安天追影高级威胁鉴定系统

使用手册

版权声明

目录

第 1 章 产品介绍

介绍

本章总体介绍追影高级威胁鉴定系统，内容包括：

- 产品概述
- 产品硬件介绍
- 部署安天追影高级威胁鉴定系统
- 访问安天追影高级威胁鉴定系统

产品概述

安天追影高级威胁鉴定系统（简称“追影”）是安天公司针对当前日益复杂的网络威胁环境、特别是 APT（高级可持续性威胁）攻击潜心研发的设备级威胁鉴定系统。追影可对用户网络中的文件进行深度、智能、持续性的分析，识别各类已知、未知安全威胁，分析并监控一切可能用于 APT 攻击的文件，并通过内容详实的文件分析报告呈现鉴定分析结果，进而帮助用户掌握网络威胁状况，提高网络安全防护能力。安天追影高级威胁鉴定系统与安天私有云安全系统以及安天网络病毒监控系统（VDS）联动，可构建针对 APT 攻击的纵深网络安全防御体系。

追影采用静态与动态相结合的智能综合检测方式对用户网络中的各类文件进行深度威胁鉴定。可鉴定文件类型包括可执行文件（EXE、DLL 等）、压缩文件（ZIP、RAR 等）、文档文件（PDF、Word、Excel、PPT、Flash 等）。同时，该系统可对 URL 网页访问行为进行监控分析，动态监控恶意网页脚本，发现浏览器溢出攻击的行为。

静态检测与动态检测

追影的静态检测技术手段包括格式识别解析、Shellcode 发现、堆喷射检测、字符串信息提取以及漏洞检测。

追影的动态检测技术将未知文件投放到虚拟机中运行，利用系统监控和网络监控手段，监控记录其运

行的本地行为，包括远程线程插入、文件操作、注册表操作、驱动加载、网络通信访问、系统文件的修改以及网络访问信息等。根据被鉴定文件在虚拟机中的行为，追影可判断被鉴定文件是否为恶意文件，同时，被鉴定文件的来源、相关联网址以及该文件试图连接的恶意网址等信息也一并被记录并反馈给用户。追影动态检测分析文件的行为，不单纯依赖特征，可以对未知 0day 攻击进行分析捕获，进而有效防范 APT 攻击。

模拟运行环境在实现仿真的同时，还具有自我保护能力。该环境中包含各种常用软件，例如 Word、WPS、Adobe Reader、QQ、游戏、杀毒软件等，同时具有网络行为响应能力（响应恶意软件的网络请求）。为实现良好的自我保护功能，该环境还具备虚拟系统特征文件（虚拟机进程、注册表、系统文件、自身监控进程等）隐藏能力。

静态检测和动态检测有机结合，基于追影云数据，配合智能学习，经过动态综合分析鉴定，追影可有效分析可疑文件，同时，结合强大的自学习能力，追影又可不断更新鉴定结果，在提高文件检测率的同时保证文件鉴定的准确率。以上文件鉴定机制区别于传统的特征匹配鉴定模式，使追影能够在文件威胁鉴定时不依赖病毒特征库，在特征库无法及时更新时，仍可准确鉴定文件。

病毒特征库、白名单库

追影搭载安天自主研发的 AVL SDK 反病毒引擎，可识别多达 9000 万（2014 年 12 月数据）种病毒，使追影具备了对大量的、已知的恶意程序的过滤能力。同时，追影提供完备的“病毒百科”，帮助用户了解病毒信息。追影的白名单库容量超过 7000 万（2014 年 12 月数据），保证了对合法软件的识别和分类，帮助降低误报。

基于强大病毒库以及白名单，追影可直接对已知威胁进行有效识别，不仅能够大幅提高追影的识别效率，还可明显减少动态分析的检测噪音，从而使系统更专注于分析未知的高级威胁。

统计信息以及分析报告

追影 Web 界面给用户呈现多维度的统计信息以及专业的文件分析报告，帮助用户从多个角度了解追影工作状态以及文件鉴定结果。

产品硬件介绍

追影硬件为机架式服务器，可放置在标准机柜中。追影硬件规格及性能参数请参考下表：

项目	规格
硬件规格	
处理器	英特尔®至强™处理器 E5 系列，6 核处理器 * 2
内存	8GB x 8
网络接口	10/100/1000 baseT × 4
硬盘控制器	系统固件：SSD 160GB x 2；RAID 模式：RAID 1 数据存储：SATA 2TB x 4（企业级）；RAID 模式：RAID 0、RAID 1
电源	700W（1+1 冗余电源）
电压	AC 220V
机箱尺寸	2U
温度	工作：10℃～35℃（50℉～95℉）；存储：-40℃～55℃（-40℉～131℉）
性能指标	
检测性能	每天最多可分析 100000 个文件
动态检测性能	每小时最少可分析 50 个文件
病毒特征库	大于 9000 万（2014 年 12 月数据）
白名单库	大于 7000 万（2014 年 12 月数据）

表 1-1：追影硬件参数

部署安天追影高级威胁鉴定系统

追影提供多种方式供用户上传需鉴定文件（单个文件上传、指定 URL 文件批量下载、文件上报工具上报），同时，追影可以与安天私有云安全系统以及安天网络病毒监控系统联动，帮助分析鉴定文件，构建完整、高效的安全防护体系，如图 1-1 所示。除此之外，追影提供开放接口，使产品可与第三方网络设备（防火墙、入侵防御系统、UTM 等）联动，实现准确、实时的在线阻断防御，如图 1-2 所示。

