EventLog Analyzer
快速操作手册

产品快速使用指南

技术支持部

本文档旨在帮助用户快速熟悉产品使用的方法。

目录

1.安装和开始使用EventLog Analyzer

从下载页下载EXE文件： https://www.manageengine.cn/products/eventlog/download.html

1.1 安装

在运行产品之前，检查是否满足前提条件。

硬件需求

32位，安装和运行Evenglog Analyzer的最小系统要求如下：
1 GHz，32-bit (x86)奔腾双核处理器或其他相同性能处理器
2 GB内存
5 GB磁盘空间

64位，安装和运行Evenglog Analyzer的最小系统要求如下：
2.80 GHz，64-bit (x64) 志强（Xeon® LV）处理器或其他相同性能处理器
2 GB内存
5 GB磁盘空间

EventLog Analyzer要求使用1024x768或以上的屏幕分辨率。

操作系统要求

EventLog Analyzer可以安装和运行在以下操作系统（32位和64位）的设备上：

Windows

Windows 2016 Server
Windows 2012 Server
Windows 2008 Server
Windows 2003 Server
Windows 2000 Server
Windows 8
Windows 7
Windows 2000
Windows Vista
Windows XP
Windows NT

Linux

Linux - RedHat RHEL
Linux - Mandrake
Linux - Mandriva
Linux - SuSE
Linux - Fedora
Linux - CentOS
Linux - Ubuntu
Linux - Debian

VMware

VMware environment　　支持的Web浏览器

支持的web浏览器

Microsoft Edge
最新Firefox
最新Chrome

支持的平台和设备

EventLog Analyzer可以对任意1设备进行日志的收集、索引、分析、归档、搜索和生产报表。默认支持以下操作系统和设备的日志：

Windows Server 2016
Windows Server 2012
Windows Server 2008 R2
Windows Server 2008
Windows Server 2003
Windows Server 2000
Windows 8
Windows 7
Windows 2000
Windows Vista
Windows XP
Windows NT
Linux - RedHat 9.0
Linux - Mandrake
Linux - Mandriva
Linux - SuSE

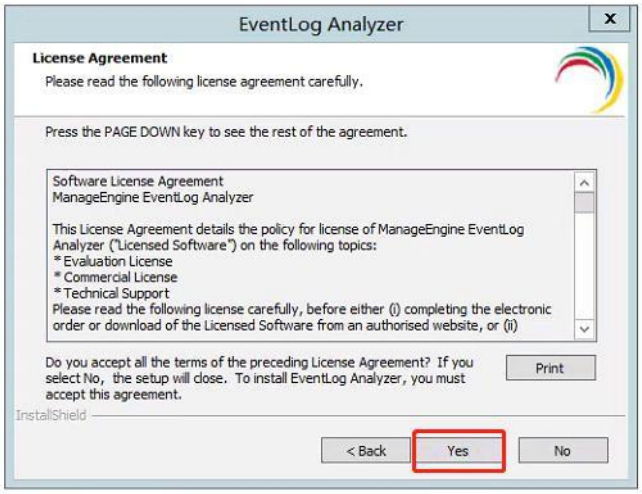
Linux - Fedora
Linux - CentOS
Linux - Ubuntu
Linux - Debian
UNIX - Solaris, HP-UX
IBM AS/400 - Variants V5R1、V5R2、V5R3、V5R4、V5R5和V6R1
IBM AIX
Cisco交换机和路由器
VMWare - Syslog版本
Windows的SNARE^

默认还支持以下应用的日志

IIS W3C Web服务器
IIS W3C FTP服务器
Apache Web服务器日志
MS SQL Server
Oracle 10 G Release 2 (10.2.0.3) - 审计日志
DHCP Windows日志
DHCP Linux日志
打印机日志

