

天空卫士™ 安全鳄® 统一内  
容安全**UCS** 技术文档中心  
管理员手册



# 内容

插图清单.....	ix
摘要.....	xi
版权声明.....	xii
序言 前言.....	xiii
<b>第 1 章 简介.....</b>	<b>15</b>
组件介绍.....	16
硬件介绍.....	17
命令行界面介绍.....	20
系统服务和授权.....	20
<b>第 2 章 必备知识.....</b>	<b>23</b>
安全策略.....	24
管理平台Web用户界面.....	25
标题栏.....	25
菜单栏.....	26
页面信息概述.....	28
浏览器和快速跳转按钮.....	28
设备管理页面.....	29
阻断页面.....	30
主页 ( 仪表板 ).....	30
数据防泄漏事件模板介绍.....	31
系统健康状态模板介绍.....	32
常用操作.....	32
查看系统健康状态.....	32
设置大屏实时监控.....	32
查看最近访问的报告.....	33
创建自定义列表报告.....	33
创建自定义图表报告.....	34
创建自定义趋势报告.....	34
创建定时任务报告.....	34
监控注册的设备.....	35
管理注册的设备.....	35
查看审计日志.....	36
查看系统日志.....	37
用户URL分类错误反馈.....	38
<b>第 3 章 管理平台.....</b>	<b>39</b>
基本设置.....	40
报告设置.....	40
存储设置.....	40
邮件服务器.....	41
系统通知.....	41

邮件告警.....	41
邮件释放.....	42
邮件审批.....	42
用户识别.....	46
SSL例外.....	47
授信地址.....	47
设置Syslog.....	47
设置SIEM.....	48
URL分类.....	48
URL分类更新.....	49
用户管理.....	50
用户目录.....	50
用户目录组.....	53
组织架构.....	53
用户凭证.....	54
分级对象.....	54
账户管理.....	55
管理员.....	55
角色.....	56
管理平台设备监控.....	57
管理平台设备管理.....	58
设备.....	58
网络.....	59
功能.....	60
其他.....	60
归档.....	62
归档DLP事件.....	62
归档ASWG日志.....	63
归档邮件日志.....	63
归档ITM报告.....	64
归档移动事件.....	64
终端安全管理.....	65
终端全局设置.....	65
终端配置.....	67
终端白名单.....	68
终端应用程序类别.....	68
终端设备.....	70
终端自定义协议.....	70
终端安装包.....	70
终端安全监控.....	71
监控终端事件.....	71
终端监控.....	76
<b>第 4 章 Web安全.....</b>	<b>79</b>
Web安全检测条件.....	80
URL分类.....	80
关键字.....	82
正则表达式.....	82
应用控制.....	83
文件类型.....	83
Header控制.....	84
Cloud App.....	85
安全URL分类.....	86

Web安全管理.....	86
Web安全策略.....	87
策略元素.....	93
规则元素.....	96
全局控制.....	98
设置.....	101
Web安全监控.....	104
用户行为统计.....	104
在线用户.....	110
实时日志.....	110
Web安全报告.....	111
用户行为报告.....	111
用户安全报告.....	115
创建定时任务报告.....	119
Web安全设备监控.....	120
Web安全设备管理.....	124
设备.....	124
网络.....	126
功能.....	127
认证.....	147
其他.....	151

## 第 5 章 数据安全.....155

数据安全检测条件.....	156
关键字.....	156
正则表达式.....	157
脚本.....	158
文件指纹.....	159
数据库指纹.....	159
字典.....	159
文件名称.....	160
文件类型.....	160
文件大小.....	161
附件数量.....	162
智能学习.....	162
ITM模板.....	162
文件属性.....	163
数据分类.....	163
标签.....	163
数据安全策略.....	164
数据安全策略.....	164
数据分类.....	181
策略元素.....	182
规则元素.....	189
标签管理.....	214
数据发现.....	215
邮件回溯.....	236
数据安全设置.....	237
数据安全监控.....	239
网络事件.....	239
发现事件.....	243
回溯事件.....	247
流量日志.....	250

数据安全报告.....	251
网络事件报告.....	252
发现事件报告.....	257
终端事件报告.....	263
创建定时任务报告.....	267
数据安全设备监控.....	267
数据安全设备管理.....	268
设备.....	268
网络.....	270
功能.....	271
其他.....	276
数据安全日志.....	279
流量日志.....	279
系统日志.....	279
审计日志.....	279
数据安全设备日志.....	279
<b>第 6 章 邮件安全.....</b>	<b>281</b>
邮件安全检测条件.....	282
反病毒.....	282
反垃圾.....	282
反欺诈.....	282
URL分类.....	282
安全URL分类.....	284
邮件安全管理.....	284
邮件安全策略.....	285
邮件策略元素.....	286
全局控制.....	289
PEM管理.....	290
设置.....	293
邮件安全监控.....	294
监控邮件日志.....	294
监控邮件连接日志.....	297
创建定时任务报告.....	298
邮件安全报告.....	298
综合邮件报告.....	299
入向邮件报告.....	302
出向邮件报告.....	306
连接日志报告.....	309
邮件安全设备监控.....	312
邮件安全设备管理.....	313
设备.....	313
网络.....	314
功能.....	316
认证.....	323
其他.....	324
<b>第 7 章 移动安全.....</b>	<b>329</b>
移动安全检测条件.....	330
应用.....	330
移动安全管理.....	330
移动安全策略.....	330

移动应用.....	331
移动客户端.....	331
移动安全设置.....	333
移动安全监控.....	334
移动邮件事件.....	334
应用管理事件.....	337
邮件安全移动端.....	338
设备安全移动端.....	339
移动流量统计.....	341
移动安全报告.....	344
移动邮件报告.....	344
应用管理报告.....	349
移动设备报告.....	350
移动流量报告.....	351
移动安全设备监控.....	354
移动安全设备管理.....	355
设备.....	355
网络.....	356
功能.....	358
认证.....	360
其他.....	361
<b>第 8 章 Hybrid云安全.....</b>	<b>365</b>
混合云Hybrid.....	366
配置云平台虚拟机.....	366
<b>第 9 章 GatorCloud云安全.....</b>	<b>369</b>
GatorCloud云安全.....	370
UCWI设备监控.....	371
UCWI监控.....	371
UCWI设备管理.....	371
设备.....	371
功能.....	373
其他.....	373
WebService API 调用指南.....	375
概述.....	376
WebService API快速配置指南.....	379
资源获取接口.....	381
内容审查接口.....	390
使用curl的示例.....	406
第三方志管理平台集成.....	408
<b>第 10 章 内部威胁防护.....</b>	<b>411</b>
ITM管理.....	412
查看预置ITM安全策略模板.....	412
预置ITM模板.....	412
ITM设置.....	412
启用专家模型.....	413
MRS任务.....	413
ITM例外.....	414
ITM报告设置.....	414

ITM异常设置.....	415
ITM报告.....	416
ITM风险用户报告.....	416
ITM 风险类型报告.....	417
ITM异常行为报告.....	417
<b>第 11 章 术语库.....</b>	<b>419</b>
索引.....	433



# 插图清单

图 1: Web用户界面.....	25
图 2: 标题栏.....	26
图 3: 菜单栏.....	27
图 4: 设备管理页面.....	29



# 摘要

---

文档的摘要信息。

## 关于本文档

天空卫士™提供技术文档中心以帮助安全管理员提供安装和使用 天空卫士™ 安全鳄® 统一内容安全UCS 解决方案系列产品，提供需要的帮助和参考信息。

## 版本声明

天空卫士帮助文档随 天空卫士™ 安全鳄® 统一内容安全UCS解决方案的软件版本3.3一同发布。

帮助文档中提供的帮助信息适用于软件版本3.3及其子版本。

## 文档语言

天空卫士™安全鳄®统一内容安全UCS解决方案帮助文档在3.3版本仅提供中文简体版本和英文版本。如需其他语言的技术文档，请联系您的客户顾问，向天空卫士™索取。

## 文档列表

截止3.3版本，天空卫士™提供以下技术文档：

天空卫士™安全鳄®统一内容安全UCS技术文档中心。

文档中心可以定制化拆分为以下手册：

- 天空卫士™安全鳄®统一内容安全UCS管理指南
- 天空卫士™安全鳄®统一内容安全UCS部署指南
- 天空卫士™安全鳄®统一内容安全UCS初始化手册
- 天空卫士™统一内容安全审查平台UCWIAPI手册

如需以上任意手册，请联系天空卫士™销售或客服顾问，向天空卫士™技术文档部门索取。

## 上下文关联的在线帮助

为了给您提供更优质的用户体验，天空卫士™将安全鳄®统一内容安全UCS技术文档中心嵌入统一内容安全管理服务器UCSS管理平台，并提供如下便捷的功能：

- 点击帮助 > 在线帮助打开当前版本的技术文档中心，并通过搜索和索引快速获取您所需要的帮助信息。
- 在管理平台的某一页面，点击帮助 > 解释此页直接跳转至关于此页面的帮助信息。

# 版权声明

---

文档中心的版权声明信息。

## 商标

- *SkyGuard*<sup>™</sup>和*SecGator*<sup>®</sup>标志是北京天空卫士信息安全技术有限公司在中国和其他国家/地区的注册商标或商标。
- 本文档提及的所有其他商标均是其各自拥有者的商标。

## 出版物

北京天空卫士信息安全技术有限公司对本出版物中可能出现的错误或遗漏不承担任何责任。北京天空卫士信息安全技术有限公司保留无需事先通知即可修改本出版物的权利。不论本手册中的任何信息是否涉及了任何现行或者将要发布的专利中的发明创造，均不能认为本手册包含侵犯版权或专利的任何许可或权利行为。

## 版权

© 2019 北京天空卫士信息安全技术有限公司保留所有权利。在中国出版。

本出版物中的信息如需修改，恕不另行通知。未经北京天空卫士信息安全技术有限公司同意，本出版物中的任何部分均不得以任何形式（照相，复印，缩微，静电复印，或者任何其他方法）重新出版或者传播，或者以任何目的收入到电子或机械信息收集系统中。

---

# 序言

---

## 前言

---

介绍文档中心的基本信息和技术支持信息。

### 技术支持

所有支持服务将会根据您的支持协议以及当时最新的企业技术支持政策进行交付。






有关支持产品和服务以及如何联系技术支持的信息，请访问我们的网站：[www.skyguard.com.cn](http://www.skyguard.com.cn)

### 技术文档版本

请确认您所拥有的技术文档为最新版本。我们提供的每篇技术文档均为其最新版本的副本。在参照手册进行操作前请务必确认版本信息。

### 注释标记

本手册中可能包含以下注释标记。

-  提示: 显示在章节和步骤中的便捷操作技巧。
-  注: 解释某种特殊状况，或展开介绍关于某一重点信息的相关知识。
-  重要: 指出关于某一章节，或某一步骤的至关重要的信息。
-  警告: 表示某一步骤或某一行为可能导致其他问题，比如数据丢失，安全隐患或性能下降。
-  警告: 表示某一步骤或某一行为可能导致严重问题，比如人员伤亡或设备损坏。



---

# 第 1 章

---

## 简介

---

内容:

- [组件介绍](#)
- [硬件介绍](#)
- [命令行界面介绍](#)
- [系统服务和授权](#)

介绍统一内容安全*UCS*解决方案的基本信息。

本文介绍了天空卫士™安全鳄®统一内容安全*UCS*解决方案的基本信息，包括平台介绍、组件介绍和硬件信息等。

统一内容安全*UCS*解决方案将Web，数据，邮件和智能移动设备安全技术解决方案有效整合为统一的内容安全解决方案，以提供全面的内容安全分析和内容安全管理功能。

## 组件介绍

介绍当前内容安全解决方案的系统组件。

当前内容安全解决方案包含以下组件：

- 安全鳄®统一内容安全管理服务器UCSS
- 安全鳄®增强型Web安全网关ASWG
- 安全鳄®数据安全网关DSG
- 安全鳄®统一内容安全终端UCSC
- 安全鳄®统一内容安全审查平台UCWI
- 安全鳄®内部威胁管理ITM
- 安全鳄®增强型安全邮件网关ASEG
- 安全鳄®移动安全网关MAG
- 天空卫士™安全鳄®统一内容安全UCS混合云Hybrid UCSG

### 增强型Web安全网关ASWG

天空卫士™安全鳄®增强型Web安全网关ASWG（以下简称ASWG）基于大数据和机器学习的动态分类技术，提供了URL分类查询功能；并采用了Web信誉评分技术，根据指定的敏感度级别来识别风险，并控制URL访问；ASWG集成的高级安全内容扫描引擎，采用了本地加云端实时查杀技术，实时应对最新的病毒、木马、网络威胁和未知威胁等。

ASWG集成了Web通道数据防泄DLP功能，采用ICAP、MTA等部署方式实现对Web、Email的数据防泄漏（DLP）检测，通过代理分析引擎截获和分析HTTP、HTTPS、FTP、SMTP(s)、POP3(s)、IMAP(s)、IM和自定义协议等通道的网络流量，在与ASWG分类策略、安全策略、DLP敏感内容策略进行匹配后，对用户访问请求进行监控、拦截、告警、时间限额、带宽管理等相应的动作，并将用户网络访问日志、数据泄漏事件和证据发送给UCSS。

### 数据安全网关DSG

天空卫士™安全鳄®数据安全网关DSG（以下简称UCSG-DSG），以集中策略为基础，对静态数据、传输数据及使用中的数据进行识别、监控和保护。其采用最先进的自然语言处理、指纹扫描、智能学习、图像识别等技术，对网络、终端、存储的数据进行全方位多层次的分析和保护，防止企业核心数据违反安全策略而泄漏。

UCSG-DSG采用旁路监控、网络串行、ICAP、MTA等部署方式，由分析引擎截获并分析来自HTTP、HTTPS、FTP、Email、ICAP、网络版IM消息和自定义协议的数据流量，在与安全策略进行匹配后，对数据流量进行监控、拦截等相应的动作，并将数据泄漏事件和证据发送至UCSS。

### 统一内容安全终端UCSC

天空卫士™安全鳄®统一内容安全终端UCSC（以下简称UCSC）安装于企业用户的终端，防止企业的核心数据资产因违反安全策略的规定而泄露。UCSC监控终端上的文件共享、邮件、Web、应用程序等传输的数据，在数据进行操作之前对打开、另存、复制、打印、拷贝、刻录、在线传输等操作进行管控，并根据安全策略执行相关的动作（如阻止、审计、提示、加密等），同时生成预警日志和审计日志。UCSC需注册至UCSS进行交互和管理，保护终端用户免遭数据窃取和泄漏。

### 统一内容安全审查平台UCWI

天空卫士™安全鳄®统一内容安全审查平台UCWI（以下简称UCWI）为客户的内部业务应用程序提供数据安全API。应用系统通过调用RESTful API，将需要检查的内容发送到UCWI，UCWI通过内置的DLP数据安全策略对内容进行分析，并向应用系统返回检测内容的安全等级，命中策略等信息，应用系统可以根据这些信息对检测内容执行存储、下载或者共享等操作。



### 内部威胁管理 *ITM*

天空卫士™安全鳄®内部威胁管理*ITM* (以下简称*ITM*) 采用最先进的统计学异常分析、双向循环神经网络、大数据分析、贝叶斯信念网络等技术对用户行为特征进行深度建模, 过异常用户行为检测 (ARS), 精准威胁行为回溯 (MRS)、专家系统 (ERS) 及其风险因子分值展现用户风险详情及风险趋势, 进一步发现内部风险行为和异常行为, 将用户风险评分结果与 UCS 统一内容安全系列产品的策略集成, 实现对风险用户进行智能化、实时监督和控制。

### 增强型安全邮件网关 *ASEG*

天空卫士™安全鳄®增强型安全邮件网关*ASEG* (以下简称*ASEG*) 通过SMTP协议接收和发送互联网邮件, 对邮件所包含的垃圾、病毒和恶链等攻击内容进行DLP策略检测并执行相应的策略动作, 为企业邮件的入向、出向和漫游三大用户场景提供全方位的安全保障。

### 移动安全网关 *MAG*

天空卫士™安全鳄®移动安全网关*MAG* (以下简称*MAG*) 拥有Mobile Email模块和Mobile App模块。Mobile Email模块对移动设备通过ActiveSync、POP3、IMAP等方式接收的企业电子邮件进行DLP检测并执行相应的审计或阻断等策略动作, 防止敏感内容被同步至移动设备而导致数据泄漏。Mobile App模块以终端安全域作为应用载体, 移动安全服务器为集中管理平台, Web安全代理为传输监控, 对移动应用执行统一的企业数据安全策略, 保证企业的应用程序和数据安全。

### 统一内容安全混合云

天空卫士™安全鳄®统一内容安全*UCS*混合云Hybrid UCSG (以下简称Hybrid UCSG) 以虚拟化的方式部署在云平台, 对混合云中的数据资产进行保护, 并通过安全分析引擎截获和分析来自HTTP、HTTPS、FTP、Email、自定义协议等网络通道的数据流量, 在与安全策略进行匹配后, 对数据流量执行监控和拦截等策略动作, 并且可以通过UCSS进行统一安全管理, 有效节约企业的设备、维护和管理成本。

Hybrid UCSG适合于拥有多个分支机构的企业, 而每个分支机构的网络出口不需要部署硬件设备的情况。拥有云平台有账户后就可以简单部署Hybrid UCSG, 只需要在各分支机构的出口路由器上通过GRE的方式将网络流量送至Hybrid UCSG即可实现数据保护。

### 统一内容安全管理服务器 *UCSS*

将Web、邮件、终端管理或数据泄漏防护技术的管理和报告功能整合到统一管理界面中, 提供了更出色的能见度、控制力和管理功能。无论针对何种解决方案模块 (例如Web、数据、终端或电子邮件安全) 和平台 (例如本地或云端), 统一内容安全管理服务器*UCSS*管理平台使您能够从一个基于Web的中央管理平台设置策略、管理事件、运行报告以及执行管理任务。

## 硬件介绍


介绍统一内容安全*UCS*的硬件参数。

### 硬件型号

当前天空卫士™安全鳄®统一内容安全*UCS*系列产品包含以下硬件型号：

产品型号	51000	11000	5100	1100
UCSS		●	●	●
UCSG-DSG	●	●	●	●
UCSG-ASWG	●	●	●	●
UCSG-ITM	●	●		

产品型号	51000	11000	5100	1100
UCSG-ASEG		•	•	•

 注：• 该设备代表可应用于该场景

### SecGator 51000 硬件规格



硬件参数	UCSG-DSG	ASWG	ITM
CPU	4*Intel Xeon E7	4*Intel Xeon E7	4*Intel Xeon E7
内存	128 GB	128 GB	128 GB
硬盘	2*600G SAS 2.5 寸 10,000rpm 磁盘	2*600G SAS 2.5 寸 10,000rpm 磁盘	2*600G SAS 2.5 寸 10,000rpm 磁盘 6*2T SATA 2.5 寸 7200rpm 磁盘
网卡	千兆管理口网口，万兆 Bypass 网口（根据实际情况选配）	千兆管理口网口，万兆 Bypass 网口（根据实际情况选配）	2*1,000/10,000 BaseT
电源	2*800 W 支持热插拔	2*800 W 支持热插拔	2*800 W 支持热插拔
尺寸	4 U 71.2*43.9*17.8 CM	4 U 71.2*43.9*17.8 CM	4 U 71.2*43.9*17.8 CM
应用场景	超大型企业	超大型企业	运营商级行为分析平台，超大型企业

### SecGator 11000 硬件规格



硬件参数	UCSS	UCSG-DSG	ASWG	ITM	ASEG
CPU	2*Intel Xeon E5	2*Intel Xeon E5	2*Intel Xeon E5	2*Intel Xeon E5	2*Intel Xeon E5
内存	64 GB	64 GB	64 GB	64 GB	64 GB