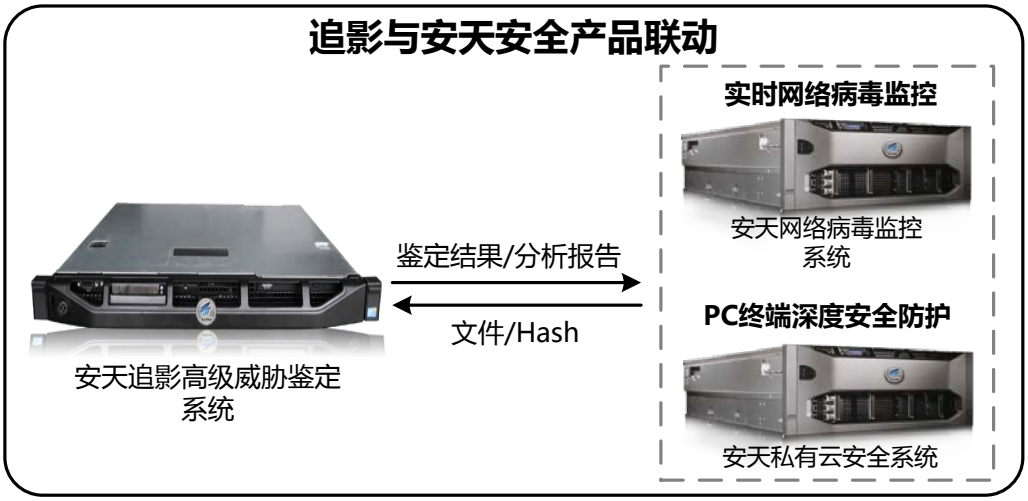

图 1-1：追影与私有云、VDS 联动工作示意图

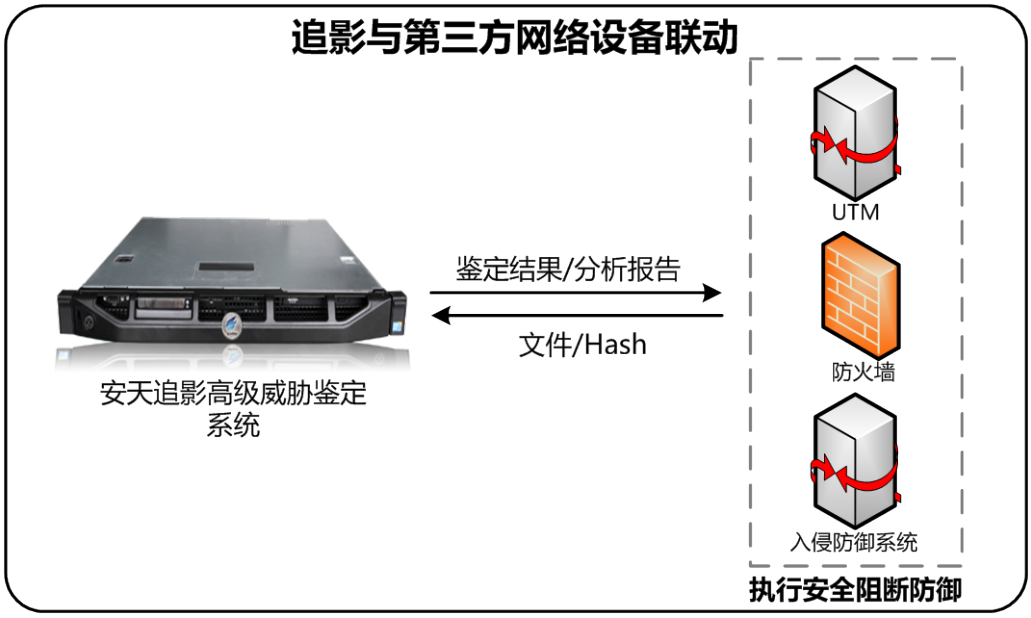

图 1-2：追影与第三方安全设备联动工作示意图

通过 Web 界面上传被鉴定文件或者与安天安全设备联动工作时，用户只需将追影接入网络，并保证追影与相关网络设备网络可达即可。

实现追影与第三方设备联动，需要用户做相关开发工作。如有第三方联动需求，请与安天联系。

配置追影 IP 地址

追影的接口 Gb1 上配有默认 IP 地址 192.168.0.1，初次使用追影时，为保证追影与所在网络的网络连通，请先按照以下步骤配置追影的 IP 地址：

1. 通过网线将追影的接口 Gb1 与 PC 相连。
2. 将 PC 的 IP 地址改成与 192.168.0.1 同网段的地址（例如 192.168.0.5）。
3. 打开 PC 浏览器，在地址栏输入 http://192.168.0.1/_lk/index.html，访问追影设备，此时即显示追影首页。
4. 点击页面右上角的“登录”选项，弹出登录对话框。在对话框中分别输入默认用户名/密码“admin/admin”，然后点击“登录系统”按钮。

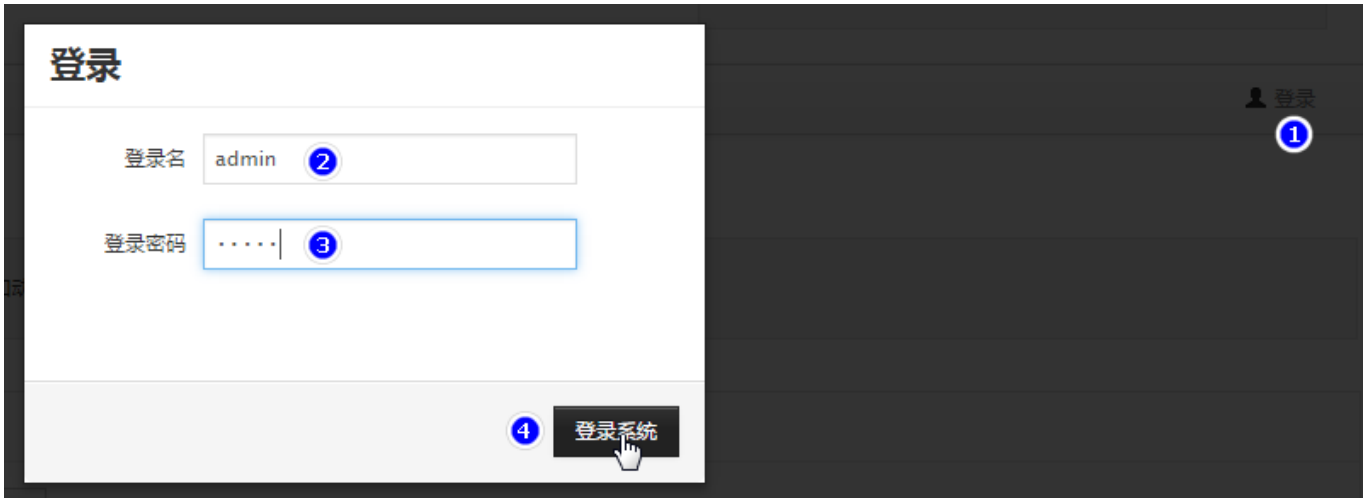

图 1-3：登录追影系统

5. 点击“配置 > 服务器配置”，进入服务器配置页面。
6. 如有需要（例如客户网络使用自有 DNS 服务器），在“DNS 配置”部分输入 DNS 服务器 IP 地址，然后点击“保存设置”。
7. 在“em1”部分，在对应的文本框分别输入 IP 地址、掩码以及网关地址，然后点击“保存设置”。

