TREND MICRO

9.5 趋势科技服务器深度安全防护系统

趋势科技服务器深度安全防护系统管理中心用户界面

专为物理、虚拟和云服务器而设计的高级防护

Cloud & Data Center

Complete End User

Cyber Threats

文档版本：1.0
文档编号：APCM96842/150106
发布日期：2015 年 1月
文档生成时间：Feb 5, 2015 (15:11:11)

目录

趋势科技服务器深度安全防护系统管理中心控制台 7

警报 8

事件和报告 9

系统事件 10

防恶意软件事件 12

隔离的文件 15

Web 信誉事件 17

防火墙事件 19

入侵防御事件 22

完整性监控事件 25

日志审查事件 27

生成报告 30

计算机 33

策略 42

策略 43

通用对象 44

目录列表 45

文件扩展名列表 48

文件列表 49

IP 列表 52

MAC 列表 53

端口列表 54

时间表 55

标记 56

上下文 57

防火墙状态配置 59

恶意软件扫描配置 63

防火墙规则 70

入侵防御规则 73

应用程序类型 76

完整性监控规则 78

日志审查规则 82

计算机和策略编辑器 85

概述（策略编辑器） 86
常规 87
使用此策略的计算机 88
事件 89
概述（计算机编辑器） 91
常规 92
操作 95
事件 97
防恶意软件 99
常规 100
云安全智能防护 102
高级 103
隔离的文件 105
事件 106
Web 信誉 107
常规 108
云安全智能防护 109
高级 110
例外 111
事件 112
防火墙 113
常规 114
接口隔离 115
侦察 116
高级 118
事件 119
入侵防御 120
常规 121
高级 122
事件 124
完整性监控 125
常规 126
高级 127
事件 128
日志审查 129
常规 130
高级 131

事件 132
接口/接口类型 133
设置 134
计算机 135
网络引擎 138
扫描 143
SIEM 144
更新（仅限计算机编辑器） 145
覆盖 146
管理 147
系统设置 148
租户 149
客户端 152
警报 154
上下文 155
SIEM 156
SNMP 157
排序 158
系统事件 160
安全 161
更新 163
智能反馈 165
SMTP 166
存储 167
代理 168
高级 169
预设任务 171
基于事件的任务 173
管理中心节点 176
管理中心节点 0
租户 178
使用授权 179
用户 180
角色 183
联系人 187
系统信息 188
更新 189
安全更新 190

规则 192
特征码 194
软件更新概述 195
下载专区 196
本地软件 197
中继组 199

趋势科技服务器深度安全防护系统管理中心控制台

警报

警报页面会显示所有活动警报。警报以摘要视图（将类似警报分组显示）显示，或以列表视图（逐一列出每个警报）显示。要在两个视图之间切换，请使用页面标题中“警报”旁边的下拉菜单。

在摘要视图中，展开警报面板（单击**“显示详细信息”**）可显示生成该特定警报的所有计算机（和/或用户）。（单击计算机将会显示计算机的**详细信息**窗口。）

在“摘要视图”中，如果计算机列表中的计算机超过五个，则第五个计算机后面会出现省略号 （″...″）。单击省略号可显示完整列表。采取适当的操作处理警报后，选中警报目标旁边的复选框，然后单击**解除**链接，即可解除警报。（在“列表视图”中，右键单击警报即可查看上下文菜单中的选项列表。）

无法解除的警报（如“中继更新服务不可用”）将在条件不存在时自动解除。

如果警报条件在同一计算机上多次出现，则警报将显示条件第一次出现的时间戳。如果警报解除后条件重新出现，则第一次出现的时间戳将消失。

警报有两种：系统警报和安全警报。系统警报由系统事件（客户端脱机、计算机上的时钟更改等）触发。安全警报由入侵防御规则、防火墙规则、完整性规则和日志审查规则触发。可以通过单击**配置警报...** 来配置警报。 ().

注意： 使用计算机过滤栏，可以只查看在特定计算机组中、具有特定策略等计算机的警报。

事件和报告

“事件和报告”部分提供了以下页面：

- *系统事件（第 10页）*
- *防恶意软件事件（第 12页）*
  - *隔离的文件（第 15页）*
- *Web 信誉事件（第 17页）*
- *防火墙事件（第 19页）*
- *入侵防御事件（第 22页）*
- *完整性监控事件（第 25页）*
- *日志审查事件（第 27页）*
- *生成报告（第 30页）*

系统事件

系统事件日志是系统相关事件的记录（相对于安全相关事件）。在主页面上可以执行下列操作：

- **查看**（）系统事件的详细信息（属性）
- **搜索**（）特定系统事件
- 将当前显示的系统事件**导出**（）为 CSV 文件
- 查看现有的**自动标记**（）规则。

另外，右键单击事件可提供下列选项：

- **添加标记：**为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记：**移除现有事件标记

查看

选择某个事件并单击**查看**（）会显示**事件查看程序属性**窗口。

常规

常规信息

- **时间：**以托管趋势科技服务器深度安全防护系统管理中心的计算机的系统时钟为准的时间。
- **级别：**发生事件的严重性级别。事件级别包括**信息**、**警告**及**错误**。
- **事件 ID：**事件类型的唯一标识符。
- **事件：**事件的名称（与事件 ID 相关联）。
- **标记：**附加到事件的任何标记。
- **事件来源：**发生事件的趋势科技服务器深度安全防护系统组件。
- **目标：**与事件有关联的系统对象将在此处标识。单击对象的标识将显示对象的属性表。
- **操作执行者：**如果事件由用户启动，则会在此处显示该用户的用户名。单击该用户名将显示**用户属性**窗口。
- **管理中心：**趋势科技服务器深度安全防护系统管理中心计算机的主机名。

描述

如果合适，此处会显示执行何种操作以在系统事件日志中触发此条目的特定详细信息。

标记

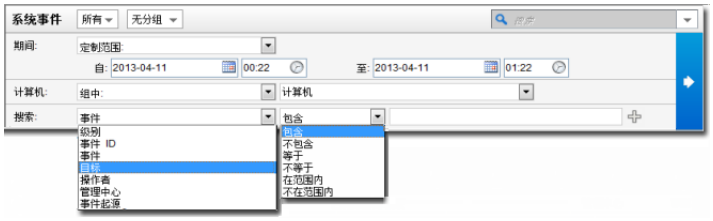
标记选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**关于事件标记的更多信息**。

过滤列表和/或搜索事件

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。

单击**高级搜索**可选择是否显示搜索栏。



按搜索栏右侧的“添加搜索栏”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交请求”按钮（位于工具栏右侧，带右向箭头）。

高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

导出

可以将显示的事件导出为 CSV 文件。（将忽略分页，所有页面都将被导出。）可以选择显示所显示的列表，也可以选择显示所选定的项目。

自动标记

单击**自动标记...** 将显示现有系统事件自动标记规则的列表。

防恶意软件事件

缺省情况下，启动每个波动信号时，趋势科技服务器深度安全防护系统管理中心会从客户端/设备中收集防恶意软件事件日志。这些事件数据用于填充趋势科技服务器深度安全防护系统管理中心的各种报告、图形及图表。

趋势科技服务器深度安全防护系统管理中心会将收集到的事件保留一段时间，该时间可在**管理 > 系统设置**页面中的**存储**选项卡上设置。

在主页面上可以执行下列操作：

- **查看** () 单个事件的属性。
- **过滤列表。**使用**期间**和**计算机**工具栏来过滤事件列表。
- 将事件列表数据**导出** () 为 CSV 文件。
- 查看现有的**自动标记** () 规则。
- **搜索** () 特定事件。

另外，右键单击事件可提供下列选项：

- 为此事件**添加标记**（请参阅**事件标记**。）
- 从此事件中**移除标记**。
- 查看生成日志条目的计算机的**计算机详细信息窗口**。
- 查看与此事件相关联的文件的**隔离文件详细信息**。（仅当与此事件相关联的处理措施为隔离时才可用。）

防恶意软件事件显示的列：

- **时间：**计算机上发生事件的时间。
- **计算机：**记录此事件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）
- **受感染文件：**受感染文件的位置和名称。
- **标记：**与此事件关联的事件标记。
- **恶意软件：**找到的恶意软件的名称。
- **扫描类型：**找到恶意软件的扫描类型（实时、预设或手动）。
- **主要病毒类型：**检测到的恶意软件的类型。可能的值有：恶作剧程序、特洛伊木马、病毒、测试程序、间谍软件、加壳软件、常规或其他。有关这些恶意软件类型的信息，请参阅防恶意软件事件的详细信息或**防恶意软件**。
- **结果：**显示与事件关联的恶意软件扫描配置中指定的处理措施的结果。
    - **已清除：** 趋势科技服务器深度安全防护系统成功终止了进程或删除了注册表、文件、cookie 或快捷方式，具体取决于恶意软件的类型。
    - **清除不成功：**因各种可能的原因而无法清除恶意软件。
    - **已删除：**已删除受感染文件。
    - **删除不成功：**因各种可能的原因而无法删除受感染文件。例如，文件可能由其他应用程序锁定、文件位于 CD 上或者正在使用中。如果可能，趋势科技服务器深度安全防护系统会在受感染文件被释放后立即将其删除。
    - **已隔离：**已将受感染文件移动到隔离文件夹中。
    - **隔离不成功：**因各种可能的原因而无法隔离受感染文件。例如，文件可能由其他应用程序锁定、文件位于 CD 上或者正在使用中。如果可能，趋势科技服务器深度安全防护系统会在受感染文件被释放后

立即将其隔离。也有可能已超出“用于存储隔离文件的最大磁盘空间”（在**策略/计算机编辑器** > **防恶意软件** > **高级**选项卡上指定）。

- **拒绝访问**：趋势科技服务器深度安全防护系统已阻止对受感染文件进行访问，而未将文件从系统中移除。
- **未处理**：趋势科技服务器深度安全防护系统未采取任何处理措施，但记录了对恶意软件的检测。

- **事件来源**：指明事件来源于趋势科技服务器深度安全防护系统的哪个部分。
- **原因**：检测到恶意软件时生效的恶意软件扫描配置。

查看事件属性

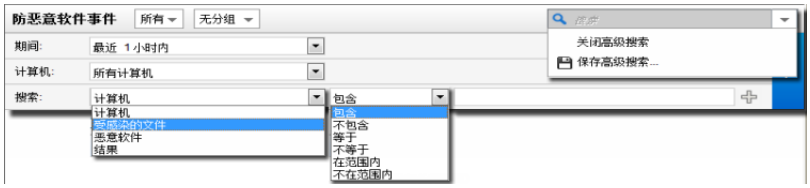
双击某个事件（或从上下文菜单中选择**查看**）会显示该条目的**属性**窗口，这样将在一个页面上显示该事件的所有信息。**标记**选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

从“搜索”下拉菜单中选择“打开高级搜索”，可选择是否显示高级搜索选项。

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

按搜索栏右侧的“加号”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交”按钮（位于工具栏右侧，带右向箭头）。

导出

单击**导出...**，可将所有或选定的事件导出为 CSV 文件。

自动标记...

单击**自动标记...** 将显示现有防恶意软件自动标记规则的列表。

隔离的文件

隔离的文件是已查明为（或包含）恶意软件且因此已进行加密并移动到特殊文件夹中的文件。（“隔离”是一种可以在创建恶意软件扫描配置时指定的扫描处理措施。）已标识和隔离文件后，您可以选择以加密和压缩格式将文件下载到计算机上。是否隔离受感染文件取决于扫描文件时生效的防恶意软件配置。

注意： *将隔离的文件下载到计算机后，**隔离的文件**向导将显示指向**管理工具**的链接，您可以使用管理工具解密、检查和恢复文件。*

为存储隔离文件设置了有限的磁盘空间。可在**策略/计算机编辑器** > **防恶意软件** > **高级** > **隔离的文件**中配置该空间容量。当没有足够空间可用于隔离可疑文件时会引发警报。

如果使用趋势科技服务器深度安全防护系统虚拟设备为虚拟机提供保护，无客户端 VM 的所有隔离文件都将存储在虚拟设备上。因此，您应该为虚拟设备上的隔离文件增加磁盘空间。

在以下情况下，将自动从虚拟设备删除隔离的文件：

- 如果 VM 经历 vMotion，将从虚拟设备删除与该 VM 关联的隔离文件。
- 如果从趋势科技服务器深度安全防护系统管理中心停用了 VM，将从虚拟设备删除与该 VM 关联的隔离文件。
- 如果从趋势科技服务器深度安全防护系统管理中心停用了虚拟设备，将删除该虚拟设备上存储的所有隔离文件。
- 如果从 vCenter 删除虚拟设备，也将删除存储在该虚拟设备上的所有隔离文件。

通过**防恶意软件隔离的文件**页面，可以管理隔离任务。使用菜单栏或右键单击上下文菜单，您可以：

- **恢复...** () 将隔离文件恢复到其原始位置和状况。
- **下载...** () 可将隔离文件从计算机或虚拟设备移动到选定位置。
- **删除...** () 可从计算机或虚拟设备删除一个或多个隔离文件。
- 将有关隔离文件（并非文件本身）的信息**导出** () 为 CSV 文件。
- **查看**隔离文件的详细信息 ()。
- 查看检测到恶意软件的计算机的**计算机详细信息** () 窗口。
- **查看防恶意软件事件...** () 显示与此隔离文件关联的防恶意软件事件。
- **添加或删除列** () 通过单击**添加/删除**可添加或删除列。
- **搜索** () 特定隔离文件。

详细信息

隔离文件**详细信息**窗口显示有关文件的更多信息，您可以将隔离文件下载到计算机或从其所在位置将其删除。

- **检测时间：**检测到感染的日期/时间（受感染计算机上）。
- **受感染的文件：**受感染文件的名称。
- **恶意软件：**找到的恶意软件的名称。
- **扫描类型：**指示恶意软件是由实时扫描、预设扫描还是手动扫描检测到的。
- **扫描结果：**检测到恶意软件时趋势科技服务器深度安全防护系统所采取的处理措施的结果。

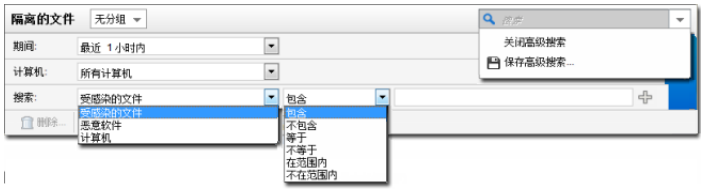
- **计算机**：找到此文件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）

过滤列表和/或搜索隔离文件

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内隔离的文件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织隔离文件条目的显示。

从“搜索”下拉菜单中选择“打开高级搜索”，可选择是否显示高级搜索选项：



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串。
- **不包含**：选定列中的条目不包含该搜索字符串。
- **等于**：选定列中的条目完全符合该搜索字符串。
- **不等于**：选定列中的条目并不完全符合该搜索字符串。
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配。
- **不在范围内**：选定列中的条目并未与任何逗号分隔的搜索字符串条目完全匹配。

按搜索栏右侧的“加号”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交”按钮（位于工具栏右侧，带右向箭头）。

- **受感染文件**：显示受感染文件的名称和特定安全风险。
- **恶意软件**：命名恶意软件感染。
- **计算机**：指明带有可疑感染的计算机的名称。

手动恢复隔离文件

要手动恢复隔离文件，必须使用隔离文件解密工具解密文件，然后将文件移回到原始位置。解密工具位于 zip 文件 QFAdminUtil_win32.zip 中，该文件位于趋势科技服务器深度安全防护系统管理中心根目录下的 "util" 文件夹中。该压缩文件包含两个执行相同功能的工具：QDecrypt.exe 和 QDecrypt.com。运行 QDecrypt.exe 会调用打开文件对话框，通过该对话框可以选择要解密的文件。QDecrypt.com 是一个命令行工具，具有以下选项：

- /h, --help：显示此帮助消息
- --verbose：生成详细日志消息
- /i, --in=<str>：要解密的隔离文件，其中 <str> 是隔离文件的名称
- /o, --out=<str>：解密文件输出，其中 <str> 是为生成的解密文件指定的名称

注意： *仅 Windows 32 位系统支持该工具。*

Web 信誉事件

缺省情况下，启动每个波动信号时，趋势科技服务器深度安全防护系统管理中心会从趋势科技服务器深度安全防护系统客户端/设备中收集 Web 信誉事件日志。这些日志的数据将用于填充趋势科技服务器深度安全防护系统管理中心中的各种报告、图形及图表。

趋势科技服务器深度安全防护系统管理中心会将收集到的事件日志保留一段时间，该时间可在**管理** > **系统设置** > **存储**中设置。

在主页面上可以执行下列操作：

- **查看** () 单个事件的属性
- **过滤列表：**使用**期间**和**计算机**工具栏来过滤事件列表
- 将事件列表数据**导出** () 为 CSV 文件
- 查看现有的**自动标记** () 规则。
- **搜索** () 特定事件

另外，右键单击事件可提供下列选项：

- **添加标记：**为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记：**移除现有事件标记
- **添加到允许列表** ( )：将触发此事件的 URL 添加到允许的 URL 列表。（要查看或编辑**允许**和**阻止**列表，请转至 **Web 信誉**主页面的**例外**选项卡。）
- **计算机详细信息：**查看生成日志条目的计算机的“详细信息”窗口

用于 Web 信誉事件显示的列：

- **时间：**计算机上发生事件的时间。
- **计算机：**记录此事件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）
- **URL：**触发此事件的 URL。
- **标记：**与此事件关联的事件标记。
- **风险：**触发此事件的 URL 的风险级别（“可疑”、“高度可疑”、“危险”、“未测试”或“已被管理员阻止”）。
- **排序：**
- **事件来源：**指明事件来源于趋势科技服务器深度安全防护系统的哪个部分。

查看事件属性

双击某个事件会显示该条目的**属性**窗口，这样将在一个页面上显示该事件的所有信息。

重新分类：如果您认为某个特定站点的站点安全评级或分类不正确，请通过位于 http://sitesafety.trendmicro.com 的站点安全中心向趋势科技发送反馈。

添加到允许列表...：使用**添加到允许列表...** 按钮可将此 URL 添加到允许的 URL 列表。（要查看或编辑**允许**和**阻止**列表，请转至 **Web 信誉**主页面的**例外**选项卡。）

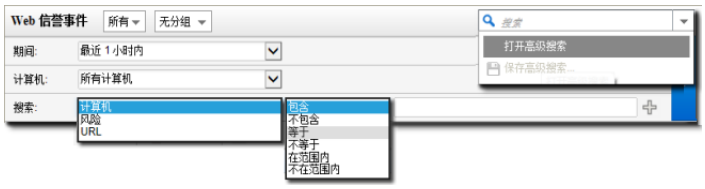
标记选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**关于事件标记的更多信息**。

过滤列表和/或搜索事件

从“搜索”下拉菜单中选择“打开高级搜索”，可选择是否显示高级搜索选项。

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

按搜索栏右侧的“加号”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交”按钮（位于工具栏右侧，带右向箭头）。

导出

单击**导出...** 按钮，可将所有或选定的事件导出为 CSV 文件。

自动标记

单击**自动标记...**将显示现有 Web 信誉自动标记规则的列表。

防火墙事件

缺省情况下，启动每个波动信号时，趋势科技服务器深度安全防护系统管理中心会从趋势科技服务器深度安全防护系统客户端/设备中收集防火墙和入侵防御事件日志。这些日志的数据将用于填充趋势科技服务器深度安全防护系统管理中心中的各种报告、图形及图表。

趋势科技服务器深度安全防护系统管理中心会将收集到的事件日志保留一段时间，该时间可在**管理** > **系统设置** > **存储**中设置。

防火墙事件图标：

-  单个事件
-  带有数据的单个事件
-  折叠事件
-  带有数据的折叠事件

注意： *当多个相同类型事件连续发生时，事件发生折叠。这样会节省磁盘空间，并防止企图使日志记录机制过载的 DoS 攻击。*

在主页面上可以执行下列操作：

- **查看** () 单个事件的属性
- **过滤列表：**使用**期间**和**计算机**工具栏来过滤事件列表
- 将事件列表数据**导出** () 为 CSV 文件
- 查看现有的**自动标记** () 规则。
- 从“事件列表”视图中添加或删除**列** ()。
- **搜索** () 特定事件

另外，右键单击事件可提供下列选项：

- **添加标记：**为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记：**移除现有事件标记
- **计算机详细信息：**查看生成日志条目的计算机的“详细信息”窗口

防火墙事件显示的列：

- **时间：**计算机上发生事件的时间。
- **计算机：**记录此事件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）
- **原因：**此页面上的日志条目是由防火墙规则设置还是由防火墙状态配置设置生成。如果该条目按照防火墙规则生成，列条目的开头会加上“防火墙规则：”，后面跟防火墙规则的名称。否则，列条目会显示生成此日志条目的“防火墙状态配置”设置。（有关可能的数据包拒绝原因的列表，请参阅**参考**一节中的“数据包拒绝原因”。）
- **标记：**应用到此事件的事件标记。
- **操作：**防火墙规则或防火墙状态配置所采取的操作。可能的操作有：允许、拒绝、强制允许和仅记录。

- **排序**：排序系统提供一种方法来量化入侵防御和防火墙事件的重要性。先为计算机分配“资产值”，并为入侵防御规则和防火墙规则分配“严重性值”，然后，将两个值相乘便可得出事件的重要性（“排序”）。这样，您在查看入侵防御或防火墙事件时，就可以按“排序”来排列事件的顺序。
- **方向**：受影响数据包的方向（传入或传出）。
- **接口**：数据包所经过的接口的 MAC 地址。
- **帧类型**：所需数据包的帧类型。可能的值有“IPV4”、“IPV6”、“ARP”、“REVARP”和“其他：XXXX”，其中 XXXX 代表帧类型的四位数十六进制码。
- **协议**：可能的值有“ICMP”、“ICMPV6”、“IGMP”、“GGP”、“TCP”、“PUP”、“UDP”、“IDP”、“ND”、“RAW”、“TCP+UDP”、及“其他：nnn”，其中，nnn 代表三位数的十进制值。
- **标志**：数据包中已设置的标志。
- **源 IP**：数据包的源 IP。
- **源 MAC**：数据包的源 MAC 地址。
- **源端口**：数据包的源端口。
- **目标 IP**：数据包的目标 IP 地址。
- **目标 MAC**：数据包的目标 MAC 地址。
- **目标端口**：数据包的目标端口。
- **数据包大小**：数据包的大小（以字节为单位）。
- **重复计数**：连续重复事件的次数。
- **事件来源**：发生事件的趋势科技服务器深度安全防护系统组件。

注意： *如果所需数据包随后没有被**拒绝**规则或未允许该数据包的**允许**规则停止，则**仅记录**规则将只生成日志条目。如果数据包被上述两种规则中的一种阻止，则这些规则（但不是**仅记录**规则）将生成日志条目。如果没有后续规则停止数据包，则“仅记录”规则会生成条目。*

查看事件属性

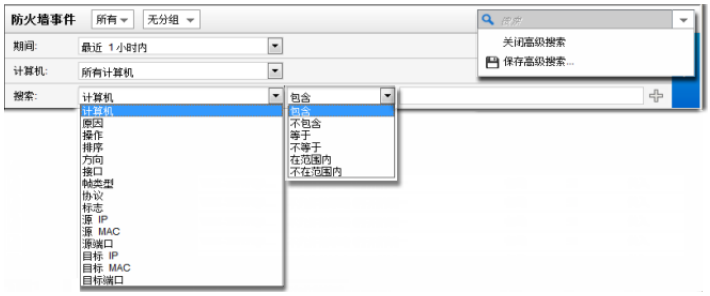
双击某个事件会显示该条目的**属性**窗口，这样将在一个页面上显示该事件的所有信息。**标记**选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

从“搜索”下拉菜单中选择“打开高级搜索”，可选择是否显示高级搜索选项。

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

按搜索栏右侧的“加号”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交”按钮（位于工具栏右侧，带右向箭头）。

导出

单击**导出...** 按钮，可将所有或选定的事件导出为 CSV 文件。

自动标记

单击**自动标记...**将显示现有防火墙自动标记规则的列表。

入侵防御事件

缺省情况下，启动每个波动信号时，趋势科技服务器深度安全防护系统管理中心会从趋势科技服务器深度安全防护系统客户端/设备中收集防火墙和入侵防御事件日志。

趋势科技服务器深度安全防护系统管理中心会将收集到的事件日志保留一段时间，该时间可在**管理** > **系统设置** > **存储**中设置。缺省设置为一星期。

在主页面上可以执行下列操作：

- **查看**（）单个事件的属性
- **过滤列表**：使用**期间**和**计算机**工具栏来过滤事件列表
- 将事件日志数据**导出**（）为 CSV 文件
- 查看现有的**自动标记**（）规则。
- 从“事件列表”视图中添加或删除**列**（）。
- **搜索**（）特定事件

另外，右键单击事件可提供下列选项：

- **全选**：选择显示的所有事件，最多 100 个事件。
- **将选定内容导出为 CSV**：创建列出了选定事件的详细信息的逗号分隔的文件。然后可在电子表格中打开 CSV 文件。
- **查看**：显示事件的详细信息
- **添加标记**：为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记**：移除现有事件标记
- **计算机详细信息**：查看生成日志条目的计算机的“详细信息”窗口

入侵防御事件显示的列：

- **时间**：计算机上发生事件的时间。
- **计算机**：记录此事件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）
- **原因**：与此事件关联的入侵防御规则。
- **标记**：附加到事件的任何标记。
- **应用程序类型**：与引起此事件的入侵防御规则关联的应用程序类型。
- **操作**：入侵防御规则采取的操作（阻止、删除、插入、替换、重置。如果规则处于**仅检测**模式下，则该操作的前缀为“仅检测:”）。
- **排序**：排序系统提供一种方法来量化入侵防御和防火墙事件的重要性。先为计算机分配“资产值”，并为入侵防御规则和防火墙规则分配“严重性值”，然后，将两个值相乘便可得出事件的重要性（“排序”）。这样，您在查看入侵防御或防火墙事件时，就可以按“排序”来排列事件的顺序。
- **严重性**：入侵防御规则的严重性值。
- **方向**：数据包的方向（传入或传出）
- **流**：触发此事件的数据包按入侵防御规则监控的流量方向（“连接流”）还是按其反方向（“反向流”）进行传递。
- **接口**：数据包所经过的接口的 MAC 地址。

- **帧类型**：所需数据包的帧类型。可能的值有“IPV4”、“IPV6”、“ARP”、“REVARP”和“其他：XXXX”，其中 XXXX 代表帧类型的四位数十六进制码。
- **协议**：可能的值有“ICMP”、“ICMPV6”、“IGMP”、“GGP”、“TCP”、“PUP”、“UDP”、“IDP”、“ND”、“RAW”、“TCP+UDP”、及“其他：nnn”，其中，nnn 代表三位数的十进制值。
- **标志**：数据包中已设置的标志。
- **源 IP**：数据包的源 IP。
- **源 MAC**：数据包的源 MAC 地址。
- **源端口**：数据包的源端口。
- **目标 IP**：数据包的目标 IP 地址。
- **目标 MAC**：数据包的目标 MAC 地址。
- **目标端口**：数据包的目标端口。
- **数据包大小**：数据包的大小（以字节为单位）。
- **重复计数**：连续重复事件的次数。
- **事件来源**：发生事件的趋势科技服务器深度安全防护系统组件。

查看事件属性

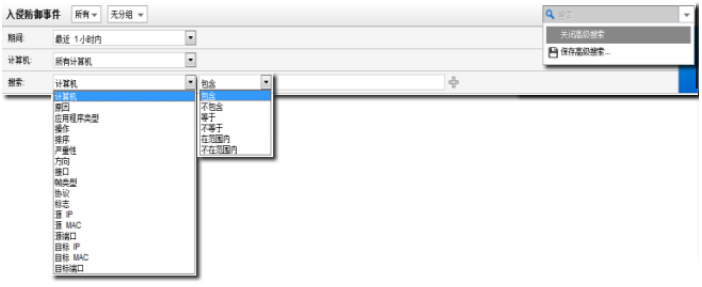
双击某个事件可显示该条目的**属性**窗口。**标记**选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

从“搜索”下拉菜单中选择“打开高级搜索”，可选择是否显示高级搜索选项。

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串

- **在范围内：**选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内：**选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

按搜索栏右侧的“加号”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交”按钮（位于工具栏右侧，带右向箭头）。

导出

单击**导出...** 按钮，可将所有事件日志条目导出为 CSV 文件。

自动标记

单击**自动标记...** 将显示现有入侵防御自动标记规则的列表。

完整性监控事件

启动每个波动信号时，趋势科技服务器深度安全防护系统管理中心会从趋势科技服务器深度安全防护系统客户端中收集完整性监控事件。这些日志的数据将用于填充趋势科技服务器深度安全防护系统管理中心中的各种报告、图形及图表。

趋势科技服务器深度安全防护系统管理中心会将收集到的事件日志保留一段时间，该时间可在**管理** > **系统设置** > **存储**中设置。缺省设置为一星期。

在主页面上可以执行下列操作：

- **查看** () 单个事件的属性
- **过滤列表**：使用**期间**和**计算机**工具栏来过滤事件列表
- 将事件列表数据**导出** () 为 CSV 文件
- 添加自动标记规则
- 从“事件列表”视图中添加或删除**列** ()。
- **搜索** () 特定事件

另外，右键单击事件可提供下列选项：

- **添加标记**：为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记**：移除现有事件标记
- **计算机详细信息**：查看生成日志条目的计算机的“详细信息”窗口
- **完整性监控规则属性**：查看与此事件关联的完整性监控规则的属性

完整性监控事件显示的列：

- **时间**：计算机上发生事件的时间。
- **计算机**：记录此事件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）
- **原因**：与此事件关联的完整性监控规则。
- **标记**：应用到此事件的事件标记。
- **更改**：完整性规则检测到的更改。可以为：创建、更新、检测或更名。
- **排序**：排序系统提供一种方法来量化入侵防御和防火墙事件的重要性。先为计算机分配“资产值”，并为入侵防御规则和防火墙规则分配“严重性值”，然后，将两个值相乘便可得出事件的重要性（“排序”）。这样，您在查看入侵防御或防火墙事件时，就可以按“排序”来排列事件的顺序。
- **严重性**：完整性监控规则的严重性值
- **类型**：发生事件的实体类型
- **注册表项**：发生事件的路径和文件名或注册表项
- **用户**：文件所有者的用户 ID
- **进程**：发生事件的进程
- **事件来源**：发生事件的趋势科技服务器深度安全防护系统组件

查看事件属性

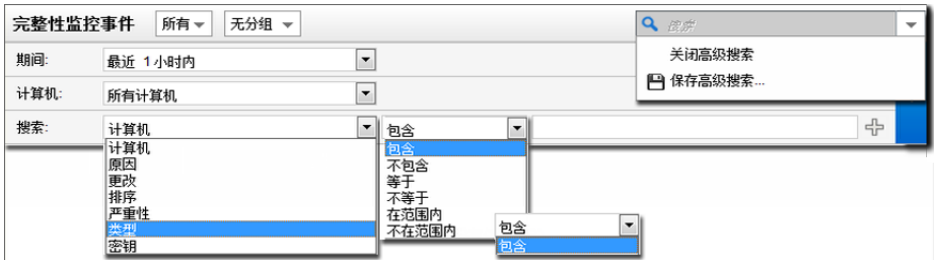
双击某个事件会显示该条目的**属性**窗口，这样将在一个页面上显示该事件的所有信息。**标记**选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。

使用“搜索”或“高级搜索”选项对显示的事件进行搜索、排序或过滤。



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

导出

单击**导出...** 按钮，可将所有或选定的事件导出为 CSV 文件。

自动标记

单击**自动标记...**将显示现有完整性监控自动标记规则的列表。

日志审查事件

启动每个波动信号时，趋势科技服务器深度安全防护系统管理中心会从趋势科技服务器深度安全防护系统客户端中收集日志审查事件。这些日志的数据将用于填充趋势科技服务器深度安全防护系统管理中心中的各种报告、图形及图表。

趋势科技服务器深度安全防护系统管理中心会将收集到的事件日志保留一段时间，该时间可在**管理** > **系统设置** > **存储**中设置。缺省设置为一星期。

在主页面上可以执行下列操作：

- **查看** () 单个事件的属性
- **搜索** () 特定事件
- **过滤列表**：使用**期间**和**计算机**工具栏来过滤事件列表
- 查看现有的**自动标记** () 规则。
- 从“事件列表”视图中添加或删除**列** ()。
- 将事件列表数据**导出** () 为 CSV 文件

另外，右键单击事件可提供下列选项：

- **添加标记**：为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记**：移除现有事件标记
- **计算机详细信息**：查看生成日志条目的计算机的“详细信息”窗口
- **日志审查规则属性**：查看与此事件关联的日志审查规则的属性

日志审查事件显示的列：

- **时间**：计算机上发生事件的时间。
- **计算机**：记录此事件的计算机。（如果已移除此计算机，此条目会显示为“未知计算机”。）
- **原因**：与此事件关联的日志审查规则。
- **标记**：附加到事件的任何标记。
- **描述**：规则的描述。
- **排序**：排序系统提供了一种量化事件重要性的方法。先为计算机分配“资产值”，并为日志审查规则分配“严重性值”，然后，将两个值相乘便可得出事件的重要性（“排序”）。这允许您按排序来排列事件的顺序。
- **严重性**：日志审查规则的严重性值。
- **组**：规则所属的组。
- **程序名称**：程序名称。取自事件的 syslog 标头。
- **事件**：事件的名称。
- **位置**：日志的来源。
- **源 IP**：数据包的源 IP。
- **源端口**：数据包的源端口。
- **目标 IP**：数据包的目标 IP 地址。
- **目标端口**：数据包的目标端口。

- **协议**：可能的值有“ICMP”、“ICMPV6”、“IGMP”、“GGP”、“TCP”、“PUP”、“UDP”、“IDP”、“ND”、“RAW”、“TCP+UDP”、及“其他：nnn”，其中，nnn 代表三位数的十进制值。
- **操作**：在事件内采取的操作
- **源用户**：事件内的发起用户。
- **目标用户**：事件内的目标用户。
- **事件主机名**：事件源的主机名。
- **原始事件**:
- **ID**:解码为来自事件的 ID 的任意 ID。
- **状态**：事件内的已解码状态。
- **命令**：在事件内调用的命令。
- **URL**：事件内的 URL。
- **数据**：从事件中提取的任意其他数据。
- **系统名称**：事件内的系统名称。
- **匹配的规则**：匹配的规则数目。
- **事件来源**：发生事件的趋势科技服务器深度安全防护系统组件。

查看事件属性

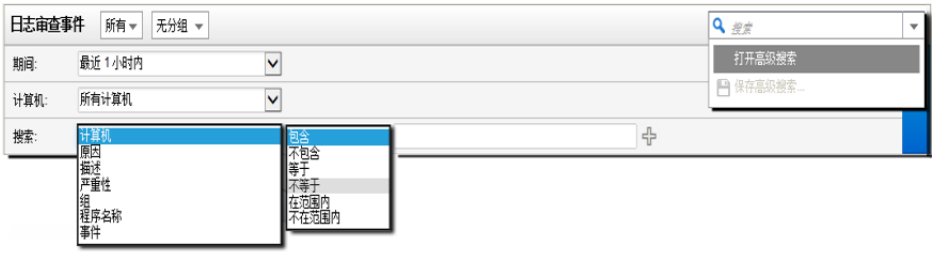
双击某个事件会显示该条目的**属性**窗口，这样将在一个页面上显示该事件的所有信息。**标记**选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。

使用“搜索”或“高级搜索”选项对显示的事件进行搜索、排序或过滤。



高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串
- **不等于**：选定列中的条目并不完全符合该搜索字符串

- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

导出

单击**导出...** 按钮，可将所有事件日志条目导出为 CSV 文件。

自动标记

单击**自动标记...**将显示现有日志审查自动标记规则的列表。

您可以使用自动标记来自动对日志审查组应用标记。LI 规则将组与规则中的标记关联。例如：

```
<rule id="18126" level="3">
<if_sid>18101</if_sid>
<id>^20158</id>
<description>Remote access login success</description>
<group>authentication_success,</group>
</rule>

<rule id="18127" level="8">
<if_sid>18104</if_sid>
<id>^646|^647</id>
<description>Computer account changed/deleted</description>
<group>account_changed,</group>
</rule>
```

每个组名都具有一个与其关联的“友好”名称字符串。在上述示例中，"authentication_success" 的友好名称为“认证成功”，"account_changed" 的友好名称为“帐户已更改”。设置此复选框后，该友好名称将自动添加为该事件的标记。如果触发了多个规则，则会有多个标记添加到事件。

生成报告

趋势科技服务器深度安全防护系统管理中心可生成 PDF 或 RTF 格式的报告。**生成报告**页面生成的大部分报告都含有可配置参数，如日期范围或按计算机组生成报告。不适用于报告的参数选项将被禁用。

单个报告

报告

各个报告可以输出为 PDF 或 RTF 格式，“安全模块使用情况报告”除外，该报告输出为 CSV 文件。可能会提供以下报告，具体取决于您使用的防护模块：

- **用户和联系人报告：**用户和联系人的内容及活动详细信息
- **警报报告：**最常见警报的列表
- **防恶意软件报告：**前 25 台受感染的计算机的列表
- **攻击报告：**包含分析活动的摘要表（按模式划分）
- **防火墙报告：**防火墙规则和状态配置活动的记录
- **取证计算机审计报告：**计算机上的客户端配置
- **计算机报告：**“计算机”选项卡上列出的每个计算机的摘要
- **安全模块使用情况报告：**防护模块的当前计算机使用情况
- **完整性监控基线报告：**特定时间的主机基线，显示类型、密钥和指纹采集日期。
- **完整性监控详细更改报告：**有关检测到的更改的详细信息
- **完整性监控报告：**检测到的更改的摘要
- **入侵防御报告：**入侵防御规则活动的记录
- **日志审查报告：**已收集的日志数据的摘要
- **日志审查详细报告：**已收集的日志数据的详细信息
- **建议报告：**“漏洞扫描（推荐设置）”活动的记录
- **摘要报告：**趋势科技服务器深度安全防护系统活动的整合摘要
- **可疑应用程序活动报告：**有关可疑恶意活动的信息
- **系统事件报告：**系统（非安全）活动的记录
- **系统报告：**计算机、联系人和用户的概述
- **Web 信誉报告：**包含大多数 Web 信誉事件的计算机列表

