在的省/市/自治区
邮政编码	客户公司的邮政编码
国家/地区	客户公司所在的国家/地区
登录 URL	客户可用于登录 Licensing Management Platform 的 URL
公司徽标	受支持的趋势科技产品控制台上显示的客户公司的自定义横幅

联系信息

客户**联系信息**选项卡可以显示 Licensing Management Platform 中存储的主要客户联系人的信息。

下表概述了**联系信息**选项卡上的可用信息。

项目	描述
帐户	联系人的帐户名称
用户角色	分配给联系人的用户角色
联系人姓名	主要联系人的姓名
联系电话	主要联系人的电话号码
电子邮件	主要联系人的电子邮件地址
时区	联系人所在的时区
语言	联系人的首选语言

客户通知

您可以使用客户**通知**选项卡配置远程管理器发送给配置的收件人和第三方远程管理和监控工具的事件通知类型以及发送的电子邮件内容的类型。

您可以接受全局通知设置，或自定义每个客户设置。

有关全局通知设置的详细信息，请参阅配置全局通知设置 第 17-3 页。

过程

1. 转至**客户** > **[客户]**。
2. 单击**通知**选项卡。
3. 在**收件人**部分中，从以下设置中选择：
   - **帐户管理器**：为管理客户的代表选择 Licensing Management 帐户
   - **其他收件人**：键入您希望远程管理器通知其客户事件的任何其他人的电子邮件地址
4. 在**第三方通知**部分中，选择您已经与远程管理器集成的远程管理和监控工具。
   - **ConnectWise**

     重要信息

     您必须首先集成远程管理器与 ConnectWise，同时为每个客户启用单独的 ConnectWise 设置，远程管理器才可以发送通知。

     有关更多信息，请参阅集成 ConnectWise Manage™ 第 11-2 页和各个客户的 ConnectWise 设置 第 3-18 页。
   - **Kaseya**

     有关更多信息，请参阅集成 Kaseya™ 第 13-2 页。
   - **Autotask**

有关更多信息，请参阅集成 Autotask™ 第 10-2 页。

5. 在**邮件内容**部分中，接受全局配置内容设置或单击**更改全局邮件内容设置**链接来修改所有远程管理器客户的邮件内容。

6. 在**事件**部分中，从以下设置中选择：

   - **使用全局通知事件设置**：将全局配置事件设置应用到客户

     单击链接可查看全局设置并进行任何必要的更改以适用于所有远程管理器客户。

   - **使用自定义通知事件设置**：选择显示远程管理器中可用的所有产品的所有事件设置列表

     启用所需的通知事件类型并为客户特定的产品配置任何必要设置。

     有关可用的事件类型的详细信息，请参阅：

     - 安全无忧软件-云端版通知 第 17-10 页
     - 安全无忧软件通知 第 17-12 页
     - Cloud App Security 通知 第 17-14 页
     - Cloud Edge 通知 第 17-15 页
     - InterScan Web Security as a Service 通知 第 17-16 页

7. 单击**保存**。

各个客户的 ConnectWise 设置

如果您想自动化远程管理器通知，则必须在远程管理器控制台上为每个趋势科技客户启用 ConnectWise Manage 通知和集成。

有关全局 ConnectWise 集成设置的详细信息，请参阅集成 ConnectWise Manage™ 第 11-2 页。

重要信息

要开始在 ConnectWise 系统中接收通知，您必须首先为每个客户配置 ConnectWise 通知设置。

有关更多信息，请参阅客户通知 第 3-17 页。

过程

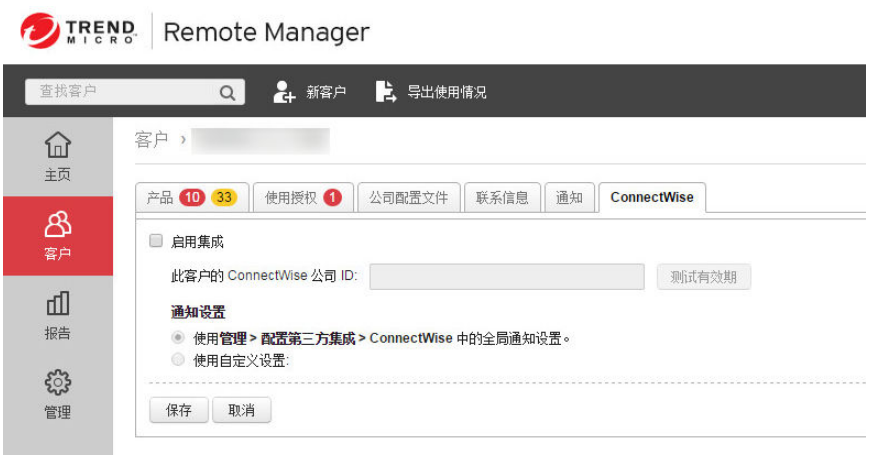
1. 转至**客户** > **[客户]**。
2. 要集成此客户的 ConnectWise Manage 设置，请单击 **ConnectWise Manage** 选项卡。
3. 选择**启用集成**。
4. 指定此客户的 **ConnectWise 公司 ID**。

   注意

   单击**验证**以确保 ConnectWise Manage 中存在该公司 ID。

5. 单击**保存**。

   趋势科技远程管理器会从 ConnectWise Manage 同步客户信息并加载任何可用的协议信息。此时会显示以下窗口：



6. 在**协议**部分中，可以向趋势科技产品分配 ConnectWise Manage 协议。

注意

通过向趋势科技产品分配协议，ConnectWise Manage 可以为趋势科技远程管理器客户提供自动结算服务。

重要信息

- 如果您以前使用 “TMRM 管理解决方案”或 “Managed Service” 协议类型配置过 ConnectWise Manage，则趋势科技产品名称旁边将显示“缺省”。
- 如果您未使用 “TMRM 管理解决方案”或 “Managed Service” 协议类型配置过 ConnectWise Manage，则可以向趋势科技产品分配 ConnectWise Manage 协议。

a. 单击**设置**。

此时会显示**产品协议**窗口。

b. 对于每种产品，请先选择协议类型，然后再选择协议名称。

c. 单击**确定**。

7. 选择以下两种集成设置之一：

- 选择**使用管理中的全局设置 > 配置第三方集成 > ConnectWise Manage 设置**以应用全局集成设置。
- 选择**使用自定义设置**来配置特定于客户的通知，以用于结算和执行摘要。
  - **在每月的 X 日将以下产品的帐单信息发送到 ConnectWise：**选择接收所选产品的帐单信息的日期。

注意

如果您选择 29、30 或 31 日，而相应月份不包含该日期，远程管理器会在相应月份的最后一天发送通知。

- **每<天、周或月>将 Hosted Email Security 的以下信息发送到 ConnectWise：**远程管理器以指定频率发送 Hosted Email security 的选定检测信息。

8. 单击**保存**。

部分 III

管理趋势科技产品

第 4 章

远程管理器中的 Cloud App Security

本节包含以下主题：

Cloud App Security

Trend Micro Cloud App Security 为 Microsoft Office 365 服务、Box、Dropbox 和 Google 云端硬盘提供高级保护，利用强大的企业级威胁和数据保护控制机制增强安全性。Cloud App Security 会防范网络钓鱼欺诈、零日恶意软件和隐藏的恶意软件以及未经授权即传输敏感数据。

Cloud App Security 将云端服务与 Exchange Online、SharePoint Online、OneDrive for Business、Box、Dropbox 和 Google 云端硬盘集成，从而维持高可用性和管理功能。

注册 Cloud App Security

过程

1. 在远程管理器 Web 控制台上添加新客户。
2. 向该客户的服务计划中添加 Cloud App Security。

   有关更多信息，请参阅使用 Licensing Management Platform 帐户添加新产品 第 3-8 页。
3. 转至 Cloud App Security Web 控制台，以激活使用授权。

注意

Cloud App Security 数据将自动与远程管理器同步。

管理 Cloud App Security

通过远程管理器，可以为注册的 Cloud App Security 安装执行以下任务。

表 4-1. Cloud App Security 管理任务

任务	描述
查看事件	从**事件**选项卡查看 Cloud App Security 事件的列表。
管理用户	从**用户**选项卡添加和删除用户，以及重置密码。
访问 Cloud App Security 控制台	单击**打开控制台**访问 Cloud App Security 控制台。

Cloud App Security 事件

注意

如果发生多个“需要采取处理措施”和“警告”事件，远程管理器会针对最严重的威胁显示 图标。

表 4-2. 威胁事件

事件类别	详细信息	事件状态
防病毒	病毒检测超出	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
文件阻止	文件阻止违例超出	：在 1 小时内检测到的文件阻止违例计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
沙盒平台	沙盒平台“高风险”检测超出	：在 1 小时内检测到的沙盒平台“高风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置）
	沙盒平台“中/低等风险”检测超出	：在 1 小时内检测到的沙盒平台“中/低等风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉	URL 违例超出	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 4-3. 系统事件

事件类别	详细信息	事件状态
帐户同步问题	Box 访问令牌无效	：无法访问指定的云存储
	Dropbox 访问令牌无效	：无法访问指定的云存储
	Google 云端硬盘访问令牌无效	：无法访问指定的云存储
	委派帐户上的同步问题	：无法与委派帐户同步

Cloud App Security 通知

表 4-4. 威胁事件

事件	详细信息
防病毒 — 病毒检测超过	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）

事件	详细信息
文件阻止 — 文件阻止违例超出	：在 1 小时内检测到的文件阻止违例计数超过了配置的阈值（如受管产品控制台上的配置）
勒索软件 — 勒索软件检测超出	：在 1 小时内检测到的勒索软件计数超过了配置的阈值（如受管产品控制台上的配置）
沙盒平台 — 沙盒平台检测超出	：在 1 小时内检测到的沙盒平台“低风险”或“中等风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置） ：在 1 小时内检测到的沙盒平台“高风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉 — URL 违例超过	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 4-5. 系统事件

事件	详细信息
帐户同步问题 — Box 访问令牌无效	：无法访问指定的云存储
帐户同步问题 — Dropbox 访问令牌无效	：无法访问指定的云存储
帐户同步问题 — Google 云端硬盘访问令牌无效	：无法访问指定的云存储
帐户同步问题 — 委派帐户上的同步问题	：无法与委派帐户同步

第 5 章

远程管理器中的 Cloud Edge

本节包含以下主题：

Cloud Edge

Cloud Edge 既有下一代内部部署防火墙的优势，又有安全即服务的便利性，可以为托管服务提供商带来双重优势。

通过深度扫描和过滤内部部署或云中的网络包，Cloud Edge 在网关中阻止威胁的攻击。Cloud Edge 可以智能地将应用程序控制与用户和端口识别、零天攻击检测、防恶意软件扫描、Web 信誉安全以及 URL 过滤结合起来，从而保护客户免受网络攻击和业务中断的影响。VPN 支持还保护移动设备、企业站点和远程员工的连接。

Cloud Edge 内部部署设备部署到客户在世界各地的办公点，通过直观的云控制台或趋势科技远程管理器集中控制用户访问和安全策略。远程管理器可以与 Cloud Edge 配合使用，提供单一点入口，以供访问图表报告和为支持的设备和趋势科技产品提供控制台数据总结。您可以使用远程管理器管理多个客户的许可和计费。

通过 Cloud Edge 设备注册客户

过程

1. 转至**客户** > **新客户**。

   此时会显示**选择新客户**窗口。

2. 选择**客户类型**。

   注意

   如果您使用的是 Licensing Management Platform 帐户，则将不会显示**选择客户类型**窗口。继续至第 4 步。

3. 单击**下一步**。

   此时会显示**输入客户信息**窗口。

4. 键入必填信息。

5. 单击**下一步**。

   此时会显示**分配服务计划**窗口。

6. 选择一个服务计划和开始日期。

7. 键入每个使用授权的单位数。

8. 可选：单击**添加设备**，然后为每个设备键入以下信息。

   - **设备名称**：键入一个与公司名称不同的名称。
   - **序列号**：序列号不区分大小写。

   注意

   设备数量不得超过指定的座席计数。

9. 单击**下一步**。

   此时会显示**配置产品缺省设置**窗口。

10. 选择缺省设置模板。

11. 可选：根据需要更改缺省模板。

    有关更多信息，请参阅为 Cloud Edge 配置缺省设置模板 第 17-19 页。

12. 单击**保存**。

    此时会关闭该窗口，然后显示**客户**窗口。

    注意

    由于 Licensing Management Platform 已与您的 Cloud Edge 帐户关联，因此，您无需输入凭证即可登录 Cloud Edge。

管理 Cloud Edge

通过远程管理器，可以为注册的 Cloud Edge 安装执行以下任务。

表 5-1. Cloud Edge 管理任务

任务	描述
为 Cloud Edge 分配沙盒平台服务计划	单击**添加**按钮，然后选择要分配到现有 Cloud Edge 设备的沙盒平台服务计划。
查看事件	从**事件**选项卡查看 Cloud Edge 事件的列表。
更新固件	从**固件更新**选项卡更新过期设备。
注册设备	从**设备**选项卡注册设备。
访问 Cloud Edge 控制台	单击**打开控制台**访问 Cloud Edge 控制台。

您还可以从产品树中选择已注册的设备，然后查看以下选项卡，了解有关特定设备的信息：

- **事件**
- **组件**
- **网络**
- **VPN**

Cloud Edge 事件

注意

Cloud Edge 中的某些威胁事件可能会显示其他渠道信息。

表 5-2. 威胁事件

事件类别	详细信息	事件状态
反垃圾邮件	垃圾邮件检测数	：在过去 1 小时检测到的垃圾邮件计数

事件类别	详细信息	事件状态
防病毒	病毒检测	：在过去 1 小时内检测到的病毒/恶意软件计数
僵尸网络	僵尸网络检测数	：在过去 1 小时检测到的僵尸网络计数
C&C 回调	C&C 回调	：在过去 1 小时内检测到的 C&C 回调计数
IPS	IPS 检测数	：在过去 1 小时检测到的 IPS 计数
预测型机器学习	预测型机器学习检测数	：在过去 1 小时检测到的预测型机器学习计数
勒索软件	勒索软件检测数	：在过去 1 小时内检测到的勒索软件计数
沙盒平台	沙盒平台检测数	：在过去 1 小时内检测到的沙盒平台计数
Web 信誉	URL 违例	：在过去 1 小时内阻止的 URL 计数
Web 威胁	Web 威胁检测数（包括 IPS、僵尸网络、防病毒或 Web 信誉违例）	：在过去 1 小时内检测到的 Web 威胁计数

表 5-3. 系统事件

事件类别	详细信息	事件状态
云电子邮件扫描	服务不可用	：Cloud Edge 无法连接到云扫描服务
	服务在过去 24 小时内暂时不可用	：Cloud Edge 在过去的 24 小时内暂时无法连接到云扫描服务

事件类别	详细信息	事件状态
固件更新	上次固件更新未成功。打开 <Cloud Edge 云控制台>了解详细信息。	：Cloud Edge 固件无法成功更新到最新的固件版本
	固件已过期	：当前版本的 Cloud Edge 固件已过期
脱机	网关脱机。策略部署和日志分析可能会受到影响。	：Cloud Edge 无法连接到网关或执行扫描
脱机 (过去 24 小时)	在过去 24 小时内网关脱机的出现次数。策略部署和日志分析可能已受到影响。	：Cloud Edge 在过去 24 小时内无法保持到所有注册网关的专用连接
资源短缺	检测到 <number> 个问题 • 超出了磁盘空间使用率 • 超出了 CPU 使用率 • 超出了的内存使用率	：设备上剩余的资源量下降到配置的警报阈值以下。
资源短缺（过去 24 小时）	检测到 <number> 个问题 • 超出了磁盘空间使用率 • 超出了 CPU 使用率 • 超出了的内存使用率	：设备上剩余的资源量在过去的 24 小时内下降到配置的警报阈值以下，但已恢复
已取消注册	无法执行云管理。此网关未注册到 Cloud Edge 云控制台。	：Cloud Edge 对网关执行扫描

Cloud Edge 通知

表 5-4. 威胁事件

事件	详细信息	警报阈值
Web 威胁 — Web 威胁检测超出	：在 1 小时内检测到的 Web 威胁计数超过了配置的阈值（如远程管理器控制台上的配置）	指定介于 1 到 300 之间的值。
C&C 回调 — C&C 回调检测超出	：在 1 小时内检测到的 C&C 回调计数超过了配置的阈值（如远程管理器控制台上的配置）	指定介于 1 到 100 之间的值。
勒索软件 — 勒索软件检测超出	：在 1 小时内检测到的勒索软件计数超过了配置的阈值（如远程管理器控制台上的配置）	指定介于 1 到 100 之间的值。

表 5-5. 系统事件

事件	详细信息	警报阈值
脱机 — 检测到脱机网关	：Cloud Edge 无法连接到网关或执行扫描	指定远程管理器何时发送通知： • **立即**：在 Cloud Edge 向远程管理器 报告事件时立即触发通知 • **超过 X 天**：如果网关在配置的天数内一直保持脱机状态，则触发通知
脱机 — 脱机设备恢复	：Cloud Edge 恢复到脱机设备的连接	不适用
云电子邮件扫描 — 服务不可用	：Cloud Edge 无法连接到云扫描服务	不适用
云电子邮件扫描 — 服务已恢复	：Cloud Edge 与云扫描服务的连接已恢复	不适用

事件	详细信息	警报阈值
资源短缺 — CPU、内存或磁盘使用率超出	 ：设备上剩余的资源量下降到配置的警报阈值以下。	在远程管理器触发通知之前，指定可以使用的最大数量的资源（介于 80% 到 95% 之间）

第 6 章

远程管理器中的 Hosted Email Security

本节包含以下主题：

Hosted Email Security

趋势科技™ Hosted Email Security 会将垃圾邮件、病毒、网络钓鱼和其他电子邮件威胁阻挡在您的网络之外，防患于未然。作为托管解决方案，它不需要安装和维护任何硬件或软件，可帮助您节省 IT 人员的时间，提高用户的工作效率，并释放带宽、邮件服务器存储空间和 CPU 容量。

此外，为了不断优化解决方案性能，趋势科技遍布全球的专家团队还会管理 Hot Fix、修补程序、更新和应用程序。

注意

有关 Hosted Email Security 的信息，请参阅以下网址上的文档：

http://docs.trendmicro.com

趋势科技远程管理器通过与位于趋势科技数据中心的 Hosted Email Security 服务器进行通信来监控和管理受 Hosted Email Security 保护的网络。

注册 Hosted Email Security

1. 在远程管理器 Web 控制台上添加新客户。
2. 添加主客户联系人。
3. 至少向该客户的帐户添加一项服务。
4. 在客户的服务控制台上输入授权码。

将 Hosted Email Security 客户连接到远程管理器 Web 控制台

要从趋势科技远程管理器 Web 控制台管理 Hosted Email Security，必须将客户的 Hosted Email Security 帐户注册到远程管理器。

注意

如果经销商已经通过 Licensing Management Platform 向您的帐户中添加了产品，则不需要执行以下步骤。

过程

1. 将产品添加到远程管理器 Web 控制台并保存 GUID 或授权码。
2. 登录到客户的 Hosted Email Security 帐户。
3. 转至**管理** > **远程管理器**。
4. 键入 GUID 或授权码，然后单击**连接**。

   输入 GUID 或授权码并单击**连接**后，Hosted Email Security 可能需要长达十分钟的时间才能完成与远程管理器 Web 控制台的连接。
5. 检查连接状态。

   新的 Hosted Email Security 数据可能需要长达三小时的时间才能在远程管理器 Web 控制台上更新。Hosted Email Security 客户信息每天更新一次。

断开 Hosted Email Security 客户与远程管理器 Web 控制台的连接

断开 Hosted Email Security 与远程管理器 Web 控制台的连接：

- 如果帐户已经与 Licensing Management Platform 集成，则经销商可以通过 Licensing Management Platform Web 控制台来删除服务计划。一旦删除了服务计划，客户将断开与远程管理器 Web 控制台的连接。
- 对于其他帐户，客户可以打开 Hosted Email Security Web 控制台上的远程管理器屏幕，然后单击**停止**。

客户随后会在 Hosted Email Security 控制台上收到通知，然后单击**确定**。

管理 Hosted Email Security

远程管理器可让您为注册的 Hosted Email Security 安装完成以下任务。

表 6-1. Hosted Email Security 管理任务

任务	描述
查看事件	从**实时状态**选项卡中查看 Hosted Email Security 事件列表。
查看策略	从**策略**选项卡中查看 Hosted Email Security 策略列表。
查看“允许的发件人”列表	从**允许的发件人**选项卡中查看允许的发件人的列表。
查看“被阻止的发件人”列表	从**被阻止的发件人**选项卡中查看被阻止的发件人的列表。
访问 Hosted Email Security 控制台	单击**打开控制台**访问 Hosted Email Security 控制台。

第 7 章

远程管理器中的 InterScan Web Security as a Service

本节包含以下主题：

InterScan Web Security as a Service

简单、快捷、经济高效的解决方案。

趋势科技深知保护您的网络安全非常重要，而要切实做到这一点需要采用昂贵的技术基础架构。因此，我们利用专业的云技术，打造了一款灵活的云安全网关产品 — InterScan Web Security as a Service (IWSaaS)。

该产品是一款基于云的应用程序，因此，无需在硬件和软件方面投入资本。通过使用 IWSaaS，您可以重点关注战略安全（如策略和体系结构），而不必在管理网络基础架构的运营任务方面劳心劳力。

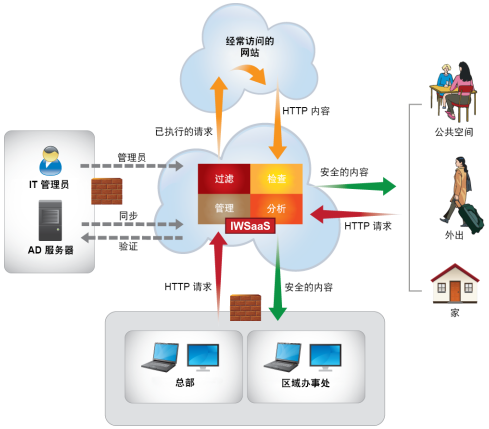
我们的云解决方案可以帮助您：

- 运用高度可配置的防恶意软件保护技术防御上传和下载文件中的病毒或其他安全风险。此外，IWSaaS 还可以扫描许多种间谍软件、灰色软件及其他种类的风险。
- 根据网站的信誉得分，屏蔽被 Web 信誉服务 (WRS) 确定为恶意网站的网站。
- 控制“应用程序控制”通过策略发现的 Internet 应用程序。
- 使用已允许/已阻止的列表控制对任意特定站点的访问权限。
- 扫描按 URL 类别（如“成人”和“赌博”）划分的流量。当有用户请求访问某个 URL 时，IWSaaS 会使用 URL 过滤策略，首先查看该 URL 的类别，然后根据设置的策略允许、拒绝或监控访问。
- 使用控制台报告和日志查询功能监控和分析 Web 流量状态。

IWSaaS 的工作原理

下图说明了 IWSaaS 如何在云中管理您的网络流量。当某个用户发送 **HTTP** 请求（不论在防火墙内部还是外部）后，该用户的流量会通过云路由。IWSaaS 会检查和分析请求，并根据管理员设置的策略过滤该请求。如果系统允许该请求且用户已登录 IWSaaS，则 IWSaaS 会将安全内容发回给用户。如果系统不允许

该请求（例如用户请求访问一个遭禁的 URL 类别），则 IWSaaS 会阻止该请求并通知用户。



点击任意页面上的蓝色问号按钮可以打开该页的帮助。页面级别的帮助显示在面板中。在此面板中，可在“步骤”选项卡中找到完成屏幕内容所需的信息，而且可在“更多”选项卡中找到支持此步骤的任何信息。

您可以访问内容类型的帮助的表格（位于主横幅部分的“帮助”菜单中的帮助内容），以及自述文件、入门说明和入门指南。

注册 InterScan Web Security as a Service (IWSaaS)

1. 在远程管理器 Web 控制台上添加新客户。
2. 向该客户的帐户添加 IWSaaS 服务。

   有关更多信息，请参阅使用 Licensing Management Platform 帐户添加新产品 第 3-8 页。

注意

由于 Licensing Management Platform 已与您的 IWSaaS 帐户关联，因此，您无需输入凭证即可登录 IWSaaS。

管理 InterScan Web Security as a Service

远程管理器可让您为注册的 InterScan Web Security as a Service (IWSaaS) 安装完成以下任务。

表 7-1. IWSaaS 管理任务

任务	描述
查看事件	查看 IWSaaS 事件列表。
访问 IWSaaS 控制台	单击**打开控制台**访问 IWSaaS 控制台。

InterScan Web Security as a Service 事件

表 7-2. 威胁事件

事件类别	详细信息	事件状态
防间谍软件	间谍软件/灰色软件检测	：在过去 24 小时内检测到的间谍软件/灰色软件计数
防病毒	病毒检测	：在过去 24 小时内检测到的病毒/恶意软件计数
应用程序控制	应用程序控制违例	：在过去 24 小时内检测到的应用程序控制违例计数
URL 过滤	URL 违例	：在过去 24 小时内检测到的 URL 过滤违例计数

事件类别	详细信息	事件状态
Web 信誉	URL 违例	 ：在过去 24 小时内阻止的 URL 计数

表 7-3. 系统事件

事件类别	详细信息	事件状态
帐户同步问题	AD/LDAP 同步问题	 ：无法与 AD/LDAP 同步

InterScan Web Security as a Service 通知

表 7-4. 系统事件

事件	详细信息
帐户同步问题 — AD/LDAP 同步问题	 ：无法与 AD/LDAP 同步

第 8 章

远程管理器中的安全无忧软件

本节包含以下主题：

安全无忧软件

趋势科技™安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版均是针对中小企业的全面的集中托管式解决方案。

安全无忧软件-网络安全版为台式机和服务器提供了客户端防病毒和防火墙防护功能。安全无忧软件-邮件与网络安全版中除了包含与安全无忧软件-网络安全版相同的功能，还为运行 Microsoft™ Exchange Server 的邮件服务器提供了反垃圾邮件和电子邮件威胁解决方案。安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版均包含服务器端组件，用于从中心位置监控和管理客户端防护。

趋势科技远程管理器通过与在安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版服务器上运行的客户端通信来监控和管理受安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版保护的网络。

有关安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版的更多信息，请参阅以下网址上的文档：

http://docs.trendmicro.com

注册安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版

1. 在远程管理器 Web 控制台上添加新客户。
2. 添加主客户联系人。
3. 至少向该客户的帐户添加一项服务。
4. 在客户的服务控制台上输入授权码。

客户端 GUID 或授权码

为了区分产品和服务，远程管理器向每个产品和服务均分配一个全局唯一标识符 (GUID) 或授权码。每次向远程管理器 Web 控制台添加某个产品或服务时，

远程管理器都会生成一个新的 GUID 或授权码。在托管服务器上安装客户端或向远程管理器 Web 控制台添加服务的用户，必须在安装过程中输入 GUID 或授权码，这样才能将产品注册到远程管理器。

用于客户产品/服务的 GUID 或授权码始终可从以下位置获得：**客户 > 所有产品（在树中） > {客户} > TMRM 客户端（选项卡）**。

图 8-1. 客户端 GUID 或授权码始终可用（“安全无忧软件-网络安全版”和“安全无忧软件-邮件与网络安全版”）

远程管理器客户端 GUID

```
1A2B3C4567D8-E1FGHI23-J456-78K9-1L23
```

安全无忧软件 6.0 及更高版本的客户端安装

在安全无忧软件-网络安全版或邮件与网络安全版 6.0 及更高版本的服务器上安装趋势科技远程管理器客户端的方法有多种。安装过程取决于客户是新客户还是已经在远程管理器 Web 控制台上有一个现有帐户。

验证趋势科技远程管理器客户端安装

验证客户端已成功安装。

检查客户端服务状态

在安装有远程管理器客户端的计算机上，检查是否启动了 `Trend Micro Information Center for CSM`。

过程

1. 单击**开始** > **设置** > **控制面板** > **管理工具** > **服务**。
2. 查找**趋势科技远程管理器**。
3. 检查**状态**是否为**已启动**。

查看“开始”菜单快捷方式

在安装有趋势科技远程管理器客户端的计算机上，选中“开始”菜单中的“程序组”。

过程

1. 单击**开始** > **程序** > **趋势科技远程管理器客户端**。
2. 验证“程序组”中包含以下项目：
   - 客户端配置工具
   - 自述

检查系统托盘图标

在安装有趋势科技远程管理器客户端的计算机上，在系统托盘中查找趋势科技远程管理器客户端图标。如果由于任何原因该图标不可见，您可以通过单击**开始** > **程序** > **趋势科技远程管理器代理** > **客户端配置工具**来启动它。

退出工具时不会停止趋势科技远程管理器服务。退出时只会关闭配置工具并从任务栏中删除该图标。您可以随时重新启动该工具。

将鼠标悬停在图标上可查看状态信息。

表 8-1. 系统托盘图标

图标	描述
	绿色图标，表示客户端已连接到趋势科技远程管理器通信服务器。客户端在正常运行。
	红色图标，表示客户端未连接到趋势科技远程管理器通信服务器，或客户端的版本与服务器不匹配，需要更新。
	带红色箭头的图标，表示客户端已从趋势科技远程管理器注销。
	带红色“X”的图标，表示客户端已禁用。

检查客户端和服务器之间的连接

为确保趋势科技远程管理器服务平稳运行，请确保远程管理器 Web 控制台上客户端的状态为“已连接”或“联机”。

转至**客户** > **{客户}** > **产品（选项卡）**。

树的**状态**栏中会列出每个客户端的状态。有关每种状态的详细信息，请参阅“客户端状态 第 8-6 页”。

除本节之外，另请参阅故障排除和常见问题解答 第 18-1 页，以了解有关服务器/客户端连接的更多问题。

管理客户端

本节包含以下主题：

从远程管理器 Web 控制台管理客户端

本节包含有关从 趋势科技™ 远程管理器™ Web 控制台管理客户端的信息。

检查客户端和服务器之间的连接

为确保趋势科技远程管理器服务平稳运行，请确保远程管理器 Web 控制台上客户端的状态为“已连接”或“联机”。

转至**客户** > **{客户}** > **产品（选项卡）**。

树的**状态**栏中会列出每个客户端的状态。有关每种状态的详细信息，请参阅“客户端状态 第 8-6 页”。

除本节之外，另请参阅故障排除和常见问题解答 第 18-1 页，以了解有关服务器/客户端连接的更多问题。

客户端状态

远程管理器客户端的状态会指示客户端是否能够从远程管理器服务器收集数据和接收其命令。状态还指示客户端无法正常运行的原因及如何处理该情况。下表描述了客户端的不同状态类型和处理对应情况的方法。

表 8-2. 客户端状态类型

状态	描述	解决方案
联机	客户端在正常运行。	无
异常	客户端显示为脱机，且无法对远程管理器服务器作出响应，但尚未发送注销请求。	如果托管服务器未正确关闭，则会出现此状态。确保托管服务器管理员知晓这一情况。如有必要，请与管理员联系。
已禁用	此状态需通过控制台手动设置。如果客户端处于已禁用状态，则该客户端会每 10 分钟查询一次来自服务器的命令。	提交命令以启用客户端（请参阅“提交客户端命令 第 8-8 页”）。
脱机	客户端在向远程管理器服务器发送注销请求后正常关闭。通常情况下，如果用户关闭了客户端服务或托管服务器被关闭，则客户端会处于此状态。	请确保托管服务器管理员知晓服务器已关闭。如有必要，请与托管服务器管理员联系。
未知	客户端运行不正常。	删除客户端并让托管服务器管理员重新安装客户端。如果此问题仍然存在，请与您的技术支持提供商联系。
插件错误	控制台检测到客户端服务插件组件中存在错误。	删除客户端并让托管服务器管理员重新安装客户端。如果此问题仍然存在，请与您的技术支持提供商联系。
已取消注册	客户端尚未注册到远程管理器服务器。	客户端可能尚未安装或无法成功与远程管理器服务器通信。请与托管服务器管理员联系。
版本不匹配	检测到以下组件版本之间不兼容： • 客户端 • 远程管理器 • 安全无忧软件（网络安全版和邮件与网络安全版）	升级客户端和托管服务器。如果不起作用，请将此问题报告给趋势科技数据中心管理员。

提交客户端命令

使用客户端命令，您可以远程解决影响安全无忧软件（网络安全版和邮件与网络安全版）客户端的问题。如果客户端处于“异常”或“已取消注册”状态，则无法向其提交命令。

过程

1. 转至**客户** > **{客户}** > **{产品}** > **组（选项卡）**。

   选择以下命令之一：

   - **立即扫描**：启动对端点的扫描。
   - **停止扫描**：停止扫描进程。

2. 转至**客户** > **{客户}** > **{产品}** > **域设置（选项卡）**。

   选择以下命令之一：

   - **启用**：将客户端从禁用状态恢复到正常工作状态。
   - **禁用**：客户端停止收集信息，但会继续每隔 10 分钟查询一次服务器命令。
   - **启动漏洞检查**：执行漏洞检查扫描。
   - **启动损害清除服务**：扫描并清除计算机中基于文件的病毒和网络病毒，以及病毒和蠕虫病毒残余。

3. 转至**客户** > **{客户}** > **{产品}** > **托管服务器（选项卡）**。

   选择以下命令之一：

   - **更新托管服务器**：下载并安装托管服务器更新。
   - **更新安全客户端**：下载并安装客户端更新。

查看客户端详细信息

过程

1. 转至**客户** > **{客户}** > **产品（选项卡）** > **WFBS-S/WFBS-A** > **端点**。

   将显示以下信息：

   - **状态**
   - **计算机名称**
   - **GUID**：全局唯一标识符；远程管理器会自动生成此字符串。请向将安装客户端程序的管理员提供 GUID。
   - **IP 地址**：安装客户端的服务器的 IP 地址。
   - **注册时间**
   - **上次更新时间**：客户端上次更新的日期和时间
   - **客户端版本**
   - **托管产品**：通过客户端托管的产品
   - **托管产品版本**：通过客户端托管的产品的版本

从托管服务器管理客户端

本节包含有关如何从托管服务器管理客户端的信息。

客户端状态消息

在托管服务器上，客户端会显示以下系统托盘图标之一：

表 8-3. 系统托盘图标

图标	描述
	绿色图标，表示客户端已连接到远程管理器通信服务器。客户端在正常运行。
	红色图标，表示客户端未连接到远程管理器通信服务器，或客户端的版本与服务器不匹配，需要更新。
	带红色箭头的图标，表示客户端已从远程管理器注销。
	带红色“X”的图标，表示客户端已禁用。

更改托管服务器上的客户端 GUID

如果您在远程管理器客户端安装期间输入了不正确的全局唯一标识符 (GUID)，请删除该客户端，然后使用正确的 GUID 重新安装。如果您无法进行这一步骤，请执行以下操作：

过程

1. 转至 `C:\Program Files\Trend Micro\TMRMAgentForWFBS`。
2. 使用文本编辑器打开 `AgentSysConfig.xml` 文件。
3. 在参数 `<AgentGUID>` 和 `</AgentGUID>` 之间查找 GUID。
4. 编辑 GUID，然后保存文件。
5. 在同一文件夹中，使用文本编辑器打开 `csmSysConfig.xml` 文件。
6. 在参数 `<ProductGUID>` 和 `</ProductGUID>` 之间查找 GUID。
7. 编辑 GUID，然后保存文件。
8. 右键单击任务栏上的趋势科技远程管理器客户端图标，然后单击**重新启动服务**。

使用客户端配置工具

可以使用客户端配置工具对远程管理器客户端配置设置进行更改。

转至**开始** > **程序** > **趋势科技远程管理器代理** > **客户端配置工具**，或右键单击托盘图标，然后单击**配置**。

请参阅“客户端配置 第 8-11 页”，了解详细信息。

客户端配置

客户端配置菜单

要配置客户端，请右键单击托盘图标以打开下面的菜单：

图 8-2. 客户端配置工具弹出菜单

将显示以下项：

- **配置**：打开客户端配置窗口。
- **选择语言**：除了其他可能的语言之外，“英语”始终存在。
- **服务**：“启动”、“停止”、“重新启动”。
- **退出**：退出工具时不会停止远程管理器服务。退出时只会关闭配置工具并从任务栏中删除该图标。您可以随时重新启动该工具。

配置工具主对话框

右键单击托盘图标，然后单击客户端配置菜单上的**配置**，打开客户端配置工具的**常规**选项卡。

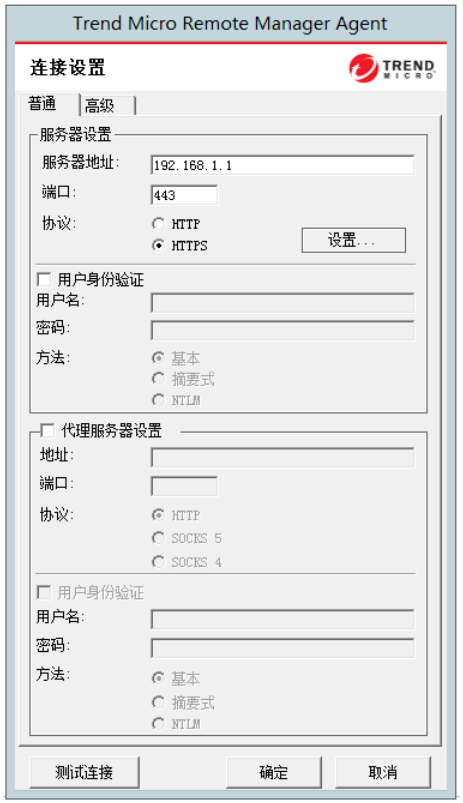


图 8-3. 客户端配置工具的“常规”选项卡

以下客户端配置窗口部分仅为此工具的当前相关部分。

- **服务器设置**：通过设置以下项可配置服务器通信：
  - **服务器地址**：远程管理器通信服务器的全限定域名 (FQDN)。每个地区的 FQDN 都各不相同，如下所示：