访问安天追影高级威胁鉴定系统

为追影配置 IP 地址后，在 PC（与追影网络连通）的浏览器上输入 http://*追影 IP 地址*/_lk/index.html 即可访问追影页面。以下为追影页面布局说明：

图 1-4：追影系统页面布局示意图

导航栏

导航栏提供追影系统的一级菜单，菜单项具体说明如下：

菜单项	说明
概要	点击进入概要页面。该页面显示追影系统当前主要的文件鉴定分析统计信息，包括最新发现的恶意文件（点击“报告”查看详情）、系统在指定时期的分析统计信息、被分析文件的类型统计信息以及被分析文件的传输协议统计信息。
统计	点击进入统计页面。用户可以在该页面查询指定时间（按日、按月、按年）的统计信息，也可导出 PDF 版统计报告。
检索	点击进入检索页面。该页面列出所有被分析文件，用户可根据需要指定检索条件对文件进行检索。
自定义	点击进入自定义页面。用户可在该页面指定信任/不信任 IP 以及查看联动设备信息并做相关配置。 ● 主机信任列表：指定的信任 / 不信任 IP 会对智能学习结果产生部分影响。信任 IP/不信任 IP 用于和第三方安全产品联动的场景（第三方网络设备根据 IP 的信任状态对 IP 做出相应的管控）。 ● 互动设备控制 :互动设备即可与追影联动的设备。互动设备列表各列信息说明如下： ■ 标识符：联动设备的名称。 ■ 首次出现时间：相应设备首次告知追影的时间。 ■ 末次交互时间：相应设备最近一次与追影交互的时间。 ■ 声称 IP：相应设备告知追影的自身的 IP 地址。 ■ 备注：显示设备的备注信息。 ■ 允许/禁止：指定追影是否与相应设备联动。
配置	点击进入配置相关页面（如弹出登录页面，请输入用户名密码并登录。默认用户名密码均为“admin”），包括： ● 分析队列：显示系统各文件分析模块对文件的处理情况。 ● 硬件资源：显示设备硬件资源实时使用情况。 ● 组件状态：显示系统后台进程运行状态。 ● 服务器设置：提供网络配置选项，供用户部署追影设备。 ● 授权管理：显示设备使用日期，提供授权续费选项。
个人历史	点击进入文件上传页面（该选项登录后可见）。用户可在该页面上传文件供追影分析检测，上传方式包括： ● 手动上传：手动上传本地单个文件到追影。 ● 下载：指定文件 URL，追影将会下载相应的文件进行分析。 ● 客户端：下载文件上报工具，批量上报本地文件到追影（如需文件上报工具，请与安天联系）。

admin@local	点击显示以下子菜单项： ● 个人历史：点击进入文件上传页面。 ● 服务器升级：点击进入升级页面对追影系统进行升级。 ● 修改密码：修改当前登录用户的密码。 ● 退出：点击退出系统。

表 1-2：导航栏菜单选项说明

系统信息

此处显示的系统信息包括系统当前软件版本号、设备持续在线时间以及系统平均分析次数统计信息。

主窗口

主窗口显示当前页面的主要信息。

第 2 章 系统管理

介绍

本章介绍追影系统管理相关内容，包括：

- 查看系统分析队列
- 查看硬件资源使用情况
- 查看系统组件状态
- 配置追影服务器（网络配置）
- 授权管理
- 管理员配置
- 系统升级

查看系统分析队列

为获得准确、及时的分析鉴定结果，实现动态持续性分析，追影内置多个文件分析模块，对文件进行分析鉴定。追影的主要分析模块包括：

- 邮件分析：针对通过邮件传输的文件进行邮件专有内容的分析；
- 安全云：通过云端技术，存储各类信息，包括分析结果信息、智能学习信息等。云数据为其他分析模块提供数据支撑；
- 智能学习：基于文件相关的各类数据，对文件进行动态智能学习；
- 聚类分析：文件经过分析后，系统会根据文件的各种信息构建文件向量，再根据向量比较的方式对文件进行聚类。该方法可以对已知家族的变种进行聚类，也可以对未知样本进行新的聚类；
- 动态行为：将执行文件、溢出文件投放到模拟系统中进行动态分析，监控并记录文件运行行为，进而判断是否存在异常行为；
- 静态分析：通过格式识别解析、Shellcode 发现、堆喷射检测、字符串信息提取以及漏洞检测等

手段对文件进行静态分析；

- 格式分析：对文件格式进行分析，从而进行更有针对性的合理分析鉴定。

系统的分析队列展现了系统当前对文件的处理情况，具体包括每个分析模块的已处理文件、待处理文件等信息。请按照以下步骤查看系统的分析队列情况：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 此时显示的即为分析队列信息（“分析队列”标签为选中状态）。该页面通过图表的方式，显示系统所有分析模块的工作状态。鼠标经过状态条，系统将显示相关详细信息。