硬件参数	UCSS	UCSG-DSG	ASWG	ITM	ASEG
硬盘	2*600G SAS 2.5 寸 10,000rpm 磁盘 2*2T SATA 3.5 寸 7200rpm 磁盘	2*600G SAS 2.5 寸 10,000rpm 磁盘	2*600G SAS 2.5 寸 10,000rpm 磁盘	2*600G SAS 2.5 寸 10,000rpm 磁盘 2*2T SATA 3.5 寸 7200rpm 磁盘	2*600G SAS 2.5 寸 10,000rpm 磁盘 2*2T SATA 3.5 寸 7200rpm 磁盘
网卡	4*10/100/1,000 BaseT	4*10/100/1,000 BaseT 4*10/100/1,000 BaseT Bypass	4*10/100/1,000 BaseT 4*10/100/1,000 BaseT Bypass	4*10/100/1,000 BaseT	4*10/100/1,000 BaseT
电源	2*800 W 支持热插拔	2*800 W 支持热插拔	2*800 W 支持热插拔	2*800 W 支持热插拔	2*800 W 支持热插拔
尺寸	2 U 71.2*43.9*8.9 CM	2 U 71.2*43.9*8.9 CM	2 U 71.2*43.9*8.9 CM	2 U 71.2*43.9*8.9 CM	2 U 71.2*43.9*8.9 CM
应用场景	大型企业	大型企业	大型企业	大型企业	大型企业

### SecGator 5100 硬件规格



硬件参数	UCSS	UCSG-DSG	ASWG	ASEG
CPU	2*Intel Xeon E7	2*Intel Xeon E5	2*Intel Xeon E5	2*Intel Xeon E7
内存	32 GB	32 GB	32 GB	32 GB
硬盘	2*600 G SAS 2.5 寸 10,000 rpm disk 2*2 T SATA 3.5 寸 7,200 rpm disk	2*600 G SAS 2.5 寸 10,000 rpm disk	2*600 G SAS 2.5 寸 10,000 rpm disk	2*600 G SAS 2.5 寸 10,000 rpm disk 2*2 T SATA 3.5 寸 7,200 rpm disk
网卡	4*10/100/1,000 BaseT	4*10/100/1,000 BaseT 4*10/100/1,000 BaseT Bypass	4*10/100/1,000 BaseT 4*10/100/1,000 BaseT Bypass	4*10/100/1,000 BaseT
电源	2*650 W 支持热插拔	2*650 W 支持热插拔	2*650 W 支持热插拔	2*650 W 支持热插拔
尺寸	1 U 67.5*43*4.4 CM	1 U 67.5*43*4.4 CM	1 U 67.5*43*4.4 CM	1 U 67.5*43*4.4 CM

硬件参数	UCSS	UCSG-DSG	ASWG	ASEG
应用场景	中型企业	中型企业	中型企业	中型企业

### SecGator1100 硬件规格



硬件参数	UCSS	UCSG-DSG	ASWG	ASEG
CPU	4*Intel Xeon E7	Intel Xeon E3	Intel Xeon E3	4*Intel Xeon E7
内存	16 GB	16 GB	16 GB	16 GB
硬盘	4*1TB SATA 7200rpm 3.5 寸磁盘	2* 1TB SATA 7200rpm 3.5 寸磁盘	2* 1TB SATA 7200rpm 3.5 寸磁盘	4*1TB SATA 7200rpm 3.5 寸磁盘
网卡	2*10/100/1,000 BaseT	2*10/100/1,000 BaseT 2*10/100/1,000 BaseT Bypass	2*10/100/1,000 BaseT 2*10/100/1,000 BaseT Bypass	4*10/100/1,000 BaseT
电源	1*650 W 支持热插拔	1*650 W 支持热插拔	1*650 W 支持热插拔	1*650 W 支持热插拔
尺寸	1 U 67.5*43*4.4 CM	1 U 67.5*43*4.4 CM	1 U 67.5*43*4.4 CM	1 U 67.5*43*4.4 CM
应用场景	小型企业	小型企业	小型企业	小型企业

## 命令行界面介绍

命令行界面用于 天空卫士™ 内容安全一体机的调试与设备初始化。

天空卫士™ 命令行管理控制台是在初始阶段控制内容安全一体机的集中管理界面。

管理员可以在控制台中完成如下任务：

- 在设备初始化界面中完成内容安全一体机的初始化任务。
- 使用控制台的命令行界面对内容安全一体机进行设备调试。

**警告：**如非经验丰富的用户，请勿使用命令行管理控制台对内容安全一体机进行调试。天空卫士™ 建议您在执行任何通过控制台调试设备的操作前，先联系我们的技术支持人员，协助您完成需要的操作。

## 系统服务和授权

天空卫士™ 统一内容安全 UCS 解决方案包括以下模块的授权项，请联系您的天空卫士™ 销售顾问购买相应授权。

授权	界面菜单项
DLP	包括DLP报告、DLP监控、DLP管理等菜单项。
ASWG	包括ASWG报告、ASWG监控、ASWG管理等菜单项。
终端 DLP	包括终端管理、终端监控、终端事件、终端报告等菜单项。
Hybrid	包括Hybrid菜单项。
OCR	包括OCR菜单项。
网络打印	包括网络打印通道的相关信息。
Web-Service Inspector	包括云应用APP菜单项。
ITM	包括ITM管理、ITM报告等菜单项。
Mobile Email	包括邮件安全移动端、移动邮件事件等菜单项。
Mobile App	包括设备安全移动端、移动行为事件、Mobile管理等菜单项。
ASEG	包括邮件报告、邮件监控、SEG管理等菜单项。

### 统一内容安全 **UCS** 系统服务

为了保护您的各种内容安全无忧，天空卫士™统一内容安全UCS解决方案提供了多个系统服务和系统组件，包括：

- 透明用户标识*XID*：该服务负责将用户识别代理、用户登录代理获取的IP、用户/计算机的信息传递给安全引擎，进行策略匹配。
- 图像识别*OCR*：该服务负责识别图片上的文字内容并发送安全引擎进行分析和策略匹配。
- *ICAP*代理*ICAP Proxy*：该服务负责接收第三方代理的数据内容并做DLP检测。
- 指纹管理*FPDB*：该服务负责管理、同步和查询DLP指纹库和智能学习库。
- 安全策略引擎*SPE*：该服务负责DLP策略和数据发现策略的匹配、SWG内容安全扫描等。
- 协议分析*ATS*：该服务负责网络流量的抓取和协议类型分析，ASWG支持HTTP、HTTPS、FTP、SMTP、POP3和IMAP等。
- 邮件转发*MTA*：该服务负责邮件转发代理的邮件转发功能。
- 设备管理：该服务负责设备注册与管理。
- 操作系统：该服务负责为安全设备运行提供操作系统。
- 数据转发：该服务负责移动终端转发网络数据。
- 用户认证：该服务负责同步授权用户信息。
- 事件上传：该服务负责向UCSS管理控制台上传日志和证据文件。
- 移动管理：该服务负责与UCSS管理控制台进行周期性同步配置、策略及应用信息。



---

# 第 2 章

---

## 必备知识

---

内容:

- [安全策略](#)
- [管理平台Web用户界面](#)
- [主页 \( 仪表板 \)](#)
- [常用操作](#)

介绍统一内容安全*UCS* 解决方案的管理员操作指导信息。

本章详细介绍了安全管理员需要在天空卫士™安全鳄®统一内容安全*UCS*管理平台上从事的各种日常安全操作任务以及必备的操作知识。

## 安全策略

---

介绍什么是安全策略，以及策略相关的基本知识。

### 关于安全策略

安全策略即组织内部的安全策略，安全管理员可直接应用安全策略模板对违反策略的流量或敏感内容进行监控或拦截。

参照以下章节获取更多关于安全策略的介绍信息。

- [Web安全策略介绍](#)
- [数据安全策略介绍](#)
- [邮件安全策略介绍](#)
- [移动安全策略介绍](#)

### 预置策略

在完成设备的安装，部署，以及授权等操作后，预置安全策略开始监控组织内部的流量或文件。在系统初次启动尚未进行配置修改的情况下，预制策略默认允许所有请求。

### 自定义策略



安全管理员可以根据组织的安全需要编辑预置策略，或创建新的自定义策略，以监控和阻断组织内部的违规流量或敏感文件。

### 策略相关操作

进入管理平台页面后，点击任意安全解决方案管理菜单，进入策略页面，即可查看对应安全解决方案中所有的策略信息。

策略页面展现现有策略信息的完整列表，每条策略均显示其策略名称和策略描述，启用状态，适用用户，最近修改时间，策略等级以及策略创建者等信息。

策略页面支持以下安全策略相关操作：

- 添加一条新的安全策略：进入添加策略页面，或按照模板添加页面，并按照页面指示操作。
- 编辑现有安全策略：点击策略名称后面的  按钮，并按照页面指示操作。
- 删除一条现有安全策略：点击策略名称后面的  按钮，并按照页面指示操作。
- 如需批量删除现有安全策略，执行以下操作。
  1. 点击策略名称前面的复选框，选择需要删除的策略。
  2. 点击页面上方的删除按钮。

### 策略等级

策略等级是指策略执行的优先级。

策略等级包含以下属性：

- 系统支持30个策略等级，数值越小优先级越高。
- 一个策略只能属于一个策略等级，一个策略等级可以包含多个策略。
- 当优先级较高的策略被命中后，继续匹配同一级别的其他策略，不再接受优先级较低策略的检查。

例如，在Web安全方案中，当匹配相同等级的多个策略时，执行动作的优先顺序为：阻止（关键字>文件类型>URL）>计时>提示>放行。

- 系统支持三层分级对象，一层分级对象有权限设置的策略等级为1-30和默认等级；二层分级对象有权限设置的策略等级为11-30和默认等级；三层分级对象有权限设置的策略等级为21-30和默认等级。



## 策略规则匹配关系

在配置了多条策略规则的情况下，部分策略规则相互冲突，或互相重叠，其匹配关系如下：

- 支持同时匹配URL分类、文件类型、关键字、正则表达式、Header内容、CloudApp分类之间的同时满足的场景，比如对用户访问“成人分类”的网站时上传文档类型的行为进行检测
- 多个检测内容规则之间为“或”的关系，只要命中其中任何一个检测内容就算命中这个策略
- 每个检测规则中包含多个URL分类时，多个URL分类之间是“或”的关系，用户请求只要命中任何一个分类就算命中（例如多个关键字、多个Cloud App分类、多个文件类型、多个正则表达式、多个Header内容等和URL分类的处理方式相同）

## 管理平台Web用户界面

介绍Web用户界面（UI）。

天空卫士™ 统一内容安全UCS Web用户界面为您的天空卫士™ 统一内容安全管理服务器UCSS一体机设备集成了统一的管理操作平台。

Web用户界面包含以下部分：



图 1: Web用户界面

图例	组件
①	标题栏
②	菜单栏
③	页面内容

### 标题栏

介绍Web用户界面的标题栏。

天空卫士™ 统一内容安全UCS Web用户界面包含的标题栏集中显示了软件版本信息，当前登录的账户信息和帮助信息。

标题栏包含以下部分：

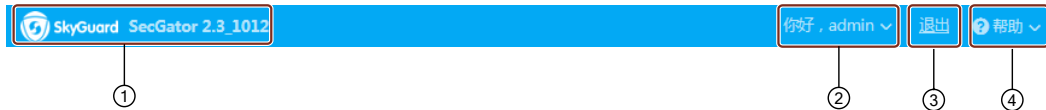



图 2: 标题栏

图例	组件
①	版本信息-查看当前统一内容安全管理服务器UCSS的版本信息。  注: 截图中的版本信息仅作为示意, 并非为最终发布的版本信息。
②	账户信息-点击向下的箭头, 您将可以管理以下账户设置 : <ul style="list-style-type: none"> <li>• 查看账户角色。</li> <li>• 查看账户邮箱。</li> <li>• 修改个人信息。</li> <li>• 修改密码。</li> </ul>
③	退出按钮
④	帮助菜单-点击向下的箭头, 可以获取以下帮助内容 : <ul style="list-style-type: none"> <li>• 返回初始化向导完成在页面初始化中遗漏的工作。</li> <li>• 打开帮助文档, 快速获取全套帮助信息文档。</li> <li>• 解释此页, 快速获取当前所在页面相关的帮助信息。</li> <li>• URL分类反馈, 将发现的风险URL或IP地址按照分类提交给天空卫士™, 以帮助我们提升URL分类的准确性。</li> <li>• 关于UCSS, 查看当前版本统一内容安全管理服务器UCSS管理平台的产品信息和天空卫士的联系方式。</li> </ul>

#### 个人信息和界面语言

在标题栏中点击修改个人信息即进入修改个人信息页面。

修改管理员个人信息、登录UCSS密码和界面显示语言。

将鼠标光标放置管理员账号处, 在显示的下拉框中选择修改个人信息或修改密码。

统一内容安全管理服务器UCSS管理平台支持两种界面语言: 中文和英文。选择主页 > 管理员账号 > 修改个人信息进行设置。

界面语言也可通过添加管理员时进行设置, 详细信息请参考[管理员](#)。如果管理员没有设置语言权限, 则只能使用初始化时设置的默认语言。

#### 菜单栏

介绍管理平台Web用户界面的菜单栏。

天空卫士™统一内容安全UCS管理平台Web用户界面包含的菜单栏集中显示了主页, 报告, 监控和各种设备管理等菜单, 以及接入大屏实时监控的按钮。

菜单栏具体包含以下部分:

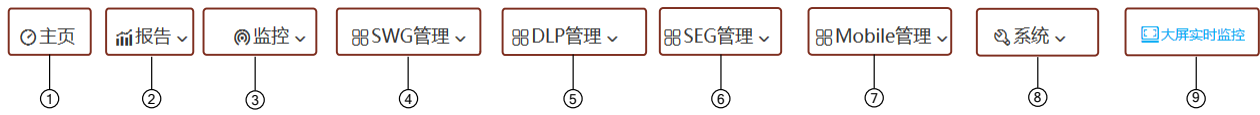


图 3: 菜单栏

图例	组件
①	<p>主页-查看11种仪表盘信息，默认包含：</p> <ul style="list-style-type: none"> <li>• 数据防泄漏事件</li> <li>• 系统健康状态</li> <li>• 网络事件               <ul style="list-style-type: none"> <li>• 排名前10的策略</li> <li>• 命中策略前10的来源</li> <li>• 排名前5的通道</li> <li>• 命中策略前10的目标</li> <li>• 安全级别事件趋势图</li> <li>• 策略事件趋势图</li> </ul> </li> <li>• 发现事件               <ul style="list-style-type: none"> <li>• 排名前10的数据发现策略</li> <li>• 排名前5的网络数据发现策略</li> </ul> </li> <li>• 移动事件-排名前10的策略</li> </ul>
②	<p>报告-以报告的形式直观的查看系统安全状态。 点击菜单栏中的报告按钮查看各子菜单选项的具体描述。</p>
③	<p>监控-实时监控系统安全事件。 点击菜单栏中的监控按钮查看各子菜单选项的具体描述。</p>
④	<p>SWG管理-管理Web安全设备增强型Web安全网关ASWG的各项设置。 点击菜单栏中的SWG管理按钮查看各子菜单选项的具体描述。  注：该菜单仅在产品授权包含Web安全模块时显示。</p>
⑤	<p>DLP管理-管理数据安全设备数据安全网关DSG的各项设置。 点击菜单栏中的DLP管理按钮查看各子菜单选项的具体描述。  注：该菜单仅在产品授权包含数据安全模块时显示。</p>
⑥	<p>SEG管理-管理邮件安全设备增强型安全邮件网关ASEG的各项设置。 点击菜单栏中的SEG管理按钮查看各子菜单选项的具体描述。  注：该菜单仅在产品授权包含邮件安全模块时显示。</p>
⑦	<p>Mobile管理-管理移动安全设备移动安全网关MAG的各项设置。 点击菜单栏中的Mobile管理按钮查看各子菜单选项的具体描述。  注：该菜单仅在产品授权包含移动安全模块时显示。</p>
⑧	<p>系统-管理UCSS系统的各项设置。</p>

图例	组件
	点击菜单栏中的系统按钮查看各子菜单选项的具体描述。
⑨	大屏实时监控-展示大屏幕实时监控到的事件仪表板。 在主页页面点击菜单栏中的大屏实时监控按钮按钮进入大数据管理分析平台页面。

## 页面信息概述

介绍管理平台Web用户界面的子页面概述页。

天空卫士™ 统一内容安全UCS 管理平台Web用户界面为每一个包含的子页面均提供了概述信息，以帮助企业安全管理员快速了解该页面的名称和主要用途。

以下是一个页面信息概述的例子，其中包含以下部分：



图例	组件
①	当前页面名称
②	当前页面包含的子页面的名称。点击可跳转至对应页面。
③	当前页面包含的子页面的描述信息。

如当前页面自动跳转为页面信息概述，则表示该页面包含若干子页面，请参照子页面的描述信息，确认您需要选择进入的页面，再进行进一步操作。

## 浏览器和快速跳转按钮

介绍Web用户界面的浏览路径和快速跳转按钮。

天空卫士™ 统一内容安全UCS Web用户界面在页面内容顶端提供了浏览器和快速跳转按钮。

### 浏览器

页面内容顶端的左边是浏览器。

浏览器显示当前页面的路径，点击浏览器中的蓝色文字可返回到上级页面。







浏览器示例如下：

监控 > SWG监控 > 用户行为统计

### 快速跳转按钮


页面内容顶端的右边是快速跳转按钮。

系统提供了以下快速跳转按钮：

按钮	介绍
	系统健康状态-点击此按钮进入主页 > 系统健康状态 页面查看系统健康状态。 提示：图表旁的数字为系统检测到的系统健康状态告警数。
	导出PDF-点击此按钮将报告和实时监控的数据导出为PDF文件。 注：在初始化中配置的公司名和LOGO将显示在导出的PDF文件中。
	导出Excel-点击此按钮将报告和实时监控的数据导出为Excel表格。按钮包含两个选项： <ul style="list-style-type: none"> <li>导出过滤列表-将所有未选中的项目导出至Excel表格。</li> <li>导出已选项-将所有已选中的项目导出至Excel表格。</li> </ul>
	主页设置-在主页点击此按钮进入主页 > 设置显示模板页面对主页的显示模板进行配置。
	刷新-点击此按钮刷新系统状态。
	返回-点击此按钮返回上一级菜单。


## 设备管理页面

介绍管理平台Web用户界面的设备管理页面。

天空卫士™ 统一内容安全UCS Web用户界面通过系统 > 设备管理列出了当前注册至统一内容安全管理服务器UCSS的各安全设备。通过点击该设备名称，或点击设备名称后的  按钮可以进入该设备的管理页面。

设备管理页面集中显示了设备的设备信息，网络配置信息，功能菜单，认证信息以及其他设备管理相关信息。

设备管理页面具体包含以下部分：



The screenshot displays the management interface for a SWG device. On the left, a sidebar (1) lists navigation options like '系统信息', '基本设置', and '网络'. The main content area (2) is divided into '系统信息' (System Info) and '设备信息' (Device Info). The '设备信息' section (3) provides details such as IP address, system version, and hardware specs. Below it, the '系统信息' section (4) shows the overall system status and a list of services like '透明用户标识服务' and '图像识别' with their operational states.