- **亚太地区**：wfrm-apaca.trendmicro.com
- **欧洲和中东地区**：wfrm-emea.trendmicro.com
- **日本**：wfrm-jpa.trendmicro.com
- **拉丁美洲**：wfrm-lara.trendmicro.com
- **北美**：wfrm-usa.trendmicro.com

- **端口**：远程管理器服务器用来与客户端通信的端口。该端口应该是 80 (HTTP) 和 443 (HTTPS)。
- **协议**：服务器与客户端之间的通信所使用的协议。

- **代理服务器设置**：如果用户的网络需要代理才能与远程管理器服务器通信，通过单击**代理服务器设置**复选框可启用此区域。
  - **地址**：代理服务器的 IP 地址
  - **端口**：代理服务器的端口
  - **协议**
- **测试连接**按钮：**测试连接**按钮用于测试客户端与远程管理器服务器之间的通信。使用此功能可测试与通信服务器间的基本连接是否正常。如果连接失败（如果工具无法连接到服务器，会显示一个弹出对话框），可能存在基本问题，如通信服务器地址及其端口，或代理服务器地址及其端口。

备份并恢复客户端设置

如果您需要卸载并在三天内重新安装使用相同 GUID 的客户端，请保留客户端设置，以避免任何重叠数据。为此，您需要手动备份配置文件，然后，在重新安装客户端后使用备份替换配置文件。

备份设置

过程

1. 在托管服务器上，右键单击客户端系统托盘图标，并单击**停止服务**以停止客户端服务。
2. 复制以下安装文件夹中的所有 .xml、.dat 和 .ini 文件：C:\Program Files\Trend Micro\TMRMAgentForWFBS 或 C:\Program Files (x86)\Trend Micro\TMRMAgentForWFBS。
   - .xml 文件
     - csmSysConfig.xml
     - csmLocalConfig.xml
     - csmLogDef.xml
     - AgentWorkConfig.xml
     - AgentSysConfig.xml
     - AgentStatus.xml
     - AgentLocalConfig.xml
   - .dat 文件
     - MSA.dat
     - logBuf.dat
     - group.dat
     - CSA.dat
     - CriticalVA.dat
   - .ini 文件
     - csmStatusData.ini

3. 复制 \Cache 文件夹中的所有的文件。
4. 重新启动客户端服务。

恢复设置

过程

1. 从本地删除客户端。

   注意

   在从本地删除客户端时，客户端将从远程管理器取消注册，并且与客户端关联的所有数据也会被自动删除。要阻止取消注册客户端，请在删除客户端之前，修改客户端界面上的服务器地址值。

2. 重新安装客户端。请确保您使用了相同的 GUID，该 GUID 可以从 agentSysConfig.xml 中获取。
3. 在托管服务器上，右键单击客户端系统托盘图标，并单击**停止服务**以停止客户端服务。
4. 使用备份文件替换配置文件。
5. 右键单击客户端系统托盘图标，并单击**启动服务**以重新启动客户端服务。

查找客户端 Build 号

您可以从控制台查看客户端的 build 号，也可以直接在客户端上查看 build 号。

通过远程管理器 Web 控制台

您可以在单个**<客户>**窗口的 **TMRM 客户端**选项卡下查找您设备上安装的 TMRM 客户端的当前 build 号。

过程

1. 转至**客户**。
2. 从“公司”列表中选择客户。该客户必须具有安全无忧软件-网络安全版或安全无忧软件-邮件与网络安全版。
3. 在**产品**选项卡的网络树下，单击**所有产品**旁边的箭头以展开列表。
4. 从列表中选择“安全无忧软件”。
5. 单击 **TMRM 客户端**选项卡。

   客户端版本的最后四位数字即为 build 号。

在客户端上查看

过程

1. 转至 `C:\Program Files\Trend Micro\WFRMAgentForCSM` 目录。
2. 右键单击 `csmplugin.dll` 文件，然后单击**属性** > **版本（选项卡）**以查看 build 号。

管理安全无忧软件

远程管理器可让您为已安装并注册的安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版完成以下任务。

表 8-4. 安全无忧软件管理任务

任务	描述
查看事件	从**事件**选项卡查看安全无忧软件事件的列表。
扫描组	从**组**选项卡开始或停止扫描。

任务	描述
管理域设置	从**域设置**选项卡执行以下任意任务。 • 启用域设置 • 禁用域设置 • 启动漏洞检查 • 启动损害清除服务
管理托管服务器	从**托管服务器**选项卡执行以下任意任务。 • 更新托管服务器 • 更新安全客户端 • 查看组件状态
查看远程管理器客户端信息	从 **TMRM 客户端**选项卡查看远程管理器客户端信息。
保存服务器信息	单击**服务器信息**，以保存和访问有关安全无忧软件服务器的信息。

安全无忧软件事件

表 8-5. 威胁事件

事件类别	详细信息	事件状态
反垃圾邮件	在收到的所有邮件中检测到的垃圾邮件数量超出	：在 1 个小时内在收到的所有邮件中检测到的垃圾邮件比率超过了配置的阈值（如受管产品控制台上的配置）
防间谍软件	需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
	间谍软件/灰色软件检测超出	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
防病毒	已在终端上禁用实时扫描	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
	已在 Exchange 服务器上禁用实时扫描	：已禁用实时扫描的 Exchange 服务器允许电子邮件中的所有附件通过，这会使客户网络容易感染群发邮件蠕虫病毒。
	未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
	终端上的病毒检测超出	：在 1 小时内在终端上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
	Exchange 服务器上的病毒检测超出	：在 1 小时内在 Exchange 服务器上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控	行为监控违例超出	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）
设备控制	设备控制违例超出	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒	网络病毒检测超出	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
爆发防御	爆发防御已启用	：已在桌面/服务器平台上启用爆发防御来应对异常威胁活动
	爆发防御已禁用	：已在桌面/服务器平台上禁用爆发防御并且已恢复正常的网络条件
URL 过滤	URL 违例超出	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉	URL 违例超出	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 8-6. 系统事件

事件类别	详细信息	事件状态
资源短缺	剩余磁盘空间小于	：服务器上剩余的磁盘空间下降到配置的警报阈值以下。
云安全智能防护服务	服务不可用	：安全无忧软件控制台无法连接到云安全服务器
更新	客户端已过期	：在过去一个小时内，超过 <number> 个安全客户端未收到最新的防病毒特征码
	Exchange 服务器已过期	：在 Exchange 服务器上检测到过期组件

安全无忧软件通知

表 8-7. 威胁事件

事件	详细信息
反垃圾邮件 — 在收到的所有邮件中检测到的垃圾邮件数量超出	：在 1 个小时内在收到的所有邮件中检测到的垃圾邮件比率超过了配置的阈值（如受管产品控制台上的配置）
防间谍软件 — 需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
防间谍软件 — 间谍软件/灰色软件检测超过	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒 — 已在终端上禁用实时扫描	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
防病毒 — 已在 Exchange 服务器上禁用实时扫描	：已禁用实时扫描的 Exchange 服务器允许电子邮件中的所有附件通过，这会使客户网络容易感染群发邮件蠕虫病毒。
防病毒 — 未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
防病毒 — 终端上的病毒检测超出	：在 1 小时内在终端上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒 — Exchange 服务器上的病毒检测超出	：在 1 小时内在 Exchange 服务器上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）

事件	详细信息
行为监控 — 行为监控违例超过	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）
设备控制 — 设备控制违例超过	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒 — 网络病毒检测超过	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）
URL 过滤 — URL 违例超过	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉 — URL 违例超过	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 8-8. 系统事件

事件	详细信息
资源短缺 — 剩余磁盘空间小于	：服务器上剩余的磁盘空间下降到配置的警报阈值以下。
云安全智能防护服务 — 服务不可用	：安全无忧软件控制台无法连接到云安全服务器
更新 — Exchange 服务器已过期	：在 Exchange 服务器上检测到过期组件
更新 — 过期的客户端	：在过去一个小时内，超过 <number> 个安全客户端未收到最新的防病毒特征码

第 9 章

远程管理器中的安全无忧软件-云端版

本节包含以下主题：

安全无忧软件-云端版

趋势科技™安全无忧软件-云端版是针对中小企业的全面的集中托管式解决方案。

安全无忧软件-云端版具有安全无忧软件-网络安全版的大多数优势，并且由于安全无忧软件-云端版是托管服务，因此您可以从任何位置集中管理安全性，而无需添加、安装、配置或维护服务器。趋势科技安全专家会为您托管并持续更新服务。

趋势科技远程管理器监控和管理趋势科技数据中心的安全无忧软件-云端版服务器。

有关安全无忧软件-云端版的更多信息，请参阅以下网址上的文档：

http://docs.trendmicro.com

注册安全无忧软件-云端版

过程

1. 转至**客户** > **新客户**。

   此时会显示**选择新客户**窗口。

2. 选择**客户类型**。

   注意

   如果您使用的是 Licensing Management Platform 帐户，则将不会显示**选择客户类型**窗口。继续至第 4 步。

3. 单击**下一步**。

   此时会显示**输入客户信息**窗口。

4. 键入必填信息。

5. 单击**下一步**。

   此时会显示**分配服务计划**窗口。

6. 选择一个服务计划和开始日期。

7. 键入每个使用授权的单位数。

8. 单击**下一步**。

   此时会显示**配置产品缺省设置**窗口。

9. 选择缺省设置模板。

10. 可选：根据需要更改缺省模板。

    有关更多信息，请参阅为安全无忧软件-云端版配置缺省设置模板 第 17-17 页。

11. 单击**保存**。

    此时会关闭该窗口，然后显示**客户**窗口。

注意

由于 Licensing Management Platform 已关联至您的安全无忧软件-云端版帐户，您无需再输入凭证以登录安全无忧软件-云端版。

将安全无忧软件-云端版的客户连接到远程管理器 Web 控制台

要将安全无忧软件-云端版的客户连接到趋势科技远程管理器 Web 控制台，请执行以下操作：

注意

如果经销商已经通过 Licensing Management Platform 向您的帐户中添加了产品，则不需要执行以下步骤。

过程

1. 将产品添加到远程管理器 Web 控制台并保存 GUID 或授权码。

   有关更多信息，请参阅使用 Licensing Management Platform 帐户添加新产品 第 3-8 页。

2. 登录到客户的安全无忧软件-云端版帐户。

3. 转至**管理** > **趋势科技远程管理器**。

4. 键入授权码，然后单击**连接**。

断开安全无忧软件-云端版客户与远程管理器 Web 控制台的连接

断开安全无忧软件-云端版与远程管理器 Web 控制台的连接：

- 如果帐户已经与 Licensing Management Platform 集成，则经销商可以通过 Licensing Management Platform Web 控制台来删除服务计划。一旦删除了服务计划，客户将断开与远程管理器 Web 控制台的连接。
- 对于其他帐户，客户可以打开安全无忧软件-云端版 Web 控制台上的远程管理器屏幕，然后单击**断开连接**。

客户随后将会在安全无忧软件-云端版控制台上收到通知。

管理安全无忧软件-云端版

远程管理器可让您为已安装并注册的安全无忧软件-云端版完成以下任务：

表 9-1. 安全无忧软件-云端版管理任务

任务	描述
查看事件	从**事件**选项卡查看安全无忧软件-网络安全版事件的列表。

任务	描述
管理组	**组**选项卡允许您执行以下任务： • 开始或停止扫描 • 更新安全客户端 • 复制客户端设置 从表中选择**组类型**，然后单击所需的任务按钮。
访问安全无忧软件-云端版控制台	单击**打开控制台**，访问安全无忧软件-云端版控制台。

安全无忧软件-云端版的安全设置

功能	描述
扫描方法	• **云安全扫描**：客户端使用其自身的扫描引擎，但并非仅使用本地特征码文件来识别威胁，而是主要依靠扫描服务器上的特征码文件。 • **传统扫描**：客户端使用其自身的扫描引擎和本地特征码文件来识别威胁。
防病毒/防间谍软件	• **启用实时防病毒/防间谍软件**：实时扫描可以防范基于文件的威胁。
防火墙	• **启用防火墙**：防火墙可以在客户端和网络之间构建屏障，从而阻止或允许特定类型的网络流量。另外，防火墙还会识别网络数据包中可能指示对客户端造成攻击的特征码。 • **简单模式: 启用防火墙，且使用趋势科技缺省设置** • **高级模式: 配置安全等级、IDS、通知和例外。** **重要信息** 选择高级模式后，您必须使用安全无忧软件-云端版控制台配置高级设置。

功能	描述

Web 信誉	• **启用 Web 信誉**：Web 信誉可增强抵御恶意网站的能力。Web 信誉利用趋势科技丰富的 Web 安全数据库来检查客户端试图访问的 URL 或用于联系网站的电子邮件中嵌入的 URL 的信誉。
	  • **高**：阻止以下页面：
	  • **危险**：已验证为诈骗网页或已知威胁来源
	  • **高度可疑**：可能是诈骗网页或威胁来源
	  • **可疑**：与垃圾邮件关联或可能危及安全的页面
	  • **未测试**：尽管趋势科技会主动测试 Web 页面的安全性，但用户在访问新的或不常见的 Web 站点时，可能会遇到未经测试的页面。虽然阻止访问未经测试的页面可以提高安全性，但也会阻止访问安全页面
	  • **中**：阻止以下页面：
	  • **危险**：已验证为诈骗网页或已知威胁来源
	  • **高度可疑**：可能是诈骗网页或威胁来源
	  • **低（缺省设置）**：阻止以下页面：
	  • **危险**：已验证为诈骗网页或已知威胁来源

URL 过滤	• **启用 URL 过滤**：URL 过滤可帮助您控制对网站的访问，从而缩短无效率的员工时间、减少 Internet 带宽使用量，以及营造更加安全的 Internet 环境。您可以选择 URL 过滤防护等级，或自定义想要筛选的网站类型。
	  • **高**：阻止已知或潜在的安全威胁、不适当或可能存在冒犯性的内容、可能会影响生产效率或带宽的内容以及未评级的页面
	  • **中**：阻止已知的安全威胁和不适当的内容
	  • **低（缺省设置）**：阻止已知的安全威胁
	  • **自定义**：选择您自己的类别，以及您是否想在工作时间或业余时间阻止这些类别。

功能	描述

行为监控	• **启用行为监控**：行为监控可保护客户端，防止对操作系统、注册表项、其他软件或文件和文件夹进行未授权的更改。
	  • **启用所有勒索软件防护功能**
	  • **启用文档保护，使其免遭未授权的加密或修改**：保护文档，避免未授权更改。
	  注意
	  启用此选项会停止用于重命名、修改和删除文件的进程，然后隔离正在运行这些进程的程序。
	  • **自动备份和恢复被可疑程序修改的文件**：若启用了文档保护，则自动备份被可疑程序修改的文件。
	  • **针对通常与勒索软件关联的进程启用阻止**：阻止通常与网络劫持尝试相关的进程，从而保护终端免受勒索软件的攻击。
	  • **启用程序检查以检测并阻止可能危及安全的可执行文件**：通过监控进程中类似勒索软件的行为来提升检测。
	  • **启用 Intuit QuickBooks 防护**：保护所有 Intuit QuickBooks 文件和文件夹，防止其他程序进行未经授权的更改。启用此功能将不会影响在 Intuit QuickBooks 程序中所做的更改，只会防止其他未经授权的应用程序更改此文件。

功能	描述

预测型机器学习	• **启用预测型机器学习**：预测型机器学习可通过高级文件特征分析和启发式进程监控保护您的网络免遭新的、以前未识别的或未知威胁的攻击。
	  • **文件**
	  • **隔离**：选择此选项可自动隔离预测型机器学习分析结果指示存在恶意软件相关特征的文件
	  • **仅记录**：选择此选项可扫描未知文件，并记录预测型机器学习分析结果，以进行进一步的内部威胁调查
	  • **进程**
	  • **终止**：选中可根据预测机器学习分析自动终止表现出恶意软件相关行为的进程或脚本
	  重要信息
	  预测机器学习将尝试清除已执行恶意进程或脚本的文件。如果清除处理措施未成功，则预测机器学习将隔离受影响的文件。
	  • **仅记录日志**：选中可扫描未知进程或脚本并记录预测机器学习分析，进一步对威胁开展内部调查

邮件扫描	• **启用 POP3 邮件扫描**：POP3 邮件扫描插件可实时保护客户端免受安全风险威胁及通过 POP3 电子邮件传送的垃圾电子邮件干扰。

有关详情，请参阅安全无忧软件-云端版联机帮助。

安全无忧软件-云端版事件

表 9-2. 威胁事件

事件类别	详细信息	事件状态
防间谍软件	需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
	间谍软件/灰色软件检测超出	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒	实时扫描已禁用	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
	未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
	病毒检测超出	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
应用程序控制	应用程序控制违例超出	：在 1 小时内检测到的应用程序控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控	行为监控违例超出	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
设备控制	设备控制违例超出	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒	网络病毒检测超出	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）
爆发防御	爆发防御已启用	：已在桌面/服务器平台上启用爆发防御来应对异常威胁活动
	爆发防御已禁用	：已在桌面/服务器平台上禁用爆发防御并且已恢复正常的网络条件
预测型机器学习	预测型机器学习检测超出	：在 1 小时内检测到的预测型机器学习计数超过了配置的阈值（如受管产品控制台上的配置）
URL 过滤	URL 违例超出	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉	URL 违例超出	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 9-3. 系统事件

事件类别	详细信息	事件状态
云安全智能防护服务	客户端已断开连接	：安全客户端无法连接到云安全智能防护网络
更新	客户端已过期	：在防病毒特征码发布两个小时后具有过期特征码的安全客户端超过了阈值

安全无忧软件-云端版通知

重要信息

对于具有可配置的阈值的事件，必须在安全无忧软件-云端版控制台上分别为每个客户配置阈值。

表 9-4. 威胁事件

事件	详细信息
防病毒 — 未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
防病毒 — 实时扫描已禁用	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
防病毒 — 病毒检测超过	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
防间谍软件 — 需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
防间谍软件 — 间谍软件/灰色软件检测超过	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉 — URL 违例超过	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）
URL 过滤 — URL 违例超过	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）

事件	详细信息
预测型机器学习 — 预测型机器学习检测超过	：在 1 小时内检测到的预测型机器学习计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控 — 行为监控违例超过	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒 — 网络病毒检测超过	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）
设备控制 — 设备控制违例超过	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
应用程序控制 — 应用程序控制违例超过	：在 1 小时内检测到的应用程序控制违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 9-5. 系统事件

事件	详细信息
更新 — 过期的客户端	：在防病毒特征码发布两个小时后具有过期特征码的安全客户端超过了阈值
云安全智能防护服务 — 客户端已断开连接	：安全客户端无法连接到云安全智能防护网络

部分 IV

集成第三方解决方案

第 10 章

AutoTask 支持

本节介绍如何向远程管理器集成 Autotask 以及趋势科技产品和服务支持的事件通知。

主题包括：

集成 Autotask™

通过配置以下设置将 Autotask™ 与远程管理器集成：

集成远程管理器与 Autotask

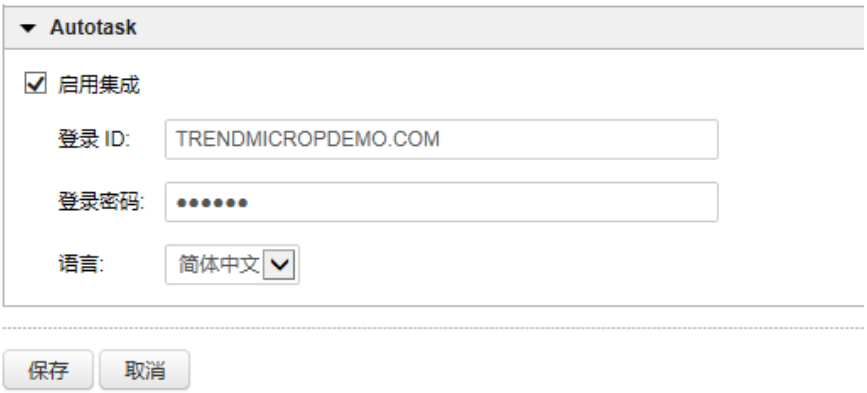
过程

1. 访问 https://ww2.autotask.net，登录 Autotask Web 控制台。
2. 转至 **Autotask Logo Menu** > **ADMIN**。

   此时，**ADMIN** 窗口将显示出来。
3. 展开 **APPLICATION-WIDE (SHARED) FEATURES**，然后单击 **Incoming Email Processing**。

   此时，**INCOMING EMAIL PROCESSING** 窗口将显示出来。
4. 将鼠标悬停在 **Add Ticket Email Service (ATES)** 菜单图标 上，然后单击 **Edit**。

   此时，**EMAIL PROCESSING MAILBOX - ADD TICKET EMAIL SERVICE (ATES)** 窗口将显示出来。
5. 记下您的 **Service Provider ID** 和 **Service Provider Password**，以便稍后输入这些详细信息。
6. 登录远程管理器 Web 控制台。
7. 转至**管理** > **配置第三方集成**。
8. 在 **Autotask** 部分，选择**启用集成**，然后键入你之前记下的**登录 ID** 和**登录密码**。从**语言**下拉菜单中，选择首选语言。



9. 单击**保存**。
10. 转至**客户**窗口。
11. 选择您想通过其接收 Autotask 通知的公司。
12. 单击**通知**选项卡。
13. 选择**我**作为收件人，以确保您将收到电子邮件通知。必要时可以添加其他收件人，只需在**其他收件人**文本框中键入其电子邮件地址即可。
14. 从**第三方通知**列表中选择 **Autotask**。

15. 选择以下选项之一：
    - **使用缺省实时电子邮件通知设置**
    - **使用自定义设置**

启用 Autotask 以显示远程管理器通知

过程

1. 访问 https://ww2.autotask.net，登录 Autotask Web 控制台。
2. 转至 **Autotask Logo Menu** > **ADMIN**。

   此时，**ADMIN** 窗口将显示出来。
3. 展开 **SERVICE DESK (TICKETS)**，然后转至 **Issue & Sub-Issue Types** > **Managed Services Alert**。
4. 将下列文本框添加到出票系统中：
   - **趋势科技威胁事件**
   - **趋势科技系统事件**
   - **趋势科技使用授权事件**
5. 单击 **Save & Close**。
6. 转至 **Autotask Logo Menu** 以返回 **ADMIN** 页面。
7. 展开 **APPLICATION-WIDE (SHARED) FEATURES**，然后转至 **Incoming Email Processing**。

   此时，**INCOMING EMAIL PROCESSING** 窗口将显示出来。
8. 将光标指向 **Add Ticket Email Service (ATES)** 菜单图标  ，然后单击 **Edit**。

   此时，**EMAIL PROCESSING MAILBOX - ADD TICKET EMAIL SERVICE (ATES)** 窗口将显示出来。

9. 单击 **Ticket** 选项卡。
10. 从 **Sub-Issue Type** 下拉菜单中选择 **Trend Micro Threat Events**。
11. 单击 **Save & Close**。
12. 转至 **Autotask Logo Menu** 以返回 **ADMIN** 页面。
13. 展开**应用程序范围(共享)功能**，然后转至**用户定义字段** > **+ 新建**。

    此时，**USER-DEFINED FIELDS** 窗口将显示出来。
14. 在 **Name** 文本框中，键入 `Trend Micro Site ID`，然后选中 **Required** 复选框。
15. 单击 **Save & Close**。

启用 Autotask 以生成帐户票证

过程

1. 转至 **Autotask Logo Menu** > **CRM**。

   此时，**ACCOUNT SEARCH** 窗口将显示出来。
2. 单击 **+ New Account**。在新打开的弹出窗口中，输入帐户信息，**Trend Micro Site ID** 也要一并输入进去。

   注意

   Trend Micro Site ID 是从远程管理器中导出的唯一 ID。登录远程管理器控制台然后转至 **Customers** > **Export All**，即可找到该 ID。在导出的 `.csv` 文件中，**Unique ID** 位于 **Company** 名称的右侧。
3. 单击 **Save & Close**。
4. 转至 **CRM** > **My Account Tickets**（在 **Reports** 下），以查看您的帐户票证。

在 Autotask 中受支持的趋势科技产品事件

远程管理器可以向 Autotask 系统发送以下事件通知。

产品	事件	
Cloud Edge	• 僵尸网络 • 入侵防御系统 (IPS)	• Web 信誉 • 病毒
Hosted Email Security	• 电子邮件总流量 • 已接受的电子邮件大小 • 威胁摘要	• 收到垃圾邮件最多的收件人 • 收到病毒最多的收件人
InterScan Web Security as a Service	• 防病毒 • 防间谍软件 • Web 信誉	• URL 过滤 • 应用程序控制
安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版	• 客户端异常 • 爆发防御 • 防病毒 • 防间谍软件 • Web 信誉 • 行为监控 • 网络病毒 • 反垃圾邮件 • 托管服务器已过期	• 系统异常事件 • 使用授权到期 • URL 过滤 • 设备控制 • Exchange Server 关闭 • Active Directory 同步问题 • 安全无忧软件-网络安全版和安全无忧软件-邮件与网络安全版服务器关闭

产品	事件	
安全无忧软件-云端版	• 客户端异常 • 爆发防御 • 防病毒 • 防间谍软件 • Web 信誉 • 行为监控 • 网络病毒	• 托管服务器已过期 • 系统异常事件 • 使用授权到期 • URL 过滤 • Exchange Server 关闭 • Active Directory 同步问题

第 11 章

ConnectWise Manage 支持

本节介绍如何向远程管理器集成 ConnectWise Manage 以及趋势科技产品和服务受支持的事件通知。

主题包括：

集成 ConnectWise Manage™

ConnectWise Manage 是专业服务自动化 (PSA) 以及远程监控和管理 (RMM) 解决方案，它可以提供托管服务提供商和经销商实时控制台和报告、事件管理、服务资产和配置管理，以及自动结算服务。

远程管理器可以电子邮件（转换为 ConnectWise Manage 票证）形式向 ConnectWise Manage 发送事件信息。为此，必须将通知收件人添加到远程管理器 Web 控制台，并在 ConnectWise Manage 票证系统中添加一些文本框。

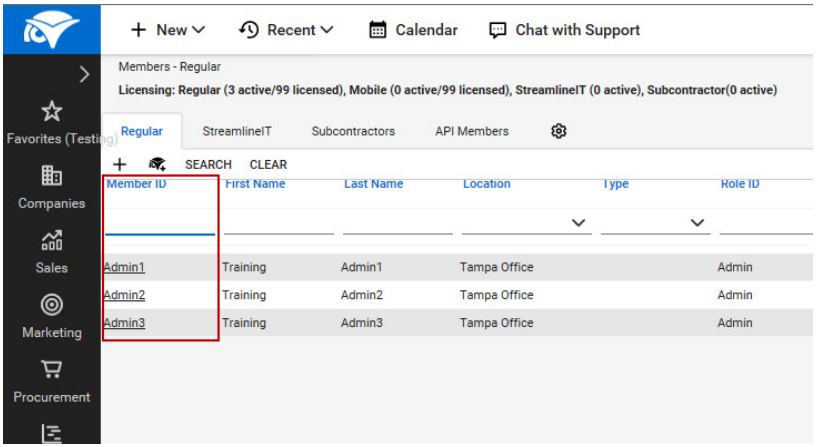
要成功集成远程管理器，开始接收通知并在 ConnectWise Manage 中生成帐户票证，请确保完成必需的集成步骤。

将 ConnectWise Manage 和远程管理器客户集成

在可以开始设置帐单周期、监控垃圾邮件统计信息或在 ConnectWise Manage 中为趋势科技远程管理器客户接收通知之前，您必须先识别 ConnectWise Manage 客户并将其与对应的趋势科技远程管理器客户关联。

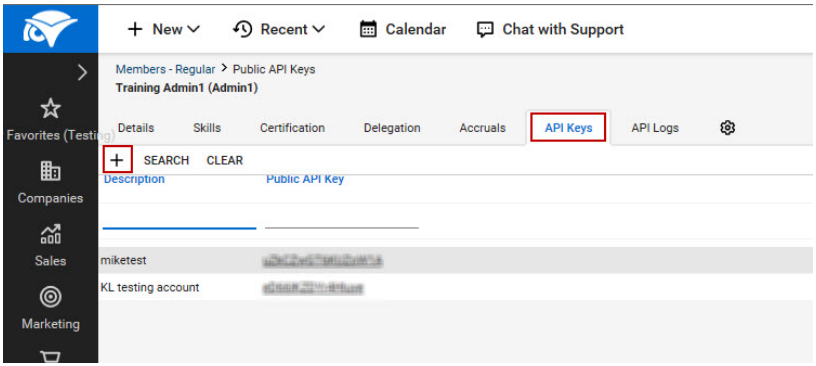
过程

1. 使用 ConnectWise Manage 控制台来获取 ConnectWise Manage 与趋势科技远程管理器通信所需的 API 密钥。
   a. 打开 ConnectWise Manage 控制台。
   b. 转至 **System** > **Members**。



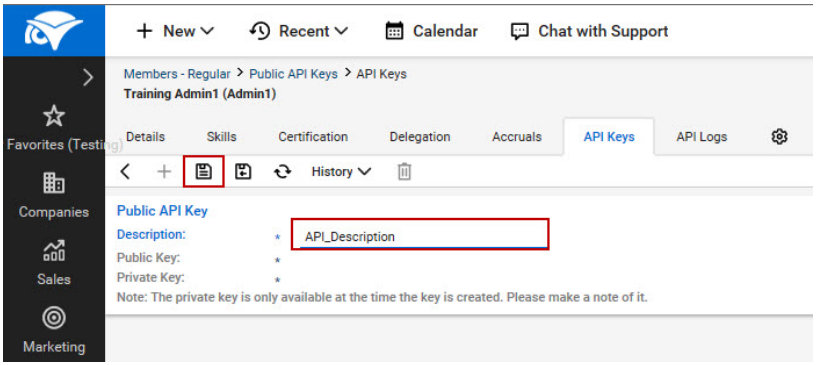
c. 单击负责 API 密钥的 **Member ID**。

d. 单击 **API Keys** 选项卡。



e. 单击 **New Item** (➕)。

f. 在 **Description** 中键入 API 密钥的描述。



g. 单击 **Save**。

重要信息

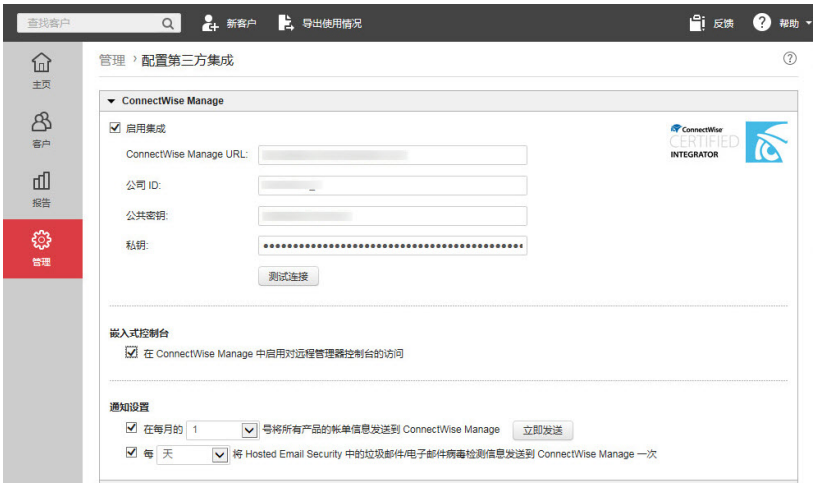
ConnectWise Manage 为新条目分配**公共密钥**和**私有密钥**。**私有密钥**将仅显示一次。请小心复制**私有密钥**。如果丢失私有密钥，则无法重新恢复**私有密钥**，并且必须创建新条目和重新配置远程管理器服务器。

2. 在趋势科技远程管理器控制台中配置全局 ConnectWise Manage 集成设置。

   a. 打开趋势科技远程管理器控制台。

   b. 转至**管理** > **配置第三方集成**。

此时会显示**配置第三方集成**窗口。



c. 在 **ConnectWise Manage** 部分中，选择**启用集成**，以允许 ConnectWise Manage 接收来自趋势科技远程管理器的通知。

- **ConnectWise Manage URL：**键入 ConnectWise Manage URL 或 FQDN。

  注意

  缺省情况下，趋势科技远程管理器自动使用 HTTPS 与 ConnectWise Manage 服务器通信。如果您的公司需要 HTTP 通信，则必须指定 URL 而不是 FQDN。

- **公司 ID：**键入用于登录 ConnectWise Manage 控制台的公司名称。
- **公共密钥：**指定趋势科技远程管理器用于加密与 ConnectWise Manage 的通信的 ConnectWise Manage 公共密钥
- **私有密钥：**指定用于对来自趋势科技远程管理器的通信进行解密的 ConnectWise Manage 私有密钥

d. 单击**测试连接**以验证与 ConnectWise Manage 的连接。

注意

如果不单击**测试连接**，则在您单击**保存**按钮时，趋势科技远程管理器会自动验证与 ConnectWise Manage 的连接。

e. 单击**保存**。

3. 在趋势科技远程管理器控制台上识别各个趋势科技远程管理器客户并将其与 ConnectWise Manage 客户关联。

a. 打开趋势科技远程管理器控制台。

b. 转至**客户** > **[客户]**。

c. 要集成此客户的 ConnectWise Manage 设置，请单击 **ConnectWise Manage** 选项卡。

d. 选择**启用集成**。

e. 指定此客户的 **ConnectWise 公司 ID**。

访问 ConnectWise Manage 控制台，以查找特定客户的公司 ID。

提示

单击**验证**以确保 ConnectWise Manage 中存在该公司 ID。

f. 单击**保存**。

g. 为每个 ConnectWise Manage 客户重复以上步骤。

您可以使用趋势科技远程管理器和 ConnectWise Manage 控制台来：

- 监控 Hosted Email Security 垃圾邮件统计信息 第 11-9 页
- 管理客户帐单 第 11-15 页
- 监控客户通知 第 11-25 页

将趋势科技产品添加到 ConnectWise Manage

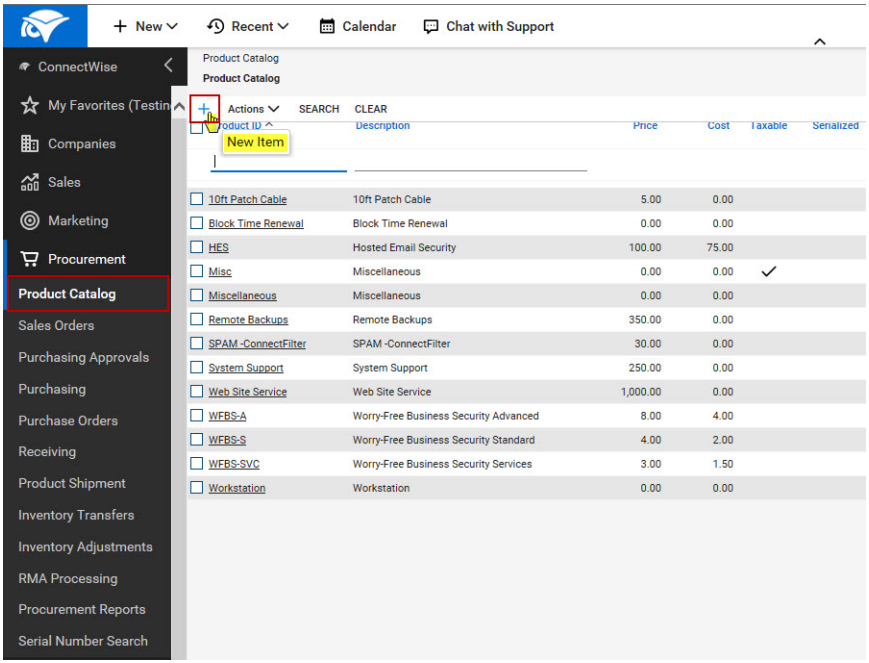
将以下趋势科技远程管理器产品/服务与 ConnectWise Manage 相集成，以便于结算：

- 安全无忧软件-网络安全版
- 安全无忧软件-邮件与网络安全版
- 安全无忧软件-云端版
- Hosted Email Security

过程

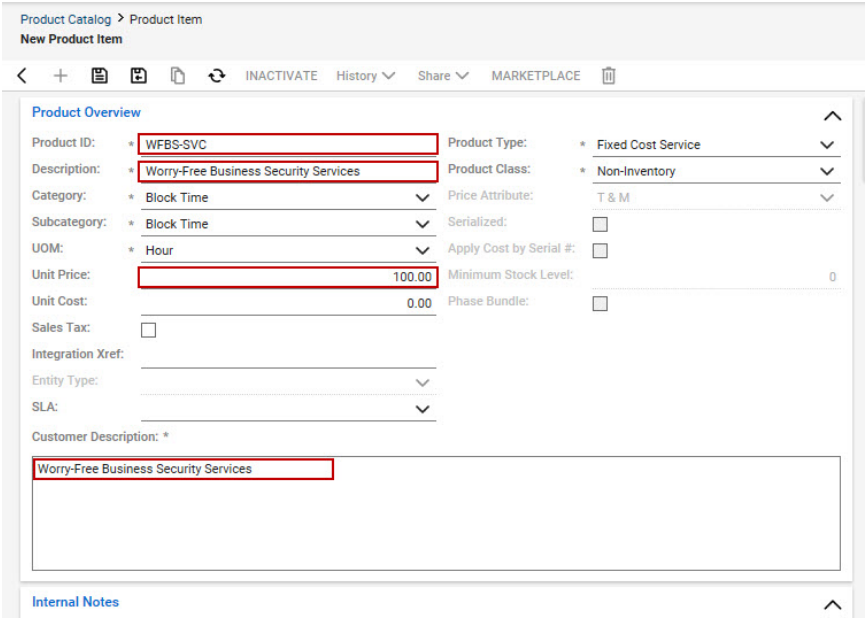
1. 在 ConnectWise Manage 控制台中，转至 **Procurement** > **Product Catalog**