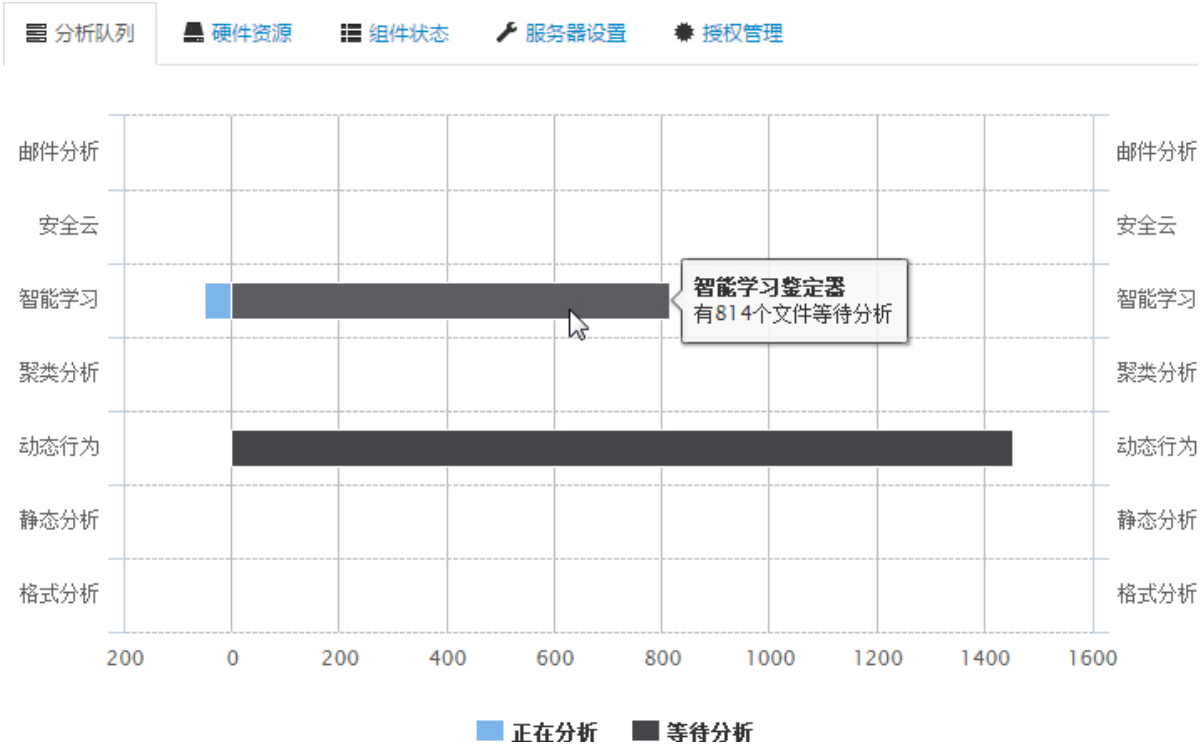

图 2-1：追影分析队列信息

查看硬件资源使用情况

系统硬件资源使用情况即设备内存、CPU 以及磁盘的使用情况，可帮助用户了解当前追影系统的硬件资源使用情况以及工作状态。请按照以下步骤查看追影硬件资源的使用情况：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html 并回车。

2. 在导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 点击“硬件资源”标签。该标签页通过图表的方式显示追影设备的内存、CPU 以及磁盘的实时使用情况。鼠标经过取值点，系统将显示相关详细信息。

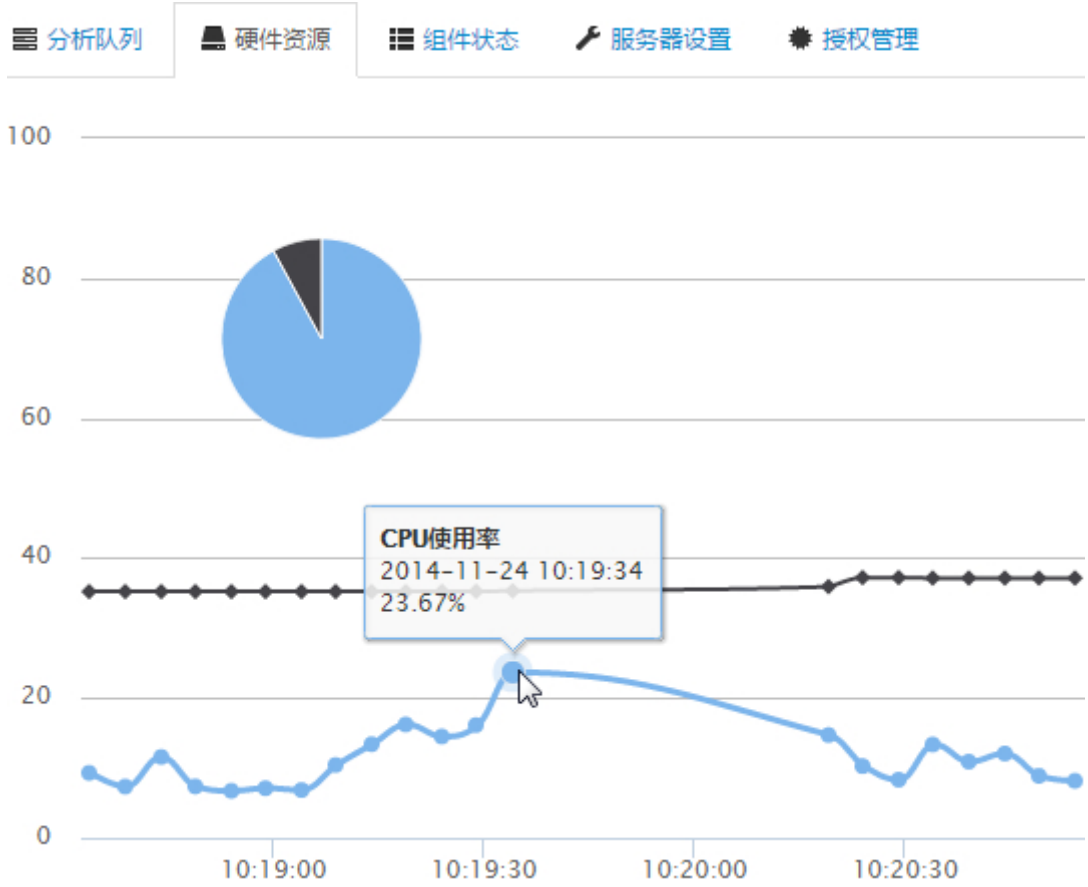

图 2-2：追影硬件资源使用情况

当磁盘利用率过高影响追影的正常工作时，建议联系安天售后，采取相应措施。

查看系统组件状态

组件状态即追影系统后台进程状态。当发现有进程状态为“停止”时，建议重启追影（轻按追影设备电源按钮，待设备进程处理完毕设备关机后再重新开机）。如果重启后进程状态仍为“停止”，建议联系安天售后解决相关问题。