图 4: 设备管理页面

图例	组件
①	设备栏-当前选中的设备。

图例	组件
②	<p>菜单栏-集中显示设备管理的各个菜单选项。</p> <p>各菜单选项分别对应了设备的设备信息，网络配置信息，功能菜单，认证信息以及其他设备管理相关信息。点击菜单栏中的按钮查看各子菜单选项的具体描述。</p>
③	<p>重启服务栏-包含重启服务按钮和重启服务列表。</p> <ul style="list-style-type: none"> <li>• 重启服务按钮-当设备配置被修改，需要重启某项服务以应用该修改时，重启服务按钮自动闪烁，将鼠标移动至重启服务按钮即可查看有哪些等待重启的服务。</li> <li>• 重启服务列表-列表集中显示了被安全管理员在设备管理页面中的修改所影响的各项系统服务。</li> </ul>
④	<p>设备管理栏-包含具体的设备管理配置内容。</p> <p>点击菜单栏中的相应菜单选项，设备管理栏将显示该菜单对应的设备管理配置内容。</p>

## 阻断页面

介绍阻断页面及其相关知识。

当用户的上网请求命中企业安全策略时，且动作为阻断、提示时，用户将被跳转至阻断页面，用户的当前请求被中断。

或者在开启URL安全扫描时，若用户访问含有木马、钓鱼、网页篡改等威胁的URL，用户将被跳转至阻断页面。

阻断页面对阻止动作给出相应的原因说明。比如用户访问“风险类”的网站时，系统弹出告警页面，询问用户是否继续。

阻断页面类型有包含：

- 策略阻止：用户自定义的策略或者系统预置的策略，并且动作都是阻止的
- 全局黑名单阻止：用户的访问命中了全局黑名单
- 安全URL检测：用户访问的内容包含木马、钓鱼、网页篡改等安全风险
- 病毒检测：用户访问的网页包含病毒程序
- SSL事件：用户访问的目标站点证书验证不合法

阻断页面中的违规内容展示规则如下：

- 针对策略是默认检测所有时，如果动作为阻止，建议阻止类型为“URL阻止”，违规原因为：访问违规的URL分类；
- 对用户策略中明确设置了具体的类型，比如“文件类型”、“应用控制”、“关键字”、“Header控制”、“正则表达式”、“Cloud App 分类”、“URL 分类”，那么日志中阻止类型填写对应的一种即可，违规原因参看后面表格的“各阻断页面变量说明”中的变量说明；
- 如果命中多个阻止策略，以第一个匹配的策略原因展示违规原因；

## 主页（仪表板）

介绍主页相关信息和设置主页显示模板的步骤。

主页


天空卫士™安全鳄®统一内容安全UCS解决方案中的统一内容安全管理服务器UCSS管理平台作为该安全方案统一设备管理平台，在其Web用户界面中提供了主页，即仪表板视图，帮助安全管理员快速了解企业内部安全运营状况，快速定位安全威胁，并及时采取应对措施。


系统默认的主页面（仪表板页面）显示区包含了系统健康状态和十块数据模板显示区，直观地显示当前的系统状态、安全威胁状态和统计数据等信息。

### 设置主页显示模板


主页面（仪表板页面）允许按照安全管理员的需要进行设置。

按照以下步骤设置主页显示模板：

1. 点击  设置主页显示模板。
2. 点击更换模板，可查看可选模板。
3. 点击复选框，选择显示模板。
4. 确认所选模板后点击确定。
5. 为选中的模板设置以下参数。

 注：最多可同时添加10个模板至主页面。

- 展现数据的图表类型，包括：
  - 柱形图
  - 折线图
  - 饼状图
- 展现数据的时间范围，包括：
  - 今天
  - 最近3天
  - 最近7天
  - 最近30天
- 展现数据的排名范围，包括：
  - 排名前5
  - 排名前10

 提示：操作中注意以下事项：

- 对以上设置做出修改以后，样例中会显示该修改的预期样例。
- 系统预置四种安全级别：高、中、低和信息。
- 信息代表该数据是安全的。
- 图表根据模板类型统计安全级别对应的数据。

### 相关概念

[数据防泄漏事件模板介绍](#) on page 31

[系统健康状态模板介绍](#) on page 32

### 相关任务

[设置大屏实时监控](#) on page 32

介绍如何设置设置大屏实时监控。



## 数据防泄漏事件模板介绍

饼状图展示命中DLP策略的高、中、低、信息四类事件级别的分布情况，点击表示事件数量的蓝色数值可跳转至相应的DLP事件列表。

- **Web**：统计从HTTP、FTP通道接收的请求数量和命中的事件数量。
- **Email**：统计从SMTP通道接收的邮件数量和命中的事件数量。
- **数据发现**：统计网络数据发现和终端数据发现所扫描的文件数量和命中的事件数量。
- **终端**：统计当前所有通过终端通道命中的事件数量。

## 系统健康状态模板介绍

系统健康状态的显示信息有以下两种，点击信息会跳转至相关的配置页面：



	说明缺少某些基本配置项。
	说明某些系统配置出现异常，比如：资源利用率高、某些设置连接失败等。

**注册设备**：表示注册至UCSS进行统一管理的设备数量，点击数值可以跳转至设备列表页面。

**Web当天流量**：统计当前经由系统分析的Web流量。

**Email当天流量**：统计当前经由系统分析过的Email流量。

页面图标功能如下：

按钮	解释
	将过滤列表或所选信息导出为PDF文件。
	刷新当前页面信息。

## 常用操作

罗列安全管理员必备的操作。

本章为您的安全管理员介绍在天空卫士™管理平台上从事安全系统相关操作所需的常用知识。

### 查看系统健康状态



介绍查看系统健康状态的步骤。

系统健康状态实时监测并告警 UCSS 设备及 DSG 等功能模块的 CPU、内存、网卡、设备授权等问题或故障，以及监测系统的邮件服务器、告警等重要配置。

系统健康状态的显示信息有以下两种：

- 黄色字体提示信息：说明缺少某些基本配置项；
- 红色字体告警信息：说明某些系统配置出现异常，如资源利用率高、某些设置连接失败等。


告警信息后端的悬浮图标功能如下：

按钮	解释
	跳转到系统 > 设备管理页面，配置相应的设备信息排除告警。
	删除当前告警信息。

### 设置大屏实时监控

介绍如何设置设置大屏实时监控。



UCSS支持大屏实时监控功能，可以实时、动态的展示当前监控的系统状态、安全威胁状态和统计数据等信息。

 注：大屏实时监控要求显示设备的分辨率最小值为1920\*1080，以避免版式误差。

点击大屏实时监控进入大数据管理分析平台展示页面，用户可自定义大数据管理分析平台名称。

屏幕展示板块介绍如下：



- 世界地图位于大屏中间区域，采用点状图显示如下目标的地理位置：
    - 数据防泄漏DLP事件事件
    - 增强型Web安全网关ASWG事件日志
    - 增强型安全邮件网关ASEG事件日志
  - 世界地图显示如下内容：
    - 命中数据防泄漏DLP策略排名前5的来源
    - 命中增强型Web安全网关ASWG安全策略前5的目标
    - 命中增强型安全邮件网关ASEG安全策略前5的目标
  - 世界地图实时翻滚显示如下内容：
    - 当前有安全风险的数据防泄漏DLP事件（提取DLP事件最近的10条信息进行实时翻滚）
    - 当前有安全风险的增强型Web安全网关ASWG事件（提取ASWG安全事件最近的10条信息进行实时翻滚）
    - 当前有安全风险的增强型安全邮件网关ASEG事件（提取ASEG安全事件最近的10条信息进行实时翻滚）
1. 选择筛选时间（今天/3天/7天），筛选特定时间段的数据，默认时间段为今天。
  2. 点击设置显示模板。选中模板名称拖动到显示区即可替换当前模板。世界地图板块不可被其他模板替换。
  3. 设置数据刷新闻隔，默认为30秒。
  4. 保存设置。点击退出大屏实时监控，返回主页面。

## 查看最近访问的报告

介绍如何查看最近访问过的报告。


选择报告 > 最近访问报告，在列表里会显示最近访问过的报告，最近一次访问过的报告位于列表顶部。


## 创建自定义列表报告


介绍创建列表报告的步骤。

列表报告支持以列表的形式展示行为和事件等信息。

按照如下步骤添加新的列表报告。

1. 进入报告页面下的任意菜单。
  2. 点击列表选项卡。  
显示系统预置模板和自定义报告。
-  提示：系统预置模板在另存后可以编辑为您的自定义模板。
3. 点击添加报告，输入报告名称和描述，表明其作用。
  4. 点击添加筛选，增加相应筛选条件，筛选后的事件信息用于生成列表报告。
  5. 选择事件显示列内容（显示列选项与筛选信息相同），点击列信息显示蓝色即选中。
  6. 点击保存，新增报告显示在列表中。

 提示：列表报告有行间操作按钮，预置报告支持另存和新建**定时任务**，自定义报告支持编辑、另存、定时任务和删除操作。


 提示：点击调整显示列可以运用不同的报告筛选条件查看具体的数据。

7. 点击列表中的报告名称，即可进入列表报告。

## 创建自定义图表报告

介绍创建图表报告的步骤。

图表报告支持以图表的形式展示行为和事件的所占比例等信息。


1. 进入报告页面下的任意菜单。
2. 点击图表选项卡。  
显示系统预置模板和自定义报告。
  -  提示：系统预置模板在另存后可以编辑为您的自定义模板。
3. 点击添加报告，选择以下报告类型：
4. 输入报告名称、描述和排名显示数量（排名最多显示前30位）。
5. 点击添加筛选，增加相应筛选条件，筛选后的事件信息用于生成图表报告。
6. 保存配置，新增事件报告显示在列表中。
7. 点击报告名称，即可呈现图标报告图形化界面。

## 创建自定义趋势报告

介绍创建趋势报告的步骤。

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

按照如下步骤添加新的趋势报告。

1. 进入报告页面下的任意菜单。
2. 选择趋势选项卡。  
显示系统预置模板和自定义报告。
  -  提示：系统预置模板在另存后可以编辑为您的自定义模板。
3. 点击添加报告，选择所需的报告类型。
4. 输入报告名称、描述和排名显示数量（排名最多显示前30）。
5. 点击添加筛选，增加相应筛选条件，筛选后的事件信息用于生成报告。
6. 点击保存，新增事件报告显示在列表中。
7. 点击报告名称，即可呈现趋势报告图形化界面。


## 创建定时任务报告



定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

按照如下步骤创建定时任务报告。

1. 选择报告 > 定时任务报告，点击新建添加定时任务。
2. 填写定时任务名称和描述，说明任务用途。
3. 点击请选择选择要发送报告的类型、报告格式（EXCEL/PDF）和是否启用此定时任务（默认为启用）。
4. 设置邮件信息。填写邮件主题、发件人名称和发件人邮箱；并从用户目录或管理员选择收件人，也可自定义收件人邮箱。
5. 设置定时任务开启的时间、执行周期和结束时间
6. 保存设置，新增定时任务显示在列表中。

表 1: 页面图标和行间操作按钮功能

图标	功能
	编辑报告，预置报告模板不支持直接编辑。

图标	功能
	将报告另存到列表。另存预置报告模板后可编辑报告。
删除	批量删除所选报告。
	直接执行当前选中的任务
添加	新建定时任务报告。

## 监控注册的设备

介绍如何监控注册至管理平台的设备。

设备监控功能记录UCSS和已注册设备的运行状态如CPU、内存、网卡和硬盘等，以及服务运行状态，如安全分析引擎、图像识别、指纹提取和代理状态（仅ASWG设备）等。

选择监控 > 设备监控，点击列表中的设备查看设备监控信息。

设备监控支持快速搜索查询已注册设备，当注册设备过多时，可根据设备名称、类型、IP地址和版本等信息进行快速筛选和查询。

相关概念

[Web安全监控](#) on page 104

介绍Web安全监控相关信息。

[数据安全监控](#) on page 239

介绍数据安全监控相关信息。

[邮件安全监控](#) on page 294

介绍邮件安全监控相关信息

[终端安全监控](#) on page 71

[移动安全监控](#) on page 334

介绍如何监控您的移动安全设备。

[UCWI设备监控](#) on page 371

介绍如何监控统一内容安全审查平台UCWI安全设备。

## 管理注册的设备

介绍如何管理注册至管理平台的设备。

设备管理主要管理UCSS和注册于UCSS的设备的功能、配置等。目前支持的设备类型有：


- 统一内容安全管理服务器UCSS
- 数据安全网关DSG
- 增强型Web安全网关ASWG
- 增强型安全邮件网关ASEG
- 移动安全网关MAG
- 统一内容安全审查平台UCWI
- 统一内容安全管理服务器UCSS Lite
- Hybrid 数据安全网关DSG
- Hybrid 增强型Web安全网关ASWG
- Hybrid 统一内容安全管理服务器UCSS Lite

选择系统 > 设备管理，显示注册设备列表中的设备信息，包括：

- 设备名称
- 系统类型

- IP地址
- 版本
- CPU使用率
- 内存使用率
- 网卡及传输速率
- 负载状态
- 策略同步状态
- 设备启用状态
- 等

在设备管理页面，您可以通过快速搜索查询已注册设备。

 提示：当注册列表中设备较多时，可根据设备名称、类型、IP地址和版本等信息进行快速筛选和查询。

点击设备名称，或查看设备信息并管理设备。

相关概念

[Web安全设备管理](#) on page 124

管理注册于UCSS的Web安全设备。

[数据安全设备管理](#) on page 268

管理注册于UCSS的Web安全设备。

[邮件安全设备管理](#) on page 313

[移动安全设备管理](#) on page 355

管理注册于UCSS的移动安全设备。

[UCWI设备管理](#) on page 371

介绍统一内容安全审查平台UCWI云安全设备管理。

## 查看审计日志

介绍审计日志监控页面的相关信息。

简介

审计日志记录所有管理员的系统操作记录，包括登录、退出、策略管理、事件管理、系统管理和数据防泄漏DLP事件的管理操作等。

在监控 > 审计日志页面管理实时监控到的审计日志信息。

页面介绍

页面显示信息支持按以下信息筛选日志：

表 2: 审计日志筛选条件

筛选条件	解释
管理员	按照系统 > 帐户管理 > 管理员页面配置的管理员名称进行筛选。
登录IP	输入登陆IP进行筛选。
角色	按照系统 > 帐户管理 > 角色页面配置的角色名称进行筛选。
类型	输入操作的功能类型进行精确查询或模糊查询。
动作	选择动作名称进行筛选。
项目	输入操作的功能对象进行精确查询或模糊查询。

筛选条件	解释
所属组件	选择系统功能组件进行筛选。

监控页面包含以下快速按钮。

表 3: 快速按钮功能介绍

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

## 查看系统日志

介绍系统日志监控页面的相关信息。

### 简介

系统日志记录统一内容安全管理服务器UCSS自身以及UCSS管理平台的设备的系统运行信息等设备以及相关组件和服务的运行日志，如：设备启动、停止日志、服务运行日志、告警和资源使用等。

在监控 > 系统日志页面管理实时监控到的系统日志信息。

### 页面介绍

页面显示信息支持按以下信息筛选日志：

表 4: 系统日志筛选条件

筛选条件	解释
日期	选择系统日志创建的时间段进行筛选。
状态	选择系统日志状态（已读/未读）进行筛选。
类别	选择系统日志或配置更改日志进行筛选。
等级	选择系统日志等级由轻到重的等级（信息/告警/错误）进行筛选。
设备	选择添加的设备名称进行筛选。
组件	选择系统功能组件进行筛选。
详细信息	输入系统日志的内容进行精确查询或模糊查询。




监控页面包含以下快速按钮。

表 5: 快速按钮功能介绍

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

监控页面提供以下操作按钮和图标。将鼠标至于系统日志ID处，将出现图标。

表 6: 操作按钮和图标功能介绍

图标	图标	解释
标记为已读		选择系统日志后标记为已读。
标记为未读		选择系统日志后标记为未读。
删除		选择系统日志后删除。

## 用户URL分类错误反馈

介绍用户如何将URL分类错误反馈给天空卫士™。

天空卫士™提供的URL分类库涵盖的URL数量庞大，难免存在有分类不当的URL。因此，天空卫士™为企业安全管理员提供了可以反馈错误URL分类的方式，并且对处理的结果及时答复。

如发现不当分类，通过在帮助菜单中点击URL分类反馈，管理员可以直接向运维团队提交有问题的URL及URL分类。

用户需要提供如下信息：

- URL地址或IP地址：URL地址支持HTTPS与HTTP的协议区分，默认是HTTP
- 原始URL分类：表示用户预期的URL地址对应的URL分类，必选项。
- 期望URL分类：表示用户提交的URL对应的原始URL分类，可选项
- 备注：用户可以添加一些补充信息，可选项
- 反馈邮箱：用户的邮箱地址，可选项。天空卫士™运维平台处理完用户提交的URL分类后，会通过该邮件地址反馈处理的结果。

如果提交失败，系统将提示用户失败原因。

---

# 第 3 章

---

## 管理平台

---

内容:

- [基本设置](#)
- [用户管理](#)
- [账户管理](#)
- [管理平台设备监控](#)
- [管理平台设备管理](#)
- [归档](#)
- [终端安全管理](#)
- [终端安全监控](#)

介绍管理平台相关的设置信息。

统一内容安全管理服务器UCSS一体机设备是天空卫士™统一内容安全UCS解决方案的管理平台设备，为安全管理员提供了一个高度集成的管理操作平台。

本章介绍统一内容安全管理服务器UCSS管理平台设备本身相关的管理操作和系统相关的设置信息。

## 基本设置

系统相关基本设置。

介绍系统设置的相关信息。

## 报告设置

用户可通过UCSS统一设置通知邮件内容和PDF报告内容。

- 通知邮件设置

1. 选择系统 > 基本设置 > 报告设置，设置报告内容。
2. 设置每封通知邮件包含的附件的大小，范围为1~15MB（整个通知邮件文件大小为1~20MB），默认5M。当报告大小或邮件原文大小超过所设阈值时，不做为附件发送。
3. 勾选压缩报告文件选项，选择是否将报告文件压缩后通过邮件发送。
4. 点击保存，配置生效。

- 导出PDF设置

1. 设置如下导出事件数量、导出文件的自定义公司Logo、免责声明等，用于导出事件或报告：

DLP事件数量限制	设置每个PDF文件包含的DLP事件数量，范围为50~500。
邮件日志数量限制	设置每个PDF文件包含的邮件日志数量，范围为50~500。
LOGO	点击预置图片，上传公司LOGO图片，显示于报告中，默认LOGO为。文件大小不超过100KB，建议LOGO高度60px，宽度不限。
企业名称	输入公司名称，显示于报告首页，默认企业名称“天空卫士”，最大长度32个字符。
底部声明	输入公司版权声明，显示于报告底部，默认底部声明“Copyright@skyguard.cn,All rights reserved.”，最大长度255个字符。

2. 点击保存，报告设置生效。

## 存储设置

用户可通过UCSS统一设置证据文件/邮件的存储方式与存储位置。

1. 选择系统 > 基本设置 > 存储设置，设置存储。
2. 选择证据文件/邮件存储方式为集中存储或分布存储：

集中存储	证据文件集中存储在UCSS设备上，默认为集中存储。
分布存储	证据文件分布存储在UCSS、UCSG、UCSS-Lite等设备上，用于做数据泄露内容分析的设备存储证据文件。分布式存储时，邮件通知中无证据附件。

3. 设置证据文件/邮件的存储位置为本地设备或远程共享设备，如果选择远程共享，需做如下配置：

共享类型	选择共享服务器类型：SMB和NFS。
远程根目录	输入存储报告的服务器根目录。
文件夹路径	输入存储报告的文件夹路径。





用户信息	输入服务器的用户信息。支持三种方式的 用户信息验证： <ul style="list-style-type: none"> <li>匿名登陆</li> <li>用户凭证登陆</li> <li>新账号（需填写用户名称、密码或域名）。</li> </ul>
测试连接	设置完成后，点击测试连接，系统会尝试使用提供的信息检测与远程证据存储共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。