   此时会显示 **Product Catalog** 窗口。



2. 单击 **New Item** (➕)，以添加新产品。

   此时会显示 **New Product Item** 窗口。



3. 在 **Product ID** 文本框中键入所需的趋势科技远程管理器托管产品/服务的产品 ID。

表 11-1. 用于 ConnectWise Manage 集成的趋势科技产品 ID

产品/服务	产品 ID
安全无忧软件-网络安全版	WFBS-S
安全无忧软件-邮件与网络安全版	WFBS-A
安全无忧软件-云端版	WFBS-SVC
Hosted Email Security	HES

4. 指定以下信息：

- **Description**
- **Unit Price**
- **Customer Description**

5. 单击 **Save**。

   ConnectWise Manage 会将新产品添加到 **Product Catalog** 中。

监控 Hosted Email Security 垃圾邮件统计信息

在可以为 Hosted Email Security 客户开始监控垃圾邮件统计信息之前，您必须先将 ConnectWise Manage 客户与趋势科技远程管理器进行集成。

有关更多信息，请参阅将 ConnectWise Manage 和远程管理器客户集成 第 11-2 页。

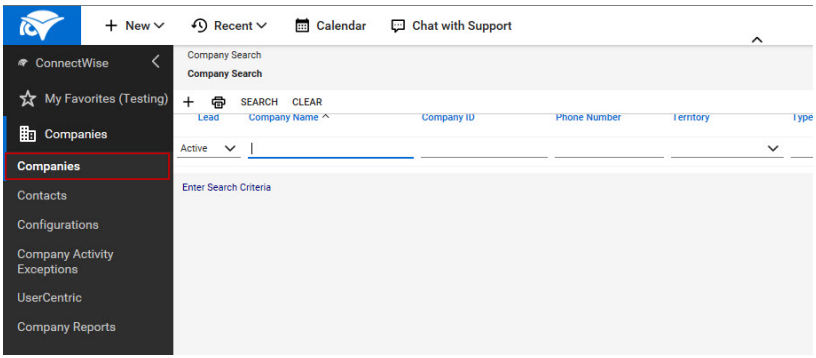
集成这两种产品和关联客户帐户之后，您可以为客户配置垃圾邮件统计信息设置。

过程

1. 配置 ConnectWise Manage 客户，以监控垃圾邮件统计信息。

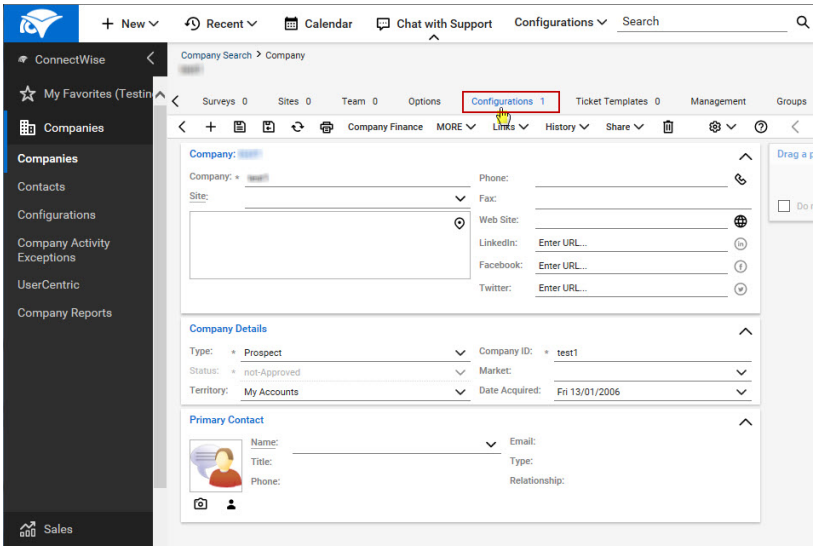
   a. 在 ConnectWise Manage 控制台中，转至 **Companies** > **Companies**。

      此时，**Company Search** 窗口将显示出来。



b. 在 **Company Name** 文本框中键入公司名称，然后单击 **Search**。

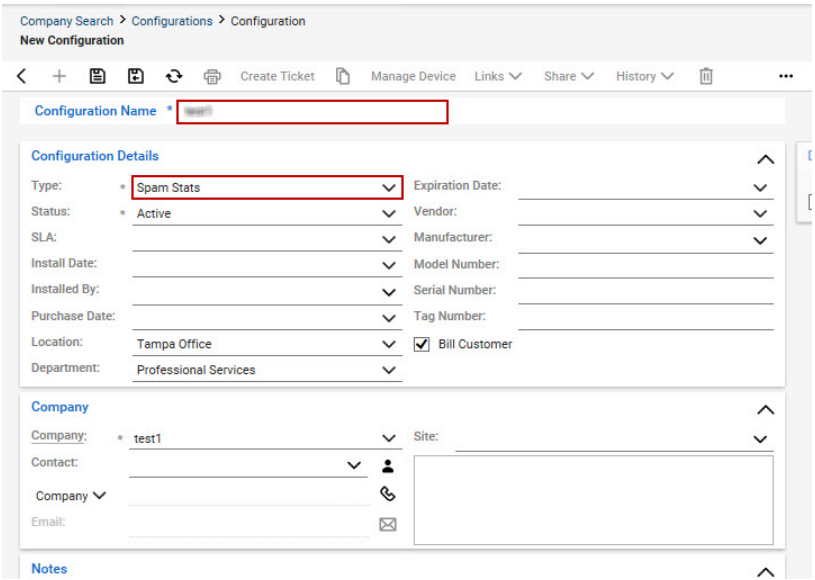
此时，**{Company}** 窗口将显示出来。



c. 单击 **Configurations** 选项卡。

d. 单击 **New Item** (➕)，以创建新配置。

此时，**New Configuration** 窗口将显示出来。



e. 在 **Configuration Name** 文本框中键入公司 ID。

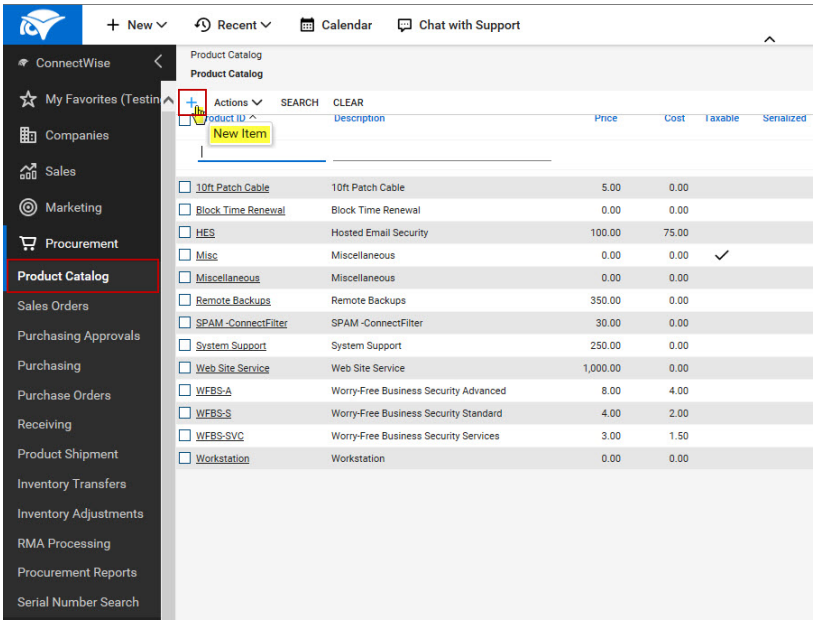
f. 从 **Type** 下拉列表中选择 **Spam Stats**。

g. 单击 **Save**。

2. 确保您已将 Hosted Email Security 产品添加到 ConnectWise Manage 控制台。

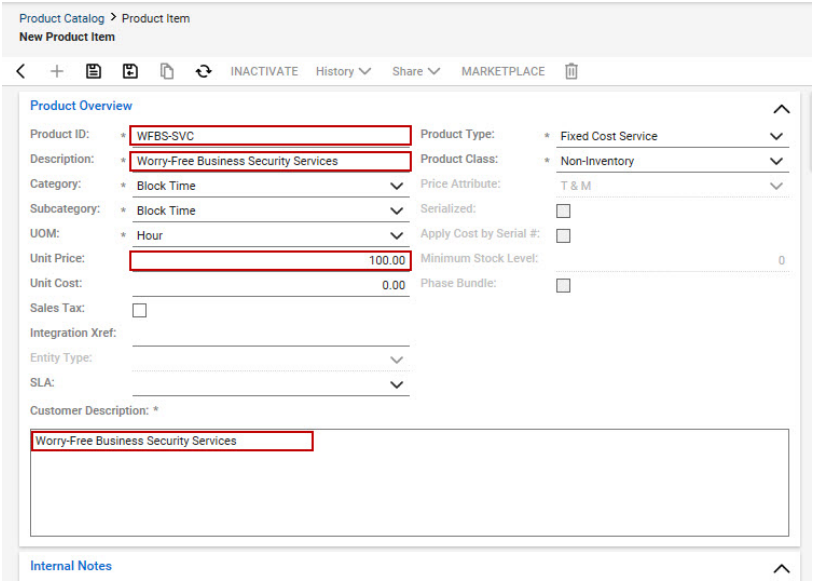
a. 在 ConnectWise Manage 控制台中，转至 **Procurement** > **Product Catalog**

此时会显示 **Product Catalog** 窗口。



b. 单击 **New Item** (➕)，以添加新产品。

此时会显示 **New Product Item** 窗口。



c. 在 **Product ID** 文本框中键入所需的趋势科技远程管理器托管产品/服务的产品 ID。

   Hosted Email Security 的 **Product ID** 为 `HES`。

d. 指定以下信息：

   - **描述**
   - **单价**
   - **客户描述**

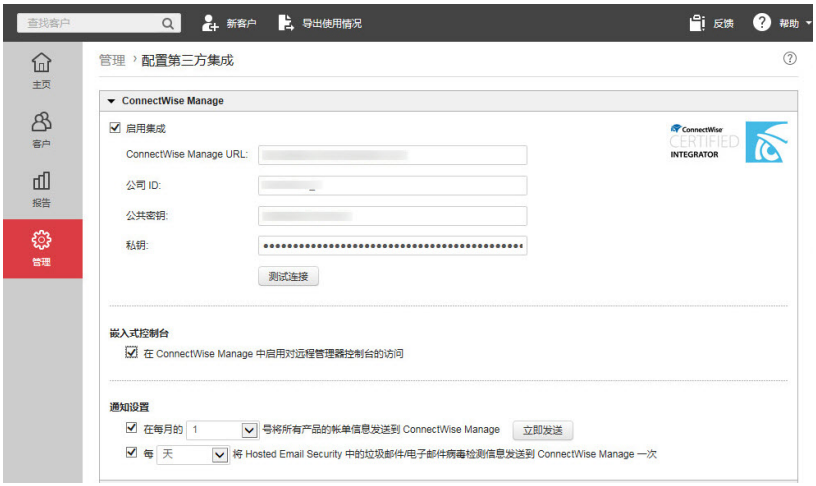
e. 单击 **Save**。

3. 在趋势科技远程管理器控制台中配置全局第三方集成设置，以向 ConnectWise Manage 客户发送 Hosted Email Security 检测信息。

a. 打开趋势科技远程管理器控制台。

b. 转至**管理** > **配置第三方集成**。

此时会显示**配置第三方集成**窗口。



c. 在**通知设置**部分中：

- 启用**每 ___ 将 Hosted Email Security 中的垃圾邮件/电子邮件病毒检测信息发送到 ConnectWise Manage 一次**，以便为 Hosted Email Security 客户执行自动安全报告。

d. 单击**保存**。

4. 在趋势科技远程管理器控制台中配置特定于客户的 ConnectWise Manage 设置，以向特定的 ConnectWise Manage 客户发送 Hosted Email Security 检测信息。

a. 打开趋势科技远程管理器控制台。

b. 要使远程管理器能够向 ConnectWise Manage 发送通知，请转至**客户** > **{公司}**。

c. 单击**通知**选项卡。

此时会显示以下窗口：

d. 在**第三方通知**部分中，选择 **ConnectWise Manage**。

e. 单击**保存**。

f. 单击 **ConnectWise Manage** 选项卡。

g. 在**通知设置**部分中：

- 选择**使用管理中的全局设置 > 配置第三方集成 > ConnectWise Manage 设置**以应用全局集成设置。
- 选择**使用自定义设置**来配置特定于客户的通知，以用于结算和执行摘要。
  - 启用**每 ___ 将 Hosted Email Security 中的垃圾邮件/电子邮件病毒检测信息发送到 ConnectWise Manage 一次**，以便为 Hosted Email Security 客户执行自动安全报告。

h. 单击**保存**。

管理客户帐单

在可以开始管理客户帐单之前，您必须先将 ConnectWise Manage 客户与趋势科技远程管理器集成。

有关更多信息，请参阅将 ConnectWise Manage 和远程管理器客户集成 第 11-2 页。

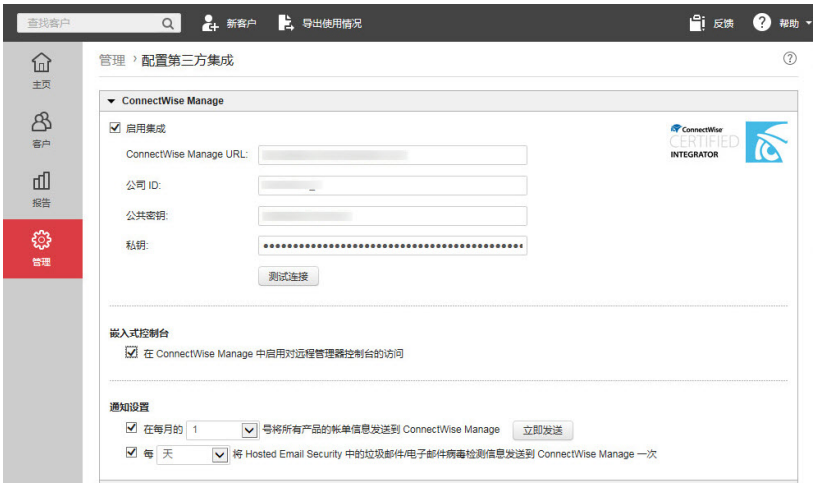
集成这两种产品和关联客户帐户之后，您可以为客户配置帐单设置。

过程

1. 在趋势科技远程管理器控制台上配置全局帐单时间表。

   a. 转至**管理** > **配置第三方集成**。

   此时会显示**配置第三方集成**窗口。



   b. 在**通知设置**部分中：

   - 启用**在每月的 __ 号将所有产品的帐单信息发送到 ConnectWise Manage**，以便为所有 ConnectWise Manage 客户自动结算所有趋势科技产品的费用。

注意

- 单击**立即发送**可将当前帐单立即发送给 ConnectWise Manage 客户。
- 如果您选择 29、30 或 31 号，而该月的结束日期早于配置的日期，则远程管理器会在该月的最后一天发送帐单信息。

c. 单击**保存**。

此时，ConnectWise Manage 就可以接收来自远程管理器的通知了。

2. 在远程管理器控制台上，为各个远程管理器客户配置协议和根据需要修改帐单时间表。

a. 要使远程管理器能够向 ConnectWise Manage 发送帐单信息，请转至**客户 > {公司}**。

b. 要集成此客户的 ConnectWise Manage 设置，请单击 **ConnectWise Manage** 选项卡。

c. 在**协议**部分中，可以向趋势科技产品分配 ConnectWise Manage 协议。

注意

通过向趋势科技产品分配协议，ConnectWise Manage 可以为趋势科技远程管理器客户提供自动结算服务。

重要信息

趋势科技远程管理器只能在 ConnectWise Manage 中显示您已在**公司** > **公司** > **{公司}** > **协议（选项卡）**上配置的协议。

如果您以前使用 “TMRM 管理解决方案”或 “Managed Service” 协议类型配置过 ConnectWise Manage，则趋势科技产品名称旁边将显示“缺省”。

有关 ConnectWise Manage 中管理解决方案帐单设置的更多信息，请参阅创建管理解决方案 第 11-18 页和创建交叉参考 第 11-22 页。

d. 单击**设置**。

此时会显示**产品协议**窗口。

e. 对于每种产品，请先选择协议类型，然后再选择协议名称。

f. 单击**确定**。

g. 选择以下两种集成设置之一：

- 选择**使用管理中的全局设置 > 配置第三方集成 > ConnectWise Manage 设置**以应用全局集成设置。
- 选择**使用自定义设置**来配置特定于客户的通知，以用于结算和执行摘要。

h. 单击**保存**。

创建管理解决方案

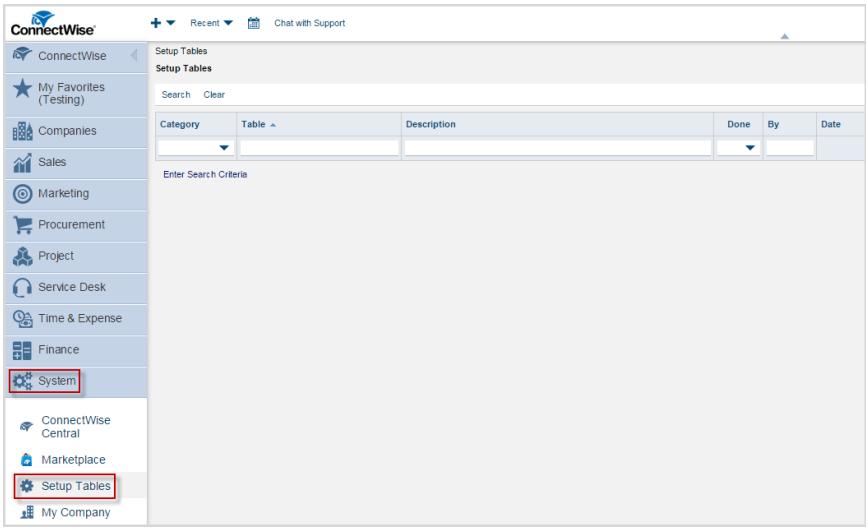
注意

此过程将显示 ConnectWise Manage 2015.1 中的窗口。根据您正在使用的 ConnectWise Manage 版本，窗口可能会有所不同。

过程

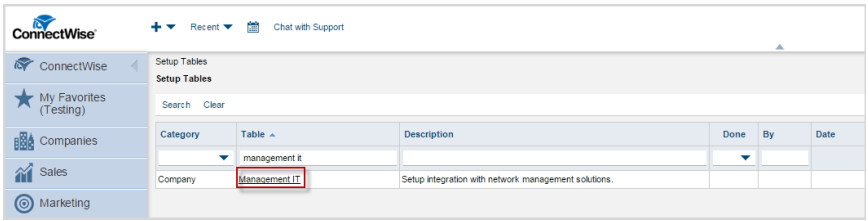
1. 在 ConnectWise Manage 控制台中，转至 **System** > **Setup Tables**。

此时，**Setup Tables** 窗口将显示出来。



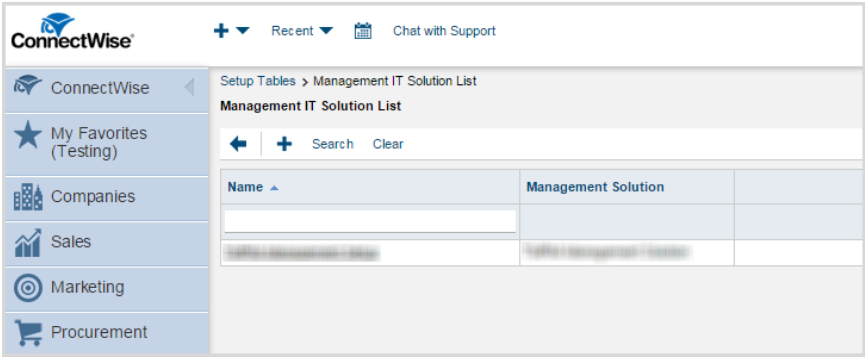
2. 在 **Table** 文本框中键入 `management it`，然后单击 **Search**。

Management IT 设置表将显示出来。



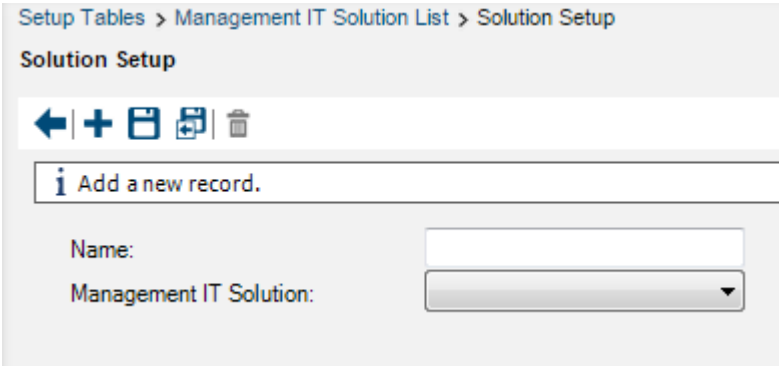
3. 单击 **Management IT** 设置表。

Management IT Solution List 将显示出来。



4. 单击 **New Item** (➕)，以创建新的管理解决方案。

   此时会显示 **Solution Setup** 窗口。



5. 指定以下信息：

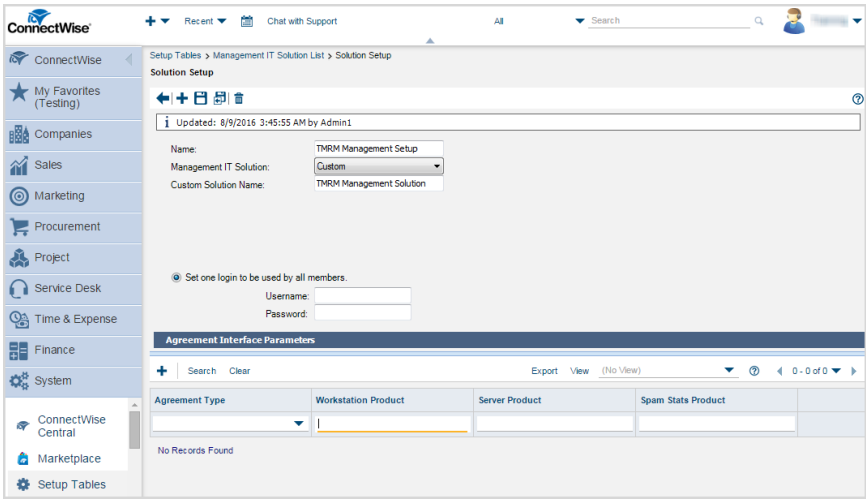
   - **Name**：键入 `TMRM Management Setup`。
   - **Management IT Solution**：选择 **Custom**。
   - **Custom Solution Name**：键入 `TMRM Management Solution`。

重要信息

趋势科技远程管理器要求指定的值与所提供的示例完全匹配。

6. 单击**保存**。

   ConnectWise Manage 将管理解决方案添加到 **Management IT Solution List**。



7. 将管理解决方案与趋势科技客户相关联。

   a. 转到 **Company** 窗口，找到趋势科技客户。

   b. 单击 **Management** 选项卡。

   c. 在 **Management Solutions** 旁，单击 **New Item** (➕)。

   d. 从 **Solution** 下拉列表中，选择 **TMRM Management Solution/TMRM Management Setup**。

   e. 指定 **Managed ID**。

   f. 单击 **Save**。

      管理解决方案现在可供使用。

8. 使用 ConnectWise 管理解决方案的客户请参阅 创建交叉参考 第 11-22 页

创建交叉参考

创建交叉参考以将远程管理器产品/服务与 ConnectWise Manage 相关联。

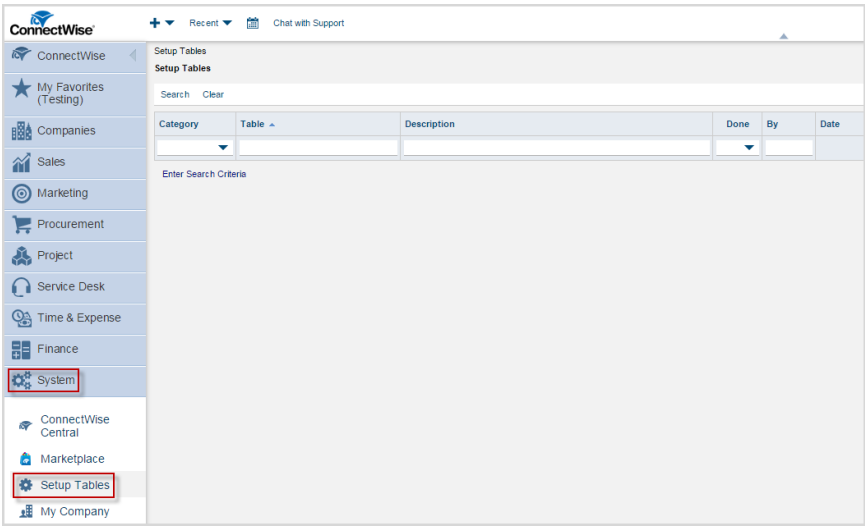
注意

此过程将显示 ConnectWise Manage 2015.1 中的窗口。根据您正在使用的 ConnectWise Manage 版本，窗口可能会有所不同。

过程

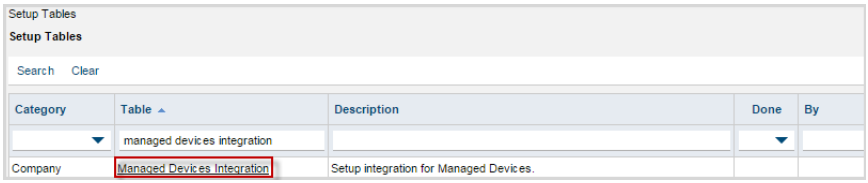
1. 在 ConnectWise Manage 控制台中，转至 **System** > **Setup Tables**。

   此时，**Setup Tables** 窗口将显示出来。



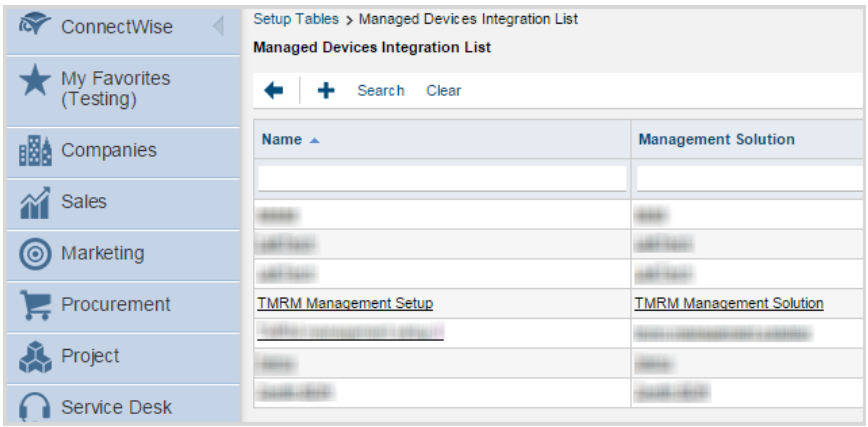
2. 在 **Table** 文本框中键入 `managed devices integration`，然后单击 **Search**。

Managed Devices Integration 设置表将显示出来。



3. 单击 **Managed Devices Integration** 设置表。

   此时会显示 **Managed Devices Integration List**。

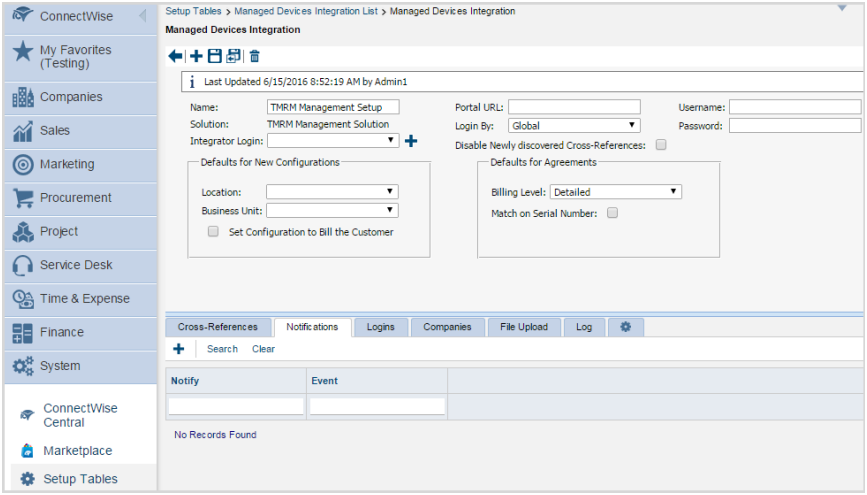


4. 单击 **Management Solution** 列中的 **TMRM Management Solution**。

注意

有关创建管理解决方案的更多信息，请参阅创建管理解决方案 第 11-18 页。

此时，**Managed Devices Integration** 窗口将显示出来。



5. 单击 **Cross-References** 选项卡。
6. 单击 **New Item** (➕)，以创建产品。
7. 为每种远程管理器托管产品/服务指定所需的设置。

产品/服务	设置
安全无忧软件-网络安全版	• **Type**：`T-WFBS-S` • **Level**：`Standard` • **Product**：`WFBS-S` • **Configuration Type**：`Spam Stats`
安全无忧软件-邮件与网络安全版	• **Type**：`T-WFBS-A` • **Level**：`Advanced` • **Product**：`WFBS-A` • **Configuration Type**：`Spam Stats`

产品/服务	设置
安全无忧软件-云端版	• **Type**：`T-WFBSS` • **Level**：`Standard` • **Product**：`WFBSS` • **Configuration Type**：`Spam Stats`
Hosted Email Security	• **Type**：`T-HES` • **Level**：`Standard` • **Product**：`HES` • **Configuration Type**：`Spam Stats`

8. 单击 **Save**。

   ConnectWise Manage 会将产品/服务添加到 **Cross-References**。

监控客户通知

在可以开始接收来自趋势科技远程管理器的客户通知之前，您必须先将 ConnectWise Manage 客户与趋势科技远程管理器集成。

有关更多信息，请参阅将 ConnectWise Manage 和远程管理器客户集成 第 11-2 页。

集成这两种产品和关联客户帐户之后，您可以进行有关开始接收客户通知的配置。

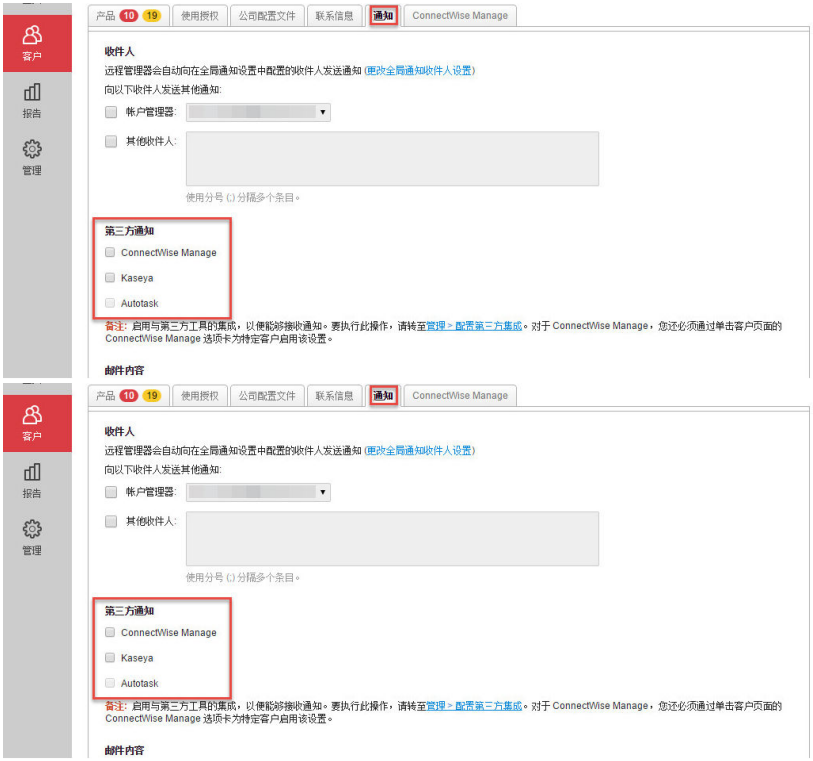
过程

1. 在趋势科技远程管理器控制台上为各个趋势科技远程管理器客户配置通知设置。

   a. 要使远程管理器能够向 ConnectWise Manage 发送通知，请转至**客户** > **{公司}**。

b. 单击**通知**选项卡。

此时会显示以下窗口：



c. 在**第三方通知**部分中，选择 **ConnectWise Manage**。

d. 选择应发送给 ConnectWise Manage 的产品通知事件。

- **使用全局通知设置**：选择此选项可使用在**管理 > 配置通知**窗口中配置的设置
- **使用自定义通知事件设置**：选择趋势科技远程管理器为该客户发送给 ConnectWise Manage 系统的通知事件

有关更多信息，请参阅：

- 使用授权通知 第 17-10 页
- 安全无忧软件-云端版通知 第 17-10 页
- Cloud App Security 通知 第 17-14 页
- Cloud Edge 通知 第 17-15 页

e. 单击**保存**。

2. 在 ConnectWise Manage 控制台上监控客户通知。

a. 在 ConnectWise Manage 控制台中，转至 **Service Desk** > **Service Board**。

重要信息

如果您正在从 ConnectWise Manage 之前的版本进行迁移，且正在使用“TMRM 事件通知”服务公告牌，则必须先为服务公告牌配置缺省服务团队，然后才能接收通知。

第 12 章

ConnectWise Automate 支持

本节介绍如何向远程管理器集成 ConnectWise Automate 以及趋势科技产品和服务受支持的事件通知。

主题包括：

集成 ConnectWise Automate™

以下主题包含有关将 ConnectWise Automate 与远程管理器相集成的信息：

安装适用于 ConnectWise Automate 的趋势科技安全无忧软件-云端版插件

借助此插件，远程管理器可与 ConnectWise Automate 同步安全无忧软件-云端版客户和检测数据。

提示

您可以从 ConnectWise Automate **解决方案中心**升级适用于 ConnectWise Automate 的趋势科技安全无忧软件-云端版插件。

重要信息

- 适用于 ConnectWise Automate 的趋势科技安全无忧软件-云端版插件不支持使用客户许可门户帐户的客户。
- 适用于 Automate 的安全无忧软件-云端版插件的某些功能需要使用安全无忧软件-云端版的最新版本。请将所有安全客户端都更新为最新版本，以确保全面支持所有新功能。

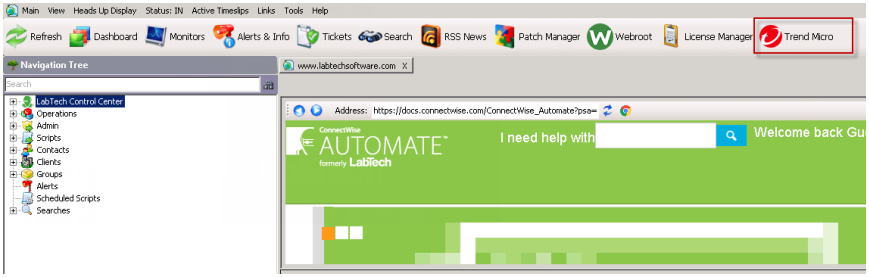
注意

此过程将显示 ConnectWise Automate 11 中的窗口。根据您正在使用的 ConnectWise Automate 版本，窗口可能会有所不同。

过程

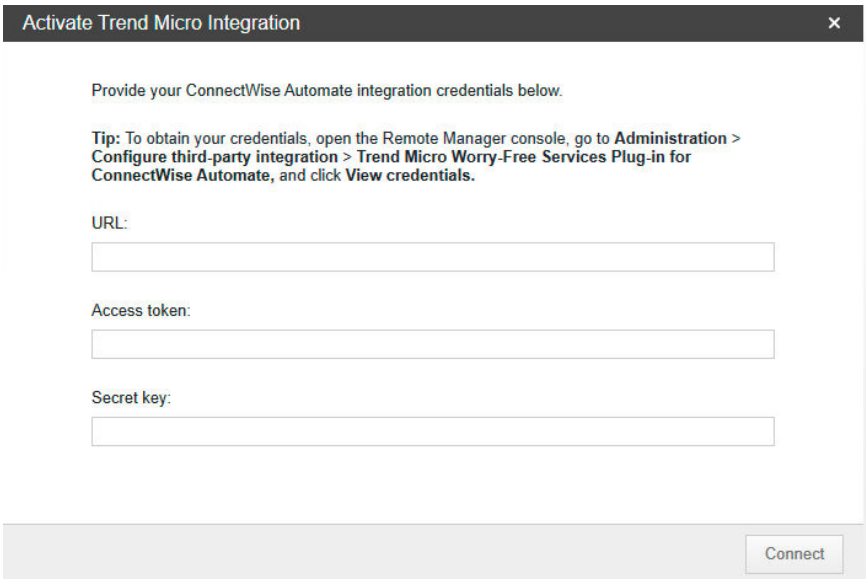
1. 从 Automate 解决方案中心安装适用于 ConnectWise Automate 的趋势科技安全无忧软件-云端版插件。
2. 返回到 Automate 控制中心窗口。