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系

统”进入系统配置相关页面（如已登录，请忽略）。

3. 点击“组件状态”标签。该页面通过表格的方式显示系统所有后台进程的工作状态。

图 2-3：追影后台进程工作状态

配置追影（网络配置）

追影的网络配置包括 DNS 服务器配置以及接口 IP 地址配置。

对于使用自有 DNS 服务器的用户，请配置 DNS 服务器以保证追影网络连通。请按照以下步骤配置 DNS 服务器：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 点击“服务器设置”标签。在页面右侧的“DNS 设置”部分文本框中输入 DNS 服务器的 IP 地址。如需指定多个 DNS 服务器，回车换行后输入新的 IP 地址。

4. 配置完成点击“保存设置”按钮。

图 2-4：配置 DNS 服务器

请按照以下步骤配置接口的 IP 地址：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 点击“服务器设置”标签。在“网卡信息”部分，为追影的接口配置 IP 地址。系统支持手动配置和自动获取两种方式，用户可根据需要进行选择。
   - 手动配置：选中“手动配置”单选按钮，分别在 IP、子网掩码、网关文本框中输入相关信息。
   - 自动获取：选中“自动获取”单选按钮。
4. 配置完成点击“保存设置”按钮。

授权管理

追影通过序列号方式管理系统的升级权限（病毒特征库、白名单以及追影系统升级）以及文件的上传权限（单个文件上传、通过指定 URL 下载文件到追影）。授权管理即通过输入正确的序列号获得追影系统在指定时期内的系统升级权限以及文件上传权限。初始设备必须安装序列号才可正常工作。

管理员配置

当前系统使用单管理员方式管理，即只有默认管理员“admin”。用户可更改管理员“admin”的密码。新密码不得少于 6 位，支持数字、字母（区分大小写）、特殊符号。请按照以下步骤更改管理员密码：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 在导航栏右侧，点击“admin@local > 修改密码 “。

图 2-5：修改密码菜单项

4. 在弹出的“修改密码”对话框输入旧密码、新密码，然后点击“确认修改”。

系统升级

升级追影系统，需要使用安天提供的升级工具。该工具存储在光盘中由安天寄出。追影升级的具体过程为：

1. 打开升级工具所在目录，双击 webSocketApp.exe 启动升级工具。

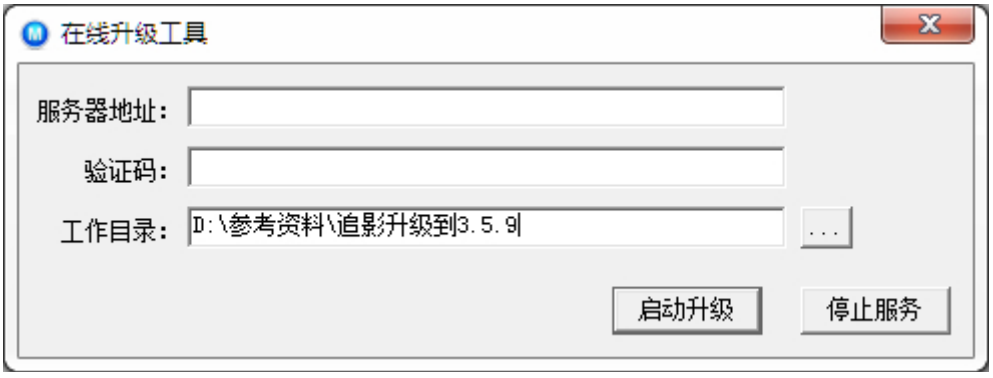

图 2-6：在线升级工具

2. 在升级工具上填写相关配置信息：
   - 服务器地址：http://*追影 IP*/ng8w/update/websocket；
   - 验证码：输入追影服务器升级页面（admin@local > 服务器升级）显示的“校验码”（实际校验码以用户界面显示内容为准，下图仅作参考）。

图 2-7：升级校验码

3. 点击升级工具的“启动升级”按钮。
4. 在追影“admin@local > 服务器升级”页面点击“升级”按钮。

第 3 章 上传文件

介绍

通过追影的 Web 页面，用户可使用以下两种方式将文件传送到追影进行分析鉴定，分别是：

- 手动上传
- URL 下载

为方用户查看上传、下载历史信息以及文件对应的分析报告，系统记录用户的上传、下载动作，并显示在相应页面。

另外，除使用追影 Web 页面上传功能外，为方便用户将本地文件批量上传至安天追影高级威胁鉴定系统进行安全分析鉴定，安天提供批量文件上报工具。该工具为客户端工具，用户可将其安装到个人 PC 进行使用。如需使用该工具，请与安天联系。

手动上传

手动上传允许用户将单个本地文件上传至追影。请按照以下步骤手动上传文件至追影：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在一级导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 点击导航栏右侧的“个人历史”或者“admin@local > 个人历史”，进入上传页面。
4. 在手动上传部分，点击“选择文件”按钮，选择需要上传的文件，点击“打开”。
5. 点击“上传”按钮。上传结束，系统弹出“文件上传”对话框，显示文件的初步鉴定信息。点击右上角的关闭按钮关闭对话框。

用户可在页面下方的上传历史部分查看文件的详细分析报告。

查看上传历史记录

手动上传文件到追影后，上传记录即会显示在个人历史页面下方的列表中。上传历史表格各列含义如

下：

列表项	说明
上传时间	显示文件上传到追影的时间。
MD5	显示文件对应的 MD5 值。点击 MD5 值可查阅相应文件的分析报告。
文件名	显示上传到追影的文件的名称。
结果	显示追影对文件执行鉴定分析后的结果，例如木马程序、间谍软件、可信程序、未见异常等。
分析报告	点击查看文件的分析报告。
指令	可对文件执行的指令，包括： ● 优先分析：另追影系统优先分析相应的文件。 ● 强制动态：对相应的文件强制执行动态检测。默认情况下，当文件在未经过动态检测即被判断为威胁文件时，系统为节省资源检测分析更高优先级文件，就不会再对其进行动态检测了，而指定强制动态后，相应的文件在此种情况下仍会经过动态检测。