1.2 启动

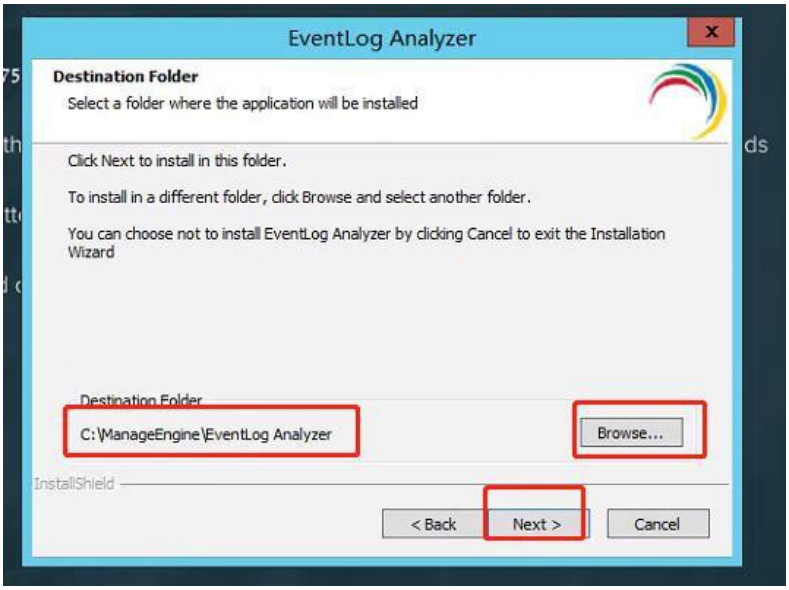
A. 双击下载后的exe文件打开安装程序，阅读并选中同意许可协议的条款和条件



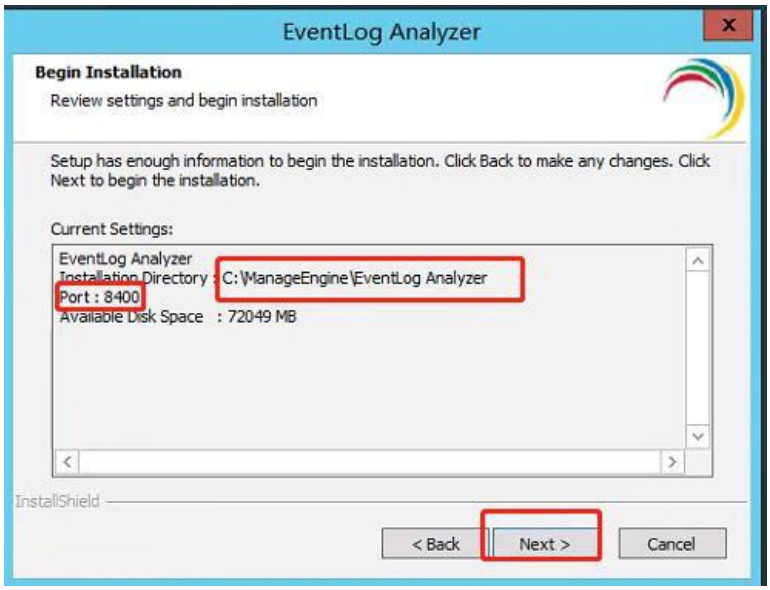
选择安装产品的文件夹

默认安装位置是C:\ManageEngine\EventLogAnalyzer。

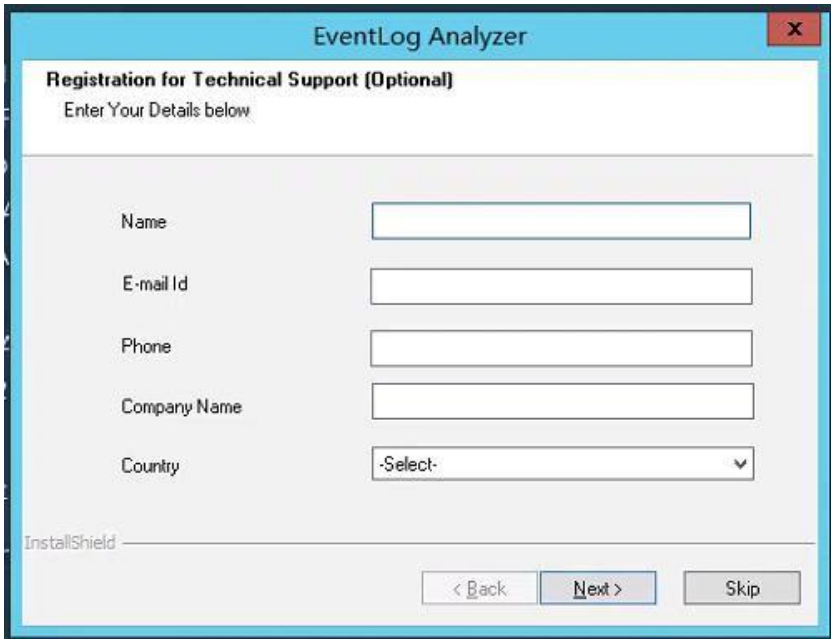
B.可以通过浏览选项，修改安装位置



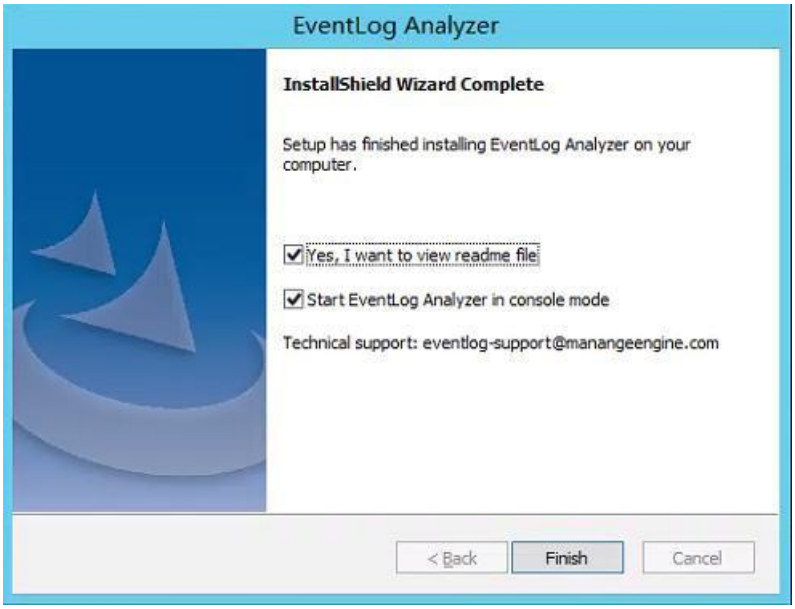
C.默认端口号是8400。确保默认和所选端口号没有被占用



D. 输入个人信息以便获取技术支持



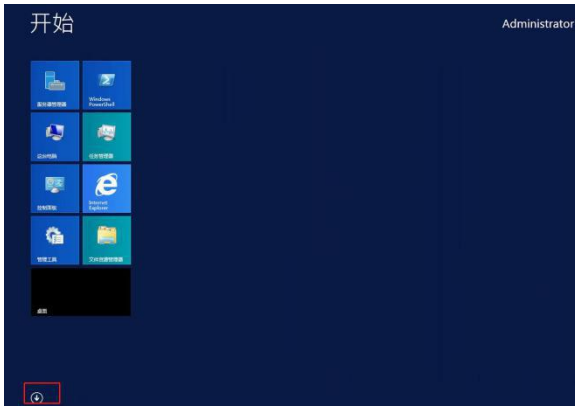
E. 安装完成后，安装向导显示自述文件并启动EventLog Analyzer服务器



F. 安装完毕后可以直接双击桌面图标启动EventLog Analyzer

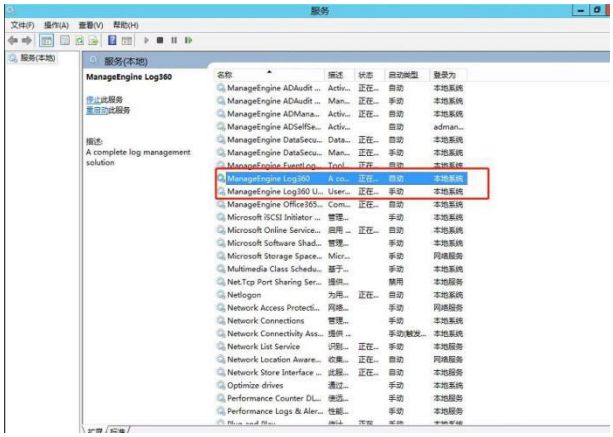