此时会看到 **Trend Micro** 图标已添加到工具栏。



3. 单击工具栏中的 **Trend Micro** 按钮。

   此时，**Activate Trend Micro Integration** 窗口将显示出来。



4. 请提供远程管理器激活凭证。

   - **URL**

- **访问令牌**
- **密钥**

提示

找到激活凭证的步骤：

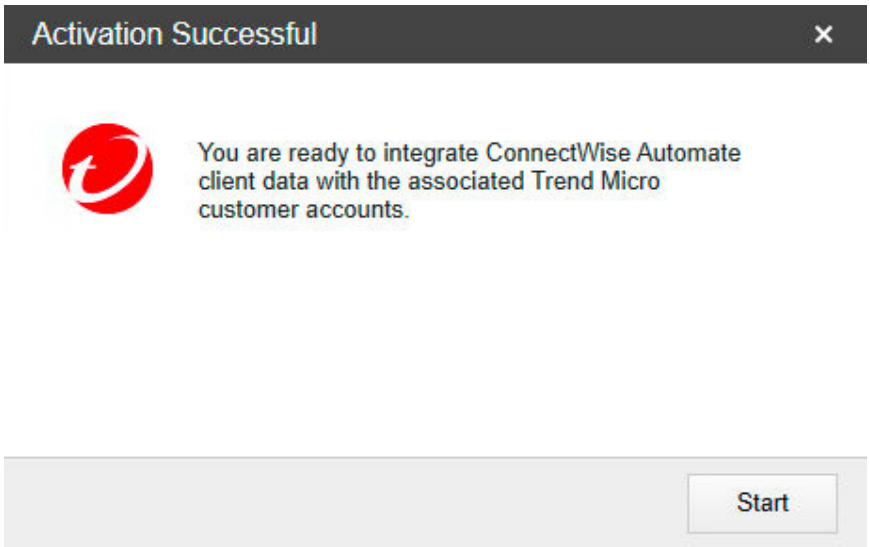
a. 打开远程管理器控制台，然后转至**管理** > **配置第三方集成** > **ConnectWise Automate**。

b. 单击 **查看凭证**。

5. 单击 **Connect**。

此时会显示 **Activation Successful** 窗口。您可以单击 **Start**，开始集成 ConnectWise Automate 客户数据与趋势科技帐户。

有关详情，请参阅导入 ConnectWise Automate 客户 第 12-8 页。



注意

如要在以后某个时间集成帐户，请单击工具栏中的 **Trend Micro** 按钮，然后转至 **Non-Trend Micro Customers**。

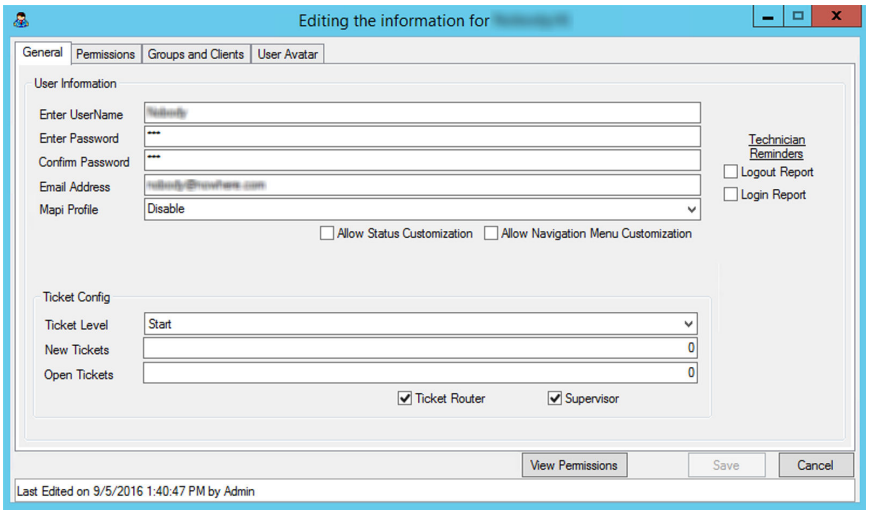
在 ConnectWise Automate 中分配趋势科技用户权限

安装好适用于 Automate 的趋势科技安全无忧软件-云端版插件后，您必须为 ConnectWise Automate 用户分配权限，之后这些用户才能访问所有插件功能。

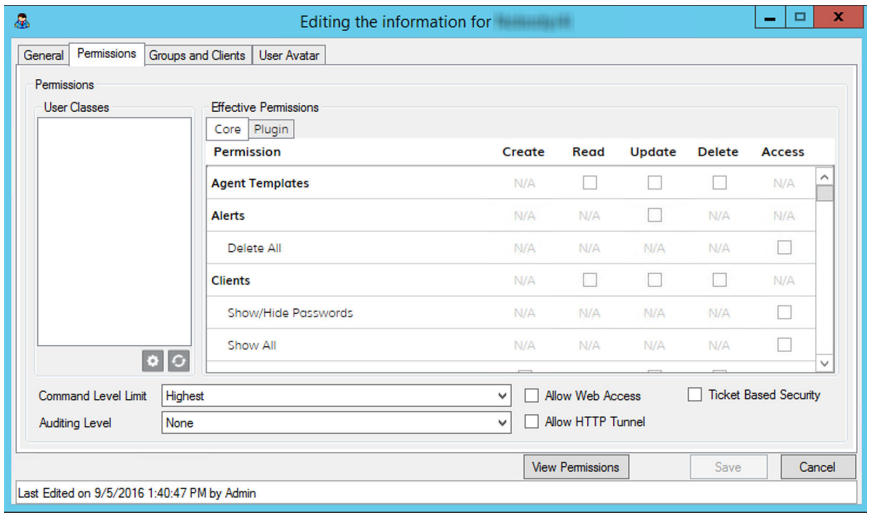
过程

1. 在 Automate 控制中心导航树中，转至 **Admin** > **Users**，然后双击您要为其分配权限的用户。

   此时，**Editing the information for {user}** 窗口将显示出来。

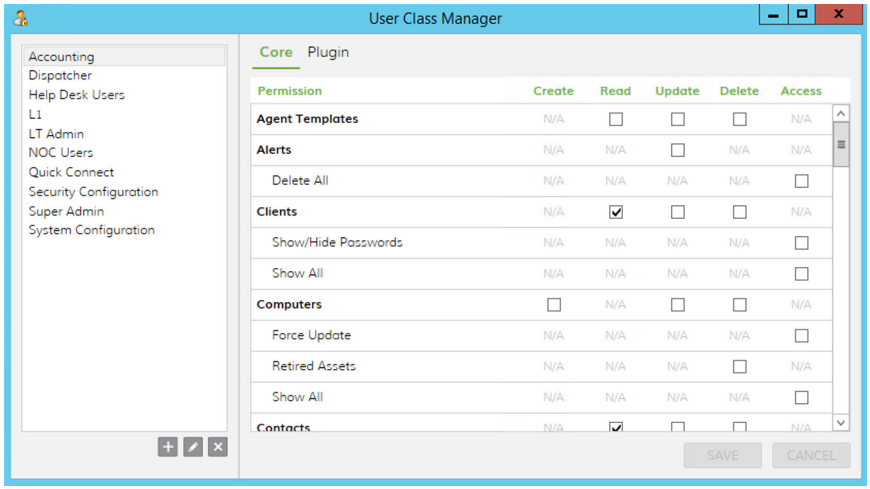


2. 单击 **Permissions** 选项卡。



3. 单击 **User Classes** 文本框下面的 **Open User Class Manager** ( ) 图标。

此时，**User Class Manager** 窗口将显示出来。



4. 选中以下复选框，以分配相应的权限。

权限	类型
Clients	读取
Contacts	读取
Database	访问
Scripts	读取

5. 单击 **SAVE**。
6. 单击 **Plugin** 选项卡。
7. 选中 **Trend Micro Worry-Free Services Plug-in for ConnectWise Automate** 旁边的 **Access** 复选框。
8. 单击**保存**。

   此时，ConnectWise Automate 用户就可以访问适用于 ConnectWise Automate 的趋势科技安全无忧软件-云端版插件功能了。

在 ConnectWise Automate 中管理趋势科技客户

激活适用于 Automate 的趋势科技安全无忧软件-云端版插件后，您便可以开始直接从 ConnectWise Automate 控制台关联 ConnectWise Automate 客户与趋势科技帐户以及管理客户关联。

- 导入 ConnectWise Automate 客户：将当前的 ConnectWise Automate 客户与预先存在的或新的趋势科技帐户相关联

  有关更多信息，请参阅导入 ConnectWise Automate 客户 第 12-8 页。

- 客户摘要窗口：显示关联的趋势科技客户以及未与趋势科技帐户关联的 ConnectWise Automate 客户

有关更多信息，请参阅客户摘要 第 12-13 页。

导入 ConnectWise Automate 客户

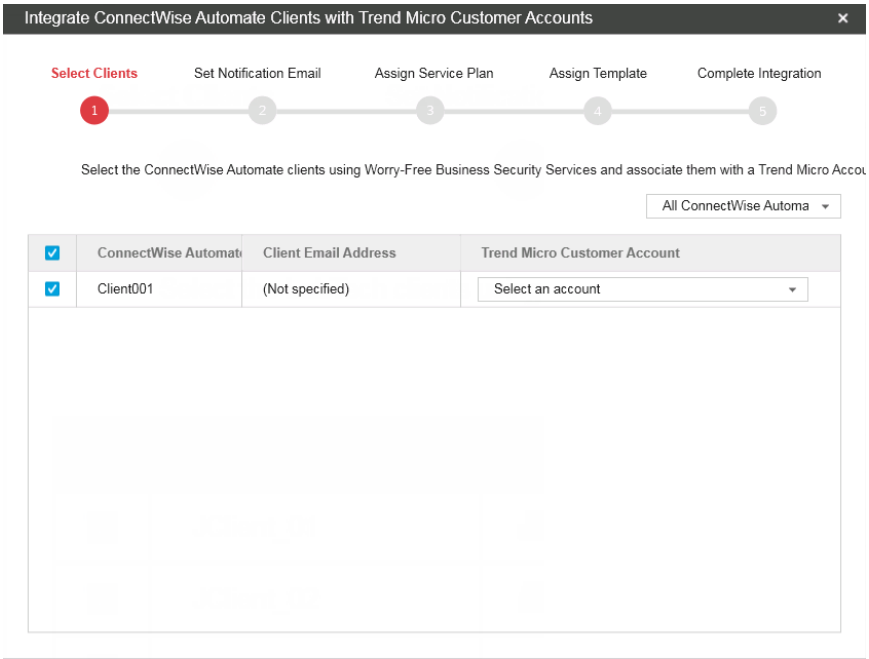
过程

1. 转至 **Integrate Automate Clients with Trend Micro Accounts** 窗口。
   - 通过 Automate 控制中心执行以下操作：
     a. 单击工具栏中的 **Trend Micro** 按钮，然后转至 **Non-Trend Micro Customers**。
     b. 选中您要导入的 ConnectWise Automate 客户旁边的复选框。
     c. 单击 **Import to Trend Micro**。
   - 在首次激活 ConnectWise Automate 插件后，从 **Activation Successful** 窗口中单击 **Start**。

重要信息

您必须在随即显示的 **Integrate Automate Clients with Trend Micro Accounts: Select Clients** 窗口中选中要与趋势科技帐户集成的 ConnectWise Automate 客户旁边的复选框。

此时会显示 **Integrate Automate Clients with Trend Micro Accounts: Select Clients** 窗口。



2. 在“Trend Micro Customer Account”下拉列表中：

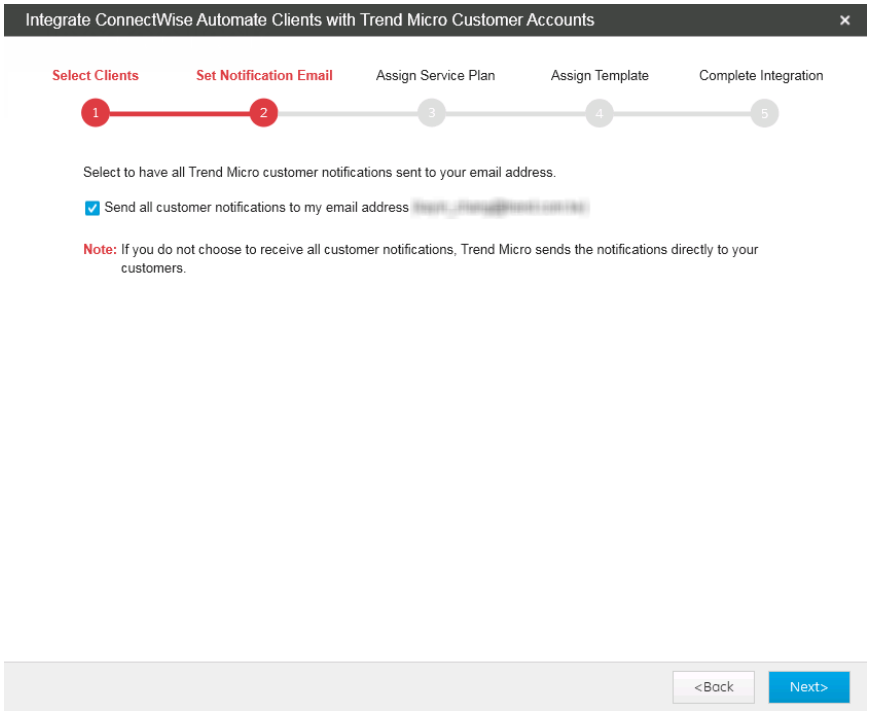
   - 列表中将显示与远程管理器客户帐户匹配的所有 ConnectWise Automate 客户。如果匹配记录不正确，请选择其他公司帐户，或创建新的趋势科技帐户。
   - 选择 **+ Create a new Trend Micro Account** 以在远程管理器中自动注册新的客户帐户，注册时将 ConnectWise Automate 客户名称用作公司名称。
   - 从尚未分配给其他帐户的现有远程管理器客户中选择。

注意

如果您已分配所有客户，则列表中将不显示任何客户信息。

3. 单击 **Next>**。

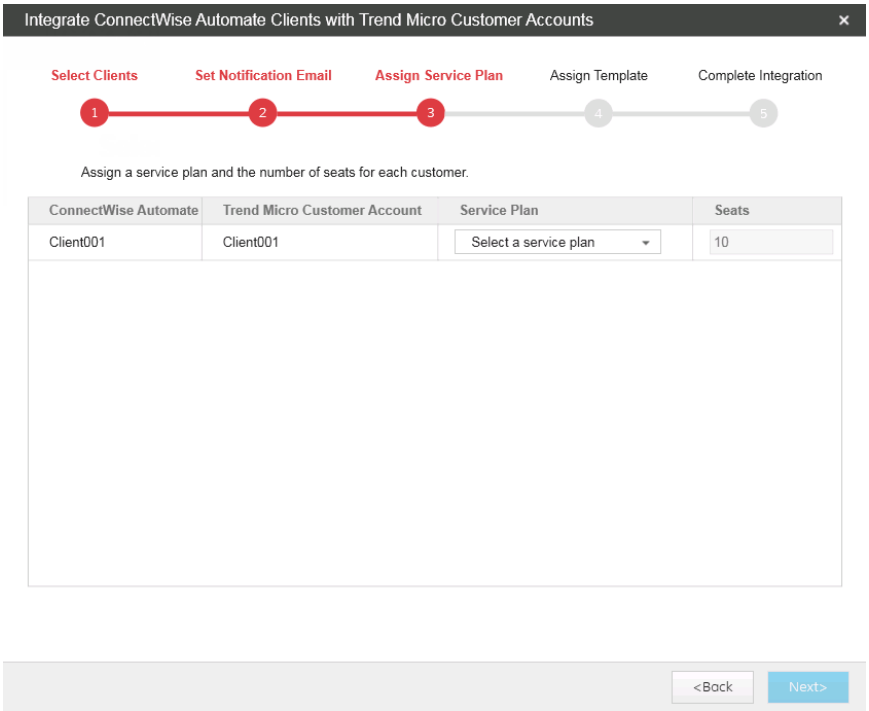
   此时，**Set Notification Email** 窗口将显示出来。



4. 如果您希望系统将有关选定客户环境的所有电子邮件通知发送到您注册的电子邮件地址中，请选择 **Send all customer notifications to my email address**。

5. 单击**下一步>**。

此时会显示 **Assign Service Plan** 窗口。



6. 如果您为任何 ConnectWise Automate 客户选择了 **+ Create a new Trend Micro Account**，请为每位客户指定以下内容：

   a. **服务计划**

   b. **Seats：**缺省情况下，远程管理器提供的座席数比客户已在 ConnectWise Automate 中注册的终端数多 20%（每位客户最少有 10 个座席）。

注意

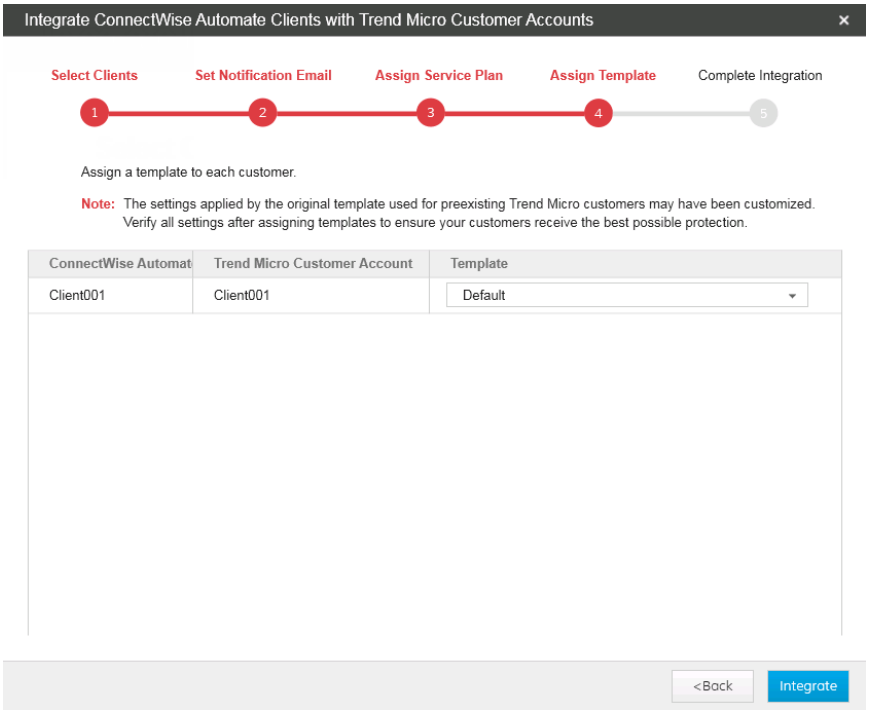
您无法修改预先存在的用户的设置。

7. 单击**下一步 >** 将选定客户添加到列表中。

重要信息

您必须为选定数量的 ConnectWise Automate 客户提供充分的 Licensing Management Platform 使用授权。如果您未提供充分的使用授权，则该插件只能导入列表中使用授权可用的前几位客户。

此时会显示**分配模板**窗口。



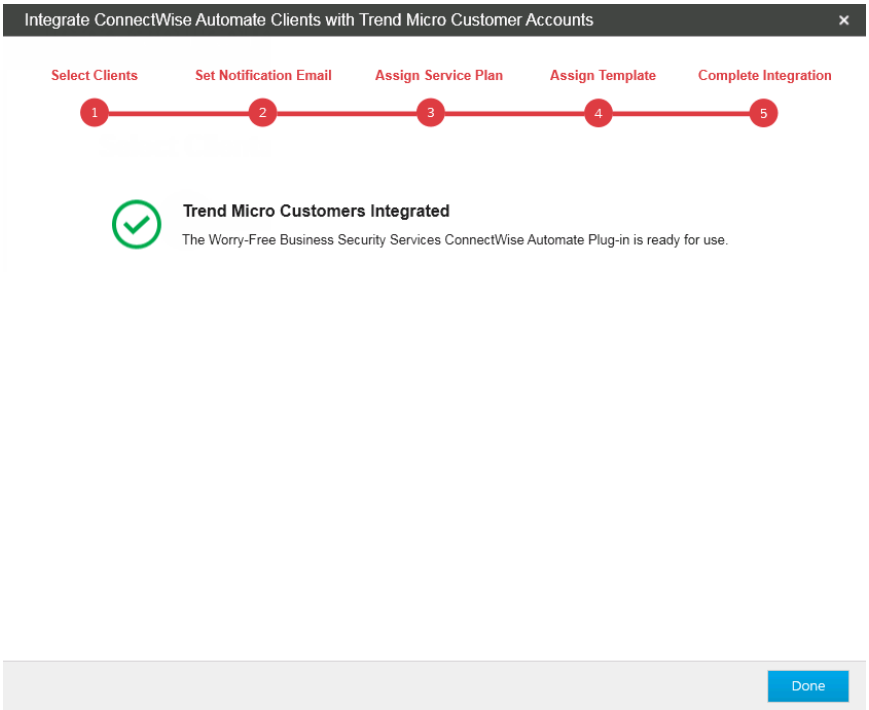
8. 在“Template”下拉列表中，向每个客户分配模板。

重要信息

用于预先存在的趋势科技客户的原始模板所应用的设置可能已被定制。请在分配模板后验证所有设置，以确保客户获得最好的保护。

9. 单击 **Integrate**。

   此时会显示 **Complete Integration** 窗口。



10. 单击 **Done** 以退出设置向导。

客户摘要

单击工具栏中的 **Trend Micro** 按钮或单击客户树中的 **Trend Micro Customers** 节点后，**Trend Micro Customers** 窗口会显示出来。您可以在此窗口中查看所有与趋势科技帐户关联的 ConnectWise Automate 客户，以及取消先前配置的 ConnectWise Automate 客户与趋势科技帐户的关联。

下表列出了 **Trend Micro Customers** 窗口的主要部分。

部分	描述
客户概要	提供通过 ConnectWise Automate 管理的所有趋势科技帐户的概览 • **Clients**：单击计数可在 **Clients** 选项卡上的表中查看所有趋势科技帐户 • **Action required**：单击计数可在 **Clients** 选项卡上的表中查看所有需要引起注意的趋势科技帐户 • **Managed machines**：显示已安装安全无忧软件-云端版安全客户端的计算机总数 • **Unmanaged machines**：显示与未安装安全客户端的趋势科技帐户相关联的计算机总数

部分	描述
客户端选项卡	显示一个表，该表概述 ConnectWise Automate 客户的趋势科技帐户信息和客户是否需要立即关注 • **Automate Client**：单击客户名称可打开该客户的安全无忧软件-云端版控制台 • **Action Required**：单击突出显示的红色单元格可在 **Statistics** 选项卡上显示 **Action Required Events** 小组件 • **Disconnect Client from Trend Micro Account**：如果某个 ConnectWise Automate 客户不再是趋势科技客户，请在表中选中该 ConnectWise Automate 客户名称旁边的复选框，然后单击 **Disconnect Client from Trend Micro Account** 以从列表中删除该客户。 **注意** 取消 ConnectWise Automate 客户与趋势科技帐户的关联并不会从客户的托管终端上卸载安全客户端。 • **Automatic Deployment**：启用此功能可将安全客户端自动部署到已分配给 ConnectWise Automate 客户的无防护终端（每小时部署一次） **重要信息** 确保 ConnectWise Automate 客户有足够多的可用使用授权，然后再启用自动部署。如果没有可用的使用授权，趋势科技安全无忧软件-云端版插件仍会部署安全客户端，但是，无使用授权的安全客户端无法向安全无忧软件-云端版控制台汇报，并且仍然留在非托管终端列表中。
统计信息选项卡	显示的控制台带有小组件，用于提供使用 ConnectWise Automate 管理的所有趋势科技帐户的概览 可用的小组件： • 需要采取处理措施的事件小组件 第 12-21 页 • 威胁管理小组件 第 12-22 页

在 ConnectWise Automate 中管理安全无忧软件客户端

适用于 ConnectWise Automate 的趋势科技安全无忧软件-云端版插件可以通过 ConnectWise Automate 控制台提供对安全客户端的有限控制。

从 ConnectWise Automate 控制台中，您可以执行以下安全无忧软件客户端任务：

- 管理趋势科技 ConnectWise Automate 客户 第 12-16 页
- 在 ConnectWise Automate 中使用趋势科技脚本 第 12-19 页

管理趋势科技 ConnectWise Automate 客户

客户信息窗口提供了基本的 ConnectWise Automate 客户摘要信息，包括主要客户联系人、电子邮件地址和安全无忧软件-云端版的当前使用授权状态。

重要信息

适用于 Automate 的安全无忧软件-云端版插件的某些功能需要使用安全无忧软件-云端版的最新版本。请将所有安全客户端都更新为最新版本，以确保全面支持所有新功能。

使用 **Endpoints** 和 **Unmanaged Endpoints** 选项卡中的信息，向安全无忧软件-云端版安全客户端发送命令，或将客户端部署到终端。

注意

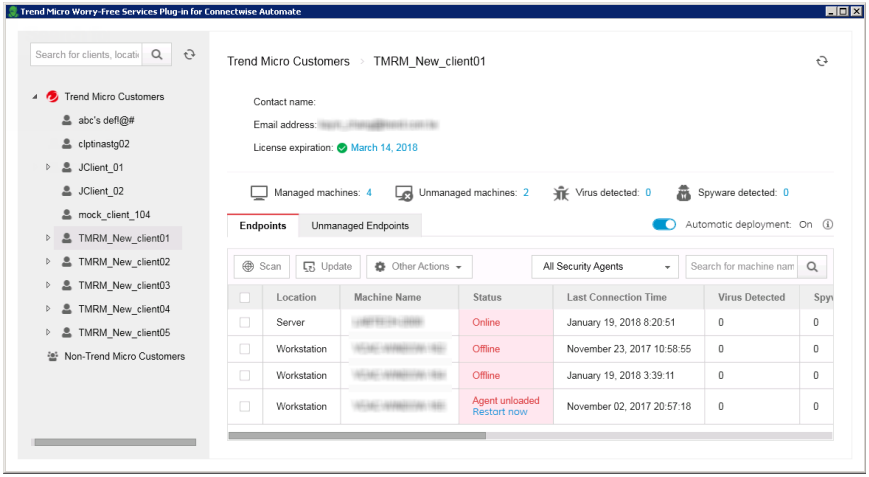
- 您可以选择在客户树的 **Trend Micro Customers** 节点下查看任意级别的客户/终端的具体信息。
- 常见的安全无忧软件-云端版客户端命令也可以使用 ConnectWise Automate 脚本来运行。

  有关更多信息，请参阅 在 ConnectWise Automate 中使用趋势科技脚本 第 12-19 页

过程

1. 打开 Automate 控制中心，转至 **Trend Micro** > **Trend Micro Customers**，然后在导航树中选择一个客户。

   显示窗口中的标题取决于客户树中所选客户信息的级别。以下图片显示的是 **Trend Micro Customers** > **{Client}** 窗口。



2. 单击使用授权过期日期，查看远程管理器提供的安全无忧软件-云端版可用使用授权的详细信息。

3. 通过单击以下任意计数查看具体终端：

   - **Managed machines**：在 **Endpoints** 选项卡中显示已安装安全无忧软件-云端版安全客户端的计算机列表
   - **Unmanaged machines**：在 **Unmanaged Endpoints** 选项卡中显示未安装安全无忧软件-云端版安全客户端的计算机列表
   - **Viruses detected**：在 **Endpoints** 选项卡中显示已进行病毒检测的安全无忧软件-云端版安全客户端列表
   - **Spyware detected**：在 **Endpoints** 选项卡中显示已进行间谍软件检测的安全无忧软件-云端版安全客户端列表

提示

对于在 **Endpoints** 选项卡中显示大量安全无忧软件-云端版安全客户端的客户，您可以使用终端表格上方的下拉控件中的状态信息进一步过滤结果。

4. 启用 **Automatic Deployment**，以便将安全客户端自动部署到已分配给 ConnectWise Automate 客户的无防护终端（每小时部署一次）。

重要信息

确保 ConnectWise Automate 客户有足够多的可用使用授权，然后再启用自动部署。如果没有可用的使用授权，趋势科技安全无忧软件-云端版插件仍会部署安全客户端，但是，无使用授权的安全客户端无法向安全无忧软件-云端版控制台汇报，并且仍然留在非托管终端列表中。

5. 在 **Endpoints** 选项卡中，选中您要管理的终端对应的复选框，然后单击列表上方的按钮发送必要的命令。

   - **Scan**：触发选定终端上的安全客户端，以在下一次服务器同步期间执行手动扫描
   - **Update**：触发安全客户端以在下一次服务器同步期间检查是否有组件更新
   - **Other Actions**：显示以下命令：
     - **Unload Agent**：在下次服务器同步期间，在指定的一段时间内从选定的终端上传安全客户端
     - **Remove Agent**：在下一次服务器同步期间从选定终端上卸载安全客户端

       警告!

       删除安全客户端可能会导致终端易受安全威胁攻击。

注意

您必须确认您要向选定安全客户端发送命令。

远程管理器下次与安全无忧软件-云端版同步时，终端会收到命令。缺省同步时间为 5 分钟。

6. 在 **Unmanaged Endpoints** 选项卡上：

   - 选择您想要将其另存为 CSV 格式的列表的非托管终端，然后单击 **Export**。
   - 选择您要在其上安装安全客户端的非托管终端，然后单击 **Deploy Agent**。

注意

您必须确认您要向选定终端发送命令。

远程管理器下次与安全无忧软件-云端版同步时，终端会收到命令。缺省同步时间为 5 分钟。

在 ConnectWise Automate 中使用趋势科技脚本

安全无忧软件-云端版 ConnectWise Automate 插件提供了以下脚本，用户可通过 **Scripts** > **Anti-Virus** > **Trend Micro** 右键单击菜单访问这些脚本。

重要信息

您必须先分配特定的 ConnectWise Automate **User Classes** 权限来访问每个脚本，然后系统才会显示右键单击脚本项。

您只能访问与趋势科技帐户关联的 ConnectWise Automate 客户的右键单击“Scripts”菜单。要将 ConnectWise Automate 客户与趋势科技帐户相关联，请参阅导入 ConnectWise Automate 客户 第 12-8 页

- **Deploy Security Agent**：将安全客户端部署到选定的终端
- **Remove Security Agent**：从选定的终端上卸载安全客户端

警告!

删除安全客户端可能会导致终端易受安全威胁攻击。

- **Restart Security Agent**：在选定的终端上重新启动安全客户端

- **Scan Now**：触发选定终端上的安全客户端以执行手动扫描
- **Unload Security Agent**：从选定的终端卸载安全客户端
- **Update Now**：触发安全客户端，以检查是否有组件更新

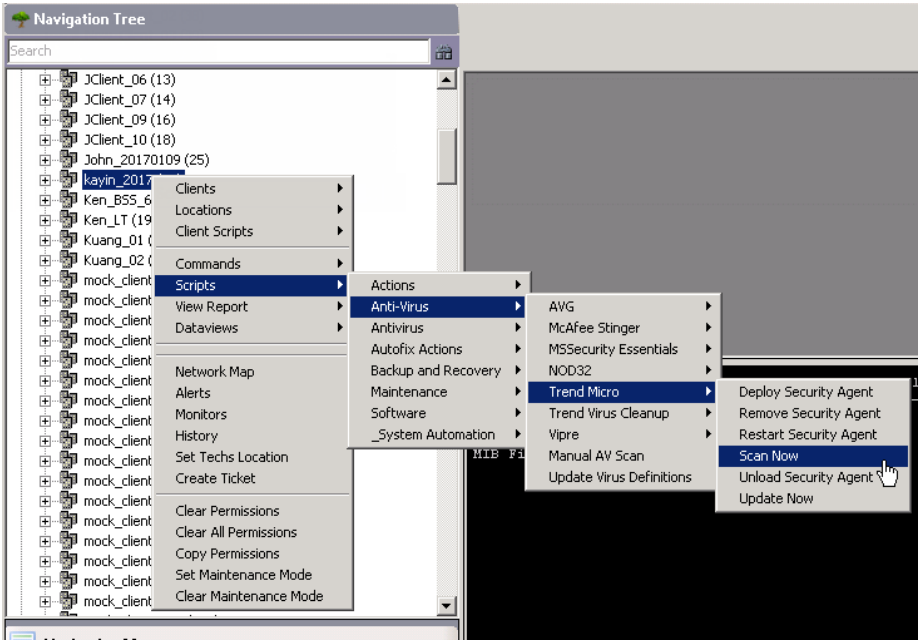


图 12-1. 趋势科技 ConnectWise Automate 的“Scripts”菜单

注意

- 远程管理器下次与安全无忧软件-云端版同步时，终端会收到命令。缺省同步时间为 5 分钟。
- 命令只能在有效的终端上运行。例如，如果选定的终端未安装安全客户端，则无法执行 **Scan Now** 功能。

监控安全无忧软件-云端版客户端

Statistics 提供了一种简单的方式来查看所有需要采取进一步处理措施，或已通过**需要采取处理措施的事件**和**威胁管理**小组件检测到安全事件的趋势科技客户。

需要采取处理措施的事件小组件

需要采取处理措施的事件小组件列出了其终端需要受到注意的客户。

事件	描述
处理措施不成功	单击**出现次数**，转至安全无忧软件-云端版控制台，然后查看客户终端上不成功的扫描结果。
实时扫描已禁用	单击**设备**，转至安全无忧软件-云端版控制台，然后查看已禁用实时扫描的终端。
需要重新启动	单击**出现次数**，转至安全无忧软件-云端版控制台，然后查看需要重新启动方能完成清除间谍软件/灰色软件操作的终端。
需要更新	单击**设备**，转至安全无忧软件-云端版控制台，然后查看需要更新的终端。

单击 **ConnectWise Automate 客户**名称可在远程管理器控制台上查看信息。

威胁管理小组件

查看拥有不同类型的安全检测的客户数量。单击链接可在远程管理器控制台上查看详细信息。

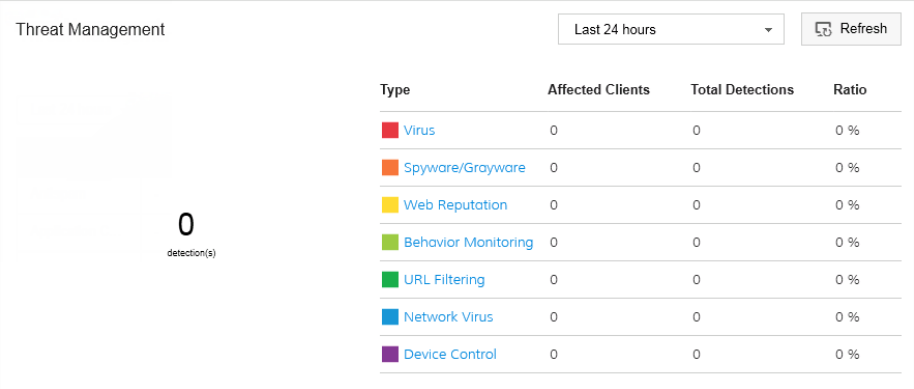


图 12-2. 威胁管理小组件

安全无忧软件-云端版票证

下表概述安全无忧软件-云端版插件生成的 ConnectWise Automate 票证。

命令类型	票证主题	可能的原因
Scan	[Action Required] Unsuccessful scan command - <machine_name> of <client_name> - Worry-Free Business Security Services	• 选定的终端未安装安全客户端 • 在选定终端上安装的安全客户端已损坏 • 选定的终端处于脱机状态或者未加载安全客户端 • 安全客户端正在进行更新 • 发生内部错误

命令类型	票证主题	可能的原因
Update Agent	[Action Required] Unsuccessful update command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 选定的终端未安装安全客户端 • 在选定终端上安装的安全客户端已损坏 • 选定的终端处于脱机状态或者未加载安全客户端 • 安全客户端正在进行扫描 • 发生内部错误
Deploy Agent	[Action Required] Unsuccessful deployment command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 服务器未完成安全客户端安装软件包的生成 • 下载安全客户端安装软件包时出错 • 选定的终端上正在安装或已安装安全客户端
	[Action Required] Exceeded seat allocation for <machine_name> of <client_name> - Worry-Free Business Security Services	• 安全客户端已部署，但因客户的剩余使用授权不足而仍然处于非托管状态

第 13 章

Kaseya 支持

本节介绍如何向远程管理器集成 Kaseya 以及趋势科技产品和服务受支持的事件通知。

主题包括：

集成 Kaseya™

以下主题包含有关将 Kaseya 与远程管理器相集成的信息：

在远程管理器中配置 Kaseya 通知设置

过程

1. 转至**管理** > **配置第三方集成**。

   此时会显示**配置第三方集成**窗口。

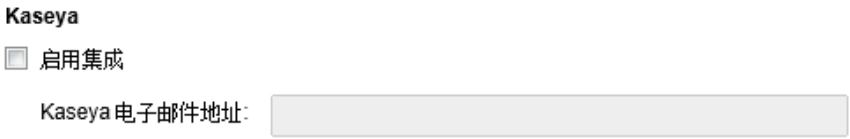


图 13-1. Kaseya 部分

2. 在 **Kaseya** 部分中，选择**启用集成**。
3. 键入 **Kaseya 电子邮件地址**。
4. 单击**保存**。

   此时会显示**成功**通知。
5. 转至**客户** > **{公司}** > **通知**。

此时会显示以下窗口：

6. 如果您想接收通知电子邮件，请选择**帐户管理器**作为收件人。
7. 在**其他收件人**文本框中，键入需要接收通知电子邮件的任何其他收件人的电子邮件地址。
8. 从“第三方通知”列表中选择 **Kaseya**。
9. 选择应发送给 Kaseya 的产品通知事件。
   - **使用全局通知设置**：选择此选项可使用在**管理 > 配置通知**窗口中配置的设置
   - **使用自定义通知事件设置**：选择趋势科技远程管理器为该客户发送给 Kaseya 系统的通知事件