表 3-1：上传历史表格含义

系统支持基于 MD5 值的搜索功能，帮助用户快速查找需要的文件。在列表右上角的搜索文本框中输入关键字，然后点击“搜索”按钮，MD5 值中含有指定关键字的文件将会显示在上传历史列表中。

URL 下载

URL 下载功能即追影通过用户指定的URL 下载文件进行分析鉴定。请按照以下步骤指定文件下载 URL：

1. 保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html。
2. 在一级导航栏点击“配置”，在“登录”对话框输入用户名密码，默认均为“admin”，点击“登录系统”进入系统配置相关页面（如已登录，请忽略）。
3. 点击页面右侧的“个人历史”或者“admin@local > 个人历史”，进入上传页面。
4. 在下载部分，输入文件 URL。如需输入多个 URL，点击回车键换行输入。
5. 点击“下载并检测”按钮。

用户可在页面下方的下载历史部分查看文件的详细分析报告。

查看下载历史记录

指定 URL 下载地址、执行下载并检测后，下载记录即会显示在个人历史页面下方的列表中（点击“下载历史”标签切换到下载历史列表）。下载历史表格各列含义如下：

列表项	说明
下载时间	显示被鉴定文件的下载时间。
最后状态更新	显示被鉴定文件最后一次状态变更的时间。
HASH	显示文件对应的哈希值。点击哈希值可查阅相应文件的分析报告。
文件名	显示被鉴定文件的名称。
检测状态	显示追影对下载文件的处理状态，例如已完成、下载失败等。
文件来源 URL	被下载鉴定文件的 URL。

表 3-2：下载历史表格含义

通过文件上报工具上报文件

安天提供文件上报工具方便用户将本地文件批量上传到追影进行鉴定。

如需使用文件上报工具，请与安天联系。

第 4 章 追影系统信息查询

介绍

追影系统在对文件进行深度、智能、持续性分析鉴定的同时，还具备强大的数据统计分析功能。通过追影的 Web 界面，用户可以轻松查看文件分析报告，也可迅速查询各类统计信息，从而获知文件鉴定情况、系统威胁状态、系统工作状态。

- 概要 :显示追影系统的基本统计信息 ,包括最新发现的威胁、系统分析次数及发现威胁次数统计、被鉴定文件类型分布统计以及文件传输协议类型统计。
- 统计：提供时间查询功能，用户可根据需要查看某天、某月、某年、某时间段的相关统计信息，包括系统分析次数以及发现威胁次数统计信息、被鉴定文件类型分布统计信息、文件传输协议类型统计信息以及威胁信息。
- 检索：提供检索功能，用户可根据需要查询指定文件的分析报告。分析报告详情说明请参阅第 5 章 文件分析报告。

概要

保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html 并回车，此时显示的即为追影系统的概要页面。概要页面通过表格、图表等方式显示系统最新发现的恶意文件以及系统的最主要统计信息。