同时，我们建议您在安装完毕后将EventLog Analyzer安装为windows服务，以windows2012为例步骤如下：

（1） 点击左下角windows图标进入系统配置界面后点击左下角的箭头



（2） 找到Log360程序，首先点击Stop Log360停止程序运行，然后点击Install Log360 in Service。

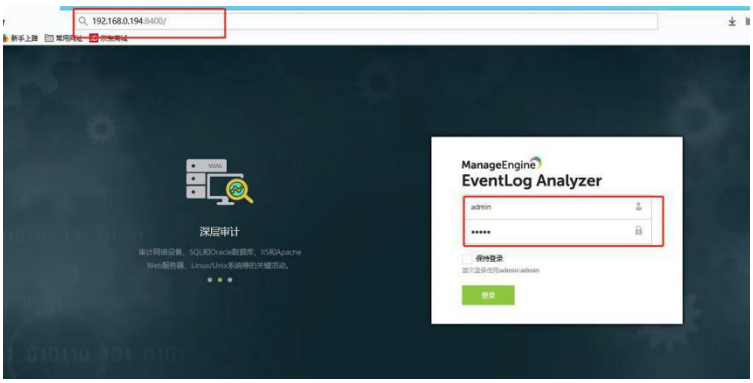
（3） 安装成功后，可以在服务中看到该程序已经启动，之后每次启动操作系统时程序会随机启动。



2.连接EventLog Analyzer服务器

成功启动服务器后，按照以下步骤访问EventLog Analyzer。

- 打开产品支持的web浏览器。键入链接URL：http://<devicename>:8400（其中<设备名称>是运行EventLog Analyzer的名称，8400是默认的web服务器端口。）
- 使用默认的用户名/密码(admin/admin)登录EventLog Analyzer。
- 点击“登录”按钮。