   有关更多信息，请参阅：
   - 使用授权通知 第 17-10 页
   - 安全无忧软件-云端版通知 第 17-10 页
   - Cloud App Security 通知 第 17-14 页
   - Cloud Edge 通知 第 17-15 页
10. 单击**保存**。

11. 针对每个客户重复执行步骤 6 到 10。

在 Kaseya 中配置通知设置

过程

1. 在 Kaseya 中，向出票系统中添加以下文本框，以显示趋势科技远程管理器通知。

   - 安全无忧软件

文本框名称	目的
TM_CreateTime	事件生成时间
TM_ProductName	产品名称
TM_AgentGUID	远程管理器客户端 GUID
TM_CustomerName	客户/公司名称
TM_EventName	事件名称
TM_ServerName	安全无忧软件服务器名称
TM_MASClientName（可选）	Exchange 服务器名称（仅影响 Exchange Server 关闭事件）

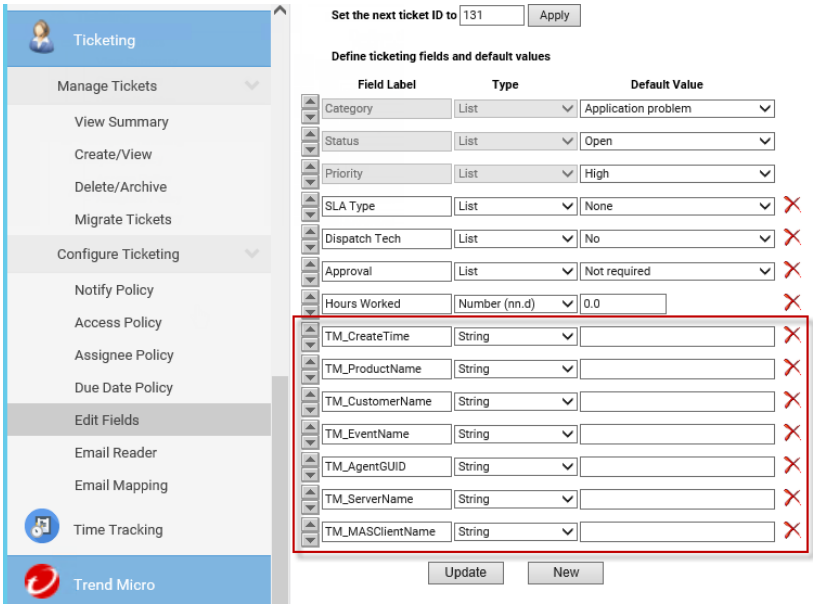


图 13-2. Kaseya 出票文本框

- 安全无忧软件-云端版

文本框名称	目的
TM_CreateTime	事件生成时间
TM_ProductName	产品名称
TM_CustomerName	客户/公司名称
TM_EventName	事件名称

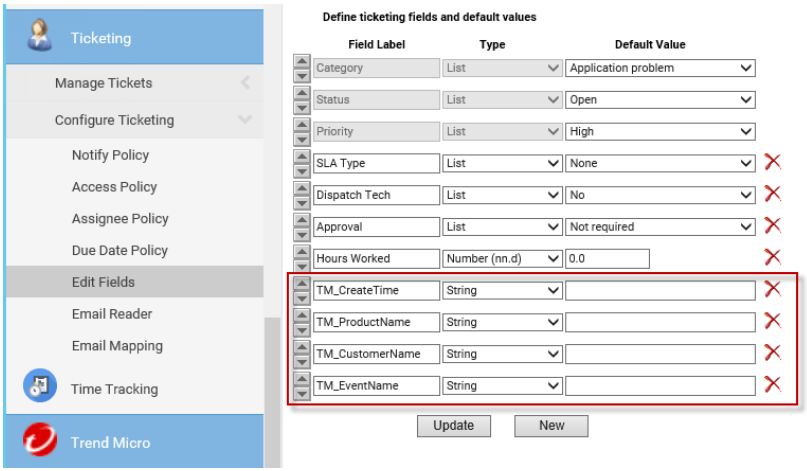


图 13-3. Kaseya 出票文本框

2. 确保电子邮件设置是正确的，如下面的窗口所示：

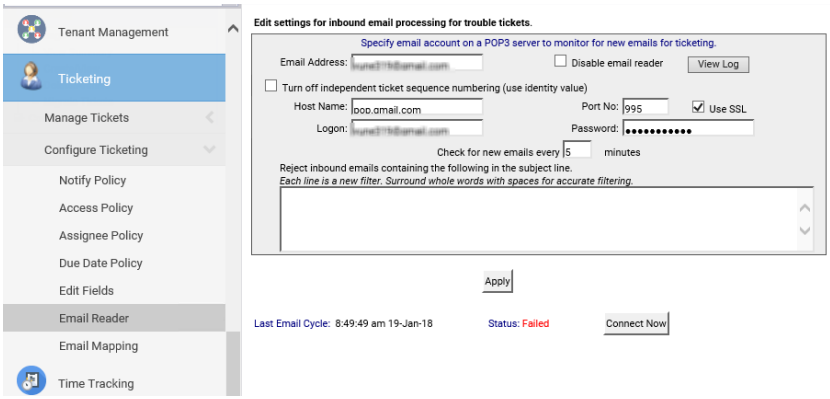


图 13-4. Kaseya 电子邮件设置

当触发某个事件后，Kaseya 会收到票证：

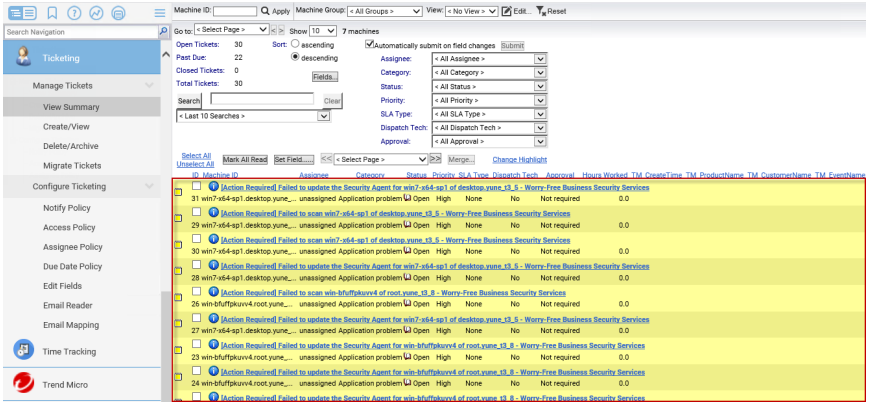


图 13-5. Kaseya 事件票证

为 Kaseya 安装趋势科技安全无忧软件插件

借助此插件，远程管理器可与 Kaseya 同步安全无忧软件-云端版客户和检测数据。

注意

适用于 Kaseya 的趋势科技安全无忧软件-云端版插件不支持使用客户许可门户帐户的客户。

过程

1. 打开远程管理器控制台，然后转至**管理** > **配置第三方集成**。

   此时会显示**配置第三方集成**窗口。

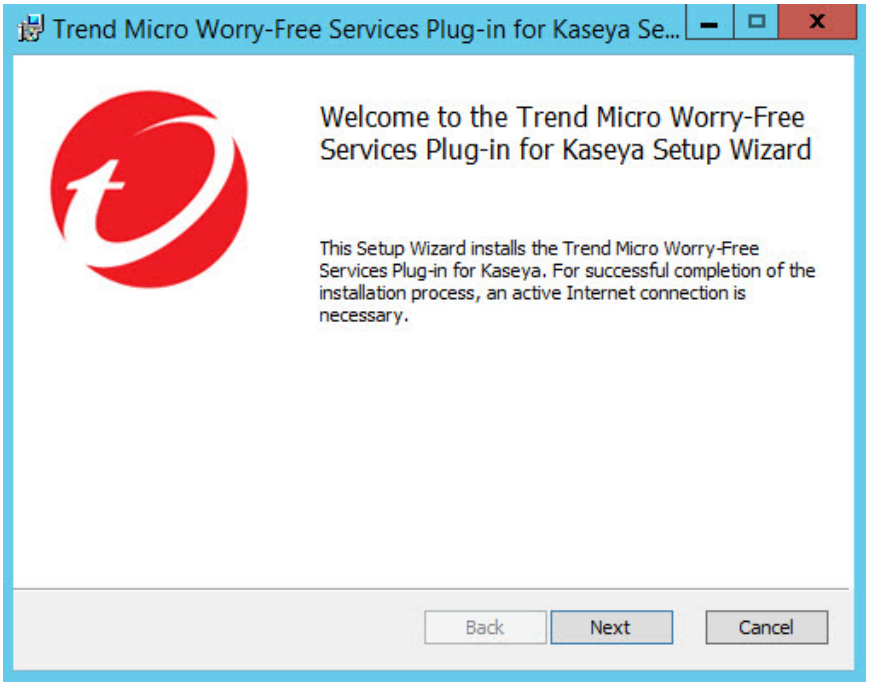
2. 转至 **Kaseya** 部分。

3. 在**适用于 Kaseya 的安全无忧软件-云端版插件**下，单击**下载**以保存此插件。

4. 将文件保存在 Kaseya VSA 服务器上。

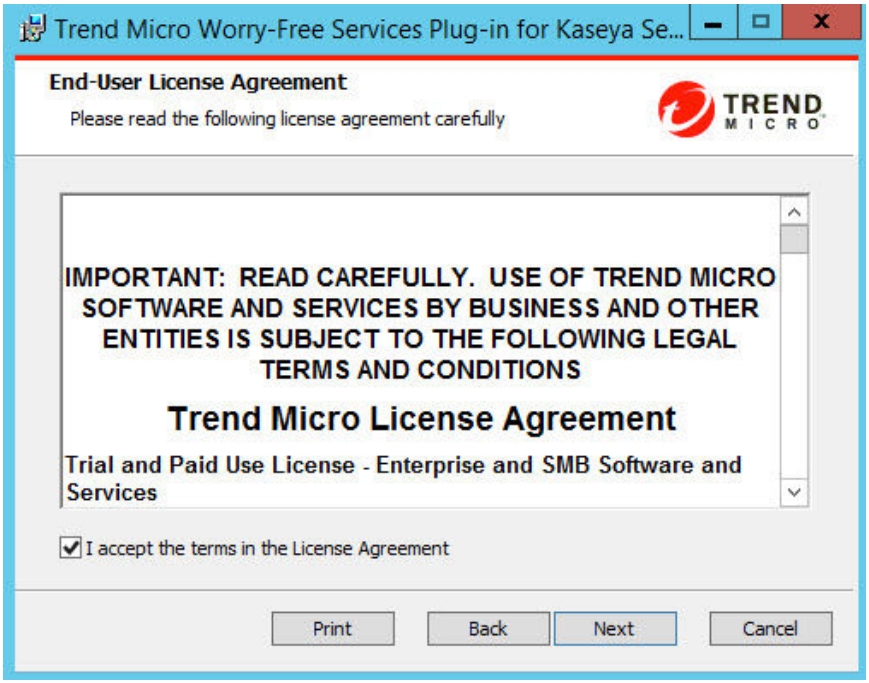
5. 执行 `TrendMicroWorryFreeServicesPluginForKaseya_X.X.X.msi` 文件。

   此时会显示欢迎窗口。



6. 单击 **Next**。

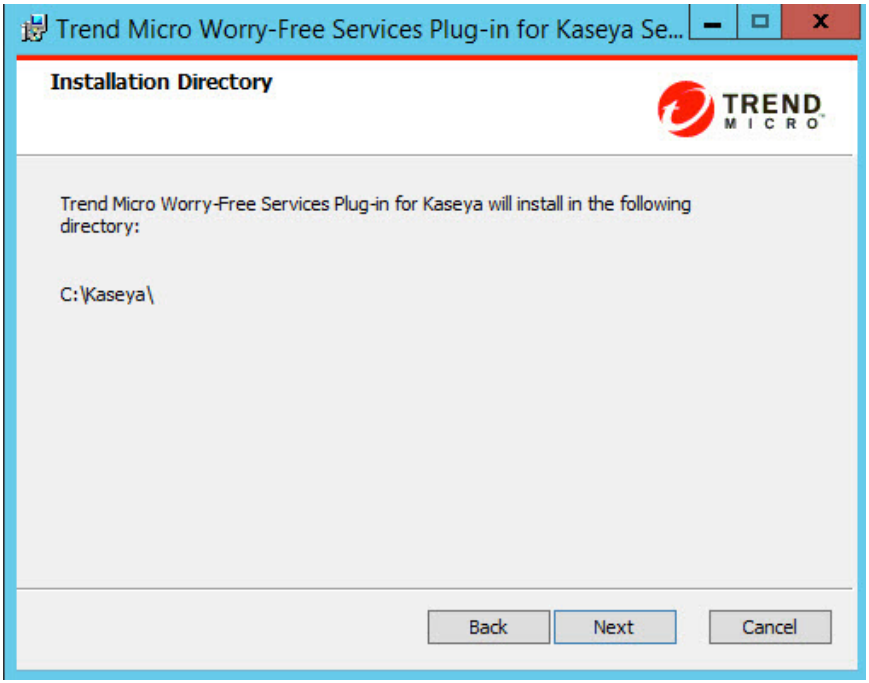
此时会显示 **End-User License Agreement** 窗口。



7. 如果您同意“许可协议”中的条款，请选中 **I accept the terms in the License Agreement** 复选框。

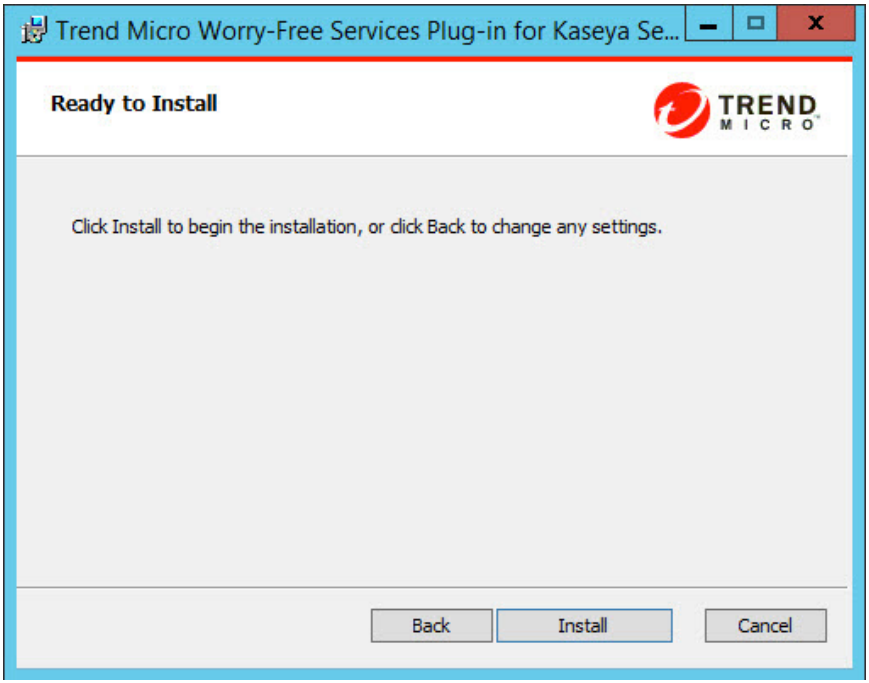
8. 单击 **Next**。

此时会显示 **Installation Directory** 窗口。



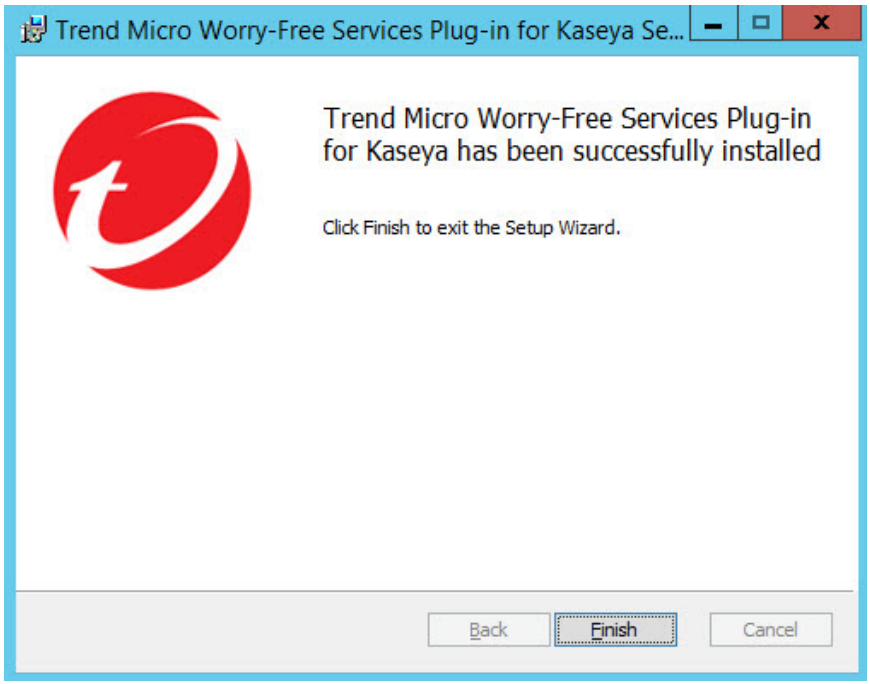
9. 确认 Kaseya 安装文件夹，然后单击 **Next**。

此时会显示 **Ready to Install** 窗口。



10. 单击 **Install**。

安装完成后，会显示 **Trend Micro Worry-Free Services Plug-in for Kaseya has been successfully installed** 窗口。



注意

在安装过程中，Kaseya 会打开一个浏览器窗口，显示有关集成过程的信息。

11. 单击 **Finish**。
12. 打开 Kaseya Web 控制台，转至 **Trend Micro** > **Worry-Free Services**。

此时会显示以下窗口：

13. 请提供远程管理器激活凭证。

- **URL**（包括 https）
- **Access token**
- **Secret key**

注意

找到激活凭证的步骤：

a. 打开远程管理器控制台，然后转至 **管理** > **配置第三方集成**，然后再转至 **Kaseya** 部分。

b. 根据**步骤 3：在 Kaseya 控制台上，转至 Trend Micro > Worry-Free Services 并激活插件**，单击 **View credentials**。

c. 复制激活凭证并将其粘贴到 Kaseya Web 控制台。

---

14. 单击 **Connect**。

此时会显示 **Activation Successful** 向导，您可以使用此向导将现有的 Kaseya 客户导入适用于 Kaseya 的趋势科技安全无忧软件插件

有关详情，请参阅导入 Kaseya 客户 第 13-20 页。

更新适用于 Kaseya 的趋势科技安全无忧软件-云端版插件

通过更新适用于 Kaseya 的趋势科技安全无忧软件-云端版插件，您可以使用所有新功能和增强功能。更新后的版本会自动应用之前配置的设置，包括客户和安全客户端终端信息。

提示

也可以直接从 Kaseya 控制台下载适用于 Kaseya 的趋势科技安全无忧软件-云端版插件的更新软件包。如果有可用的更新，适用于 Kaseya 的趋势科技安全无忧软件-云端版插件的所有窗口的顶部均会显示一个信息栏。单击 **Download Now** 可获取软件包。

过程

1. 打开远程管理器控制台，然后转至**管理** > **配置第三方集成**。

   此时会显示**配置第三方集成**窗口。

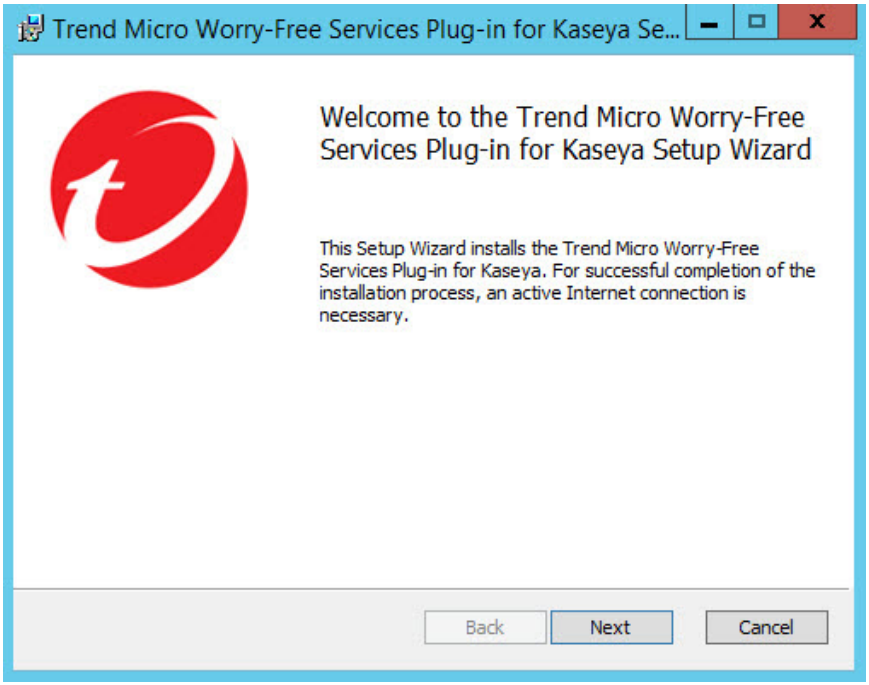
2. 转至 **Kaseya** 部分。

3. 在**适用于 Kaseya 的安全无忧软件-云端版插件**下，单击**下载**以保存此插件。

4. 将文件保存在 Kaseya VSA 服务器上。

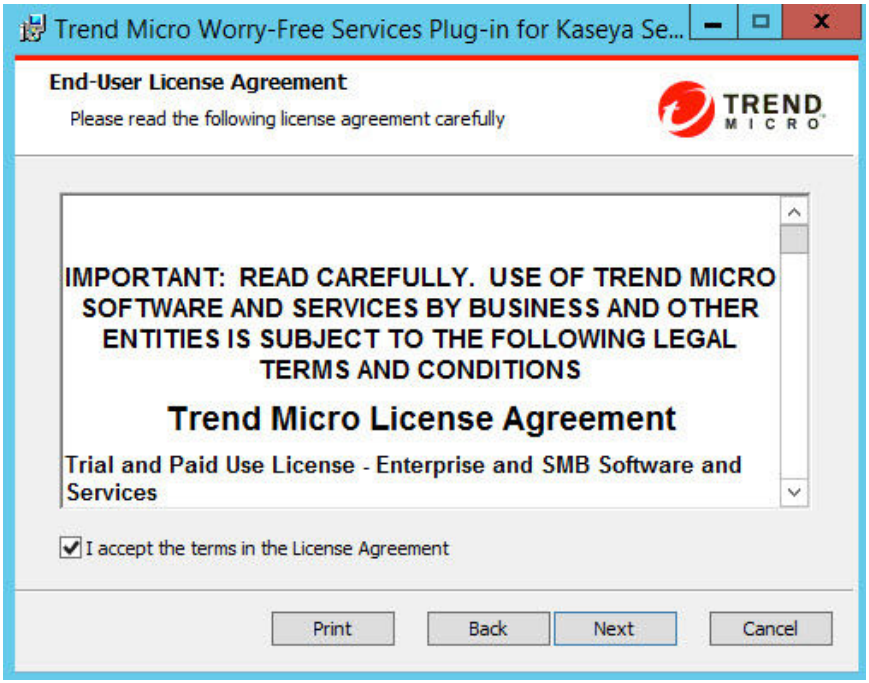
5. 执行 `TrendMicroWorryFreeServicesPluginForKaseya_X.X.X.msi` 文件。

此时会显示欢迎窗口。



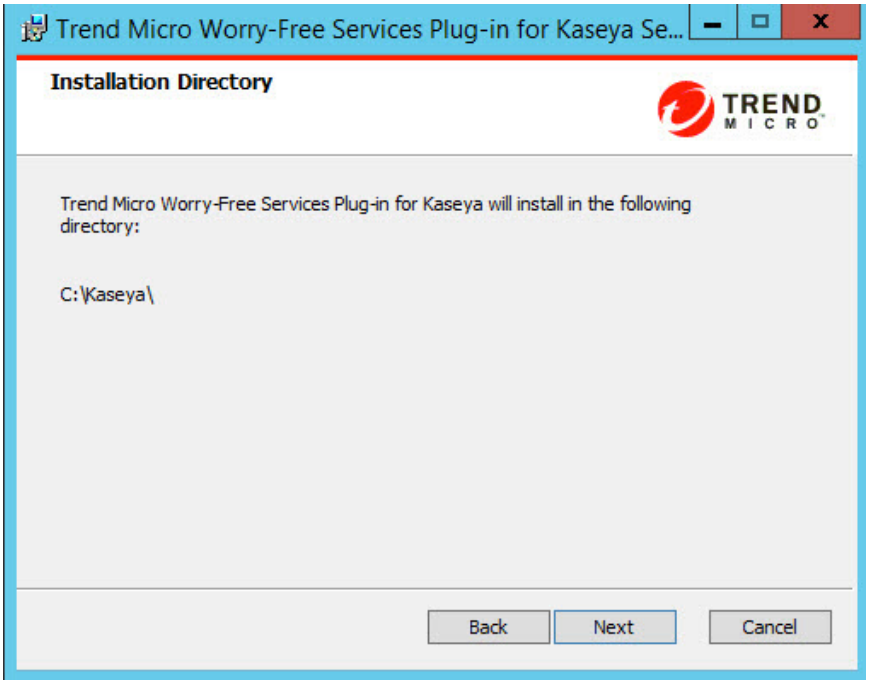
6. 单击 **Next**。

此时会显示 **End-User License Agreement** 窗口。



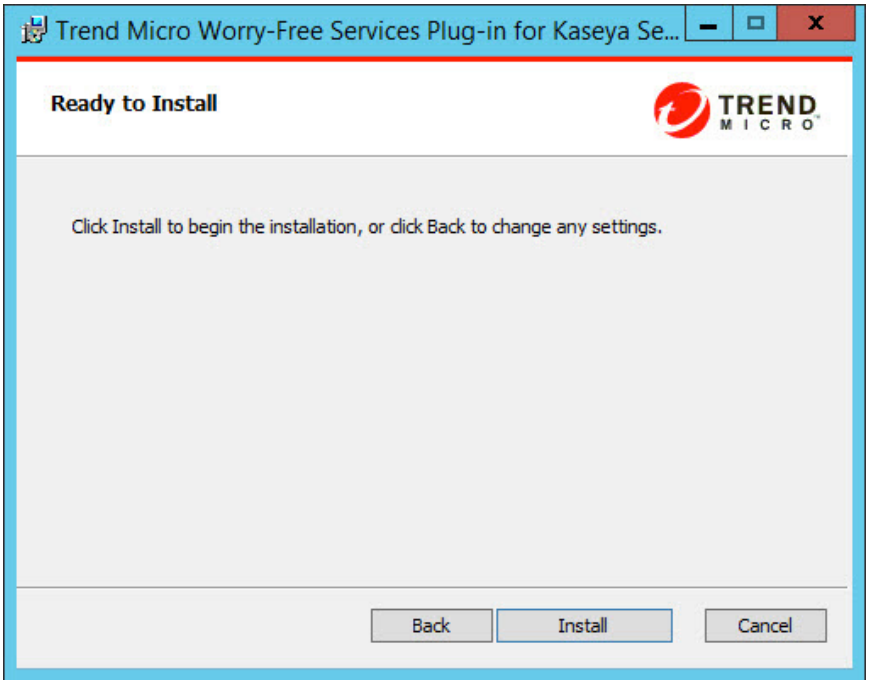
7. 如果您同意“许可协议”中的条款，请选中 **I accept the terms in the License Agreement** 复选框。
8. 单击 **Next**。

此时会显示 **Installation Directory** 窗口。



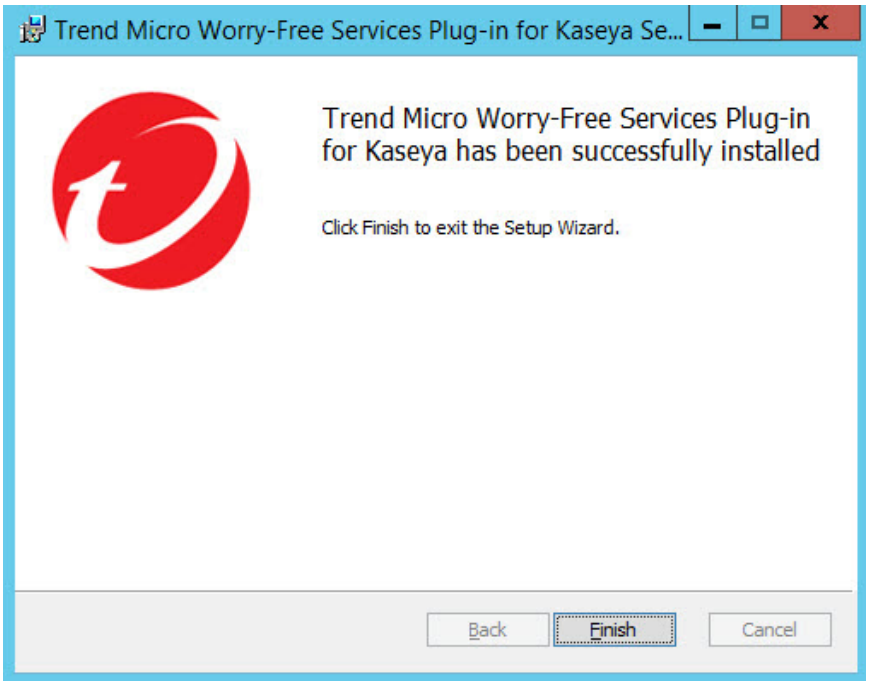
9. 确认 Kaseya 安装文件夹，然后单击 **Next**。

此时会显示 **Ready to Install** 窗口。



10. 单击 **Install**。

安装完成后，会显示 **Trend Micro Worry-Free Services Plug-in for Kaseya has been successfully installed** 窗口。



注意

在安装过程中，Kaseya 会打开一个浏览器窗口，显示有关集成过程的信息。

11. 单击 **Finish**。

已更新适用于 Kaseya 的安全无忧软件-云端版插件。

在 Kaseya 中管理趋势科技客户

为 Kaseya 激活趋势科技安全无忧软件-云端版插件后，您便可以开始直接从 Kaseya 控制台关联 Kaseya 客户与趋势科技帐户以及管理客户关联。

- 导入 Kaseya 客户：将当前的 Kaseya 客户与预先存在的或新的趋势科技帐户相关联

  有关更多信息，请参阅导入 Kaseya 客户 第 13-20 页。

- 客户摘要窗口：显示关联的趋势科技客户以及未与趋势科技帐户关联的 Kaseya 客户

  有关更多信息，请参阅客户摘要 第 13-24 页。

导入 Kaseya 客户

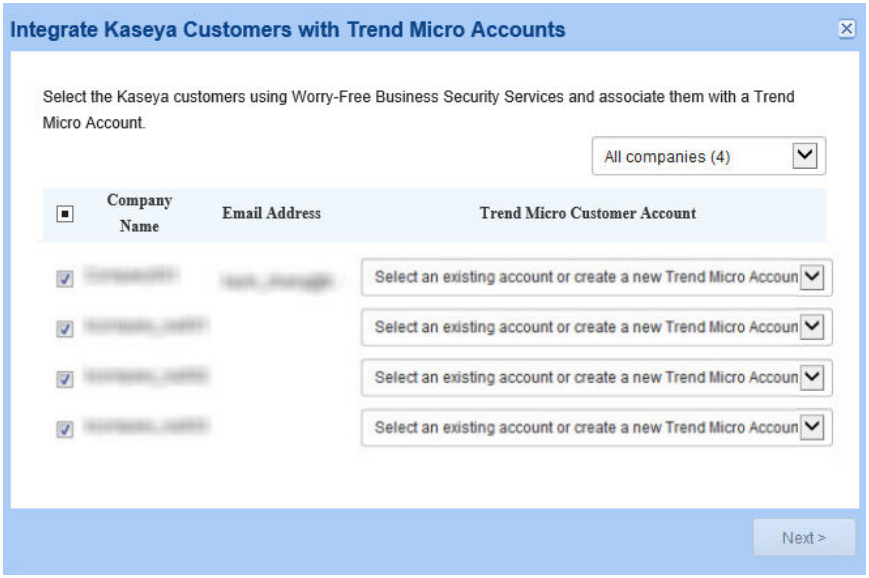
过程

1. 转至 **Integrate Kaseya Customers with Trend Micro Accounts** 窗口。
   - 从 Kaseya 导航树：
     a. 转至 **Trend Micro** > **Worry-Free Services** > **Customers**。
     b. 单击 **Non-Trend Micro Customers** 选项卡。
     c. 选中您想将其与趋势科技帐户关联的客户旁边的复选框。
     d. 单击 **Import to Trend Micro**。
   - 在首次激活 Kaseya 插件后，在 **Activation Successful** 窗口中单击 **Start**。

重要信息

您必须在随即显示的 **Integrate Kaseya Customers with Trend Micro Accounts** 窗口中选中想与趋势科技帐户集成的 Kaseya 客户旁边的复选框。

此时会显示 **Integrate Kaseya Customers with Trend Micro Accounts** 窗口。



2. 在 **Trend Micro Customer Account** 下拉列表中：

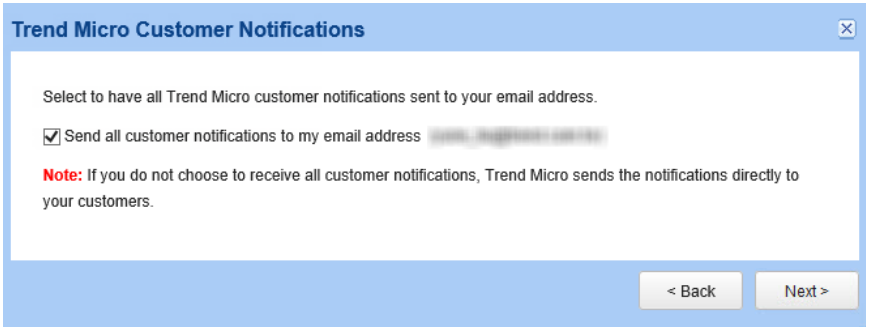
   - 选择 **+ Create a new Trend Micro Account**，以便在 Licensing Management Platform 中注册新客户
   - 从尚未分配给其他帐户的现有 Licensing Management Platform 客户中选择

注意

如果所有客户均已分配，则列表中不会显示任何客户信息。

3. 单击 **Next>**。

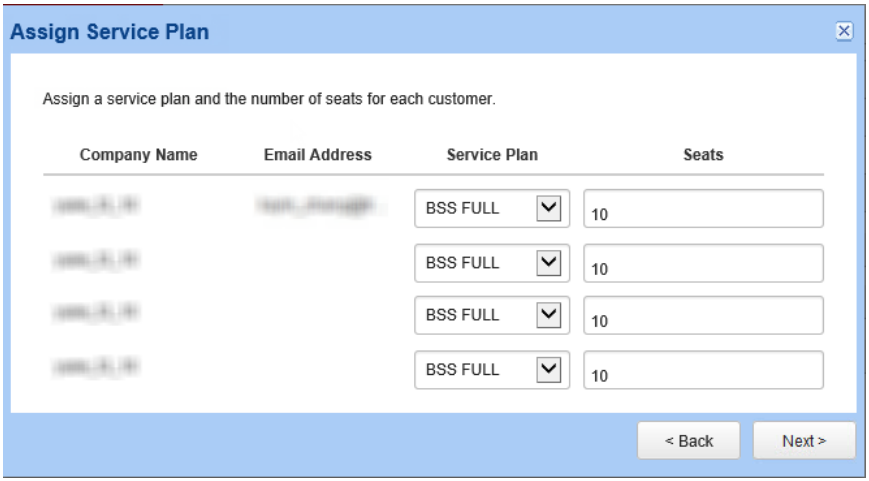
此时会显示 **Trend Micro Customer Notifications** 窗口。



4. 如果您希望系统将有关选定客户环境的所有电子邮件通知发送到您注册的电子邮件地址中，请选择 **Send all customer notifications to my email address**。

5. 单击 **Next>**。

   此时会显示**分配服务计划**窗口。



6. 为每个客户选择 **Service Plan**。

7. 验证分配给每个客户的 **Seats** 数量是否正确，然后单击 **Next >**，以将选定的客户添加到列表中。

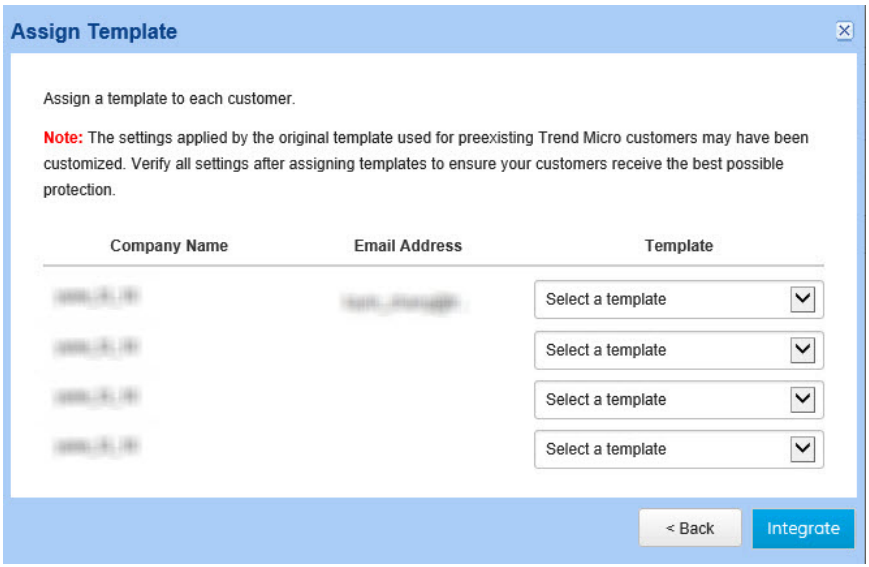
注意

缺省情况下，远程管理器提供的座席数比客户已在 Kaseya 中注册的终端数多 20%（每个客户最少有 10 个座席）。

重要信息

您必须为选定数量的 Kaseya 客户提供充分的 Licensing Management Platform 使用授权。如果您未提供充分的使用授权，则该插件只能导入列表中使用授权可用的前几位客户。