- 最新恶意文件：显示系统最新鉴定出的 5 个恶意文件。

  点击文件对应的“报告”，可查看详细文件分析报告。分析报告详情说明请参阅第 5 章 文件分析报告。

图 4-1：概要页面——最新恶意文件列表

- 分析次数统计：通过柱状图显示追影的分析次数以及发现威胁的统计数据信息。

  点击柱状图上方的时间标签（“8 小时内”、“最近一周”、“最近 8 周”）查看不同时间段的统计信息；鼠标悬停在柱状图上，系统将显示详细信息。

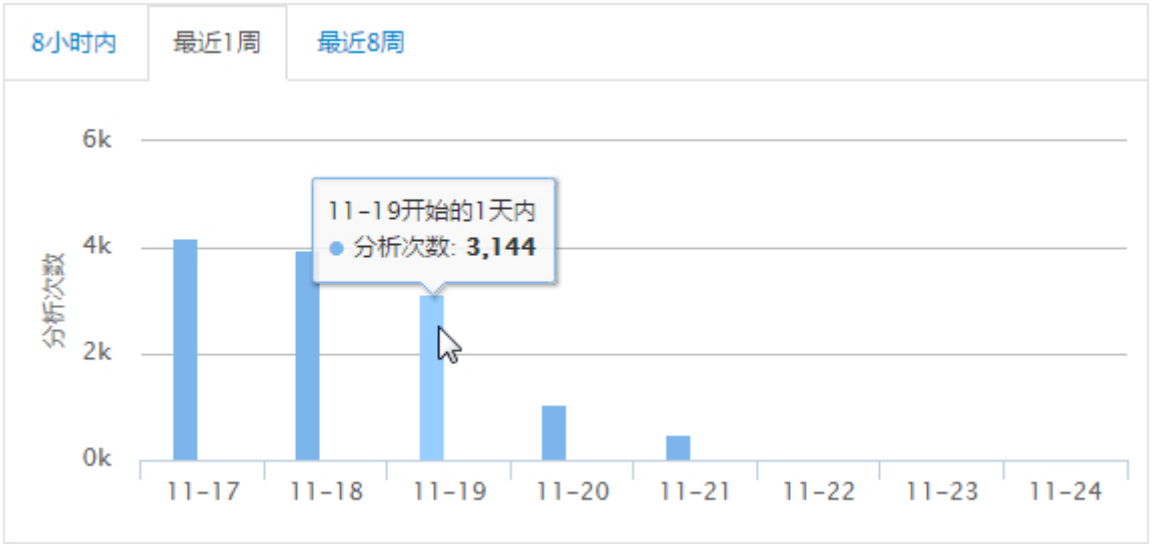

图 4-2：概要页面——分析次数柱状图

- 文件类型分布：通过柱状图显示被鉴定文件的文件类型分布统计数据信息。

  点击柱状图上方的时间标签（“8 小时内”、“最近一周”、“最近 8 周”）查看不同时间段的统计信息；鼠标悬停在柱状图上，系统将显示详细信息。

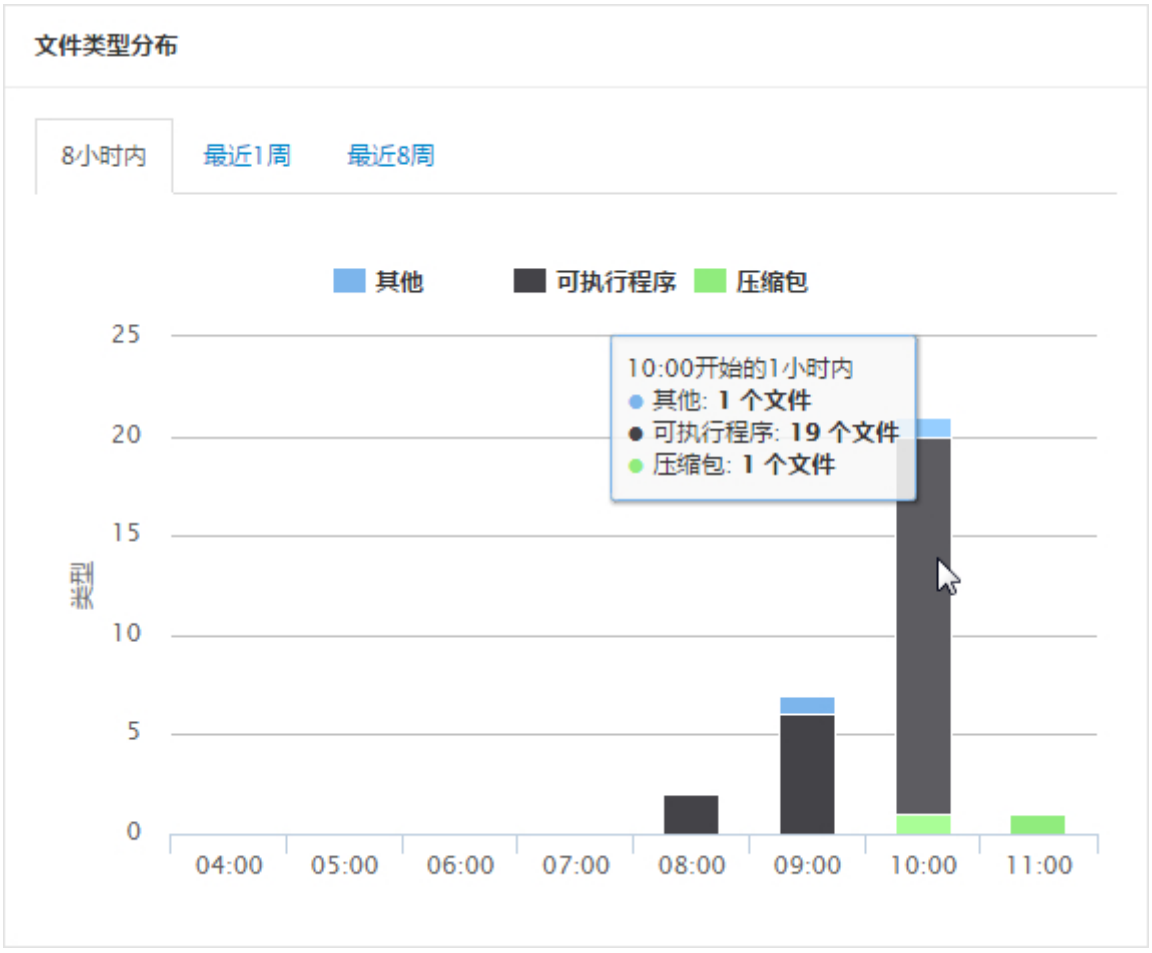

图 4-3：概要页面——文件类型分布柱状图

- 协议类型分布：当追影与安天网络病毒监控系统（VDS）联动时，系统通过该柱状图显示被鉴定文件的传输协议统计信息。

  点击柱状图上方的时间标签（“8 小时内”、“最近一周”、“最近 8 周”）查看不同时间段的统计信息；鼠标悬停在柱状图上，系统将显示详细信息。

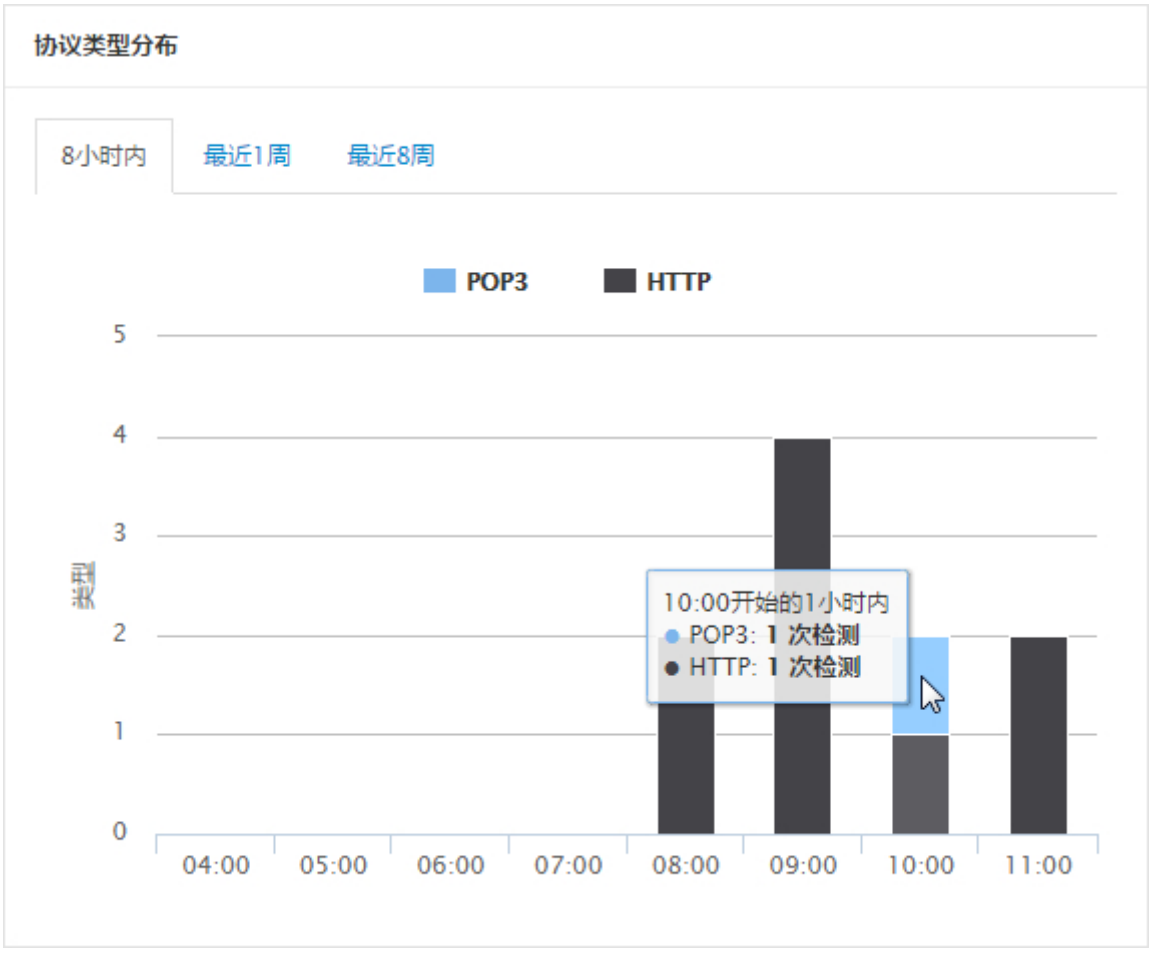

图 4-4：概要页面——协议类型分布柱状图

统计

保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html 并回车，点击“统计”进入统计页面。

统计页面通过图表、表格等方式显示分析次数统计信息、文件类型分布统计信息、协议类型分布统计信息以及具体的威胁信息，并提供基于日期的查询功能，用户可根据需要查看某天、某月、某年、某时间段的相关统计信息。

点击页面上方的 

，系统将会把当前指定时间的统计报告从系统中导出。

检索

保证追影网络连通后，在浏览器输入 http://*追影 IP 地址*/_lk/index.html 并回车，点击“检索”进入检索页面。

- 根据鉴定结果过滤：根据需要，选择列表左上角的“全部”、“恶意”、“安全”或者“未见异常”单选按钮，列表中将显示相应类型的文件。
- 根据 MD5 值进行搜索：在搜索文本框输入关键字，系统将查找 MD5 值与指定关键字相匹配的文件报告。
- 高级搜索：点击“高级”按钮，从弹出菜单中选择需要的关键字。

点击“分析”列的“基本信息”（未经过动态分析的文件）或者“分析报告”（已经过动态分析的文件），可查看相应文件的分析报告。关于报告的具体说明，请参阅第 5 章 文件分析报告。

第 5 章 文件分析报告

介绍

文件分析报告详细记录了被鉴定文件的各类鉴定信息。系统提供导出功能方便用户存储查阅文件分析报告。文件分析报告列出文件判定结果的具体鉴定依据，帮助用户充分了解被鉴定文件，从而做出正确判定。根据鉴定方式（静态或者动态）、所使用鉴定器的不同，报告中包含的内容不同。