## 邮件服务器

UCSS预置邮箱服务器，用于发送策略通知邮件、告警信息邮件和DLP定时报告。管理员也可自定义邮件服务器作为发送邮件服务器。

1. 选择系统 > 基本设置 > 邮件服务器，点击添加，设置邮件服务器。
2. 输入邮件服务器名称和描述，表明其用途。
3. 输入服务器对应的主机名或IP，以及其对应的端口号，默认端口号25。
4. 选择是否启用邮件服务器身份认证。勾选后，必须使用用户身份验证（输入用户名和密码），才能和邮件服务器正常通信。
5. 验证与邮件服务器的连通性。点击 [测试邮件服务器](#)，弹出“测试邮件服务器”输入框，输入接收测试的邮箱地址，点击发送测试邮件。在邮件接收端能看到测试邮件。默认情况下，可与邮件服务器匿名连通，也可选择通过邮件服务器身份认证连通。
6. 点击保存，新建邮件服务器添加于列表中。

表 7: 页面图标和行间操作按钮功能

	编辑邮件服务器。
	删除邮件服务器。
删除	批量删除所选邮件服务器。


## 系统通知

统一内容安全管理服务器UCSS管理平台支持基于不同群组和告警类型设置告警通知模板。

在系统 > 系统通知页面设置告警通知模板。

按照以下步骤配置系统通知。


1. 点击启用状态滑动按钮，启用系统通知。
2. 输入系统通知发件人的名称。
3. 输入系统通知发件人的邮箱。
4. 选择邮件服务器。

 注：如不选择任何邮件服务器，系统将通过查询MX（邮件交换）记录进行投递。

## 邮件告警

UCSS在设备状态异常或License过期时，发送告警信息至邮件告警接收方，实时告知管理员系统运行状态，告警功能默认关闭。

1. 选择系统 > 基本设置 > 邮件告警，设置邮件告警。
2. 滑动状态条启用告警服务器，默认不启用。

3. 输入告警邮件的发件人名称，默认为DLP通知。
4. 输入发送告警的邮箱地址，默认发件人为 DLP-Alert@Notification.com。
5. 选择邮件服务器投递邮件。如果没有选择邮件服务器，系统将通过查询MX（邮件交换）记录进行投递。
6. 点击  从用户目录或管理员列表选择收件人。也支持自定义收件人，输入接收告警邮件的收件人邮箱地址，支持多个收件人。
7. 勾选触发告警邮件的发送条件，支持多选。
8. 2. 点击保存，邮件告警设置生效。

## 邮件释放

邮件释放页面的页面信息介绍。

当邮件触发策略被系统隔离后，管理员可以通过UCSS管理页面或邮件审核功能释放被隔离的邮件。且系统支持通过发送邮件方式对数据防泄漏DLP隔离的邮件事件进行释放或拒绝等邮件审批操作。

选择系统 > 基本设置 > 邮件释放，设置邮件释放。

### 释放设置

邮件释放支持以下释放设置。

选项	说明
反弹邮件	被释放的邮件会发给检测到该邮件的网关，由网关完成邮件投递。
指定邮件网关	被释放的邮件会发给指定的网关进行邮件投递。输入网关主机名/IP和端口号，点击测试连接，系统将给出指定网关连通成功或者失败的提示信息。

### 邮件审核接收设置

邮件审批人员处于企业外部时很难通过页面邮件 workflow 链接、或登录审批平台等方式拒绝或释放被隔离的邮件，为此天空卫士™提供了邮件审核功能，支持通过直接回复邮件邮件方式对DLP隔离邮件事件进行释放或拒绝等审批操作。

通过邮件隔离通知，审批人员可以点击同意释放，或拒绝释放，快速完成邮件审批操作。

邮件接收审核支持以下释放设置。

选项	说明
同意释放收件人	通知邮件回复结果为同意释放时，系统将发送邮件通知至该收件人，发送后对应的事件将被释放。
拒绝释放收件人	通知邮件回复结果为拒绝释放时，系统将发送邮件通知至该收件人，发送后对应的事件将被拒绝释放。

### 邮件释放通知

可选择释放邮件状态通知的接收人为释放者、源发送人、主管或审批员。

## 邮件审批

邮件审批用于设置多级审批流程，目前版本支持一级和二级审批。

邮件审批功能主要包括以下三部分：

- 审批架构设置
- 审批平台设置
- 审批平台操作

## 邮件审批及二级审批流程

介绍邮件审批和邮件审批流程的相关知识。

### 邮件审批

邮件审批支持多级审批，审批人员审批完成后可选择是否继续请上级进行审批，如果不继续，则邮件完成释放；如果继续，则需要等待上级完成审批后才完成邮件释放。

- 一级审批：违规用户触发策略后，策略通知直接通知到的一级审批员审批结果直接决定放行或拒绝。
- 二级审批：一级审批员审批放行后，该事件需要继续等待二级审批员的审批结果决定放行或拒绝。

### 邮件二级审批流程

一级审批流程：

- 一级审批员放行，则从待审批队列消失，计入审批历史，邮件被放行，发送通知给违规用户，记录UCSS事件历史
- 一级审批员拒绝，则从待审批队列消失，计入审批历史，邮件被拒绝，发送通知给违规用户，记录UCSS事件历史
- 以上审批支持添加备注，用于审批员表明审批原因

二级审批流程：

- 一级审批员放行，则从待审批队列消失，计入审批历史，进入二级审批员待审批队列，发送通知给违规用户，记录UCSS事件。



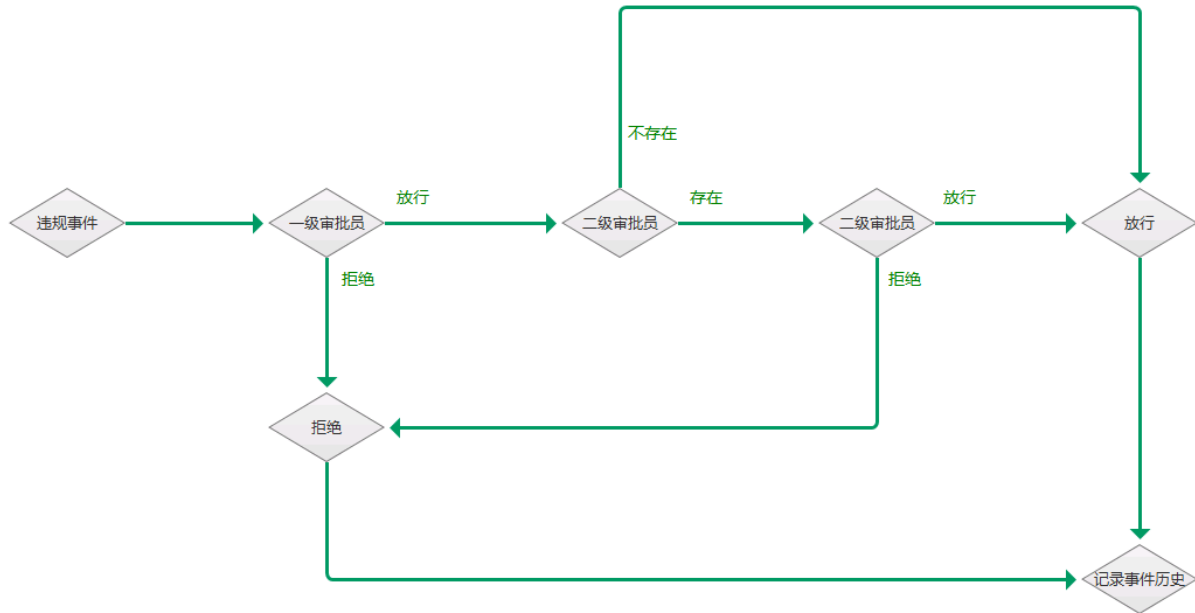
注：

- 支持选择指定二级审批人员，可选范围来自审批架构，至少选择一个。
- 如果审批架构设置为用户目录主管方式，则不支持选择二级审批员。
- 一级审批员拒绝，则从待审批队列消失，计入审批历史，不会进入二级审批员待审批队列，发送通知给违规用户，记录UCSS事件。
- 二级审批员放行，则从待审批队列消失，计入审批历史，邮件被放行，发送通知给一级审批员和违规用户，记录UCSS事件。
- 二级审批员拒绝，则从待审批队列消失，计入审批历史，邮件被拒绝，发送通知给一级审批员和违规用户，记录UCSS事件。



注：以上审批支持添加备注，用于审批员表明审批原因。

邮件审批流程如以下示意图所示。






## 审批架构

介绍设置审批架构的步骤。

## 设置步骤

邮件审批流程支持多级审批，可以通过以下两种方法来设置审批架构：

- 点击  按钮导入CSV文件进行自定义。
  -  注：自软件版本3.3起，CSV导入创建的审批架构可在页面上直接进行修改和删除等操作，无需在本地编辑后再次上传。
- 使用用户目录的架构。
  -  注：审批员按照邮箱地址识别，即每个审批员对应一个邮箱地址。

## 定期同步

审批架构可通过如下步骤与用户目录进行定期同步：

1. 勾选启用，开启定期同步功能。
2. 选择选择共享服务器类型，支持SMB和NFS。
3. 输入提供审批架构的服务器主机名/IP，以及存储文件的根目录。
4. 输入服务器的用户信息。

支持三种方式的用戶信息验证：

- 匿名登陆
  - 用戶凭証登陆
  - 新账号 ( 需填写用戶名称、密码或域名 )
5. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与远程证据存储共享服务器的连通性。
  6. 设置同步时间。
  7. 点击确定，保存并应用定期同步设置。

### 审批平台设置

介绍配置审批平台设置的步骤。

审批平台可通过UCSS统一管理启用、登录、审批员认证等设置。

1. 滑动状态条，开启审批平台功能。
2. 输入登录审批平台的主机名/IP和端口号。
3. 设置审批员认证架构：
  - a) 从下拉菜单中选择用户目录属性，支持Active Directory、LDAP、Lotus Domino、ADAM。
  - b) 从下拉菜单中选择服务器来源，支持新建和用戶目录。
    - 如果选择新建服务器，填写如下参数：

参数	解释
主机名/IP	输入新服务器的主机名或IP地址。
端口	输入新服务器的端口号。
用户名	输入登录新服务器的用户名。
密码	输入登录新服务器的密码。

- 如果选择用户目录，填写如下参数：

参数	解释
用户目录	选择用户目录类型。
主机名/IP	输入所选用户目录的主机名或IP地址。
端口	输入所选用户目录的端口号。

- c) 输入目录根节点。如果服务器来源选择的是用户目录，系统会自动读取此用户目录的根节点。
  - d) 选择是否使用SSL安全连接，SSL安全连接提高数据传输的安全性。
  - e) 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。
4. 设置审批通知属性。
 

邮件审批通知将由该发件人按照配置的发件人名称和邮箱地址向审批人发送，以便于审批人识别需要审批的邮件。
  5. 设置其他选项。
    - a) 勾选是否启用登陆认证。
 

邮件审批管理员在审批平台页面输入用户名密码后，系统将发送请求至用户目录进行认证。认证成功后，审批管理员方可完成登陆。
    - b) 勾选是否启用审批委派。

审批委派支持审批员可以根据自己实际需要在审批平台管理页面中，通过指定委派人邮箱的方式，将个人待审批队列中的待审批事件委派给其他人审批人进行代查看和管理操作。

6. 点击保存，审批平台设置完成。

### 审批平台操作

审批员通过接收的通知邮件登录审批平台进行邮件审批相关操作。

在监控 > **DLP**监控 > 网络事件页面，管理员在列表中选择命中策略的事件后，可点击通知发送事件信息到相应的主管或设定的收件人邮箱。

在通知邮件页面底部点击邮件审批，即可跳转至审批平台登录界面。

输入审批员的邮件地址和密码，点击登录，进入邮件审批平台页面，显示待审批和已审批选项卡。

#### 查看待审批的邮件列表

1. 选择待审批选项卡，显示事件ID、主题、发件人、收件人、邮件发送时间、审批流程等信息。

- 点击事件ID显示事件详情，包括事件属性详细信息、命中策略及详情和证据等。
- 点击审批流程下的详情按钮，显示审批记录，包括审批时间、审批员和审批状态等信息。
- 点击操作下的释放按钮可以放行邮件给二级审批员；或者点击拒绝按钮拒绝该邮件，并发送拒绝通知给违规用户。


#### 查看已审批的邮件列表

2. 选择已审批选项卡，显示事件ID、主题、发件人、收件人、邮件发送时间、审批动作、审批时间、审批流程等信息

- 点击事件ID显示事件详情，包括事件属性详细信息、命中策略及详情和证据等。
- 点击审批流程下的详情按钮，显示审批记录，包括审批时间、审批员和审批状态等信息。

## 用户识别

用户识别用于配置DC Agent、Logon Client等用户识别模块，查询获取用户IP地址和登录名的对应关系，将事件或日志来源IP关联到用户的登录名信息，并通过查询用户目录，关联到用户的显示名。有关用户目录的详细信息请参考[用户目录](#)。

 注：设备初始化时需安装用户代理识别服务器。

1. 选择系统 > 基本设置 > 用户识别，设置用户识别。
2. 设置用户识别代理。点击添加，输入用户识别代理服务器的名称、主机名/IP和端口号。点击删除，删除所选的用户识别代理。
3. 设置用户识别例外。设置不需要用户识别代理进行识别的来源IP地址或IP段。点击添加，输入IP或IP段。点击删除，删除所选的用户识别例外。

点击查看缓存用户查看用户识别代理已经识别并缓存于本地的用户IP和登录名对应关系。

用户识别缓存弹窗可查询以下信息：

- 用户（域名/登录名/主机名）
- 用户IP（登录IP）
- 服务器名称（用户登录的服务器名称）
- 服务器IP（用户登录服务器所在的IP地址）
- 服务器类型（登录代理/域控代理）
- 识别时间（系统识别到用户的时间）

点击管理安装包创建代理服务器安装包。详细信息请参考[终端安装包](#)。

## SSL例外

介绍SSL例外设置的相关信息。

系统对用户行为中匹配SSL例外的来源视为安全事件，不进行策略检测。










1. 选择系统 > 基本设置 > SSL例外，点击 ，添加来源和目标例外。
2. 点击来源选项卡，输入用户名称和IP/IP段，点击  添加于来源例外列表。
3. 点击目标选项卡，选择域名或IP例外：
  - 域名：输入域名，点击  添加于目标例外列表。
  - IP/IP段：输入用户名称和IP/IP段，点击  添加于目标例外列表。

表 8: 页面图标功能

	删除邮件服务器。
	清除列表中的所有来源或目标例外。
记录日志 	启动记录来源例外中IP的日志功能。
	导入CSV格式的SSL例外文件，可以参考模板生成导入文件。
	导出CSV格式的SSL例外文件到本地。

## 授信地址

介绍授信地址设置的相关信息。

授信地址即为可信任的地址，无需安全检测。只有授予权限的IP地址/IP段才有权限访问管理平台，默认授信IP为0.0.0.0~255.255.255.255，即允许任何IP进行登录。可通过授信IP页面或者CLI清除授信IP地址。




1. 选择系统 > 基本设置 > 授信地址，选择IP或IP段并输入可信任的地址，点击  添加于授信地址列表。
2. 点击保存，授信地址添加成功。

表 9: 页面图标和行间操作按钮功能

	编辑所选的IP或IP段。。
	删除所选来源或目标例外。

## 设置Syslog

介绍Syslog设置的相关信息。

UCSS使用Syslog服务器记录系统日志，管理员通过查看系统记录随时了解系统状况。

1. 选择系统 > 基本设置 > Syslog，设置Syslog。
2. 滑动状态条启用Syslog，默认不启用。
3. 输入Syslog服务器的IP地址和端口号（默认端口514）。
4. 选择Syslog模块，即日志发送格式。默认Syslog格式user-level messages。
5. 点击发送测试信息按钮，验证Syslog设置是否有效。
6. 选择是否设置自定义分隔符用于日志内容。

7. 选择是否发送空值到服务器。
8. 选择发送至Syslog服务器的内容：
  - 系统日志：勾选此项后，发送UCSS以及全部注册设备的系统日志至Syslog服务器。
  - DLP事件：勾选此项后，发送DLP事件信息至Syslog服务器。
  - ASWG代理日志：勾选此项后，发送ASWG代理日志至Syslog服务器。
  - 邮件日志：勾选此项后，发送UCSS以及全部注册设备的邮件日志至Syslog服务器。
  - 邮件连接日志：勾选此项后，发送UCSS以及全部注册设备的邮件连接日志至Syslog服务器。
  - 审计日志：勾选此项后，发送UCSS管理平台的审计日志至Syslog服务器。
9. 点击保存，Syslog设置生效。

## 设置SIEM

介绍SIEM设置的相关信息。

SIEM为网络、系统和应用产生的安全信息（包括日志、告警等）进行统一的实时监控、历史分析；对来自外部的入侵和内部的违规、误操作行为进行监控、审计分析、调查取证、出具各种报表报告。

1. 选择系统 > 基本设置 > SIEM，设置SIEM。
2. 滑动状态条启用SIEM，默认不启用。
3. 输入SIEM服务器的IP地址和端口号（默认端口514）。
4. 选择SIEM服务器的数据传输方式为UDP或TCP。
5. 点击发送测试信息验证SIEM设置是否有效。
6. 选择是否设置自定义分隔符用于日志内容。
7. 选择是否发送空值到服务器。
8. 选择发送至SIEM服务器的内容：

系统日志	勾选此项后，发送UCSS以及全部注册设备的系统日志至SIEM服务器。
DLP事件	勾选此项后，发送DLP事件信息至SIEM服务器。
ASWG代理日志	勾选此项后，发送ASWG代理日志至SIEM服务器。
邮件日志	勾选此项后，发送UCSS以及全部注册设备的邮件日志至SIEM服务器。
邮件连接日志	勾选此项后，发送UCSS以及全部注册设备的邮件连接日志至SIEM服务器。
审计日志	勾选此项后，发送UCSS管理平台的审计日志至SIEM服务器。

9. 点击保存，SIEM设置生效。

## URL分类

介绍设置URL分类的相关信息。




ASWG对海量的URL站点进行分类，方便管理员在用户策略中引用，从而有效的控制员工的Web访问。

系统预置常见的基本URL分类。管理员可以在预置分类或自定义分类中添加URL地址，自定义URL分类在策略匹配中优先于预置URL分类。UCSS可以根据名称、描述和类型，搜索URL分类。

1. 选择ASWG管理 > 策略元素 > URL分类，点击添加，配置如下参数，新建URL分类：






名称	填写URL分类名称，说明其用途。
----	------------------



描述	填写URL分类描述，详细说明其用途。
分类组	添加自定义分类或将URL添加到现有分类中。
URL地址	点击  ，输入URL地址，点击确定，添加到列表。支持HTTP和HTTPS协议，不支持通配符匹配。
正则表达式	<p>点击输入用于筛选URL地址的正则表达式，点击确定，添加到列表。</p> <p> 注： 正则表达式仅对URL地址进行正则匹配检测，不对网页内容进行匹配。</p>

2. 点击保存，新增URL分类添加到列表，点击所属分类组进行查看。

表 10: 页面图标和行间操作按钮功能

图标	解释
	编辑URL分类，可查看最后修改时间，创建者信息和URL分类使用情况。系统预置URL分类可以添加URL地址和正则表达式，不能修改名称和描述。修改预置策略后状态栏显示已修改。预置URL分类修改后类型变为预置（已修改）。
	删除自定义URL分类。系统预置URL分类不可以删除。
删除	批量删除所选URL分类。
	导入CSV格式的URL或正则表达式文件，可以参考模板生成导入文件。
	导出CSV格式的URL或正则表达式文件到本地。
	清空列表中的URL分类。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