此时会显示**分配模板**窗口。



8. 在“Template”下拉列表中，向每个客户分配模板。

重要信息

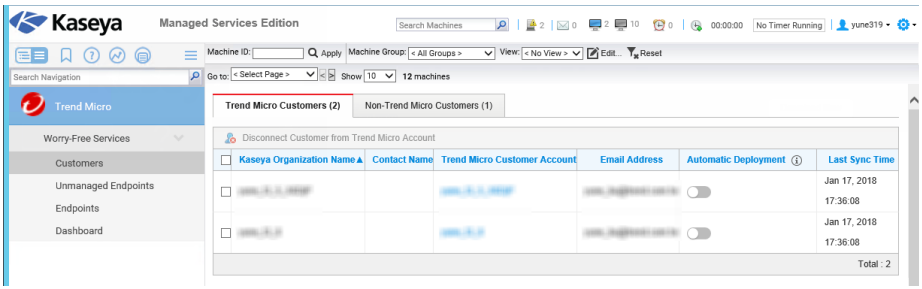
用于预先存在的趋势科技客户的原始模板所应用的设置可能已被定制。请在分配模板后验证所有设置，以确保客户获得最好的保护。

9. 单击 **Integrate**。

   此时会显示 **Complete Integration** 窗口。

客户摘要

Customers 窗口提供有关 Kaseya 客户的信息，其中包括 Kaseya 组织名称、主要客户联系人、趋势科技客户帐户、联系人电子邮件地址、自动部署状态以及上次与安全无忧软件-云端版同步的时间。



下表概述 **Customers** 窗口的主要部分。

部分	描述
“Trend Micro Customers”选项卡	显示用以列出 Kaseya 客户的趋势科技帐户信息的表格 启用 **Automatic Deployment**，以便将安全客户端自动部署到已分配给 ConnectWise Automate 客户的无防护终端（每小时部署一次）。 **重要信息** 确保 Kaseya 客户有足够多的可用使用授权，然后再启用自动部署。如果没有可用的使用授权，趋势科技安全无忧软件-云端版插件仍会部署安全客户端，但是，无使用授权的安全客户端无法向安全无忧软件-云端版控制台汇报，并且仍然留在非托管终端列表中。
“Non-Trend Micro Customers”选项卡	显示用以列出未与趋势科技帐户关联的 Kaseya 客户帐户信息的表格 **注意** 要部署趋势科技安全客户端，请选中您要管理的终端旁边的复选框，然后单击 **Deploy Agent**。 有关更多信息，请参阅导入 Kaseya 客户 第 13-20 页。

在 Kaseya 中管理安全无忧软件客户端

Endpoints 窗口提供当前已安装安全客户端的 Kaseya 客户终端的相关信息。

下表概述 **Endpoints** 窗口的主要部分。

部分	描述
命令交互	显示可对选定终端的安全客户端执行的多个命令交互 • **Scan**：对选定的终端执行扫描 有关更多信息，请参阅扫描安全无忧软件客户端 第 13-29 页。 • **Update**：在选定的终端上更新安全客户端 有关更多信息，请参阅更新安全无忧软件客户端 第 13-31 页。 • **Unload Agent**：从选定的终端卸载安全客户端 有关更多信息，请参阅卸载安全无忧软件客户端 第 13-30 页。 • **Remove Agents**：从选定的终端删除安全客户端 有关更多信息，请参阅删除安全无忧软件客户端 第 13-28 页。
终端摘要	显示一个表，该表概述 Kaseya 客户的终端信息并指出终端是否需要立即关注 **注意** 在 **Status** 列中，脱机安全客户端的背景将显示为红色。 **Status** 列指示安全客户端的连接状态和已发送到安全客户端的命令的状态。

有关非托管终端的更多信息，请参阅将安全客户端部署到非托管的终端 第 13-26 页。

将安全客户端部署到非托管的终端

您可通过 **Unmanaged Endpoints** 窗口查看当前尚未安装安全客户端的所有客户终端的 Kaseya 列表。

重要信息

在将安全客户端部署到终端之前，您必须先为 Kaseya 安装 Kaseya 客户端程序脚本。

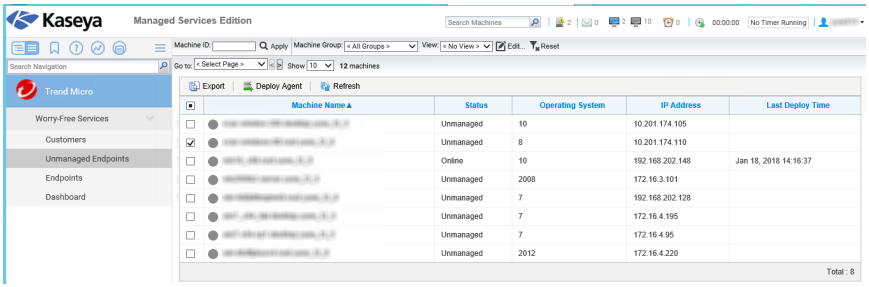
提示

您可以导出 CSV 格式的非托管的终端列表，以便进一步评估。

过程

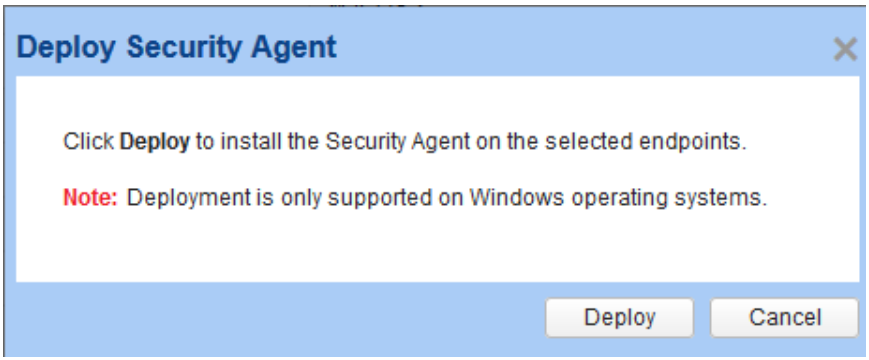
1. 打开 Kaseya Web 控制台，转至 **Trend Micro** > **Worry-Free Services** > **Unmanaged Endpoints**。

   此时会显示以下窗口：



2. 使用 Kaseya 搜索栏过滤搜索结果。
3. 选中您要在其上部署安全无忧软件客户端的计算机旁边的复选框。
4. 单击 **Deploy Agent**。

   此时会显示 **Deploy Security Agent** 窗口。



5. 单击 **Deploy**。

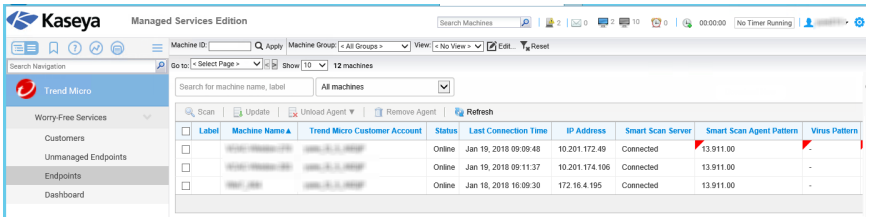
> **注意**
>
> 远程管理器下次与安全无忧软件-云端版同步时，终端会收到命令。缺省同步时间为 5 分钟。仅在尚未安装安全客户端的终端上进行安装。

删除安全无忧软件客户端

过程

1. 打开 Kaseya Web 控制台，转至 **Trend Micro** > **Worry-Free Services** > **Endpoints**。

   此时会显示以下窗口：



2. 使用下拉列表过滤终端：

   - **All machines**
   - **Online**
   - **Offline**
   - **Outdated**
   - **With virus detections**
   - **With spyware detections**

3. 选中所需终端旁边的复选框，然后单击 **Remove Agent**。

   此时会显示确认窗口。

4. 单击 **Remove**。

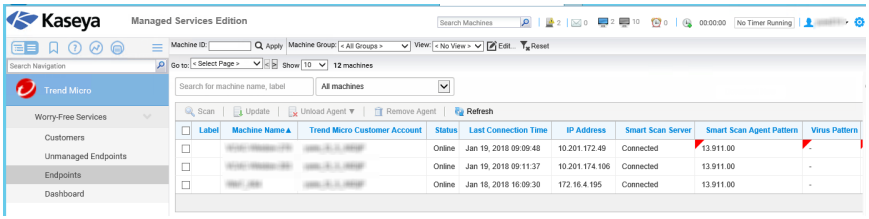
   在选定的终端上会立即卸载安全客户端程序。

扫描安全无忧软件客户端

过程

1. 打开 Kaseya Web 控制台，转至 **Trend Micro** > **Worry-Free Services** > **Endpoints**。

   此时会显示以下窗口：

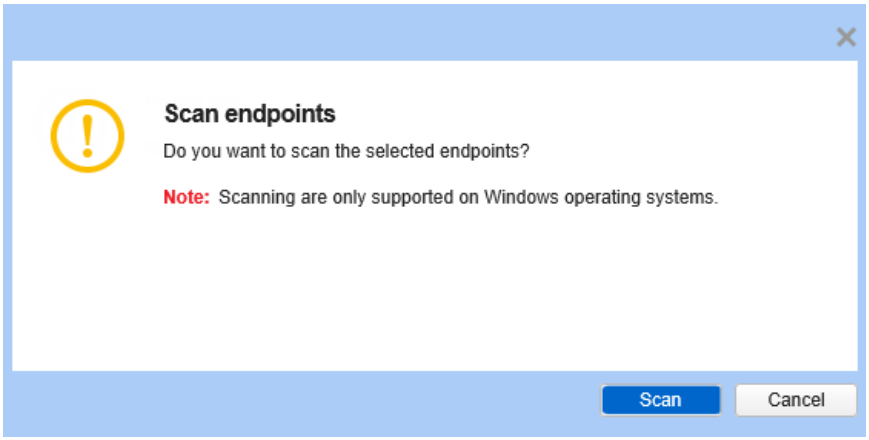


2. 使用下拉列表过滤终端：

   - **All machines**
   - **Online**
   - **Offline**
   - **Outdated**
   - **With virus detections**
   - **With spyware detections**

3. 选中您要扫描的终端旁边的复选框，然后单击 **Scan**。

   此时会显示确认窗口。



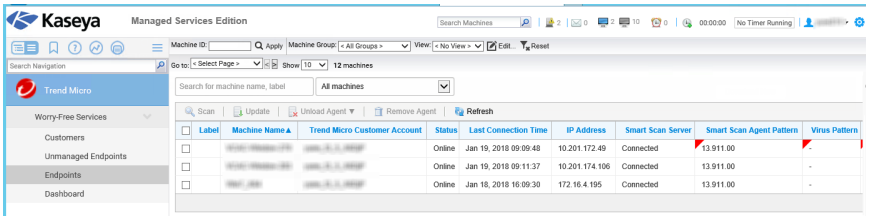
4. 单击 **Scan**。

卸载安全无忧软件客户端

过程

1. 打开 Kaseya Web 控制台，转至 **Trend Micro** > **Worry-Free Services** > **Endpoints**。

   此时会显示以下窗口：



2. 使用下拉列表过滤终端：

   - **All machines**
   - **Online**
   - **Offline**
   - **Outdated**
   - **With virus detections**
   - **With spyware detections**

3. 选中您要卸载的终端旁边的复选框，然后单击 **Unload Agent**。在出现的下拉列表中，选择选定的安全客户端应在多长时间内保持卸载状态。

   此时会显示确认窗口。

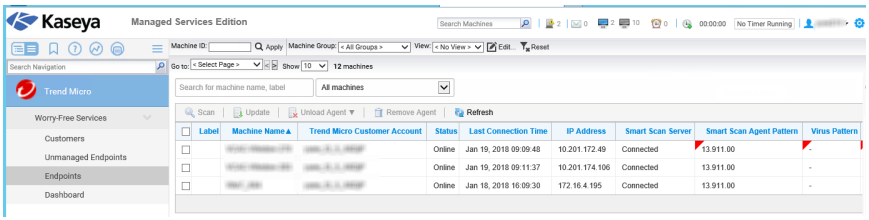
4. 单击 **Unload**。

更新安全无忧软件客户端

过程

1. 打开 Kaseya Web 控制台，转至 **Trend Micro** > **Worry-Free Services** > **Endpoints**。

   此时会显示以下窗口：



2. 使用下拉列表过滤终端：

- **All machines**
- **Online**
- **Offline**
- **Outdated**
- **With virus detections**
- **With spyware detections**

3. 选中您要更新的终端旁边的复选框，然后单击 **Update**。

   此时会显示确认窗口。

4. 单击 **Update**。

趋势科技控制台

使用**控制台**可快速查看您的 Kaseya 客户的安全状态以及安全无忧软件-云端版检测到的威胁的总数。

控制台可以提供以下小组件：

- Action Required Events 小组件 第 13-32 页
- Threat Management 小组件 第 13-33 页

Action Required Events 小组件

Action Required Events 小组件列出了其终端需要受到注意的客户。

事件	描述
处理措施不成功	单击 **Occurrences**，转至安全无忧软件-云端版控制台，然后查看客户终端上不成功的扫描结果。

事件	描述
需要实时扫描	单击 **Endpoints**，转至安全无忧软件-云端版控制台，然后查看已禁用实时扫描的终端。
需要重新启动	单击 **Occurrences**，转至安全无忧软件-云端版控制台，然后查看需要重新启动方能完成清除间谍软件/灰色软件操作的终端。
需要更新	单击 **Endpoints**，转至安全无忧软件-云端版控制台，然后查看需要更新的终端。

单击 **Company** 名称可在远程管理器控制台上查看信息。

Threat Management 小组件

查看拥有不同类型的安全检测的客户数量。单击威胁 **Type**，可在远程管理器控制台上查看详细信息。

Kaseya 中的安全无忧软件-云端版票证

下表概述安全无忧软件-云端版插件生成的 Kaseya 票证。

命令类型	票证主题	可能的原因
Scan	[Action Required] Unsuccessful scan command - <machine_name> of <client_name> - Worry-Free Business Security Services	• 选定的终端未安装安全客户端 • 在选定终端上安装的安全客户端已损坏 • 选定的终端处于脱机状态或者未加载安全客户端 • 安全客户端正在进行更新 • 发生内部错误

命令类型	票证主题	可能的原因
Update Agent	[Action Required] Unsuccessful update command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 选定的终端未安装安全客户端 • 在选定终端上安装的安全客户端已损坏 • 选定的终端处于脱机状态或者未加载安全客户端 • 安全客户端正在进行扫描 • 发生内部错误
Deploy Agent	[Action Required] Unsuccessful deployment command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 服务器未完成安全客户端安装软件包的生成 • 下载安全客户端安装软件包时出错 • 选定的终端上正在安装或已安装安全客户端
Automatic Deployment	[Action Required] Exceeded seat allocation for <machine_name> of <client_name> - Worry-Free Business Security Services	• 安全客户端已部署，但因客户的剩余使用授权不足而仍然处于非托管状态

部分 V

监控客户

第 14 章

了解控制台

趋势科技远程管理器配有监控控制台，可让您快速查看所有客户的安全、系统和使用授权状态。

本节包含以下主题：

控制台状态窗口

“控制台”是查看受监控网络的状态的中央窗口。“控制台”仅列出了状态不正常的产品。例如，如果客户的安全无忧软件-云端版使用授权即将到期，或者客户受到的威胁太多，这些客户就会列在此处。

要访问“控制台”，请打开兼容的浏览器，然后登录到您所在地区的趋势科技远程管理器站点。

控制台上的大多数项目都带有链接，以帮助您解决问题。单击项目（图表、链接、数字）可解决问题。

有关更多信息，请参阅产品/服务信息 第 3-4 页。

使用选项卡和小组件

选项卡能容纳小组件。**主页**窗口上的每个选项卡能容纳多达 20 个小组件。**主页**窗口本身能支持多达 30 个选项卡。

小组件是控制台的核心组件。小组件提供了有关安全性或授权相关事件的具体信息。某些小组件允许您执行特定任务。

小组件显示的信息来自：

- Cloud App Security
- Cloud Edge 服务器和客户端
- Hosted Email Security 服务
- InterScan Web Security as a Service
- 安全无忧软件服务器和客户端
- 安全无忧软件-云端版服务器

选项卡任务

下表列出了所有选项卡相关的任务：

任务	步骤
添加选项卡	单击**主页**窗口顶部的添加图标 (+)。此时会显示一个新的选项卡。
重命名选项卡	将鼠标悬停在选项卡名称上并单击向下箭头 ( )，然后单击**重命名**。为选项卡键入新名称。
编辑选项卡布局	将鼠标悬停在选项卡名称上并单击向下箭头 ( )，然后单击**更改布局**。此时会打开**更改布局**窗口。 有关更多信息，请参阅更改布局窗口 第 14-4 页。
删除选项卡	将鼠标悬停在选项卡名称上并单击向下箭头 ( )，然后单击**删除**。单击**确定**以删除此选项卡。
播放选项卡幻灯片	单击选项卡右侧显示的**设置**按钮 ( )，然后单击**选项卡幻灯片**滑块。在滑块下的下拉菜单中，选择显示所选选项卡的时间间隔。

任务	步骤
移动选项卡	使用拖放操作更改选项卡的位置。 **注意** 仅部分浏览器支持拖放功能。 有关推荐浏览器的更多信息，请参阅浏览器要求 第 1-7 页。

更改布局窗口

在选项卡的下拉菜单 ( ) 中单击**更改布局**选项后，系统会打开**更改布局**窗口。

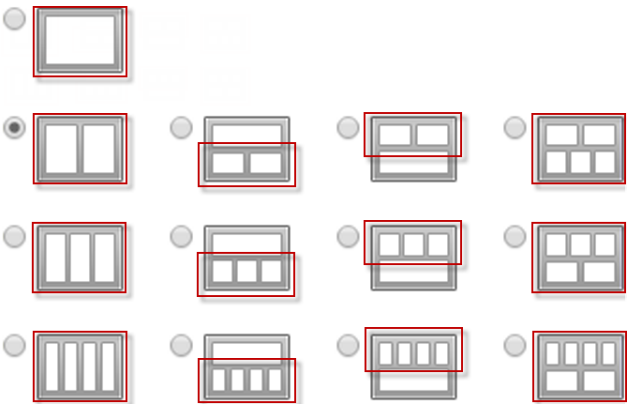
提示

趋势科技建议根据您选择的布局使用以下最小窗口分辨率：

- 2 列：800 x 600 或以上
- 3 列：1280 x 720 或以上
- 4 列：1680 x 1050 或以上

小组件任务

下表所列为与小组件相关的任务：

任务	步骤
添加小组件	打开一个选项卡，然后在选项卡右上角单击**添加小组件**。屏幕上会显示**添加小组件**窗口。
刷新小组件数据	单击刷新图标 ( )。
查看帮助	单击**帮助** (?)。
删除小组件	单击**关闭小组件** ( )。此操作会从包含该小组件的选项卡删除该小组件，但是不会从其他选项卡或从**添加小组件**窗口的小组件列表中删除该小组件。
移动小组件	使用拖放操作将小组件移动到选项卡上的其他位置。
调整小组件尺寸	要调整小组件大小，请将光标指向小组件的右边缘。当您看到一条粗垂直线和箭头（如下图所示）时，按住鼠标，然后将光标向左或向右移。  只有多列标签上的小组件可以调整尺寸。这些选项卡采用任意以下布局，其中的突出显示部分包含可以调整尺寸的小组件。 

远程管理器小组件

控制台中显示以下远程管理器小组件：

“具有通知的客户”小组件

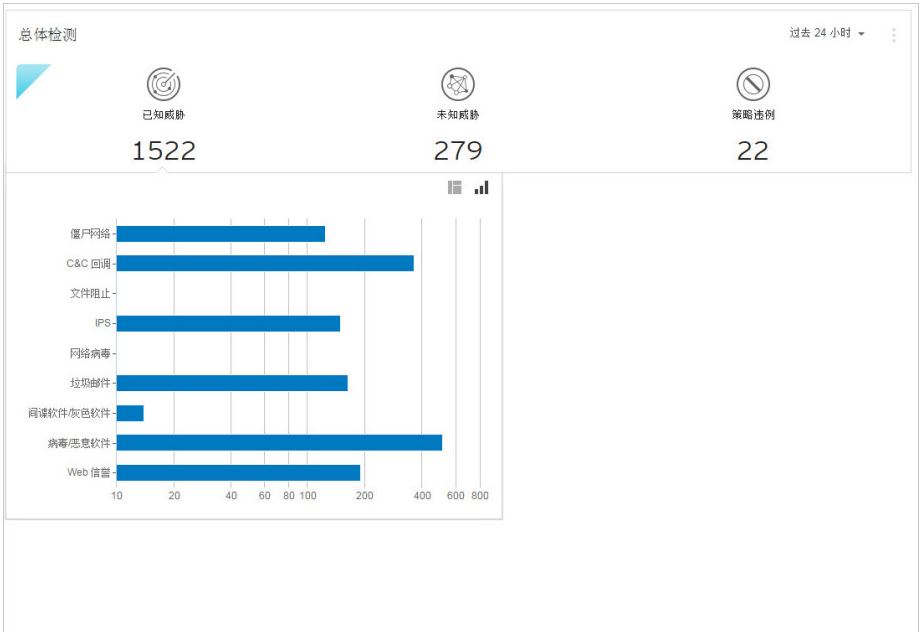
此小组件统计您当前具有“需要采取处理措施”或“警告”事件状态的远程管理器客户数。

将鼠标悬停在客户计数上可查看最近受影响客户的顶级事件类别。

要打开**通知中心**并查看当前状态的详细说明，请单击特定**类别**的**出现次数**计数，或者单击**在通知中心中查看全部**以查看所有受影响的客户。

有关更多信息，请参阅通知中心 第 14-32 页。

“总体检测”小组件



此小组件可以概述选定时间范围内的所有威胁检测和策略违例。

将鼠标悬停在威胁或违例计数上可查看每个组出现的特定类型检测的详细信息。

要切换视图，请单击右上角的表格图标或条形图图标。要在表格视图中查看特定功能的日志，请单击右侧的计数。要在条形图视图中查看特定功能的日志，请单击右侧的条形。

表 14-1. 检测类别

类别	描述
已知威胁	显示趋势科技确认的可以检测安全威胁的所有功能 • 僵尸网络 • C&C 回调 • 文件阻止 • IPS • 网络病毒 • 垃圾邮件 • 病毒/恶意软件 • 间谍软件/灰色软件 • Web 信誉
未知威胁	显示使用高级启发式功能、分析功能或建模功能检测潜在威胁的所有功能 • 预测型机器学习 • 行为监控 • 沙盒平台
策略违例	显示包含特定于您公司的安全标准的策略违例的所有功能 • 应用程序控制 • 设备控制 • URL 过滤

最需要注意的客户小组件

显示出现事件最多且需要立即采取行动或做出响应的客户的最新数量。数据显示在表格和饼图中。单击显示图标 ( ) 即可在表格和饼图之间切换。

- 如果处于特定状态的客户端的数量是 1 或更多，您可以点击数字，以在产品树中查看事件。
- 点击客户名称可以查看该客户的所有事件；展开客户名称可以查看某些类别的事件。
- **需要采取处理措施**下的事件数是应尽快处理的事件的数量。
- **警告**下的事件数是不如“需要采取处理措施”下的事件紧急，但是仍然需要尽快处理的事件的数量。

勒索软件检测结果数最多的客户小组件

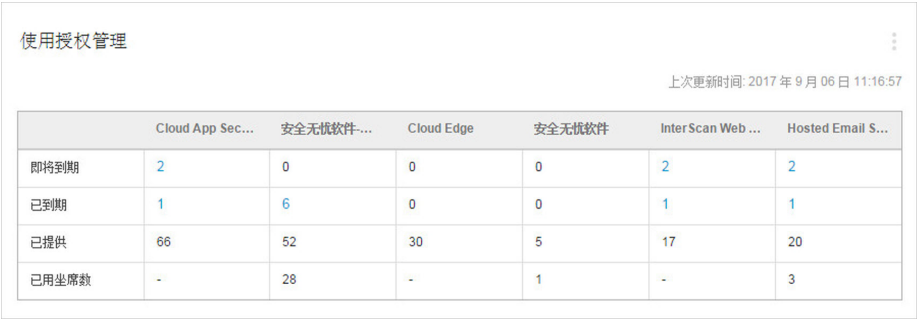
此小组件显示在选定时间范围内勒索软件检测结果数最多的 Cloud Edge 和安全无忧软件-云端版客户。

要切换视图，请单击右上角的表格图标或条形图图标。

查看	选项
表	• 单击**客户**名称以打开**客户> [客户]** 窗口。 • 单击任意一项检测计数以查看事件日志。
条形图	• 将鼠标悬停在长条上以查看特定客户产品的检测结果数。 • 单击任意一个长条以查看事件日志。

使用授权管理小组件

显示客户正在使用的使用授权的当前状态。



系统会针对客户和产品显示以下与使用授权有关的信息：

- **即将到期**：虽然尚未到期，但很快就会到期的使用授权的数量。
- **已到期**：已到期的使用授权。

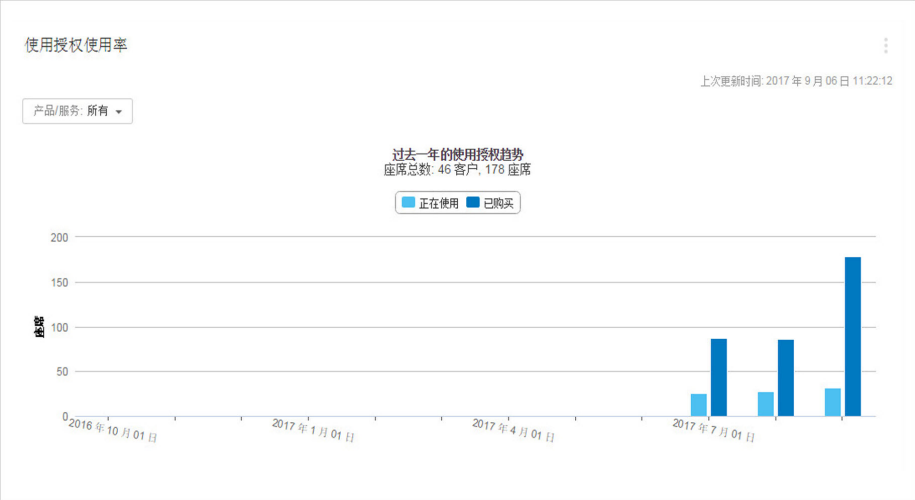
注意

趋势科技建议尽快续订这些使用授权。

- **已用座席数**：这些是当前已使用的座席数。
- **已提供**：这些是客户提供的座席数。

使用授权使用率小组件

显示已分配的和实际购买的座席的图形分析。这样可以帮助您确定应增加还是减少座席分配。



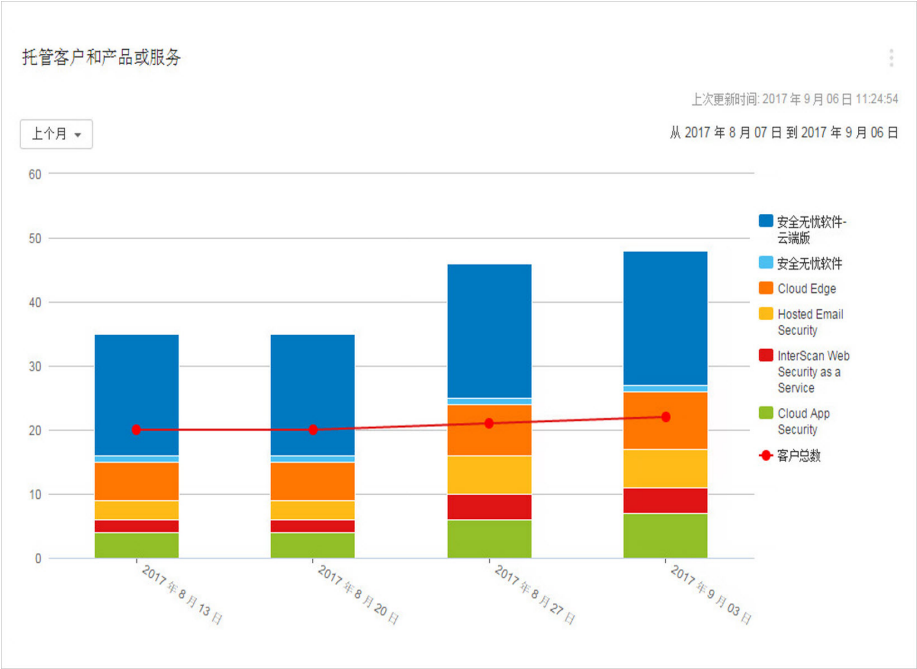
您可以更改产品/服务，具体选项有：

- 所有
- Hosted Email Security
- 安全无忧软件
- 安全无忧软件-云端版
- Cloud Edge

- InterScan Web Security as a Service
- Cloud App Security

托管客户和产品或服务小组件

显示指定时间段内每种产品的托管客户数量。



- 您可以更改数据显示的时间范围，具体选项有：
  - 上个月（缺省）
  - 过去 3 个月

  - 过去 6 个月
  - 去年
- 您可以在右侧已注册产品的名称，从而向图中添加或从图中删除数据。
- 每个条形图代表一周或一月。
- 条形图显示产品/服务总数。

勒索软件检测小组件

显示来自 Cloud App Security、Hosted Email Security、安全无忧软件-云端版、Cloud Edge、InterScan Web Security as a Service 和安全无忧软件的勒索软件检测数据。

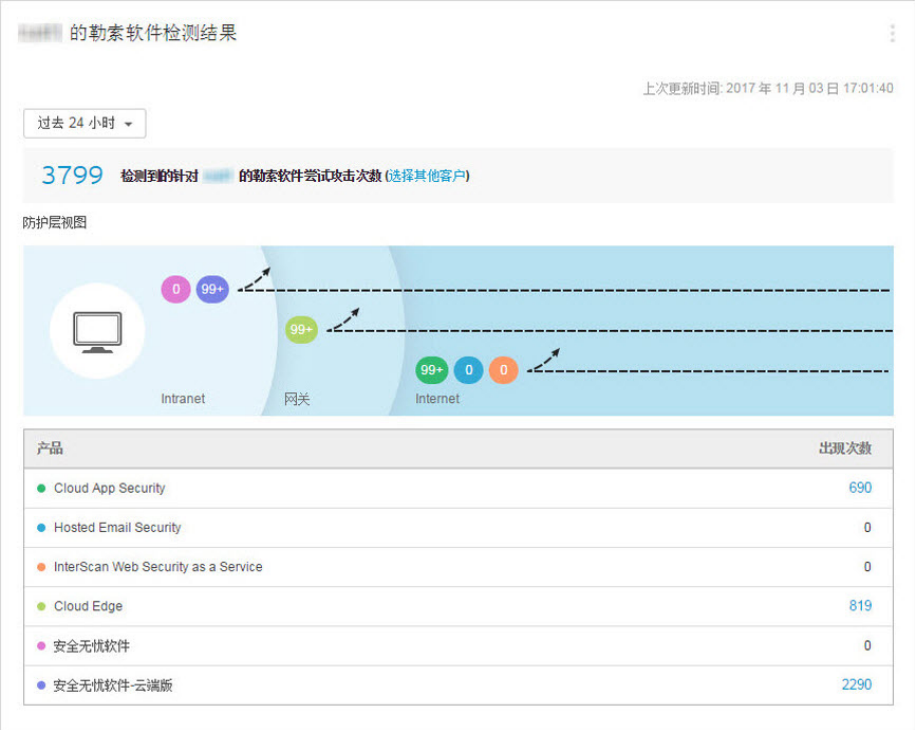
- 您可以更改所显示数据的时间范围，具体选项有：
  - 过去 24 小时（缺省）

- 过去 7 天
- 过去 30 天

- 您可以通过单击以下计数，查看勒索软件事件日志：
  - **感染攻击次数**：显示按出现次数排序的勒索软件事件日志。
  - **检测到勒索软件攻击的客户数量**：显示按公司名称排序的勒索软件事件日志。
- 展开信息框 ()，查看**全面强化安全无忧软件-云端版的勒索软件防护**链接。单击此链接，以便为所有客户启用勒索软件防护。

  有关在远程管理器中配置勒索软件防护的更多信息，请参阅全面强化勒索软件防护常见问题解答 第 18-11 页。

所有客户的勒索软件检测结果小组件



此小组件显示在选定时间范围内受支持产品的勒索软件检测结果总数。您可以自定义此小组件以显示单个客户的数据。

单击任意一项检测计数以查看事件日志。

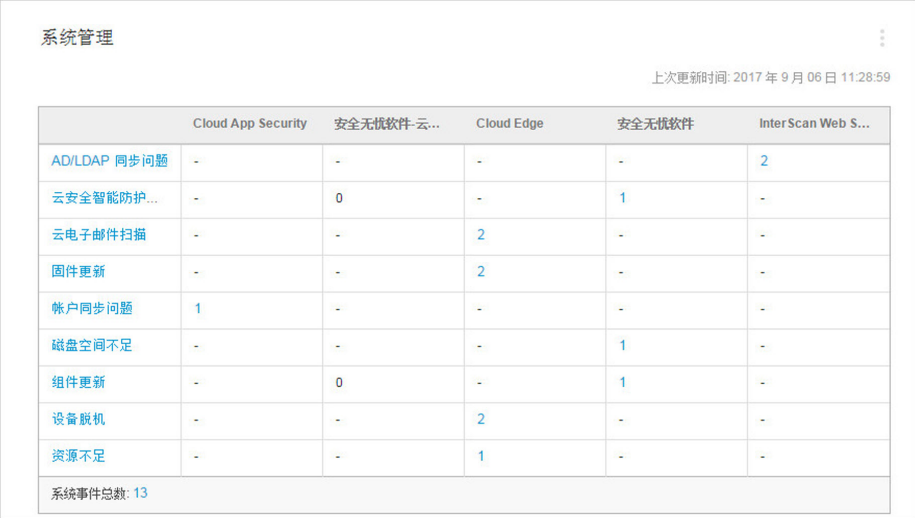
要查看特定客户的数据，请单击**显示特定客户的数据**链接，并选择您想要显示的客户和产品。您还可以更改小组件的标题。

表 14-2. 防护层

防护层	描述
Internet	**Internet** 层包含在云中的威胁到达用户的网关前对其进行检测的产品。 在此层运行的产品包括： • Cloud App Security • Hosted Email Security • InterScan Web Security as a Service 将鼠标悬停在圆形的产品图标上以显示有关该产品检测到的勒索软件尝试攻击次数的数据。
网关	**网关**层包含保护路由器、服务器和其他网关设备的产品。 在此层运行的产品包括： • Cloud Edge 将鼠标悬停在圆形的产品图标上以显示有关该产品检测到的勒索软件尝试攻击次数的数据。
Intranet	**Intranet** 层包括保护网关内的终端的产品。 在此层运行的产品包括： • 安全无忧软件 • 安全无忧软件-云端版 将鼠标悬停在圆形的产品图标上以显示有关该产品检测到的勒索软件尝试攻击次数的数据。

系统管理小组件

显示已注册产品的当前所有系统事件的数量。您可以使用此数据确定服务器或客户端的硬件问题或事件。



	Cloud App Security	安全无忧软件-云...	Cloud Edge	安全无忧软件	InterScan Web S...
AD/LDAP 同步问题	-	-	-	-	2
云安全智能防护...	-	0	-	1	-
云电子邮件扫描	-	-	2	-	-
固件更新	-	-	2	-	-
帐户同步问题	1	-	-	-	-
磁盘空间不足	-	-	-	1	-
组件更新	-	0	-	1	-
设备脱机	-	-	2	-	-
资源不足	-	-	1	-	-

系统事件总数: 13

如果处于特定类别的事件的数量是 1 或更多，您可以点击数字，以在事件日志中查看事件。

威胁管理小组件

显示所有已注册产品的威胁事件计数。


威胁管理

上次更新时间: 2017 年 9 月 06 日 11:54:00

过去 24 小时

从 2017 年 8 月 30 日 到 2017 年 9 月 06 日

	Cloud App Security	安全无忧软件-云端版	Hosted Email Security
C&C 回调	-	-	-
IPS	-	-	-
URL 过滤	-	6010	-
Web 信誉	1404	3450	-
僵尸网络	-	-	-
勒索软件	7020	15470	2814
反垃圾邮件	-	-	482400
应用程序控制	-	3690	-
文件阻止	1404	-	-
沙盒平台	4212	-	-
病毒/恶意软件	1404	6620	8844000
网络病毒	-	3690	-
行为监控	-	6700	-
设备控制	-	1472	-
间谍软件/灰色软件	-	3690	-
预测型机器学习	-	3680	-