标记过滤器

选择包含事件数据的报告时，可以选择使用“事件标记”过滤报告数据。为所有事件选择**所有**，仅为未标记的事件选择**未标记**，或选择**标记**并指定一个或多个标记以仅包含那些具有所选标记的事件。

时间过滤器

可以针对记录存在的任意期间设置时间过滤器。这对安全审计非常有用。

时间过滤器选项：

- **最近 24 小时内：**包含最近 24 小时内的事件，起止于整点。例如，如果在 12 月 5 日上午 10:14 生成报告，则可以获取 12 月 4 日上午 10:00 到 12 月 5 日上午 10:00 之间发生的事件的报告。
- **最近 7 天内：**包含上周内的事件，止于当日午夜。例如，如果在 12 月 5 日上午 10:14 生成报告，则可以获取 11 月 28 日午夜 00:00 到 12 月 5 日午夜 00:00 之间发生的事件的报告。
- **上个月：**包含上一整月的事件，起止于午夜 (00:00)。例如，如果您在 11 月 15 日选择此选项，则将收到从 10 月 1 日午夜到 11 月 1 日午夜的事件报告。
- **定制范围：**允许为报告指定自己的日期和时间范围。如果开始日期早于两天以前，则报告中的开始时间可能会更改为午夜。

注意： *报告使用计数器中存储的数据。计数器是从事件定期聚合的数据。最近三天的计数器数据会每小时聚合一次。当前这一小时的数据不包括在报告中。三天前的数据将存储在按天聚合的计数器中。基于此原因，最近三天的报告所涵盖的时间段能以每小时级别的粒度来指定，但是，如果超出三天，此时间段只能以每天级别的粒度来指定。*

计算机过滤器

设置将其数据包含在报告中的计算机。您可以包括您有查看权限的任何计算机。查看权限在角色的“计算机权限”选项卡上指定。（有关更多信息，请参阅*角色（第 183页）*。）

计算机过滤器选项：

- **所有计算机：**如果查看权限允许您看到趋势科技服务器深度安全防护系统管理的所有计算机，则选择此选项可以在报告中包含所有计算机。
- **我的计算机：**如果查看权限只允许您看到某些计算机，则选择此选项可以包括您能查看的所有计算机。
- **组中：**允许您在报告中仅包含属于选定组的计算机（其子组可选）。
- **使用策略：**允许您在报告中仅包含使用选定策略的计算机（其子策略可选）。
- **计算机：**允许您在报告中仅包含一台选定的计算机。

注意： *要在多个计算机组的特定计算机上生成报告，请创建一个仅对所需计算机具有查看权限的用户，然后再创建一个预设任务，以为该用户定期生成“所有计算机”报告，或者以该用户身份登录，并运行“所有计算机”报告。只有该用户具有查看权限的计算机才会包含在报告中。*

加密

您可以使用密码保护报告。

加密选项：

- 禁用报告密码：报告将不受密码保护。
- 使用当前用户的报告密码：报告将受当前登录用户的密码保护。如果您的角色为“完全访问权限”，此选项不可用。

- 使用定制报告密码:报告将受您在**使用定制报告密码**和**确认密码**框中输入的密码保护。

定期报告

定期报告只是定期为任意数量的用户和联系人生成和分发报告的预设任务。大多数选项与单个报告的选项相同，但“时间过滤器”除外，该选项如下所示：

- **最近 [N] 小时内：**如果 [N] 小于 60，开始时间和结束时间是指定小时的整点时间。如果 [N] 大于 60，在时间范围开始时不提供每小时数据，因此报告中的开始时间将更改为开始日期的午夜 (00:00)。
- **最近 [N] 天内：**包括 [N] 天前午夜到当前日期午夜的数据。
- **最近 [N] 周内：**包含最近 [N] 周内的事件，起止于午夜 (00:00)。
- **最近 [N] 个月内：**包含最近 [N] 个完整自然月内的事件，起止于午夜 (00:00)。例如，如果您在 11 月 15 日选择“最近 1 个月内”，则将收到从 10 月 1 日午夜到 11 月 1 日午夜的事件报告。

注意： *报告使用计数器中存储的数据。计数器是从事件定期聚合的数据。最近三天的计数器数据会每小时聚合一次。当前这一小时的数据不包括在报告中。三天前的数据将存储在按天聚合的计数器中。基于此原因，最近三天的报告所涵盖的时间段能以每小时级别的粒度来指定，但是，如果超出三天，此时间段只能以每天级别的粒度来指定。*

有关预设任务的更多信息，请转至**管理 > 预设任务**。

计算机

趋势科技服务器深度安全防护系统管理中心的**计算机**部分用于管理和监控网络上的计算机。此页面会定期刷新以显示最新信息。（可以每个用户为基础修改刷新速率。转至**管理** > **用户管理** > **用户**，然后双击用户打开用户**属性**窗口。可在**设置**选项卡的**刷新速率**区域中设置**计算机列表**的刷新速率。）

计算机图标：

- 普通计算机（物理计算机或作为物理计算机管理的虚拟机）
- 趋势科技服务器深度安全防护系统中继
- ESXi Server
- 虚拟计算机（VMware vCenter 管理的虚拟机）
- 虚拟计算机（已启动）
- 虚拟计算机（已停止）
- 虚拟计算机（已暂停）
- 虚拟设备
- 虚拟设备（已启动）
- 虚拟设备（已停止）
- 虚拟设备（已暂停）

预览窗格

单击列出的计算机旁边的**预览**图标（ ）以展开其下的显示区域。预览中显示的信息取决于计算机的类型。

普通计算机

普通计算机的预览窗格显示客户端的存在情况、计算机状态以及防护模块的状态。（注意，日志审查模块已关闭，并且插件未安装。）

防护模块状态

趋势科技服务器深度安全防护系统中继

趋势科技服务器深度安全防护系统中继的预览窗格显示其状态、可用于分发的安全更新组件的数量，以及其内置的趋势科技服务器深度安全防护系统客户端提供的防护模块的状态。

ESXi Server

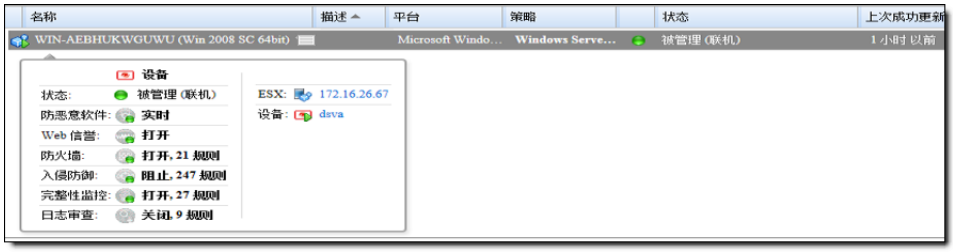
ESXi Server 的预览窗格显示其状态以及 ESXi 软件和趋势科技服务器深度安全防护系统过滤器驱动程序的版本号。它还显示此服务器上 vShield Endpoint 的状态（必须安装 vShield Endpoint 才能提供防恶意软件保护）。**客户虚拟机**区域中显示存在的趋势科技服务器深度安全防护系统虚拟设备，以及此主机上运行的虚拟机。

虚拟设备

虚拟设备的预览窗格显示其状态、设备的版本号以及此设备上 vShield Endpoint 的状态（必须注册 vShield Endpoint 才能提供防恶意软件保护）。在**受保护的客户虚拟机**区域中，将显示受保护的虚拟机。

采用无客户端防护的虚拟机

虚拟机的预览窗格显示其受虚拟设备、客户虚拟机客户端或这两者保护。它显示有关虚拟机上运行的组件的详细信息。因为此时设备不能提供日志审查保护，所以它将显示为“不可用”。设备和客户虚拟机客户端的防火墙和入侵防御配置将始终相同。



注意： *请记住，虚拟机可以像趋势科技服务器深度安全防护系统管理中心所管理的普通计算机一样运行客户端。无需经过 vCenter 集成将其“导入”到管理中心。有关 VMware 集成的更多信息，请参阅《安装指南》。*

向趋势科技服务器深度安全防护系统管理中心添加计算机

有关向趋势科技服务器深度安全防护系统管理中心添加计算机的详细说明，请参阅**添加计算机**。

注意： *在计算机上安装客户端之后，必须由趋势科技服务器深度安全防护系统管理中心“激活”该客户端。在此过程中，趋势科技服务器深度安全防护系统管理中心会向客户端发送“指纹”。这之后，客户端将只接受来自具有该唯一指纹的管理中心的指令。*

注意： *如果将客户端安装在之前由趋势科技服务器深度安全防护系统虚拟设备提供无客户端保护的虚拟机上，必须从管理中心重新激活该虚拟机，以注册计算机上存在的客户端。*

定义新的计算机

在工具栏中单击**新建**显示计算机创建向导。键入新计算机的主机名或 IP 地址，并从下拉列表中选择要应用到新计算机的策略（可选）。单击**下一步**会指示管理中心在网络上查找该计算机。

- **如果未找到您所指定的计算机，**管理中心仍会在**计算机**页面中为其创建一个条目，但您必须确保管理中心可以访问此计算机且已安装并激活客户端。然后，可以为其应用适当的策略。
- **如果已找到计算机但未识别到任何客户端，**管理中心将在**计算机**页面中为此计算机创建一个条目。您必须在该计算机上安装客户端并激活它。
- **如果已找到计算机且已检测到客户端，**管理中心将在**计算机**页面中创建一个条目。在您退出向导（通过单击**完成**）后，管理中心会立刻激活计算机上的客户端并应用您所选定的策略。

查找计算机

在工具栏中单击**发现...**显示**发现计算机**对话框。在发现期间，管理中心会在网络中搜索尚未列出的所有可见计算机。找到新计算机后，管理中心会尝试检测是否存在客户端。当发现完成时，管理中心会显示已检测到的所有计算机并在**状态**列显示这些计算机的状态。在发现操作之后，计算机可能处于以下某种状态：

- **已查找（无客户端/设备）：**已检测到计算机，但不存在客户端/设备。如果已安装客户端/设备，但之前已将其激活且已针对客户端/设备启动的通信进行配置，则计算机也可能处于此状态。由于从客户端/设备的单向通信，管理中心将无法知道客户端/设备的状态。在这种情况下，您必须停用计算机上的客户端/设备并从管理中心重新激活它。
- **已发现（需要激活）：**客户端已安装且正在侦听来自管理中心的通信，但尚未激活。此状态也可能表示客户端/设备已安装且正在侦听，已被激活但尚未受管理中心管理。如果此管理中心曾经管理该客户端/设备，但客户端/

设备的公共证书已不再位于管理中心的数据库中，可能发生这种情况。如果计算机已从管理中心移除，之后又被发现时，可能会出现这种情况。要在此计算机上开始管理客户端/设备，请右键单击计算机并选择“激活/重新激活”。一旦重新激活，状态将更改为“联机”。

- **已发现（需要停用）**：客户端/设备已安装且正在侦听，但已由其他管理中心激活。在这种情况下，必须先停用客户端/设备，然后再由此管理中心进行激活。
- **已查找（未知）**：已检测到计算机，但无法确定客户端/设备是否存在。

注意： *查找操作将仅检查新发现的计算机的状态。要更新已列出的计算机的状态，请右键单击已选定的计算机并选择**操作 > 检查状态**。*

注意： *在发现计算机时，您可以指定要将发现的计算机添加到的计算机组。根据您已选择的组织计算机组的方式，创建名为“新找到的计算机”或“在网络区段 X 上新找到的计算机”（如果要扫描多个网络区段）的计算机组可能会很方便。然后，您便可以将已发现的计算机基于其属性移到其他计算机组并将其激活。*

注意： *在启用了**自动将 IP 解析为主机名**选项的情况下运行查找操作时，查找操作可能会找到趋势科技服务器深度安全防护系统管理中心无法找到的主机名。发现可以回退为使用 WINS 查询或 NetBIOS 广播解析主机名（除 DNS 外）。趋势科技服务器深度安全防护系统管理中心仅支持通过 DNS 查找主机名。*

注意： *查找操作不会查找 vCenter 中作为虚拟机运行的计算机。 查找操作不会查找 Microsoft Active Directory 中的计算机。*

添加目录

趋势科技服务器深度安全防护系统管理中心可以连接到 Microsoft Active Directory 并与之同步。有关从 Active Directory 导入计算机列表的详细说明，请参阅 **Active Directory**。

添加 VMware vCenter

趋势科技服务器深度安全防护系统管理中心支持与 VMware vCenter 和 ESXi Server 的紧密集成。您可以从 vCenter 和 ESXi 节点导入组织和操作信息，并允许对企业的 VMware 基础架构应用详细的安全。有关从 VMware 系统导入虚拟计算机的详细说明，请参阅 **VMware vCenter**。

添加云帐户

趋势科技服务器深度安全防护系统可以连接到 Amazon EC2、VMware vCloud 和 Microsoft Azure 服务提供的计算机（虚拟机或物理计算机）并对其进行管理。有关从云提供程序添加计算机的详细说明，请参阅**云帐户**。

搜索计算机

使用**搜索**文本框在已发现的（即已列出的）计算机中搜索特定的计算机。对于更复杂的搜索选项，请使用下面的“高级搜索”选项。

高级搜索功能（搜索不区分大小写）：

- **包含**：选定列中的条目包含该搜索字符串
- **不包含**：选定列中的条目不包含该搜索字符串
- **等于**：选定列中的条目完全符合该搜索字符串

- **不等于**：选定列中的条目并不完全符合该搜索字符串
- **在范围内**：选定列中的条目与其中的一个逗号分隔的搜索字符串条目完全匹配
- **不在范围内**：选定列中的条目并未与任意逗号分隔的搜索字符串条目完全匹配

导出选定的计算机

将计算机列表导出到 XML 或 CSV 文件。当需要备份计算机信息、将其与其他报告系统相集成或者将计算机迁移到其他趋势科技服务器深度安全防护系统管理中心时，您可能希望执行此操作。（这会为您省去从新的管理中心重新发现和扫描计算机的麻烦。）

注意： *导出的计算机文件不包括任何已分配的策略、防火墙规则、防火墙状态配置或入侵防御规则。为了导出此配置信息，请使用**策略**页面中的“策略导出”选项。*

激活/重新激活计算机上的客户端/设备

当计算机未受管理时，只有激活客户端/设备才能使计算机进入受管状态。客户端/设备在激活之前处于下列状态之一：在**计算机**页面中，右键单击要激活/重新激活其客户端/设备的计算机，然后从**操作**菜单中选择“激活/重新激活”。（或者，可以在计算机的**详细信息**窗口中单击**激活**或**重新激活**按钮。）

- **无客户端/设备**：指明缺省端口上没有正在运行或侦听的客户端/设备。“无客户端/设备”状态也可能表示客户端/设备已安装且正在运行，但正在配合另一个管理中心工作，并且通信已配置为“客户端/设备已启动”，因此，客户端/设备没有侦听此管理中心。（如果要更正后面这种情况，必须在该计算机上停用客户端。）
- **需要激活**：客户端/设备已安装且正在侦听，已准备好由管理中心激活。
- **需要重新激活**：客户端/设备已安装且正在侦听，正在等待由管理中心重新激活。
- **需要停用**：客户端/设备已安装且正在侦听，但已由其他管理中心激活。
- **未知**：已导入计算机（位于已导入计算机列表中）但未导入其状态信息，或者已通过 LDAP 目录查找过程添加计算机。

客户端/设备在成功激活后，状态将变成“联机”。如果激活不成功，计算机状态将显示“激活不成功”，同时在括号中注明不成功原因。单击此链接会显示系统事件，以提供激活不成功的详细原因。

注意： *虽然趋势科技服务器深度安全防护系统 8 及较早版本的客户端和设备支持 IPv6，但缺省情况下已阻止此功能。要允许在趋势科技服务器深度安全防护系统 8 客户端和设备上进行 IPv6 通信，请转至策略编辑器或计算机编辑器中的**设置 > 网络引擎**选项卡的**高级网络引擎设置**区域，然后将**对 8.0 及更高版本的客户端和设备阻止 IPv6** 选项设置为**否**。*

检查计算机的状态

此命令检查计算机的状态，而不尝试执行扫描或激活。

停用计算机上的客户端/设备

您可能需要在两个趋势科技服务器深度安全防护系统管理中心安装之间转移计算机的控制权。如果这样，必须停用客户端/设备，随后再由新的管理中心重新激活客户端/设备。可以从当前管理该客户端的管理中心停用客户端/设备。*也可以直接在计算机上从命令行停用客户端。还可以直接在 ESXi Server 控制台上通过选择“重置设备”来停用设备。*

向计算机发送更新策略

当您使用趋势科技服务器深度安全防护系统管理中心更改计算机上的客户端/设备的配置（应用新的入侵防御规则、更改日志记录设置等）时，趋势科技服务器深度安全防护系统管理中心必须将新的信息发送给该客户端/设备。这是一个“发送策略”指令。策略更新通常会立刻执行，但也可以通过单击**发送策略**来强制执行更新。

下载安全更新

此命令从已配置的中继下载最新安全更新到客户端/设备。

获取事件

覆盖正常事件检索时间表（通常在发出每个波动信号时），并立即从计算机检索事件日志。

清除警告/错误

使用此命令可清除计算机的所有警告和错误。此命令在以下情况下非常有用：

- 计算机的客户端已在本地重置
- 在您有机会停用或从计算机列表中删除此计算机之前，此计算机已经从网络中移除。

升级计算机上的客户端/设备软件

要升级客户端或设备，首先需要将较新版本的客户端或设备软件包导入 趋势科技服务器深度安全防护系统管理中心。可以从“趋势科技下载专区”（如下文所述）导入客户端或设备软件包，或者将软件从本地目录手动导入管理中心（请参阅*本地软件（第 197页）*）。

要将软件包从“下载专区”导入趋势科技服务器深度安全防护系统：

1. 转至**管理** > **更新**> **软件** > **下载专区**。此页列出了趋势科技下载专区上的所有可用软件包。已经导入 趋势科技服务器深度安全防护系统管理中心的软件包在**导入**列中有一个绿色复选标记（）。它们也列在**管理** > **更新**> **软件** > **本地**选项卡上。已过期的软件包在**导入**列中有  。
2. 要更新已过期的软件包，请右键单击软件包名称并单击**导入**。

导入软件包后，即可使用它来升级一个或多个客户端或设备。

升级客户端/设备：

1. 在**计算机**页面上，右键单击要升级其客户端或设备的计算机，然后选择**操作** > **升级客户端/设备软件**。
2. 如果没有合适平台及版本（版本必须高于客户端/设备版本）的安装程序，将显示以下消息：“没有可用于选定的计算机平台或版本的认证客户端/设备软件安装程序。在升级趋势科技服务器深度安全防护系统客户端/设备之前，请使用**管理** > **更新** > **软件**页面上的**下载专区**或**本地**面板，添加适当的客户端/设备软件安装程序。否则，将显示“升级客户端/设备软件包”对话框。在该对话框中，选择要安装的客户端/设备版本并指定何时进行升级。您可以选择立即升级客户端/设备，或者选择**使用升级时间表**并指定趋势科技服务器深度安全防护系统检查并安装升级客户端/设备软件的频率。

注意： *在极少数情况下，计算机可能需要重新启动才能完成升级。如果是这样，将会触发警报。要立刻查明是否需要重新启动计算机，请检查“已升级客户端软件”或“已升级虚拟设备”事件的文本，查看平台安装程序是否指示需要重新启动。*

注意： *必须手动解除“需要重新启动”警报，该警报不会自动解除。*

注意： *趋势科技服务器深度安全防护系统虚拟设备使用 Red Hat Enterprise Linux 6（64 位）软件包。将虚拟设备导入趋势科技服务器深度安全防护系统管理中心时，Red Hat 客户端也将被导入。激活计算机上的虚拟设备时，趋势科技服务器深度安全防护系统会升级 Red Hat 客户端至趋势科技服务器深度安全防护系统管理中心中的最新版本。不可以删除最新版的 Red Hat 客户端，除非首先移除所有虚拟设备软件包。只能删除未在使用的 Red Hat 客户端旧版本。*

漏洞扫描（推荐设置）

趋势科技服务器深度安全防护系统管理中心可以扫描计算机并随后针对安全规则提出建议。可以在各种**规则**页面的计算机**详细信息**窗口中看到“漏洞扫描（推荐设置）”结果。请参阅**计算机详细信息**窗口的文档，以获取更多信息。

清除建议

清除在该计算机上执行“漏洞扫描（推荐设置）”后生成的规则建议。这也会移除在执行“漏洞扫描（推荐设置）”后生成的警报中列出的相应计算机。

注意： *此操作不会取消分配根据以往建议分配的任何规则。*

完整扫描恶意软件

在选定的计算机上执行完整的恶意软件扫描。完整扫描采取的处理措施取决于此计算机上生效的**恶意软件手动扫描配置**。有关更多信息，请参阅*恶意软件扫描配置（第 63页）*。

快速扫描恶意软件

扫描关键系统区域中当前活动的威胁。快速扫描将查找当前活动的恶意软件，但是不会执行深度文件扫描以查找休眠文件或存储的受感染文件。在较大的驱动器中，它的速度明显快于完整扫描。

注意： *快速扫描仅按需提供。无法作为预设任务的一部分预设快速扫描。*

扫描计算机上有无打开的端口

扫描打开的端口在所有选定的计算机上执行端口扫描，检查计算机上安装的客户端，以确定客户端的状态是“需要停用”、“需要激活”、“要求重新激活客户端”还是“联机”。（缺省情况下，扫描操作扫描端口 1-1024。您可以在**策略/计算机编辑器 > 设置 > 扫描**中更改此范围。）

注意： *无论端口范围设置如何，会始终扫描端口 4118。管理中心启动的通信发送到计算机上的这个端口。如果计算机的通信方向设置为“客户端/设备已启动”（**策略/计算机编辑器 > 设置 > 计算机 > 通信方向**），会关闭端口 4118。*

注意： *将不会检测网络上的新计算机。要查找新计算机，必须使用**发现**工具。*

取消当前正在执行的所有端口扫描操作

如果启动对许多台计算机和/或很大范围内的端口的一系列端口扫描，并且扫描已花费很长的时间，使用此选项可取消扫描。

扫描完整性

完整性监控跟踪对计算机系统和文件所做的更改。方法是创建基线并随后执行定期扫描以将计算机的当前状态与基线做比较。有关详细信息，请参阅**完整性监控**页面的文档。

重新生成完整性基线

在此计算机上为完整性监控重新生成基线。

将计算机移到计算机组

要将计算机移到新的计算机组，请右键单击该计算机并选择**操作** > **移动到组...**

将策略分配给计算机

随后会打开一个包含下拉列表的窗口，可在其中将策略分配给计算机。**计算机**页面上的**策略**列会显示分配给计算机的策略的名称。

注意： *如果将其他设置应用到计算机（例如，添加其他防火墙规则或修改防火墙状态配置设置），策略的名称将会使用粗体，表示缺省设置已更改。*

分配资产值

通过资产值，您可以按重要性对计算机和事件进行排序。各个安全规则都有一个严重性值。触发计算机上的规则时，将规则的严重性值与计算机的资产值相乘。该值可用于按重要性对事件进行排序。有关详细信息，请参阅**管理** > **系统设置** > **排序**。

分配中继组

要为此计算机选择中继组以从其下载更新，请右键单击此计算机，然后选择**处理措施** > **分配中继组...**。

删除计算机

如果要删除计算机，将一并删除与该计算机有关的所有信息。如果重新查找计算机，则必须重新分配策略以及之前分配的任何规则。

检查与计算机关联的事件

检查与计算机关联的系统事件和安全方面的事件。

添加新的计算机组

从组织角度来看，创建计算机组非常有用，这会加快应用和管理策略的过程。右键单击要在其下创建新计算机组的计算机组，然后选择**添加组**。

添加从 Microsoft Active Directory 结构导入的计算机和计算机组

通过从基于 LDAP 的目录（例如，Microsoft Active Directory）导入来发现计算机。已根据目录中的结构导入并同步计算机。有关更多信息，请参阅**添加计算机**。

移除组

仅当计算机组不包含任何计算机且没有子组时，才可以将其移除。

将计算机从当前组移到其他组

您可以将计算机从一个计算机组移到另一个计算机组，但请记住，策略是在计算机级别上而不是计算机组级别上应用的。将计算机从一个计算机组移到另一个计算机组不会影响分配给该计算机的策略。

查看或编辑计算机组的属性

组的属性包括组的名称和描述。

注意： *此页面上介绍的一些功能仅在相应模块启用之后才会出现。例如，当单击**计算机**页面上的**操作**时，仅在防恶意软件和完整性监控模块启用后才会显示**完整扫描恶意软件**和**扫描完整性更改**。*

策略

策略

“策略”页面会在分层树结构中显示现有策略，这些策略可显示其父/子关系。

- *策略（第 43页）*

通用对象

“通用对象”页面列出了在整个趋势科技服务器深度安全防护系统中可供许多构造（如策略和规则）共享的对象。这可以被视为共享对象的根存储库。策略编辑器窗口和计算机编辑器窗口会显示对象的同一个列表，但可针对策略或特定计算机覆盖这些通用对象的属性。有关如何在策略或计算机级别继承和覆盖通用对象属性的更多信息，请参阅**策略、继承和覆盖**。

规则

“规则”页面会列出现有防护模块规则（针对使用规则的这些模块）。

- *防火墙规则（第 70页）*
- *入侵防御规则（第 73页）*
- *完整性监控规则（第 78页）*
- *日志审查规则（第 82页）*

列表

- *目录列表（第 45页）*
- *文件扩展名列表（第 48页）*
- *文件列表（第 49页）*
- *IP 列表（第 52页）*
- *MAC 列表（第 53页）*
- *端口列表（第 54页）*

其他

- *上下文（第 57页）*
- *防火墙状态配置（第 59页）*
- *恶意软件扫描配置（第 63页）*
- *时间表（第 55页）*
- *标记（第 56页）*

策略

策略允许保存规则和配置设置集合，以更方便地将其分配给多台计算机。

策略页面会在分层树结构中显示现有策略。在“策略”页面上，您可以执行以下操作：

- 从头开始创建**新**策略 ()
- 从 XML 文件（位于**新建**菜单下）**导入**策略 ()

注意： *导入策略时，请确保您创建策略的系统和将接收这些策略的系统都具有最新的安全更新。如果接收策略的系统运行的是较旧的安全更新，则它可能不具备最新系统的策略中所引用的某些规则。*

- 检查或修改现有策略的**详细信息** ()
- **复制**（然后修改并重新命名）现有策略 ()
- **删除**策略 ()
- 将策略**导出**到 XML 文件 ()

注意： *将选定的策略导出到 XML 时，策略所拥有的任何子策略都将包含在导出的数据包内。导出的数据包包含与策略相关联的所有实际对象，以下各项除外：入侵防御规则、日志审查规则、完整性监控规则和应用程序类型。*

单击**新建** () 会打开**策略**向导，该向导会提示您输入新策略的名称，然后提供用于打开**策略详细信息窗口**的选项。单击**详细信息** () 可显示**策略详细信息**窗口。

注意： *您可以基于计算机的“漏洞扫描（推荐设置）”来创建新策略。要执行此操作，请选择一台计算机，然后运行“漏洞扫描（推荐设置）”。（在**计算机**页面上右键单击该计算机，然后选择**处理措施 > 漏洞扫描（推荐设置）**）。扫描完成后，请返回至**策略**页面，然后单击**新建**，以显示**新建策略**向导。出现提示时，选择在“现有计算机的当前配置”上建立新策略。然后，从计算机的属性中选择“建议的应用程序类型和入侵防御规则”、“建议的完整性监控规则”和“建议的日志审查规则”。*

注意： *策略将仅包含计算机上建议的元素，而不会考虑当前将哪些规则分配给了该计算机。*

将策略分配给计算机：

1. 在趋势科技服务器深度安全防护系统管理中心中，转至**计算机**。
2. 从计算机列表中选择计算机，右键单击并选择**处理措施 > 分配策略**。
3. 从层次结构树中选择策略，然后单击**确定**。

有关如何使用策略保护计算机的更多信息，请参阅**快速入门：保护服务器**。

有关层次结构树中的子策略如何继承或覆盖父策略的设置和规则的更多信息，请参阅**策略、继承和覆盖**。

将策略分配给计算机之后，您仍应该在计算机上运行定期“漏洞扫描（推荐设置）”，以确保计算机上的所有漏洞均受到保护。有关更多信息，请参阅**漏洞扫描（推荐设置）**。

通用对象

通用对象包括：

- *目录列表（第 45页）*
- *文件列表（第 49页）*
- *文件扩展名列表（第 48页）*
- *IP 列表（第 52页）*
- *MAC 列表（第 53页）*
- *端口列表（第 54页）*
- *上下文（第 57页）*
- *防火墙状态配置（第 59页）*
- *时间表（第 55页）*
- *标记（第 56页）*
- *防火墙规则（第 70页）*
- *入侵防御规则（第 73页）*

目录列表

目录列表是可重用的目录列表。

在主页面上可以执行下列操作：

- 从头开始创建**新建目录列表**（）
- **从文件导入**（）可从 XML 文件导入扫描目录列表
- 查看或修改现有目录列表的**属性**（）
- **复制**（然后修改）现有的目录列表（）
- **删除**目录列表（）
- 将一个或多个目录列表**导出**（）到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列**（） 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建**（）或**属性**（）将显示目录列表**属性**窗口。

目录列表属性

常规信息

目录列表的名称和描述。

目录

键入要出现在列表上的目录。每一行只输入一个目录。

支持的格式

注意： *包含目录设置接受正斜杠 "/" 或反斜杠 "\"，以同时支持 Windows 和 Linux 惯例。*

下表介绍了可用于定义目录列表的语法：

目录	格式	描述	示例
目录	DIRECTORY	包含指定目录中的所有文件以及所有子目录中的所有文件。	*C:\Program Files* 包含 "Program Files" 目录以及所有子目录中的所有文件。
网络资源	\\NETWORK RESOURCE	包含作为目标计算机上的网络资源包含在内的计算机上的文件。	*\\12.34.56.78* *\\some-comp-name* 包含使用 IP 或主机名标识的网络资源上的所有文件。 *\\12.34.56.78\somefolder* *\\some-comp-name\somefolder*

目录	格式	描述	示例
			包含使用 IP 或主机名标识的网络资源上的文件夹 "somefolder" 中的所有文件。
包含通配符 (*) 的目录	DIRECTORY*\	包含具有任意子目录名称的所有子目录，但不包含指定目录中的文件。	*C:\abc** 包含所有 "abc" 子目录中的所有文件，但不包含 "abc" 目录中的文件。 *C:\abc\wx*z* *匹配：* C:\abc\wxz\ C:\abc\wx123z\ *不匹配：* C:\abc\wxz C:\abc\wx123z *C:\abc*wx* *匹配：* C:\abc\wx\ C:\abc\123wx\ *不匹配：* C:\abc\wx C:\abc\123wx
包含通配符 (*) 的目录	DIRECTORY*	包含具有匹配名称的所有子目录，但不包含该目录以及所有子目录中的文件。	*C:\abc** *匹配：* C:\abc\ C:\abc\1 C:\abc\123 *不匹配：* C:\abc C:\abx\ C:\xyz\ *C:\abc*wx* *匹配：* C:\abc\wx C:\abc\123wx *不匹配：* C:\abc\wx\ C:\abc\123wx\ *C:\abc\wx*z* *匹配：* C:\abc\wxz C:\abc\wx123z *不匹配：* C:\abc\wxz\ C:\abc\wx123z\ *C:\abc\wx** *匹配：* C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\

目录	格式	描述	示例
			C:\abc\wxz\ *不匹配：* C:\abc\wx123z\
环境变量	${ENV VAR}	包含由格式为 ${ENV VAR} 的环境变量定义的所有文件和子目录。对于虚拟设备，必须在**系统设置 > "计算机"选项卡 > 环境变量覆盖**中定义环境变量的值对。	***${windir}*** 如果该变量解析为 "c:\windows"，请包含 "c:\windows" 及其所有子目录中的所有文件。
注释	DIRECTORY # 注释	允许您向包含定义添加注释。	*c:\abc #Include the abc directory*

已分配给

已分配给选项卡列出使用此目录列表的规则。单击规则名称会显示其**属性**窗口。

文件扩展名列表

文件扩展名列表页面包含**恶意软件扫描配置**使用的一系列文件扩展名。例如，多个恶意软件扫描配置可以使用一列文件扩展名来将带有这些扩展名的文件包括在扫描中。多个恶意软件扫描配置也可以使用另一列文件扩展名从扫描中排除带有这些扩展名的文件。

在主页面上可以执行下列操作：

- 从头开始创建**新建文件扩展名列表** ()
- **从文件导入** () 可从 XML 文件导入扫描文件扩展名
- 查看或修改现有文件扩展名列表的**属性** ()
- **复制**（然后修改）现有的文件扩展名列表 ()
- **删除**文件扩展名列表 ()
- 将一个或多个文件扩展名列表**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建** () 或**属性** () 显示文件扩展名列表**属性**窗口。

文件扩展名列表属性

常规信息

文件扩展名列表的名称和描述。

文件扩展名

键入要出现在列表上的文件扩展名。每一行只输入一个扩展名。

已分配给

已分配给选项卡列出使用此文件扩展名列表的规则。单击规则名称会显示其**属性**窗口。

文件列表

文件列表是可重用的文件列表。

常规

使用**文件列表**部分可以创建可重复使用的有效文件列表。在主页面上可以执行下列操作：

- 从头开始创建**新建文件列表** ()
- **从文件导入** () 可从 XML 文件导入扫描文件
- 查看或修改现有文件列表的**属性** ()
- **复制**（然后修改）现有的文件列表 ()
- **删除**文件列表 ()
- 将一个或多个文件列表**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建** () 或**属性** () 将显示文件列表**属性**窗口。

文件列表属性

常规信息

文件列表的名称和描述。

文件

键入要出现在列表上的文件。每一行只输入一个文件名。

支持的格式

注意： *包含设置接受正斜杠 "/" 或反斜杠 "\"，以同时支持 Windows 和 Linux 惯例。*

下表介绍了可用于定义文件列表包含的语法：

包含	格式	描述	示例
文件	FILE	包含具有指定文件名的所有文件，无论这些文件位于何位置或目录。	*abc.doc* 包含所有目录中名为 "abc.doc" 的所有文件。不包含 "abc.exe"。
文件路径	FILEPATH	包含由文件路径指定的特定文件。	*C:\Documents\abc.doc* 仅包含 "Documents" 目录中名为 "abc.doc" 的文件。

包含	格式	描述	示例
包含通配符 (*) 的文件	FILE*	包含文件名中具有匹配特征码的所有文件。	*abc*.exe* 包含前缀为 "abc" 且扩展名为 ".exe" 的所有文件。 **.db* *匹配：* 123.db abc.db *不匹配：* 123db 123.abd cbc.dba **db* *匹配：* 123.db 123db ac.db acdb db *不匹配：* db123 *wxy*.db* *匹配：* wxy.db wxy123.db *不匹配：* wxydb
包含通配符 (*) 的文件	FILE.EXT*	包含文件扩展名中具有匹配特征码的所有文件。	*abc.v** 包含文件名为 "abc" 且扩展名以 ".v" 开头的所有文件。 *abc.*pp* *匹配：* abc.pp abc.app *不匹配：* wxy.app *abc.a*p* *匹配：* abc.ap abc.a123p *不匹配：* abc.pp *abc.** *匹配：* abc.123 abc.xyz *不匹配：* wxy.123

包含	格式	描述	示例
包含通配符 (*) 的文件	FILE*.EXT*	包含文件名及扩展名中具有匹配特征码的所有文件。	*a*c.a*p* *匹配：* ac.ap a123c.ap ac.a456p a123c.a456p *不匹配：* ad.aa
环境变量	${ENV VAR}	包含由格式为 ${ENV VAR} 的环境变量指定的文件。可以使用**系统设置 > "计算机" 选项卡 > 环境变量覆盖**来定义或覆盖这些文件。	*${myDBFile}* 包含文件 "myDBFile"。
注释	FILEPATH # 注释	允许您向包含定义添加注释。	*C:\Documents\abc.doc #This a comment*

已分配给

已分配给选项卡列出使用此文件列表的文件名称。单击文件列表名称会显示其**属性**窗口。

IP 列表

使用 **IP 列表**页面可创建可重复使用的 IP 地址列表，供多个防火墙规则使用。
在主页面上可以执行下列操作：

- 从头开始创建**新的** IP 列表 ()
- 从 XML 文件**导入** () IP 列表
- 查看或修改现有 IP 列表的**属性** ()
- **复制**（然后修改）现有的 IP 列表 ()
- **删除** IP 列表 ()
- 将一个或多个 IP 列表**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）

单击**新建** () 或属性 () 显示 IP 列表**属性**窗口。

IP 列表属性

常规信息

IP 列表的名称和描述。

IP

键入要出现在列表上的 IP 地址、屏蔽的 IP 地址及 IP 地址范围。每行只输入这些地址中的一个。

支持的格式

除了单个地址外，您还可以输入 IP 范围和屏蔽的 IP。请参考下列示例来正确设置条目的格式。（在文本的前面加上井号 ("#")，便可以在 IP 列表中插入注释。）

已分配给

已分配给选项卡列出使用此 IP 列表的规则。单击规则名称会显示其**属性**窗口。

MAC 列表

使用 **MAC 列表**部分可以创建可重用的 MAC 地址列表。
在主页面上可以执行下列操作：

- 从头开始创建**新的** () MAC 列表
- 从 XML 文件**导入** () MAC 列表
- 查看或修改现有 MAC 列表的**属性** ()
- **复制**（然后修改）现有的 MAC 列表 ()
- **删除** MAC 列表 ()
- 将一个或多个 MAC 列表**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）