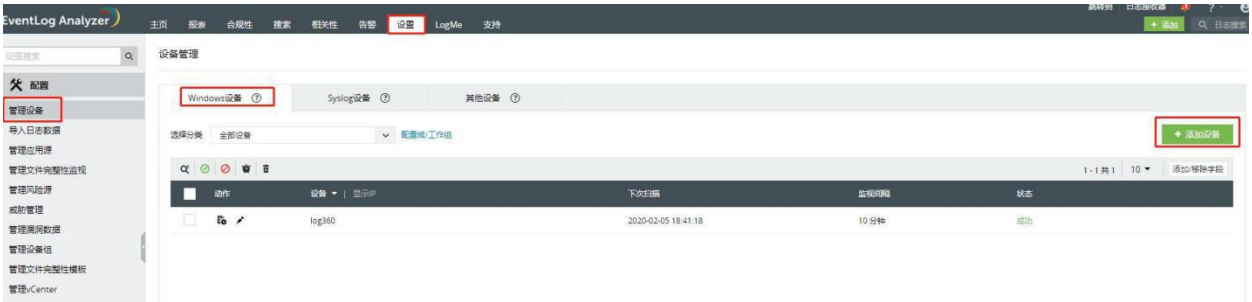
3.添加监控设备

3.1 Windows设备

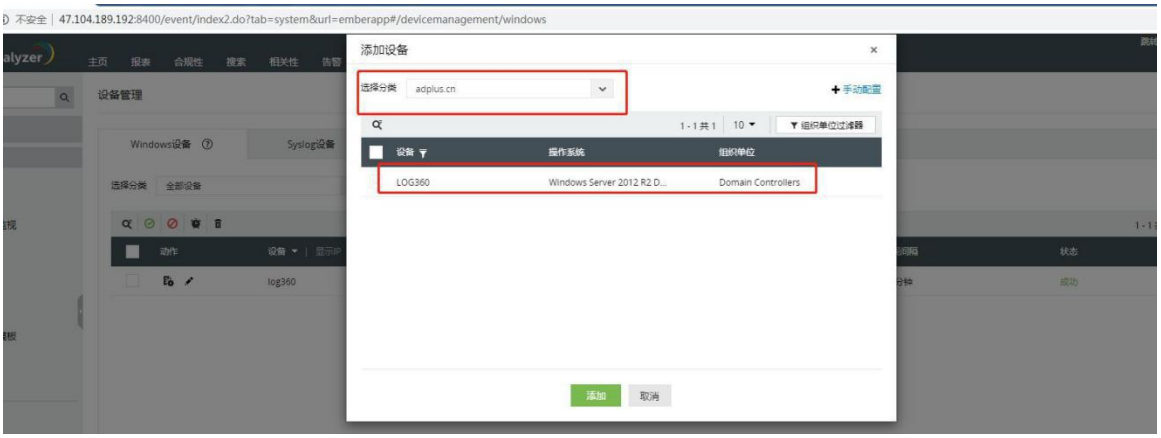
在所有的Windows设备，确保已启用WMI、DCOM，并且为各自的模块/对象启用日志。请使用第三方工具，如SNARE，转发syslog格式的Windows事件日志。

A.添加Windows设备 1.