威胁事件总数: 9399130

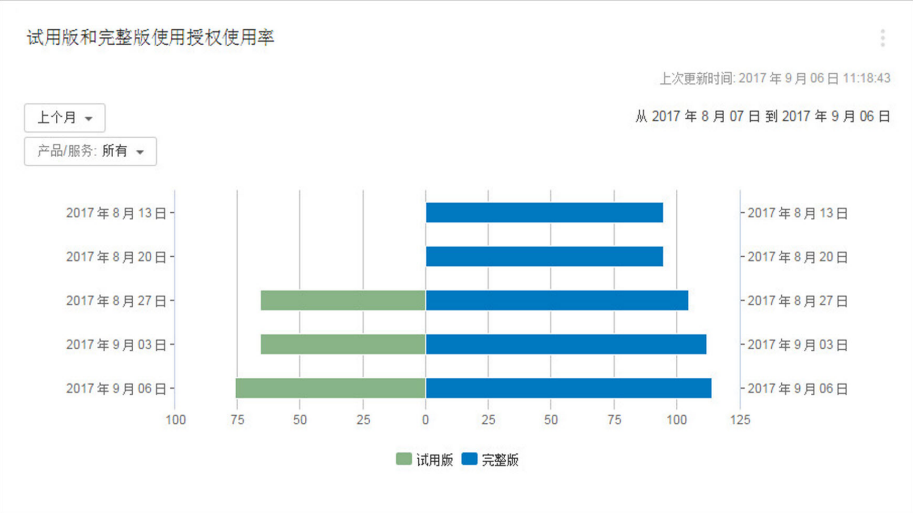
- 您可以更改数据显示的时间范围，具体选项有：
  - 过去 24 小时（缺省）

- 过去 7 天
- 过去 30 天

- 如果处于特定类别的事件的数量是 1 或更多，您可以点击数字，以在事件日志中查看事件。

试用版和完整版使用授权使用率小组件

显示已用于已注册产品的试用版或完整版使用授权的数量。



您可以更改数据显示的时间范围，具体选项有：

- 上个月（缺省）
- 过去 3 个月
- 过去 6 个月
- 去年

您可以更改产品/服务，具体选项有：

- 所有
- Hosted Email Security
- 安全无忧软件
- 安全无忧软件-云端版
- Cloud Edge
- InterScan Web Security as a Service
- Cloud App Security

查看针对特定产品的事件

针对特定产品的事件会显示实时事件的列表。

过程

1. 转至**客户** > **{公司名称}** > **{产品}**。
2. 根据选择的产品，执行以下其中一项操作：

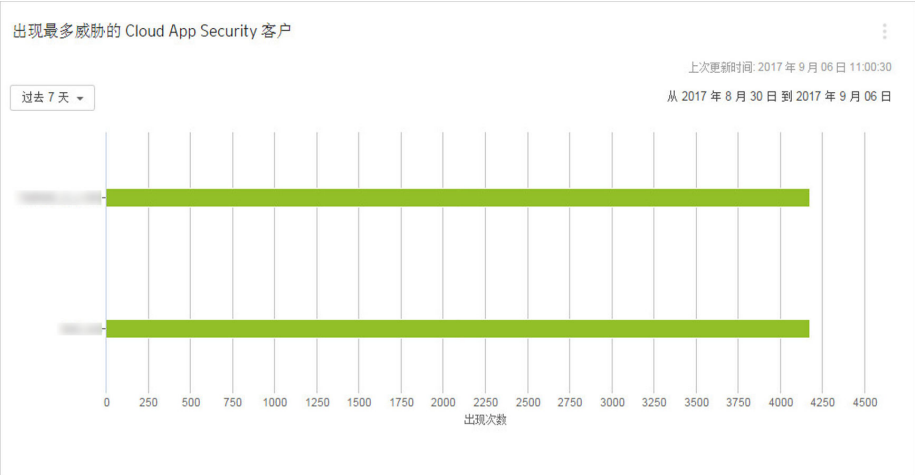
产品	步骤
Cloud App Security	转至**事件**选项卡。
Cloud Edge	转至**事件**选项卡。
InterScan Web Security as a Service	从网络树中选择 IWSaaS 产品后，会自动显示事件列表。
安全无忧软件	转至**事件**选项卡。
安全无忧软件-云端版	转至**事件**选项卡。

Cloud App Security 小组件

控制台中显示以下 Cloud App Security 小组件：

出现威胁最多的 Cloud App Security 客户小组件

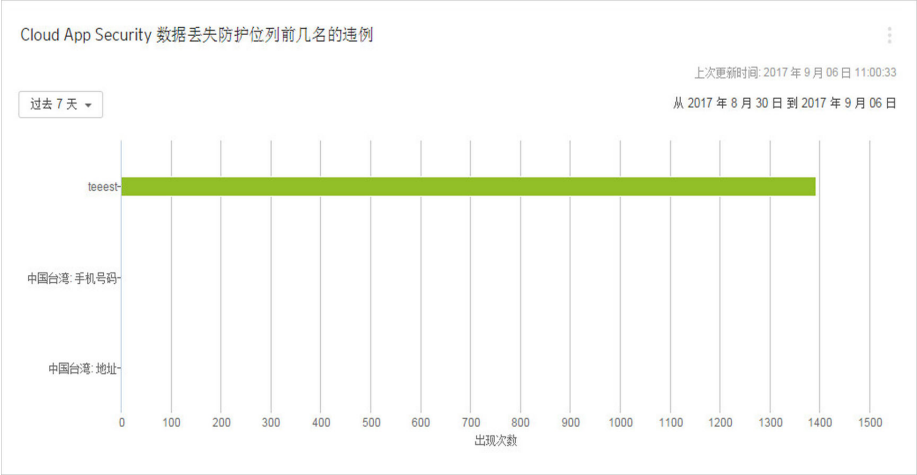
显示出现威胁事件数最多的 Cloud App Security 客户。



单击直条可查看事件日志。

Cloud App Security 数据丢失防护位列前几名的违例小组件

显示出现数据丢失防护模板违例最多的 Cloud App Security 客户。

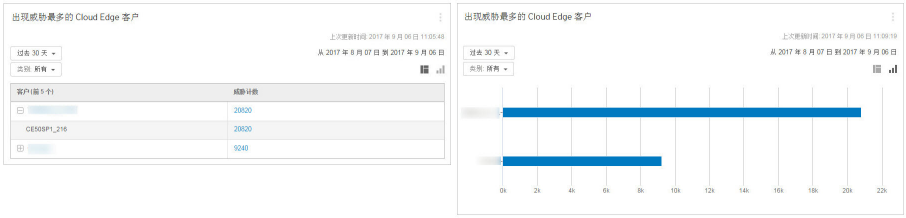


单击直条可查看事件日志。

Cloud Edge 小组件

控制台中显示以下 Cloud Edge 小组件：

出现威胁最多的 Cloud Edge 客户小组件



此小组件显示出现威胁事件最多的 Cloud Edge 客户。

数据显示在表格和条形图中。要切换视图，请单击右上角的表格图标或条形图图标 ( )。

- 单击右侧的计数可查看来自 Cloud Edge 控制台的详细威胁信息。
- 单击**客户**名称以打开**客户 > [客户]** 窗口。
- 通过选择以下选项更改所显示的数据类别：
  - 所有
  - 僵尸网络
  - C&C 回调
  - IPS
  - 预测型机器学习
  - 勒索软件 (电子邮件渠道)
  - 勒索软件 (网络渠道)
  - 勒索软件 (Web 渠道)
  - 垃圾邮件
  - 沙盒平台

- 病毒 (电子邮件渠道)
- 病毒 (Web 渠道)
- Web 信誉

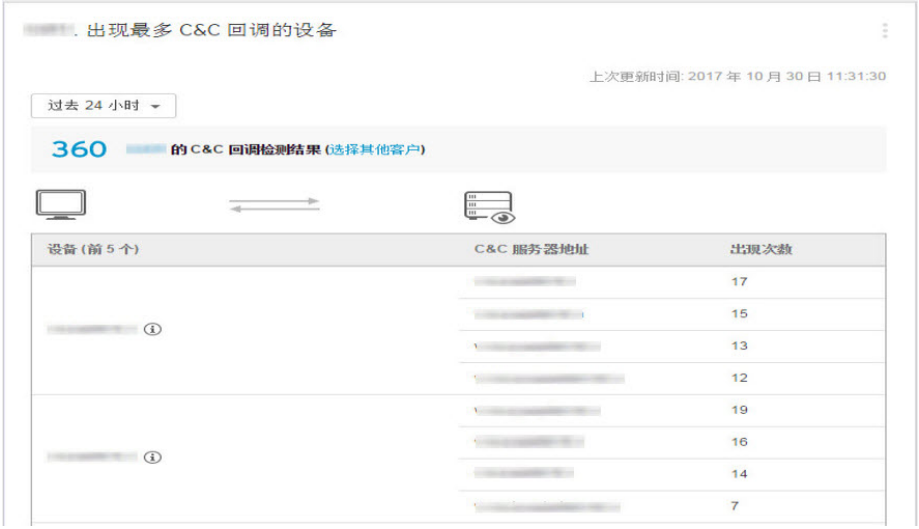
出现威胁最多的 Cloud Edge 设备小组件

此小组件显示出现威胁事件最多的 Cloud Edge 设备。

- 单击右侧的计数可查看来自 Cloud Edge 控制台的详细威胁信息。
- 单击**客户**名称以打开**客户 > [客户]** 窗口。
- 通过选择以下选项更改所显示的数据类别：
  - 所有
  - 僵尸网络
  - C&C 回调
  - IPS
  - 预测型机器学习
  - 勒索软件 (电子邮件渠道)

- 勒索软件 (网络渠道)
- 勒索软件 (Web 渠道)
- 垃圾邮件
- 沙盒平台
- 病毒 (电子邮件渠道)
- 病毒 (Web 渠道)
- Web 信誉

单个客户出现最多 C&C 回调的设备小组件



此小组件显示在选定时间范围内特定客户出现最多 C&C 回调的排名靠前的设备。设备由服务器地址和设备名称（如果可行）标识。

重要信息

您必须先选择要监控的客户，然后才能显示 C&C 回调检测数据。

您可以单击其中一个客户选择链接来选择要监控的客户。在随即出现的**小组件设置**屏幕上，您可以选择要监控的客户、更改小组件的名称以及选择要显示的排名靠前的设备数量。

单击 **C&C 回调检测**计数以查看事件日志，或单击**客户**名称以打开**客户 > [客户]** 窗口。单击**选择其他客户**链接可选择新客户。

Hosted Email Security 小组件

控制台中显示以下 Hosted Email Security 小组件：

具有最多隔离邮件的 Hosted Email Security 客户

显示具有最多隔离邮件的 Hosted Email Security 客户。数据显示在表格和饼图中。单击显示图标 ( ) 即可在表格和饼图之间切换。

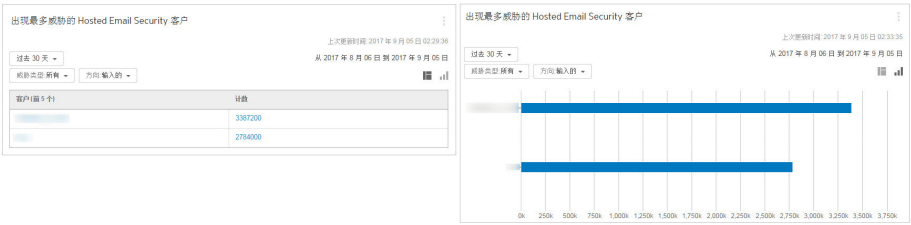
- 您可以更改数据显示的时间范围，具体选项有：
  - 过去 24 小时

- 过去 7 天
- 过去 30 天（缺省）

- 您可以更改数据显示的方向类型，具体选项有：
  - 输入的
  - 传出
- 单击客户名称即可查看客户信息。
- 单击邮件计数可查看事件日志。

出现最多威胁的 Hosted Email Security 客户

显示出现威胁事件数最多的 Hosted Email Security 客户。数据显示在表格和饼图中。单击显示图标 ( ) 即可在表格和饼图之间切换。



- 您可以更改数据显示的时间范围，具体选项有：
  - 过去 24 小时
  - 过去 7 天
  - 过去 30 天（缺省）
- 您可以更改数据显示的威胁类型，具体选项有：
  - 垃圾邮件

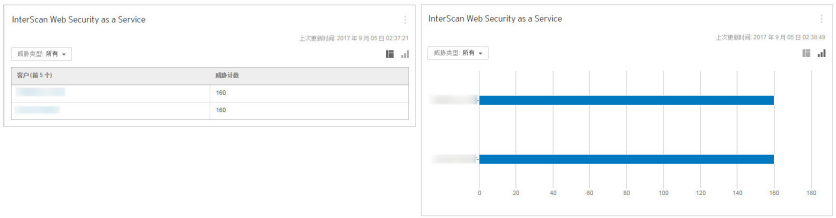
  - 病毒
  - 全部（缺省）
- 您可以更改数据显示的方向类型，具体选项有：
  - 输入的
  - 传出
- 单击客户名称即可查看客户信息。
- 单击威胁计数可查看事件日志。

InterScan Web Security as a Service 小组件

控制台中显示以下 InterScan Web Security as a Service 小组件：

InterScan Web Security as a Service 小组件

显示出现威胁事件最多的 InterScan Web Security as a Service (IWSaaS) 客户。数据显示在表格和饼图中。单击显示图标 ( ) 即可在表格和饼图之间切换。



- 您可以更改数据显示的威胁类型，具体选项有：

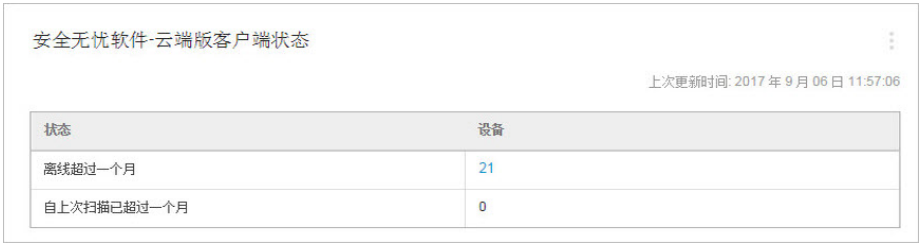
- 所有
- 防间谍软件
- 防病毒
- 应用程序控制
- URL 过滤
- Web 信誉

- 单击客户名称即可查看客户信息。

安全无忧软件-云端版小组件

控制台中显示以下安全无忧软件-云端版小组件：

安全无忧软件-云端版客户端状态



此小组件显示已脱机或无法完成扫描长达一个多月之久的安全无忧软件-云端版设备。

注意

设备计数仅包括已启用预设扫描设置的安全无忧软件-云端版客户端数。

单击任意一项设备计数以查看事件日志。

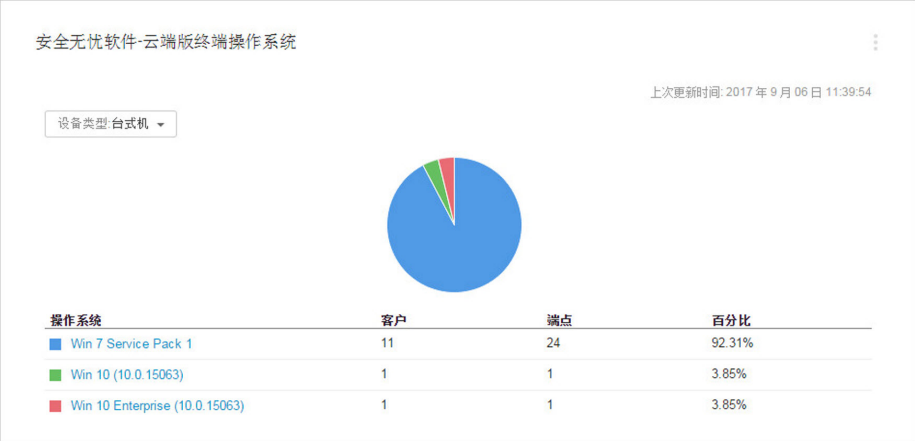
出现最多威胁的安全无忧软件-云端版客户小组件

此小组件显示出现最多威胁事件的安全无忧软件-云端版客户。

要切换视图，请单击右上角的表格图标或条形图图标 ( )。

查看	选项
表	• 单击**客户**名称以打开**客户 > [客户]** 窗口。
条形图	• 将鼠标悬停在长条上以查看该特定客户和产品的检测结果数。 • 单击任意一个长条以查看事件日志。

安全无忧软件-云端版终端操作系统



此小组件显示安全无忧软件-云端版终端上使用的操作系统。

- 通过选择以下选项更改所显示的数据设备类型：
  - 台式机
  - 服务器
  - 移动设备
- 单击表格或饼图中的操作系统版本，以查看事件日志。

通知中心

通知中心可以提供识别具有“需要采取处理措施”事件和“警告”事件的客户的快速方式。

通过**具有通知的客户**小组件访问**通知中心**。

有关更多信息，请参阅“具有通知的客户”小组件 第 14-7 页。

下表概述了**通知中心**窗口上**需要采取处理措施**和**警告**选项卡可用的选项。

选项	描述
全部导出	单击可导出包含与具有事件的客户相关的所有数据的 CSV 文件。
清除	在终端上采用手动处理措施解决受管产品无法直接解决的问题后清除通知。 选择受支持的受管产品的一个或多个事件，然后单击**清除**可从**通知中心**、相关的远程管理器小组件以及以下受管产品控制台（如果适用）删除相关事件数据： • 安全无忧软件 • 安全无忧软件-云端版 **注意** 清除事件并不会删除任何与事件相关的日志数据。远程管理器只会清除事件通知信息。
配置通知	单击可打开**管理 > 配置通知**窗口，然后在远程管理器中配置全局通知设置。 有关更多信息，请参阅配置全局通知设置 第 17-3 页。
类型	选择表中显示的事件的类型。 • **所有**：显示所有事件类型的通知 • **使用授权**：仅显示使用授权通知 • **系统**：仅显示系统通知 • **威胁**：仅显示威胁通知
公司	单击表格中的**公司**名称即可打开**客户 > [客户]** 窗口，然后查看与特定客户相关的所有事件。 有关更多信息，请参阅客户产品 第 3-3 页。

选项	描述
出现次数	单击**出现次数**计数即可查看特定事件的详细信息。 根据受管产品，事件详细信息如下显示： • 安全无忧软件（网络安全版或邮件与网络安全版）：此时会显示弹出窗口，列出特定事件所有出现次数的详细信息 • 安全无忧软件-云端版:此时会显示**事件详情**窗口，显示有关事件和建议的解决方案处理措施的其他信息。 有关更多信息，请参阅事件详情 第 14-34 页。 • 所有其他受管产品：远程管理器会打开受管产品控制台，您可以在其中找到有关事件的更多信息。

事件详情

事件详情窗口可让您更详细地查看影响安全无忧软件-云端版客户的威胁事件和系统事件。

下表概述了**事件详情**窗口中提供的信息。

信息	描述
事件类型	显示以下事件类型的图标和描述： • 需要采取处理措施 • 警告
事件类别	介绍显示的特定事件和子类别
描述	介绍与事件通知相关的问题和任何阈值设置
建议的处理措施	针对受管产品无法直接解决的事件提供建议

信息	描述
处理措施按钮	可用的处理措施因特定事件而异 可能的处理措施包括： • **清除通知**：在终端上采用手动处理措施解决受管产品无法直接解决的问题后清除通知。 清除事件通知后，远程管理器会从**通知中心**、相关的远程管理器小组件以及安全无忧软件-云端版控制台删除相关事件数据。 **注意** 清除事件不会删除与事件相关的任何日志数据。远程管理器仅清除事件通知信息。 • **下载工具**：如果其他趋势科技工具可以帮助解决安全威胁，请单击获取软件包。 **注意** 您必须在受影响的终端上手动运行此工具才能解决安全威胁。 • **启用实时扫描**：单击即可在受影响的终端上自动启用“实时扫描”服务。 • **更新安全客户端**：单击即可在受影响且已过时的终端上触发更新过程。
受影响的终端列表	显示受影响的终端列表以及与事件类别关联的特定事件数据

事件日志

单击控制台上显示的各类小组件上的计数后，系统会显示**事件日志**窗口。事件日志提供了受管产品针对特定客户报告的检测结果的详细视图。

您可以单击**出现次数**计数获取有关特定类型事件的更多信息。根据受管产品，单击**出现次数**计数会执行以下操作：

- 对于安全无忧软件-云端版事件：显示 **WFBSS 日志查询**窗口

  有关更多信息，请参阅执行 WFBS-SVC 日志查询 第 14-36 页。

- 对于安全无忧软件事件：显示已检测到的事件的日志窗口
- 对于所有其他受管产品：打开受管产品控制台，您可以在那里查看受影响客户的产品特定日志

执行 WFBS-SVC 日志查询

您可以查询安全无忧软件-云端版日志，确定不同的事件类型如何影响您所有的远程管理器客户。

过程

1. 转至**主页**。
2. 在任何适用的安全无忧软件-云端版小组件上单击数据链接，打开**事件日志**窗口。
3. 单击任意安全无忧软件-云端版客户的**出现次数**计数。

   此时会显示 **WFBS-SVC 日志查询**窗口，显示与您单击的**出现次数**计数相关的威胁类别的检测信息。
4. （可选）查看其他安全无忧软件-云端版日志数据。
   a. 从**期限**下拉列表中，指定检测数据的日期范围。
   b. 从**类别**下拉列表中，选择可用的威胁类别。如果已选择**勒索软件**类别，请从可用感染途径中选择。
   c. 单击**显示日志**。

      此时会显示所有远程管理器客户的与搜索条件匹配的所有安全无忧软件-云端版日志。
5. （可选）单击**全部导出**可将数据保存为 CSV 文件。

第 15 章

管理事件

本节包含以下主题：

了解事件

远程管理器可以将事件定义为任何需要引起管理员注意的活动。提供的信息因选择的产品和事件类型而异。

远程管理器可提供两种类型的事件列表。

表 15-1. 远程管理器事件列表

列表	描述
事件日志	显示来自小组件的事件列表。 远程管理器根据指定范围显示选择的小组件的事件列表。根据小组件，您可以选择显示过去 24 小时、7 天或 30 天的信息。 有关更多信息，请参阅事件日志 第 14-35 页。
针对特定产品的事件：	显示实时事件列表 远程管理器可以与支持的产品同步，并且每隔 5 分钟刷新一次列表。 **注意** 有关更多信息，请参阅查看针对特定产品的事件 第 14-21 页。

事件严重性

针对特定产品的事件可能具有以下任一严重等级。

- **需要采取操作：**需要马上注意的事件。
- **警告：**作为警告但无需立即注意的通知。

事件状态

针对特定产品的事件可能具有以下任一状态。

- **未解决**：需要引起注意的事件。
- **忽略/立即更新**：已解决但仍需要产品或服务更新的事件。

受管产品事件

远程管理器事件因每个受管产品/服务而异。

- Cloud App Security 事件 第 15-3 页
- Cloud Edge 事件 第 15-4 页
- InterScan Web Security as a Service 事件 第 15-7 页
- 安全无忧软件事件 第 15-7 页
- 安全无忧软件-云端版事件 第 15-10 页

Cloud App Security 事件

注意

如果发生多个“需要采取处理措施”和“警告”事件，远程管理器会针对最严重的威胁显示 图标。

表 15-2. 威胁事件

事件类别	详细信息	事件状态
防病毒	病毒检测超出	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
文件阻止	文件阻止违例超出	：在 1 小时内检测到的文件阻止违例计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
沙盒平台	沙盒平台“高风险”检测超出	：在 1 小时内检测到的沙盒平台“高风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置）
	沙盒平台“中/低等风险”检测超出	：在 1 小时内检测到的沙盒平台“中/低等风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉	URL 违例超出	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 15-3. 系统事件

事件类别	详细信息	事件状态
帐户同步问题	Box 访问令牌无效	：无法访问指定的云存储
	Dropbox 访问令牌无效	：无法访问指定的云存储
	Google 云端硬盘访问令牌无效	：无法访问指定的云存储
	委派帐户上的同步问题	：无法与委派帐户同步

Cloud Edge 事件

注意

Cloud Edge 中的某些威胁事件可能会显示其他渠道信息。

表 15-4. 威胁事件

事件类别	详细信息	事件状态
反垃圾邮件	垃圾邮件检测数	：在过去 1 小时检测到的垃圾邮件计数
防病毒	病毒检测	：在过去 1 小时内检测到的病毒/恶意软件计数
僵尸网络	僵尸网络检测数	：在过去 1 小时检测到的僵尸网络计数
C&C 回调	C&C 回调	：在过去 1 小时内检测到的 C&C 回调计数
IPS	IPS 检测数	：在过去 1 小时检测到的 IPS 计数
预测型机器学习	预测型机器学习检测数	：在过去 1 小时检测到的预测型机器学习计数
勒索软件	勒索软件检测数	：在过去 1 小时内检测到的勒索软件计数
沙盒平台	沙盒平台检测数	：在过去 1 小时内检测到的沙盒平台计数
Web 信誉	URL 违例	：在过去 1 小时内阻止的 URL 计数
Web 威胁	Web 威胁检测数（包括 IPS、僵尸网络、防病毒或 Web 信誉违例）	：在过去 1 小时内检测到的 Web 威胁计数

表 15-5. 系统事件

事件类别	详细信息	事件状态
云电子邮件扫描	服务不可用	：Cloud Edge 无法连接到云扫描服务
	服务在过去 24 小时内暂时不可用	：Cloud Edge 在过去的 24 小时内暂时无法连接到云扫描服务

事件类别	详细信息	事件状态
固件更新	上次固件更新未成功。打开 <Cloud Edge 云控制台>了解详细信息。	：Cloud Edge 固件无法成功更新到最新的固件版本
	固件已过期	：当前版本的 Cloud Edge 固件已过期
脱机	网关脱机。策略部署和日志分析可能会受到影响。	：Cloud Edge 无法连接到网关或执行扫描
脱机 (过去 24 小时)	在过去 24 小时内网关脱机的出现次数。策略部署和日志分析可能已受到影响。	：Cloud Edge 在过去 24 小时内无法保持到所有注册网关的专用连接
资源短缺	检测到 <number> 个问题 • 超出了磁盘空间使用率 • 超出了 CPU 使用率 • 超出了的内存使用率	：设备上剩余的资源量下降到配置的警报阈值以下。
资源短缺（过去 24 小时）	检测到 <number> 个问题 • 超出了磁盘空间使用率 • 超出了 CPU 使用率 • 超出了的内存使用率	：设备上剩余的资源量在过去的 24 小时内下降到配置的警报阈值以下，但已恢复
已取消注册	无法执行云管理。此网关未注册到 Cloud Edge 云控制台。	：Cloud Edge 对网关执行扫描

InterScan Web Security as a Service 事件

表 15-6. 威胁事件

事件类别	详细信息	事件状态
防间谍软件	间谍软件/灰色软件检测	：在过去 24 小时内检测到的间谍软件/灰色软件计数
防病毒	病毒检测	：在过去 24 小时内检测到的病毒/恶意软件计数
应用程序控制	应用程序控制违例	：在过去 24 小时内检测到的应用程序控制违例计数
URL 过滤	URL 违例	：在过去 24 小时内检测到的 URL 过滤违例计数
Web 信誉	URL 违例	：在过去 24 小时内阻止的 URL 计数

表 15-7. 系统事件

事件类别	详细信息	事件状态
帐户同步问题	AD/LDAP 同步问题	：无法与 AD/LDAP 同步

安全无忧软件事件

表 15-8. 威胁事件

事件类别	详细信息	事件状态
反垃圾邮件	在收到的所有邮件中检测到的垃圾邮件数量超出	：在 1 个小时内在收到的所有邮件中检测到的垃圾邮件比率超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
防间谍软件	需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
	间谍软件/灰色软件检测超出	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒	已在终端上禁用实时扫描	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
	已在 Exchange 服务器上禁用实时扫描	：已禁用实时扫描的 Exchange 服务器允许电子邮件中的所有附件通过，这会使客户网络容易感染群发邮件蠕虫病毒。
	未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
	终端上的病毒检测超出	：在 1 小时内在终端上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
	Exchange 服务器上的病毒检测超出	：在 1 小时内在 Exchange 服务器上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控	行为监控违例超出	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
设备控制	设备控制违例超出	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒	网络病毒检测超出	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）
爆发防御	爆发防御已启用	：已在桌面/服务器平台上启用爆发防御来应对异常威胁活动
	爆发防御已禁用	：已在桌面/服务器平台上禁用爆发防御并且已恢复正常的网络条件
URL 过滤	URL 违例超出	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉	URL 违例超出	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 15-9. 系统事件

事件类别	详细信息	事件状态
资源短缺	剩余磁盘空间小于	：服务器上剩余的磁盘空间下降到配置的警报阈值以下。
云安全智能防护服务	服务不可用	：安全无忧软件控制台无法连接到云安全服务器
更新	客户端已过期	：在过去一个小时内，超过 <number> 个安全客户端未收到最新的防病毒特征码
	Exchange 服务器已过期	：在 Exchange 服务器上检测到过期组件

安全无忧软件-云端版事件

表 15-10. 威胁事件

事件类别	详细信息	事件状态
防间谍软件	需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
	间谍软件/灰色软件检测超出	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒	实时扫描已禁用	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
	未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
	病毒检测超出	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
应用程序控制	应用程序控制违例超出	：在 1 小时内检测到的应用程序控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控	行为监控违例超出	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）

事件类别	详细信息	事件状态
设备控制	设备控制违例超出	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒	网络病毒检测超出	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）
爆发防御	爆发防御已启用	：已在桌面/服务器平台上启用爆发防御来应对异常威胁活动
	爆发防御已禁用	：已在桌面/服务器平台上禁用爆发防御并且已恢复正常的网络条件
预测型机器学习	预测型机器学习检测超出	：在 1 小时内检测到的预测型机器学习计数超过了配置的阈值（如受管产品控制台上的配置）
URL 过滤	URL 违例超出	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉	URL 违例超出	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 15-11. 系统事件

事件类别	详细信息	事件状态
云安全智能防护服务	客户端已断开连接	：安全客户端无法连接到云安全智能防护网络
更新	客户端已过期	：在防病毒特征码发布两个小时后具有过期特征码的安全客户端超过了阈值

查看针对特定产品的事件

针对特定产品的事件会显示实时事件的列表。

过程

1. 转至**客户** > **{公司名称}** > **{产品}**。
2. 根据选择的产品，执行以下其中一项操作：

产品	步骤
Cloud App Security	转至**事件**选项卡。
Cloud Edge	转至**事件**选项卡。
InterScan Web Security as a Service	从网络树中选择 IWSaaS 产品后，会自动显示事件列表。
安全无忧软件	转至**事件**选项卡。
安全无忧软件-云端版	转至**事件**选项卡。

第 16 章

管理报表

本节包含以下主题：

报表概述

可以使用趋势科技远程管理器生成、下载和自动发送报表。报表简要概述客户网络中的使用授权状态、评估结果、威胁事件、主要威胁及最受影响的计算机、文件和电子邮件地址。

报表包括来自安全无忧软件（全部版本）和 Hosted Email Security 的一系列统计信息。远程管理器包括报表配置文件、一次性和定期报表、日期范围和多个电子邮件收件人。远程管理器会保存 30 个最新的每日报表、10 个最新的每周报表和 5 个最新的每月报表。常规报表适用于经销商和客户。详细报表适用于经销商和合作伙伴。

图 16-1. 报表页面

通过报表配置文件，可以从单个配置文件创建多份报表。例如，您可以今天创建一份一次性报表，然后生成该报表，而明天只需更改某些选项并重新生成报表即可，无需重新创建整份报表。远程管理器当前支持常规报表和详细报表。

创建报表

趋势科技远程管理器提供了以下方法来创建报表模板：

- 单击现有报表，修改报表，然后单击在窗口底部的**保存**。
- 创建新报表模板。请参阅创建报表模板 第 16-3 页了解更多信息。

创建报表模板

过程

1. 转至**报表** > **新报表**。

此时将打开**新报表**窗口。

2. 指定以下内容：
   - **报表名称**
   - **报表类型**：请参阅“报表概述 第 16-2 页”，以了解详细信息。
3. 选择**日期范围**：
   - **一次性报表**

选项	描述
过去 24 小时	使用从午夜 12 点到生成报表时刻接收到的数据计算报表（基于选择的时区）。 **注意** 报表所依据的时区是销售商在创建配置文件时选择的时区。并不是由客户计算机所决定的。
过去 7 天	使用过去 7 天的数据计算报表（今天的数据除外）。
过去 30 天	使用过去 30 天的数据计算报表（今天的数据除外）。
特定范围	“起始”日期必须晚于或等于上月的第一天（远程管理器仅存储上月和当月的数据）；“终止”日期不能晚于今天。

- **周期性报表**

选项	描述
每日报表	结束日期必须晚于今天。指定时间范围内的每一天都会根据前一天的数据生成报表。 例如，如果时间范围设置为从 2009 年 1 月 27 日到 2009 年 1 月 29 日，则： • 在 27 日，远程管理器将会根据 26 日的数据生成报表 • 在 28 日，远程管理器将会根据 27 日的数据生成报表 • 在 29 日，远程管理器将会根据 28 日的数据生成报表
每周报表	远程管理器会在每周一使用上一周的数据生成每周报表。因此，要为本周生成报表，那么结束日期最早也要设置到下周的周一。
每月报表	远程管理器会在每月的第二天使用上一个月的数据生成每月报表。这意味着要为本月生成报表，结束日期最早也要设置到下月的第二天。

4. 指定以下报表格式元素：

选项	说明
报表格式	报表可以导出为 PDF 或 CSV 文件。
报表语言	趋势科技远程管理器支持英语、法语、德语、意大利语、日语、简体中文和西班牙语。
备注	该信息供内部使用，不会显示在报表上。

5. 单击**下一步**。

   此时会显示**选择报表数据**窗口。

6. 选择报表模板以及要生成的数据。

   注意

   如果经销商未连接到客户的服务器或无数据，则不会显示客户的任何数据。

7. 单击**下一步**。

   此时会显示**为特定客户生成报表**窗口。

8. 选择将生成此报表的客户。

9. 指定电子邮件报表的详细信息。**发送邮件至**选项下的收件人来自公司联系人列表。您还可以添加将收到生成的报表的电子邮件地址。

   注意

   每个选定的客户会有不同的电子邮件收件人。根据客户的不同，您可以添加或删除电子邮件收件人。

10. 可选：选择**启用**，可显示客户的徽标。

11. 单击**完成**

    远程管理器会将模板添加到报表模板列表中。

查看报表

报表必须至少生成一次才能进行查看。

转至**报表** > **{报表名称}** > **报表文件（选项卡）** > **{“查看”下的文件}**。

请参阅“报表概述 第 16-2 页”，以了解详细信息。

编辑报表

转至**报表** > **{报表名称}**。

请参阅“创建报表模板 第 16-3 页”，以了解详细信息。

下载和发送报表

您可以下载报表并将其发送给收件人。尽管您在定义报表时指定了收件人，但仍可以修改收件人列表。

过程

1. 转至**报表** > **{“报表文件”下的项目或项目数}** > **{“查看”下的报表}**。
2. 选择您要发送或下载的报表。
3. 单击**发送**或**下载**。

   请参阅“订阅报表 第 16-8 页”，以了解详细信息。

订阅报表

过程

1. 转至**报表** > **{报表名称}** > **目标受众（选项卡）** > **添加目标**。
2. 选择客户报表。

   注意

   创建报表时所用的电子邮件收件人列表来自“联系人”详细信息。

3. 按照需要修改主题行。
4. 单击 **保存**。

部分 VI

管理远程管理器

第 17 章

管理远程管理器

注意

有关第三方产品集成的信息，请参阅部分 IV：集成第三方解决方案。

本节包含以下主题：

管理设置

您可以使用**管理**窗口配置全局客户设置，远程管理器控制台设置，查看并设置第三方软件集成，以及查看系统日志。

部分	描述
系统设置	• **配置通知**：可让您配置全局通知设置 **提示** 趋势科技建议您以如下的适用于大部分客户的方式配置全局通知设置。尽管您可针对每个客户自定义通知设置，但全局设置是更快速的客户通知配置方式。 有关更多信息，请参阅配置全局通知设置 第 17-3 页。 • **控制台设置**：可让您更改远程管理器控制台上显示的横幅图片。 有关更多信息，请参阅配置控制台设置 第 17-16 页。
第三方集成	• 查看与第三方软件集成的远程管理器功能的当前状态 • **配置第三方集成**：可让您与受支持的第三方软件集成并配置全局集成设置 有关更多信息，请参阅部分 IV：集成第三方解决方案 第 1 页。

部分	描述
产品/服务的缺省设置	**配置缺省设置模板**：可让您配置适用于新客户或现有客户的整个受管产品/服务控制台设置 **提示** 配置模板可以预先配置受管产品的安全策略和例外列表，您稍后可将其应用到多个客户中，从而帮助您节省时间。 **重要信息** 远程管理器仅支持安全无忧软件-云端版和 Cloud Edge 的缺省设置模板。 有关更多信息，请参阅缺省设置模板 第 17-17 页。
系统日志	**管理日志**：显示与用户执行的远程管理器控制台更改相关的信息 有关更多信息，请参阅查看管理日志 第 17-20 页。

配置全局通知设置

设置全局通知可以监控需要关注的常见事件。远程管理器通过电子邮件、在**具有通知的客户**小组件或通过您的第三方软件提供通知。

提示

趋势科技建议您以如下的适用于大部分客户的方式配置全局通知设置。尽管您可针对每个客户自定义通知设置，但全局设置是更快速的客户通知配置方式。

过程

1. 转至**管理**。
2. 在**系统设置**部分中，单击**配置通知**。

   此时会显示**管理 > 配置通知**窗口。

3. 在**电子邮件设置**部分中，指定接收通知电子邮件的**收件人**。

   - **帐户管理器**：为接收所有客户电子邮件通知的主远程管理器管理员选择 Licensing Management 帐户。
   - **其他收件人**：手动键入远程管理器应联系的其他人的电子邮件地址