单击**新建** () 或属性 () 显示 MAC 列表**属性**窗口。

MAC 列表属性

常规信息

列表的名称和描述。

MAC

键入要出现在列表上的 MAC 地址。每行只输入这些地址中的一个。

支持的格式

MAC 列表支持使用连字符 (-) 和冒号分隔格式的 MAC 地址。请参考下列示例来正确设置条目的格式。（在文本的前面加上井号 ("#")，便可以在 MAC 列表中插入注释。）

已分配给

已分配给选项卡列出使用此 MAC 列表的规则。单击规则名称会显示其**属性**窗口。

端口列表

使用**端口列表**页面可创建可重复使用的端口列表。
在主页面上可以执行下列操作：

- 从头开始创建**新的**端口列表 ()
- 从 XML 文件**导入** () 端口列表
- 查看或修改现有端口列表的**属性** ()
- **复制**（然后修改）现有的端口列表 ()
- **删除**端口列表 ()
- 将一个或多个端口列表**导出** () 到 XML 或 CSV 文件。（使用**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）

单击**新建** () 或**属性** () 将显示端口列表**属性**窗口。

端口列表属性

常规信息

列表的名称和描述。

端口

键入要出现在列表上的端口。每行只输入这些地址中的一个。

注意： *有关普遍接受的端口分配的列表，请访问 Internet Assigned Numbers Authority (IANA)*

支持的格式

列表上可以包含单个端口和端口范围。请参考下列示例来正确设置条目的格式。（在文本的前面加上井号 ("#")，便可以在端口列表中插入注释。）

已分配给

已分配给选项卡列出使用此端口列表的规则。单击规则名称会显示其**属性**窗口。

时间表

时间表是可重用的时间表。

从工具栏或右键单击快捷方式菜单，您可以：

- 从头开始创建**新的**时间表 ()
- 从 XML 文件**导入** () 时间表
- 查看或修改现有时间表的**属性** ()
- **复制**（然后修改）现有的时间表 ()
- **删除**时间表 ()
- 将一个或多个时间表**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）

单击“新建”() 或属性 () 显示“时间表属性”窗口。

时间表属性

时间表期间是由以小时为单位的时间块定义的。单击某个时间块可以选择该时间块，按住 Shift 单击可取消选择。

已分配给

已分配给选项卡显示使用此时间表的规则的列表。

标记

利用事件标记，管理员可以使用预定义的标签（“攻击”、“可疑”、"patch"、“可接受的更改”、“误报”、“高优先级”等）手动标记事件并可以定义定制标签（“分配给 Tom 进行检查”等）。

除了手动标记事件外，还可以使用“可信计算机”（对于管理完整性监控事件尤其有用）实现自动事件标记。例如，Patch 的推出计划可应用于可信计算机，与 Patch 应用相关联的事件可标记为 "Patch X"，其他系统上提出的类似事件可自动视为“可接受的更改”，从而减少需要由管理员分析的事件数量。

事件标记启用专门的事件视图、控制板和报告，并应用于单个事件、类似事件，甚至应用于将来出现的所有类似事件。

标记

所有当前已定义的标记将显示在**策略** > **通用对象** > **其他** > **标记**页面中。这包括预定义标记和定制标记。（仅显示当前使用的标记。）

删除标记：删除标记将从与其关联的所有事件中移除该标记。

自动标记规则

自动标记规则是通过选择事件以及标记类似的项目创建的。

有关事件标记步骤的信息，请参阅**事件标记**。

上下文

上下文是根据计算机网络环境实施不同安全策略的强大途径。

上下文与防火墙规则和入侵防御规则相关联。如果满足了上下文中定义的与规则相关的条件，则应用此规则。（要使安全规则与上下文相关联，请转至安全规则的**属性**窗口上的**选项**选项卡，并从“上下文”下拉式菜单中选择“上下文”。）

上下文可以用来向客户端提供“位置感知”。为了判断计算机的位置，上下文会检查计算机与其域控制器的连接性质及其 Internet 连接。选择**上下文在域控制器连接是以下情况时应用**选项并从以下选项中进行选择：

- **本地连接到域：**仅在计算机可以直接连接到其域控制器时，选择该项
- **远程连接到域：**如果计算机只可通过 VPN 连接到其域控制器，选择该项
- **未连接到域：**在计算机无法连接到其域控制器时，选择该项
- **未连接到域，无 Internet 连接：**如果计算机无法通过任何方式连接到其域控制器并且该主机无 Internet 连接，选择该项。（可以在**管理 > 系统设置 > 上下文**中配置 Internet 连接测试。）

评估计算机与其域控制器或 Internet 连接的能力之后，客户端就可以实施规则，例如：限制 HTTP 流量仅到达非可路由的（“专用”）IP 地址。

注意： 对于使用上下文实施防火墙规则的策略的示例，请检查“位置感知 — 高”策略的属性。

从工具栏或**上下文**页面上的右键单击快捷方式菜单，您可以：

- 从头开始创建**新的**() 上下文
- **从 XML 文件导入** () 上下文（位于**新建**菜单下。）
- 查看或修改现有上下文的**属性** ()
- **复制**（然后修改）现有的上下文 ()
- **删除**上下文 ()
- 将一个或多个上下文**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建**() 或属性 () 显示上下文**属性**窗口。

上下文属性：

常规信息

上下文规则的名称和描述，以及与该规则兼容的趋势科技服务器深度安全防护系统客户端的最早版本。

选项

上下文在域控制器是以下情况时应用

在此处指定选项将根据计算机与其域控制器或 Internet 连接的能力来确定防火墙规则是否有效。（可以在**管理 > 系统设置 > 上下文**中配置 Internet 连接的测试条件。）

如果可以直接连接域控制器（通过 ICMP），则该连接是“本地”。如果只能通过 VPN 连接，则该连接是“远程 (VPN)”。

域控制器连接测试的时间间隔与 Internet 连接的测试间隔一样，也可以在**管理 > 系统设置 > 上下文**中配置。

注意： *仅在计算机无法连接到其域控制器时，才会执行 Internet 连接测试。*

上下文应用于接口隔离受限接口

该上下文将应用于通过使用接口隔离来限制流量的网络接口。（主要用于允许或强制允许防火墙规则。）

已分配给

已分配给选项卡显示使用此上下文的规则的列表。

防火墙状态配置

趋势科技服务器深度安全防护系统的防火墙状态配置机制会根据网络通信历史记录、TCP 和 IP 标头值的正确性以及 TCP 连接状态转换情况分析每个数据包。如果使用无状态协议（例如 UDP 和 ICMP），则会根据网络通信历史记录分析而实施虚拟状态机制。状态机制处理数据包的方式如下：

1. 如果静态防火墙规则条件允许数据包通过，数据包会传递至状态例程；
2. 检查数据包以判断数据包是否属于现有连接；
3. 检查 TCP 标头的正确性（例如，序列号、标志组合等）。

注意： ICMP 状态过滤仅在趋势科技服务器深度安全防护系统客户端版本 8 或更早版本中可用。

通过**防火墙状态配置**页面可以定义多个状态检查配置，然后，您可以将这些配置加入策略。在工具栏或快捷方式菜单中可以执行下列操作：

- 从头开始创建**新的** () 防火墙状态配置
- 从 XML 文件（位于**新建**菜单下）**导入** () 防火墙配置。
- 查看或修改现有防火墙状态配置的**属性** ()
- **复制** ()（然后修改）现有的防火墙状态配置
- **删除**防火墙状态配置 ()
- 将一个或多个防火墙状态配置**导出** () 到 XML 或 CSV 文件。（使用**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建** () 或**属性** () 显示**防火墙状态配置属性**窗口。

防火墙状态配置属性

常规信息

- **名称：**防火墙状态配置的名称。
- **描述：**键入防火墙状态配置的描述。此描述只会出现在这里。

IP 数据包检查

- **拒绝所有的传入片段化数据包：**如果启用此选项，则会丢弃所有片段化数据包，并写入以下日志条目："IP fragmented packet"。如果存在总长度小于 IP 标头长度的数据包，则该规则就会出现例外：以静默方式丢弃这些数据包。
  攻击者有时会创建并发送片段化数据包，以企图绕开防火墙规则。

注意： *缺省情况下，防火墙引擎会对片段化数据包执行一系列检查。这是缺省行为，不能重新配置。存在以下特征的数据包将被丢弃：*

- ***无效的片段标志/偏移量：**当 IP 标头中的 DF 或 MF 标志设为 1 时，或者当标头包含设为 1 的 DF 标志和不是 0 的 Offset 值时，就会丢弃数据包。*
- ***第一个片段太小：**如果数据包的 MF 标志设为 1、Offset 值是 0，并且总长度小于 120 字节（最大合计标头长度），就会丢弃数据包。*
- ***IP 片段超出界限：**如果数据包的 Offset 标志值和数据包合计长度超过数据报的最大大小 65535 字节，就会丢弃数据包。*
- ***IP 片段偏移量太小：**如果数据包的 Offset 标志不是零，且包含一个小于 60 字节的值，就会丢弃数据包。*

TCP

TCP 数据包检查

- **拒绝包含 CWR 和 ECE 标志的 TCP 数据包：**网络堵塞时会设置这些标志。

注意： *RFC 3168 规定需要将保留文本框的六位中的两位用于 ECN（显式堵塞通知），如下所述：*

- *位 8 到 15：CWR-ECE-URG-ACK-PSH-RST-SYN-FIN*
- *TCP 标头标志位名称参考：*
  - *位 8：CWR（堵塞窗口已减小）[RFC3168]*
  - *位 9：ECE (ECN-Echo) [RFC3168]*

数据包自动传输（例如拒绝服务攻击所产生的传输等）通常会生成设置这些标志的数据包。

- **启用 TCP 状态检查：** 在 TCP 级别启用状态检查。如果启用状态 TCP 检查，将提供下列选项：
  - **启用 TCP 状态日志记录：** 将记录 TCP 状态检查事件。
  - **将来自单台计算机的传入连接数限制为：**限制来自单台计算机的连接数可降低拒绝服务攻击的影响。

    注意： *传入连接数限制仅在趋势科技服务器深度安全防护系统客户端 8 或更早版本中可用。*

  - **将指向单台计算机的传出连接数限制为：**限制指向单台计算机的传出连接数可以大幅降低 Nimda 型蠕虫病毒的影响。

    注意： *传出连接数限制仅在趋势科技服务器深度安全防护系统客户端 8 或更早版本中可用。*

  - **将来自单台计算机的半开连接数限制为：** 在此处设置一个限制可以防止您受到 SYN Flood 之类的 DoS 攻击。虽然大多数服务器都有超时设置可用于关闭半开连接，但在此处设置一个值可以避免半开连接成为重大问题。如果达到指定的 SYN-SENT（远程）条目限制，就会丢弃来自该特定计算机的后续 TCP 数据包。

    注意： *半开连接数限制仅在趋势科技服务器深度安全防护系统客户端 8 或更早版本中可用。*

注意： *在确定要允许的来自单台计算机的开放连接数时，您可以根据目前使用的协议类型，确定您认为来自单台计算机的半开连接的合理数目，再确定能承担的且不会造成系统堵塞的单台计算机半开连接数，然后在这两个数之间选择一个合理的数字。*

- **在已确认的数据包数超过以下数值时启用 ACK 风暴防护：**设置此选项以记录已发生 ACK 风暴攻击的事件。
  - **检测到 ACK 风暴时断开连接：**设置此选项以在检测到此类攻击时断开连接。

注意： *ACK 风暴防护选项仅在趋势科技服务器深度安全防护系统客户端 8 或更早版本中可用。*

FTP 选项

以下 FTP 选项仅在趋势科技服务器深度安全防护系统客户端 8 或更早版本中可用。

- **主动 FTP**
  - **允许传入：**当此计算机充当服务器时允许主动 FTP。
  - **允许传出：**当此计算机充当客户端时允许主动 FTP。
- **被动 FTP**
  - **允许传入：**当此计算机充当服务器时允许被动 FTP。
  - **允许传出：**当此计算机充当客户端时允许被动 FTP。

UDP

- **启用 UDP 状态检查：** 选中该复选框可对 UDP 网络通信启用状态检查。

注意： *UDP 状态机制会丢弃未经请求的传入 UDP 数据包。对于每个传出 UDP 数据包，规则会更新其 UDP“状态”表，然后仅允许在提出请求后 60 秒内发出的 UDP 响应。如果要允许特定的传入 UDP 网络通信，必须创建**强制允许**规则。例如，如果运行 DNS 服务器，则只有创建**强制允许**规则，才能让传入 UDP 数据包到达目标端口 53。*

如果没有对 UDP 网络通信执行状态检查，攻击者可能会伪装成 DNS 服务器，然后从源端口 53 向防火墙后面的计算机发送未经请求的 UDP“响应”。

- **启用 UDP 状态日志记录：** 选中此选项将启用对 UDP 状态检查事件的日志记录。

ICMP

注意： *ICMP 状态检查仅在趋势科技服务器深度安全防护系统客户端版本 8 或更早版本中可用。*

- **启用 ICMP 状态检查：** 选中该选项将对 ICMP 网络通信启用状态检查。

注意： *ICMP（假）状态机制会丢弃未经请求的传入 ICMP 数据包。对于每个传出 ICMP 数据包，规则都会创建或更新其 ICMP“状态”表，然后仅允许在提出请求后 60 秒内发出的 ICMP 响应。（支持的 ICMP 对类型：类型 0 和 8、13 和 14、15 和 16、17 和 18。）*

例如，在启用状态 ICMP 检测后，可以只在已发送回显请求时才允许 ICMP 回显响应。未经请求的 Echo 响应可能代表各种攻击的迹象，包括 Smurf 扩大攻击、主机与守护程序之间的 Tribe Flood Network 通信，或 Loki 2 后门。

- **启用 ICMP 状态日志记录：** 选中此选项将对 ICMP 状态检查事件启用日志记录。

已分配给

已分配给选项卡可列出使用此状态检查配置的策略和计算机。

恶意软件扫描配置

趋势科技服务器深度安全防护系统允许您创建各种恶意软件扫描配置，以自动处理执行恶意软件检测的方式。配置选项包括：要扫描哪些文件、实时执行扫描还是根据预设执行扫描，以及检测到恶意软件时执行哪些处理措施。通过此页面，您可以定义全局恶意软件扫描配置。在策略和计算机级别上设置这些配置在计算机上生效的方式、组合及时间。此外，与趋势科技服务器深度安全防护系统中的大多数元素一样，许多全局设置可以在策略和计算机级别进行覆盖。（有关更多信息，请参阅**策略、继承和覆盖**。）

存在以下两种恶意软件扫描配置：**实时扫描**和**手动/预设扫描**。虽然大多数的操作适用于这两种类型的扫描，但是有些操作（如**拒绝访问**）仅适用于实时扫描，而其他选项（如 **CPU 使用率**）仅适用于手动/预设扫描。

在全局**恶意软件扫描配置**页面上，您可以执行以下操作：

- 创建**新的** () 实时或手动/预设扫描配置
- 从 XML 文件**导入** () 现有的扫描配置（位于**新建**菜单下）。
- 查看恶意软件扫描配置的**属性** ()。
- **复制** ()（然后修改）现有的文件配置。
- 从配置列表中**删除** () 突出显示的配置文件。
- 将已显示的或已选定的配置**导出** () 到 XML 或 CSV 文件。
- 从显示中**添加或删除列** ()。
- **搜索** () 特定配置文件。

属性

常规

常规信息

- 恶意软件扫描配置的名称和描述，以及这是实时扫描还是手动/预设扫描类型。

扫描设置

- **要扫描的目录：**指定要对其扫描恶意软件的目录。您可以扫描**所有目录**或从定义的**目录列表**中进行选择。
- **要扫描的文件：**指定要对其扫描恶意软件的文件。在**所有文件**和**由 IntelliScan 扫描的文件类型**之间进行选择，或从定义的**文件扩展名列表**（会扫描使用列表中定义的扩展名的所有文件）中进行选择。

> *注意：* *IntelliScan 仅扫描易于感染的文件类型（如 .zip 或 .exe）。IntelliScan 不依靠文件扩展名来确定文件类型，而是读取文件的标头和/或内容来确定是否应扫描它。相比于扫描所有文件，使用 IntelliScan 可以减少要扫描的文件总数，从而增强了性能。*

排除

允许您排除对特定目录、文件及文件扩展名的扫描。例如，如果要为 Microsoft Exchange Server 创建恶意软件扫描配置，则应该排除 SMEX 隔离文件夹以避免重新扫描已确认为恶意软件的文件。

注意： *扫描排除目录设置接受正斜杠 "/" 或反斜杠 "\"，以同时支持 Windows 和 Linux 惯例。*

下表介绍了可用于定义目录列表排除的语法：

排除	格式	描述	示例
目录	DIRECTORY	排除指定目录中的所有文件以及所有子目录中的所有文件。	*C:\Program Files* 排除 "Program Files" 目录以及所有子目录中的所有文件。
包含通配符 (*) 的目录	DIRECTORY*\	排除具有任意子目录名称的所有子目录，但不排除指定目录中的文件。	*C:\abc** 排除所有 "abc" 子目录中的所有文件，但不排除 "abc" 目录中的文件。 *C:\abc\wx*z* *匹配:* C:\abc\wxz\ C:\abc\wx123z\ *不匹配:* C:\abc\wxz C:\abc\wx123z *C:\abc*wx* *匹配:* C:\abc\wx\ C:\abc\123wx\ *不匹配:* C:\abc\wx C:\abc\123wx
包含通配符 (*) 的目录	DIRECTORY*	排除具有匹配名称的所有子目录，但不排除该目录以及所有子目录中的文件。	*C:\abc** *匹配:* C:\abc\ C:\abc\1 C:\abc\123 *不匹配:* C:\abc C:\abx\ C:\xyz\ *C:\abc*wx* *匹配:* C:\abc\wx C:\abc\123wx *不匹配:* C:\abc\wx\ C:\abc\123wx\ *C:\abc\wx*z* *匹配:* C:\abc\wxz

排除	格式	描述	示例
			C:\abc\wx123z *不匹配:* C:\abc\wxz\ C:\abc\wx123z\ *C:\abc\wx** *匹配:* C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\ C:\abc\wxz\ *不匹配:* C:\abc\wx123z\
环境变量	${ENV VAR}	排除由格式为 ${ENV VAR} 的环境变量定义的所有文件和子目录。对于虚拟设备，必须在**策略/计算机编辑器 > 设置 > 计算机 > 环境变量覆盖**中定义环境变量的值对。	*${windir}* 如果该变量解析为 "c:\windows"，请排除 "c:\windows" 及其所有子目录中的所有文件。
注释	DIRECTORY #注释	允许您向排除定义添加注释。	*c:\abc #Exclude the abc directory*

下表介绍了可用于定义文件列表排除的语法：

排除	格式	描述	示例
文件	FILE	排除具有指定文件名的所有文件，无论这些文件位于何位置或目录。	*abc.doc* 排除所有目录中名为 "abc.doc" 的所有文件。不排除 "abc.exe"。
文件路径	FILEPATH	排除由文件路径指定的特定文件。	*C:\Documents\abc.doc* 仅排除 "Documents" 目录中名为 "abc.doc" 的文件。
包含通配符 (*) 的文件	FILE*	排除文件名中具有匹配特征码的所有文件。	*abc*.exe* 排除前缀为 "abc" 且扩展名为 ".exe" 的任何文件。 *.db* *匹配:* 123.db abc.db *不匹配:* 123db 123.abd cbc.dba **db* *匹配:* 123.db 123db ac.db acdb db *不匹配:* db123

排除	格式	描述	示例
			wxy.db* *匹配：* wxy.db wxy123.db *不匹配：* wxydb
包含通配符 (*) 的文件	FILE.EXT*	排除文件扩展名中具有匹配特征码的所有文件。	*abc.v** 排除文件名为 "abc" 且扩展名以 ".v" 开头的任何文件。 *abc.*pp* 匹配： abc.pp abc.app *不匹配：* wxy.app *abc.a*p* *匹配：* abc.ap abc.a123p *不匹配：* abc.pp *abc.** *匹配：* abc.123 abc.xyz *不匹配：* wxy.123
包含通配符 (*) 的文件	FILE*.EXT*	排除文件名及扩展名中具有匹配特征码的所有文件。	*a*c.a*p* *匹配：* ac.ap a123c.ap ac.a456p a123c.a456p *不匹配：* ad.aa
环境变量	${ENV VAR}	排除由格式为 ${ENV VAR} 的环境变量指定的文件。可以使用**系统设置 > "计算机" 选项卡 > 环境变量覆盖**来定义或覆盖这些文件。	*${myDBFile}* 排除文件 "myDBFile"。
注释	FILEPATH #注释	允许您向排除定义添加注释。	*C:\Documents\abc.doc #This a comment*

下表介绍了可用于定义文件扩展名列表排除的语法：

排除	格式	描述	示例
文件扩展名	EXT	排除文件扩展名匹配的所有文件。	*doc* 排除所有目录中扩展名为 ".doc" 的所有文件。
注释	EXT #Comment	允许您向排除定义添加注释。	*doc #This a comment*

下表包含可用于定义进程镜像文件列表排除（仅限实时扫描）的语法：

排除	格式	描述	示例
文件路径	FILEPATH	排除文件路径指定的特定进程镜像文件。	*C:\abc\file.exe* 仅排除 "abc" 目录中文件名为 "file.exe" 的文件。

操作

可识别的恶意软件

检测时

通过选择**使用 ActiveAction 确定的处理措施**选项，可以指示趋势科技服务器深度安全防护系统自动决定在检测到恶意软件时采取哪些处理措施。

> *注意：* *ActiveAction 是为每种恶意软件类别优化的一组预定义清理处理措施。趋势科技不断调整 ActiveAction 中的处理措施以确保正确处理各个检测。ActiveAction 扫描处理措施会随病毒码的更新而更新。*

下表列出了选择 ActiveAction 时采取的处理措施：

恶意软件类型	实时扫描	手动/预设扫描	注意
病毒	清除	清除	病毒可以通过插入恶意代码感染正常文件。通常，只要打开受感染的文件，恶意代码就会自动运行，除了感染其他文件外，还会传送有效载荷。一些更常见的病毒类型包括 COM 和 EXE 感染源、宏病毒和引导扇区病毒。
特洛伊木马	隔离	隔离	特洛伊木马是没有文件感染能力的非感染可执行恶意文件。
加壳软件	隔离	隔离	加壳软件是压缩和/或加密后的可执行程序。为避开检测，恶意软件作者通常打包经多层压缩和加密的现有恶意软件。防恶意软件检查可执行文件以查找与恶意软件关联的压缩特征码。
间谍软件（灰色软件）	隔离	隔离	虽然可能合法，但是灰色软件会表现出与间谍软件类似且可能不需要的行为。
可能的恶意软件	不予处理	不予处理	检测为可能是恶意软件的文件通常是未知的恶意软件组件。缺省情况下，将记录下这些检测，并且文件将匿名发送回趋势科技，供分析使用。
Cookie	N/A	删除	Cookie 是 Web 浏览器存储的文本文件。Cookie 包含与站点相关的数据，如身份验证信息和站点首选项。Cookie 不是可执行文件，因此不受感染；但它们可以用作间谍软件。即使是从合法 Web 站点发送的 Cookie 也可用于恶意目的。
其他威胁	清除	清除	“其他威胁”类别包括显示错误通知或操控屏幕行为但通常无害的恶作剧程序。

或者，可以手动指定希望趋势科技服务器深度安全防护系统在检测到恶意软件时采取的处理措施。趋势科技服务器深度安全防护系统在遇到受感染文件时，会采取以下五种可能的处理措施：

1. **不予处理：**允许完全访问受感染文件，不对文件执行任何操作。（仍将记录防恶意软件事件。）
2. **清除：**在允许完全访问文件之前清除可清除的文件。（不适用于“可能的恶意软件”。）
3. **删除：**删除受感染文件。
4. **拒绝访问：**仅可在实时扫描期间执行此扫描处理措施。当趋势科技服务器深度安全防护系统检测到某操作尝试打开或执行受感染文件时，会立即阻止该操作。如果在执行手动或预设扫描期间应用已选定“拒绝访问”选项的恶意软件扫描配置，则将应用“不予处理”处理措施，并记录防恶意软件事件。
5. **隔离：**将文件移动到计算机或虚拟设备上的隔离目录中。（隔离后，您可以将文件下载到选定位置。有关更多信息，请参阅**防恶意软件 > 隔离的文件**。）

可能的恶意软件

选择在文件被确定为可能的恶意软件时采取的处理措施。可能的恶意软件是显示可疑特性但无法分类为特定恶意软件变种的文件。如果将此选项的设置保留为“缺省”，将采取在**检测时**（上面）中选定的处理措施。检测到可能的恶意软件时，趋势科技建议您联系支持提供商获取帮助以进一步分析文件。

选项

常规选项

- **启用间谍软件/灰色软件扫描：**间谍软件扫描引擎会扫描间谍软件/灰色软件，并执行**处理措施**选项卡上指定的处理措施。
- **扫描压缩文件：**指定在什么条件下扫描文件以及是否扫描压缩文件。
  - **从中提取文件的最大压缩级别：** 文件或文件组可以进行多层压缩。通过此选项，可以指定希望趋势科技服务器深度安全防护系统扫描的压缩级别数。
  - **单个提取文件的最大大小：**要扫描的压缩归档中各个文件的最大大小。

    注意： 扫描采用多层压缩的大型文件可能会影响性能。

  - **要提取的文件的最大数量：**要从压缩归档中提取并扫描的文件的最大数量。
- **扫描嵌入式 Microsoft Office 对象：**某些 Microsoft Office 版本使用对象链接和嵌入 (OLE) 将文件和其他对象插入到 Office 文件中。这些嵌入的对象可能包含恶意代码。由于嵌入的对象可能包含其他对象，因此在单个 Office 文件中可能存在多个嵌入层。为减轻对性能的影响，可以选择仅扫描每个文件中几个嵌入对象层。
  - **扫描 Microsoft Office 对象中的入侵代码：**试探性入侵检测可通过检查 Microsoft Office 文件中是否存在入侵代码来识别恶意软件。

注意： 指定的层数同时适用于 OLE 对象和扫描入侵代码选项。

- **启用 IntelliTrap（仅实时）：**病毒制造者经常尝试通过使用实时压缩算法来避开病毒过滤。IntelliTrap 可阻止实时压缩的可执行文件并将它们与其他恶意软件特征进行配对，以帮助减少此类病毒进入网络的风险。（IntelliTrap 仅在实时模式下起作用。）

注意： 因为 IntelliTrap 会将此类文件识别为安全风险，且可能会不正确地阻止安全文件，所以请在启用 IntelliTrap 时考虑隔离（而非删除或清除）文件。如果用户定期交换实时压缩的可执行文件，请禁用 IntelliTrap。IntelliTrap 使用以下防恶意软件组件：病毒扫描引擎、IntelliTrap 特征码、IntelliTrap 例外特征码。

- **启用网络目录扫描（仅实时）：**要扫描网络共享和映射网络驱动器中的文件和文件夹，请启用此选项。

注意： 在 "~/.gvfs" 中通过 GVFS（GNOME 桌面可用的虚拟文件系统）访问的资源将被视为本地资源，而非网络驱动器。

- **文件扫描时间（仅实时）：**在仅当打开文件进行读取时扫描和打开文件进行读写时扫描间进行选择。
- **CPU 使用率（仅手动/预设扫描）：**指定分配给扫描的 CPU 资源。
  - **高：**逐个扫描文件而不暂停
  - **中：**建议使用；在整体 CPU 使用率超过 50% 时暂停
  - **低：**在整体 CPU 使用率超过 20% 时暂停

警报

选择在此恶意软件扫描配置触发事件时是否引发警报。

已分配给

指明正在使用此特定恶意软件扫描配置的策略和计算机。

防火墙规则

防火墙规则会检查单个数据包中的控制信息。然后，根据这些页面中定义的规则来阻止或允许数据包。防火墙规则直接分配到计算机，或分配到策略再转而分配到计算机或计算机组。

注意： *Solaris 客户端将仅检查 IP 帧类型的数据包，Linux 客户端将仅检查 IP 或 ARP 帧类型的数据包。将允许其他帧类型的数据包通过。请注意，虚拟设备没有这些限制，可以检查所有帧类型，而不管它所保护的虚拟机是什么操作系统。*

防火墙规则图标：

-  常规防火墙规则
-  根据时间表运行的防火墙规则

在主页面上可以执行下列操作：

- 从头开始创建**新的** () 防火墙规则
- 从 XML 文件（位于**新建**菜单下）**导入** () 防火墙规则。
- 查看或修改现有防火墙规则的**属性** ()
- **复制**（然后修改）现有的防火墙规则 ()
- **删除**防火墙规则 ()
- 将一个或多个防火墙规则**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

注意： *无法删除已分配给一台或多台计算机或属于策略的防火墙规则。*

单击**新建** () 或属性 () 显示**防火墙规则属性**窗口。

防火墙规则属性

常规信息

- **名称：** 防火墙规则的名称。
- **描述：** 防火墙规则的详细描述。
- **操作：**防火墙规则有四种不同的行为方式。下面按照优先级对此进行说明：
  1. 网络通信可以完全**绕开**防火墙。这是一个特殊规则，可造成数据包完全绕开防火墙和入侵防御引擎。对于不需要过滤的媒体密集协议，可使用此设置。要了解**放行**规则的更多信息，请参阅**参考**一节中的“放行规则”。
  2. 它可以是**仅记录**。这意味着它只会在日志中写入条目，而不干扰网络通信。
  3. 它可以**强制允许**定义的网络通信（将允许此规则所定义的网络通信，但*不*排除其他任何网络通信）。
  4. 它可以**拒绝**网络通信（拒绝此规则定义的网络通信）。

5. 它可以**允许**网络通信（将*单方面* 允许此规则所定义的网络通信）。

> *注意：* *如果计算机上没有任何**允许**规则生效，除非被**拒绝**规则特别阻止，否则将允许所有流量。一旦创建了单个**允许**规则，就会阻止所有其他网络通信，除非满足**允许**规则的要求。此情况有一个例外：除非**拒绝**规则明确阻止 ICMPv6 网络通信，否则始终允许该网络通信。*

> *注意：* *对于任何特定的数据包只会应用一个规则操作，优先级相同的规则按上述顺序应用。*

- **优先级**：如果选择“强制允许”、“拒绝”或“仅记录”作为规则操作，则可以在此处设置 0（低）到 4（最高）的优先级。设置优先级可让您结合规则操作实现一系列规则效果。**仅记录**规则的优先级只能是 4，而**允许**规则的优先级只能是 0。

> *注意：* *优先级确定规则的应用顺序。先应用高优先级的规则，然后应用低优先级的规则。例如，在对数据包应用优先级为 2 的端口 80 传入强制允许规则之前，优先级为 3 的端口 80 传入拒绝规则会丢弃该数据包。*

- **数据包流向**：选择此规则是要应用到**传入**还是**传出**网络通信。
- **帧类型**：选择帧类型。使用**非**复选框可指定是要过滤该帧类型，还是过滤除该帧类型以外的*其他任何*类型。

> *注意：* *您可以仅选择 IPv4 或 IPv6。要指定其中之一（两者），请选择 IP。*

> *注意：* *有关帧类型的列表，请访问 Internet Assigned Numbers Authority (IANA) Web 站点。*

- **协议**： 选择或指定规则查找的协议。使用此复选框可指定是要过滤该协议，还是过滤除该协议以外的*其他任何*协议。

> *注意：* *您可以从预定义的常用协议下拉列表中选择，也可以选择“其他”，然后自行输入协议代码（介于 0 和 255 之间的三位数十进制值）。*

数据包源

下列选项适用于数据包标头的源信息：

- **IP**：指定 IP 地址、屏蔽的 IP 地址和 IP 范围，或从您在 **IP 列表**页面中定义的 IP 列表中选择 IP 列表。
- **MAC**：指定 MAC 地址，或从您在 **MAC 列表**页面中定义的 MAC 列表中选择 MAC 列表。
- **端口**：您可以在端口选项中指定逗号分隔的端口列表或短划线分隔的端口范围，以及单个端口（例如 80、443、1-100），或从您在**端口列表**页面中定义的端口列表中选择端口列表。

数据包目标

下列选项适用于数据包标头的目标信息：

- **IP**：指定 IP 地址、屏蔽的 IP 地址和 IP 范围，或从您在 **IP 列表**页面中定义的 IP 列表中选择 IP 列表。
- **MAC**：指定 MAC 地址，或从您在 **MAC 列表**页面中定义的 MAC 列表中选择 MAC 列表。
- **端口**：您可以在端口选项中指定逗号分隔的端口列表或短划线分隔的端口范围，以及单个端口（例如 80、443、1-100），或从您在**端口列表**页面中定义的端口列表中选择端口列表。

特定标志

如果在以上“常规信息”一节中选择了 TCP、ICMP 或 TCP+UDP 作为协议，您可以指示防火墙规则观察特定的标志。

事件

根据此规则选择是否启用或禁用日志记录事件。如果启用事件日志记录，则可以使用事件记录数据包数据。

注意： *请注意，任何形式的允许规则（允许、强制允许和绕开）都不会记录任何事件，因为它们会塞满数据库。*

选项

警报

选择此防火墙规则是否在触发时触发警报。如果只要在特定时间段激活此规则，请在下拉列表中指定某个预设时间。

注意： *只能将“操作”设置为“拒绝”或“仅记录”的防火墙规则配置为触发警报。（这是因为警报是由计数器触发的，而计数器会随着日志文件中数据的增加而递增。）*

时间表

选择是否应只在预设时间段激活防火墙规则。

注意： *只在预设时间活动的防火墙规则显示于**防火墙规则**页面时，其图标上方有一个小时钟（  ）。*

注意： *通过基于客户端的防护，时间表使用与端点操作系统相同的时区。对于无客户端防护，时间表使用与趋势科技服务器深度安全防护系统虚拟设备相同的时区。*

上下文

规则上下文是根据计算机网络环境实施不同安全策略的强大途径。上下文最常用于创建以下策略：该策略根据计算机（通常是便携式计算机）是在办公室内还是办公室外应用不同的防火墙和入侵防御规则。

上下文与防火墙规则和入侵防御规则相关联。如果满足了上下文中定义的与规则相关的条件，则应用此规则。

为了确定计算机的位置，上下文会检查计算机与其域控制器连接的性质。有关上下文的更多信息，请参阅**策略** > **通用对象** > **其他** > **上下文**。

注意： *对于使用上下文实施防火墙规则的策略的示例，请查看“Windows 便携式计算机”策略的属性。*

已分配给

此选项卡显示含有此防火墙规则的策略列表，以及此防火墙规则直接分配到的所有计算机。可以在**策略**页面上将防火墙规则分配给策略；可以在**计算机**页面上将防火墙规则分配给计算机。

入侵防御规则

防火墙规则和防火墙状态配置会检查数据包的控制信息（用来描述数据包的数据），而入侵防御规则会检查数据包的实际内容（以及数据包的序列）。然后根据入侵防御规则中设置的条件，对这些数据包采取各种操作：例如，替换明确定义的或可疑的字节序列、完全丢弃数据包和重置连接。

入侵防御规则图标：

-  常规入侵防御规则
-  根据时间表运行的入侵防御规则
-  具有配置选项的入侵防御规则

通过**入侵防御规则**页面，可以创建和管理入侵防御规则。从工具栏或右键单击快捷方式菜单，您可以：

- 从头开始创建**新的**入侵防御规则 ()
- 从 XML 文件（位于**新建**菜单下）**导入** () 入侵防御规则。
- 查看或修改现有入侵防御规则的**属性** ()
- **复制**（然后修改）现有入侵防御规则 ()
- **删除**入侵防御规则 ()
- 将一个或多个入侵防御规则**导出** () 到 XML 或 CSV 文件。（使用**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建** () 或**属性** () 显示**入侵防御规则属性**窗口。

注意： *请注意**配置**选项卡。无法通过趋势科技服务器深度安全防护系统管理中心直接编辑趋势科技的入侵防御规则。如果入侵防御规则需要（或允许）配置，则**配置**选项卡上会提供这些配置选项。可以编辑您自己编写的定制入侵防御规则，在这种情况下，会显示**规则**选项卡。*

入侵防御规则属性

常规信息

- **名称：**入侵防御规则的名称。
- **描述：**入侵防御规则的描述。
- **最低客户端/设备版本：**实施此入侵防御规则所需的趋势科技服务器深度安全防护系统客户端/设备的最低版本。

详细信息

- **应用程序类型：**对此入侵防御规则进行分组所依据的应用程序类型。您可以选择现有的类型，也可以创建新的类型。

> *注意：* *您还可以从这个面板编辑现有的类型。记住，如果在此处编辑现有的应用程序类型，则更改会应用到所有使用该应用程序类型的安全元素。*

- **优先级：**入侵防御规则的优先级级别。先应用高优先级的规则，然后应用低优先级的规则。
- **严重性：**规则的严重性设置不会影响执行或应用规则的方式。当查看入侵防御规则列表时，严重性级别可作为排序条件。更重要的是，每个严重性级别都与一个严重性值相关联；将此值乘以计算机的资产值以确定事件的排序。（请参阅**管理 > 系统设置 > 排序**。）
- **CVSS 分数：**一种评估漏洞严重性程度的标准，由美国国家漏洞数据库计算。
- **仅检测：**测试新的规则时，请使用此复选框。如果选中此复选框，该规则就会创建一个前缀为文字“仅检测：”的日志条目，但不影响网络通信。如果在下一个面板中设置“禁用日志记录”复选框（见下文），则不管是否选中“仅检测”，都不会记录规则的活动。

> *注意：* *一些入侵防御规则设计为只在“仅检测”模式下运行，无法将其配置为阻止流量。对于这些规则，将选中并锁定“仅检测”选项，以使其无法更改。*

事件

- **禁用事件日志记录：**选中该选项可禁用事件日志记录。
  - **在数据包丢弃时生成事件：**记录数据包丢弃/阻止活动。
  - **始终包含数据包数据：**在日志条目中包含数据包数据。
  - **启用调试模式：**记录触发该规则的数据包前后的多个数据包。趋势科技建议只在技术支持提供商指示您这样做的时候才使用此选项。

标识（仅对趋势**科技**规则显**示**）

- **类型：**可以是“智能”（一个或多个已知和未知的（零时差）漏洞）、“入侵”（特定入侵，通常以签名为基础）或“漏洞”（可能遭受一种或多种入侵的特定漏洞）。
- **发布时间：**规则发布的日期（不是下载日期）。
- **最近更新时间：**上次在本地或安全更新下载期间修改规则的时间。
- **标识符：**规则的唯一标识符标记。