1.选中配置选项卡，在左侧下拉菜单中选择设备管理，选中，点击添加windows设备选项卡，点击右侧添加设备



2.在弹出的对话框中选择域/工作组，并添加搜索到的设备



B.手动添加Windows设备

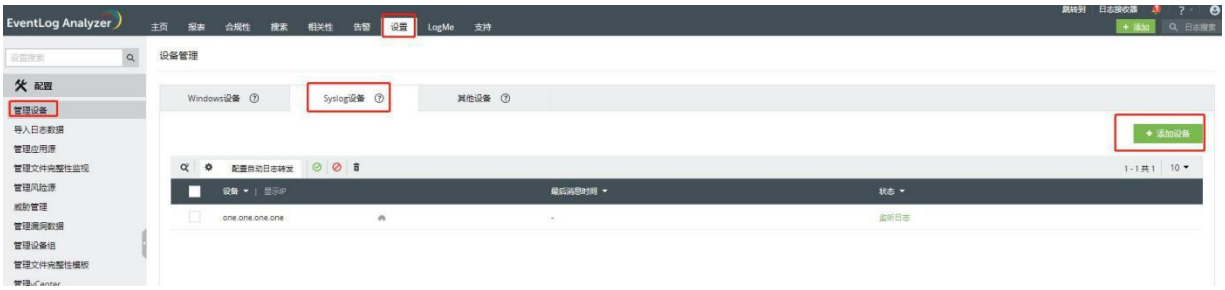
您还可以通过点击手动配置链接，手动添加设备。1.输入设备名称或IP地址。

2.使用管理员凭证，输入用户名和密码，点击验证登录链接。

3.点击“添加”按钮。

3.2 syslog设备及其它设备

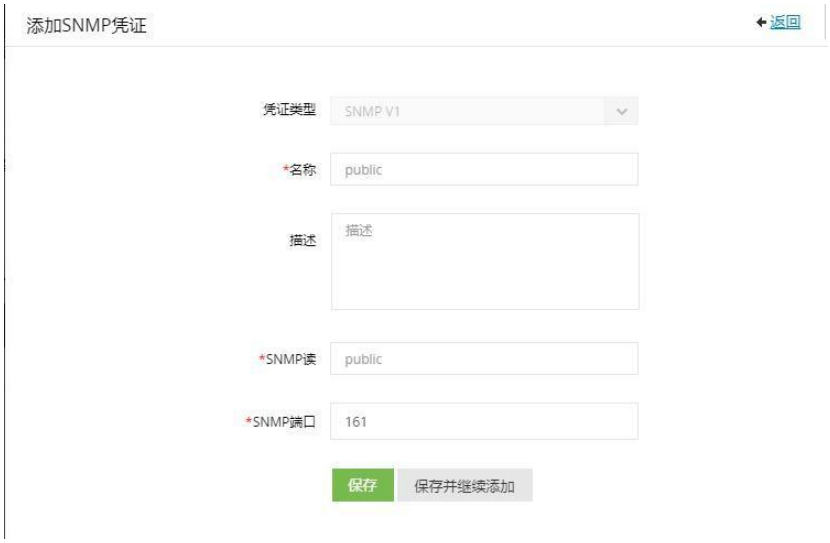
1.选中配置选项卡，在左侧下拉菜单中选择设备管理，选中，点击添加syslog设备选项卡，点击右侧添加设备



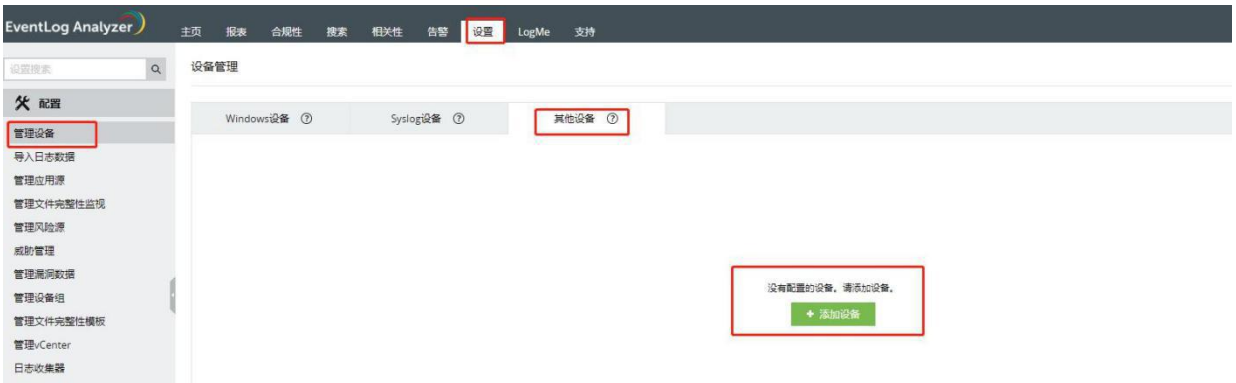
2.添加Syslog设备窗口，点击发现&添加链接。您可以根据IP范围（开始IP至结束IP）或CIDR，发现您网络中的Syslog设备。

3.输入开始IP和结束IP或CIDR范围，发现Syslog设备。

4.选择SNMP凭证，自动发现您网络中的Syslog设备。默认下，公共SNMP凭证可用于 扫描您网络中的Syslog设备。或者，您可以通过点击添加凭证按钮“+”，添加SNMP 凭证。选择SNMP凭证后，点击“扫描”按钮，自动发现指定IP或CIDR范围内的Syslog 设备。