### 安全扫描分类

安全扫描分类用于控制URL的安全访问。

安全扫描分类包含黑名单和白名单两种类型。黑名单中的URL分类因包含不安全内容被阻止用户访问，白名单中的URL分类是安全站点可直接放行。

选择SWG管理 > 策略元素 > URL分类，点击添加URL地址/正则表达式到黑名单或白名单。

## URL分类更新

介绍设置URL分类更新的相关信息。

UCSS支持自动和手动更新URL分类库，并将分类更新的结果录入系统日志。

 注：URL分类更新的状态在ASWG license有效期内显示激活或停用。

URL分类更新功能处于激活状态时，可显示如下信息并进行相关操作：

- 在URL分类更新区域显示URL分类更新库版本号，以及是否为最新。
  - 如页面显示有可用的新版本，可直接点击立即更新下载更新并应用。
  - 如页面显示当前版本已是最新，则无需更新。

- 在自动更新区域：
  - 勾选更新计划，设定更新时段和更新间隔，系统可以自动按照设定时间从SkyGuard官网进行最新版本的URL分类下载和更新。
  - 勾选代理服务器设置，设置代理服务器后，UCSS可以在内网环境下通过代理服务器下载和更新最新版本的URL分类库。

点击保存，启用URL分类库自动更新设置。






## 用户管理

管理用户相关信息。

### 用户目录

用户目录支持同步用户目录信息，可用于策略配置、报告过滤等功能操作时调用。目前支持的用户目录类型包括CSV、ADAM、Active Directory、Lotus Domino和Generic LDAP等。

表 11: 页面图标和行间操作按钮功能

	编辑用户目录。
	启用用户目录，启用状态一栏显示启用。
	禁用用户目录，启用状态一栏显示禁用。
	同步用户目录与服务器的信息，同步状态应显示为成功。
	删除用户目录。
调整优先级	调整用户目录优先级，系统会优先匹配优先级高的用户目录类型。
同步	批量同步用户目录与服务器信息，同步状态应显示为成功。
定期同步	设置定期同步用户目录的同步时间。定期同步功能默认禁用，启用后可根据天、周或月设置定期同步计划。
同步详情	显示同步服务器用户目录的详细信息。包括： <ul style="list-style-type: none"> <li>名称（通用名）</li> <li>服务器名称</li> <li>用户唯一识别名</li> <li>类型（包含用户、组、组织单元、计算机）</li> <li>登陆名</li> <li>邮箱</li> <li>主管</li> </ul> 并支持关键字搜索查询指定用户同步信息。

### Active Directory用户目录

- 选择系统 > 用户管理 > 用户目录 > 添加，点击添加，选择Active Directory，添加Active Directory用户目录。

2. 输入用户目录名称。
3. 选择启用或禁用该用户目录。
4. 连接用户目录，配置如下：

主机名/IP	输入Active Directory服务器的主机名或IP。
端口号	输入Active Directory服务器的端口号，默认为389。
用户名	输入登录Active Directory服务器的用户名。
密码	输入登录Active Directory服务器的密码。
目录根节点	输入服务器的目录根节点，读取用户目录信息。

5. 选择是否使用SSL加密连接到目录服务器，SSL安全连接提高数据传输的安全性。
6. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
7. 点击测试属性，输入某一用户的邮箱地址并选择用户属性（职位、部门、主管、移动电话、座机），可查询该用户的属性，验证连接成功。
8. 点击保存，新建用户目录显示于列表。

#### ADAM用户目录

1. 选择系统 > 用户管理 > 用户目录，点击添加，选择ADAM，添加ADAM用户目录。
2. 输入用户目录名称。
3. 选择启用或禁用该用户目录。
4. 连接用户目录，配置如下：

主机名/IP	输入ADAM服务器的主机名或IP。
端口号	输入ADAM服务器的端口号，默认为389。
用户名	输入登录ADAM服务器的用户名。
密码	输入登录ADAM服务器的密码。
目录根节点	输入服务器的目录根节点，读取用户目录信息。

5. 选择是否使用SSL加密连接到目录服务器，SSL安全连接提高数据传输的安全性。
6. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
7. 点击测试属性，输入某一用户的邮箱地址并选择用户属性（职位、部门、主管、移动电话、座机），可查询该用户的属性，验证连接成功。
8. 点击保存，新建用户目录显示于列表。

#### Generic LDAP用户目录

1. 选择系统 > 用户管理 > 用户目录，点击添加，选择Generic LDAP，添加Generic LDAP用户目录。
2. 输入用户目录名称。
3. 选择启用或禁用该用户目录。
4. 连接用户目录，配置如下：

LDAP主机名/IP	输入LDAP服务器的主机名。
端口号	输入LDAP服务器的端口号，默认为389。
用户名	输入登录LDAP服务器的用户名。

密码	输入登录LDAP服务器的密码。
目录根节点	输入服务器的目录根节点，读取用户目录信息。

5. 选择是否使用SSL加密连接到目录服务器，SSL安全连接提高数据传输的安全性。
6. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
7. 点击测试属性，输入某一用户的邮箱地址并选择用户属性（职位、部门、主管、移动电话、座机），可查询该用户的属性，验证连接成功。
8. 点击保存，新建用户目录显示于列表。

### Lotus Domino用户目录

1. 选择系统 > 用户管理 > 用户目录，点击添加，选择**Lotus Domino**，添加Lotus Domino用户目录。
2. 输入用户目录名称。
3. 选择启用或禁用该用户目录。
4. 连接用户目录，配置如下：

主机名/IP	输入Lotus Domino服务器的主机名或IP。
端口号	输入Lotus Domino服务器的端口号，默认为389。
用户名	输入登录Lotus Domino服务器的用户名。
密码	输入登录Lotus Domino服务器的密码。
目录根节点	输入服务器的目录根节点，读取用户目录信息。

5. 选择是否使用SSL加密连接到目录服务器，SSL安全连接提高数据传输的安全性。
6. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
7. 点击测试属性，输入某一用户的邮箱地址并选择用户属性（职位、部门、主管、移动电话、座机），可查询该用户的属性，验证连接成功。
8. 点击保存，新建用户目录显示于列表。

### CSV用户目录

1. 选择系统 > 用户管理 > 用户目录，点击添加，选择**CSV**，添加CSV用户目录。
2. 输入用户目录名称。
3. 选择启用或禁用该用户目录。
4. 连接用户目录，配置如下：

共享类型	选择共享服务器类型，支持Samba和NFS。
远程根目录	输入共享服务器的远程根目录，格式为IP/主机名\共享目录。
用户信息	如果选择Samba共享服务器，需输入用户登录信息，也可通过上传用户凭证登录。关于用户凭证的详细信息请参考 <a href="#">用户凭证</a> 。

5. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
6. 点击保存，新建用户目录显示于列表。

## 用户目录组

用户目录组将用户目录分组，重新定义组织内的用户目录结构，并可将自定义的用户目录组用于配置策略的来源目标、筛选、报告和例外等。



1. 选择系统 > 用户管理 > 用户目录组，点击添加，新建用户目录组。
2. 输入用户目录组名称和描述，表明其用途。
3. 输入该用户目录组的主管姓名，支持设置两名主管。
4. 从下拉框中，选择用户目录，点击  从该用户目录中选择用户，添加到同一用户目录组中。
5. 点击保存，新建用户目录组显示于列表。





表 12: 页面图标功能

图标	解释
	批量删除所选用户目录。被策略、来源目标、例外引用的用户目录组不能被删除。


## 组织架构

组织架构是轻量级的目录结构，在没有AD的情况下，用于管理公司的用户，部门和计算机，可在策略配置、报告过滤和ASWG认证时调用。

表 13: 页面图标功能


	编辑组织架构中的用户、部门或计算机。
移动	修改所选部门的层级。
	重置用户密码，ASWG设备本地认证时使用。
定期同步	设置定期同步组织架构的时间。定期同步功能默认禁用，启用后可配置远程服务器，并根据天、周或月设置定期同步计划，获取最新的AD文件，同步组织架构信息。
	导入CSV文件中的组织架构、用户或计算机。点击可下载CSV模板。
	导出全部或所选的组织架构信息。

### 部门

1. 选择系统 > 用户管理 > 组织架构，点击添加，选择组织架构类型为部门。
2. 输入部门名称。
3. 选择该部门隶属的上级部门。
4. 点击  从已有的用户目录中选择部门主管。添加用户目录的详细信息请参考[添加用户目录](#)。
5. 点击保存，新建部门显示于列表。

### 用户

1. 选择系统 > 用户管理 > 组织架构，点击添加，选择组织架构类型为用户。
2. 分别输入员工姓名、用户名和公司邮箱。

3. 选择员工所在部门，并输入IP地址和职称。
4. 点击  从已有的用户目录中选择部门主管。添加用户目录的详细信息请参考[添加用户目录](#)。
5. 输入员工电话。
6. 记录员工所在的AD域。
7. 点击图片区上传员工头像照片。
8. 点击保存，新建用户显示于列表。

#### 计算机




1. 选择系统 > 用户管理 > 组织架构，点击添加，选择组织架构类型为计算机。
2. 输入计算机名称。
3. 选择该计算机隶属的部门。
4. 输入计算机的主机名。
5. 输入计算机全域名(FQDN)，即主机名加上全路径。
6. 输入计算机的网络IP地址。
7. 输入对计算机的描述。
8. 点击保存，新建计算机显示于列表。

#### 用户凭证

用户凭证包含用户名、密码和域信息等预定义的登陆信息，可在配置指纹、数据发现、备份、归档、恢复等任务的共享目录时调用，可简化多次输入用户和密码的操作，同时防止密码等信息外泄。

1. 选择系统 > 用户管理 > 用户凭证，点击添加，新建用户凭证。
2. 输入该用户凭证的名称。
3. 输入该用户凭证的用户名。
4. 设置用户凭证密码并确认。
5. 输入Windows AD域名。
6. 输入与凭证相关的描述，说明凭证的用处。

表 14: 页面图标和行间图标功能

	编辑用户凭证信息。
	删除所选用户凭证。
	批量删除所选用户凭证。

#### 分级对象

分级对象应用于集团公司为分公司设置各自的管理员，根据分级管理原则分配管理员权限，界定每个角色所能管理的人员范围。每个分级对象可以管理多个用户目录、IP/IP段或者组织架构中的用户，组，组织单元，计算机、设备等。目前仅支持三级分级对象，不同的分级对象拥有不同的策略、事件和报告的设置和查看权限。

系统预置一个默认的分级对象，默认为所有对象，代表管理所有人员。如果不使用分级对象的功能，每个角色的默认分级对象即为系统预置所有对象的分级对象。

1. 选择系统 > 用户管理 > 分级对象，点击添加，新建分级对象。







2. 输入分级对象的名称和描述，说明分级对象的用处。
3. 选择该分级对象的上级，即父分级对象，只能有一个父分级对象。
4. 设置分级对象的管理范围。如果选择指定范围，可通过用户目录或者IP地址添加范围：
  - 通过用户目录添加范围：点击  添加用户，即该分级对象管理的用户；点击  删除所选的用户目录。
  - 通过IP地址添加范围：输入IP或IP段的数值，点击  添加到该分级对象
5. 添加管理设备。
  - a) 点击  弹出管理设备窗口，选择注册于UCSS的设备进行管理。
  - b) 点击  添加到有效区域。
  - c) 点击确认，设备添加成功。
6. 点击保存，新建分级对象的名称、上级分级对象、描述和创建者状态等信息显示于列表。

表 15: 页面图标功能

图标	功能
	批量删除所选分级对象。

## 账户管理

管理账户和管理员相关信息



### 管理员

管理员类型包括本地管理员和网络管理员。本地管理员在UCSS上创建，网络管理员可以通过AD创建。系统预置5种管理员角色类型，包含超级管理员、安全管理、事件管理员、审计管理员和日志管理员。

1. 选择系统 > 账户管理 > 管理员，点击添加，新建管理员。
2. 选择管理员类型为本地管理员或网络管理员。
  - 新建本地管理员
    - a. 输入管理员登陆账号和密码，并确认密码。
    - b. 设置密码有效天数。
    - c. 输入管理员的邮箱和电话。
    - d. 选择管理员的角色（超级管理员、安全管理、事件管理员、审计管理员和日志管理员）。添加角色请参考 [添加角色](#)。
    - e. 设置界面语言为中文或者英文。也可通过主页>管理员账号>修改个人信息修改界面语言。
    - f. 填写本地管理员的描述。
    - g. 根据需要勾选以下功能：

启用此账号	勾选后，启用本地管理员账号。
只有查看权限	勾选后，本地管理员账号登陆系统后只具有查看权限。
下一次登陆必须更改密码	勾选后，本地管理员下次登陆时需要修改密码。




- 新建网络管理员

- a. 点击  从AD中选择用户添加为网络用户。点击  删除所选用户。
- b. 选择管理员的角色。添加角色的详细信息请参考[添加角色](#)。
- c. 填写本地管理员的描述。
- d. 根据需要勾选以下功能：

启用此账号	勾选后，启用本地管理员账号。
只有查看权限	勾选后，本地管理员账号登陆系统后只具有查看权限。

3. 点击保存，新建管理员的信息显示于列表。

表 16: 页面图标和行间操作按钮

	查看管理员详情。
	删除所选的管理员。
	上级管理员可手动解锁锁定账号；被系统锁定的管理员帐号，将在24小时后自动解锁。

创建数据安全角色和管理员  
创建DLP的管理员和角色。


天空卫士UCSS的登录账号是按照角色和管理员来创建的，关于详细的角色和管理员信息，参考[账户管理](#) on page 55。不同的使用场景需要控制登录账号的权限在合理的范围内，以下步骤描述了如何给企业的数据安全管理员创建一个仅限于操作DLP相关设置的账号。

1. 在UCSS主页面，选择系统 > 账号管理 > 角色。
2. 在角色页面，点击添加按钮进入角色创建页面。
3. 填入角色名称和描述，例如：DLP管理。
4. 在角色权限区域，勾选DLP相关以及其他必需的选项，然后点击保存。到这一步，一个DLP管理角色创建成功，以下几步描述了基于这个角色，创建具体的DLP管理员账号。
5. 选择系统 > 账号管理 > 管理员。
6. 在管理员页面，点击添加按钮进入管理员创建页面。
7. 选择管理员类型、账号、密码、邮件等信息。
8. 在选择角色一行，在下拉菜单中选择刚刚创建的DLP管理角色。
9. 完成页面上其他必需的设置，点击保存。

## 角色

角色拥有系统各功能模块不同的访问和操作权限，管理员可使用角色进行权限管理。


UCSS支持五种预置管理员角色：超级管理员、系统管理员、安全管理员、事件管理员和审计管理员。点

击  悬浮图标，可以查看角色权限和该角色对应的帐户名称。

1. 选择系统 > 账户管理 > 角色，点击添加，新建角色。
2. 输入角色的名称和描述，说明其用途。
3. 勾选角色权限，进行权限管理。
4. 选择该角色管理的分级对象，可选择所有分级对象或某一分级对象。
5. 点击保存，新建角色的名称、描述、使用状态和创建者等信息显示于列表。



表 17: 页面图标和行间操作按钮

图标	解释
删除	批量删除所选角色。
	删除所选的角色。

## 管理平台设备监控

在监控 > 设备监控页面查看和管理UCSS管理平台设备的实时设备状态信息。


UCSS设备监控信息包括系统资源和服务状态，并支持三种数据统计时段（1小时/24小时/7天）。

表 18: UCSS系统资源信息

设备信息统计	解释
设备信息统计	统计当前设备的基本信息，如主机名称、IP地址、系统类型、CPU、物理内存、硬盘容量和网卡数量等。
CPU资源利用率	统计当前设备CPU使用率，包括用户占用、系统占用和空闲的CPU的比例。
网卡速率	统计当前网卡的发送和接收速率，以及总速率。
内存资源利用率	统计当前内存用于系统及应用、缓存的使用情况。
IO速率	设备输入接口和输出接口的读写速率。
硬盘资源使用情况	统计系统硬盘和数据硬盘的使用情况。
设备配置监控	设备配置监控包含邮件服务器和用户目录服务器，点击服务器类型可进入服务器配置页面。

表 19: UCSS服务状态信息

UCSS服务状态	解释
设备版本信息对比	当前UCSS作为基准设备，将注册设备各功能模块的版本信息与基准设备版本信息同步。可选同时同步或单独同步。
安全引擎负载统计	统计安全分析引擎CAE的负载状况。
分析请求数量统计	统计设备接收到的需要进行分析的请求数量。
命中事件统计	统计设备接收到的请求命中DLP策略产生事件的数量。
数据发现对象统计	统计数据发现任务扫描的对象数量。
数据发现事件统计	统计数据发现任务扫描的对象命中DLP数据发现策略产生事件的数量。
OCR引擎负载统计	统计OCR图像识别引擎的负载情况。
OCR队列状态统计	统计OCR图像识别引擎队列中等待分析和扫描超时的图片数量。
终端服务负载统计	统计终端服务的负载状态。
终端服务事件统计	统计终端服务的负载状态，包括接收事件数量和接收的数据流量。

 注：设备配置监控中的服务器也可通过系统页面进行配置，详细信息如下：

- 选择系统 > 基本设置 > 邮件服务器，可配置邮件服务器。
- 选择系统 > 用户管理 > 用户目录，可配置用户目录服务器。

## 管理平台设备管理

---

介绍如何管理您的统一内容安全管理服务器UCSS设备。

本章介绍如何执行统一内容安全管理服务器UCSS设备的功能、配置，以及设备、服务的启动、停止和重启等操作。

### 设备

配置设备相关的选项页面。

该菜单包含设备相关的选项页面。

#### 系统信息

介绍设备的系统信息界面。

系统信息包括设备的基本信息和服务状态信息。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 系统信息菜单。

系统信息页面支持查看以下信息。

#### 设备信息

设备信息包括主机名称，IP地址，系统类型等只读的信息。

在此栏中，可以一键重启或关闭设备。

#### 系统信息

系统信息包括系统负载状态和各种系统服务的运行状态。


参考[系统服务介绍](#)，可以获得各种系统服务的基本介绍。

在此栏中，可以选择对某项服务进行重启、停止或启动，或对所有服务进行批量操作。

### UCSS基本设置


介绍如何进行UCSS基本设置。

基本设置包括设备名称、时区和时间设置。只有统一内容安全管理服务器UCSS设备可设置时间及时区信息，其他注册设备自动从UCSS同步时间。

1. 点击系统 > 设备管理进入设备管理页面。
2. 将鼠标移至您的统一内容安全管理服务器UCSS设备，点击进入UCSS设备管理页面。
3. 点击进入设备选项卡中的基本设置菜单。
4. 配置主机名。
  - a) 输入设备名称
  - b) 输入设备描述，说明其用途以便于他人理解。
5. 配置时区设置。
  - a) 在下拉框中选择系统对应的时区。
  - b) 选择直接手动设置时间或自动从NTP服务器同步时间。

 注：如选择自动从NTP服务器同步时间，则需输入时间服务器域名。

6. 点击保存，配置生效。

 注：高级设置请务必在在天空卫士™技术支持工程师的指导下修改。

### 授权许可

介绍如何管理设备的授权许可设置。

在系统 > 设备管理页面进行设备授权许可。

1. 选择系统 > 设备管理进入设备管理页面。点击要查看的设备，进入设备 > 授权许可页面。
2. 选择以下授权方式：


项目	描述
授权码	在线授权需输入授权码。
授权文件	离线授权需上传授权文件。

授权成功后，在当前页面显示授权信息如下：

表 20: 当前授权状态

设备编号	显示当前设备编号
授权号	显示当前设备所使用的授权号。
用户名称	显示License授予时的用户名称，一般为企业名称。
工作模式	显示当前设备工作模式，支持阻断和审计。
授权类型	显示授权类型，包括正式版本和测试版本。
功能模块列表	显示授权的功能模块，每个功能模块的已授权数量，当前状态和使用的有效期。