漏洞（仅对趋势**科技**规则显**示**）

显示此特定漏洞的相关信息。适用时，将显示通用安全漏洞评分系统 (CVSS)。（有关此评分系统的信息，请参考美国国家漏洞数据库上的 CVSS 页面。）

配置（仅对趋势**科技**规则显**示**）

- **配置选项：**如果下载的规则有任何可配置选项，则会显示在此处。示例选项包括标头长度、允许的 HTTP 扩展名、cookie 长度等。如果您应用规则时未设置必需的选项，则会触发警报，通知您需要配置哪台（哪些）计算机上的哪个规则。（这也适用于通过安全更新下载和自动应用的所有规则。）

> *注意：* *有配置选项的入侵防御规则显示于**入侵防御规则**页面中时，其图标上方有一个小的复选标记（  ）。*

查看规则（仅对定制入侵防御规则可用）

查看规则... 按钮将对趋势科技尚未标记为机密的入侵防御规则可用。（有关自行编写入侵防御规则的信息，请与趋势科技联系。）

选项

警报

选择此入侵防御规则是否在触发时触发警报。如果只要在特定时间段激活此规则，请在下拉列表中指定某个预设时间。

时间表

选择是否应只在预设时间段激活入侵防御规则。

注意：	*只在预设时间活动的入侵防御规则显示于**入侵防御规则**页面时，其图标上方有一个小时钟（  ）。*

注意：	*通过基于客户端的防护，时间表使用与端点操作系统相同的时区。对于无客户端防护，时间表使用与趋势科技服务器深度安全防护系统虚拟设备相同的时区。*

上下文

上下文是根据计算机网络环境实施不同安全策略的强大途径。上下文最常用于创建以下策略：该策略根据计算机（通常是便携式计算机）是在办公室内还是办公室外应用不同的防火墙和入侵防御规则。

上下文与防火墙规则和入侵防御规则相关联。如果满足了上下文中定义的与规则相关的条件，则应用此规则。

为了确定计算机的位置，上下文会检查计算机与其域控制器连接的性质。有关上下文的更多信息，请参阅**策略 > 通用对象 > 其他 > 上下文**。

建议选项

使用该选项将此入侵防御规则从在执行完“漏洞扫描（推荐设置）”后提出的规则建议中排除。

已分配给

这个选项卡显示了为其分配了此入侵防御规则的计算机和策略的列表。

应用程序类型

根据通信方向、所用协议以及通信通过的端口来确定应用程序类型定义的应用程序。应用程序类型很适合用来将入侵防御规则分组。可以使用它们将用途相同的入侵防御规则进行分组。这样就可以更轻松地选择一组入侵防御规则，以将它们分配给计算机。例如，假设在保护流向 Oracle Report Server 的 HTTP 网络通信时需要一组入侵防御规则。将这些入侵防御规则分组到应用程序类型后，就能轻松地在 "Web Server Common" 和 "Web Server Oracle Report Server" 组合中选择规则，同时，比如说，还能排除 IIS 服务器专用的一组规则。

应用程序类型图标：

-  没有配置选项的应用程序类型
-  具有配置选项的应用程序类型

在主页面上可以执行下列操作：

1. 定义**新的** () 应用程序类型
2. 从 XML 文件（位于**新建**菜单下）**导入** () 应用程序类型。
3. 查看或编辑现有应用程序类型的**属性** ()
4. **复制**（然后修改）现有的应用程序类型 ()
5. 将一个或多个应用程序类型**导出** () 到 XML 或 CSV 文件。（使用**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）
6. **删除** ()应用程序类型
7. **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建** () 或**属性** () 显示应用程序类型**属性**窗口。

常规

常规信息

应用程序类型的名称和描述。“最低客户端/设备版本”指明了支持此应用程序类型所需的趋势科技服务器深度安全防护系统客户端/设备的版本。

连接

- **方向：**启动通信的方向。也就是在两台计算机之间建立连接的第一个数据包的方向。例如，如果要为 Web 浏览器定义应用程序类型，您应该选择“传出”，因为发送第一个数据包给服务器以建立连接的是 Web 浏览器（即使您只需要检查从服务器到浏览器的网络通信传递，也是如此）。可编写与特定应用程序类型关联的入侵防御规则，以检查向任一方向传递的单个数据包。
- **协议：**该应用程序类型应用到的协议。
- **端口：**此应用程序类型监控的端口（*不是*网络通信专用端口。）

配置

配置选项卡显示的选项控制与该应用程序类型关联的入侵防御规则的行为。例如，"Web Server Common" 应用程序类型具有“监控来自 Web 服务器的响应”选项。如果取消选定此选项，与该应用程序类型关联的入侵防御规则将不会检查源端口 80 上的响应通信。

选项

选项选项卡中的项目控制趋势科技服务器深度安全防护系统管理中心使用和应用应用程序类型的方式。例如，大多应用程序类型都有从“漏洞扫描 (推荐设置)”中排除自身的选项。这意味着，如果选中“从建议中排除”选项，“漏洞扫描 (推荐设置)”将不对计算机建议此应用程序类型及其关联的入侵防御规则，即使检测到此类应用程序也是如此。

已分配给

已分配给选项卡列出与该应用程序类型关联的入侵防御规则。

完整性监控规则

完整性监控规则允许趋势科技服务器深度安全防护系统客户端扫描和检测对计算机的文件、目录、注册表项及其值所做的更改，以及对已安装软件、进程、侦听端口和运行的服务所做的更改。这些更改会作为事件记录在管理中心中，并与任何其他事件一样可配置以生成警报。可将完整性监控规则直接分配给计算机，或将其制作为策略的一部分。

完整性监控规则指定要监控其更改的实体（文件、注册表项、服务等）。趋势科技服务器深度安全防护系统会扫描由分配给计算机的规则指定的所有实体，并创建用于与将来的计算机扫描相比较的基线。如果将来的扫描与此基线不一致，趋势科技服务器深度安全防护系统管理中心会记录完整性监控事件并触发警报（如果已这样配置）。

完整性监控规则图标：

-  常规完整性监控规则
-  具有配置选项的完整性监控规则

在主页面上可以执行下列操作：

- 从头开始创建**新的**完整性监控规则 ()
- 从 XML 文件**导入** () 完整性监控规则
- 查看或修改现有完整性监控规则的**属性** ()
- **复制**（然后修改）现有完整性监控规则 ()
- **删除**完整性监控规则 ()
- 将一个或多个完整性监控规则**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）

注意： *无法删除已分配给一台或多台计算机或属于策略的完整性监控规则。*

单击**新建** () 或属性 () 显示**完整性监控规则属性**窗口。

完整性监控规则属性

常规信息

完整性监控规则的名称和描述，以及使该规则正常运行所需的客户端和趋势科技服务器深度安全防护系统管理中心的最低版本（如果该规则由趋势科技发布）。

详细信息

规则的严重性设置不会影响执行或应用规则的方式。当查看完整性监控规则列表时，严重性级别可作为排序条件。更重要的是，每个严重性级别都与一个严重性值相关联；将此值乘以计算机的资产值以确定事件的排序。（请参阅**管理 > 系统设置 > 排序**。）

标识

首次发布规则以及上次更新规则的日期，以及规则的唯一标识符。

内容

注意： *内容选项卡仅针对您自己创建的完整性监控规则显示。而趋势科技发布的完整性监控规则具有一个显示完整性监控规则配置选项（如果有）的**配置**选项卡。趋势科技发布的完整性监控规则不可编辑（然而可对其进行复制，然后再编辑副本）。*

您可以选择以下三种模板之一来创建新的完整性规则：**注册表值**模板、**文件**模板或**定制 (XML)** 模板。使用**注册表值**模板创建监控注册表值的更改的完整性监控规则。使用**文件**模板创建仅监控文件的更改的简单完整性监控 AddeAddAdded 日志审查规则。使用**定制 (XML)** 模板以 XML 格式编写监控目录、注册表值、注册表项、服务、进程、已安装软件、端口（以及文件）的规则。

帮助的此部分介绍了如何使用**注册表值**和**文件**模板。有关使用定制 (XML) 模板以 XML 格式编写完整性监控规则的信息，请参阅**参考**部分中的**完整性监控规则语言**。

注册表值模板

基本键

选择要监控的基本项以及是否监控子项的内容。

值名称

列出要包含或排除的值名称。可以使用 "?" 和 "*" 作为通配符。

属性

使用“标准”监控大小或内容的更改。有关其他属性，请参阅**参考**一节中“完整性规则语言”下的 *RegistryValueSet*。

文件模板

基本目录

指定规则的基本目录。关于此规则的其他所有信息都是相对于该目录的。选择“包含子目录”可包含子目录。例如，有效条目为 `C:\Program Files\MySQL` 并选择“包含子目录”。

文件名

使用**文件名**文本框来包含或排除特定文件。可以使用通配符（"?" 用于代替单个字符，"*" 用于代替零个或多个字符）。

注意： *这些文本框可保留为空，用于监控基本目录中的所有文件，但是，如果目录中有很多和/或很大的文件，这对系统资源要求很高。*

属性

可监控以下文件属性的更改：

- **Created**：创建文件的时间戳。
- **LastModified**：上次修改文件的时间戳。
- **LastAccessed**：上次访问文件的时间戳在 Windows 上，不会立即更新此值，并且记录上次访问的时间戳会因性能增强而遭到禁用。有关详细信息，请参阅文件时间。扫描文件需要客户端打开该文件，这将更改其上次访问时间戳。在 Unix 上，客户端在打开文件时将使用 O_NOATIME 标志（如果可用），这将防止操作系统更新上次访问时间戳并可以加快扫描的速度。
- **Permissions**：在 Windows 上，是文件的安全描述符，格式为 SDDL；或在支持 ACL 的 Unix 系统上，是 Posix 样式的 ACL，否则将会是数字（八进制）格式的 Unix 样式 rwxrwxrwx 文件权限。
- **Owner**：文件所有者的用户 ID（在 Unix 上通常指 "UID"）。
- **Group**：文件所有者的组 ID（在 Unix 上通常指 "GID"）。
- **Size**：文件的大小。
- **Sha1**：SHA-1 哈希。
- **Sha256**：SHA-256 哈希。
- **Md5**：MD5 哈希。
- **Flags**：仅限 Windows。由 GetFileAttributes() Win32 API 返回的标志。Windows 资源管理器将以下内容称为文件的“属性”：只读、已归档、已压缩等。
- **SymLinkPath**（仅限 Unix）：如果文件是符号链接，则链接的路径存储在此处。Windows NTFS 支持类似于 Unix 的符号链接，但仅限目录，并不包括文件。Windows 快捷方式对象不是真的符号链接，因为它们不由操作系统来处理；Windows 资源管理器处理快捷方式文件 (*.lnk)，但是打开 *.lnk 文件的其他应用程序将看到 lnk 文件的内容。
- **InodeNumber**（仅限 Unix）：文件的 inode 编号。
- **DeviceNumber**（仅限 Unix）：存储与文件相关的 inode 的磁盘的设备号。
- **BlocksAllocated**（仅限 Unix）：已分配用于存储文件的块的数量。

您可以使用速记关键字 "STANDARD" 来查找以下项的更改：

- Created
- LastModified
- Permissions
- Owner
- Group
- Size
- Contents
- Flags（仅限 Windows）
- SymLinkPath（仅限 Unix）

选项

- **此规则记录事件时发出警报**：如果触发了规则，则触发警报。
- **允许实时监控**：缺省情况下，选择此选项。如果未选择此选项，将仅在扫描更改时生成完整性监控事件。

已分配给

显示含有此完整性监控规则的策略列表，以及此完整性监控规则直接分配到的所有计算机。可以在**策略**页面上将完整性监控规则分配给策略；可以在**计算机**页面上将完整性监控规则分配给计算机。

日志审查规则

OSSEC 日志审查引擎集成在趋势科技服务器深度安全防护系统趋势科技服务器深度安全防护系统客户端中，并为趋势科技服务器深度安全防护系统提供了对计算机上运行的操作系统和应用程序生成的日志和事件进行审查的功能。可将日志审查规则直接分配给计算机，或使其成为策略的一部分。与完整性监控事件类似，可以将日志审查事件配置为在趋势科技服务器深度安全防护系统管理中心生成警报。

日志审查图标：

-  常规日志审查规则
-  具有配置选项的日志审查规则

在主页面上可以执行下列操作：

- 从头开始创建**新的** () 日志审查规则
- 从 XML 文件**导入** () 日志审查规则
- 查看或修改现有日志审查规则的**属性** ()
- **复制**（然后修改）现有日志审查规则 ()
- **删除**日志审查规则 ()
- 将一个或多个日志审查规则**导出** () 到 XML 或 CSV 文件。（单击**导出...** 按钮可将它们全部导出，也可以从下拉列表中进行选择，只导出选定或显示的那些内容）

注意：	*无法删除已分配给一台或多台计算机或属于策略的日志审查规则。*

注意：	*趋势科技服务器深度安全防护系统管理中心随附一组标准的 OSSEC 日志审查规则。有关日志审查的更多信息，请参阅***查看日志审查规则***和***日志审查***。有关使用基于 XML 的语言编写自己的日志审查规则的更多帮助，请查阅 OSSEC 文档或联系您的支持提供商。*

单击**新建** () 或属性 () 显示**日志审查规则属性**窗口。

常规

常规信息

日志审查规则的名称和描述，以及使该规则正常运行所需的客户端和趋势科技服务器深度安全防护系统管理中心的最低版本（如果该规则由趋势科技发布）。

标识

首次发布规则以及上次更新规则的日期，以及规则的唯一标识符。

内容

注意： *内容选项卡仅针对您自己创建的日志审查规则显示。而趋势科技发布的日志审查规则具有一个显示日志审查规则的配置选项（如果有）的**配置**选项卡。趋势科技发布的日志审查规则不可编辑（虽然可对其进行复制，然后再编辑副本）。*

模板

在**内容**选项卡中，选择“基本规则”模板。

常规信息

输入规则 ID。规则 ID 是规则的唯一标识符。OSSEC 将 100000 - 109999 定义为用户定义规则的空间。(趋势科技服务器深度安全防护系统管理中心将使用新的唯一规则 ID 来预填充该文本框。)

为规则提供一个级别。零 (0) 表示该规则从不记录事件，尽管可能触发监控该规则的其他规则。（请参阅下面的依赖关系文本框。）

还可以将该规则分配给一个或多个以逗号分隔的组。这可以在使用依赖关系时发挥作用，因为您可以创建在触发某个规则时即触发的规则或者创建属于特定组的规则。

特征码匹配

这是规则将要在日志中查找的特征码。如果匹配，将触发该规则。特征码匹配支持正则表达式或简单的字符串特征码。“字符串特征码”特征码类型比 RegEx 快，但它仅支持三种特定操作：

- ^（**插入符号**）：指定文本的开头
- $（**美元符号**）：指定文本的结尾
- |（**管道符**）：在多个特征码之间创建 "OR"

注意： *有关日志审查模块使用的正则表达式语法的信息，请参阅 http://www.ossec.net/doc/syntax/regex.html*

复合

频率是指触发规则前在指定的时间帧内必须匹配的次数。

时间帧是一个时间段（以秒为单位），在该时间段内，规则必须触发一定的次数（上述频率）才能记录事件。

关联

设置对其他规则的依赖关系将导致在触发本区域中指定的规则时，您的规则仅记录事件。

文件

键入规则要监控的文件的完整路径并指定文件的类型。

选项

警报

选择此规则是否在趋势科技服务器深度安全防护系统管理中心中触发警报。

仅在规则中写入了“多个规则”时才使用“警报最低严重性”设置（如果使用“基本”模板，可能无法执行某些操作）。但是，如果在使用“基本”模板创建规则后，编辑规则的 XML 并向具有不同严重性级别的 XML 中添加其他规则，则可以使用“警报最低严重性级别”下拉菜单设置要触发警报的多个规则的最低严重性。

已分配给

列出要使用此日志审查规则的安全配置文件或计算机。

建议

可以将趋势科技服务器深度安全防护系统配置为执行定期“漏洞扫描 （推荐设置）”，“漏洞扫描 （推荐设置）”会扫描计算机，并对各种安全规则的应用提供建议。选中该复选框将会将建议的日志审查规则自动分配给计算机，并自动取消分配不需要的规则。

要打开或关闭建议引擎，请转至**策略/计算机编辑器 > 设置 > 扫描**。

计算机和策略编辑器

趋势科技服务器深度安全防护系统管理中心主窗口用于管理和组织整个趋势科技服务器深度安全防护系统的元素，而**策略编辑器**和**计算机编辑器**窗口则用于从趋势科技服务器深度安全防护系统管理中心中选择趋势科技服务器深度安全防护系统的元素，并将这些元素应用于策略或特定计算机。

策略的**详细信息**窗口与趋势科技服务器深度安全防护系统管理中心主窗口非常相似，只是策略的“详细信息”窗口中的所有元素专门应用于策略。缺省情况下，所有设置将从趋势科技服务器深度安全防护系统管理中心主窗口的全局设置继承。可以在策略窗口中进行仅适用于此策略的更改。在趋势科技服务器深度安全防护系统管理中心主窗口中修改某个元素（防火墙规则、入侵防御规则等）的属性时，唯一的选项是修改“属性”。当在策略“详细信息”窗口中修改某个元素的属性时，有其他选项可用：“属性（适用于此策略）”。

如果编辑“属性（适用于此策略）”，则只有在此策略将元素应用于计算机时，更改才会对该元素产生影响。

如果编辑“属性”，则更改将对元素产生全局影响（该元素被覆盖的其他位置除外）。

已“针对此策略”编辑其属性的元素将以粗体字显示在任务窗格中，表示该元素在作为此策略的一部分应用于计算机时具有特殊属性。

另请参阅：

- **策略、继承与覆盖**

概述（策略编辑器）

策略**概述**页面具有以下选项卡：

- *常规（第 87页）*
- *使用此策略的计算机（第 88页）*
- *事件（第 89页）*

常规

常规

- **名称：**显示在“显示名称”列中“主机名”值旁边的括号中。
- **描述：**计算机的描述。

继承

标识当前策略从中继承其设置的父策略（如果有）。

模块

- **防恶意软件：**如果防恶意软件防护处于打开状态，则防恶意软件的状态指示灯为绿色。关闭时，防恶意软件的状态指示灯为灰色。
- **Web 信誉：**Web 信誉是处于打开状态还是关闭状态。
- **防火墙：**防火墙是处于打开状态还是关闭状态以及有多少个规则生效。
- **入侵防御：**入侵防御是处于打开状态还是关闭状态以及有多少个规则生效。
- **完整性监控：**完整性监控是处于打开状态还是关闭状态以及有多少个规则生效（仅客户端）。
- **日志审查：**日志审查是处于打开状态还是关闭状态以及有多少个规则生效（仅客户端）。

使用此策略的计算机

列出此策略分配到的计算机。

事件

注意： *策略编辑器中的事件列表仅显示与当前策略关联的事件。*

系统事件日志是系统相关事件的记录（相对于安全相关事件）。在主页面上可以执行下列操作：

- **查看**（）系统事件的详细信息（属性）
- **搜索**（）特定系统事件
- 将当前显示的系统事件**导出**（）为 CSV 文件
- 查看现有的**自动标记**（）规则。

另外，右键单击事件可提供下列选项：

- **添加标记：**为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记：**移除现有事件标记

查看

选择某个事件并单击**查看**（）会显示**事件查看程序属性**窗口。

常规

常规信息

- **时间：**以托管趋势科技服务器深度安全防护系统管理中心的计算机的系统时钟为准的时间。
- **级别：**发生事件的严重性级别。事件级别包括**信息**、**警告**及**错误**。
- **事件 ID：**事件类型的唯一标识符。
- **事件：**事件的名称（与事件 ID 相关联）。
- **目标：**与事件有关联的系统对象将在此处标识。单击对象的标识将显示对象的属性表。
- **事件来源：**发生事件的趋势科技服务器深度安全防护系统组件。
- **操作执行者：**如果事件由用户启动，则会在此处显示该用户的用户名。单击该用户名将显示**用户属性**窗口。
- **管理中心：**趋势科技服务器深度安全防护系统管理中心计算机的主机名。

描述

如果合适，此处会显示执行何种操作以在系统事件日志中触发此条目的特定详细信息。

标记

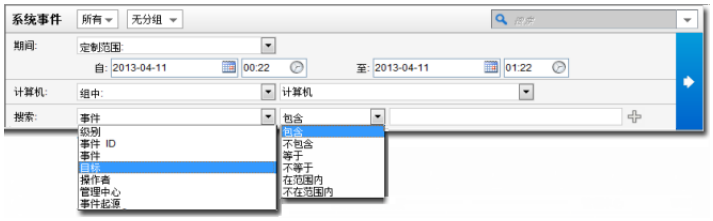
标记选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。

单击**搜索** > **打开高级搜索**可选择是否显示高级搜索栏。



按搜索栏右侧的“添加搜索栏”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交请求”按钮（位于工具栏右侧，带右向箭头）。

导出

可以将显示的事件导出为 CSV 文件。（将忽略分页，所有页面都将被导出。）可以选择显示所显示的列表，也可以选择显示所选定的项目。

自动标记

单击**自动标记...** 将显示现有系统事件自动标记规则的列表。

概述（计算机编辑器）

计算机**概述**页面具有以下选项卡：

- *常规（第 92页）*
- *操作（第 95页）*
- *事件（第 97页）*

常规

常规

- **主机名：**显示在**计算机**页面的**名称**列中。此名称必须是计算机的 IP 地址或计算机的主机名。（如果使用主机名来代替 IP 地址，则将使用完全限定主机名或相对主机名。）
- **显示名称：**显示在“显示名称”列中“主机名”值旁边的括号中。
- **描述：**计算机的描述。
- **平台：**此处将显示计算机操作系统的详细信息。
- **组：**计算机所属的计算机组将显示在下拉列表中。可以将计算机重新分配给任何其他现有的计算机组。
- **策略：**分配给此计算机的策略（如果有）。

> *注意：* *请记住，从计算机上取消分配策略时，如果规则是独立于策略进行分配的，则这些规则在该计算机上可能仍然生效。*

- **资产严重性：**趋势科技服务器深度安全防护系统管理中心使用排序系统来量化安全事件的重要性。为规则分配“严重性等级”（高、中、低等），为资产（计算机）分配“资产重要性”等级。这些级别均有数值显示。触发计算机上的规则时，就会将“资产重要性”值与“严重性级别”值相乘。这样将产生一个得分，可用于按照重要性对事件进行排序。（在**事件**页面中可以看到事件排序。）使用此**资产重要性**下拉列表，将资产重要性级别分配给此计算机。（要编辑与严重性级别和重要性级别相关的数值，请转至**管理 > 系统设置 > 排序**。）
- **从以下位置下载安全更新：**使用下拉列表选择此计算机上的客户端/设备将从中下载安全更新的中继组。（客户端充当中继时不显示。）

状态

计算机状态

“状态”区域显示有关计算机及计算机上生效的防护模块的最新可用信息。顶行显示计算机是由客户端还是设备（或者协调保护时使用二者）进行保护。

- **状态：**

- 如果计算机未被管理，该状态代表客户端/设备的激活状态。该状态会显示“已找到”或“新的”，后面跟着括在括号中的客户端/设备状态（“无客户端/设备”、“未知”、“需要重新激活”、“需要激活”或“需要停用”）。
- 如果计算机被管理且未出现任何计算机错误，该状态会显示“被管理”，后面跟着括在括号中的客户端/设备状态（“联机”或“脱机”）。
- 当计算机接受管理并且客户端/设备正在执行操作时（例如“完整性扫描正在进行中”、“正在升级客户端（已发送安装程序）”等），将显示相应的任务状态。
- 如果计算机发生错误（例如，“脱机”、“更新不成功”等），该状态将显示错误。当发生一个以上的错误时，此状态会显示“多个错误”，且其后会列出各个错误。

防护模块状态

实施趋势科技服务器深度安全防护系统 9.5 防护模块的软件将根据需要安装并部署到客户端。首次安装客户端时，仅包含核心功能。

状态区域提供有关趋势科技服务器深度安全防护系统模块的安装状态信息。该状态反映了模块在客户端上的状态及其在趋势科技服务器深度安全防护系统管理中心的配置情况。状态“打开”表示在趋势科技服务器深度安全防护系统管理中心配置了该模块，而且在趋势科技服务器深度安全防护系统客户端上安装了该模块并正在运行。

当处于“打开”状态并且正在工作时，模块将显示绿色的状态指示灯。此外，对于允许单独分配规则的模块，必须先为其分配至少一个规则，才会显示绿色指示灯。例如，在上面的图片中，完整性监控模块处于“打开”状态，并且由于已为其分配了一个规则，因此其状态指示灯为绿色。

- **防恶意软件：**如果防恶意软件防护处于打开状态，则防恶意软件的状态指示灯为绿色。关闭时，防恶意软件的状态指示灯为灰色。
- **Web 信誉：**Web 信誉是处于打开状态还是关闭状态。
- **防火墙：**防火墙是处于打开状态还是关闭状态以及有多少个规则生效。
- **入侵防御：**入侵防御是处于打开状态还是关闭状态以及有多少个规则生效。
- **完整性监控：**完整性监控是处于打开状态还是关闭状态以及有多少个规则生效（仅客户端）。
- **日志审查：**日志审查是处于打开状态还是关闭状态以及有多少个规则生效（仅客户端）。
- **联机：**指示管理中心当前是否可与客户端/设备进行通信。
- **上次通信：**在此计算机上管理中心上次与客户端/设备成功进行通信的时间。
- **检查状态：**通过此按钮可强制管理中心立即执行波动信号操作，以检查客户端/设备的状态。“检查状态”不会执行客户端/设备的安全更新。（如果需要更新，请单击**操作**选项卡上的**立即更新**按钮。）如果将管理中心与客户端/设备之间的通信设置为“客户端/设备已启动”，将禁用**检查状态**按钮。（检查状态不会更新此计算机的日志。要更新此计算机的日志，请转至**操作**选项卡。）
- **清除警告/错误：**解除此计算机上的任何警报或错误。
- **ESXi Server：**如果计算机是受虚拟设备保护的虚拟机，则将显示托管 ESXi Server。
- **设备：**如果计算机是受虚拟设备保护的虚拟机，则将显示用于进行保护的设备。
- **ESXi 版本：**如果计算机是 ESXi Server，则将显示 ESXi 版本号。
- **过滤器驱动程序版本：**如果计算机是 ESXi Server，则将显示过滤器驱动程序版本号。
- **客户虚拟机：**如果计算机是 ESXi Server，则将显示虚拟设备和客户虚拟机。
- **设备版本：**如果计算机是虚拟设备，则将显示设备版本号。

- **防恶意软件就绪：**如果计算机是虚拟机，则“防恶意软件就绪”表示是否已安装 VMware vShield Endpoint 瘦客户端。如果计算机是虚拟设备，则“防恶意软件就绪”表示是否已在托管 ESXi Server 上安装 VMware vShield Endpoint 驱动程序。
- **受保护的客户虚拟机：**如果计算机是虚拟设备，则将显示 ESXi Server 和受保护的客户虚拟机的 IP。

VMware 虚拟机摘要

本节显示有关在其上运行客户端/设备的虚拟机（仅 VMware 虚拟机）的硬件和软件配置信息摘要。

操作

操作

激活

新安装的趋势科技服务器深度安全防护系统客户端/设备需要由趋势科技服务器深度安全防护系统管理中心“激活”，然后才能向其发送策略、规则和事件日志请求等。激活过程包括交换唯一标识管理中心（或其中一个节点）与客户端/设备的 SSL 密钥。由趋势科技服务器深度安全防护系统管理中心激活后，客户端/设备将仅接受激活它的趋势科技服务器深度安全防护系统管理中心（或其中一个节点）的指令，或仅与该管理中心（或其中一个节点）进行通信。

未激活的客户端/设备可以由任意趋势科技服务器深度安全防护系统管理中心激活。

客户端/设备只能在计算机本地停用，或通过激活它的趋势科技服务器深度安全防护系统管理中心来停用。如果客户端/设备已激活，则本区域中的按钮将显示为**重新激活**，而不是**激活**。重新激活与激活的效果是一样的。重新激活会将客户端/设备重置为第一次安装之后的状态，并启动新一组 SSL 密钥的交换。

注意： *使用协调保护时，可以单独停用/重新激活客户端和设备提供的保护。*

策略

当您使用趋势科技服务器深度安全防护系统管理中心更改计算机上的客户端/设备的配置（应用新的入侵防御规则、更改日志记录设置等）时，趋势科技服务器深度安全防护系统管理中心必须将新的信息发送给该客户端/设备。这是一个“发送策略”指令。策略更新通常会立刻执行，但也可以通过单击**发送策略**按钮来强制执行更新。

软件

该软件将显示当前计算机上所运行的客户端/设备的版本。如果有较新版本的客户端/设备可供计算机平台使用，可以单击**升级客户端...**或**升级设备...**按钮，从趋势科技服务器深度安全防护系统管理中心远程升级该客户端或设备。您可以转至**管理** > **系统设置** > **更新**选项卡，将趋势科技服务器深度安全防护系统管理中心配置为在有适用于任何计算机的新版本客户端/设备软件时触发警报。

注意： *在要升级的计算机上必须禁用“客户端自我保护”。要配置“客户端自我保护”，请转至**策略/计算机编辑器** > **设置**页面上的**计算机**选项卡。“客户端自我保护”功能仅限于 Windows。*

版本 9.5 及更高版本的 Windows 和 Linux 客户端可以通过配置充当趋势科技服务器深度安全防护系统中继。中继用于在网络中分发安全更新和软件更新。单击**启用中继**可在客户端上启用此功能。客户端启用中继功能后，将检索最新的安全更新和软件更新，并按照现有的更新设置分发这些更新。有关中继的更多信息，请参阅**中继组**。

支持

创建诊断数据包... 按钮可创建计算机上客户端/设备状态的快照。支持提供商可能会要求创建此快照以进行故障排除。

如果丢失与计算机的通信，则可在本地创建诊断数据包。

在 Windows 计算机上本地创建诊断数据包：

1. 从命令行键入：
   C:\Program Files\Trend Micro\Deep Security Agent> dsa_control -d
   然后按 Enter 键。
2. 将在同一目录中创建一个包含诊断信息的已编号 zip 文件（例如 "341234567.zip"）。

在 Linux 计算机上本地创建诊断数据包：

1. 从命令行键入：
   $ /opt/ds_agent/dsa_control -d
   并按 Enter 键。
2. 将在同一目录中创建一个包含诊断信息的已编号 zip 文件（例如 "341234567.zip"）。

在趋势科技服务器深度安全防护系统虚拟设备计算机上本地创建诊断数据包：

1. 1. 从命令行键入：
   $ sudo /opt/ds_agent/dsa_control -d
   并按 Enter 键。
2. 将在同一目录中创建一个包含诊断信息的已编号 zip 文件（例如 "341234567.zip"）。

TPM（仅限 ESXi 虚拟机监控程序）

可信平台模块 (TPM) 是一种用于进行硬件认证的芯片。VMware 将 TPM 用于其 ESXi 虚拟机监控程序。在引导顺序期间，ESXi 会在加载时将每个虚拟机监控程序组件的 SHA-1 哈希写入一组寄存器。如果从一个引导顺序到下一个引导顺序期间这些值意外更改，则表明可能出现值得调查的安全问题。趋势科技服务器深度安全防护系统可以在每次引导后监控 ESXi 上的 TPM，如果检测到任何更改，则发出警报。如果在不支持 TPM 监控的 ESXi 上选择启用该监控的选项，则该选项将自动禁用。

注意： *要进行 TPM，必须具有趋势科技服务器深度安全防护系统完整性监控模块。*

TPM 监控的最低要求是：

- 趋势科技服务器深度安全防护系统管理中心 9+
- vCenter 5.1+
- ESXi 5.1+
- ESXi 上安装并启用了 TPM/TXT（有关详细信息，请查看 VMware 文档）
- 对于此 ESXi ，趋势科技服务器深度安全防护系统完整性监控模块必须处于启用状态。

事件

注意： *计算机编辑器中的事件列表仅显示与当前计算机关联的事件。*

系统事件日志是系统相关事件的记录（相对于安全相关事件）。在主页面上可以执行下列操作：

- **查看**（）系统事件的详细信息（属性）
- **搜索**（）特定系统事件
- 将当前显示的系统事件**导出**（）为 CSV 文件
- 查看现有的**自动标记**（）规则。

另外，右键单击事件可提供下列选项：

- **添加标记：**为此事件添加事件标记（请参阅**事件标记**。）
- **移除标记：**移除现有事件标记

查看

选择某个事件并单击**查看**（）会显示**事件查看程序属性**窗口。

常规

常规信息

- **时间：**以托管趋势科技服务器深度安全防护系统管理中心的计算机的系统时钟为准的时间。
- **级别：**发生事件的严重性级别。事件级别包括**信息**、**警告**及**错误**。
- **事件 ID：**事件类型的唯一标识符。
- **事件：**事件的名称（与事件 ID 相关联）。
- **目标：**与事件有关联的系统对象将在此处标识。单击对象的标识将显示对象的属性表。
- **操作执行者：**如果事件由用户启动，则会在此处显示该用户的用户名。单击该用户名将显示**用户属性**窗口。
- **管理中心：**趋势科技服务器深度安全防护系统管理中心计算机的主机名。

描述

如果合适，此处会显示执行何种操作以在系统事件日志中触发此条目的特定详细信息。

标记

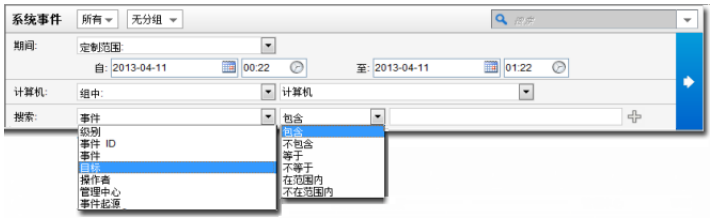
标记选项卡显示已附加到此事件的标记。有关事件标记的更多信息，请参阅**策略** > **通用对象** > **其他** > **标记**以及**参考**部分中的**事件标记**。

过滤列表和/或搜索事件

使用**期间**工具栏可以过滤列表，从而只显示在特定时间范围内发生的事件。

使用**计算机**工具栏，可以按照计算机组或计算机策略来组织事件日志条目的显示。

单击**高级搜索**可选择是否显示搜索栏。



按搜索栏右侧的“添加搜索栏”按钮 (+) 将显示另一个搜索栏，这样可将多个参数应用于搜索。准备就绪后，按“提交请求”按钮（位于工具栏右侧，带右向箭头）。

导出

可以将显示的事件导出为 CSV 文件。（将忽略分页，所有页面都将被导出。）可以选择显示所显示的列表，也可以选择显示所选定的项目。

自动标记

单击**自动标记...** 将显示现有系统事件自动标记规则的列表。

防恶意软件

防恶意软件模块针对基于文件的威胁（包括常称为恶意软件、病毒、特洛伊木马以及间谍软件的威胁）同时提供实时保护和按需保护。为识别威胁，防恶意软件会使用综合的威胁数据库对文件进行检查，该数据库的部分文件托管在服务器上或本地保存为可更新的特征码。防恶意软件还检查文件是否有某些特征，如压缩和已知的入侵代码。

为解决威胁，防恶意软件会在对系统的损害降至最低的情况下，选择性地执行可包含和移除威胁的操作。防恶意软件可以清除、删除或隔离恶意文件。它还可以终止进程并删除与已识别威胁关联的其他系统对象。

注意：	*最新安装的趋势科技服务器深度安全防护系统客户端无法提供防恶意软件保护，直到连接到更新服务器并下载防恶意软件特征码和更新。确保趋势科技服务器深度安全防护系统客户端在安装后可以与趋势科技服务器深度安全防护系统中继或全局趋势科技更新服务器进行通信。*

防恶意软件页面包含以下选项卡式部分：

- *常规（第 100页）*
- *云安全智能防护（第 102页）*
- *高级（第 103页）*
- *隔离的文件（第 105页）*
- *事件（第 106页）*

常规

防恶意软件状态

打开或关闭防恶意软件。可以将此策略或计算机配置为从其父策略继承防恶意软件的打开/关闭状态，也可以在本地覆盖该设置。

实时扫描

实时扫描是一种持续不断的扫描。每次接收、打开、下载、复制或修改文件时，实时扫描都会扫描文件中是否存在安全风险。如果趋势科技服务器深度安全防护系统未检测到安全风险，文件将保留在原位置，用户可以继续访问文件。如果趋势科技服务器深度安全防护系统检测到安全风险，会显示一条通知消息，指出受感染文件和具体的安全风险。

要执行实时恶意软件扫描，必须选择扫描配置和该配置生效的时间表。

注意： ***恶意软件扫描配置****决定了扫描的文件类型、扫描的目录、扫描的恶意软件类型以及对检测到的恶意软件执行的操作等设置。您可以通过从下拉菜单中选择扫描配置并单击****编辑****来检查扫描配置的属性。要管理所有不同的恶意软件扫描配置，请在趋势科技服务器深度安全防护系统管理中心中转至****策略 > 通用对象 > 其他 > 恶意软件扫描配置****。*

手动扫描

手动扫描是一种按需扫描，会在用户在计算机上运行扫描后立即开始。完成扫描所需的时间取决于要扫描的文件数量和计算机的硬件资源。

要执行手动恶意软件扫描，必须选择扫描配置。

注意： ***恶意软件扫描配置****决定了扫描的文件类型、扫描的目录、扫描的恶意软件类型以及对检测到的恶意软件执行的操作等设置。您可以通过从下拉菜单中选择扫描配置并单击****编辑****来检查扫描配置的属性。要管理所有不同的恶意软件扫描配置，请在趋势科技服务器深度安全防护系统管理中心中转至****策略 > 通用对象 > 其他 > 恶意软件扫描配置****。*