5. 选中配置选项卡，在左侧下拉菜单中选择设备管理，选中，点击其它设备选项卡，点击下方添加设备按钮



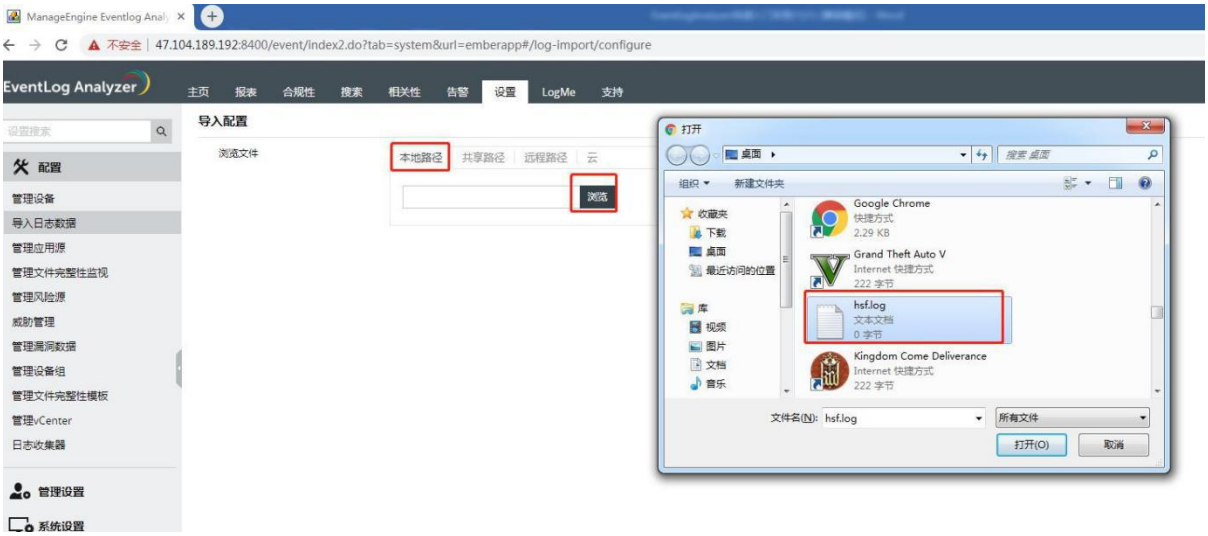
6.选择设备类型，输入设备名称后点击添加

4.导入日志

EventLog Analyzer可以让您导入任何常用日志，并为Windows(EVTX格式)、syslog设备、应用程序和归档文件提供预定义报表。

1. 选中配置选项卡，在左侧下拉菜单中选择导入日志数据，点击右侧导入数据按钮

2.选择导入日志的方式（以本地导入为例），选择本地路径→浏览→找到在本地的日志并导入



3.选择在弹出的对话框中选择设备后点击导入即可

5.使用预定义报表

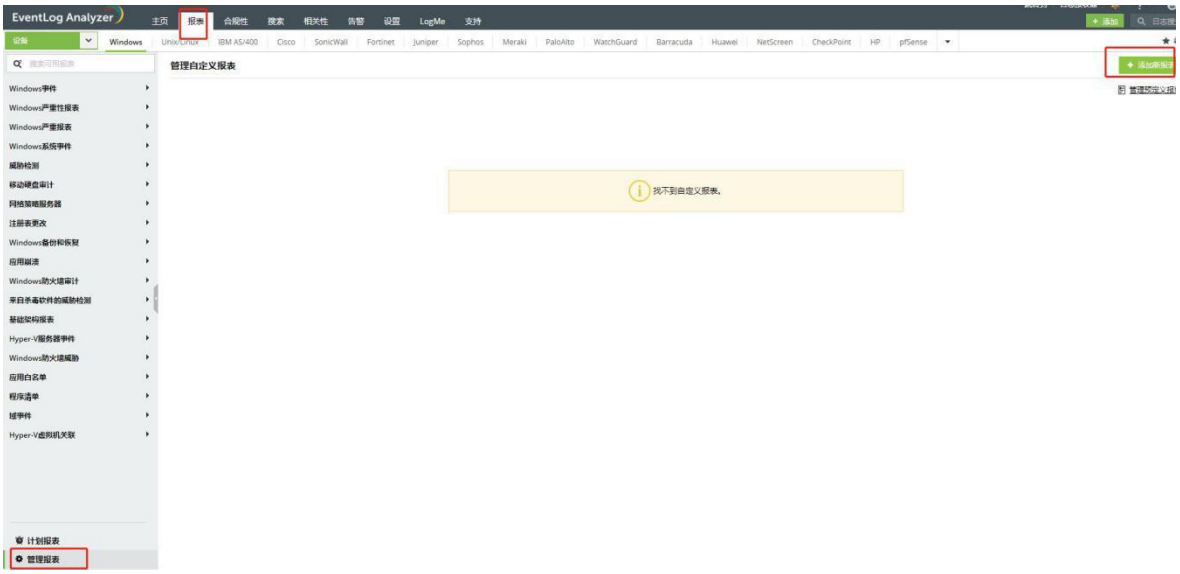
EventLog Analyzer提供固有报表，帮助分析网络安全和审计内部用户的活动。报表提供超过750种日志来源的信息，包括：

- 网络设备，如防火墙、路由机、交换机和IDS/IPS
- 应用程序包括Oracle和MSSQL服务器数据库
- Web服务器
- Windows和Linux/Unix机器
- IBMAS400系统