3. 点击保存，设置生效。

 提示：点击下载设备ID可下载设备ID信息为记事本格式，查询和授权License时可以使用该文件。




## 网络


配置网络相关的选项页面。

该菜单包含网络相关的选项页面。

### UCSS网卡设置

网络设置主要包括网卡配置，UCSS的网卡包括Mgmt网卡负责管理设备（只能通过firstboot配置），另外的Mgmt1网卡未启用。

1. 选择系统 > 设备管理进入设备管理页面。
2. 选择网络 > 网卡配置进入网卡配置页面。
3. 点击  查看Mgmt网卡的配置信息。
4. 点击  配置并启用Mgmt1网卡，输入网卡的IP地址和子网掩码。并选择适配模式，即工作模式。
5. 点击确定，网卡设置完成。
6. 选择设备网卡并输入网卡的默认网关。
7. 输入DNS服务器IP，点击  添加于列表。

如需删除，点击  删除列表中所选的DNS服务器。

8. 点击保存，配置生效。

## 功能

配置功能相关的选项页面。

该菜单包含功能相关的选项页面。

### OCR功能

介绍管理OCR功能的步骤。

在系统 > 设备管理页面设置OCR功能。

OCR识别图像功能支持本地和外置OCR服务器，外置OCR服务器可以解析网络流量中的图片内容并进行DLP分析，提高了对大量图片内容的处理速率，减轻系统资源消耗。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > **OCR**页面。
2. 滑动状态条，开启OCR功能。
3. 选择OCR工作的精确度，平衡系统资源消耗：

快速	效率高但是精确度低。
平衡	兼顾效率和精确度。
精确	精确度高但是效率低。

4. 选择OCR识别的语言，包括简体中文、繁体中文和英文。
5. 设置OCR图像识别引擎检测文件的大小限制，0表示不限制大小。
6. 选择OCR服务器，包括本地OCR引擎和远程OCR引擎。
7. 点击保存，设置生效。

## 其他

其他的选项页面。

该菜单包含其他的选项页面。


### SNMP功能

介绍管理SNMP功能设置的步骤。

在系统 > 设备管理页面设置SNMP功能。

设备支持外部应用访问SNMP服务器来收集设备信息。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > **SNMP**页面，设置SNMP功能。。
2. 滑动状态条，开启SNMP功能。
3. 选择SNMP query版本，可以设置为v1或v2c。
4. 输入SNMP的团体名，即SNMP的用户名或密码，只允许使用此团体名访问SNMP服务器。
5. 选择以下SNMP的连接方式：

任何IP	任何IP地址都可访问SNMP。
仅限于下列IP	输入IP地址，点击  添加到可访问SNMP的IP列表。

6. 点击保存，设置生效。



### 收集日志

介绍配置收集日志功能的步骤。

在系统 > 设备管理页面设置收集日志功能。

设备支持收集系统日志信息，了解系统运行状态。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 收集日志页面，设置收集日志功能。
2. 选择收集日志的时间段。
3. 选择收集日志的类型。
4. 点击收集日志，收集所设定日期和指定类型的日志，显示于日志收集历史列表中。

点击  可将得收集得日志文件下载到本地；点击  可删除所选日志文件。

### 备份和恢复

介绍备份/恢复功能设置的步骤。

在系统 > 设备管理页面设置备份和恢复功能。

UCSS设备支持立即备份和立即恢复系统配置，包括配置信息、证据文件、邮件、网络及主机信息等，并支持定期备份功能。

1. 选择设备 > 其他 > 备份,进入备份或恢复页面。
2. 点击定期备份启动定期备份，设置定期备份的时间。
3. 点击备份设置，选择以下备份方式和备份内容：

备份至本地	选择备份至本地设备，设置备份日志数量的最大值，若本地保存数量大于设置的最大值则会删除最早的备份。
备份至远程	支持备份至Samba服务器和NFS服务器，需输入服务器的IP/主机名、文件夹路径和用户信息，并进行测试连接。

备份记录会出现在备份历史中，点击删除可删除所选备份。

4. 点击保存，设置生效。

### 升级和补丁

介绍升级/补丁功能设置的步骤。

在系统 > 设备管理页面设置升级和补丁功能。

设备支持在线版本升级和补丁安装，但升级不支持版本回退。选择系统 > 设备管理进入设备管理页面后。点击要查看的设备，进入设备 > 其他 > 升级/补丁页面，然后进行升级或补丁设置。

#### • 升级

选择升级选项卡，点击检查更新连接天空卫士的安装包服务器，获取安装包列表，选择安装包下载并安装。如果用户设备无法直接访问互联网，可通过代理服务器配置使用代理进行检查更新，点击代理服务器配置代理服务器。

点击上传安装包从本地上传升级安装包。

#### • 补丁

选择不定选项卡，查看当前版本和可用补丁。点击上传安装包从本地上传补丁安装包，安装之后可以选择卸载。

### 远程控制

介绍远程控制功能设置的步骤。

在系统 > 设备管理页面设置远程控制功能。

设备启用SSH连接后，可通过SSH执行远程设备故障排查。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 远程控制页面。

## 2. 选择是否启用以下功能：

启用远程控制	启用远程控制以后可以开启SSH端口并使用设备管理账号（例如ucssadmin帐号）登录设备进行命令操作。
启用技术支持模块	启用技术模块之后，获取6位密码。该密码需要提供给天空卫士进行解密后使用。
启用超时限制	设置在指定时间之后自动关闭远程控制。

## 3. 点击保存，设置生效。



注：

远程访问记录可在远程访问历史中查询。

## 系统工具

介绍系统工具设置的步骤。

在系统 &gt; 设备管理页面设置系统工具。

系统工具预置多条CLI命令，即使不连接后台时也可以使用系统工具进行故障排查，并显示执行结果。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，从下拉框中选择索要执行的命令。
2. 输入出现故障的设备主机名或IP，点击执行开始运行故障排查命令，点击停止可终止执行命令。执行结果显示于黑色屏幕中。

## 归档

---

### 归档DLP事件

1. 选择系统 > 归档,选择DLP事件选项卡，点击归档设置选择归档至本地或归档至远程。如果选择归档到远程服务器需做以下配置：

共享类型	选择远程服务器，支持SMB和NFS。
远程服务器	输入归档时访问共享服务器IP或主机名。
文件夹路径	输入归档文件可达目录。该文件夹必须真实存在，且具备可写权限。
用户信息	输入登录共享服务器用户名称、密码或域名。
测试连接	设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。

2. 点击保存，归档方式设置生效。



提示：归档周期默认为90天，从系统开始运行的时间记起。当列表中分区状态为只读时，说明分区可以进行归档。

表 21: 页面图标功能

立即归档	立即归档所选分区的DLP事件，状态栏变为已归档。
------	--------------------------

恢复	恢复所选分区的DLP事件到系统中，状态栏变为已恢复。
删除	批量删除所选归档事件。

## 归档ASWG日志




1. 选择系统 > 归档,选择ASWG 日志选项卡，点击归档设置选择归档至本地或归档至远程。如果选择归档到远程服务器需做以下配置：

共享类型	选择远程服务器，支持SMB和NFS。
远程服务器	输入归档时访问共享服务器IP或主机名。
文件夹路径	输入归档文件可达目录。该文件夹必须真实存在，且具备可写权限。
用户信息	输入登录共享服务器用户名称、密码或域名。
测试连接	设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。

2. 点击保存，归档方式设置生效。

归档周期默认为90天，从系统开始运行的时间记起。点击手工创建分区创建新分区记ASWG日志，分区名称默认为ASWG-创建时间-序号，起始时间为当前所处归档周期的开始时间，结束时间为手工创建分区时间。当列表中分区状态为只读时，说明分区可以进行归档。

表 22: 页面图标功能

	立即归档所选分区的ASWG日志，状态栏变为已归档。
	恢复所选分区的ASWG日志到系统中，状态栏变为已恢复。
	批量删除所选归档事件。

## 归档邮件日志




1. 选择系统 > 归档,选择邮件日志选项卡，点击归档设置选择归档至本地或归档至远程。如果选择归档到远程服务器需做以下配置：

共享类型	选择远程服务器，支持SMB和NFS。
远程服务器	输入归档时访问共享服务器IP或主机名。
文件夹路径	输入归档文件可达目录。该文件夹必须真实存在，且具备可写权限。
用户信息	输入登录共享服务器用户名称、密码或域名。
测试连接	设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。

2. 点击保存，归档方式设置生效。

归档周期默认为90天，从系统开始运行的时间记起。当列表中分区状态为只读时，表明分区可以进行归档。

表 23: 页面图标功能

	立即归档所选分区的邮件日志，状态栏变为已归档。
	恢复所选分区的邮件日志到系统中，状态栏变为已恢复。
	批量删除所选邮件日志。

## 归档ITM报告

- 选择系统 > 归档，选择ITM报告选项卡，点击归档设置选择归档至本地或归档至远程。如果选择归档到远程服务器需做以下配置：
  - 选择远程服务器，支持SMB和NFS。
  - 输入归档时访问共享服务器IP或主机名。
  - 输入归档文件可达目录。该文件夹必须真实存在，且具备可写权限。
  - 输入登录共享服务器用户名称、密码或域名。
  - 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
- 点击保存，归档方式设置生效。

归档周期默认为90天，从系统开始运行的时间记起。当列表中分区状态为只读时，表明分区可以进行归档。

表 24: 页面图标功能

立即归档	立即归档所选分区的ITM报告，状态栏变为已归档。
恢复	恢复所选分区的ITM报告到系统中，状态栏变为已恢复。
删除	批量删除所选ITM报告。

## 归档移动事件

归档移动事件，并以文件形式存储，便于了解移动设备的存储和使用情况。

- 选择系统 > 归档,选择移动事件选项卡，点击归档设置选择归档至本地或归档至远程。如果选择归档到远程服务器需做以下配置：

共享类型	选择远程服务器，支持SMB和NFS。
远程服务器	输入归档时访问共享服务器IP或主机名。
文件夹路径	输入归档文件可达目录。该文件夹必须真实存在，且具备可写权限。
用户信息	输入登录共享服务器用户名称、密码或域名。
测试连接	设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。



2. 点击保存，归档方式设置生效。

表 25: 页面图标功能

立即归档	立即归档所选分区的Moble日志，状态栏变为已归档。
恢复	恢复所选分区的Moble日志到系统中，状态栏变为已恢复。
删除	批量删除所选归档Moble日志。

## 终端安全管理

介绍终端安全管理的相关功能。

终端安全管理相关页面集中位于菜单栏的系统 > 终端管理选项下。

通过在这些页面上的操作，管理员可以：

- 管理全局设置
- 管理终端配置
- 管理终端应用程序类别
- 管理终端设备
- 管理终端协议
- 管理终端安装包

### 终端全局设置

终端全局设置的页面介绍。

全局设置管理所有注册终端的资源占用限制、卸载密码与终端服务器的通讯频率等。

在系统 > 终端管理 > 全局设置页面管理终端的全局设置。

#### 卸载密码

卸载密码用于计算机申请卸载终端时使用或在控制面板中选择卸载程序后输入卸载密码。


勾选启用卸载密码，填写卸载密码并确认，保存设置。

#### 连接频率

链接频率包括以下设置项。

字段	解释
策略同步频率	设置终端同步策略和配置文件的频率，范围为1~60分钟。
重试连接频率	设置连接终端服务器失败时重试连接终端服务器的频率，范围为1~60分钟。
判断断开时间	设置断开时限，终端服务器上的终端在设置时间内未做更新则认为终端与终端服务器断开，范围为5~60分。
判断清除时间	设置清除时限，终端服务器上的终端在设置的时间内未做更新则被自动删除列，0表示永不删除，范围为0~365天。

### 终端邮件保护域

输入内部邮件保护域，点击  添加到列表。

注意选择邮件方向为出向或者内部，出向邮件即检测发往保护域外部的邮件，内部邮件即检测保护域内部邮件。

### 终端资源占用

终端资源占用包括以下配置项。

字段	解释
CPU占用上限	限制终端运行资源的利用率，默认为20%，0表示不限制。
终端宽带传输	限制终端传输事件和证据文件时占用带宽，0表示不限制。

### 终端磁盘空间使用

为日志文件、事件存储和临时存储分配磁盘空间。

字段	解释
日志文件	限制终端运行时日志占用的空间大小。
事件存储	限制连接终端服务器失败时本地保存事件及证据文件大小。
临时存储	限制终端引擎进行分析时的临时文件存储空间大小。
隔离文件存储	限制终端隔离文件所占用的本地存储空间大小。
空间占用	显示用于日志文件、事件存储和临时存储的总空间。

### 终端刻录

设置是否允许终端刻录：

字段	解释
允许不在终端应用程序列表里的刻录应用	允许没有添加到应用程序列表里的刻录程序执行刻录。
禁用不在终端应用程序列表里的刻录应用	没有添加到应用程序列表里的刻录程序不能执行刻录。

### 双向SSL通信

设置是否阻断双向SSL通信。

字段	解释
阻断双向SSL通信	勾选后双向SSL通信直接阻断，例如：网银支付。

### 终端服务器

输入终端服务器的外网IP地址和主机名称，创建终端安装包时可以选用，保存设置。

## 语言模板

终端命中数据防泄漏DLP策略以后会有气泡提示和弹窗等信息，用户可以下载系统预置的中英文语言模板对以上提示信息进行自定义修改并上传使用。

点击默认模板下载预置模板，点击选择上传自定义语言模板。

## 终端配置

介绍设置终端配置的步骤。


终端配置用于管理针对指定计算机的终端运行状态、运行模式和终端服务器配置等。

1. 选择系统 > 终端管理 > 终端配置，进入终端配置页面。
2. 点击添加，新建终端配置，或直接编辑默认终端配置。
3. 输入终端配置名称和描述，说明该终端配置的作用。
4. 选择启用或禁用该终端配置。
5. 选择终端的工作模式：仅监控或阻断。
6. 选择以下终端运行模式：

模式	介绍
显性模式	在任务栏里可以看到终端图标和拦截弹泡。可选择允许申请禁用、显示拦截时的告警提示或显示扫描过程中的状态提示。
隐性模式	用户无法看到终端图标和任何拦截提示。

7. 选择启用以下终端功能：

功能	介绍
终端DLP	启用终端DLP数据防泄漏功能，保护终端的数据安全。
终端Web过滤	对用户的Web访问进行管理。
终端行为监控	选择终端行为的监控范围： <ul style="list-style-type: none"> <li>• 基础监控：监控系统日志、DLP日志、Web日志、第三方日志等信息进行ITM用户行为分析。</li> <li>• 高级监控：监控进程日志等信息进行ITM用户行为分析。</li> </ul>

8. 配置确认提示时长和超时后执行的动作（阻断/放行）。
9. 选择管理所有计算机或点击  选择已注册的计算机或对IP/IP段、用户所对应的计算机进行管理。
10. 选择终端在线或离线状态时需要禁用的功能。
11. 设置终端服务器优先级，优先级高的终端服务器会被优先连接。
12. 设置以下终端升级稳定版本，可以选择启用自动升级：


设置	介绍
升级服务器地址	当终端升级时，终端从指定的升级服务器下载安装程序。
最低稳定版本(Windows)	指定稳定版本，终端版本低于该版本号的终端将升级到该版本。
最低稳定版本(MAC)	指定稳定版本，终端版本低于该版本号的终端将升级到该版本。

启用自动升级后，系统在设定的时间检查终端版本，自动将低于最低稳定版本的终端升级至最低稳定版本。

13. 设置终端设备代理方式：

- 禁止终端修改浏览器手动代理配置：清空并禁用终端设备上浏览器的手动代理设置。
  - 设置终端浏览器自动配置脚本：指定终端设备上浏览器的自动代理配置使用自动配置脚本。
14. 选择自动或手动判断终端位置为公司内部或外部。  
如果选择手动，可通过DNS解析或内网解析的结果进行判断。
15. 点击保存，新建终端配置添加到列表中。

表 26: 页面图标和行间操作按钮功能

	编辑终端配置。
	删除终端配置。使用中的终端配置不可以删除。
调整优先级	调整终端配置优先级，可通过上下箭头调整优先级或者点击输入优先级数值。

## 终端白名单

介绍设置终端白名单的步骤。


天空卫士™终端安全解决方案允许安全管理员为保护用户隐私，对用户访问部分网站的通信数据以及软件或系统自动更新数据等无需监控的数据进行例外放行，不进行任何内容检测。

为了确保业务应用不受安全控制的影响，天空卫士™终端安全解决方案默认放行的网站包括：

- 部分银行网站
- 部分系统或软件升级网站
- 部分输入法网站
- 部分调用应用API的网站
- 部分上传错误日志的网站

### 添加自定义白名单

在系统 > 终端管理 > 终端白名单页面，安全管理员如需将自定义网址，域名或邮箱添加到终端白名单，按照以下步骤操作。

1. 点击  按钮，进入添加终端白名单对话框。
2. 输入易于识别的白名单名称。
3. 选择白名单类型。截止软件版本3.3，以支持的类型包括：
  - 来源IP、IP段
  - 目标IP、IP段
  - 目标域名
  - 发件人邮箱地址
  - 目标UNC路径：配置UNC目标路径白名单时，不要添加最前面的\\，也不要再在末尾添加\
  - 来源与目标组合
  - 应用程序路径
4. 输入上一步中所选类型对应的值。
5. 点击确认添加至白名单。
6. 点击保存按钮，保存新的白名单设置。

## 终端应用程序类别

终端需添加应用程序类别进行内容分析检测，在定义策略的来源/目标时可复用。

1. 选择系统 > 终端管理 > 终端应用程序类别。




2. 点击添加，新建终端应用程序类别。
3. 输入终端应用程序类别的名称和描述，说明其用途。
4. 点击，添加终端应用程序到该类别。详细信息请参考[添加终端应用程序](#)。
5. 点击保存，新建终端应用程序类别添加于列表中。

表 27: 页面图标和行间操作按钮功能


图标	功能
	编辑终端应用程序类别，可查看该终端应用程序包含的终端应用程序和使用的策略信息。
	删除终端应用程序类别。使用中的终端应用程序类别不可以删除。

## 终端应用程序


介绍终端应用程序的设置步骤。

按照以下步骤设置终端应用程序。

1. 选择系统 > 终端管理 > 终端应用程序类别。
2. 点击终端应用程序进入终端应用程序页面。
3. 点击添加进入添加终端应用程序页面。
4. 输入终端应用程序的名称，说明其用途，如：记事本。
5. 输入终端应用程序的进程名称，或点击选择，创建应用程序指纹，如notepad.exe。


 提示：在程序名称上传程序文件后，系统会自动生成程序指纹。


6. 输入该终端应用程序的版本和出品公司名称。
7. 选择是否信任该程序名称，即设置该应用程序的DLP操作控制。
  - 信任：勾选后，DLP不控制该程序。
  - 不信任：需要设置拷贝/剪切、粘贴、截屏、水印和文件访问的权限。可选择一下操作控制：
    - 允许：直接放行该应用程序。
    - 阻断：直接阻断该应用程序。
    - 内容分析/审计：命中策略后，不执行策略中的动作设置，均执行放行动作。
    - 内容分析/阻断：命中策略后，执行相应的策略动作设置。
    - 启用：打开该应用程序显示屏幕水印。
    - 禁用：打开该应用程序不显示屏幕水印。
    - 内容分析后水印：打开该应用程序，如果是敏感文件，则显示水印，否则不显示。

 注：如果选择不信任，可以勾选程序启动时不检测对某些目录文件的访问来设置文件访问白名单，设置成功后，在打开应用程序30秒内，不检测所设置的目录下的任何文件。

8. 输入支持的进程属性：
  - Networkbypass：进程不做网络通道的内容分析。
  - Block：阻止进程启动
9. 点击保存，将新建的终端应用程序成功添加至列表。