预设扫描

预设扫描将在指定的日期和时间自动运行。使用预设扫描可自动执行日常扫描，提高扫描管理效率。

要执行预设恶意软件扫描，必须选择扫描配置。

注意： ***恶意软件扫描配置****决定了扫描的文件类型、扫描的目录、扫描的恶意软件类型以及对检测到的恶意软件执行的操作等设置。您可以通过从下拉菜单中选择扫描配置并单击****编辑****来检查扫描配置的属性。要管理所有不同的恶意软件扫描配置，请在趋势科技服务器深度安全防护系统管理中心中转至****策略 > 通用对象 > 其他 > 恶意软件扫描配置****。*

恶意软件扫描（仅限计算机编辑器）

显示上次执行手动恶意软件扫描和预设恶意软件扫描的时间和日期，并允许您执行或中止快速恶意软件扫描或完整恶意软件扫描。

另请参阅：

- 策略、继承与覆盖

云安全智能防护

云安全扫描

云安全扫描将许多恶意软件和间谍软件扫描功能转移到云安全智能防护服务器。无需下载完整的恶意软件特征码文件到本地计算机，而是下载一个小得多的特征码版本，它可识别文件是“确定安全的”还是“可能危险的”。“可能危险的”文件将与较大的完整特征码文件比较（该文件存储在趋势科技云安全智能防护服务器中），以明确确定它们是否会带来安全风险。此方法可使本地特征码文件保持较小，并减少客户端/设备所需的更新大小和数量。

注意： *配置为使用云安全扫描的计算机将不会本地下载完整的防恶意软件特征码。因此，如果您的防恶意软件使用授权在计算机配置为使用云安全扫描时过期，关闭云安全扫描将不会导致使用本地特征码扫描恶意软件，因为本地不存在任何防恶意软件特征码。*

用于文件信誉服务的云安全智能防护服务器

用于文件信誉的云安全智能防护服务提供云安全扫描所需的文件信誉信息。选择是否直接连接到趋势科技的云安全智能防护服务或是否连接到一个或多个本地安装的云安全智能防护服务器。

选择**在域外时，连接到 Internet 云安全智能防护服务。(仅限 Windows。)** 选项，当计算机在域外时，使用 Internet 云安全智能防护服务。如果计算机无法连接到其域控制器，即被视为在域外。（此选项只适用于 Windows 客户端。）

注意： *可以在**管理 > 系统设置**窗口的**代理服务器**选项卡上查看并编辑可用代理服务器列表。*

云安全智能防护服务器连接警告

此事件确定在计算机丢失了到云安全智能防护服务器的连接时，是否生成错误事件或发出警报。

注意： *如果您在本地安装了云安全智能防护服务器，则应至少在一台计算机上将此选项设置为**是**，以便在云安全智能防护服务器自身出错时会通知您。*

高级

隔离的文件

用于存储隔离文件的最大磁盘空间：此设置确定可用于存储隔离文件的磁盘空间大小。它可全局应用到所有计算机：物理计算机、虚拟机和虚拟设备。可在策略级别和计算机级别覆盖此设置。如果使用虚拟设备为虚拟机提供保护，无客户端 VM 的所有隔离文件都将存储在虚拟设备上。因此，您应该为虚拟设备上的隔离文件增加磁盘空间。

在以下情况下，将自动从虚拟设备删除隔离的文件：

- 如果 VM 经历 vMotion，将从虚拟设备删除与该 VM 关联的隔离文件。
- 如果从趋势科技服务器深度安全防护系统管理中心停用了 VM，将从虚拟设备删除与该 VM 关联的隔离文件。
- 如果从趋势科技服务器深度安全防护系统管理中心停用了虚拟设备，将删除该虚拟设备上存储的所有隔离文件。
- 如果从 vCenter 删除虚拟设备，也将删除存储在该虚拟设备上的所有隔离文件。

扫描限制

要扫描的最大文件大小：超过此文件大小的文件将不进行扫描。（将值设置为 0 表示没有最大大小。将扫描所有文件。）

恶意软件扫描的资源分配

使用多线程处理进行恶意软件扫描 （如果可用）：在支持此功能的系统上启用多线程处理。仅适用于手动/预设扫描，而不适用于实时扫描。

注意：	*使用多线程处理可能会减少可供计算机上运行的其他进程使用的资源。请注意，必须重新启动启用多线程处理的计算机才能使该设置生效。*

允许的间谍软件/灰色软件

允许的间谍软件/灰色软件：使用此设置可维护一份已被趋势科技服务器深度安全防护系统确定为间谍软件/灰色软件的允许的应用程序列表。

注意：	*此选项仅在 Windows 计算机上有效。在 Linux 计算机上，可以使用**扫描例外文件列表**标识应在恶意软件扫描过程中忽略的特定文件，以达到相似的结果。扫描例外对象是**恶意软件扫描配置**的一个属性，恶意软件扫描配置是**安全策略**的一个属性。* ***要在恶意软件扫描配置中指定扫描例外文件列表：****在趋势科技服务器深度安全防护系统管理中心中，转至**策略 > 通用对象 > 恶意软件扫描配置**。您可以在恶意软件扫描配置的**属性**窗口的**例外**选项卡上的**扫描例外**区域中指定文件列表。* ***要在安全策略中选择恶意软件扫描配置：****打开策略编辑器并转至**常规**选项卡，从**实时扫描**、**手动扫描**或**预设扫描**区域中的下拉列表中选择恶意软件扫描配置。*

注意：	*间谍软件/灰色软件扫描引擎将忽略**允许的间谍软件/灰色软件**列表中的应用程序。这些应用程序的存在将不会被记录或存储为防恶意软件事件。*

可使用两种方式之一将间谍软件/灰色软件添加到允许列表。您可以使用检测到应用程序的防恶意软件事件进行添加，也可以手动输入间谍软件/灰色软件的名称。

使用防恶意软件事件将间谍软件/灰色软件添加到允许的间谍软件/灰色软件列表：

1. 在**防恶意软件事件**页面中查找检测事件。
2. 右键单击该事件。
3. 选择**允许**。

如果扫描引擎已检测到应用程序，则它可能已被隔离或删除，具体取决于当前的间谍软件/灰色软件设置。如果已被隔离，您必须恢复或重新安装该应用程序。有关恢复隔离文件的信息，请参阅**防恶意软件 > 隔离的文件**。或者，可以通过将**处理措施**设置为“不予处理”模式来运行间谍软件/灰色软件扫描，以便在**防恶意软件事件**页面上记录所有间谍软件/灰色软件检测，但既不是已隔离也不是已删除，而是“未处理”。然后使用此方法将所选间谍软件/灰色软件添加到允许列表，再将**处理措施**设置为“隔离”或“删除”模式。

将间谍软件/灰色软件手动添加到允许的间谍软件/灰色软件列表：

请注意应用程序显示在防恶意软件事件日志中的名称，并将其手动添加到**允许的间谍软件/灰色软件列表**。

注意： *此列表中的条目区分大小写。这些条目必须与其在事件日志所显示的完全相同。*

注意： *有关检测到的间谍软件/灰色软件的信息，请参考趋势科技间谍软件/灰色软件百科全书。*

本地事件通知

当检测到恶意软件时显示本地通知：此设置决定趋势科技服务器深度安全防护系统通知程序（如果计算机本地安装了该程序）是否会在检测到恶意软件时显示弹出通知。

VM 扫描缓存

扫描缓存由虚拟设备用于最大限度地提高虚拟机恶意软件扫描和完整性监控扫描的效率。有关扫描缓存配置的信息，请参阅**虚拟设备扫描缓存**。

NSX 安全标记

一旦检测到恶意威胁，趋势科技服务器深度安全防护系统可将 **NSX 安全标记**应用于受保护的 VM。NSX 安全标记是 VMware vSphere NSX 环境的一部分，并且不能与趋势科技服务器深度安全防护系统事件标记混淆。有关 NSX 安全标记的更多信息，请查看 VMware 文档。有关趋势科技服务器深度安全防护系统事件标记的更多信息，请参阅**事件标记**。

您可以选择仅在防恶意软件引擎尝试的阻止操作不成功时才应用 NSX 安全标记。（阻止操作由生效的恶意软件扫描配置决定。要查看生效的恶意软件扫描配置，请转到**计算机/策略编辑器 > 防恶意软件 > 常规**选项卡，然后检查**实时扫描**、**手动扫描**和**预设扫描**区域。）

您也可以选择在后续恶意软件扫描未检测到任何恶意软件时，移除安全标记。应仅在所有恶意软件扫描都将是同一类型时使用此设置。

隔离的文件

除了只列出此计算机上隔离的文件外，隔离文件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。（请参阅*隔离的文件（第 15页）*。）

事件

除了只显示与此策略或特定计算机相关联的事件外，防恶意软件事件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。（请参阅*防恶意软件事件（第 12页）*。）

Web 信誉

Web 信誉模块根据 Web 页面的信誉评级对其进行阻止。它通过查询趋势科技云安全智能防护网络服务器获取这些评级，这些评级汇总于多个来源，包括 Web 页面链接、域和 IP 地址关系、垃圾邮件源以及垃圾邮件中的链接。通过从云安全智能防护网络获取评级，Web 信誉可使用可用的最新信息来阻止有害页面。

除非您选择覆盖它们，否则此策略或计算机的 Web 信誉配置将从其父策略继承其打开或关闭状态。

“Web 信誉服务”页面包含以下选项卡式部分：

- *常规（第 108页）*
- *例外（第 111页）*
- *云安全智能防护（第 109页）*
- *高级（第 110页）*
- *事件（第 112页）*

常规

Web 信誉

可以将此策略或计算机配置为从其父策略继承 Web 信誉打开/关闭状态，也可以本地锁定设置。

安全级别

Web 信誉评级系统为 URL 指定以下风险级别：

- **危险**：已确认 URL 为欺诈性页面或者已知威胁源
- **高度可疑**:怀疑 URL 为欺诈性页面或者已知威胁源
- **可疑**：URL 与垃圾邮件相关或者可能有危害
- **安全**：URL 不存在风险

选择要实施的安全级别：

高：阻止以下类型的页面：

- 危险
- 高度可疑
- 可疑

中：阻止以下类型的页面：

- 危险
- 高度可疑

低：阻止以下类型的页面：

- 危险

阻止未经趋势科技测试的页面：阻止以下类型的页面：

- 未经趋势科技评定

云安全智能防护

用于 Web 信誉服务的云安全智能防护服务器

用于 Web 信誉的云安全智能防护服务提供 Web 信誉模块所需的 Web 信誉信息。选择是否直接连接到趋势科技的云安全智能防护服务或是否连接到一个或多个本地安装的云安全智能防护服务器。

选择**在域外时，连接到 Internet 云安全智能防护服务。（仅限 Windows。）**选项，当计算机在域外时，使用 Internet 云安全智能防护服务。如果计算机无法连接到其域控制器，即被视为在域外。（此选项只适用于 Windows 客户端。）

注意： *在**管理** > **系统设置** > **代理服务器**选项卡上查看可用代理服务器的列表。*

云安全智能防护服务器连接警告

此事件确定在计算机丢失了到云安全智能防护服务器的连接时，是否生成错误事件或发出警报。

注意： *如果您在本地安装了云安全智能防护服务器，则应至少在一台计算机上将此选项设置为**是**，以便在云安全智能防护服务器自身出错时会通知您。*

高级

阻止页面

当用户尝试访问被阻止的 URL 时，系统将把他们重定向到一个阻止页面。提供一个他们可用来请求访问被阻止 URL 的链接。

警报

选择记录 Web 信誉事件时是否发出警报。

端口

选择要监控可能有害的 Web 页面的特定端口。

本地事件通知

阻止访问恶意 Web 站点时通过**趋势科技服务器深度安全防护系统通知程序**显示本地通知。

例外

例外是不管其安全评级为何均阻止或允许的 URL 的列表。

注意： ***允许****列表优先于****阻止****列表。与****允许****列表中的条目匹配的 URL 不会再基于****阻止****列表进行检查。*

已允许

无论允许列表中所含的 URL 的安全评级为何，都可以访问这些 URL。一次可添加多个 URL，但各个 URL 之间必须使用换行符来分隔。将 URL 添加到允许列表时，可选择允许域相同的所有 URL 还是允许该 URL：

- **允许来自域的 URL：**允许该域的所有页面。支持子域。仅包括条目中的域（子域可选）。例如，"example.com" 和 "another.example.com" 为有效条目。
- **允许 URL：**将允许所输入的 URL。支持通配符。例如，"example.com/shopping/coats.html" 和 "example.com/shopping/*" 为有效条目。

已阻止

阻止列表中的 URL 及含有阻止列表中所指定关键字的 URL 始终会被阻止（除非允许列表中存在覆盖条目）。一次可添加多个 URL 或关键字，但各个之间必须使用换行符来分隔。阻止 URL 时，可选择阻止某个域中的所有 URL、阻止该 URL 或阻止含有特定关键字的 URL。

- **阻止来自域的 URL：**阻止该域的所有页面。支持子域。仅包括条目中的域（子域可选）。例如，"example.com" 和 "another.example.com" 为有效条目。
- **阻止 URL：**将阻止所输入的 URL。支持通配符。例如，"example.com/shopping/coats.html" 和 "example.com/shopping/*" 为有效条目。
- **阻止包含此关键字的 URL：**将阻止含有该关键字的所有 URL。

事件

除了只显示与使用此策略的计算机相关的事件外，Web 信誉事件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。

防火墙

防火墙模块提供双向状态防火墙保护。它可阻止拒绝服务攻击，为所有基于 IP 的协议和帧类型提供覆盖范围，并且过滤端口以及 IP 和 MAC 地址

“防火墙”页面包含以下选项卡式部分：

- *常规（第 114页）*
- *接口隔离（第 115页）*
- *侦察（第 116页）*
- *高级（第 118页）*
- *事件（第 119页）*

常规

防火墙

可以将此策略或计算机配置为从其父策略继承防火墙打开/关闭状态，也可以本地锁定设置。

防火墙状态配置

选择要应用于此策略的防火墙状态配置。如果您已为此策略定义了多个接口（如上所示），则可以为每个接口指定独立的配置。

端口扫描（仅限计算机编辑器）

上次端口扫描：趋势科技服务器深度安全防护系统管理中心上次在此计算机上运行端口扫描的时间。

扫描的端口：在最近一次端口扫描期间扫描的端口。

打开的端口：本地计算机的 IP 地址下将列出已发现处于打开状态的端口的列表。

扫描打开的端口和**取消端口扫描**按钮使您能够在此计算机上启动或取消端口扫描。趋势科技服务器深度安全防护系统管理中心将扫描**策略/计算机编辑器 > 设置 > 扫描 > 打开的端口 > 要扫描的端口**中定义的端口范围。

注意： *无论配置的待扫描端口如何，趋势科技服务器深度安全防护系统管理中心始终会扫描客户端/设备的缺省端口（4118）。*

已分配防火墙规则

显示对此策略或计算机生效的防火墙规则。要添加或移除防火墙规则，请单击**分配/取消分配...**此时将出现一个窗口，显示可从中选择或取消选择规则的所有可用防火墙规则。

在“编辑器”窗口中，可以编辑防火墙规则以便将更改仅本地应用到编辑器（计算机或策略编辑器）的上下文，也可以编辑规则以便将更改全局应用到使用规则的所有其他策略和计算机。

要对规则进行本地编辑，请选择“规则”并单击“属性...”()，或右键单击“规则”并单击**属性...**

要对规则进行全局编辑，请右键单击“规则”并单击**属性（全局）...**

另请参阅：

- **策略、继承与覆盖**

接口隔离

接口隔离

可以将此策略或计算机配置为从其父策略继承接口隔离启用/禁用状态，也可以本地锁定设置。

接口特征码

启用接口隔离后，防火墙会尝试将正则表达式特征码与本地计算机上的接口名称进行匹配。

注意：	*趋势科技服务器深度安全防护系统使用 POSIX 基本正则表达式来匹配接口名称。有关基本 POSIX 正则表达式的信息，请访问 http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03*

只有与最高优先级特征码相匹配的接口才会允许传输网络通信。其他接口（与列表上剩余的任一特征码相匹配）都将“受限”。除非使用**允许**防火墙规则允许特定的通信通过，否则受限接口将阻止所有通信。

选择**限制为一个活动接口**将限制仅流向单个接口（即使多个接口与最高优先级特征码相匹配）的网络通信。

另请参阅：

- **策略、继承与覆盖**

侦察

侦察扫描

通过**侦察**页面，用户能够在所有或选定的计算机上启用和配置流量分析设置。

- **已启用侦察扫描检测：**打开或关闭检测侦察扫描功能。
- **要对其执行检测的计算机/网络：**从下拉列表中选择要保护的 IP。从现有的 IP 列表中选择。（为此，您可以使用**策略** > **通用对象** > **列表** > **IP 列表**页面来专门创建 IP 列表。）
- **不检测来自以下位置的流量：**从一组 IP 列表中选择要忽略的计算机和网络。（同上，您可以为此使用**策略** > **通用对象** > **列表** > **IP 列表**页面来专门创建 IP 列表。）

对于每一种攻击，可指示客户端/设备将信息发送给趋势科技服务器深度安全防护系统管理中心，在这里将会触发警报。您可以将管理中心配置为在触发警报时发送电子邮件通知。（请参阅**管理** > **系统设置** > **警报**。警报包括：“检测到网络或端口扫描”、“检测到计算机操作系统指纹探测”、“检测到 TCP Null 扫描”、“检测到 TCP FIN 扫描”和“检测到 TCP Xmas 扫描”。）请对此选项选择**立即通知 DSM**。

注意： *要使侦察防护发挥作用，必须打开状态检查并启用 TCP 和 UDP 日志记录。可以在**策略/计算机编辑器** > **防火墙** > **常规**选项卡上启用状态检查，在**策略/计算机编辑器** > **防火墙** > **高级**选项卡上启用日志记录。*

检测到攻击后，您可以指示客户端/设备阻止来自源 IP 的流量一段时间。使用**阻止流量**下拉列表可设置分钟数。

- **计算机操作系统指纹探测：**客户端/设备会识别主动 TCP 堆栈操作系统指纹尝试并做出反应。
- **网络或端口扫描：**客户端/设备会识别端口扫描并做出反应。
- **TCP Null 扫描：**客户端/设备会拒绝未设置标志的数据包。
- **TCP SYNFIN 扫描：**客户端/设备会拒绝只设置了 SYN 和 FIN 标志的数据包。
- **TCP Xmas 扫描：**客户端/设备会拒绝只设置了 FIN、URG 和 PSH 标志或只具有 0xFF 值（设置了每个可能的标志）的数据包。

注意： *只从单个数据包无法识别“计算机操作系统指纹探测”和“网络或端口扫描”，这与其他三种侦察类型是不同的。*

如果客户端/设备检测到有远程 IP 以异常的 IP-端口比访问系统，客户端/设备会报告“计算机或端口扫描”。客户端/设备计算机通常只会看到流向自身的网络通信，因此，端口扫描是最常检测到的探测类型。但是，如果计算机充当路由器或网桥，则可以看到流向其他许多计算机的网络通信，所以客户端/设备可以检测到计算机扫描（例如，在整个子网络中扫描已打开端口 80 的计算机）。

检测这些扫描可能需要几秒的时间，因为客户端/设备需要能够跟踪不成功的连接，并能够在比较短的时间内判断来自单台计算机的不成功连接数有异常。

计算机/端口扫描检测中所采用的统计分析方法，源自 "Connectionless Port Scan Detection on the Backbone" 文件中建议的 "TAPS" 算法，该文件由 Sprint/Nextel 发布，并在 Malware 研讨会上提出（与 IPCCC 同样于 2006 年 4 月在美国亚利桑那州凤凰城举办）。

注意： *在装有浏览器应用程序的 Windows 计算机上运行的趋势科技服务器深度安全防护系统客户端由于接收到来自已关闭的连接的剩余网络通信，有时会误报侦察扫描。*

注意： *要使“立即通知 DSM”选项发挥作用，必须将客户端/设备配置为执行**客户端/设备启动的**通信或**双向**通信（在**策略/计算机编辑器 > 设置 > 计算机**中设置）。启用后，一旦检测到攻击或探测，客户端/设备会立即对趋势科技服务器深度安全防护系统管理中心启动波动信号。*

高级

事件

设置是否生成“不允许的策略”的数据包的事件。这些数据包由于未得到**允许**防火墙规则的明确允许而受到阻止。将此选项设置为**是**可能会生成大量事件，具体取决于生效的防火墙规则。

事件

除了只显示与此策略或特定计算机相关的事件外，防火墙事件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。

入侵防御

入侵防御模块可保护计算机免遭已知和零时差漏洞攻击、SQL 注入攻击、跨站点脚本攻击和其他 Web 应用程序漏洞利用。屏蔽漏洞直到代码修复完成。它可识别访问网络的恶意软件，并增加对访问网络的应用程序的可见性，或者增加对其的控制。

入侵防御页面包含以下选项卡式部分：

- *常规（第 121页）*
- *高级（第 122页）*
- *事件（第 124页）*

常规

入侵防御

可以将此策略或计算机配置为从其父策略继承入侵防御打开/关闭状态，也可以本地锁定设置。

将入侵防御行为设置为“阻止”或“检测”。

如果是首次应用一组新的入侵防御规则，则可以选择将入侵防御行为设置为“检测”。在检测模式下，入侵防御引擎会将所有相同的入侵防御规则应用到通信，而不会丢弃数据包，它将只记录事件并允许该通信通过。使用此行为以确保新入侵防御规则不会干扰合法通信。

注意： *仅当网络引擎在桥接模式下运行时（即实时通信通过趋势科技服务器深度安全防护系统网络引擎进行流式传输），才适用此设置。桥接模式的备用选择是分接模式，实时通信在该模式下被克隆，而且网络引擎仅分析该克隆的通信。在分接模式下，由于网络引擎并不控制实时通信流，因此无法使用阻止模式。*

*要在桥接模式和分接模式之间切换，请打开策略编辑器或计算机编辑器，然后转至**设置 > 网络引擎 > 网络引擎模式**。*

已分配的入侵防御规则

显示对此策略或计算机生效的入侵防御规则。要添加或移除入侵防御规则，请单击**分配/取消分配...**此时将出现一个窗口，显示可从中选择或取消选择规则的所有可用入侵防御规则。

在“编辑器”窗口中，可以编辑入侵防御规则以便将更改仅本地应用到编辑器（计算机或策略编辑器）的上下文，也可以编辑规则以便将更改全局应用到使用规则的所有其他策略和计算机。

要对规则进行本地编辑，请选择“规则”并单击“属性...”()，或右键单击“规则”并单击**属性...**

要对规则进行全局编辑，请右键单击“规则”并单击**属性（全局）...**

建议

趋势科技服务器深度安全防护系统可以执行定期的“漏洞扫描 （推荐设置）”，这类扫描会扫描计算机，并对各种安全规则的应用提供建议。选择该复选框将会将建议的规则自动分配给计算机，并自动取消分配不需要的规则。

注意： *如果选择此选项，还应选择允许趋势科技服务器深度安全防护系统规则更新功能自动分配新的入侵防御规则。转至**管理 > 系统设置 > 更新**，然后选择**规则更新**区域中的**自动将新规则更新应用到策略**。*

要预设定期“漏洞扫描 （推荐设置）”，请在趋势科技服务器深度安全防护系统管理中心内转至**管理 > 预设任务**，然后创建新的预设任务。

另请参阅：

- **策略、继承与覆盖**

高级

事件数据

允许入侵防御规则捕获每个规则第一次命中的数据（以期间为单位）：决定趋势科技服务器深度安全防护系统是否将保存触发入侵防御规则的数据包数据。此设置与可在**计算机/策略编辑器 > 设置 > 网络引擎 > 高级网络引擎设置**中找到的高级*网络引擎设置（第 138页）*配合使用。

- **记录所有数据包数据：**记录与特定防火墙规则或入侵防御规则无关的事件的数据包数据。也就是说，记录诸如“丢弃的重新传送量”或“ACK 无效”等事件的数据包数据。

  注意： *由于事件发生折叠而聚合的事件无法保存其数据包数据。*

- **在期间内仅记录一个数据包：**如果已启用此选项且未启用**记录所有数据包数据**，则大多数日志将仅包含标头数据。将定期附加完整数据包，如**在期间内仅记录一个数据包的期间**设置所指定。
- **在期间内仅记录一个数据包的期间：**启用**在期间内仅记录一个数据包**后，此设置会指定日志包含完整数据包数据的频率。
- **捕获数据包数据时存储的最大数据大小：** 要添加到日志的标头数据或数据包数据的最大大小。

规则更新

按照已更新的应用程序类型和入侵防御规则关联的要求自动分配新的入侵防御规则：安全更新有时包括新的或已更新的应用程序类型和入侵防御规则（需要分配辅助入侵防御规则）。如果在安全更新期间分配给策略或计算机的应用程序类型或入侵防御规则需要这些规则，此设置将允许趋势科技服务器深度安全防护系统自动分配这些规则。

SSL 配置（仅限计算机编辑器）

趋势科技服务器深度安全防护系统管理中心支持对 SSL 网络通信进行入侵防御分析。“SSL 配置”页面允许您为一个或多个接口上的指定凭证-端口对创建 SSL 配置。证书可以使用 P12 或 PEM 格式导入，Windows 计算机可以选择直接使用 Windows CryptoAPI。

要创建新的 SSL 配置，请单击**新建**并遵循 **SSL 配置**向导中的步骤。

如果在托管趋势科技服务器深度安全防护系统管理中心的计算机上安装要配置的计算机，该向导将允许您使用趋势科技服务器深度安全防护系统管理中心中已存储的凭证。

双击现有配置以显示其**属性**窗口。

分配

- **常规信息：**SSL 配置的名称和描述，以及在此计算机上是否已启用。
- **接口分配：**要应用此配置的接口。
- **IP 分配：**应用此配置的一个或多个 IP。
- **端口选择：**应用此配置的端口。

凭证

凭证选项卡中列出了现有凭证，且提供了**分配新的凭证...**按钮，可用于更改这些凭证。

> *注意：* *只有趋势科技服务器深度安全防护系统客户端支持过滤 SSL 流量，趋势科技服务器深度安全防护系统设备不支持。客户端不支持过滤实行 SSL 压缩的 SSL 连接。*

有关设置 SSL 过滤的信息，请参阅 **SSL 数据流**。

NSX 安全标记

如果受保护计算机为 NSX vCenter 中的 VM，您可以在发生趋势科技服务器深度安全防护系统入侵防御事件时将 NSX 安全标记应用于 VM。入侵防御事件具有一个严重性级别，此级别由引发此事件的入侵防御规则的严重性级别所决定。

> *注意：* *入侵防御规则的严重性级别可在**规则属性 > 常规**选项卡上进行配置。*

入侵防御规则严重性级别与 NSX 标记的映射关系如下所示：

IPS 规则严重性	NSX 安全标记
严重	IDS_IPS.threat=high
高	IDS_IPS.threat=high
中	IDS_IPS.threat=medium
低	IDS_IPS.threat=low

可通过指定会导致将 NSX 安全标记应用于 VM 的最低入侵防御严重性级别，配置标记机制的敏感度。

触发应用 NSX 安全标记的最低规则严重性设置的选项包括：

- **缺省（无标记）**：未应用任何 NSX 标记。
- **严重**：如果触发了严重性级别为**严重**的入侵防御规则，NSX 标记将应用于 VM。
- **高**：如果触发了严重性级别为**高**或**严重**的入侵防御规则，NSX 标记将应用于 VM。
- **中**：如果触发了严重性级别为**中**、**高**或**严重**的入侵防御规则，NSX 标记将应用于 VM。
- **低**：如果触发了严重性级别为**低**、**中**、**高**或**严重**的入侵防御规则，NSX 标记将应用于 VM。

为在阻止模式下运行的规则和在仅检测模式下运行的规则提供独立设置。

> *注意：* *IPS 规则是在阻止模式还是在仅检测模式下运行，不仅取决于入侵防御模块设置（**计算机/策略编辑器 > 入侵防御 > 常规**选项卡），还取决单个规则本身的配置（**规则属性 > “常规”选项卡 > 详细信息**）。*

事件

除了只显示与此策略或特定计算机相关的事件外，入侵防御事件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。

完整性监控

ESXi 可信平台模块

当 TPM 监控检测到 ESXi 虚拟机监控程序配置有更改时发出警报：可信平台模块 (TPM) 是附加到 VMware ESXi 上的基于硬件的加密模块。它监控 ESXi 的引导顺序并生成加密签名。更改 ESXi 引导顺序可能导致存储图像损坏、篡改、意外或未授权更新或者其他类型的更改。

完整性监控模块可监控计算机上特定区域的更改。它能够监控已安装的软件、运行的服务、进程、文件、目录、侦听端口、注册表项和注册表值。它通过对已分配规则中指定的计算机上的区域执行基线扫描，然后定期重新扫描这些区域以查看其更改来发挥作用。

完整性监控页面包含以下选项卡式部分：

- *常规（第 126页）*
- *高级（第 127页）*
- *事件（第 128页）*

常规

完整性监控

可以将此策略或计算机配置为从其父策略继承完整性监控打开/关闭状态，也可以本地锁定设置。

完整性扫描（仅限计算机编辑器）

单击**扫描完整性**可在此计算机上执行按需完整性扫描。

基线（仅限计算机编辑器）

基线是将完整性扫描的结果与之进行比较的原始安全状态。单击**重新生成基线**可在此计算机上为完整性扫描创建新的基线。单击**查看基线**可查看当前基线数据。

已分配完整性监控规则

显示对此策略或计算机生效的完整性监控规则。要添加或移除完整性监控规则，请单击**分配/取消分配...**此时将出现一个窗口，显示可从中选择或取消选择规则的所有可用完整性监控规则。

在“编辑器”窗口中，可以编辑完整性监控规则以便将更改仅本地应用到编辑器（计算机或策略编辑器）的上下文，也可以编辑规则以便将更改全局应用到使用规则的所有其他策略和计算机。

要对规则进行本地编辑，请选择“规则”并单击“属性...”()，或右键单击“规则”并单击**属性...**

要对规则进行全局编辑，请右键单击“规则”并单击**属性（全局）...**

建议

显示上次执行“漏洞扫描（推荐设置）”的时间和建议完整性监控规则的数量。

另请参阅：

- **策略、继承与覆盖**

高级

内容哈希算法

选择完整性监控模块将用于存储基线信息的哈希算法。您可以选择多个算法，但是不建议这样做，因为这会对性能产生不利影响。

VM 扫描缓存

有关完整性监控扫描缓存配置的信息，请参阅**虚拟设备扫描缓存**。

CPU 使用率

完整性监控会在创建初始基线的系统扫描以及将后续系统状态与之前创建的基线进行比较的系统扫描期间使用本地 CPU 资源。如果您发现完整性监控占用的资源超出了您的预想，可以将 CPU 使用率限制为以下级别：

- **高**：不限制 CPU 使用率
- **中**：完整性监控进程占用的 CPU 资源不超过 50%。
- **低**：完整性监控进程占用的 CPU 资源不超过 25%。

事件

除了只显示与此策略或特定计算机相关的事件外，完整性监控事件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。

日志审查

日志审查模块可标识包含在计算机日志文件中的安全事件。可以将可疑事件转发到 SIEM 系统或集中式日志记录服务器，以进行最终关联、报告及归档。它通过实施 OSSEC.net 上提供的开放源软件来发挥作用。

“日志审查”页面具有以下选项卡：

- *常规（第 130页）*
- *高级（第 131页）*
- *事件（第 132页）*

常规

日志审查

可以将此策略或计算机配置为从其父策略继承日志审查的打开/关闭状态，也可以本地锁定该设置。

已分配日志审查规则

显示对此策略或计算机生效的日志审查规则。要添加或移除日志审查规则，请单击**分配/取消分配...**此时将出现一个窗口，显示可从中选择或取消选择规则的所有可用日志审查规则。

在“编辑器”窗口中，可以编辑日志审查规则以便将更改仅本地应用到编辑器（计算机或策略编辑器）的上下文，也可以编辑规则以便将更改全局应用到使用规则的所有其他策略和计算机。

要对规则进行本地编辑，请选择“规则”并单击“属性...”()，或右键单击“规则”并单击**属性...**

要对规则进行全局编辑，请右键单击“规则”并单击**属性（全局）...**

建议

显示上次执行“漏洞扫描（推荐设置）”的时间和建议日志审查规则的数量。

另请参阅：

- **策略、继承与覆盖**

高级

严重性剪辑

当客户端/设备事件等于或超出以下严重性级别时，将这些事件发送到 syslog：日志审查规则具有严重性级别。此设置确定将这些规则触发的哪些事件发送到 syslog 服务器（如果已启用 syslog）。（要启用 syslog，请转至**管理 > 系统设置 > SIEM**。）

当事件等于或超出以下严重性级别时，将这些事件存储在客户端/设备中以供 DSM 以后检索：此设置确定哪些日志审查事件保存在数据库中并显示在**日志审查事件**页面中。

事件

除了只显示与此策略或特定计算机相关的事件外，日志审查事件的显示方式与它们在趋势科技服务器深度安全防护系统管理中心主窗口中的显示方式相同。

接口/接口类型

接口（计算机编辑器）

显示在计算机上检测到的接口。如果具有多个接口分配的策略已分配给此计算机，则将标识与在策略中定义的特征码相匹配的接口。

接口类型（策略编辑器）

显示在计算机上检测到的接口。如果具有多个接口分配的策略已分配给此计算机，则将标识与在策略中定义的特征码相匹配的接口。

网络接口特性

如果计算机具有多个接口，您可以将策略的各个元素（防火墙规则等）分配给每个接口。要为多个接口配置策略，请选择**规则可应用于特定接口**，然后在下面的文本框中键入与字符串匹配的名称和特征码。

接口类型名称仅供参考。虽然任何名称都可用于映射到您的网络拓扑，但常见名称有“LAN”、“WAN”、“DMZ”和“Wi-Fi”。

“匹配”定义了一个基于通配符的接口名称匹配，用于将接口自动映射到相应的接口类型。例如“Local Area Connection *”、“eth*”和“Wireless *”等。无法自动映射接口时将触发警报。可以从特定计算机的计算机编辑器中的**接口**页面对其进行手动映射。

注意：	*如果在计算机上检测到接口，但这些接口不与其中任何一个条目匹配，则管理中心将会触发警报。*

接口类型（接口特征码）

要强制实现接口隔离，请设置**策略/计算机编辑器** > **防火墙** > **接口隔离**选项卡上的**启用接口隔离**选项，并输入与计算机上接口名称匹配的字符串特征码（按优先级顺序）。

注意：	*趋势科技服务器深度安全防护系统使用 POSIX 基本正则表达式来匹配接口名称。有关基本 POSIX 正则表达式的信息，请访问 http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03*

注意：	*如果输入的字符串特征码与计算机上的多个接口匹配，将允许在所有这些匹配的接口上进行网络通信。要确保只有一个接口处于活动状态，请设置**限制为一个活动接口**选项。*

设置

设置页面包含以下选项卡式部分：

- *计算机（第 135页）*
- *网络引擎（第 138页）*
- *扫描（第 143页）*
- *SIEM（第 144页）*

计算机

通信方向

- **双向：**缺省情况下，通信是双向的。这意味着客户端/设备通常会启动波动信号，但仍会在客户端端口上侦听管理中心的连接。管理中心仍可以自行联系客户端/设备，以执行所需的操作。这样，当安全配置发生更改时，管理中心可立即将更改应用到客户端/设备。
  *趋势科技服务器深度安全防护系统虚拟设备仅能在双向模式下运行。*将虚拟设备的此设置更改为其他任何模式都将破坏功能。
- **管理中心已启动：**选择此选项后，所有管理中心与客户端/设备之间的通信将由管理中心启动。这些通信包括安全配置更新、波动信号操作以及对事件日志的请求等。
- **客户端/设备已启动：**选择此选项后，客户端/设备将不会侦听端口 4118，而是在波动信号设置指定的波动信号端口（缺省为 4120）上联系管理中心。当客户端/设备与管理中心建立 TCP 连接后，便开始执行所有的标准通信：管理中心会先请求客户端/设备的状态和任何事件。（这就是波动信号操作）。如果有待处理的操作需要在计算机上执行（例如，需要更新策略），则会在关闭连接之前执行这些操作。在此模式下，管理中心与客户端/设备之间的通信仅在每个波动信号启动时发生。如果客户端/设备的安全配置已更改，则只有在启动下一个波动信号时才会更新安全配置。

  注意： *在针对客户端/设备启动的通信配置客户端/设备之前，请确保客户端/设备可访问管理中心 URL 和波动信号端口。如果客户端/设备无法解析管理中心 URL，或无法访问 IP 和端口，则此客户端/设备的“客户端/设备启动的通信”将不成功。在**管理 > 系统信息**页面的**系统详细信息**区域中列有管理中心 URL 和波动信号端口。*

注意： *客户端/设备会根据趋势科技服务器深度安全防护系统管理中心的主机名在网络中查找管理中心。因此，您的本地 DNS 中**必须**有管理中心的主机名，才能执行客户端/设备启动的通信或双向通信。*

注意： *为了实现管理中心与客户端/设备之间的通信，管理中心将自动执行（隐藏的）防火墙规则（优先级为 4 的“放行”规则），此规则会在客户端/设备上打开端口 4118，以接受传入的 TCP/IP 网络通信。缺省设置将对任何 IP 地址和任何 MAC 地址开放此端口。您可以建立一个优先级为 4 的“强制允许”或“放行”的新防火墙规则，以限制此端口上的传入网络通信，此规则仅允许来自特定 IP 和/或 MAC 地址的传入 TCP/IP 网络通信。如果这个新防火墙规则的设置符合下列条件，则会替换隐藏的防火墙规则：*

***操作：**强制允许或放行*
***优先级：**4 - 最高*
***数据包流向：**传入*
***帧类型：**IP*
***协议：**TCP*
***数据包目标端口：**4118（或包含 4118 的列表或范围）*

只要这些设置有效，新规则就会替换隐藏的规则。然后，您就可以键入 IP 和/或 MAC 地址的数据包源信息，以限制流向计算机的网络通信。

波动信号

- **波动信号间隔（以分钟为单位）：**两个波动信号之间经过的时间。
- **在引发警报之前可以错过的波动信号数：**此设置确定在管理中心触发警报之前允许错过的波动信号数量。（例如，输入 3 会使管理中心在错过第 4 个波动信号时触发警报。）