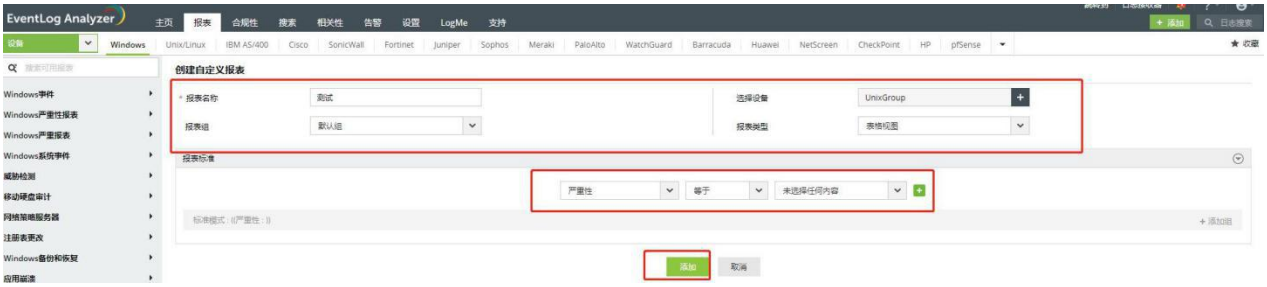
报表组包括Windows、应用程序、网络设备、漏洞、vCenter、我的报表、收藏夹 和基于用户的报表。