表 28: 页面图标和行间操作按钮功能

图标	功能
	编辑终端应用程序类别，可查看该终端应用程序包含的终端应用程序和使用的策略信息。


图标	功能
	删除终端应用程序类别。使用中的终端应用程序类别不可以删除。

## 终端设备

介绍终端设备的设置步骤。



终端添加打印机、USB、刻录机的设备名称后可对其进行内容分析检测，在定义策略的来源/目标时可复用。

1. 选择系统 > 终端管理 > 终端设备。
2. 点击添加，添加终端设备。
3. 输入终端设备的名称，说明其用途。

 注：可以定义设备的Device ID作为设备名称进行策略匹配，如同一厂商相同型号的U盘Device ID基本固定，由此避免用户通过修改U盘设备名称绕过DLP检测的情况。

4. 输入设备名称，该名称可以从设备属性里查看。在新建策略时可选该终端设备作为目标。
5. 输入终端设备描述，详细说明其用途。
6. 选择设备所属类型为打印、USB存储或刻录。
7. 点击保存，新建终端设备添加于列表中。

表 29: 页面图标和行间操作按钮功能

	编辑终端设备信息，可查看该终端应用程序包含的终端应用程序和使用的策略信息。
	删除终端设备信息。使用中的终端应用程序类别不可以删除。



## 终端自定义协议

介绍终端自定义协议的设置步骤。

DLP系统支持添加终端自定义协议，并检测该协议内容。

1. 选择系统 > 终端管理 > 终端自定义协议。
2. 点击添加，新建终端自定义协议。
3. 输入终端自定义协议的名称和描述，说明其用途。
4. 选择是否启用该终端自定义协议。
5. 输入适用该终端自定义协议的端口号。预置协议支持新增端口。
6. 点击保存，新建终端自定义协议添加于列表中。

表 30: 页面图标和行间操作按钮功能

	编辑终端自定义协议。
	删除终端自定义协议。使用中的终端自定义协议不可以删除。

## 终端安装包

介绍生成终端安装包的步骤。

终端安装包分别适配于Windows和MAC两种操作系统，用于部署主机时安装使用。

1. 选择系统 > 终端管理 > 终端安装包。
2. 点击上传安装包，选择相应的终端版本上传。

- 勾选安装包版本后，点击创建，选择已注册服务器或指定服务器，设置终端服务器，确认后自动创建安装包。
- 点击下载，比较MD5值，确认安装包文件完整。

## 终端安全监控

终端安全监控功能监控终端事件和所有已安装终端的计算机，同时管理注册的终端。

### 监控终端事件

介绍发现终端事件实时监控的相关信息。

终端事件监控功能记录所有终端通道流量命中数据防泄漏DLP策略的事件详情和证据文件信息。



默认显示检测时间为最近3天，状态为未忽略的所有事件。

在监控 > DLP监控 > 终端事件管理监控到的实时终端事件信息。

#### 页面介绍

实时监控页面包含以下快速按钮。

表 31: 快速按钮功能介绍

按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

实时监控页面包含以下操作按钮。

表 32: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>下载的文件为解密后的eml格式文件。</li> <li>支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>添加的备注信息可以在历史记录中进行查看。</li> <li>支持为事件批量添加备注信息。</li> </ul>

按钮	功能
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>• 选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>• 事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>• 支持事件的批量忽略和取消忽略。</li> </ul>



按钮	功能
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

#### 筛选条件/显示列

介绍数据安全报告的筛选条件/显示列。


下表罗列了数据安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
事件ID	事件识别号
流量UUID	流量通用唯一识别码
事件时间	事件发生的时间
检测时间	检测事件的时间
来源	用户名(用户识别模块)/IP地址/主机名/Email地址
目标	用户名(用户识别模块)/IP地址/URL地址/设备名(Endpoint USB/DVD/Printing)/Email地址
策略组	事件命中策略的组，支持多选。
策略名称	DLP策略名称
通道	事件所发生的通道（HTTP/HTTPS/FTP/IM/SMTP/自定义协议/网络打印/IMAP/POP3/"WebService应用/文件共享）。
动作	策略所对应的动作（放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放/水印）。
事件状态	五种事件状态（新/进行中/关闭/误报/提级）
安全级别	四种安全级别（高/中/低/信息）
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称

释放状态	事件是否被手动释放
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
事件标签	为事件添加的标签
忽略状态	事件状态为已忽略或未忽略
工作模式	支持仅监控/阻断
违规内容	事件详细的违规内容，如机密等
组	组织架构定义的组名
组织单元	组织架构定义的组织单元名
来源IP	来源IP地址
目标IP	目标IP地址
邮箱	组织架构中配置或同步AD的用户邮箱
主管	组织架构中配置或同步AD的主管信息
部门	组织架构定义的部门名称
URL分类	DLP策略定义的URL分类
国家	国家名称
城市	城市名称
位置	事件发生的位置
释放者	邮件的释放者
释放时间	释放邮件的时间
职位	组织架构定义的职位名称
发现任务	发现任务名称
主机名	生成发现/移动事件的主机名
IP地址	生成发现事件的IP地址
文件路径	触发发现事件的文件路径
文件夹路径	触发发现事件的文件夹路径
文件大小	触发发现事件的文件大小
文件所有者	触发发现事件的文件所有者
文件夹所有者	触发发现事件的文件夹所有者
文件扩展名	触发发现事件的文件扩展名
锁定状态	发现事件是否被锁定
发现类型	发现任务类型，包括文件共享、SharePoint、Lotus Domino、Exchange、Outlook PST终端、数据库、邮件、Exchange Online、Salesforce、Salesforce Online、OneDrive、SharePoint Online。
设备类型	终端设备类型
操作系统	终端的操作系统


终端位置	终端属于公司内部或外部
来源RiskLevel	事件来源的RiskLevel ( 较低、普通、严重、危险、高危 )
匹配总数	事件命中所有规则的匹配数量总和



查看终端事件详情

点击事件详情图标 ，显示事件属性、命中策略详情、证据和历史记录等信息。

- 事件属性详细信息

事件属性	解释
登录名	生成事件的终端设备名称\用户名。
IP地址	生成事件的终端IP地址。
主机名	生成事件的用户主机名称。
域名	生成事件的域名。
TRS分值	生成事件来源的总风险值。
方向	三种数据流向：入向/出向/内部。
应用名称	应用软件名称。
通道	检测网络数据的通道。
动作	违规后触发策略所执行的动作（放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放）。
事件状态	五种事件状态（新/进行中/关闭/误报/提级）。
最大匹配	触发策略规则项的最大匹配。如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
检测时间	引擎模块检测到违规事件触发策略的时间。
事件时间	管理平台收到违规事件的时间。
检测引擎	DLP检测数据的引擎模块。
分析引擎	后端分析数据的引擎ATS。
工作模式	DLP设备工作模式，支持仅监控/阻断。

 注：事件属性来源的显示优先级依次为：用户名、邮箱、IP/主机名和用户名。

 注：点击  显示个人用户风险报告，详细信息请参考查看个人用户风险报告。

- 命中策略及详情：显示该事件命中的策略名称和详细违规内容。策略配置请参考《第六章 DLP管理》DLP策略。
- 证据：包括事件来源（终端名称\用户名）和终端设备名称。






 注：若需显示证据信息，则要开启记录证据文件功能，具体操作请参考《第七章 DLP管理》DLP策略元素>添加策略动作，通过编辑策略开启此功能。

表 33: 证据页面图标功能

图标	解释
	全屏显示证据文件。
	预览事件包含的文件。
	下载事件包含的文件。
	返回到事件列表。

- 历史记录包括所有对该事件的操作信息，若该事件被删除，则不会记录而显示在审计日志中。详细信息请参考查看审计日志。



## 终端监控

介绍查看终端监控信息的步骤。

终端监控页面记录所有已安装终端的设备的运行状态及详细信息。

选择监控 > 终端监控，进入终端监控查看页面，显示当前已安装终端的设备列表。

列表提供如下丰富的页面操作按钮，便于管理员查询和管理：

- 添加筛选：筛选当前计算机的列表信息，显示主机名、登录帐号、运行模式、禁用状态等信息。
- 调整显示列：重新选择列表中显示的列信息。关于列信息的含义介绍，请参考[终端监控筛选条件/显示列](#)。点击恢复初始按钮 ，可恢复为系统默认列信息；勾选保存为默认配置选项，点击确定将当前所选的列信息保存为默认显示列。
- 详情：点击全域名（FQDN）的悬浮图标  可以查看完整的终端监控详情，包括主机信息、终端状态、同步状态和数据发现状态等信息。
- 启用：在线启用所选设备的终端监控功能，若终端处于离线状态，一旦其在线会马上接收到禁用指令。
- 禁用：在线禁用所选设备的终端监控功能，若终端处于离线状态，一旦其在线会马上接收到启用指令。当终端离线时需要使用申请禁用的功能
- 删除：删除所选设备。若设备仍然在线，则默认5分钟后重新出现在列表中，设置连接频率请参考[终端全局设置](#) on page 65。
- 统计：点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。
- 更多操作

设备控制	当终端处于在线或离线状态时，单独控制设备一些功能的使用，详细信息请参考 <a href="#">终端配置</a> on page 67。
卸载	远程卸载选择的终端，在线状态时立即执行，若终端处于离线状态时，系统会5分钟检测一次直至其在线后执行卸载。
升级	升级所选择的终端。
清除手动配置	清除手动设置的终端状态、设备控制等功能，清除以后终端将会从 <a href="#">终端全局设置</a> on page 65章节获取配置参数。
生成卸载密码	生成随机卸载密码。
清除卸载密码	清除随机卸载密码。

- 终端数据发现：开始、暂停或停止终端数据发现功能。暂停终端数据发现任务后，选择开始会继续执行；停止终端数据发现任务后，选择开始会重新执行。若需开启终端发现任务，详细信息请参考[管理终端任务](#) on page 234。
- 申请禁用：申请在离线时禁用或仅监控所选终端。

时长	申请终端禁用或监控的时长，从提交禁用ID开始计算。
禁用	终端所有功能失效。
监控	不影响终端用户体验，终端改为监控模式。
生成	根据终端ID生成禁用码，在对应的终端上输入禁用码即可在指定的时长内禁用/监控终端。


- 离线、在线：显示列表中离线、在线的设备数量。

### 终端监控详情

在终端监控页面，点击任意终端名称，或点击名称后的  按钮，进入终端监控详情页面，显示在该终端设备上监控到的详细信息。

显示的信息包括：

- 主机信息

 注：自软件版本2.1起，天空卫士™统一内容安全UCS解决方案支持检测MAC主机的[系统完整性保护SIP](#)功能的开启状态，系统管理员可依据检测到的结果提醒用户开启该功能，以增强对MAC主机的系统保护。

- 终端状态
- 同步状态
- 数据发现状态



---

# 第 4 章

---

## Web安全

---

内容:

- [Web安全检测条件](#)
- [Web安全管理](#)
- [Web安全监控](#)
- [Web安全报告](#)
- [Web安全设备监控](#)
- [Web安全设备管理](#)

介绍天空卫士™Web安全解决方案。

天空卫士™安全鳄®统一内容安全UCS ( UCS ) 解决方案采用增强型Web安全网关ASWG作为其Web安全模块，以帮助您的企业和机构应对散布在网络中的各种安全威胁。

ASWG利用基于大数据和机器学习的动态分类技术，提供了可扩展的、快速的URL分类查询功能，包含了本地基本分类、本地高速缓存分类、云端实时分类查询技术；同时采用了Web信誉评分技术，根据指定的敏感度级别来识别风险，以及确定是否允许URL访问。

ASWG集成的高级安全内容扫描引擎，采用了本地加云端实时查杀技术，实时应对最新的病毒、木马、网络威胁、未知威胁等，在威胁到达网络之前对其进行拦截。

## Web安全检测条件

介绍Web安全检测条件的相关信息。

天空卫士™安全鳄®统一内容安全UCS解决方案中的Web安全模块在安全策略中运用多种检测条件检测违反企业安全制度的内容和行为，并在有必要的情况下，采取对应的策略行为，限制或阻断通信，确保企业Web安全。

Web安全解决方案支持以下检测条件。

- URL分类
- 关键字
- 正则表达式
- 文件类型
- 应用控制
- Header控制
- Cloud App云应用
- 安全URL分类

### URL分类

介绍检测条件中的URL分类及其相关知识。

#### URL分类

浏览网页已经是员工日常主要的互联网访问行为。每天都有大量的新增网站以及网页产生，随着大量的社交型网站出现，员工在公工作时间访问这些互联网站点，不仅降低了员工的工作效率，同时也可能会一些潜在的安全隐患，甚至可能会给公司造成信息资产流失等巨大的损失。天空卫士™通过对海量的互联网站点进行静态分类和云端智能分类结合的方式，帮助管理员通过URL分类配置访问策略，从而规范员工的上网行为，将潜在的安全风险拒之门外。

天空卫士™提供业界领先的分类工具和流程，以及人工监控和分类技术，为企业安全管理员提供最精准的，最及时的，和覆盖最完整的URL分类库。

天空卫士™安全鳄®统一内容安全UCS解决方案运用URL分类检测条件，结合系统预置的URL分类库和自定义分类，对用户的网络访问请求中的URL进行分析，并基于分析结果，结合管理员设置的策略，控制用户的访问请求操作。

- URL分类包含预置分类和自定义分类，URL分类匹配的顺序为：自定义优先预置分类。  
比如：用户将原本属于搜索引擎分类的 <https://www.baidu.com> 添加到购物分类，那么用户访问 <https://www.baidu.com> 时，就总是属于购物分类，如果策略不允许访问购物分类，那么用户访问 <https://www.baidu.com> 时，就会被阻止。
- 一些URL会属于多个分类（预置URL分类库或者在不同URL分类中添加了一些正则表达式），安全管理员对这些分类均可进行策略匹配。
- 自定义URL支持正则表达式，URL地址。支持在预置分类和自定义分类中添加URL地址、正则表达式，天空卫士™统一内容安全UCS解决方案对这些添加的自定义URL能够保持自动同步。
- URL分类可以划分到不同的URL风险级别和URL风险类别。

#### URL风险级别

员工通过网络访问不同的网站或应用时，可能给企业引入不同的风险。天空卫士™借助自身强大的URL分类库，对潜在的风险网站进行了风险级别划分。一方面有助于帮助管理员定制有效的安全访问策略，另一方面管理员可以根据风险级别统计内网用户的上网行为。

风险级别分为以下四个等级：

- 高



- 中
- 低
- 安全

风险级别有2种来源

- 系统预置的风险级别，系统根据现有URL类别库、Cloud App 分类，进行风险级别的划分。
- 管理员也可以根据URL分类、Cloud App 分类重新定义。

命中安全URL扫描：自定义安全URL黑名单、云端安全URL黑名单（如：挂马、篡改网页、钓鱼、恶意软件下载、木马等恶意网址），都归类到高风险级别；

风险级别冲突时的优先原则：当风险级别冲突时，处理原则，就高不就低

比如：用户访问某网站时，预置库里对于该网站定义的风险级别为低，但该访问同时命中了安全URL检测（风险级别为：高），那么最终的日志记录风险级别为高

比如管理员可以对风险级别为“高”的风险URL访问行为进行阻断。

### URL风险类别

在Web安全用户场景中，安全管理员会对不同的URL分类进行风险类别划分，从而方便管理员按照风险类别配置策略或统计员工的上网活动，生成不同的风险类别报告。







- 增强型Web安全网关ASWG预置了6种风险类别，分别为：安全风险、带宽占用、商业用途、法律责任、生产力损失、Web2.0，用户也可以添加自定义的风险类别
- 一个URL分类、Cloud App 分类可以属于不同的风险类别，比如流媒体URL分类，可以属于带宽占用，也可以属于生产力损失
- Web安全策略可以根据风险类别配置，比如安全管理员可以通过预置或自定义的风险类别对带宽占用、生产力损失的URL访问行为进行阻断


应用检测条件

URL分类，URL风险级别和URL风险类别均可被策略引用。

在策略配置页面，点击添加匹配或添加例外，选择URL分类，可应用URL分类检测条件。

所涉及页面包含如下按钮和图标。

图标	解释
URL分类	在该栏下点击  进入URL分类对话框，在系统预置和自定义的数据库中选择需要检测的URL分类。
URL风险级别	在该栏下点击  进入URL风险级别对话框，在高中低三个级别中选择需要检测的风险级别。
URL风险类别	在该栏下点击  进入URL风险类别对话框，在系统预置和自定义的数据库中选择需要检测的风险类别。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。

 注：设置多条URL分类规则时，匹配一条即为命中策略。

## 关键字

介绍检测条件中的关键字及其相关知识。

### 检测条件介绍

关键字是指在用户请求的文件中或用户请求的URL等用户请求内容中的一个关键字字符串，如词语，短语或缩写等。

统一内容安全UCS解决方案支持对内容中的关键词进行检测，通过在企业安全策略中定义常用安全的关键字和期望排除的关键字，安全管理员可定义关键字检测，即按照请求中包含的关键字进行检测。

关键字不需要预定义，在添加策略时如果类型是关键字则直接输入多个关键字即可（逗号分隔），可以在策略中选择设置大小写是否敏感（默认不敏感）。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择关键字，即可将关键字检测条件应用至策略。

仅支持输入任意关键字，即可对用户请求包含的关键字进行检测，如“机密信息”等。

 注：设置URL和CGI检测范围设置会影响URL的关键字策略匹配的命中结果。

## 正则表达式

介绍检测条件中的正则表达式及其相关知识。

### 检测条件介绍

正则表达式是指一种可用于匹配多个字符串和文字搭配组合的模板，或常用的固定表达形式。

假设有这样一条简单的正则表达式：`skyguard.(com|org|net)`。

这个正则表达式可以匹配以下的URL。

- `skyguard.com`
- `skyguard.org`
- `skyguard.net`

需谨慎使用正则表达式。正则匹配内容中效果突出，但是需要良好的设计。缺乏良好设计的正则表达式可能导致大量漏报，大量错报，以及系统资源占用过高。将正则表达式应用为策略匹配条件可能会增加内存占用。

如需了解更多关于正则的信息，请参考以下外部链接。

- [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression)
- <http://www.regular-expressions.info/>

统一内容安全UCS解决方案支持对内容中的正则表达式进行检测，通过在企业安全策略中定义常用安全的正则和期望排除的正则，安全管理员可定义正则表达式检测，即按照请求中包含的正则进行检测。




### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择正则表达式，可应用正则表达式检测条件。

在拥有多条正则匹配规则的情况下，为正则表达式添加适当便于区分的名称以便统一管理。

 注：多条正则表达式规则时，匹配一条即为命中策略。

## 应用至Web安全策略

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮清除所有的匹配条件。

## 应用至数据安全策略

参照以下章节将正则表达式检测条件应用于数据安全策略。

[正则表达式匹配/例外](#) on page 175

## 应用控制

介绍检测条件中的应用控制及其相关知识。

### 检测条件介绍

应用是指在企业用户终端设备，或云端环境中安装的，可连接至Web或读取文件，以执行业务相关操作或非业务相关操作的软件应用程序。

应用控制检测条件可针对具体的应用程序进行检测。

天空卫士™安全鳄®统一内容安全UCS解决方案在其管理平台中内置了应用程序库，安全管理员可以在应用程序分类页面添加自定义的应用程序和应用程序分类。通过在企业安全策略中定义常用安全的应用和期望排除的应用，安全管理员可定义应用程序检测，即按照执行用户请求的应用程序进行检测。





### 检测条件配置

在策略配置页面，点击添加匹配或添加例外，选择应用控制，可配置应用控制检测条件。

检测内容匹配中的应用控制允许安全管理员对基于HTTP协议交互的应用程序进行访问控制，如QuickTime。

应用类型包括浏览器应用程序，客户端应用程序，即时消息应用程序和流媒体应用程序。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮清除所有的匹配条件。