> *注意：* *如果计算机是服务器，连续错过的波动信号过多可能表示客户端/设备或计算机本身出现问题。但是，如果计算机是便携式计算机或任何其他可能会持续断开连接的系统，此设置应设为“无限制”。*

- **引发警报之前计算机上的本地系统时间在波动信号之间的最大变化（以分钟为单位）：**对于能够检测系统时钟更改的客户端（Windows 客户端），这些事件会以客户端事件 5004 向管理中心报告。如果更改超过这里列出的时钟更改，就会触发警报。对于不支持此功能的客户端（非 Windows 客户端），管理中心将监控客户端在每次波动信号操作时报告的系统时间，并在检测到的更改超出此设置中指定的允许更改范围时触发警报。

  > *注意：* *一旦触发**计算机时钟已更改**警报，就必须手动解除此警报。*

- **对非活动的虚拟机引发脱机错误：**设置在虚拟机停止或暂停时是否引发脱机错误。

立即发送策略更改

缺省情况下，**自动将策略更改发送到计算机**设置的值为“是”。这意味着对安全策略的任何更改都将自动应用于使用该策略的计算机。如果将此设置更改为“否”，您将需要在**计算机**页面上查找受影响的计算机，然后右键单击这些计算机并从上下文菜单中选择“发送策略”。

故障排除

您可以增加日志记录级别的粒度并记录更多事件以进行故障排除，但使用此选项时请小心，因为启用此选项会大幅增加事件日志的总大小。

客户端自我保护

> *注意：* *“客户端自我保护”功能仅限于 Windows。*

使用这些设置可防止本地用户干扰客户端功能。

- **防止本地最终用户卸载、停止或以其他方式修改客户端：**此操作将防止本地用户卸载客户端、停止客户端服务、修改客户端相关的 Windows 注册表项或修改客户端相关的文件。您可以从命令行发出本地指令来覆盖这些限制。（请参阅**命令行工具**。）启用了客户端自我保护后，如果尝试通过本地操作系统的图形用户界面对客户端进行修改，会收到一条类似于“安全设置禁止删除或修改此应用程序”的消息。
  - **本地覆盖需要密码：**趋势科技服务器深度安全防护系统管理中心可能会失去与客户端通信的能力。在这种情况下，您必须使用客户端的命令行界面与客户端本地进行交互。在此处输入密码，以使用密码保护本地命令行功能。（推荐。）

    > *注意：* *将此密码存储在安全位置。如果丢失或忘记密码，必须联系支持提供商获取帮助以覆盖此保护。*

防恶意软件保护必须处于“**启用**”状态，以防止发生以下情况：

- 停止客户端服务
- 修改客户端相关的 Windows 注册表项
- 修改客户端相关的文件

防恶意软件保护对于防止本地用户卸载客户端不是必需的。

从命令行关闭或打开客户端自我保护：

1. 以管理员身份登录到本地计算机
2. 从客户端（或中继）的安装目录运行命令提示符
3. 输入以下命令（其中 "password" 是使用**本地覆盖需要密码**设置所设置的密码）：
   - 关闭自我防护：
     ```
     dsa_control --selfprotect=0 --passwd=password
     ```
   - 打开自我防护：
     ```
     dsa_control --selfprotect=1 --passwd=password
     ```

   注意： *如果未设置任何密码，请省略 "--passwd" 参数。*

注意： *在趋势科技服务器深度安全防护系统 9.0 及较早版本中，此选项为 --harden=<num>*

或者，可以使用**重置**参数，该参数将重置客户端并禁用客户端自我保护：

- `dsa_control --reset`

环境变量覆盖

完整性监控模块使用环境变量表示 Windows 操作系统的目录系统中的一些标准位置。例如，Microsoft Windows - 'Hosts' file modified 完整性监控规则，其监控对 Windows hosts 文件的更改，并在 C:\WINDOWS\system32\drivers\etc 文件夹中查找该文件。但是，不是所有 Windows 安装都使用 C:\WINDOWS\ 目录，因此完整性监控规则使用 WINDIR 环境变量，并以 %WINDIR%\system32\drivers\etc 的方式表示该目录。

注意： *在虚拟机上执行无客户端完整性监控时，环境变量主要由虚拟设备使用。这是因为虚拟设备无法知道特定虚拟机上的操作系统是否正在使用标准目录位置。*

以下是完整性监控模块使用的缺省环境变量：

名称	值
ALLUSERSPROFILE	C:\ProgramData
COMMONPROGRAMFILES	C:\Program Files\Common Files
PROGRAMFILES	C:\Program Files
SYSTEMDRIVE	C:
SYSTEMROOT	C:\Windows
WINDIR	C:\Windows

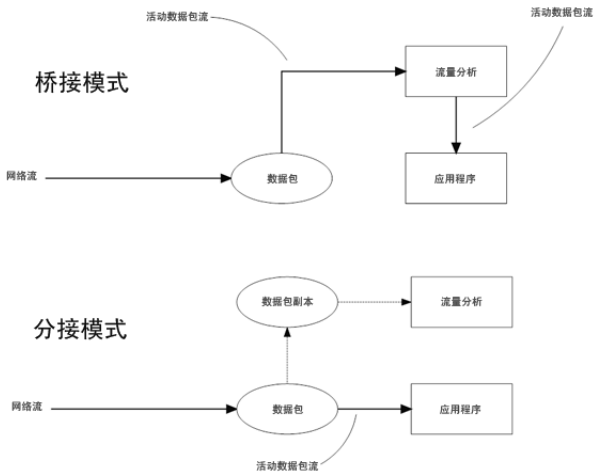
覆盖上述任一环境变量：

1. 单击**查看环境变量...** 按钮显示**环境变量覆盖**页面。
2. 单击菜单栏中的**新建**，然后输入新的名称/值对（例如，WINDIR 和 D:\Windows），然后单击**确定**。

网络引擎

网络引擎

客户端/设备的网络引擎可以桥接模式或分接模式运行。以桥接模式运行时，活动数据包流会经过网络引擎。系统会维护状态表、应用防火墙规则并执行网络通信规范化，以便可以将入侵防御规则应用到有效载荷内容。以分接模式运行时，系统会克隆活动数据包流并从主数据流中转移。在分接模式下，不会修改活动数据包流，所有操作都将在克隆的数据流上执行。



事件

您可以设置每个日志文件的最大大小，以及最新文件的保留数目。系统会不断地在事件日志文件中写入数据，直到达到允许的最大大小，此后，将创建一个新的文件，并开始在其中写入数据，直到达到最大大小，以此类推。达到最大文件数目时，会先删除最旧的文件，然后创建新的文件。事件日志条目的平均大小通常约为 200 字节，因此一个 4 MB 的日志文件大约可保留 20,000 个日志条目。日志文件填满的速度取决于现有规则的数目。

- **事件日志文件的最大大小（在客户端/设备上）**：如果在一台或多台计算机上开始显示“磁盘空间不足”的警报，请调整这些设置。
- **要保留的事件日志文件数（在客户端/设备上）**：如果在一台或多台计算机上开始显示“磁盘空间不足”的警报，请调整这些设置。

> *注意：* ***事件****是单个事件的记录。****计数器****是单个事件发生次数的记录。事件可用于填充****事件****页面。计数器可用于填充“控制台”Widget（过去 7 天的防火墙事件数目等）和“报告”。例如，如果您使用 syslog 来收集事件，则您可能只想要收集计数器；事件可能占用大量的磁盘空间，因此您不会希望存储数据两次。*

- **不记录以下源 IP 的事件**：如果不希望趋势科技服务器深度安全防护系统记录来自某些可信计算机的网络通信事件，可以使用此选项。

> *注意：* *使用以下三种设置可以微调事件聚合。为了节省磁盘空间，趋势科技服务器深度安全防护系统客户端/设备会提取多次出现的相同事件，然后将这些事件聚合到一个条目中，并附加“重复计数”、*

“首次出现”时间戳和“末次出现”时间戳。要聚合事件条目，趋势科技服务器深度安全防护系统客户端/设备需要在内存中缓存这些条目，同时在将其写入磁盘之前聚合它们。

- **缓存大小：**确定在任何给定时间要跟踪的事件类型数。将该值设置为 10 意味着将跟踪 10 种类型的事件（使用重复计数、首次出现时间戳以及末次出现时间戳。）当出现新类型的事件时，最早聚合的 10 个事件将从缓存中刷新并写入磁盘。
- **缓存期限：**确定在将记录刷新到磁盘之前要在缓存中保存该记录的时间。如果此值为 10 分钟，且没有其他内容导致刷新该记录，则保存达 10 分钟的任何记录都会 被刷新到磁盘中。
- **缓存失效时间：**确定保存其重复计数最近未递增的记录的时间。如果缓存期限为 10 分钟，缓存失效时间为 2 分钟，则已经过 2 分钟且未递增的事件记录将被刷新并写入磁盘。

注意： *不管上述设置如何，只要将事件发送给趋势科技服务器深度安全防护系统管理中心，就会刷新缓存。*

高级

使用定制驱动程序设置

- **CLOSED 超时：**用于网关。当网关传递“强制关闭”(RST) 时，网关上收到 RST 的一端会在这段时间内将连接保持在可用状态，然后才会关闭连接。
- **SYN_SENT 超时：**关闭连接之前保持 SYN-SENT 状态的时间。
- **SYN_RCVD 超时：**关闭连接之前保持 SYN-RCVD 状态的时间。
- **FIN_WAIT1 超时：** 关闭连接之前保持 FIN-WAIT1 状态的时间。
- **ESTABLISHED 超时：**关闭连接之前保持 ESTABLISHED 状态的时间。
- **ERROR 超时：**使连接保持错误状态的持续时间。（对于 UDP 连接，错误可能是由任何一种 UDP 问题造成的。对于 TCP 连接，错误可能是由于防火墙丢弃数据包而造成的。）
- **DISCONNECT 超时：** 连接在断开前保持空闲的时间。
- **CLOSE_WAIT 超时：**关闭连接之前保持 CLOSE-WAIT 状态的时间。
- **CLOSING 超时：**关闭连接之前保持 CLOSING 状态的时间。
- **LAST_ACK 超时：**关闭连接之前保持 LAST-ACK 状态的时间。
- **ACK 风暴超时：**在 ACK 风暴中两次重新传送 ACK 之间的最长时间段。换而言之，如果以较低频率重新传送 ACK 时超时，则不会将其视为 ACK 风暴的一部分。
- **引导启动超时：**用于网关。当网关引导时，可能已经建立了通过网关的连接。此超时定义允许非 SYN 数据包的时间长短，此数据包可能是网关引导关闭前已建立的连接的一部分。
- **冷启动超时：**允许非 SYN 数据包的时间长短，此数据包可能属于在状态机制启动前已建立的连接。
- **UDP 超时：**UDP 连接的最长持续时间。
- **ICMP 超时：**ICMP 连接的最长持续时间。
- **允许空 IP：**允许或阻止没有源和/或目标 IP 地址的数据包。
- **在版本 8 及较早版本的客户端和设备上阻止 IPv6：**在较早版本 8 的客户端和设备上阻止或允许 IPv6 数据包。

注意： *趋势科技服务器深度安全防护系统客户端和设备版本 8 及较早版本无法将防火墙或 DPI 规则应用到 IPv6 网络流量，因此这些较早版本的缺省设置是阻止 IPv6 网络通信。*

- **在版本 9 及更高版本的客户端和设备上阻止 IPv6：**在当前的客户端和设备上阻止或允许 IPv6 数据包。
- **连接清理超时：** 清理已关闭连接的间隔时间（参阅下一个设置）。
- **每次清理的最大连接数：**每次定期连接清理所要清理的最大已关闭连接数（请参阅上一个设置）。
- **阻止相同的源-目标 IP 地址：**阻止或允许具有相同的源 IP 地址和目标 IP 地址的数据包。（不适用于回环接口。）
- **最大 TCP 连接数：** 最大同时 TCP 连接数。
- **最大 UDP 连接数：** 最大同时 UDP 连接数。
- **最大 ICMP 连接数：** 最大同时 ICMP 连接数。
- **每秒最大事件数：**每秒可写入的最大事件数。
- **TCP MSS 限制：**MSS 是 TCP 数据包中可以发送且不会被片段化的最大段大小（或最大数据量）。该限制通常在两台计算机建立通信时建立。但在某些情况下，网络通信会通过 MSS 较小的路由器或交换机。在这种情况下，MSS 可以更改。这将造成数据包的重新传送，客户端/设备会将这些数据包记录为“丢弃的重新传送量”。当存在大量丢弃的重新传送量事件条目时，您可能希望降低此限制，并查看卷是否减少。
- **事件节点数：**驱动程序将用于存储日志/事件信息以供随时进行折叠的最大内核内存量。

> *注意：* *当多个相同类型事件连续发生时，事件发生折叠。在这种情况下，客户端/设备会将所有事件“折叠”为一个事件。*

- **忽略状态代码：**使用此选项可忽略某些类型的事件。例如，如果您获取大量“标志无效”，则只需忽略该事件的所有实例。
- **忽略状态代码：**同上。
- **忽略状态代码：**同上。
- **高级日志记录策略：**
  - **放行：** 不执行事件过滤。覆盖“忽略状态代码”设置（如上所述）及其他高级设置，但不覆盖趋势科技服务器深度安全防护系统管理中心中定义的日志记录设置。例如，在趋势科技服务器深度安全防护系统管理中心中通过“防火墙状态配置属性”窗口设置的“防火墙状态配置”日志记录选项将不会受到影响。
  - **缺省：**如果引擎处于分接模式，将切换至“分接模式”（下方）；如果引擎处于桥接模式，将切换至“正常”（上方）。**正常：** 除了丢弃的重新传送量，将记录所有事件。
  - **向后兼容性模式：**仅供支持人员使用。
  - **详细模式：** 除了包括丢弃的重新传送量，均与“正常”相同。
  - **状态和规范化抑制：**忽略丢弃的重新传送量、连接断开、标志无效、序列无效、ACK 无效、未经请求的 UDP、未经请求的 ICMP 以及不允许的策略。
  - **状态、规范化和片段抑制：** 忽略**“状态和规范化抑制”**忽略的一切内容，以及与片段化相关的事件。
  - **状态、片段和验证程序抑制：** 忽略**“状态、规范化和片段抑制”**忽略的一切内容，以及与验证程序相关的事件。
  - **分接模式：**忽略丢弃的重新传送量、连接断开、标志无效、序列无效、ACK 无效、最大的 ACK 重新传送量和已关闭连接中的数据包。

> *注意：* *有关在**状态和规范化抑制；状态、规范化和片段抑制；状态、片段和验证程序抑制以及分接**模式下忽略了哪些事件的更完整列表，请参阅参考部分中的***高级日志记录策略模式**。

- **静默 TCP 连接丢弃：** 当启用“静默 TCP 连接丢弃”时，RST 数据包将仅发送至本地堆栈。未在线发送任何 RST 数据包。这将减少发送回潜在攻击者的信息量。

> *注意：* *如果启用“静默 TCP 连接断开”，还必须调整“DISCONNECT 超时”。“DISCONNECT 超时”的可能值范围为 0 秒至 10 分钟。该超时值必须设置得足够高，以便连接在被趋势科技服务器深度安全防护系统客户端/设备关闭之前先由应用程序关闭。影响 DISCONNECT 超时值的因素包括操作系统、创建这些连接的应用程序以及网络拓补。*

- **启用调试模式：**在调试模式下，客户端/设备会捕获一定数量的数据包（由以下设置指定：要在调试模式下保留的数据包数）。如果触发某个规则且调试模式处于打开状态，客户端/设备将保留触发该规则之前传递的最后 X 个数据包的记录。它会将这些数据包作为调试事件返回给管理中心。

> *注意：* *调试模式极易生成大量日志，且只有在客户端服务部门的监督下才能使用。*

- **要在调试模式下保留的数据包数量：**当调试模式开启时要保留和记录的数据包数量。
- **记录所有数据包数据：**记录与特定防火墙规则或入侵防御规则无关的事件的数据包数据。也就是说，记录诸如“丢弃的重新传送量”或“ACK 无效”等事件的数据包数据。

> *注意：* *由于事件发生折叠而聚合的事件无法保存其数据包数据。*

- **在期间内仅记录一个数据包：**如果已启用此选项且未启用**记录所有数据包数据**，则大多数日志将仅包含标头数据。将定期附加完整数据包，如**在期间内仅记录一个数据包的期间**设置所指定。
- **在期间内仅记录一个数据包的期间：**启用**在期间内仅记录一个数据包**后，此设置会指定日志包含完整数据包数据的频率。
- **捕获数据包数据时存储的最大数据大小：**要添加到日志的标头数据或数据包数据的最大大小。
- **生成 TCP 连接事件：**每次建立 TCP 连接时都会生成防火墙事件。
- **生成 ICMP 连接事件：**每次建立 ICMP 连接时都会生成防火墙事件。
- **生成 UDP 连接事件：**每次建立 UDP 连接时都会生成防火墙事件。
- **绕开 Cisco WAAS 连接：**对于使用选定的专有 CISCO WAAS TCP 选项启动的连接，此模式会绕开对 TCP 序列号的状态分析。此协议会在无效的 TCP 序列号和 ACK 编号中包含额外信息，这会影响防火墙状态检查。仅当使用 CISCO WAAS 且在防火墙日志中显示与无效的 SEQ 或 ACK 的连接时，启用此选项。选择此选项后，对于未启用 WAAS 的连接，将仍执行 TCP 序列号状态检查。
- **丢弃规避重新传送量：**将丢弃包含已经过处理的数据的传入数据包，以避免可能的不明确重新传送攻击技术。
- **验证 TCP 校验和：**片段的校验和文本框数据将用于评估该片段的完整性。
- **最小片段偏移量：**定义可接受的最小 IP 片段偏移量。其偏移量小于此值的数据包将被丢弃，原因是“IP 片段偏移量太小”。如果将其设置为 0，则无任何限制。（缺省值为 60）
- **最小片段大小：**定义可接受的最小 IP 片段大小。大小小于此值的片段化数据包将被丢弃，原因是“第一个片段太小”，可能包含恶意内容。（缺省值为 120）
- **SSL 会话大小：**设置为 SSL 会话密钥维护的最大 SSL 会话条目数。
- **SSL 会话时间：**设置 SSL 会话续订密钥在过期之前的有效时间。
- **过滤 IPv4 隧道：**未用于趋势科技服务器深度安全防护系统 9.5。
- **过滤 IPv6 隧道：**未用于趋势科技服务器深度安全防护系统 9.5。
- **严格的 Teredo 端口检查：**未用于趋势科技服务器深度安全防护系统 9.5。
- **丢弃 Teredo 异常：**未用于趋势科技服务器深度安全防护系统 9.5。
- **最大隧道深度：**未用于趋势科技服务器深度安全防护系统 9.5。
- **超出最大隧道深度时的操作：**未用于趋势科技服务器深度安全防护系统 9.5。
- **丢弃 IPv6 扩展类型 0：**未用于趋势科技服务器深度安全防护系统 9.5。
- **丢弃低于最低 MTU 的 IPv6 片段：**丢弃不满足 IETF RFC 2460 规定的最低 MTU 大小的 IPv6 片段。

- **丢弃 IPv6 保留地址**：丢弃以下保留地址：
  - IETF reserved 0000::/8
  - IETF reserved 0100::/8
  - IETF reserved 0200::/7
  - IETF reserved 0400::/6
  - IETF reserved 0800::/5
  - IETF reserved 1000::/4
  - IETF reserved 4000::/2
  - IETF reserved 8000::/2
  - IETF reserved C000::/3
  - IETF reserved E000::/4
  - IETF reserved F000::/5
  - IETF reserved F800::/6
- **丢弃 IPv6 站点本地地址**：丢弃站点本地地址 FEC0::/10。
- **丢弃 IPv6 Bogon 地址**：丢弃以下地址：
  - "loopback ::1
  - "IPv4 compatible address", ::/96
  - "IPv4 mapped address" ::FFFF:0.0.0.0/96
  - "IPv4 mapped address", ::/8
  - "OSI NSAP prefix (deprecated by RFC4048)" 0200::/7
  - "6bone (deprecated)", 3ffe::/16
  - "Documentation prefix", 2001:db8::/32
- **丢弃 6to4 Bogon 地址**：丢弃以下地址：
  - "6to4 IPv4 multicast", 2002:e000:: /20
  - "6to4 IPv4 loopback", 2002:7f00:: /24
  - "6to4 IPv4 default", 2002:0000:: /24
  - "6to4 IPv4 invalid", 2002:ff00:: /24
  - "6to4 IPv4 10.0.0.0/8", 2002:0a00:: /24
  - "6to4 IPv4 172.16.0.0/12", 2002:ac10:: /28
  - "6to4 IPv4 192.168.0.0/16", 2002:c0a8:: /32
- **丢弃有效载荷为零的 IP 数据包**：丢弃有效载荷为零长度的 IP 数据包。
- **片段超时**：如果采用此配置，若入侵防御规则认为数据包（或数据包片段）的内容可疑，则会检查这些内容。此设置将确定在检查后到丢弃数据包之前，等待剩余数据包片段的时间长短。
- **要保存的最大片段 IP 数据包数量**：指定趋势科技服务器深度安全防护系统将保留的片段化数据包的最大数。
- **发送 ICMP 以表示片段数据包超时**：启用此设置且片段超时后，ICMP 数据包将发送到远程计算机。

扫描

打开的端口

选择趋势科技服务器深度安全防护系统管理中心在发现的计算机上执行端口扫描时要使用的端口列表。（下拉列表中的端口列表与**共享**部分中**端口列表**页面中定义的端口列表相同。）

建议

客户端可以定期扫描其计算机上的常见应用程序，然后根据检测结果来提出规则建议。对于已配置为允许扫描的计算机，此设置可以设置计算机的扫描时间间隔。

注意： *此设置与执行“漏洞扫描 （推荐设置）”的预设任务不同。如果希望定期进行“漏洞扫描 （推荐设置）”，应选择此选项或者创建预设任务（**管理 > 预设任务**），但不要同时执行两种操作。有关预设任务的更多信息，请参阅预设任务（第 171页）。*

虚拟设备扫描（仅限策略编辑器）

虚拟设备包含各种设置，可以显著提高已执行无客户端保护的大型虚拟机环境中的安全扫描效率。

- **最大并发扫描数：**扫描请求由虚拟设备进行排队并按到达的顺序执行。但是，虚拟设备能够在多个 VM 上执行并发扫描。建议的并发扫描数为 5。如果超过 10，虚拟设备的性能可能会开始下降。
- **恶意软件按需扫描的最大缓存条目数:**对于手动（按需）恶意软件扫描，此设置可确定标识并描述要保留的文件或其他类型的可扫描内容的最大记录数。一百万个条目将使用约 100MB 的内存。
- **恶意软件实时扫描的最大缓存条目数:**对于实时恶意软件扫描，此设置可确定标识并描述要保留的文件或其他类型的可扫描内容的最大记录数。一百万个条目将使用约 100MB 的内存。
- **完整性监控扫描的最大缓存条目数：**对于完整性监控，此设置可确定完整性监控的基线数据中包括的最大条目数。二十万个实体将使用约 100MB 的内存。

SIEM

事件转发频率（来自客户端/设备）

选择将事件从客户端/设备发送到警报收件人的频率。（在“事件转发”区域输入 syslog 配置。）

事件转发

来自各个防护模块的事件都可以通过 syslog 转发到远程计算机。有关配置 Syslog 的信息，请参阅 Syslog 集成(SIEM)。

更新（仅限计算机编辑器）

如果已为此计算机启用中继模块，则“安全更新”页面将显示中继当前分发至客户端/设备的组件（特征码），这些客户端/设备依靠该组件进行安全更新。如果为此计算机启用了防恶意软件模块，此页面还将显示在计算机本地生效的特征码集。

下载安全更新：获取可从趋势科技服务器深度安全防护系统中继组分配至此计算机的最新安全更新。

还原安全更新：将当前安全更新还原到之前在此计算机上生效的安全更新。此按钮将不会为中继显示。

覆盖

趋势科技服务器深度安全防护系统中的策略设计采用层级结构进行创建。作为管理员，您首先创建一个或多个基本策略，然后创建多个子策略级别，这些子策略将更为详细。您可以在顶级策略分配广泛适用的规则和其他配置设置，之后在子策略级别向下时便会更有针对性，最后在单个计算机级别执行规则和配置分配。

随着您在策略树中向下移动，能够分配更具体的设置，同时也可以从策略树的更高级别覆盖设置。此**覆盖**页面向您显示是否在此策略或特定计算机级别覆盖了设置以及覆盖了多少设置。要在此级别撤销覆盖，请单击**移除**按钮。

有关更多信息，请参阅**策略、继承与覆盖**。

管理

趋势科技服务器深度安全防护系统管理中心的“管理”部分包括以下部分：

- 使用*系统设置（第 148页）*部分可控制对趋势科技服务器深度安全防护系统的管理。
- 所有当前已定义的标记将显示在*标记（第 56页）*页面中。
- 使用*预设任务（第 171页）*部分可配置自动完成的重复性任务。
- 使用*基于事件的任务（第 173页）*部分可配置发生特定事件时将要执行的任务。
- *系统信息（第 188页）*页面包含有关趋势科技服务器深度安全防护系统管理中心的当前状态的详细信息。
- 使用*角色（第 183页）*部分可定义具有不同权限的各种角色。然后将角色分配给用户。
- 使用*用户（第 180页）*部分可创建和修改趋势科技服务器深度安全防护系统管理中心用户的用户帐户。
- 使用*联系人（第 187页）*部分可创建和修改联系人。
- *使用授权（第 179页）*页将显示有关趋势科技产品使用授权的详细信息，如哪些趋势科技服务器深度安全防护系统防护模块可用以及授权您可以在多少台计算机上安装客户端/设备软件。
- *更新（第 189页）*部分用于管理安全和软件更新。

系统设置

系统设置页面包含以下选项卡式页面：

- *租户（第 149页）*
- *客户端（第 152页）*
- *警报（第 154页）*
- *上下文（第 155页）*
- *SIEM（第 156页）*
- *SNMP（第 157页）*
- *排序（第 158页）*
- *系统事件（第 160页）*
- *安全（第 161页）*
- *更新（第 163页）*
- *智能反馈（第 165页）*
- *SMTP（第 166页）*
- *存储（第 167页）*
- *代理（第 168页）*
- *高级（第 169页）*

租户

多租户选项

- **多租户使用授权模式：**可以在设置多租户后更改多租户使用授权模式，但是请务必注意，从“已继承”切换到“每租户”将使现有租户不再具有任何授权的模块。
- **允许租户使用“备份”预设任务：**确定**备份**预设任务是否可供租户使用。在大多数情况下，备份应由数据库管理员管理，且应选中该选项。
- **允许租户使用“运行脚本”预设任务：**脚本存在潜在危险的系统访问权限级别，但可以缓解风险，因为必须在管理中心上使用文件系统访问权限安装脚本。
- **允许租户运行“计算机查找”(直接以及作为预设任务)：**确定查找是否公开。在禁止网络查找的服务提供商环境中，可能不需要执行此操作。
- **允许租户运行“端口扫描”(直接以及作为预设任务)：**确定是否可以执行端口扫描。在禁止网络扫描的服务提供商环境中，可能不需要执行此操作。
- **允许租户添加 VMware vCenter：**确定 vCenter 连接是否应公开。如果要对公共服务进行部署，很可能应禁用此选项，因为没有从托管服务到 vCenter 的路由。
- **允许租户添加云帐户：**确定租户是否可以设置云同步。这通常对所有部署均适用。
- **允许租户与 LDAP 目录同步：**确定租户是否可以设置用户和计算机与目录（对于计算机为 LDAP 或 Active Directory，对于用户仅为 Active Directory）同步。如果要对公共服务进行部署，很可能应禁用此选项，因为没有从托管服务到目录的路由。
- **允许租户配置 SNMP 设置：**允许租户将系统事件转发到远程计算机（通过 SNMP）
- **向租户显示简介 (仅当启用了所有“添加”和“同步”选项时建议使用)：**租户首次登录时，自动向其显示介绍幻灯片。（可通过以下方式访问幻灯片：单击 趋势科技服务器深度安全防护系统管理中心窗口右上角的**帮助**链接并选择**简介**。）
- **显示“忘记密码？”选项：**登录窗口中将显示一个链接，用户可通过该链接重置密码。（请注意，必须在**管理 > 系统设置 > SMTP** 选项卡上正确配置 SMTP 设置，此选项才能有效。）
- **显示“记住帐户名和用户名”选项：**趋势科技服务器深度安全防护系统将记住用户的帐户名和用户名，并会在登录窗口加载时填充这些字段。
- **允许租户控制从主租户访问：**缺省情况下，主租户可以使用**管理 > 租户**页面上的**以租户身份登录**选项，登录到租户帐户。选中**允许租户控制从主租户访问**选项后，租户可以（在**管理 > 系统设置 > 高级**下）允许或阻止主租户访问其趋势科技服务器深度安全防护系统环境。（此选项启用后，租户环境中的缺省设置是阻止主租户访问。）

  注意： *无论何时主租户访问租户帐户，访问都将记录在租户的系统事件中。*

- **允许租户使用我的“缺省中继组”中的中继 (对于未分配的中继)：**允许租户自动访问主租户中的中继设置。这使租户可以免于为安全更新设置专用中继。

  注意： *租户转至**管理 > 系统设置**页面上的**更新**选项卡，并取消选择**使用主租户中继组作为我的缺省中继组（对于未分配的中继）**选项即可拒绝使用“共享”中继。如果租户取消选择此设置，则他们必须为自己设置专用中继。*

  注意： *如果共享中继，主租户有责任使中继保持最新。这通常涉及定期为所有中继创建**下载安全更新**预设任务。*

- **新租户自动下载最新的安全更新：**新建租户帐户后，该帐户会立即检查并下载最新的可用安全更新。
- **锁定并隐藏以下项（所有租户都将使用为主租户配置的选项）：**
  - **“客户端”选项卡上的“数据隐私”选项：**允许主租户配置数据隐私设置。（此设置仅适用于**管理 > 系统设置 > 客户端**选项卡上的“允许对加密流量 (SSL) 进行数据包数据捕获”。）
  - **“SIEM”选项卡上的所有选项（所有租户对所有事件类型使用 SIEM 选项卡上的设置，syslog 将通过管理中心中继）：**允许主租户一次为所有租户配置 syslog。在 CEF 格式中，租户名称作为 TrendMicroDsTenant 包含其中。
  - **“SMTP”选项卡上的所有选项：**锁定 SMTP 选项卡上的所有设置。
  - **“存储”选项卡上的所有选项：**锁定**存储**选项卡上的所有设置。

数据库服务器

缺省情况下，将在随趋势科技服务器深度安全防护系统管理中心一起安装的同一数据库服务器上创建所有租户。为提供其他可伸缩性，趋势科技服务器深度安全防护系统管理中心支持添加其他数据库服务器。

对于 SQL Server，辅助数据库服务器需要主机名、用户名和密码（域和命名实例是可选的）。TCP/命名管道设置必须与主数据库相同（始终建议 TCP）。用户（趋势科技服务器深度安全防护系统管理中心）必须具有以下权限：

- 创建数据库、
- 删除数据库和
- 定义架构。

此帐户不仅用于创建数据库，而且还用于认证创建的数据库。

Oracle 多租户使用不同的型号。新数据库定义定义了绑定到表空间的用户。该用户用于在 Oracle 上“启动”其他用户的创建。

有关为多租户设置数据库用户帐户的信息，请参阅**多租户**。

如果服务器上没有租户，则可以删除数据库服务器（主服务器除外）。

如果主机名、用户名、密码或任何详细信息发生更改，则可以使用 GUI 更改数据库服务器（主服务器除外）。要更改主服务器的值，必须关闭趋势科技服务器深度安全防护系统管理中心（所有节点），并使用新的详细信息编辑 dsm.properties 文件。

新建租户模板

租户模板功能提供了一种为新租户创建定制的“全新”体验的方便方法。

过程包括：

1. 创建新租户
2. 以该租户身份登录
3. 定制示例策略（添加/删除/修改）和安全更新版本（应用较新版本）
4. 返回主租户并运行租户模板向导
5. 选择要创建快照的租户

所有将来的租户将具有示例策略和包含在快照中的规则更新版本。

此功能在某些示例不适用或需要创建特殊示例的服务提供商环境中可能有用。

与往常一样，示例必须是起点。建议租户根据其特定需求创建策略。

注意：	*创建新模板不会影响现有租户。*

防护使用情况监控

趋势科技服务器深度安全防护系统会收集有关受保护计算机的信息。此信息在控制台上的**租户** Widget 和**租户防护活动** Widget 中可见。租户报告中也提供了此信息，并且可通过 REST API 获得该信息。

注意：	*在大多数基本情况下，监控可以帮助确定趋势科技服务器深度安全防护系统管理中心的防护小时数百分比（通过报告或 API）。通常称为 "viewback" 或 "chargeback"，此信息可用于各种方式。在更高级的情况下，此信息可用于根据诸如租户计算机操作系统等特征来定制收费。*

使用这些选项可确定要记录租户计算机的其他哪些详细信息。

客户端

主机名

如果将某个 IP 作为一个主机名使用，并且在客户端/设备启动的通信或查找之后，在计算机上检测到 IP 发生更改，请更新“主机名”条目：如果检测到 IP 发生更改，则更新计算机的“主机名”属性字段中显示的 IP 地址。(趋势科技服务器深度安全防护系统管理中心始终根据唯一的指纹而不是其 IP 地址或主机名来识别计算机。)

如果将某个 IP 不作为一个主机名使用，并且在客户端/设备启动的通信或查找之后，在计算机上检测到主机名发生更改，请更新“主机名”条目：如果检测到主机名发生更改，则更新计算机的“主机名”属性字段中显示的主机名。(趋势科技服务器深度安全防护系统管理中心始终根据唯一的指纹而不是其 IP 地址或主机名来识别计算机。)

客户端启动的激活

在计算机上安装和激活客户端的标准方法是在计算机上安装客户端，然后使用趋势科技服务器深度安全防护系统管理中心“激活客户端”。此激活操作会将唯一的加密指纹从管理中心发送到客户端，此时客户端会拒绝任何未经该指纹确认为来自该管理中心的指令。

但在某些情况下，此激活最好由客户端启动，而不是由管理中心启动。(例如，大型、分布式安装。)在这种情况下，必须将管理中心配置为允许客户端与其通信并启动激活。使用**客户端启动的激活**面板设置限制，根据该限制，计算机可以启动其自己的客户端激活。

客户端启动的激活是从命令行执行的。以下是与客户端激活相关的命令行选项：

用法： `dsa_control [-a <str>] [-g <str>] [-c <str>] [-r]`		注意
`-a <str>`	在指定的 URL 使用管理中心**激活**客户端。URL 格式必须为“dsm://hostOrIp:port/”	"port" 是管理中心的波动信号端口。(缺省端口为 4120。)
`-g <str>`	**客户端** URL。缺省情况下为 "https://127.0.0.1:4118/"	
`-c <str>`	证书文件	
`-r`	重置客户端配置	

注意： *可以指示趋势科技服务器深度安全防护系统管理中心将缺省的策略发送给自我激活的客户端，这些客户端尚未分配策略。使用**要分配的策略 (如果策略未由激活脚本分配)**选项选择策略。*

如果允许客户端启动的激活，则可以进一步配置多种选项：

指定要允许客户端启动的激活的计算机：

- **对于任何计算机：**所有计算机，无论是否已列在趋势科技服务器深度安全防护系统管理中心的**计算机**页面中。
- **对于现有计算机：**仅限**计算机**页面中已列出的计算机。
- **对于以下 IP 列表中的计算机：**仅限在指定的 IP 列表中具有匹配的 IP 地址的计算机。

要分配的策略 (如果激活脚本未分配任何策略)：要分配给计算机的安全策略(如果未在激活脚本中指定任何策略)。

注意： *如果存在基于事件的任务（此任务会将策略分配给激活是通过客户端启动的计算机），则在基于事件的任务中指定的策略将覆盖在此处或者在激活脚本中分配的策略。*

如果同名计算机已存在：如果**计算机**页面中已列出具有相同主机名的计算机，趋势科技服务器深度安全防护系统管理中心可以执行以下操作：

- **不允许激活：**趋势科技服务器深度安全防护系统管理中心将不允许激活客户端。
- **激活同名的新计算机：**如果列出的计算机未激活，则将允许客户端启动的激活以继续进行操作，并且新计算机将取代“计算机”页面中已列出的计算机。
- **重新激活现有计算机：**新计算机将激活/重新激活并取代列出的计算机，而无论列出的计算机是否已激活。

允许重新激活克隆 VM：当运行已激活的趋势科技服务器深度安全防护系统客户端的新 VM 克隆向趋势科技服务器深度安全防护系统管理中心发送波动信号时，趋势科技服务器深度安全防护系统管理中心会将其识别为克隆，并将其作为新计算机重新激活。系统不会将可能存在于原始 VM 上的任何策略或规则分配给新 VM。新 VM 仅如同一个新激活的计算机。

允许重新激活未知 VM：对于以前激活、已从云环境中移除且已从趋势科技服务器深度安全防护系统管理中心中删除的 VM，如果它们已添加回 VM 目录，则可将其重新激活。趋势科技服务器深度安全防护系统管理中心将识别 VM 上的有效证书，并允许将其重新激活。系统不会将可能存在于原始 VM 上的任何策略或规则分配给新 VM。新 VM 仅如同一个新激活的计算机。

注意： *有关客户端启动的激活的更多信息，请参阅***命令行工具***和***部署脚本***。*

数据隐私

允许对加密流量 (SSL) 进行数据包数据捕获：入侵防御模块允许您记录触发入侵防御规则的数据包数据。通过此设置，可以在对加密流量应用入侵防御规则时关闭数据捕获。

无客户端 vCloud 保护

允许 vCloud VM 的设备保护：允许趋势科技服务器深度安全防护系统虚拟设备保护 vCloud 环境中的虚拟机，并允许多租户趋势科技服务器深度安全防护系统环境中的租户管理虚拟机的安全。