6.创建自定义报表

1.点击报表→管理报表→添加新报表



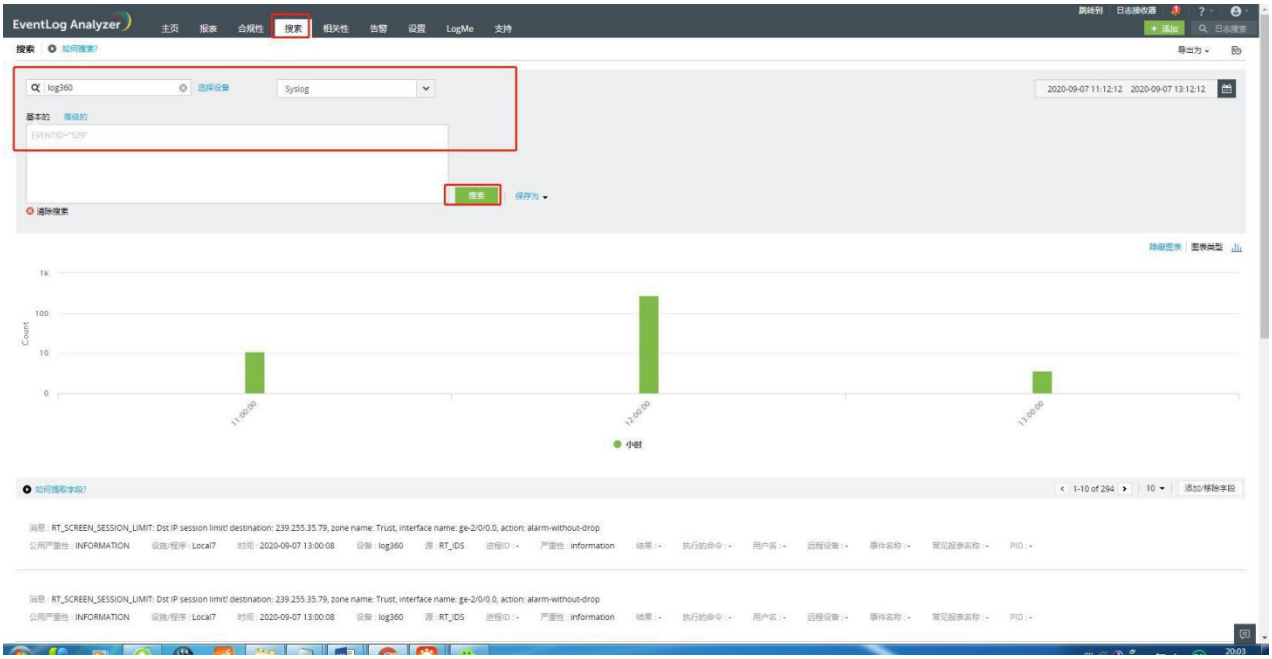
2.在弹出的页面中依次填入报表名称，选择好设备及其它信息后，点击添加即可



7.日志搜索

EventLog Analyzer的日志搜索功能非常简单，您可以搜索任何信息。默认下，在日志中查找输入的搜索项。搜索结果可以保存为PDF和CSV格式。

要搜索日志，请点击搜索选项卡，选择好设备及日志类型后点击搜索即可



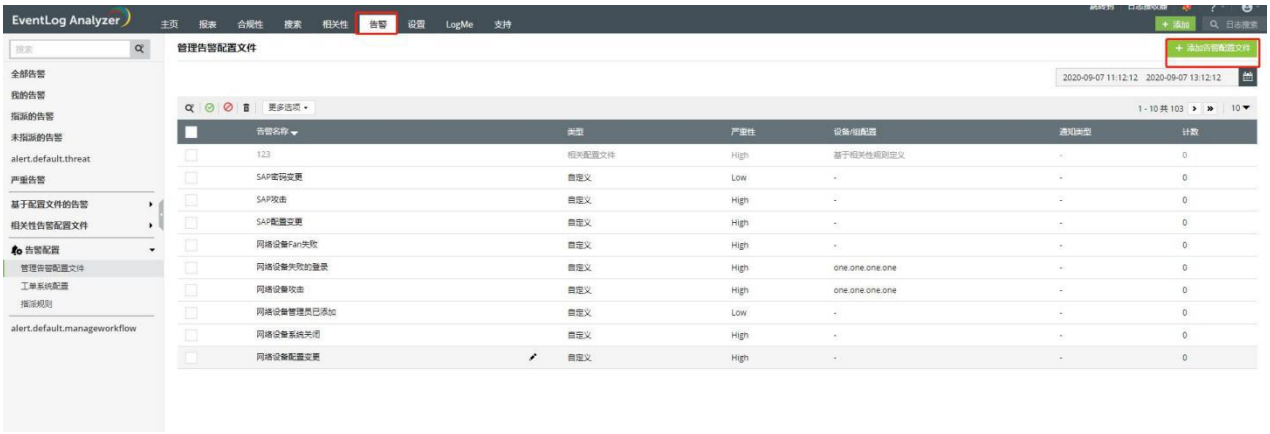
8.创建告警配置

EventLog Analyzer可以配置为，当发生指定的安全事件时，产生告警。您可以：

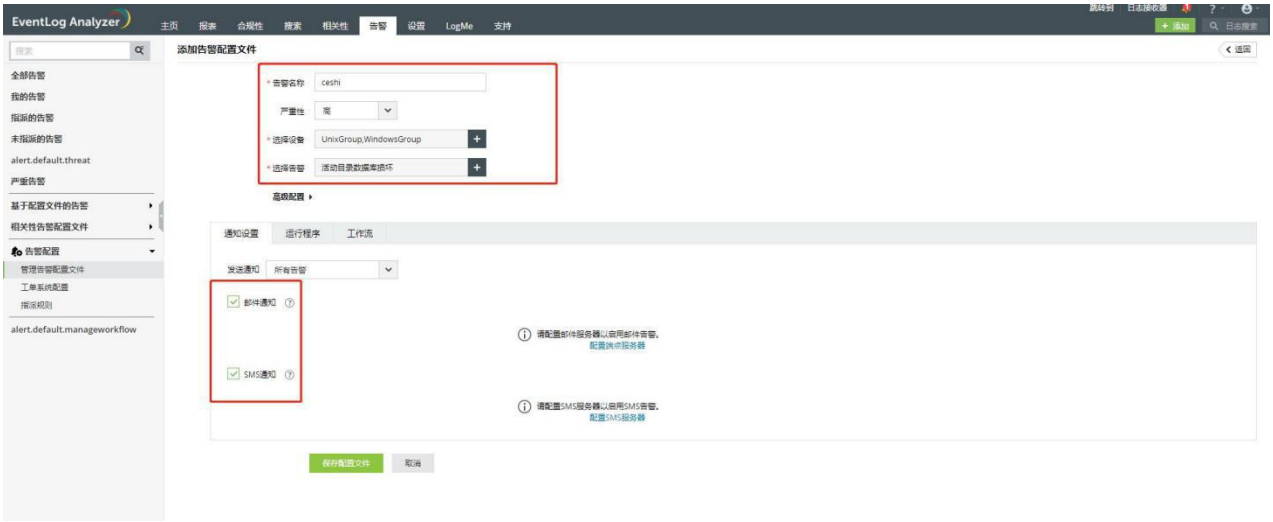
- 从500多种预定义告警中选择或自定义告警
- 当发生任何需要关注的事件时，通过电子邮件或短信获取实时通知。
- 指定生成告警时运行的程序。
- 配置事件监控的设备或设备组。
- 指定触发告警事件发生的次数和时间段。
- 对任何合规策略事件进行告警。
- 接收相关性告警，例如，两件或多件相关事件，需要进一步调查。

需要创建告警配置文件：

1.点击告警选项卡，选择右侧添加告警配置文件



2.在弹出的对话框中输入告警名称，所需要的告警的设备，以及需要选择告警的类型，并选择好告警通知管理员的方式。



3.单击保存配置文件的按钮后，即可生成新的配置文件

9.高级配置

数据库维护

在数据库维护中可以设置当前存储大小，定义收集的原始日志将保留在数据库中的天数、相关性保留期定义格式化日志数据将保留在数据库中的天数、告警保留期定义告警将在数据库中保留的天数。

在设置选项卡中单击数据库维护设置即可看到，并可以在相应位置设置您需要保留的天数。

归档设置

EventLog Analyzer可以定期归档日志。您可以配置归档间隔和保留期限，归档日志为加密和设置时间戳的日志。

在设置选项卡中单击管理存档后，在上方选择设备，即可看到相应的数据