文件分析报告内容说明

在“检索”页面的报告列表中点击“基本信息”或“分析报告”，系统即在新标签页显示相应的分析报告。分析报告的具体内容包括：

- 基本信息：告知文件鉴定结果、所用鉴定器，总结被鉴定文件的基本信息，包括文件名称、类型、大小、MD5 值等。
- 静态启发式检测：显示静态启发式检测的相关结果信息。
- 危险行为：提取文件在恶意代码传播、隐蔽、对抗、窃取、网络等方面的可疑危险行为，并确定行为危险等级。
- 其他行为：记录文件除危险行为外的其他行为的详细信息，为用户提供更为全面的鉴定依据。
- 文件操作：记录被鉴定文件的相关操作，包括文件的增加、删除、修改，并显示操作的具体文件路径。
- 进程监控：监控被鉴定文件运行时的相关系统进程，并以树状图形式展示进程间衍生关系。
- 动态截屏：追影会对文件在虚拟环境中运行时打开的窗口进行截屏，并在报告中进行展示。截屏功能可帮助用户直观了解文件的运行状态。
- 最近查询记录：显示联动设备（安天 VDS、安天私有云、第三方网络设备）最近一次向追影查询该文件是否安全的相关记录信息。

导出文件分析报告

系统提供文件分析报告导出功能，用户可将分析报告（HTML 文件或者 PDF 文件）从系统中导出并保存到本地。

导出文件分析报告，点击文件分析报告右上角的“导出 HTML”或者“导出 PDF”即可。

附录：名词解释

名词	解释
APT	Advanced Persistent Threat，即高级可持续性攻击。由组织、机构支撑的，通过各类攻击手段对某一特定目标执行持续性的有效攻击。
可执行文件	可移植可执行（PE）文件格式的文件，可以加载到内存中，并由操作系统加载程序执行。可执行文件可以是.exe 文件、.sys 文件、.com 文件等。
Shellcode	Shellcode 是攻击者发送到服务器的利用特定漏洞的代码，是溢出攻击程序的核心。
堆喷射	在漏洞利用中帮助实现任意代码执行的技术。
远程线程插入	通过在另一个进程中创建远程线程的方法进入目标进程的内存地址空间。
漏洞	漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，可以使攻击者在未授权的情况下访问或破坏系统。
0day 攻击	Zero-day attack，指利用系统或应用的未知漏洞（未被发现、无修补补丁）发起的攻击。攻击中被利用的未知漏洞称为 0day 漏洞。
反病毒引擎	一组通过接口调用、依托可维护的数据结构（规则库）对输入对象进行病毒检测处理的程序模块的统称。
MD5	消息摘要算法第五版（Message-Digest Algorithm 5），是当前计算机领域用于确保信息传输完整一致而广泛使用的摘要算法之一。
Hash	译为“散列”或“哈希”，就是把任意长度的输入（又叫做预映射），通过散列算法，变换成固定长度的输出，该输出就是散列值。

版本号：UG-01-1502-V1

服务热线：400-636-5241

公司网址：www.antiy.cn