警报

警报

查看警报配置... 配置趋势科技服务器深度安全防护系统管理中心的所有可能警报。在大多数情况下，这表示将其打开或关闭、设置其严重性级别以及配置警报的电子邮件通知设置。

引发警报前更新可以保持未决状态的时间： 在执行正在发送的安全更新的指令与在引发警报前执行的指令之间可能需要的时间。

警报事件转发 (来自管理中心)

输入用于接收所有警报电子邮件的电子邮件地址，不管是否设置了接收通知的用户，都会发送到此电子邮件地址。（在趋势科技服务器深度安全防护系统管理中心的**警报**部分中配置哪些警报会触发发送电子邮件的操作。）

上下文

使用此页面可配置趋势科技服务器深度安全防护系统设置，以确定受保护计算机是否连接到 Internet 的设置。可以根据计算机的网络连接状况，有条件地应用某些趋势科技服务器深度安全防护系统规则。这称为“位置感知”。可以在某个特定规则的**属性**窗口的**选项**选项卡上配置该规则的 Internet 连接条件选项。在实施接口隔离时也可以使用 Internet 连接测试。（请参阅*接口隔离（第 115页）*和*接口/接口类型（第 133页）*。）

Internet 连接测试

- **测试 Internet 连接状态所用的 URL：**将 HTTP 请求发送到此 URL，以测试 Internet 连接。（必须包括 "http://"。）
- **确认 Internet 连接状态所用的返回内容的正则表达式：**将应用到返回内容的正则表达式，用以确认 HTTP 通信是否成功。（如果确定返回内容，则可以使用字符的简单字符串。）

  注意： *趋势科技服务器深度安全防护系统使用 POSIX 基本正则表达式来匹配接口名称。有关基本 POSIX 正则表达式的信息，请访问 http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03*

- **测试间隔：**两次连接测试之间的时间间隔。

示例

例如，要测试 Internet 连接，可以使用 URL "http://www.example.com"，以及在该 URL 中由服务器返回的字符串 "This domain is established to be used for illustrative examples in documents"。

SIEM

系统事件通知 (来自管理中心)

将系统事件转发到远程计算机 (通过 Syslog)：通知可发送到 Syslog 服务器。在此处键入 syslog 服务器的详细信息。

在策略和计算机级别配置防护模块事件转发。要配置防护模块事件转发，请转到**策略/计算机编辑器 > 设置 > SIEM**。

有关配置 Syslog 的信息，请参阅 **Syslog 集成 (SIEM)**。

SNMP

将系统事件转发到远程计算机 (通过 SNMP)

趋势科技服务器深度安全防护系统支持 SNMP 将系统事件转发到管理中心的某台计算机上。MIB 文件 ("DeepSecurity.mib") 位于 \Trend Micro\Deep Security Manager\util

排序

排序

排序系统提供了一种量化事件重要性的方法。先为计算机分配“资产值”，并为规则分配严重性或风险值，然后，将两个值相乘便可得出事件的重要性（“排序”）。这允许您按排序来排列事件的顺序。

Web 信誉事件风险值

Web 信誉事件的风险值与 **Web 信誉**页面的**常规**选项卡上的 Web 信誉设置使用的三种风险级别相关联：

- **危险:**对应于“已确认为欺诈性或已知威胁源的 URL”。
- **高度可疑：**对应于“怀疑为欺诈性或已知威胁源的 URL”。
- **可疑：**对应于“与垃圾邮件相关或者可能有危害的 URL”。
- **已被管理员阻止：**位于 Web 信誉服务**阻止**列表中的 URL。
- **未测试：**没有风险级别的 URL。

防火墙规则严重性值

防火墙规则的严重性值与防火墙规则的操作相关联，这些操作包括：“拒绝”、“仅记录”和“数据包拒绝”。（后者指由于防火墙状态配置设置而拒绝数据包。）使用此面板可以编辑严重性值，将此值与计算机的资产值相乘就可以确定防火墙事件的排序。（可以在规则的**属性**窗口查看和编辑防火墙规则处理措施。）

入侵防御规则严重性值

入侵防御规则严重性值与其严重性级别相关联，严重性级别包括：“严重”、“高”、“中”、“低”或“错误”。使用此面板可以编辑值，将此值与计算机的资产值相乘就可以确定入侵防御事件的排序。可以在规则的**属性**窗口查看入侵防御规则的严重性设置。

完整性监控规则严重性值

完整性监控规则严重性值与其严重性级别相关联，严重性级别包括：“严重”、“高”、“中”或“低”。使用此面板可以编辑其值，将此值与计算机的资产值相乘就可以确定完整性监控事件的排序。可以在规则的**属性**窗口查看完整性监控规则的严重性。

日志审查规则严重性值

日志审查规则严重性值与其严重性级别相关联，严重性级别包括：“严重”、“高”、“中”或“低”。使用此面板可以编辑其值，将此值与计算机的资产值相乘就可以确定日志审查事件的排序。可以在规则的**属性**窗口查看和编辑日志审查规则的严重性级别。

资产值

资产值与其任何其他属性（如入侵防御规则或防火墙规则）无关联。资产值本身就是属性。可以从计算机的**详细信息**窗口查看和编辑计算机资产值。要简化分配资产值的过程，可以预定义一些要在计算机**详细信息**窗口第一个页面中的**资产重要性**下拉列表中出现的值。要查看现有的预定义计算机资产值，请在此面板中单击**查看资产值...** 按钮。**资产值**窗口会显示预定义的设置。可以更改这些值，也可以创建新值。（新的设置会出现在所有计算机的下拉列表中。）

系统事件

系统事件

“系统事件”包括客户端/设备和趋势科技服务器深度安全防护系统管理中心的活动及其配置的变更。它们还包括在趋势科技服务器深度安全防护系统正常操作期间可能发生的错误。

可在此页面为每种类型的系统事件配置**记录**和**转发**选项：

- **记录：** 趋势科技服务器深度安全防护系统管理中心将记录此类事件，并将其列在**事件 & 报告** > **事件** > **系统事件**页面上。
- **转发：** 如果您已在**管理** > **系统设置** > SIEM 或**管理** > **系统设置** > SNMP 页面上配置了系统事件通知，则 趋势科技服务器深度安全防护系统管理中心会将此类事件转发至远程计算机。

有关所有可能的系统事件列表，请参阅**参考**部分中的**系统事件**。事件会保留一段时间，此时间可通过**管理** > **系统设置** > **存储**页面进行设置。

安全

用户安全

- **会话超时：**指定要求用户重新登录的间隔不活动时间段。
- **允许的不正确登录尝试次数（在锁定之前）：**单个用户（即具有特定用户名）在被锁定之前可以使用不正确密码尝试登录的次数。只有具有“可以编辑用户属性”权限的用户才可以解锁已锁定的用户。
- **每个用户允许的并发会话数：**每个用户允许的最多并发会话数。
- **用户密码过期：**密码失效的天数。也可将密码设置为永不过期。
- **用户密码最小长度：**密码所需的最少字符数。
- **用户密码需要使用字母和数字：**密码必须由字母（a-z、A-Z）以及数字（0-9）组成。
- **用户密码需要使用大写和小写字符：**必须既使用大写字符又使用小写字符。
- **用户密码需要使用非字母数字字符：**密码必须包括非字母数字字符。

注意：	*为了更安全起见，应严格满足密码要求：最少 8 个字符，同时包括数字和字母，使用大小写，包括非字母数字字符，并且定期过期。*

注意：	*在同时以两个用户的身份登录时，请注意：记住将 Firefox 的会话 Cookie 设置为以每个进程为基础，而非以每个窗口为基础。这表示，由于某些原因您需要同时以两个用户的身份登录，您将必须使用两个不同的浏览器（如果其中一个为 Firefox），或者从两台单独的计算机登录。*

注意：	*如果某用户由于特殊原因（例如，不成功的登录尝试次数太多）而被锁定，且其余用户没有足够权限将该帐户解锁，请联系趋势科技以获取帮助。*

登录页面消息

输入将在趋势科技服务器深度安全防护系统管理中心的登录页面显示的文本。

信任证书

单击**查看证书列表...** 可查看 趋势科技服务器深度安全防护系统管理中心接受的所有安全证书的列表。

生成用于 Microsoft Azure 的证书和密钥对

在将 Microsoft Azure 资源添加到趋势科技服务器深度安全防护系统管理中心之前，您需要生成证书和密钥对。生成所需文件后，将证书（.cer 文件）导入 Azure Web 服务控制台。添加 Microsoft Azure 资源后，将密钥对（.pem 文件）上传至趋势科技服务器深度安全防护系统管理中心。

创建证书和密钥对：

1. 在趋势科技服务器深度安全防护系统管理中心，转至**管理** > **系统设置** > **安全**。

2. 在**密钥对生成**下，单击**生成密钥对**。
3. 单击**创建密钥对**。
4. 本地保存 .pem 文件。
5. 单击**导出证书**。
6. 本地保存 .cer 文件。
7. 单击**关闭**。

更新

要确保获得最大程度的保护，必须保持软件、安全规则和特征码是最新的。通过**管理** > **系统设置**页面上的**更新**选项卡可设置趋势科技服务器深度安全防护系统管理中心检查更新的位置。要查看当前更新的状态，请转至**管理** > **更新**页面。

安全更新

主安全更新源

- **趋势科技更新服务器：**连接到缺省的趋势科技更新服务器。
- **其他更新源：**如果提供有备用的更新源，请在此处输入 URL（包括 "http://" 或 "https://"）。（支持 SSL 连接。）

特征码

- **如果趋势科技服务器深度安全防护系统中继不可用，则允许客户端/设备从此源下载特征码更新：**如果客户端/设备无法与中继通信，则将从趋势科技更新服务器（或其他更新源）直接更新。
- **如果趋势科技服务器深度安全防护系统管理中心无法访问，则允许客户端/设备下载特征码更新：**通常，趋势科技服务器深度安全防护系统管理中心会指示客户端/设备：即使客户端无法与趋势科技服务器深度安全防护系统管理中心通信，客户端也将继续从其已配置的源接收更新。

规则

- **自动将规则更新应用到策略：**选择此选项后，新下载的安全规则更新将自动应用于趋势科技服务器深度安全防护系统策略。如果未选择此选项，则必须将下载的规则更新手动应用到策略，方法为从**管理** > **更新** > **安全**页面上单击**将规则应用到策略...**按钮。

> *注意：* *缺省情况下，策略更改将自动应用到计算机上。可通过打开**策略/计算机编辑器** > **设置** > **计算机**窗口，更改**立即发送策略更改**区域中的**自动将策略更改发送到计算机**设置，更改此功能。*

中继

- **支持 9.0（及较早版本）的客户端：**趋势科技服务器深度安全防护系统 9.5 安全更新软件包在格式上与趋势科技服务器深度安全防护系统 9.0 以及较早版本有所不同。如果未运行趋势科技服务器深度安全防护系统 9.0 客户端或设备，则应取消选中此选项从而避免下载不必要的内容。
- **为所有区域导入特征码：**如果未选中此选项，则中继仅为安装趋势科技服务器深度安全防护系统管理中心的区域（地区）下载和分发特征码。如果您在多租户模式下运行，并且您有任何租户在您自己的区域之外运行其趋势科技服务器深度安全防护系统安装，则您应保持选中此选项。
- **使用主租户中继组作为我的缺省中继组（对于未分配的中继）：**缺省情况下，主租户允许租户访问其中继，这表示租户不需要为安全更新设置其自己的中继。如果您不希望自己的租户环境使用这些共享中继，请取消选择此选项并为此租户设置专用中继。

注意： *如果您的主租户已经选择不共享缺省中继组，则单击**管理** > **更新** > **中继组**时，中继组名称将为“缺省中继组”而不是“主租户中继组”，并且您需要设置自己的专用中继。*

软件更新

趋势科技下载专区

- **自动将更新下载到导入的软件：**选择此选项可将更新自动下载到已导入趋势科技服务器深度安全防护系统的任何软件。此设置将把软件下载到趋势科技服务器深度安全防护系统，但不会自动更新您的客户端或设备软件。

注意： *更新计算机上的趋势科技服务器深度安全防护系统软件，必须手动选择**计算机**页面上的计算机，然后从**操作**菜单上选择**升级客户端软件...**，或者打开计算机的编辑器窗口，转至**概述** > **操作** > **软件**，然后单击**升级客户端软件...** .*

要替换趋势科技服务器深度安全防护系统中继的其他软件更新分发服务器：

趋势科技服务器深度安全防护系统中继通常用于托管客户端软件更新。但是，您可以选择使用自己的 Web 服务器来分发客户端软件包。要使用自己的 Web 服务器分发软件，请输入托管软件的目录的 URL。

注意： *即使使用自己的 Web 服务器分发软件，也必须使用**管理** > **更新** > **软件**窗口中的选项将客户端软件从趋势科技下载专区导入到趋势科技服务器深度安全防护系统管理中心。然后，必须确保您的软件 Web 服务器包含已导入到趋势科技服务器深度安全防护系统管理中心的同一软件，否则警报和通知可用更新的其他指示器将无法正常运行。有关配置自己的软件分发 Web 服务器的更多信息，请参阅**配置软件 Web 服务器**。*

虚拟设备版本控制

趋势科技服务器深度安全防护系统虚拟设备使用与 64 位 Red Hat 客户端相同的防护模块插件软件包。虚拟设备一旦激活，趋势科技服务器深度安全防护系统将检查已导入软件的清单，查找 Red Hat 客户端最新版，以查看是否有可用的更新。您可以使用此控件来管理用于更新任何新激活虚拟设备的 Red Hat 客户端软件的版本。

智能反馈

趋势科技智能反馈在趋势科技产品和公司的 24/7 威胁研究中心和技术之间提供持续的信息传送。通过使用智能反馈，产品成为实时共享和分析大量威胁数据的趋势科技云安全智能防护网络的活动组成部分。通过这种互连，可以前所未有的速率分析、识别和阻止新威胁 — 解决每日发布的数千个新威胁和威胁变种的响应能力级别。

注意： *智能反馈将使用在**管理 > 系统设置 > 代理服务器**选项卡中指定的**客户端、设备和中继（安全更新）**代理服务器。*

智能反馈是趋势科技云安全智能防护网络的组成部分。云安全智能防护网络使用威胁情报传感器的全球网络在云端持续更新电子邮件、Web 和文件信誉数据库，从而实时识别和阻止威胁。

趋势科技服务器深度安全防护系统可以直接访问云安全智能防护服务，也可以安装本地云安全智能防护服务器。云安全智能防护服务器旨在将操作本地化到公司网络以优化效率。可从趋势科技下载专区获取云安全智能防护服务器软件以及安装和配置说明，网址为：http://downloadcenter.trendmicro.com/?regs=CH。

注意： *您可以输入多个云安全智能防护服务器的地址。趋势科技建议安装多个本地服务器，以确保在出现硬件、软件或连接故障时有可用的服务器。*

SMTP

SMTP

键入 SMTP 邮件服务器的地址。（如果它与缺省 SMTP 端口 25 不同，则只需指定端口。）请输入要发送电子邮件的“发件人”电子邮件地址。可以选择输入“退信”地址，在无法向一个或多个用户发送警报电子邮件时，会将失败通知发送到该地址。如果 SMTP 邮件服务器需要传出验证，请输入用户名和密码凭证。如果 SMTP 服务器支持协议，请选择 STARTTLS。

输入必要的信息后，请使用**测试 SMTP 设置**来测试设置。

存储

数据清除

这些设置定义在从数据库中清除事件记录和计数器、较早的安全更新以及其他存储对象之前对其存储的时间。

对于事件设置，应该根据目前使用的数据库系统的稳健性、可用的存储空间量以及确定要记录的事件来决定。

下面是有关事件日志记录的一些提示：

- 对于不感兴趣的计算机，请修改日志收集的数量。可以在**策略/计算机编辑器** > **设置** > **网络引擎**选项卡的**事件**和**高级网络引擎设置**区域中完成此操作。
- 考虑禁用防火墙状态配置中的事件日志记录选项，从而减少防火墙规则活动的事件日志记录。（例如，禁用 UPD 日志记录便可排除未经请求的 UDP 日志条目）
- 对于入侵防御规则，最佳的做法是只记录丢弃的数据包。日志记录数据包修改可能会产生大量日志条目。
- 对于入侵防御规则，当您想要调查攻击来源时，只包含数据包数据即可（入侵防御规则**属性**窗口中的一个选项）。否则，保留数据包数据会大幅增加日志大小。

注意： ***计数器****是从事件日志聚合的数据，可用于生成报告和填充控制台 Widget。*

注意： ***服务器日志****是趋势科技服务器深度安全防护系统管理中心 Web 服务器活动的记录。这些日志不包含与网络中的计算机安全相关的信息。*

代理

代理服务器使用

- **客户端、设备和中继（安全更新）：**选择趋势科技服务器深度安全防护系统中继在连接到您在**更新**选项卡的**中继**区域中指定的**更新源**（**趋势科技更新服务器**或**其他更新源**）时要使用的代理服务器。

  注意： *缺省情况下，客户端/设备从趋势科技服务器深度安全防护系统中继获取其安全更新的防恶意软件组件。但是，如果客户端/设备无法连接到已分配的中继，并且已选择**如果趋势科技服务器深度安全防护系统中继不可用，则允许客户端/设备从此源下载安全更新**选项（参见上述内容），则客户端/设备还将使用此代理服务器。*

- **趋势科技服务器深度安全防护系统管理中心（软件更新、CSSS、使用授权通知、连接到云帐户）：**选择趋势科技服务器深度安全防护系统管理中心在连接到以下目标时要使用的代理服务器：连接到趋势科技以验证趋势科技服务器深度安全防护系统使用授权，连接到安全软件认证服务（完整性监模块中的一项功能）以及连接到 Amazon Web 服务 (AWS) 和 VMware vCloud 云帐户。

  注意： *只有在重新启动趋势科技服务器深度安全防护系统管理中心和所有管理中心节点之后，对用于 CSSS 的代理服务器设置所做的更改才会生效。（必须手动重新启动这些服务。）*

- **趋势科技服务器深度安全防护系统管理中心（云帐户）：**为趋势科技服务器深度安全防护系统管理中心选择一个代理服务器，以便在连接到基于云的实例（已按照“添加云帐户”过程添加至趋势科技服务器深度安全防护系统管理中心）时使用。

可以在**管理** > **系统设置**窗口的**代理服务器**选项卡上查看并编辑可用代理服务器列表。

代理服务器

定义可供各种趋势科技服务器深度安全防护系统客户端和服务使用的代理服务器（例如**策略/计算机编辑器** > **防恶意软件** > **云安全智能防护**中用于云安全智能防护的代理服务器）。

下表列出了趋势科技服务器深度安全防护系统服务和客户端支持的代理服务器协议：

服务	起源	HTTP 支持	SOCKS4 支持	SOCKS5 支持
软件更新	DSM	是	是	是
安全更新	DSA/DSVA/DSR	是	是	是
使用授权和产品注册	DSM	是	是	否
安全软件认证服务	DSM	是	否	否
智能反馈	DSA/DSR	是	是	是
Amazon AWS 云帐户	DSM	是	否	否
Vmware vCloud 云帐户	DSM	是	否	否
Microsoft Azure 云帐户	DSM	是	否	否

高级

主租户访问

缺省情况下，主租户可以访问您的趋势科技服务器深度安全防护系统环境。然而，主租户可以启用您环境中的“主租户访问”设置。这些设置允许您阻止主租户访问您的趋势科技服务器深度安全防护系统环境，或授予其时间有限的访问权限。

负载平衡器

如果部署趋势科技服务器深度安全防护系统管理中心和趋势科技服务器深度安全防护系统中继时未使用负载平衡器，客户端将获得管理中心和中继主机名的列表，并按随机循环顺序自动联系这些服务器。

您可以选择在管理中心或中继节点前端放置负载平衡器以调节自动缩放。通过在此输入负载平衡器设置，您无需更新客户端的地址即可执行此操作。您在此提供的主机名和端口将覆盖客户端当前使用的主机名和端口。

注意： *可以在正常端接的 SSL 负载平衡器后部署管理中心 Web 控制台和中继端口。客户端的波动信号端口（缺省情况下为 4120）必须是非端接负载平衡器，因为在波动信号通信中相互进行 SSL 认证。*

注意： *此处提供的负载平衡器设置也将覆盖由部署脚本生成器生成的地址。（该脚本生成器会写入用户连接到的管理中心的地址。）这确保了即使移除了某个管理中心节点，脚本也将继续正常运行。*

趋势科技服务器深度安全防护系统管理中心插件

“插件”是趋势科技服务器深度安全防护系统管理中心的模块、报告和其他附加软件。趋势科技有时会生成作为自行安装软件包分发的可插入项的新版本或其他版本。

SOAP Web 服务 API

趋势科技服务器深度安全防护系统管理中心的大多数功能可通过调用 SOAP 的 Web 服务来控制。在页面的面板所显示的 URL 中可以找到 WSDL（Web 服务描述语言）。如需有关趋势科技服务器深度安全防护系统管理中心 Web 服务 API 的帮助，请与支持提供商联系。

注意： *用户在趋势科技服务器深度安全防护系统管理中心中访问 Web 服务的权限将取决于授予该用户的适当权限。这些权限与已分配给该用户的角色相关联。此设置位于**角色属性**窗口（位于**管理 > 用户管理 > 角色**中）的**常规**选项卡中。*

状态监控 API

通过 REST 状态监控 API，您可以查询趋势科技服务器深度安全防护系统管理中心（包括单个管理中心节点）的状态信息，例如，CPU 和内存使用率、排队的作业数、总数据库大小和特定租户的数据库大小。如需有关趋势科技服务器深度安全防护系统管理中心 REST 状态监控 API 的帮助，请与支持提供商联系。

导出

导出文件字符编码：从趋势科技服务器深度安全防护系统管理中心导出数据文件时所用的编码。

已导出诊断数据包语言：支持提供商可能会要求您生成趋势科技服务器深度安全防护系统诊断数据包并发送给他们。此设置指定诊断数据包将使用的语言。诊断数据包在**管理 > 系统信息**页面中生成。

Whois

记录入侵防御和防火墙事件时要使用的 Whois 查找。在输入搜索 URL 时，将 "[IP]" 作为要查找的 IP 地址的占位符。（例如，"http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver"。）

使用授权

- **对新用户隐藏未授权的防护模块：**确定是否对后来创建的用户隐藏未授权的模块，而不是仅将其变成灰色。（在**管理 > 用户管理 > 用户 > 属性**窗口上可针对每个用户对此设置进行覆盖。）

扫描缓存配置

单击**查看扫描缓存配置...** 可显示已保存的扫描缓存配置列表。扫描缓存配置是虚拟设备用于最大限度地提高在虚拟环境中执行防恶意软件和完整性扫描的效率的设置。有关更多信息，请参阅**虚拟设备扫描缓存**。

漏洞扫描（推荐设置）过程中的 CPU 使用率

此设置控制用于执行建议扫描的 CPU 资源的数量。如果您发现 CPU 使用率达到不合理的高水平，请尝试更改为较低值或改正这种情况。有关其他性能控制的信息，请参阅**管理 > 管理中心节点 > 属性 > 性能配置文件**。

NSX

如果趋势科技服务器深度安全防护系统用于保护 VMware NSX 环境中的虚拟机，且它与多个趋势科技服务器深度安全防护系统管理中心节点一起安装，则此设置将确定与 NSX Manager 进行通信的趋势科技服务器深度安全防护系统管理中心节点。（有关趋势科技服务器深度安全防护系统与 NSX 环境集成的更多信息，请参阅**《用于 VMware NSX 的趋势科技服务器深度安全防护系统安装指南》**。有关多个趋势科技服务器深度安全防护系统管理中心节点的更多信息，请参阅**多节点管理中心**。）

徽标

您可以将趋势科技服务器深度安全防护系统管理中心右上角的趋势科技服务器深度安全防护系统徽标替换为您自己的徽标。（徽标也显示在登录页面和报告的顶部。）图形必须是一张宽 320 像素、高 35 像素且小于 1MB 的 PNG 图片。（趋势科技服务器深度安全防护系统管理中心的 "installfiles" 目录中提供了一个模板。）

单击**导入徽标...** 以导入您自己的图形，或**重置徽标...** 以将徽标重置为缺省徽标。

预设任务

使用**预设任务**页面可自动化和预设某些常见任务。

在主页面上可以执行下列操作：

- 创建**新的**预设任务 ()
- **删除**预设任务 ()
- 查看或修改现有预设任务的**属性** ()
- **复制**（然后修改）现有预设任务 ()
- **运行** () 选定的预设任务。

单击**新建** ()，然后选择“新建预设任务”。显示的向导将引导您完成创建新的预设任务的所有步骤。可能会提示您提供不同的信息，具体视任务类型而定。

预设任务

可以预设以下任务：

- **备份**：定期执行数据库备份。（仅当使用 Derby 或 Microsoft SQL Server 数据库时，该选项才可用。）
- **检查安全更新**：定期检查安全更新，并在有可用更新时将其导入趋势科技服务器深度安全防护系统。
- **检查软件更新**：定期检查趋势科技服务器深度安全防护系统软件更新，并在有可用更新时下载。
- **发现计算机**：通过预设发现操作定期在网络上检查新计算机。可能会提示您提供 IP 范围并要求您指定要添加新计算机的计算机组。
- **生成和发送报告**：自动生成报告并（可选）将这些报告通过电子邮件发送给列表中的用户。
- **运行脚本**：如果 Syslog 选项不符合您的事件通知要求，可由趋势科技使用自行撰写的脚本来提供解决方案。如需详细信息，请联系趋势科技。
- **扫描计算机上有无完整性更改**：使趋势科技服务器深度安全防护系统管理中心执行完整性扫描以将计算机的当前状态与其基线进行比较。
- **扫描计算机上有无恶意软件**：预设恶意软件扫描。扫描配置均与在**策略/计算机编辑器 > 防恶意软件**页面上为每台计算机指定的配置相同。
- **扫描计算机上有无打开的端口**：在一台或多台计算机上预设定期端口扫描。可以指定属于某个特定计算机组的单独计算机或所有计算机。要扫描的端口是已在**策略/计算机编辑器 > 设置**页面中的**扫描**选项卡上定义的端口。
- **扫描计算机上有无建议项目**：使趋势科技服务器深度安全防护系统管理中心扫描计算机中的常见应用程序，然后基于检测结果给出建议。
- **发送未决警报摘要**：生成列出所有未决（待解决）警报的电子邮件。
- **发送策略**：定期检查并发送更新策略。
- **同步目录**：将计算机列表与添加的 LDAP 目录同步。（仅在将 LDAP 目录添加到趋势科技服务器深度安全防护系统管理中心时才可用。）
- **同步用户/联系人**：将用户和联系人列表与已添加的 Active Directory 同步。（仅在已将 Active Directory 添加到趋势科技服务器深度安全防护系统管理中心时才可用。）
- **同步 VMware vCenter**：将**计算机**列表与添加的 VMware vCenter 同步。（仅在已将 VMware vCenter 添加到趋势科技服务器深度安全防护系统管理中心时才可用。）

注意： *对于基于客户端的防护，预设任务使用与端点操作系统相同的时区。对于无客户端防护，预设任务使用与趋势科技服务器深度安全防护系统虚拟设备相同的时区。*

启用或禁用预设任务

可以启用或禁用现有的预设任务。例如，如果您不希望在执行某些管理任务期间发生任何活动，则可能需要暂时禁用预设任务。用于启用或禁用预设任务的控件位于任务**属性**窗口的**常规**选项卡中。

基于事件的任务

您可以通过基于事件的任务针对特定事件监控受保护计算机，并基于一定的条件执行任务。

在主页面上可以执行下列操作：

- 创建**新的**基于事件的任务 ()
- 查看或修改现有的基于事件的任务的**属性** ()
- **复制**（然后修改）现有的基于事件的任务 ()
- **删除**基于事件的任务 ()

单击**新建** ()，然后选择**新建基于事件的任务**。显示的向导将引导您完成创建新任务的所有步骤。可能会提示您提供不同的信息，具体视任务类型而定。

事件

可以监控以下事件：

- **已创建计算机（由系统）：**在与 Active Directory 或云提供程序帐户同步期间添加到趋势科技服务器深度安全防护系统管理中心的计算机，或者在运行虚拟设备的受管理 ESXi Server 上创建的虚拟机。
- **已移动计算机（由系统）：** 从一个 vApp 移到同一 ESXi 中另一个 vApp 的虚拟机，或从一台 ESXi 上的一个数据中心移动到另一个数据中心，或从一台 ESXi 移动到另一台 ESXi （包括从未受管理的 ESXi Server 移动到运行虚拟设备的受管理 ESXi Server）的虚拟机。
- **客户端启动的激活：**使用客户端启动的激活激活客户端。
- **IP 地址已更改：**计算机已开始使用不同的 IP。
- **NSX 安全组已更改：**以下情况会触发此事件（事件将记录在每个受影响的 VM 上）：
  - 将 VM 添加到与 NSX 趋势科技服务器深度安全防护系统服务配置文件（间接）关联的组中
  - 从与 NSX 趋势科技服务器深度安全防护系统服务配置文件关联的 NSX 组中移除 VM
  - 将与 NSX 趋势科技服务器深度安全防护系统服务配置文件关联的 NSX 策略应用于 NSX 组
  - 从 NSX 组中移除与 NSX 趋势科技服务器深度安全防护系统服务配置文件关联的 NSX 策略
  - NSX 策略与 NSX 趋势科技服务器深度安全防护系统服务配置文件关联
  - 从 NSX 趋势科技服务器深度安全防护系统服务配置文件中移除 NSX 策略
  - 与 NSX 趋势科技服务器深度安全防护系统服务配置文件关联的 NSX 组更改了名称

条件

您可以要求满足特定的匹配条件以便执行任务。（按“加号”按钮可添加其他条件。）如果您指定多个条件，必须满足所有条件才能执行任务。（也就是说，多个条件是 "AND" 关系的条件，而不是 "OR" 关系的条件。）

使用 **Java 正则表达式语法** (http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html) 在以下文本框中匹配特征码：

- **云实例镜像 ID：**云实例镜像 ID。

> *注意：* ***云实例安全组名称****匹配条件只适用于 AWS 云实例。*

- **云实例元数据：**匹配的元数据对应于 Amazon 环境下的 AWS“标记”。

> *注意：* ***云实例元数据****匹配条件只适用于 AWS 云实例。目前，与某台计算机相关联的元数据显示在该计算机编辑器窗口的****概述****页面上。要定义匹配的条件，必须提供两条信息：元数据标记键和元数据标记值。例如，要匹配元数据键名为 "AlphaFunction" 以及值为 "DServer" 的计算机，需要输入 "AlphaFunction" and "DServer"（不包括引号）。如果想匹配多个可能的条件，可以使用正则表达式并输入 "AlphaFunction" and ".*Server"，或 "AlphaFunction" and "D.*"。*

- **云实例安全组名称：**云实例应用到的安全组。

> *注意：* ***云实例安全组名称****匹配条件只适用于 AWS 云实例。*

- **云帐户名称：**云帐户属性窗口中的“名称”字段。
- **计算机名称：**计算机属性窗口中的“主机名”字段。
- **ESXi 名称：**托管 VM 计算机的 ESXi Server 中的“主机名”字段。
- **文件夹名称：**计算机在其本地环境中所处的文件夹或目录的名称。
- **NSX 安全组名称：**此条件下的潜在组列表仅指的是与 NSX *趋势科技服务器深度安全防护系统*服务配置文件的关联 NSX 策略相关联的 NSX 组。VM 可能是其他 NSX 组的成员，但是对于此匹配条件它是不相关的。
- **平台：**计算机的操作系统。
- **vCenter 名称：**添加到趋势科技服务器深度安全防护系统管理中心的计算机的 vCenter 属性的“名称”字段。

Java 正则表达式示例：

要匹配：	**请使用：**
任意字符串（但不能为空）	.+
空字符串（无文本）	^$
文件夹 Alpha	Folder\ Alpha
FIN-1234	FIN-\d+ **或** FIN-.*
RD-ABCD	RD-\w+ **或** RD-.*
AB **或** ABC **或** ABCCCCCCCCC	ABC*
Microsoft Windows 2003 **或** Windows XP	.*Windows.*
Red Hat 6 **或** Some_Linux123 **或** abcFreeBSD	.*Red.*|.*Linux.*|.*FreeBSD.*

以下两个条件匹配 True 或 False 条件：

- **设备保护可用**：趋势科技服务器深度安全防护系统虚拟设备可以保护托管 VM 的 ESXi 上的 VM。VM 可能处于也可能不处于“已激活”状态。
- **设备保护已激活**：趋势科技服务器深度安全防护系统虚拟设备可以保护托管 VM 的 ESXi 上的 VM，且 VM“已激活”。

最后一个条件选项在 IP 列表中查找此 IP 的匹配项：

- **上次使用的 IP 地址**：计算机的当前 IP 地址或最后一次的已知 IP 地址。

注意： *某些文本框可能不可用，具体取决于新计算机的来源。例如，对于因与 Active Directory 同步而添加的计算机，“平台”将不可用。*

操作

可根据检测到的上述事件执行以下操作：

- **激活计算机**：在计算机上激活趋势科技服务器深度安全防护系统防护。
  - **延迟激活时间（分钟）**：按指定的分钟数延迟激活。

注意： *如果基于事件的任务要对某个 VM 应用防护，而该 VM 将 vMotion 到受趋势科技服务器深度安全防护系统虚拟设备保护的 ESXi，请在激活前增加两分钟的延迟，以便完成任何未决的 VMware 管理任务。*

注意： *仅当尚未激活计算机时，才执行激活操作。也就是说，仅当计算机未受客户端或虚拟设备保护或计算机仅受客户端保护但虚拟设备保护处于可用状态时，才执行激活操作。*

- **停用计算机**：在计算机上停用趋势科技服务器深度安全防护系统防护。
- **分配策略**：自动为新计算机分配策略。（必须首先激活该计算机。）
- **分配中继组**：为新计算机自动分配中继组，并从该中继组接收安全更新。
- **分配给计算机组**：将计算机置于“计算机”页面的其中一个计算机组。

执行顺序

如果同一条件触发了多个基于事件的任务，将按任务名称的字母顺序执行这些任务。

启用或禁用基于事件的任务

可以启用或禁用现有的基于事件的任务。例如，如果您不希望在执行某些管理任务期间发生任何活动，则可能需要暂时禁用基于事件的任务。用于启用或禁用基于事件的任务的控件位于任务**属性**窗口的**常规**选项卡中。

管理中心节点

管理中心节点页将显示所有活动管理中心节点的列表。双击列表中的管理中心节点以显示其**属性**窗口：

- **主机名：**趋势科技服务器深度安全防护系统管理中心主机计算机的主机名。
- **描述：**管理中心节点的描述。
- **性能配置文件：**趋势科技服务器深度安全防护系统管理中心的性能受多种因素影响，其中包括 CPU 数、可用带宽和数据库响应能力。管理中心的缺省性能设置旨在适用于大多数安装环境。但是，如果您遇到性能问题，您的支持提供商可能会建议您更改分配给一个或多个趋势科技服务器深度安全防护系统管理中心节点的性能配置文件。（在咨询您的支持提供商之前，请勿更改这些设置。）

  注意： *下表中提到的“终端磁盘和网络作业数”包括防恶意软件扫描、完整性监控扫描、侦察扫描、向计算机发送策略更新以及分发安全更新。）*

  - **主动型：**此性能配置文件针对 趋势科技服务器深度安全防护系统管理中心安装在一台专用服务器上的安装进行了优化。下表说明了如何为使用**主动型**性能配置文件的每个管理中心节点分配一些常用并发操作：

操作	双核系统	八核系统
激活	10	20
更新	25	50
漏洞扫描（推荐设置）	5	12
检查状态	100	相同 (100)
客户端/设备启动的波动信号	20 个处于活动状态 40 个处于排队等待状态	50 个处于活动状态 40 个处于排队等待状态
同时运行的终端磁盘和网络作业数	50	50
每个 ESXi 同时运行的终端磁盘和网络作业数	3	3

  - **标准型：**此性能配置文件针对趋势科技服务器深度安全防护系统管理中心与数据库共享同一主机的安装进行了优化。下表说明了如何为使用**标准型**性能配置文件的每个管理中心节点分配一些常用并发操作：

操作	双核系统	八核系统
激活	5	10
更新	16	46
漏洞扫描（推荐设置）	3	9
检查状态	65	100
客户端/设备启动的波动信号	20 个处于活动状态 40 个处于排队等待状态	50 个处于活动状态 40 个处于排队等待状态
同时运行的终端磁盘和网络作业数	50	50
每个 ESXi 同时运行的终端磁盘和网络作业数	3	3

  - **无限的客户端磁盘和网络用法：**此设置与**主动型**相同，但对计算机磁盘和网络用法操作无任何限制。

操作	双核系统	八核系统
激活	10	20
更新	25	25
漏洞扫描（推荐设置）	5	12
检查状态	100	相同 (100)
客户端/设备启动的波动信号	20 个处于活动状态 40 个处于排队等待状态	50 个处于活动状态 40 个处于排队等待状态
同时运行的终端磁盘和网络作业数	无限制	无限制
每个 ESXi 同时运行的终端磁盘和网络作业数	无限制	无限制

注意： 所有性能配置文件都将并发组件更新数限制为每个中继组 100 个。

- **状态：**表示从您登录到的趋势科技服务器深度安全防护系统管理中心节点来看，您要查看其属性的趋势科技服务器深度安全防护系统管理中心节点是否处于联机和活动状态。
- **选项：**您可以选择取消配置管理中心节点。此节点必须脱机（卸载或服务停止），才能取消其配置。

有关多节点趋势科技服务器深度安全防护系统管理中心安装的更多信息，请参阅**多节点管理中心**。

租户

租户页面显示安装趋势科技服务器深度安全防护系统时注册的租户的列表。在主页面上可以执行下列操作：

- 创建**新租户**()
- **删除**租户 ()
- 查看或修改现有租户的**属性** ()
- **以租户身份登录**，使您能够像租户一样使用趋势科技服务器深度安全防护系统管理中心。