   注意

   使用分号 (;) 分隔多个条目。

4. 在**电子邮件设置**部分中，指定通知电子邮件中显示的**邮件内容**。

选项	描述	可能的通知
针对所有需要采取处理措施的事件和所有警告事件向所有客户发送单独的合并电子邮件	远程管理器可以合并所有客户的所有需要采取处理措施的事件和所有警告事件，并且会在远程管理器服务器每次与受管产品服务器同步时针对各个严重等级逐一发送包含所有事件摘要的电子邮件。 **注意** 单击**编辑主题前言**可以指定在电子邮件主题行中显示为初始文本的自定义前言。	• 针对所有需要采取处理措施的事件向每个受管产品的所有客户发送的一封合并电子邮件 • 针对所有警告事件向每个受管产品的所有客户发送的一封合并电子邮件 • 针对所有使用授权事件发送的单独的电子邮件（与**通知事件设置**中的配置相同）

选项	描述	可能的通知
针对所有警告事件向所有客户逐一发送合并电子邮件，但针对每个需要采取处理措施的事件向所有客户逐一发送电子邮件	远程管理器可以合并所有客户的所有警告事件并且会在远程管理器服务器每次与受管产品服务器同步时逐一发送包含所有警告事件摘要的电子邮件。远程管理器还会在受管产品每次报告任何客户的需要采取处理措施的事件时发送一封新的电子邮件。 **注意** 单击**编辑警告主题前言**可以指定显示为合并警告事件电子邮件主题行初始文本的自定义前言。	• 针对每个需要采取处理措施的事件向每个客户发送的单独的电子邮件 • 针对所有警告事件向每个受管产品的所有客户发送的一封合并电子邮件 • 针对所有使用授权事件发送的单独的电子邮件（与**通知事件设置**中的配置相同）
针对每个需要采取处理措施事件和警告事件向客户逐一发送电子邮件	远程管理器可以在受管产品每次报告任何客户的警告或需要采取处理措施的事件时发送一封新的电子邮件。	• 针对每个需要采取处理措施的事件向每个客户发送的单独的电子邮件 • 针对每个警告/信息事件向每个客户发送的单独的电子邮件 • 针对所有使用授权事件发送的单独的电子邮件（与**通知事件设置**中的配置相同）

重要信息

选择此选项后，您可以单击**通知事件设置**中的事件名称，为每个安全无忧软件-云端版和 Cloud Edge “警告”和“需要采取处理措施”的事件自定义各个电子邮件内容。

5. 在**语言**下的**电子邮件设置**部分中，选择远程管理器发送电子邮件通知使用的语言。

6. 在**每日通知摘要**下的**电子邮件设置**部分中，启用**发送每日通知摘要**选项可以接收每日电子邮件报告，该报告总结了每天所有客户的所有**使用授权事件**、**系统事件**和**威胁事件**。

提示

单击**查看示例**链接可以显示远程管理器发送的饼图和表格数据预览。

7. 在**通知事件设置**部分中，配置远程管理器如何针对特定产品和事件类型发送通知。

   - 通用设置：
     - **在通知中显示**：选择该复选框可以在**具有通知的客户**小组件和**通知中心**窗口中显示通知事件
     - **电子邮件**：选择该复选框可以使远程管理器在发生事件的任何时候发送一封电子邮件（基于**邮件内容**设置）
     - **警报阈值**：如果可用，请指定事件的阈值设置

     注意

     使用每个客户的安全无忧软件-云端版 Web 控制台为安全无忧软件-云端版配置阈值设置。

   - 通知产品和事件类型：每个产品和事件类型的通知事件各不相同。请参考以下列表获取每个部分的特定信息：

部分	描述
所有使用授权事件	从提供的列表中选择要监控的特定事件类型。 **注意** 远程管理器向所有客户发送包含所有授权通知的单独的合并电子邮件。 有关通知事件的详细信息，请参阅使用授权通知 第 17-10 页。

部分	描述
安全无忧软件-云端版	从提供的列表中选择要监控的特定事件类型。 有关通知事件的详细信息，请参阅安全无忧软件-云端版通知 第 17-10 页。 **重要信息** 启用**请勿从受管产品中向远程管理器收件人发送通知**以减少收件人在**电子邮件设置**的**收件人**部分中指定的重复电子邮件数量。远程管理器会比较**电子邮件设置**中的收件人与在安全无忧软件-云端版控制台为每个客户配置的收件人。对于两个列表中都显示的电子邮件地址，远程管理器会阻止安全无忧软件-云端版向重复的电子邮件地址发送通知。 **提示** 如果在**邮件内容**部分中选择针对“警告”或“需要采取处理措施”的事件逐一接收电子邮件，您可以单击事件名称自定义电子邮件内容。 有关更多信息，请参阅自定义电子邮件通知内容 第 17-8 页。
安全无忧软件	您仅可以选择是否基于**威胁**和**系统**事件类型接收通知。 有关通知事件的详细信息，请参阅安全无忧软件通知 第 17-12 页。
Cloud App Security	您仅可以选择是否基于**威胁**和**系统**事件类型接收通知。 有关通知事件的详细信息，请参阅Cloud App Security 通知 第 17-14 页。

部分	描述
Cloud Edge	从提供的列表中选择要监控的特定事件类型。 有关通知事件的详细信息，请参阅 Cloud Edge 通知 第 17-15 页。 **重要信息** 对于“信息”事件类型，远程管理器会根据**邮件内容**部分中配置的“警告”事件设置发送通知。 **提示** 如果在**邮件内容**部分中选择针对“警告”或“需要采取处理措施”的事件逐一接收电子邮件，您可以单击事件名称自定义电子邮件内容。 有关更多信息，请参阅自定义电子邮件通知内容 第 17-8 页。
InterScan Web Security as a Service	您仅可以选择是否基于**系统**事件类型接收通知。 有关通知事件的详细信息，请参阅 InterScan Web Security as a Service 通知 第 17-16 页。

8. 单击**保存**。

注意

您可以单击**恢复缺省值**将所有全局通知设置恢复为缺省配置。

自定义电子邮件通知内容

如果在**邮件内容**部分中选择针对“警告”或“需要采取处理措施”的事件逐一接收电子邮件，您可以单击事件名称自定义电子邮件内容。

有关更多信息，请参阅配置全局通知设置 第 17-3 页。

重要信息

自定义电子邮件模板仅适用于安全无忧软件-云端版和 Cloud Edge 事件。

提示

单击**预览示例**链接可先了解通知邮件的布局，然后再开始自定义通知内容。

过程

1. 在**主题**字段中：
   - 拖放**变量列表**中的字段以添加动态更新的数据。

     重要信息

     仅在使用 Chrome 或 Firefox 浏览器时才可以使用拖放功能。
   - 手动键入静态文本，以提高可读性。
2. 在**内容**字段中：
   - 拖放**变量列表**列表中的字段以添加动态更新的数据。
   - 手动键入静态文本，以提高可读性。
   - 使用可用的编辑工具栏按钮可格式化邮件内容。
3. 单击**保存**。

使用授权通知

事件	频率	警报阈值
使用授权 — 即将过期	选择以下其中一项： • **每 7 天**：系统从到期前 14 天开始，每 7 天发送一次电子邮件通知。 • **每 14 天**：系统从到期前 28 天开始，每 14 天发送一次电子邮件通知。 • **每 30 天**：系统从到期前 60 天开始，每 30 天发送一次电子邮件通知。	远程管理器会根据以下**频率**设置显示**警报阈值**： • **每 7 天**：使用授权将在 14 天后到期 • **每 14 天**：使用授权将在 28 天后到期 • **每 30 天**：使用授权将在 60 天后到期
使用授权 — 已过期	按事件 当有已到期的使用授权时发送通知	不适用
使用授权 — 分配已超限	按事件 当已使用的座席数超过提供的座席数一定百分比时发送通知	分配超限 (%)：<数量> **注意** 您可以指定已使用的座席数超出客户获得的座席数的百分比。这个百分比可以是介于 100 到 120 之间的任何值。

安全无忧软件-云端版通知

重要信息

对于具有可配置的阈值的事件，必须在安全无忧软件-云端版控制台上分别为每个客户配置阈值。

表 17-1. 威胁事件

事件	详细信息
防病毒 — 未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
防病毒 — 实时扫描已禁用	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染
防病毒 — 病毒检测超过	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
防间谍软件 — 需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
防间谍软件 — 间谍软件/灰色软件检测超过	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉 — URL 违例超过	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）
URL 过滤 — URL 违例超过	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
预测型机器学习 — 预测型机器学习检测超过	：在 1 小时内检测到的预测型机器学习计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控 — 行为监控违例超过	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒 — 网络病毒检测超过	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）

事件	详细信息
设备控制 — 设备控制违例超过	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
应用程序控制 — 应用程序控制违例超过	：在 1 小时内检测到的应用程序控制违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 17-2. 系统事件

事件	详细信息
更新 — 过期的客户端	：在防病毒特征码发布两个小时后具有过期特征码的安全客户端超过了阈值
云安全智能防护服务 — 客户端已断开连接	：安全客户端无法连接到云安全智能防护网络

安全无忧软件通知

表 17-3. 威胁事件

事件	详细信息
反垃圾邮件 — 在收到的所有邮件中检测到的垃圾邮件数量超出	：在 1 个小时内在收到的所有邮件中检测到的垃圾邮件比率超过了配置的阈值（如受管产品控制台上的配置）
防间谍软件 — 需要重新启动设备的检测	：显示受管产品无法完全清除且需要客户重启终端才能完成这一过程的受间谍软件/灰色软件感染的终端的数量
防间谍软件 — 间谍软件/灰色软件检测超过	：在 1 小时内检测到的间谍软件/灰色软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒 — 已在终端上禁用实时扫描	：已禁用实时扫描的安全客户端无法保护终端免受新创建或执行的文件中的病毒/恶意软件感染

事件	详细信息
防病毒 — 已在 Exchange 服务器上禁用实时扫描	：已禁用实时扫描的 Exchange 服务器允许电子邮件中的所有附件通过，这会使客户网络容易感染群发邮件蠕虫病毒。
防病毒 — 未处理的威胁	：处理措施不成功表示病毒或恶意软件已成功绕开病毒防护，并已感染其他终端。 **注意** 远程管理器假设带有未成功清除、隔离或删除病毒或恶意软件的计算机已受到感染。
防病毒 — 终端上的病毒检测超出	：在 1 小时内在终端上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
防病毒 — Exchange 服务器上的病毒检测超出	：在 1 小时内在 Exchange 服务器上检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
行为监控 — 行为监控违例超过	：在 1 小时内检测到的行为监控违例计数超过了配置的阈值（如受管产品控制台上的配置）
设备控制 — 设备控制违例超过	：在 1 小时内检测到的设备控制违例计数超过了配置的阈值（如受管产品控制台上的配置）
网络病毒 — 网络病毒检测超过	：在 1 小时内检测到的网络病毒计数超过了配置的阈值（如受管产品控制台上的配置）
URL 过滤 — URL 违例超过	：在 1 小时内检测到的 URL 过滤违例计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉 — URL 违例超过	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 17-4. 系统事件

事件	详细信息
资源短缺 — 剩余磁盘空间小于	：服务器上剩余的磁盘空间下降到配置的警报阈值以下。
云安全智能防护服务 — 服务不可用	：安全无忧软件控制台无法连接到云安全服务器
更新 — Exchange 服务器已过期	：在 Exchange 服务器上检测到过期组件
更新 — 过期的客户端	：在过去一个小时内，超过 <number> 个安全客户端未收到最新的防病毒特征码

Cloud App Security 通知

表 17-5. 威胁事件

事件	详细信息
防病毒 — 病毒检测超过	：在 1 小时内检测到的病毒/恶意软件计数超过了配置的阈值（如受管产品控制台上的配置）
文件阻止 — 文件阻止违例超出	：在 1 小时内检测到的文件阻止违例计数超过了配置的阈值（如受管产品控制台上的配置）
勒索软件 — 勒索软件检测超出	：在 1 小时内检测到的勒索软件计数超过了配置的阈值（如受管产品控制台上的配置）
沙盒平台 — 沙盒平台检测超出	：在 1 小时内检测到的沙盒平台“低风险”或“中等风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置） ：在 1 小时内检测到的沙盒平台“高风险”对象的检测计数超过了配置的阈值（如受管产品控制台上的配置）
Web 信誉 — URL 违例超过	：在 1 小时内检测到的 Web 信誉违例计数超过了配置的阈值（如受管产品控制台上的配置）

表 17-6. 系统事件

事件	详细信息
帐户同步问题 — Box 访问令牌无效	：无法访问指定的云存储
帐户同步问题 — Dropbox 访问令牌无效	：无法访问指定的云存储
帐户同步问题 — Google 云端硬盘访问令牌无效	：无法访问指定的云存储
帐户同步问题 — 委派帐户上的同步问题	：无法与委派帐户同步

Cloud Edge 通知

表 17-7. 威胁事件

事件	详细信息	警报阈值
Web 威胁 — Web 威胁检测超出	：在 1 小时内检测到的 Web 威胁计数超过了配置的阈值（如远程管理器控制台上的配置）	指定介于 1 到 300 之间的值。
C&C 回调 — C&C 回调检测超出	：在 1 小时内检测到的 C&C 回调计数超过了配置的阈值（如远程管理器控制台上的配置）	指定介于 1 到 100 之间的值。
勒索软件 — 勒索软件检测超出	：在 1 小时内检测到的勒索软件计数超过了配置的阈值（如远程管理器控制台上的配置）	指定介于 1 到 100 之间的值。

表 17-8. 系统事件

事件	详细信息	警报阈值
脱机 — 检测到脱机网关	：Cloud Edge 无法连接到网关或执行扫描	指定远程管理器何时发送通知： • **立即**：在 Cloud Edge 向远程管理器 报告事件时立即触发通知 • **超过 X 天**：如果网关在配置的天数内一直保持脱机状态，则触发通知
脱机 — 脱机设备恢复	：Cloud Edge 恢复到脱机设备的连接	不适用
云电子邮件扫描 — 服务不可用	：Cloud Edge 无法连接到云扫描服务	不适用
云电子邮件扫描 — 服务已恢复	：Cloud Edge 与云扫描服务的连接已恢复	不适用
资源短缺 — CPU、内存或磁盘使用率超出	：设备上剩余的资源量下降到配置的警报阈值以下。	在远程管理器触发通知之前，指定可以使用的最大数量的资源（介于 80% 到 95% 之间）

InterScan Web Security as a Service 通知

表 17-9. 系统事件

事件	详细信息
帐户同步问题 — AD/LDAP 同步问题	：无法与 AD/LDAP 同步

配置控制台设置

控制台设置确定客户在横幅中看到的徽标和非活动用户的自动超时频率。

过程

1. 单击**管理** > **控制台设置**。
2. 选择您要在横幅中使用的图片。

   重要信息

   徽标必须是 .png、.jpg、.bmp 或 .gif 图片，建议尺寸为 600（宽）x 60（高）。

3. 选择**会话超时**频率，远程管理器将按照该频率自动注销非活动的用户。
4. 单击 **保存**。

缺省设置模板

缺省设置模板包含特定客户或组的预先配置。这些模板仅适用于安全无忧软件-云端版和 Cloud Edge，而且前提是趋势科技远程管理器与 Licensing Management Platform 集成。

趋势科技远程管理器提供的控制台与安全无忧软件-云端版和 Cloud Edge 控制台类似，用于进行模板配置。在模板配置控制台上配置的设置不会影响注册的产品。

有关配置设置的更多信息，请参阅产品文档。

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

http://docs.trendmicro.com/en-us/smb/cloud-edge.aspx

为安全无忧软件-云端版配置缺省设置模板

仅当趋势科技远程管理器与 Licensing Management Platform 集成后才可使用缺省设置模板。

有关配置设置的更多信息，请参阅产品文档。

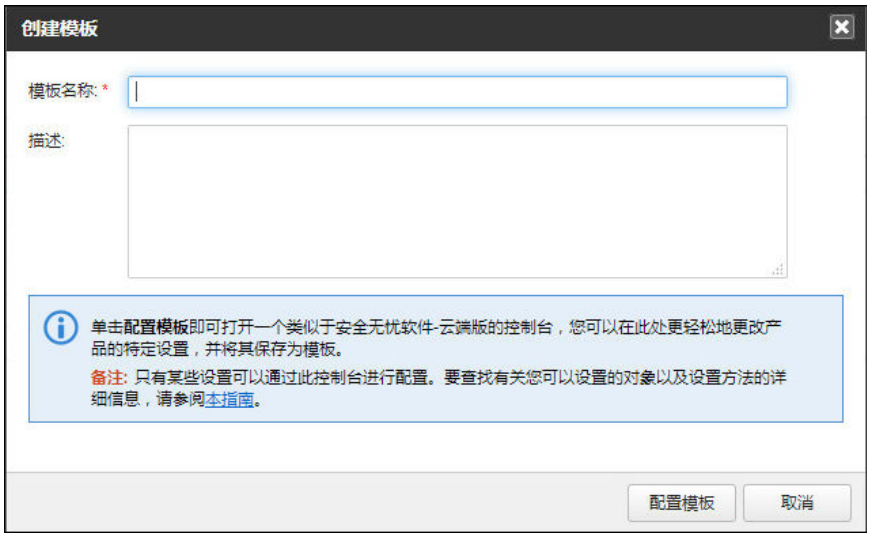
http://docs.trendmicro.com/zh-cn/smb/worry-free-business-security-services.aspx

过程

1. 转至**管理** > **配置缺省设置模板**。

   此时会显示**配置缺省设置模板**窗口。

2. 在**安全无忧软件-云端版**下，单击**创建**。



3. 键入模板的名称和说明。

4. 单击**配置模板**。

   此时，屏幕上会打开一个与安全无忧软件-云端版控制台类似的控制台。

   重要信息

   在此控制台上配置的设置不会影响注册的产品。

5. 配置所需的设置。

重要信息

配置以下任何设置之后，确保单击**保存**以将更改应用到每个窗口。

设置	位置
策略	• 对于服务器平台：**设备** > **服务器（缺省）** > **配置策略** • 对于桌面平台：**设备** > **设备（缺省）** > **配置策略**
扫描设置	• **扫描** > **手动扫描（选项卡）** • **扫描** > **预设扫描（选项卡）** • **扫描** > **漏洞扫描（选项卡）**
通知设置	• **管理** > **通知（选项卡）**
全局设置	• **管理** > **全局设置** > **安全设置（选项卡）** • **管理** > **全局设置** > **允许/阻止的设置（选项卡）** • **管理** > **全局设置** > **客户端控制（选项卡）** • **管理** > **全局设置** > **设备管理（选项卡）**

6. 单击**完成**以保存模板设置。

为 Cloud Edge 配置缺省设置模板

仅当趋势科技远程管理器与 Licensing Management Platform 集成后才可使用缺省设置模板。

有关配置设置的更多信息，请参阅产品文档。

http://docs.trendmicro.com/en-us/smb/cloud-edge.aspx

过程

1. 转至**管理** > **配置缺省设置模板**。

此时会显示**配置缺省设置模板**窗口。

2. 在 **Cloud Edge** 下，单击**创建**。

   此时会打开**创建模板**窗口。

3. 键入模板的名称和说明。

4. 单击**配置模板**。

   此时会打开一个与 Cloud Edge 云控制台类似的控制台。

   注意

   在此控制台上配置的设置不会影响注册的产品。

5. 配置所需的设置，然后单击**保存**。

6. 单击**完成**以保存模板设置。

查看管理日志

管理日志中列出了远程管理器管理员执行的操作。

过程

1. 转至**管理** > **系统日志**。

2. 单击**管理日志**。

3. 使用下拉列表或通过日历指定日期，来指定日期范围。

4. 单击**显示日志**。

   管理日志表随即显示。

5. 有关策略部署日志，请单击**描述**列中的链接以查看有关成功或未成功策略部署操作的详细信息。

部分 VII

获取帮助

第 18 章

故障排除和常见问题解答

本节包含以下主题：

故障排除

如果您在使用远程管理器时遇到问题，请尝试找到以下问题的解决方案步骤：

趋势科技远程管理器 Web 控制台问题

下列主题介绍了与趋势科技远程管理器 Web 控制台相关的故障排除信息：

无法访问

用户无法登录趋势科技远程管理器。

解决方案

可能有两种原因会导致此问题：

- 在浏览器上禁用了 JavaScript。远程管理器要求启用此选项。有关说明，请参阅浏览器的文档。
- 配置文件尚未同步。如果您刚刚在 Trend Micro Licensing Management Platform 上注册，那可能暂时无法登录。请稍等几分钟，让信息同步。

状态图标不一致

在收集数据的初始阶段（在服务器中注册客户端之后），远程管理器显示的防病毒和反垃圾邮件状态图标可能与显示的病毒数和垃圾邮件事件数不一致。

在服务器中注册客户端后，客户端将传输来自安全无忧软件（全部版本）的当前防病毒和反垃圾邮件状态，但是，并不传输这些状态所基于的历史数据。因此，可能会出现显示红色状态符号，但没有事件的情况。

解决方案

一旦安全无忧软件（全部版本）检测到事件，远程管理器即显示正确的图标和数据。

树中的节点无法展开

单击域树上的某个节点时，如果无法展开该节点（**客户**选项卡下），则说明安全无忧软件服务器和趋势科技远程管理器服务器上的组和客户端信息可能不同步。

要解决此问题，请执行以下操作：

1. 转至**客户** > **[客户]**窗口。
2. 将鼠标悬停在未展开的**产品**选项卡上的节点上。
3. 单击**设置**图标 ()。
4. 单击**同步**。

   趋势科技远程管理器可以指示安全无忧软件服务器重新发送组信息。

无法显示页面

尝试打开趋势科技远程管理器服务器 URL 时，显示**页面无法显示**。如果存在以下情况，则会发生此错误：

- URL 不正确。

- 趋势科技远程管理器服务器的 URL 不是 Internet Explorer 的可信站点。

解决方案

1. 确保趋势科技远程管理器服务器的 URL 是 Internet Explorer 的可信站点。
   a. 打开 Internet Explorer。
   b. 单击**工具** > **Internet 选项** > **安全** > **可信站点** > **站点**。
   c. 检查趋势科技远程管理器服务器 URL 是否在列表中。如果没有，请键入此 URL，然后单击**确定**。

客户端问题

一旦将鼠标移到系统托盘图标上，即会显示一则状态消息，指示客户端是否在正常运行。

表 18-1. 客户端系统托盘图标所显示的状态消息

消息	描述
遇到了未知错误。请检查系统或重新启动客户端。	遇到了未知错误。请检查系统或重新启动客户端。 意外错误（通常是系统错误）阻止客户端正常运行。 解决方案： 检查托管服务器是否存在内存不足或其他系统问题。
无法在远程服务器中注册。	您提供的 GUID 可能不正确，或者可能存在网络问题。 解决方案 有两种情况可能导致此问题： • 确认您是否使用了正确的 GUID。请参阅客户端 GUID 或授权密钥 第 8-2 页，在远程管理器 Web 控制台找到正确的 GUID。 • 如果网络存在问题，客户端将无法连接到服务器。检查安全无忧软件（网络安全版和邮件与网络安全版）服务器和趋势科技远程管理器服务器之间的网络连接。

消息	描述
无法连接到远程服务器。	托管服务器可能遇到 Internet 连接问题。 解决方案 检查托管服务器上的 Internet 连接。另外，检查客户端的代理设置以及指定的服务器地址和端口。
客户端已通过远程管理器禁用。	已通过远程管理器 Web 控制台临时禁用了客户端。 解决方案 通过远程管理器 Web 控制台启用客户端。
客户端与客户端服务器邮件安全 (CSM) 不匹配。	客户端服务器或客户端服务器邮件安全版与客户端版本不一致。 解决方案 将客户端服务器或客户端服务器邮件安全版服务器升级到最新版本，然后安装最新的客户端。
客户端服务已停止。	客户端已从远程管理器注销。 解决方案 启动客户端服务，方法是右键单击客户端系统托盘图标并单击**启动服务**。
无法加载组件。您可能需要重新安装客户端。	客户端在加载某些组件时遇到了问题。 解决方案 请首先尝试重新启动客户端服务，方法是右键单击客户端系统托盘图标，然后单击**重新启动服务**或**启动服务**。如果不起作用，请卸载客户端，然后重新安装。确保您使用的是同一 GUID。

受管产品或第三方软件的连接问题

- 与 Hosted Email Security 相关的连接问题 第 18-6 页
- 无法连接到 ConnectWise 客户 第 18-6 页

与 Hosted Email Security 相关的连接问题

如果您无法连接或断开 Hosted Email Security，页面底部可能会显示以下任何消息：

消息	解决方案
无法连接到远程管理器服务器。请检查网络连接和远程管理器的状态。	请再次检查网络连接和远程管理器的状态。
授权码无效	验证 GUID。如果 GUID 有误，请删除客户端并重新尝试连接。
授权码重复	验证 GUID。如果 GUID 有误，请删除客户端并重新尝试连接。
无法连接到远程管理器远程管理器服务器。请检查网络连接和远程管理器服务器状态。	请再次检查网络连接和远程管理器的状态。
服务器内部错误	与您的技术支持提供商联系。

无法连接到 ConnectWise 客户

远程管理器无法在 ConnectWise 服务器中发生公司 ID 更新后连接到 ConnectWise 客户信息。

要解决此问题，请执行以下操作：

在 ConnectWise 中的“远程管理器客户”窗口中，更新为新的公司 ID。

常见问题解答

以下部分概述了与远程管理器配置相关的常见问题：

- Web 控制台常见问题 第 18-7 页
- 全面强化勒索软件防护常见问题解答 第 18-11 页

Web 控制台常见问题

对我的客户许可门户帐户执行的更改需要多久才能显示在“我的帐户”窗口中？

更改您的客户许可门户帐户信息后，系统需要 2 个小时的时间与远程管理器 Web 控制台同步所做的更改。

更新设置后，远程管理器控制台为何不显示已更新状态？

在服务间同步数据需要花费几分钟时间。更改延迟的一些例子包括更新使用授权或席位、重置计数器等。

我在尝试打开安全无忧软件-云端版控制台时为何收到登录错误？

如果安全无忧软件-云端版已关闭以进行维护，或者 Licensing Management Platform 有问题，就会发生此情况。请稍等片刻，然后再尝试重新访问控制台。

在 Licensing Management Platform 创建新客户后，为什么远程管理器中不显示此客户？

在服务间同步数据需要花费几分钟时间。

如何将新产品添加到现有远程管理器客户帐户？

向现有远程管理器客户帐户添加产品的方法因您使用的趋势科技帐户类型而异。

- Licensing Management Platform 帐户：您可以直接从远程管理器 Web 控制台向现有远程管理器客户帐户添加新产品。

  有关更多信息，请参阅使用 Licensing Management Platform 帐户添加新产品 第 3-8 页。

- 联机注册门户帐户：您只能通过接收受管产品的授权码并在受管产品控制台注册产品向现有远程管理器客户添加安全无忧软件、安全无忧软件-云端版和 Hosted Email Security 产品。

  有关更多信息，请参阅使用客户许可门户帐户添加新产品 第 3-11 页。

如何远程管理器访问受管产品控制台？

在远程管理器 Web 控制台上，转至**客户** > **[客户]** > **产品**，然后单击树视图中的产品名称。

在表格的右上角，将显示**打开控制台**链接。单击此链接即可打开受管产品控制台。

远程管理器是否支持基于角色的管理？

否。远程管理器仅支持使功能完备的管理帐户。

远程管理器中的 Licensing Management Platform 帐户和客户许可门户帐户有什么区别？

下表概述了远程管理器在使用不同帐户类型时的功能差别。

功能	LICENSING MANAGEMENT PLATFORM 帐户	客户许可门户帐户
客户管理 — 删除客户	不支持	支持
产品管理 — 删除产品	不支持	支持
产品描述 — 编辑	不支持	支持
支持的产品	• Cloud App Security • Cloud Edge • Hosted Email Security • InterScan Web Security as a Service • 安全无忧软件（网络安全版和邮件与网络安全版） • 安全无忧软件-云端版	• Hosted Email Security • 安全无忧软件（网络安全版和邮件与网络安全版） • 安全无忧软件-云端版

功能	LICENSING MANAGEMENT PLATFORM 帐户	客户许可门户帐户
第三方插件支持	• Autotask • ConnectWise Automate • ConnectWise Manage • Kaseya	• Autotask • ConnectWise Manage
模板管理	支持： • Cloud Edge • 安全无忧软件-云端版	不支持
模板分配给新客户	支持： • Cloud Edge • 安全无忧软件-云端版	不支持
模板分配给现有客户	支持： • Cloud Edge • 安全无忧软件-云端版	不支持
我的帐户信息	不支持	支持
产品注册到远程管理器	支持通过服务计划分配自动注册	需要授权码
合并 OLR 帐户	支持	不适用
Licensing Management Platform 访问	支持	不支持
长 Beta 版	支持	不支持
许可证续订和座席分配	支持	不支持

全面强化勒索软件防护常见问题解答

单击主页窗口上的全面强化勒索软件防护按钮会发生什么情况？

此时会显示**针对所有客户全面强化安全无忧软件-云端版的勒索软件防护**窗口。

单击**启用全部**会针对除“服务器 (缺省)”组以外的所有组的所有客户启用以下功能：

- 行为监控
  - 勒索软件防护
- Web 信誉
- 新遇到的程序检测

如何验证是否已启用所有与勒索软件相关的设置？

可以在**客户**窗口的**安全设置**选项卡中验证是否已启用所有与勒索软件相关的设置。

重要信息

您可以打开安全无忧软件-云端版控制台，仅验证是否已启用新遇到的程序检测功能。

过程

1. 转至**客户** > **{公司}**。

   此时会显示 {公司} 窗口。

2. 在**产品**选项卡上，展开产品树中的安全无忧软件-云端版产品计划。

3. 选择**设备（缺省）**。

   此时会显示**设备**和**安全设置**选项卡。

4. 单击**安全设置**选项卡。

此时会显示以下窗口：


设备
安全设置
扫描方法
云安全扫描
传统扫描
防病毒/防间谍软件
启用实时防病毒/防间谍软件
防火墙
启用防火墙
简单模式: 启用防火墙，且使用趋势科技缺省设置
高级模式: 配置安全等级、IDS、通知和例外。
Web 信誉
启用 Web 信誉
高
中
低 (缺省设置)
URL 过滤
启用 URL 过滤
高
中
低
定制
行为监控
启用行为监控
启用所有勒索软件防护功能
启用 Intuit™ QuickBooks™ 保护
邮件扫描
启用对 POP3 邮件的实时扫描
保存
取消

5. 在 **Web 信誉**下，验证是否已启用了以下功能：
   - **启用 Web 信誉**
6. 在**行为监控**下，验证是否已启用了以下功能：
   - **启用行为监控**
   - **启用所有勒索软件防护功能**
7. 单击**保存**。

   客户端收到通知进行更改。

启用勒索软件防护有何风险？

启用勒索软件防护功能可能会带来以下风险：

- 启用行为监控和勒索软件防护可能会造成一些与某些应用程序的兼容性问题。

  要解决此问题，请将这些应用程序添加到“例外”列表中，或者禁用行为监控和勒索软件防护。

  如果问题依然存在，请与您的技术支持提供商联系。
- 启用勒索软件防护的自动备份功能需要 100MB 的额外存储空间。
- 启用程序检查有助于检测可能危及安全的可执行文件并提高总体检测比率，但可能会降低系统性能。

Hosted Email Security 常见问题

为什么实时状态中未显示最近 3 小时内的数据？

在 Hosted Email Security 服务器上，数据收集的周期为 2 小时。为确保远程管理器服务器获得来自 Hosted Email Security 服务器的完整数据，数据收集会延迟 3 个小时。

为什么右键单击客户树上的 Hosted Email Security 时，“与服务器同步”和“转至客户控制台”会呈灰显状态？

导致 Hosted Email Security 不活动的原因可能有三个。

- Hosted Email Security 尚未连接到远程管理器。
- 客户终止了连接。请参阅将 Hosted Email Security 客户连接到远程管理器 Web 控制台 第 6-2 页。
- 客户树可能需要刷新。

当我尝试在客户将 Hosted Email Security 连接到远程管理器后重定向到客户的 Hosted Email Security 控制台时，为什么会收到错误消息“您的 Hosted Email Security 客户尚未连接到远程管理器，或者 Hosted Email Security 已断开其连接。请与您的管理员联系”？

输入 GUID 或授权码并单击**连接**后，Hosted Email Security 可能需要长达十分钟的时间才能完成与远程管理器 Web 控制台的连接。如果问题依然存在，请与趋势科技技术支持联系。

为什么远程管理器 Web 控制台上的 Hosted Email Security 客户激活码 (AC) 和到期日期显示“N/A”？

如果 Hosted Email Security 客户未将 Hosted Email Security 服务连接到远程管理器或已经断开连接，远程管理器将无法检索数据。另一个原因是 Hosted Email Security 找不到此客户的有效激活码和到期日期。这种情况较为少见。

报表常见问题

对于可以存储的报表数是否有限制？

有。远程管理器会限制存储的报表数。达到配额后，会自动删除旧报表。存储的报表数为：

- **每日报表**：最多存储 30 个报表。
- **每周报表**：最多存储 10 个报表。
- **每月报表**：最多存储 5 个报表。

为什么创建一次性报表配置文件后，在报表历史记录中没有生成新报表？

请在创建报表配置文件后等待一到两分钟。此报表会显示在报表历史记录中。如果仍未能生成报表，请打开报表配置文件，并再次保存。如果问题依然存在，请与趋势科技技术支持联系。

为什么报表历史记录中有报表时，无法通过电子邮件接收每日/每周/每月报表？

请确保客户的电子邮件地址是有效的，且在报表配置文件收件人列表中。如果两者均无问题，则可能是网络问题。

在生成的报表中，为什么显示的数据时间与我所在的时区不符？

报表所依据的时区是销售商在创建配置文件时选择的时区。这不是由客户的计算机所决定的。

创建一次性报表后，“N/A”表示什么意思？

对于一次性报表，状态列将始终显示“N/A”。发生此种情况是因为一次性报表没有状态（无法禁用、启用、中止等）。

使用 SSL (HTTPS) 连接时，无法查看报表。

“不将加密的页存盘”是 Internet Explorer 的安全设置，该设置在处理 SSL (HTTPS) 连接时开始起作用。如果选中此设置，将不会向缓存保存任何内容，并且您将无法打开或下载报表。

要在 Internet Explorer 11.0 中修复此问题，请单击**工具** > **Internet 选项** > **高级** > **安全**，然后禁用**不将加密的页存盘**选项。

第 19 章

技术支持

了解以下主题：

联系支持

使用支持门户

趋势科技支持门户是全天候在线资源，无论是常见问题还是不常见问题，都能在里面找到相关最新信息。

过程

1. 转至 https://success.trendmicro.com/business-support。
2. 使用**搜索支持**文本框搜索可用的解决方案或关键字。
3. 单击**所有产品**下拉列表并选择您的产品。
4. 如果找不到任何解决方案，请单击**联系支持**并选择所需的支持类型。

   提示

   要在线提交支持案例，请访问以下 URL：

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   趋势科技的技术支持工程师会调查您提交的案例，并在 24 小时之内给您回复。

加快支持呼叫的处理速度

为了能够更好地解决问题，请准备好以下信息：

- 重现问题的步骤

- 设备或网络信息
- 计算机品牌、型号及所连接的任何其他硬件或设备
- 内存大小和可用硬盘空间
- 操作系统和 Service Pack 版本
- 已安装的客户端的版本
- 序列号或激活码
- 安装环境的详细描述
- 收到的任何错误消息的准确文本

将可疑内容发送给趋势科技

将可疑内容发送给趋势科技进行进一步分析时，有多个选项可供选择。

电子邮件信誉服务

查询特定 IP 地址的信誉，并提名将邮件传输客户端包括到全局允许列表：

https://ers.trendmicro.com/

要将邮件示例发送给趋势科技，请参考以下知识库条目：

http://esupport.trendmicro.com/solution/zh-CN/1112106.aspx

文件信誉服务

收集系统信息并将可疑文件内容提交给趋势科技：

http://esupport.trendmicro.com/solution/zh-cn/1059565.aspx

记录案例编号以备跟踪。

Web 信誉服务

查询疑似网络钓鱼站点的 URL 或其他所谓的“恶意站点”（Internet 威胁的源意向，例如间谍软件和恶意软件）的安全等级和内容类型：

http://global.sitesafety.trendmicro.com/

如果分配的等级不正确，请将重新分类请求发送给趋势科技。

资源故障排除

联系技术支持之前，请考虑访问以下趋势科技联机资源。

威胁百科全书

恶意软件如今大多是由混合威胁组成，两项或更多项技术在其中结合起来，企图绕过计算机安全协议。趋势科技通过可创建定制防御策略的产品来抵御这种复杂恶意软件。威胁百科全书提供了各种混合性威胁的名称和症状完整列表，包括已知恶意软件、垃圾邮件、恶意 URL 和已知漏洞。

请访问 http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=cn&tab=malware 了解更多信息：

- 当前处于活跃状态或“正在传播”的恶意软件和恶意活动代码
- 描述完整的 Web 攻击案例的相关威胁信息页面
- 有关针对性攻击和安全威胁的 Internet 威胁预警
- Web 攻击和联机趋势信息
- 每周恶意软件报告

下载专区

趋势科技可能会不定期发布针对报告的已知问题的 Patch 或适用于特定产品或服务的升级。要查找是否有任何 Patch 可用，请访问以下网址：

http://www.trendmicro.com/download/zh-cn/

如果未应用某个 Patch（Patch 已过时），请打开自述文件确定该 Patch 是否与您的环境相关。自述文件还包含安装说明。

文档反馈

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何文档有任何问题、意见或建议，请通过

service@trendmicro.com.cn 与我们联系。

索引

趋势科技（中国）有限公司
上海市淮海中路 398 号世纪巴士大厦 8 楼
电话：800-820-8839，未开通800 服务地区的用户请拨打（021-26037677）
手机用户可拨打：400-820-8839
电子邮件：service@trendmicro.com.cn

www.trendmicro.com.cn
文档代码：APCMS8158/180130