  注意： *如果选择**管理** > **系统设置** > **租户** > **允许租户控制从主租户访问**选项，则租户可禁用您以租户身份登录的能力。*

- 在租户升级失败后，可使用**数据库升级**按钮来强制进行升级过程。
- 将一个或多个租户**导出** () 到 CSV 文件。（从下拉列表中选择**导出为 CSV...**将其全部导出，也可以选择**将选定内容导出为 CSV...**以仅导出选定的内容）
- **添加或删除列** () 通过单击**添加/删除列**可添加或删除列。通过将列拖曳到新的位置，可以控制列的显示顺序。可按照任意列的内容来排序和搜索所列出的项目。

单击**新建** () 或**属性** () 将显示租户**属性**窗口。

使用授权

显示有关趋势科技服务器深度安全防护系统产品使用授权的详细信息。趋势科技服务器深度安全防护系统包括五个模块包：防恶意软件和 Web 信誉；防火墙和入侵防御；完整性监控；日志审查和多租户。每个模块包都可完全授权，或者授权使用试用版。单击**查看详细信息**可查看各个包的使用授权状态。如果要升级使用授权，请与趋势科技联系。如果趋势科技为您提供了新的激活代码，请单击**输入新的激活代码...**，然后在此处输入该激活代码。新授权的功能将立即可用。

使用授权过期后，现有功能仍可用，但不再提供更新。

如果任意模块将要过期或已过期，将会生成警报。

AWS Marketplace 的使用授权

在 AWS Marketplace 中，有两个单独的趋势科技服务器深度安全防护系统管理中心 AMI，每个 AMI 提供不同的使用授权选项：“自带使用授权”或“按使用情况付费”。您使用的使用授权类型显示在趋势科技服务器深度安全防护系统管理中心控制台中的**管理** > **使用授权**下。

- **自带使用授权**（Bring-Your-Own-License，BYOL）适用于已从其他来源获取趋势科技服务器深度安全防护系统 9.5 使用授权的客户。此类型使用授权的工作方式与上述标准趋势科技服务器深度安全防护系统使用授权相同。
- **按使用情况付费**（Pay-Per-Use，PPU）允许客户基于要运行的 AWS 实例规模进行付费。使用 PPU 时，每种 EC2 实例类型都有一个关联的坐席数限制（坐席数是指可运行的趋势科技服务器深度安全防护系统客户端的数量）。可以随时更改实例的规模。也可运行多个实例以增加坐席数限制。在其他实例上安装趋势科技服务器深度安全防护系统管理中心时，请在“数据库”选项卡上选择“此趋势科技服务器深度安全防护系统安装将用作已部署的趋势科技服务器深度安全防护系统安装中的附加管理中心节点”。此选项指定每个节点将使用同一数据库。以下是趋势科技服务器深度安全防护系统管理中心所支持的每种 EC2 实例类型的坐席数限制：
  - M3 Large (m3.large)：最多 25 个客户端
  - M3 XL (m3.xlarge)：最多 50 个客户端
  - M3 2XL (m3.2xlarge)：最多 100 个客户端
  - C3 4XL (c3.4xlarge)：最多 200 个客户端

  启动或关闭趋势科技服务器深度安全防护系统管理中心节点时，将重新计算当前使用的坐席数并在**管理** > **使用授权**页面上显示剩余的坐席数限制。

注意： *AWS Marketplace 上的趋势科技服务器深度安全防护系统不支持使用 vCenter 和趋势科技服务器深度安全防护系统虚拟设备 (DSVA)。此外，PPU 使用授权不提供多租户支持。*

用户

“用户”是指所有 趋势科技服务器深度安全防护系统管理中心的帐户持有者。利用本节可创建、修改和删除用户帐户。在**用户**页面上，可执行下列操作：

- 创建**新**用户帐户 ()
- 查看或修改现有用户帐户的**属性** ()
- 设置（或更改）用户帐户的**密码** ()
- **删除**用户帐户 ()
- **搜索** () 特定用户
- 与用户的**目录**列表**同步** ()
- 查看与此用户相关的**系统事件** ()
- 设置或更改此用户的**角色** ()

单击**新建** () 或**属性** () 将显示**用户属性**窗口。

常规

常规信息

- **用户名：**与此用户的密码相关的用户名。
- **名称：**帐户持有者的名称。
- **描述：**帐户持有者的描述。
- **角色：**使用下拉列表将预定义的角色分配给此用户。（还可以在“列表视图”模式下利用右键单击菜单来分配角色。）

注意： *趋势科技服务器深度安全防护系统管理中心随附了两个预先配置的角色：完全访问权限和审计员。“完全访问权限”角色授予用户在管理趋势科技服务器深度安全防护系统方面的所有可能的权限，例如创建、编辑和删除计算机、计算机组、策略、规则等。“审计员”角色使用户能够**查看**趋势科技服务器深度安全防护系统中的所有信息，但不能修改除其个人设置（密码、联系信息、视图首选项等）以外的任何设置。您可以在**角色**页面中或通过选择**角色**下拉列表中的“新建...”来创建和修改具有各种系统访问权限级别的角色。*

- **语言：**此用户登录时要在界面中使用的语言。
- **已锁定：**选中此选项可阻止此用户登录到管理中心。（如果用户在尝试登录时多次输入了错误密码，此用户将被自动锁定。如果已解决此问题，请清除此选项。）（还可以在“列表视图”模式下通过右键单击菜单锁定或解除锁定用户。）

选项

单击**设置密码**按钮可以更改此用户的密码或为其分配密码。可以在以下位置设置密码要求（如最小长度、大小写等）：**管理 > 系统设置 > 安全。**

联系信息

此用户的联系信息。选中**接收通知**复选框可将此用户包含在触发警报时接收电子邮件通知的用户的列表中。

设置

模块

- **隐藏未授权的模块：**确定是否对此用户隐藏未授权的模块，而不是仅将其变成灰色。（可在**管理** > **系统设置** > **高级**选项卡中全局设置此选项）

刷新速率

- **状态栏：**此设置确定在执行各种操作（例如，发现或扫描计算机）期间管理中心的状态栏刷新的频率。
- **警报列表/摘要：**在列表视图或摘要视图中刷新**警报**页面中数据的频率。
- **菜单/计算机列表：**刷新**计算机**页面中数据的频率。

> *注意：* *除非手动重新加载此页面，否则不会重新计算**上次成功更新**列的值。*

- **“计算机详细信息”窗口：**单台计算机的属性页面将自身刷新为包含最新信息的频率（如果需要）。

列表视图

- **记住每个页面的上一个标记过滤器：**通过“事件”页面可以按标记过滤显示的事件。此列表视图设置确定在离开并返回“事件”页面时是否保留“标记”过滤器设置。
- **记住每个页面的上一个时间过滤器：**通过“事件”页面可以按时间段和计算机过滤显示的事件。这些列表视图设置确定在离开并返回某个“事件”页面时是否保留“时间段”和“计算机”过滤器设置。
- **记住每个页面的上一个计算机过滤器：**通过“事件”页面可以按时间段和计算机过滤显示的事件。这些列表视图设置确定在离开并返回某个“事件”页面时是否保留“时间段”和“计算机”过滤器设置。
- **记住每个页面的上一次高级搜索：**如果已在“事件”页面上执行了“高级搜索”，此设置将确定在离开并返回该页面时是否保留搜索结果。
- **单页上显示的最佳项目数：**显示项目列表的窗口将在每个“页面”上显示特定数量的项目。要查看下一页，必须使用分页控件。使用此设置可更改每页显示的列表项数。
- **单页上显示的最大项目数：**趋势科技服务器深度安全防护系统管理中心的许多列表按类别进行分组。例如，入侵防御规则可根据应用程序类型分组。趋势科技服务器深度安全防护系统管理中心在分页时会尽量避免拆分这些组，并可以覆盖上述“最优”设置，以便将同一组中的项目保留在一起。使用此设置可设置每页显示的固定最大项目数。如果组中的项目数超过此数值，该组将被拆分开且该组的标题将显示该组已拆分的信息。
- **从数据库中检索的最大项目数：**此设置限制可从数据库中检索以显示的项目的数量。这可以防止趋势科技服务器深度安全防护系统管理中心在尝试显示数据库查询返回的过量结果时停止运行。如果某个查询生成的结果数大于此数值，则在该窗口的顶部将显示一则消息，以通知您将仅显示部分结果。

> *注意：* *增大这些值将影响趋势科技服务器深度安全防护系统管理中心的性能。*

报告

- **启用 PDF 加密：**确定以 PDF 格式导出的报告是否受密码保护。

重置为缺省设置：将此页面上的所有设置重置为其缺省值。

与目录同步

用户列表可与 Active Directory 同步，这允许用户使用此目录中存储的密码登录。单击工具栏中的**与目录同步**将显示**与目录同步**向导。键入目录服务器的名称以及您的访问凭证。随后将提示您选择要导入的 Active Directory 用户组以及是将其视为“用户”还是“联系人”。将其导入后，您可以选择创建预设任务以定期与目录进行同步，以使您的列表保持最新。缺省情况下，导入的用户列表被锁定在趋势科技服务器深度安全防护系统管理中心之外。必须修改其属性才能允许他们登录到管理中心。

注意： *要成功将 Active Directory 用户帐户导入到趋势科技服务器深度安全防护系统作为趋势科技服务器深度安全防护系统用户或联系人，Active Directory 用户帐户必须具有一个 userPrincipalName 属性值。（userPrincipalName 属性对应于 Active Directory 帐户持有者的“用户登录名”。）*

注意： *如果从趋势科技服务器深度安全防护系统管理中心删除了因与 Active Directory 同步而添加的用户，然后又重新与该目录同步，则该用户又将出现在用户列表中（如果该用户仍位于 Active Directory 中）。*

过滤 Active Directory

与目录同步向导的第一个页面包含一个名为**搜索选项**的区域，可以在该区域中编写过滤器来指定将一部分用户导入趋势科技服务器深度安全防护系统管理中心。过滤器语言遵循 Internet 工程任务组的“轻量型目录访问协议 (LDAP)：搜索过滤器的字符串表示 RFC 4515”。

缺省过滤器 "(objectClass=group)" 会导入所有用户。

可以使用 RFC 4515 过滤器语法来过滤目录中的特定用户和/或组。例如，以下过滤器将仅导入 Active Directory 组 "DeepSecurityUsers" 的成员用户："(&(objectClass=group)(cn=DeepSecurityUsers))"。

可在 http://datatracker.ietf.org/doc/rfc4515/ 找到 RFC 4515 的定义。

注意： *尽管新用户处于“已锁定”状态，但已授予其“完全访问权限”用户角色。*

角色

趋势科技服务器深度安全防护系统使用基于角色的访问控制来限制用户对趋势科技服务器深度安全防护系统各个部分的访问。安装趋势科技服务器深度安全防护系统管理中心后，应为每个用户创建单独的帐户并为每个用户分配一个角色，该角色将限制除那些完成其职责所必需的活动外的所有活动。

趋势科技服务器深度安全防护系统随附了两个预先配置的角色：

- **完全访问权限：**“完全访问权限”角色可以授予用户有关管理趋势科技服务器深度安全防护系统的所有可能的权限，包括创建、编辑和删除计算机、计算机组、策略、规则、恶意软件扫描配置以及其他项。
- **审计员：**“审计员”角色可以为用户提供在趋势科技服务器深度安全防护系统中查看所有信息的功能，但不能修改除其个人设置（例如密码、联系信息、控制台布局首选项以及其他设置）之外的所有设置。

注意： *管理中心界面中的控件的状态可以为“可见且可更改”、“仅可见但已禁用”或“已隐藏”，具体取决于授予的访问权限级别。有关预先配置的角色中授予的权限列表以及创建新角色时的缺省权限设置，请参阅***用户管理**。

您可以创建新角色来限制用户编辑甚至查看趋势科技服务器深度安全防护系统的对象（例如，特定计算机、安全规则的属性或系统设置）。

创建用户帐户之前，请确定用户将拥有的角色，并详细列举这些角色需要访问的趋势科技服务器深度安全防护系统对象以及访问权限的性质（查看、编辑、创建等）。创建角色后，则可以开始创建用户帐户并为其分配特定角色。

注意： *请勿通过复制然后修改**完全访问权限**角色来创建新角色。要确保新角色仅授予所需的权限，请通过单击工具栏中的**新建**来创建新角色。缺省情况下，新角色的权限设置具有最强的限制性。然后，可继续仅授予所需的权限。如果复制**完全访问权限**角色，然后应用限制，则会存在授予一些不需要的权限的风险。*

在主页面上可以执行下列操作：

- 创建**新**角色 ()
- 查看或修改现有角色的**属性** ()
- **复制**（然后修改）现有角色 ()
- **删除**角色 ()

单击**新建** () 或**属性** () 将显示**角色属性窗口**，该窗口包括六个选项卡（**常规**、**计算机权限**、**策略权限**、**用户权限**、**其他权限**和**已分配给**）。

常规

常规信息

此角色的名称和描述。

访问类型

选择具有此角色的用户是有权访问趋势科技服务器深度安全防护系统管理中心的基于 Web 的用户界面权限，或者有权访问趋势科技服务器深度安全防护系统管理中心的 Web 服务 API，还是同时具有这两种访问权限。

注意： *要启用 Web 服务 API，请转至**管理** > **系统设置** > **高级** > **SOAP Web 服务 API**。*

计算机权限

计算机和组权限

使用**计算机和组权限**面板可以将查看、编辑、删除、解除警报和事件标记的权限授予具有某角色的用户。这些权限可应用到所有计算机和计算机组中，也可以将其仅限制到某些计算机。如果希望限制访问权限，请选择**选定的计算机**单选按钮并选中具有此角色的用户有权访问的计算机组和计算机旁边的框。

注意： *这些权限限制不仅影响用户对趋势科技服务器深度安全防护系统管理中心内的计算机的访问权限，还会影响可见的信息（包括事件和警报）。此外，只有电子邮件通知与用户有权访问的数据相关时，才会发送电子邮件通知。*

提供以下四个基本选项可供选择：

- **允许查看未选定的计算机和数据：**如果限制了具有此角色的用户的编辑/删除/解除警报权限，您仍可以通过选中此框来允许他们查看（但不能更改）有关其他计算机的信息。
- **允许查看与计算机无关的事件和警报：**设置此选项可允许具有此角色的用户查看与计算机无关的信息（例如，系统事件，如当前已锁定的用户、创建的新防火墙规则、删除的 IP 列表等）。

  注意： *前两种设置影响用户可以访问的数据。虽然已限制用户更改计算机，但这两种设置控制用户是否可以查看与其不可以访问的计算机相关的信息。这包括接收与这些计算机相关的电子邮件通知。*

- **允许在选定组中创建新的计算机：**设置此选项可允许具有此角色的用户在其有权访问的计算机组中创建新的计算机。
- **允许在选定组中添加/移除子组：**设置此选项可允许具有此角色的用户在其有权访问的计算机组中创建和删除子组。

高级权限

- **允许导入计算机文件：**允许具有此角色的用户使用通过趋势科技服务器深度安全防护系统管理中心的**导出计算机**选项创建的文件来导入计算机。
- **允许添加、移除和同步目录：**允许具有此角色的用户添加/移除和同步使用基于 LDAP 的目录（如 MS Active Directory）管理的计算机。
- **允许添加、移除和同步 VMware vCenter：**允许具有此角色的用户添加、移除和同步 VMware vCenter。
- **允许添加、移除和同步云提供程序：**允许具有此角色的用户添加、移除和同步云提供程序。

策略权限

确定具有特定角色的用户拥有的创建、删除、修改或导入策略的权限。

策略权限

使用**策略权限**面板可以将查看、编辑和删除的权限授予具有某角色的用户。这些权限可应用到所有策略，或者这些权限仅限于某些策略。如果希望限制访问权限，请选择**选定的策略**单选按钮，然后选中具有此角色的用户有权访问的策略旁边的框。

> *注意：* *向具有子策略的策略授予权限后，用户也会自动获得子策略的权限。*

提供以下两个基本选项可供选择：

- **允许查看未选定的策略：**如果限制了具有此角色的用户的编辑/删除权限，您仍可以通过选中此框来允许他们查看（但不能更改）有关其他策略的信息。
- **允许创建新策略：**设置此选项可允许具有此角色的用户创建新的策略。

高级权限

- **允许策略导入：**允许具有此角色的用户使用通过趋势科技服务器深度安全防护系统管理中心的**策略**选项卡上的**导出**选项创建的文件来导入策略。

用户权限

用户权限

利用**用户权限**选项卡上的选项可设置具有此角色的用户对其他用户所拥有的权限类型。

- **仅更改自身密码和联系信息：**具有此角色的用户仅能更改自身密码和联系信息。
- **创建和管理具有同等或较低访问权限的用户：**具有此角色的用户可创建和管理具有同等或较低访问权限的所有用户。即使仅有一项权限超出具有此角色的用户的权限，具有此角色的用户也无法创建或管理它们。
- **完全控制所有角色和用户：**具有此角色的用户可以无限制地创建和编辑用户或角色。

> *注意：* *请谨慎使用这最后一个选项。如果将此选项分配给一个角色，则可能为具有受限权限的用户提供以下能力：创建对趋势科技服务器深度安全防护系统管理中心所有方面都具有非限制访问权限的用户，然后以该用户身份登录。*

定制权限

您可以选择**定制**然后使用**定制权限**面板中的选项，进一步限制用户查看/创建/编辑/删除用户和角色的能力。如果选择了**仅可操控具有同等或较低权限的用户**选项，一些用户的某些选项可能受限制（请参阅下面内容）。

委派授权

选择**仅可操控具有同等或较低权限的用户**选项，将限制具有此角色的用户的授权。他们仅能实现与其具有同等或较低权限的用户的更改。

选择此选项后，具有此角色的用户将不能创建、编辑或删除角色。

选择此选项还会对**定制权限**区域中的某些选项进行限制：

- **可以创建新用户**：仅能创建具有同等或较低权限的用户。
- **可以编辑用户属性**：仅能编辑具有同等或较低权限的用户（或设置/重置密码）。
- **可以删除用户**：仅能删除具有同等或较低权限的用户。

其他权限

可以针对角色可控制的趋势科技服务器深度安全防护系统对象来对角色进行限制。对于每个元素，新角色的缺省设置为“仅查看”或“隐藏”，但这些权限可扩展到“完全控制”，或通过从下拉列表中选择“定制”对其进行定制。

已分配给

已分配给选项卡显示已分配有此角色的用户列表。

联系人

用户可以创建“联系人”。联系人不能登录到趋势科技服务器深度安全防护系统管理中心，但可以定期向他们发送报告（使用预设任务）。可以为联系人分配映射到现有角色的“清除”级别。当向联系人发送某报告时，该报告将不包含同级别用户无法访问的任何信息。

在**联系人**页面上，可执行下列操作：

- 创建**新**联系人 ()
- 查看或修改现有联系人的**属性** ()
- **删除**联系人 ()
- 与**目录**列表**同步** ()

单击**新建** () 或**属性** () 会显示**联系人属性**窗口。

常规信息

此联系人的名称、描述和首选语言。

联系信息

如果此联系人包含在报告分发列表中，则此处输入的电子邮件地址为要将报告发送到的电子邮件地址。（有关更多信息，请参阅**报告**页面。）

清除

此处指定的角色将确定允许此联系人查看的信息。例如，如果已预设将计算机报告发送给此联系人，则此报告将仅包括此联系人的角色所允许他访问的计算机相关信息。

报告

选择是否为此用户加密报告。

与目录同步

联系人列表可与 Active Directory 同步。单击工具栏中的**与目录同步**将显示**与目录同步**向导。键入目录服务器的名称以及您的访问凭证。随后将提示您选择要导入的用户组以及是将其视为“用户”还是“联系人”。将其导入后，您可以选择创建预设任务以定期 与目录进行同步，以使您的列表保持最新。

注意： *要成功将 Active Directory 用户帐户导入到趋势科技服务器深度安全防护系统作为趋势科技服务器深度安全防护系统用户或联系人，Active Directory 用户帐户必须具有一个 userPrincipalName 属性值。（userPrincipalName 属性对应于 Active Directory 帐户持有者的“用户登录名”。）*

系统信息

创建诊断数据包...

单击工具栏中的**创建诊断数据包...**将显示**诊断数据包**向导，该向导将创建一个 zip 文件，其中包含安装/卸载和调试日志、系统信息、数据库内容（最后一小时，仅适用于时间敏感的项目）、文件列表以及属性文件（已移除密码）。可以将此信息提供给您的支持提供商以帮助解决任何问题。

注意： *诊断数据包的缺省最大大小约为 200MB。可使用以下命令行指令来增加诊断数据包的大小：*

```
dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value ####
```

以下示例将数据包的大小增加到 1GB (1000MB)：

```
dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value 1000
```

不要更改诊断数据包的大小，除非您的支持提供商指示您这样做。

扩展...

扩展可以是趋势科技服务器深度安全防护系统管理中心的报告或插件。

演示模式...

如果要在测试环境中评估趋势科技服务器深度安全防护系统，并希望查看完整的趋势科技服务器深度安全防护系统安装在企业环境中的外观，可通过单击**系统信息**页面工具栏上的**演示模式...**启用演示模式。

处于演示模式时，管理中心使用模拟计算机、事件、警报和其他数据填充其数据库。最初生成七天的数据，但会不断生成新数据以使用这些数据填充管理中心的“控制台”、“报告”和“事件”页面。

注意： *虽然演示模式可以用于混合真实计算机和模拟计算机的情况，但是不打算将其用于生产环境中！*

演示模式也可以同一方式关闭。

系统活动 (最近 1 小时内)

此面板显示不同管理中心节点执行的各种图形化详细活动。有关**系统活动**面板中显示的详细信息，请参阅**多节点管理中心**。

系统详细信息

此面板显示您的支持提供商用于进行故障排除的系统详细信息。

更新

趋势科技服务器深度安全防护系统管理中心的“更新”部分包括以下部分：

- 可通过*安全（第 190页）*部分管理您的安全更新。
- 可通过*软件（第 195页）*部分管理您的软件更新。
- 可通过*中继组（第 199页）*部分创建和修改 趋势科技服务器深度安全防护系统中继组。

安全更新

安全更新概述页面显示安全更新（从趋势科技更新服务器到趋势科技服务器深度安全防护系统分发网络，再到受保护计算机）的状态。

特征码更新由防恶意软件和 Web 信誉防护模块使用。

规则更新由下列模块使用：

- 防火墙
- 入侵防御
- 完整性监控
- 日志审查安全

特征码更新

趋势科技更新服务器

表示趋势科技服务器深度安全防护系统中继能否连接到趋势科技更新服务器检查最新的特征码和规则更新。

趋势科技服务器深度安全防护系统

- **上次检查更新的时间：**上次成功执行特征码更新检查的时间。
- **检查更新并下载...：**检查可用的特征码更新。如果有新更新可用，将自动进行下载。
- **上次下载时间：**上次成功检查特征码更新后下载新更新的时间。
- **所有中继均已同步：**指示是否所有中继均在分发最新成功下载的特征码更新。未同步的中继通常处于该状态，因为它们无法与趋势更新服务器进行通信。这可能是因为这些中继有意留“间隙”，因此需要手动更新；也有可能是因为网络连接有问题。 如果有任何中继不同步，此处将提供指向这些中继的链接。
- **下次预设检查的时间：**下次运行检查特征码更新的预设任务的时间。

计算机

- **所有计算机已是最新/计算机已过期：**表示*针对中继中存储的特征码更新*，是否有任何计算机已过期。
- **将特征码发送到计算机：**指示所有计算机从其分配的中继检索最新的特征码更新。

注意：	*在特征码更新已经从趋势科技下载并可使用一小时以上但电脑仍未更新时，会引发警报。*

规则更新

趋势科技更新服务器

表示趋势科技服务器深度安全防护系统中继能否连接到趋势科技更新服务器检查最新的规则更新。

趋势科技服务器深度安全防护系统

- **上次检查更新的时间：**上次成功执行规则更新检查的时间。
- **检查更新并下载...：**检查可用的规则更新。如果有新更新可用，将自动进行下载。
- **上次下载时间：**上次成功检查规则更新后下载新更新的时间。
- **将规则应用到策略...：**将最新下载的规则更新应用到安全策略。（如果已在**管理** > **系统设置** > **更新**选项卡中选择**自动将新规则更新应用到策略**选项，则将自动执行此操作。）
- **策略正在使用规则更新 xx-yyy：**安全策略当前正在应用的规则集。如果使用的不是最新下载的更新，将显示警告。
- **下次预设检查的时间：**下次运行检查规则更新的预设任务的时间。

计算机

- **所有计算机已是最新/计算机已过期：***表示针对已应用于趋势科技服务器深度安全防护系统管理中心中所存储策略的规则更新*，是否有任何计算机已过期。
- **将策略发送到计算机：**单击将具有已更新规则集的策略发送到任何没有该策略的计算机。

注意： *在规则更新已经从趋势科技下载并可使用三十分钟以上但电脑仍未更新时，会引发警报。*

规则

显示已下载到趋势科技服务器深度安全防护系统管理中心数据库的最新的入侵防御、完整性监控和日志审查规则的列表。如果需要，您可以将当前的规则集重新应用到趋势科技服务器深度安全防护系统保护的计算机，也可以还原到以前的规则集。可以转至**管理** > **系统设置** > **存储**选项卡，来配置趋势科技服务器深度安全防护系统管理中心的数据库中保留的规则更新数。

在**规则更新**页面上，可执行下列操作：

- **导入**（）规则更新
- **删除**（）规则更新
- **查看**规则更新的属性（）
- **还原**（）到之前的规则更新
- **导出**（）规则更新

导入

规则更新将在“检查安全更新”预设任务期间，或在您单击**管理** > **更新** > **安全**页面上的**检查更新并下载**时自动导入到趋势科技服务器深度安全防护系统中。只有在安装未连接到趋势科技更新服务器或您的支持提供商要求您手动更新规则时，您才需要手动导入规则更新。

查看属性

规则更新的**属性**窗口将显示：

常规信息

- **名称：**规则更新文件的名称
- **版本：**规则更新的版本号
- **发布日期：**趋势科技发布规则更新的日期
- **导入日期：**将规则更新导入趋势科技服务器深度安全防护系统的日期
- **应用日期：**规则更新应用到策略的日期

内容

详细列举规则更新中包括的新对象。

还原

如果最近的规则更新导致您的环境中出现问题，您可能希望还原到以前的规则更新。如果还原到以前的更新，受还原影响的所有策略将立即在*使用这些策略的所有计算机*上进行更新。

导出

在正常情况下，除非您的支持提供商要求您导出规则更新，否则不应执行此操作。

特征码

特征码页面显示构成特征码更新的组件的列表。此页面仅当趋势科技服务器深度安全防护系统有活动中继时才出现。

表示趋势科技服务器深度安全防护系统中继能否连接到趋势科技更新服务器检查最新的特征码和规则更新。

- **组件**：更新组件的类型。
- **产品名称**：此组件针对的趋势科技服务器深度安全防护系统产品。
- **平台**：将进行更新的操作系统。
- **当前版本**：当前从趋势科技下载到趋势科技服务器深度安全防护系统，并由中继和趋势科技服务器深度安全防护系统管理中心进行分发的更新内组件的版本。
- **最近更新时间**：从趋势科技检索当前已下载的安全更新的时间。

可在**计算机编辑器** > **更新**页面上找到特定计算机上已生效的安全更新组件的版本号。

软件更新概述

软件更新概述页面显示从 趋势科技更新服务器到 趋势科技服务器深度安全防护系统分发网络再到受保护计算机的软件更新状态。

趋势科技下载专区

概述页面的此区域显示是否有任何针对已导入趋势科技服务器深度安全防护系统的软件的可用更新。

注意： *趋势科技服务器深度安全防护系统仅会通知您针对所导入软件的次要版本的更新。例如，如果您使用的客户端版本为 9.5.100，而趋势科技发布了客户端版本 9.5.200，趋势科技服务器深度安全防护系统会通知您有可用的软件更新。但是，如果趋势科技随后又发布了客户端版本 9.6.xxx，而您的数据库清单中没有早期的 9.6 版本系列客户端，则不会收到可用更新的通知（即使您已安装了 9.5.100 客户端）。*

趋势科技服务器深度安全防护系统

概述页面的此区域显示上次执行软件更新检查的时间以及检查是否成功。**检查更新**按钮执行按需检查。将显示下一次软件更新预设任务的日期。如果不存在预设任务，将显示警告消息。

计算机

显示是否有任何计算机正在运行有可用更新的客户端。此检查仅针对已下载到趋势科技服务器深度安全防护系统的软件，不针对下载专区中提供下载的软件。如果有任何计算机过期，可单击**升级客户端/设备软件**按钮，会打开经过过滤的、显示过期计算机的**计算机**页面。

注意： *仅当趋势科技服务器深度安全防护系统数据库清单中有针对客户端次要版本的可用更新时，趋势科技服务器深度安全防护系统才会将计算机视为过期。例如，如果计算机运行的客户端版本为 9.5.100，然后您从趋势科技下载专区导入客户端版本 9.5.200，趋势科技服务器深度安全防护系统会通知您计算机已过期。但是，如果计算机运行的客户端版本为 9.5.200，然后导入客户端版本 9.6.xxx，趋势科技服务器深度安全防护系统不会将计算机视为过期，而会显示绿色勾选标记，指示计算机已处于最新状态。*

升级客户端/设备软件

计算机上的客户端软件必须手动升级。要升级所有客户端，请单击**升级客户端软件...**。要在单个计算机上升级客户端软件，请转到**计算机**页面，然后从上下文菜单中选择**操作 > 升级客户端**。

下载专区

显示趋势科技下载专区可供下载的最新软件的列表。软件包将包含新版本的管理中心、客户端、虚拟设备和过滤器驱动程序。

注意： *此页面仅列出最新的趋势科技服务器深度安全防护系统软件。如需较早版本，请直接访问下载专区网站：http://downloadcenter.trendmicro.com/?regs=CH（第 1页）*

- **名称：**软件包的文件名
- **发行说明：**软件包发行说明的链接
- **平台：**软件包的平台
- **导入日期：**如果已将软件下载到趋势科技服务器深度安全防护系统数据库，将显示勾选标记。
- **版本：**软件版本号
- **发布日期：**趋势科技发布软件的日期
- **直接导入可用：**如果软件包可从下载专区直接导入趋势科技服务器深度安全防护系统管理中心，会显示一个图标（  ）。不能直接导入的软件包必须从趋势科技下载专区网站下载到本地文件夹中，然后在**管理** > **更新** > **软件** > **本地**页面手动导入。

导入

使用此导入功能可手动从趋势科技下载专区导入软件。

本地软件

本地软件页面列出已导入到趋势科技服务器深度安全防护系统的软件。

必须将软件从趋势科技下载专区导入到趋势科技服务器深度安全防护系统数据库，才可供网络中的计算机使用。如果引发警报，指示计算机上的软件已过期，这是因为趋势科技服务器深度安全防护系统中有更新的本地可用的客户端或设备软件版本。也就是说，系统是对本地清单进行检查，而非对下载专区中可用的内容进行检查。（这是针对下载专区中的新软件单独引发的警报。）

要在计算机上安装趋势科技服务器深度安全防护系统客户端或设备，必须先将软件从下载专区导入到趋势科技服务器深度安全防护系统，然后提取安装包。

在**本地软件**页面上，可执行下列操作：

- **导入**（）软件更新
- **删除**（）软件更新
- **查看**软件更新的属性（）
- **导出**（）软件包或安装程序
- **生成部署脚本**（）以在计算机上安全客户端

导入

在正常情况下，从下载专区自动导入软件，或从 **管理** > **更新** > **软件** > **下载专区**页面手动导入。使用此导入功能可手动从除趋势科技下载专区以外的位置导入软件。

删除

从趋势科技服务器深度安全防护系统数据库中删除软件包。

趋势科技服务器深度安全防护系统数据库必须包含受管计算机上当前安装的所有软件的副本。首次激活趋势科技服务器深度安全防护系统客户端时，计算机上只安装了正在应用的安全策略中“打开”的防护模块。如果以后打开防护模块，趋势科技服务器深度安全防护系统将从数据库的客户端软件包中检索新安全模块的插件以安装在计算机上。如果缺少该软件，则无法安装安全模块插件。

为了节省空间，趋势科技服务器深度安全防护系统将定期从趋势科技服务器深度安全防护系统数据库移除未使用的软件包。可以被删除的软件包有以下两种类型：客户端软件包和内核支持包。

注意： *趋势科技服务器深度安全防护系统虚拟设备依赖于 64 位 Red Hat 客户端软件包中的“防护模块”插件。如果您已激活虚拟设备并试图删除 64 位 Red Hat 客户端，将返回一条错误消息，通知您软件正在使用中。*

在单租户模式下删除客户端软件包

在单租户模式下，趋势科技服务器深度安全防护系统会自动删除客户端当前未使用的客户端软件包（客户端-*平台-版本*.zip）。数据库中保留的旧软件包数在**系统设置** > **存储**选项卡中配置。也可以手动删除不使用的客户端软件包。如果尝试删除受管计算机之一正在使用的软件，则将收到警告，并且无法删除该软件。

注意： *对于 Windows 和 Linux 客户端软件包，只有正在使用的软件包（其版本与客户端安装程序相同）不能被删除。*

在多租户模式下删除客户端软件包

在多租户模式下，不会自动删除未使用的客户端软件包（客户端-*平台*-*版本*.zip）。出于隐私考虑，趋势科技服务器深度安全防护系统不能确定当前是否有租户正在使用软件，即使您和您的租户共享趋势科技服务器深度安全防护系统数据库中的同一软件存储库。作为主租户，趋势科技服务器深度安全防护系统不会阻止您删除您自己帐户的计算机当前未运行的软件，但在删除软件包之前，请务必确保没有其他租户正在使用该软件。

注意： *对于 Linux 内核支持包，只有最新版不能删除。*

删除内核支持包

在单租户和多租户两种模式下，趋势科技服务器深度安全防护系统都会自动删除未使用的内核支持包（内核支持-*平台*-*版本*.zip）。数据库中保留的旧软件包数在**系统设置** > **存储**选项卡中配置。满足以下两个条件才可以删除内核支持包：

- 无具有同一组标识符的客户端软件包。
- 存在具有同一组标识符和更高 Build 号的其他内核支持包。

也可以手动删除未使用的内核支持包。

查看属性

将显示软件更新的**属性**窗口：

常规信息

- **名称**：软件更新文件的名称
- **平台**：针对其构建软件的操作系统
- **版本**：软件更新的版本号
- **指纹**：文件的数字指纹。
- **导入日期**：规则更新导入到趋势科技服务器深度安全防护系统的日期
- **说明**：要附加到文件中的其他说明

导出

导出软件包：此选项将导出整个软件包。使用此选项导出软件，与可选的更新 Web 服务器一起使用。（更新 Web 服务器是处于您控制之下的 Web 服务器，可用作软件分发点，而非中继。可在**管理** > **系统设置** > **更新**选项卡上配置更新 Web 服务器。有关更新 Web 服务器的更多信息，请参阅《用户指南》中的**软件更新**。）

导出安装程序：此选项从客户端软件包中提取核心客户端安装程序。核心客户端安装程序用于在计算机上安装核心客户端软件。这是轻量型软件包，不包含任何防护模块所需的任何插件。激活客户端并打开防护模块时，趋势科技服务器深度安全防护系统管理中心从趋势科技服务器深度安全防护系统数据库的软件包中检索所需的插件，并将其发送到要在计算机上安装的客户端。有关安装趋势科技服务器深度安全防护系统客户端的信息，请参考《安装指南》。

生成部署脚本

安装客户端，将其激活，以及使用安全策略应用防护需要多个步骤才能完成，可从要保护的计算机上的命令行编写脚本。部署脚本生成器工具将生成要在计算机上运行的定制脚本，该脚本可从趋势科技服务器深度安全防护系统管理中心下载客户端软件，安装并激活此软件，然后应用安全策略。有关使用部署脚本生成器的信息，请参阅**部署脚本**。

中继组

趋势科技服务器深度安全防护系统中继是将安全更新和软件更新从趋势科技分发至受保护资源的网络的一部分。如果要将您的防护保持为最新，必须至少拥有一个正常运行的趋势科技服务器深度安全防护系统中继。所有 64 位 Windows 和 Linux 趋势科技服务器深度安全防护系统 9.5 客户端均包含中继功能。

每个中继都属于一个中继组（即使只是具有一个成员的组）。客户端/设备将分配给中继组，而非各个中继。这样就会在组内单个中继脱机的情况下提供一些冗余。系统中存在一个名为“缺省中继组”的组，缺省情况下所有新中继均分配给该中继组。您可以拥有多个中继组，并且这些中继组可以组织到层次结构中，以便处于顶级的组从趋势科技更新服务器获取其更新，然后通过子组层次结构传递这些中继组。

注意： *中继可从另一个中继组获取安全更新，而不是从另一个中继（即使它们两个都是同一中继组的一部分）。中继必须从另一层级较高的中继组或另一已配置的安全更新源处获取更新。有关配置安全更新的更多信息，请参阅*安全更新。

有关在客户端上启用中继功能的信息，请参阅《用户指南》中的**中继组**。

在**中继组**页面上，可执行下列操作：

- **新建** () 中继组
- **删除** () 中继组
- 查看中继组的**属性** ()

中继组属性

常规

常规信息：中继组的名称和描述。

安全更新：选择此中继组将从中下载并分发安全更新的源。缺省中继组将始终使用在**管理 > 更新 > 中继组**中定义的主更新源。不过，您创建的任何其他中继组也都可以使用此主更新源或您配置的另一个更新源。

代理服务器：指定访问主安全更新源必须使用的代理服务器。主安全更新源通常为趋势科技更新服务器，在**管理 > 系统设置 > 更新**选项卡上进行配置。如果中继组配置为使用主安全更新源，则该组中的中继将使用代理服务器。如果该中继组配置为从其他中继组获取其安全更新，则仅当丢失与其他中继组的连接时才使用代理服务器，并且该组必须回退为主安全更新源。

成员：是组中成员的中继。

已分配给

已分配给选项卡显示将此中继用作安全和软件更新源的计算机。

趋势科技·中国 趋势科技（中国）有限公司
上海市淮海中路 398 号世纪巴士大厦 8 楼
电话：021-6384 8899　传真：021-6384 1899 service@trendmicro.com.cn
www.trendmicro.com
Item Code: APCM96842/150106