## 文件类型

介绍检测条件中的文件类型及其相关知识。

### 检测条件介绍

文件类型检测条件可检测某一特定文档类型，如Microsoft Word文档，或者基于文件内部的特征码检测一系列相似的文件类型，如各种压缩文件。

天空卫士™安全鳄®数据安全解决方案中包含了文件类型库中，其中包含了系统预置的大量文件类型，其中包括：

- 风险文件
- 文本文件
- 多媒体文件
- 图像文件
- 可执行文件
- 文档文件
- 压缩文件
- 不可识别的文件类型
- 等。。。

注：这些预置的类型中包含预置的扩展名

文件类型可编辑，系统支持在预置类型文件中添加扩展名称，也支持添加新的文件类型。

 注：将文件类型应用至检测条件之前，务必确认以下注意事项。





- 一个扩展名文件可以属于不同的文件类型，比如doc可以属于文档文件，也可以同时属于同文本文件
- 不可识别的文件类型用于标识不在文件类型定义（预置和自定义）的扩展名，内容为空，用户不能添加


### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择文件类型，可将文件类型检测条件应用至策略。

系统支持文件的扩展名类型和MIME类型检测。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。

 注：当匹配多条文件类型规则时，匹配一条即为命中策略。

## Header控制

介绍检测条件中的Header控制及其相关知识。

### 检测条件介绍

根据HTTP Header里的不同属性，可以对用户的请求分析并控制，比如根据User-Agent限制用户使用的应用程序（如浏览器）或者用户使用的终端类型（比如windows、Linux、Mac等），根据Content-Type可以控制特定应用访问的应用文件，从而侧方面的实现限制用户使用某些应用通过HTTP协议访问网络的功能。

通过策略对Header中User-Agent或其他属性处理，控制用户使用的应用程序（如各种浏览器、即时消息、P2P应用、终端类型等）；

- 可以控制常见的浏览器，比如IE、360浏览器、搜狗浏览器、Chrome、Safari、腾讯浏览器、Firefox、遨游、UC等；

- 控制即时消息应用的使用（如微信、QQ）；
- 控制P2P应用的使用（如：迅雷、QQ旋风）
- 可以控制常见的终端，PC包括：Windows、Linux、Mac、Solaris，是否再细分，比如Window 7、Windows XP 需要研发分析一下；移动设备包含：iOS、Andriod；

支持自定义Header内容控制，比如通过对Header的特定属性进行分析控制分片上传文件到百度网盘、163邮箱等；

- 策略里支持Header的属性字段与 Key value对应的增、删操作；

#### 检测条件配置



在策略配置页面，点击添加匹配或添加例外，选择Header控制，可配置Header控制检测条件。

字段名称和字段内容对应HTTP中的Header和相应的内容。

字段内容支持关键字和正则表达式两种方式。

关键字的字段内容不区分大小写。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。

## Cloud App

介绍检测条件中的云应用Cloud App及其相关知识。

#### 检测条件介绍

随着云应用的普及，管理员在不知情的情况下，员工通过浏览器访问各种云端应用（比如office365、Gmail、DropBox等）可能会引入安全风险或者数据泄漏，增强型Web安全网关ASWG能够对这些云端应用定制访问控制策略。

Cloud App在策略配置中可以和URL分类、关键字、正则表达式、文件类型、应用程序控制、Header控制同时使用，同时检测匹配和违规行为。（和其他元素之间是与的关系，互不冲突。）

#### Cloud App分类

和URL分类一样，Cloud App分类帮助安全管理员了解最新的针对性威胁和高级安全威胁，并通过Cloud App分类库对这些最新的威胁进行管理，以确保用户可以使用安全的Cloud App云应用程序，控制对包含安全威胁的云应用程序的访问。





- 可对Cloud App按类进行配置策略，类似URL的策略，同时支持某些Cloud App例外。
- 如果Cloud App的策略与URL分类的策略发生冲突时，Cloud App优先。比如：Cloud App策略中对LinkedIn的动作为阻止，而URL分类策略对LinkedIn的是放行，那么用户最终访问LinkedIn的结果是被阻止的；

#### 检测条件配置

在策略配置页面，点击添加匹配或添加例外，选择Cloud App，可配置Cloud App检测条件。

可配置的Cloud App分类类型包括Cloud App、Cloud App分类和信任级别。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。

#### 相关信息

[管理Cloud App on page 96](#)

介绍管理云应用Cloud App的步骤。

## 安全URL分类

介绍检测条件中的安全URL分类及其相关知识。

#### 检测条件介绍

为了灵活的控制对URL的安全进行检测（不再默认对安全URL分类访问进行阻断），安全管理员可以通过定义该检测条件对指定类别的安全URL类型进行检测（比如：挂马、网页篡改、钓鱼等类型等），并且结合策略的动作控制员工的网络访问。

是否允许包含安全风险的URL访问，取决于策略的动作，如果动作是阻止，则无法访问，并触发阻断页面。

如URL分类中包含安全分类，比如用户访问购物网站被阻止，同时也被安全URL分类中的“钓鱼”分类命中，那么在阻断页面的URL分类显示为“购物,钓鱼”。

#### URL沙箱检测





沙箱用于对可疑文件进行深入分析，提供了对[高级持续威胁APT](#)，零日威胁和的额外安全防护。

天空卫士™安全设备通过在虚拟环境中运行并分析这些可疑的文件，以检测恶意行为。

#### 检测条件配置

在策略配置页面，点击添加匹配或添加例外，选择安全URL分类，可配置安全URL分类检测条件。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。

## Web安全管理

介绍Web安全管理相关功能。

Web安全管理相关页面集中于管理平台菜单栏的SWG管理选项下。

通过这些页面上的操作，管理员可以：

- 管理Web安全策略
- 管理Web安全策略元素
- 管理Web安全规则元素
- 管理全局控制设置
- 管理其他Web安全设置

## Web安全策略

介绍Web安全策略相关信息。

### 基本介绍

在SWG管理 > 策略页面管理Web安全策略。

Web安全策略根据用户、网络行为和时间段等因素灵活设定，监控内网员工的Web访问行为，防止员工上网引入潜在的网络安全风险。

Web安全策略支持自定义策略和通过预置/自定义模板添加策略。系统预置的Web安全策略模板包括ITM安全策略，URL访问过滤策略和应用程序访问过滤策略，详细信息请参考[预置ASWG策略模板](#)。





配置一条完整的安全策略需要具备以下信息。



- 策略基本信息
- 策略检测内容
- 策略通道
- 策略用户
- 策略动作

### 页面图标和按钮

Web安全策略页面包含以下图标和操作按钮。

表 34: 页面图标和行间操作按钮功能

图标按钮	解释
添加	点击按钮可选择按照以下方式创建新策略。 <ul style="list-style-type: none"> <li>• 直接创建新策略，详情见<a href="#">创建新策略</a>页面。</li> <li>• 从模板添加策略，详情见<a href="#">根据模板创建策略</a>页面</li> </ul>
启动	点击按钮启用所选策略，启用状态栏显示为启用。
禁用	点击按钮禁用所选策略，启用状态栏显示为禁用。
删除	点击按钮删除所选策略。
	编辑所选策略并显示当前策略信息。
	启用所选策略。
	禁用所选策略。
	将所选策略的内容导出为PDF文件。

图标按钮	解释
	将鼠标移动至图标可选择显示哪些预置的安全策略。   注：默认只显示上级策略和本级策略。上级策略是指上层分级对象制定的策略，下级策略是指下层分级对象制定的策略，本级策略是指本层分级对象制定的策略。本层分级对象没有权限查看上级策略。
批量修改	点击按钮进入策略批量管理页面，对多条策略进行批量管理和设置。

### 页面显示列

Web安全策略页面显示以下内容。

表 35: 页面显示列

图标按钮	解释
名称	策略名称
启用状态	点击按钮启用所选策略，启用状态包括启用和禁用。
描述	为区分策略，所输入的特性描述。
用户	策略适用的用户范围。预置策略默认对所有用户适用。
上次修改时间	策略的最近一次修改时间。
策略等级	启用所选策略。
创建者	策略的创建者。

### 策略基本信息


介绍策略基本信息页面。

### 进入页面

在SWG管理 > 策略页面管理Web安全策略。

策略配置页面包括新策略页面和策略编辑页面。

在页面按钮中点击添加 > 新策略进入创建新策略页面。


在页面显示的策略列表中，点击某一现有策略名称，或点击现有策略名称后的  按钮，进入策略编辑页面。

点击保存至策略模板按钮，可以将当前配置保存为策略模板，复用当前策略内容项。


### 策略基本信息


策略配置页面的策略基本信息部分可配置以下信息。

- 名称 - 注意填写区别于其他条目的名称。

 注：名称支持中英文，数字，以及部分特殊符号，输入系统不支持的特殊符号将导致策略保存失败。

- 描述 - 需说明其用途。

 提示：描述需包含安全管理员对条目进行长期管理所需的必要信息。

 注：不能与现有或内置的条目名称相同。

- 来源Risk Level - Risk Level 1-5，分别对应“较低、普通、严重、危险、高危”。
- 启用状态 - 是否启用该项目。



- 策略等级 - 策略所属[策略等级](#)，即将策略分级。

### 策略检测内容

介绍配置策略检测内容页面。

### 简介

在策略配置页面，点击检测内容选项卡即可配置匹配和例外的检测内容。

Web安全解决方案中策略的匹配和例外选项中可应用以下内容检测条件。

- [URL分类检测条件](#)
- [关键字检测条件](#)
- [正则表达式检测条件](#)
- [文件类型检测条件](#)
- [应用控制检测条件](#)
- [Header控制检测条件](#)
- [Cloud App检测条件](#)
- [安全URL分类检测条件](#)

### 策略通道

介绍配置策略通道页面。

通道用于设置策略可以识别的协议以及方法，方便安全管理对其关注的代理协议进行管理。

策略通道可应用的常见场景包括：

- 出于安全需要，禁止员工向论坛、贴吧发表评论或上传文件
- 出于安全需要，禁止员工访问返回内容包含可执行文件的下载操作

在策略配置页面，点击通道选项卡即可配置策略适用的通道。

通道页面分为网络和终端两个部分。

- 网络部分

数据安全可配置的选项包括各种协议和WebService应用等。

Web安全支持HTTP协议、HTTPS加密协议和FTP协议的网络通道内容检查，默认为HTTP和HTTPS协议。选择HTTP或HTTPS协议时，同时可配置控制阶段和请求方法的高级设置。

- 终端部分

数据安全可配置的选项包括各种协议和终端应用程序等。

Web安全支持HTTP协议、HTTPS加密协议和FTP协议的网络通道内容检查，默认为HTTP和HTTPS协议。选择HTTP或HTTPS协议时，同时可配置控制阶段和请求方法的高级设置。


点击页面上的复选框对相应通道执行激活或者禁用操作。

### 请求方法

HTTP、HTTPS 支持对方法的选择，方法包含：

- • GET
- POST
- PUT
- TRACE
- DELETE
- HEAD
- OPTIONS
- CONNECT

- 自定义：指定的特殊HTTP请求方法，比如方式是CERTVERY的HTTP请求

 注：自定义添加的方法不能和已经预置的方法重复。

- 其它：以上预置方法之外的HTTP/HTTPS方法

### 策略来源

介绍配置策略来源页面。

来源是指策略所适用的来源类型，包含用户、组、组织单元、自定义用户、IP或IP段等，默认为所有即该策略对所有来源生效。

在策略配置页面，点击来源选项卡即可配置策略匹配和例外的来源。





来源匹配和来源例外配置页面完全相同。

系统支持以下条件来添加策略适配的来源或者需要例外的来源：

- 用户：通过系统关联的AD目录、自定义组织架构、自定义目录组进行匹配
- IP/IP段：通过用户的IP地址或IP段进行匹配
- 组/组织单元：通过用户所在的用户组或组织单元进行匹配

策略添加“来源”（原用户）时，支持用户、组/组织单元、IP/IP段、三种类型的内容“与”的关系，即必须选中的条件均被满足时，匹配才生效。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮清除所有的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。

### 策略动作

介绍配置策略动作页面。

在策略配置页面，点击动作选项卡即可配置策略对应的响应动作和动作的生效时间。

### 动作和时段

Web安全策略所支持的策略所支持的动作类型如下：

动作	解释
计时	控制用户访问网络的时间。用户收到计时提示页面，显示是否使用配额时间继续计时浏览。如果用户确认使用，则计时器开始计算配额时间和次数。
提示	提示用户在进行风险网络访问，是否继续。如果用户确认继续访问，则用户在设定的间隔时间内再次命中该策略，或命中其他动作为提示的策略时不再重复提示，直接放行并记录日志；当超时设定的间隔时间后，如果用户再次命中该策略，则再次弹出提示页面。
阻止	阻止用户的网络访问行为。用户的网络请求被阻止，并显示阻断页面。
放行	允许用户的网络访问行为。用户可以访问目标，系统将监控用户行为，并记录用户的网络访问行为日志，供安全管理员查阅

需注意以下事项：



注：

- 所设置的时间段不能重复
- **SWG管理 > 设置 > 基本设置**页面中的策略动作设置会影响计时、提示动作的执行。
- 如果ASWG设备的主机名不能被DNS正常解析，会导致用户命中计时或提示的动作策略时弹出的提示页面不正常，管理员需在ASWG设备上配置重定向地址（选择**SWG管理 > 设置 > 基本设置**，设置重定向主机）。

动作与时段的关系：管理员也可以根据不同的时段定义不同的动作，比如工作时段不允许访问购物类网站，非工作时段员工可以访问购物类网站。

## 高级动作

Web安全解决方案支持以下高级动作：

- **HTTP Header 操作**：选择是否开启HTTP Header 操作，开启后增强型Web安全网关ASWG可以对HTTP协议插入或者移除特定隐私header头，系统支持对header头进行添加，修改，删除和部分替换等操作。
- **内容分析**：
  - 选择是否开启内容分析，开启后设备会将获取的用户请求提交给数据防泄漏DLP引擎做进一步的内容分析，设备可根据其分析结果控制用户访问。
  - 选择将DLP策略检测全面应用于所有策略，或选择将DLP策略检测应用于指定的某几条策略。指定策略检测可避免策略关联的低优先级的DLP策略被高优先级的DLP策略绕过而导致的漏报。



注：本设置对阻止动作不生效。

- **安全扫描**：选择是否启用安全扫描，启用后对命中该策略的用户做Web安全病毒检测。安全扫描开关与设置安全扫描相关联。若安全扫描开关开启，会对命中策略的数据做病毒扫描。
- **第三方ICAP分析**：选择是否启用第三方ICAP代理ICAP Proxy分析，启用后可将用户的上网数据请求通过ICAP投递给第三方ICAP sever 处理。



注：增强型Web安全网关ASWG本机的安全分析和第三方内容分析是串行的，如果被本机的安全分析阻止的数据请求不会再投递给第三方ICAP Server处理

- **带宽限速**：选择是否启用带宽限速，并选择带宽控制对象，控制其网络访问的带宽速率。

## 页面图标介绍

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮编辑所对应的匹配条件。
	点击按钮清除所有的匹配条件。

## 根据模板创建策略

介绍根据模板创建策略页面。

在**SWG管理 > 策略** 页面通过系统预置模板快速添加策略。点击添加按钮，选择从模板添加选项。进入根据模板创建策略页面。





系统预置以下两组模板：

- **基本安全策略模板**限制用户访问安全风险分类里的网站，包括代理规避，钓鱼，动态DNS，恶意软件，恶意网站，间谍软件，僵尸网络，可疑内容，垃圾邮件网站，网页篡改，网站协作与分析，新注册的网站，帐号密码和自定义加密传输等。

- 仅监控策略模板则允许用户访问所有网站。

管理员可以根据需要选择系统预置的策略模板（仅监控策略模板或基本安全策略模板）或用户自定义的策略模板。由策略模板产生的策略默认适用于“所有用户”。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。

#### 预置ASWG策略模板


介绍查看ASWG预制策略模板的步骤。

#### Web安全预制策略模板

天空卫士™ 安全鳄® 统一内容安全 UCS Web安全解决方案提供了预制的策略模板，以帮助安全管理员用于创建和编辑Web安全策略。

#### 查看策略模板

按照以下步骤查看Web安全策略模板。

1. 点击进入SWG管理 > 策略 > 根据模板创建策略页面。
2. 点击  按钮，进入选择策略模板对话框。

系统预制的Web安全策略模板显示在对话框的左侧。

#### 策略批量管理

介绍策略批量管理页面。

策略批量管理页面方便安全管理员同时对多条策略进行批量设置。

在SWG管理 > 策略页面批量管理策略。

点击批量修改按钮，进入策略批量管理页面。

批量修改支持修改具体某几条策略或当前所有策略的内容分析、安全扫描、检测内容、通道、用户和动作。

在选择页面栏可选择多条安全策略同时进行管理。

在设置管理内容栏可对以下策略管理内容进行批量设置。

- 策略等级
- 检测内容
- 通道
- 用户
- 动作

#### 相关信息

[策略基本信息](#) on page 88

介绍策略基本信息页面。

[策略检测内容](#) on page 89

介绍配置策略检测内容页面。

[策略通道](#) on page 89

介绍配置策略通道页面。

[策略来源](#) on page 90

介绍配置策略来源页面。

[策略动作](#) on page 90

介绍配置策略动作页面。

## 策略元素

介绍Web安全策略元素相关信息。

在SWG管理 > 策略元素页面管理Web安全策略元素。

Web安全策略预定义多种策略元素用于创建策略时配置检测内容。

Web安全策略包含以下元素：

- 时段
- 带宽限速
- 策略模板

系统初始化时，每个策略元素都包含有预置内容，管理员可以调整策略元素中的内容。

来源

来源管理页面的页面介绍。

来源是指策略所适用的来源类型，包含用户、组、组织单元、自定义用户、IP或IP段等，默认为所有即该策略对所有来源生效。

在本页配置好的来源，可以在配置策略时，直接引用。

页面包含以下配置项。

- 名称 - 注意填写区别于其他条目的名称。



注：名称支持中英文，数字，以及部分特殊符号，输入系统不支持的特殊符号将导致策略保存失败。

- 描述 - 需说明其用途。



提示：描述需包含安全管理员对条目进行长期管理所需的必要信息。





注：不能与现有或内置的条目名称相同。

- 来源

- 用户：通过系统关联的AD目录、自定义组织架构、自定义目录组进行匹配
- IP/IP段：通过用户的IP 地址或IP 段进行匹配

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮清除所有的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。

图标	解释
	在IP/IP段设置栏，按照以下步骤导入预先编辑好的CSV文件。 1. 点击按钮进入模板导入页面。 2. 下载CSV格式的模板文件至本地，并添加IP/IP段信息。 3. 导入编辑好的CSV格式文件
	点击按钮导出现有的IP/IP段信息到CSV文件中，以方便安全管理员统一配置。

## 时段


时段设置的页面的页面介绍。


在SWG管理 > 策略元素 > 时段页面管理Web安全策略的时段设置。

时段用于表示策略动作的生效时间。

系统预置以下3个时段。



- 工作时间
- 非工作时间
- 全天

1. 选择SWG管理 > 策略元素 > 时段，点击添加，新建策略生效时段。
2. 输入名称和描述，说明该时段的用途。
3. 点击  添加时段，以每周为周期设置生效时段，点击确定。

 提示：支持添加多个时间段。

4. 点击保存，新增时段添加到列表。

表 36: 页面图标和行间操作按钮功能

图标	解释
	编辑文件类型，可查看最后修改时间，创建者信息和文件类型使用情况。
	删除文件类型。
删除	批量删除所选文件类型。

## 管理带宽限速



介绍管理带宽限速的步骤。

在SWG管理 > 策略元素 > 带宽限速页面管理Web安全策略的带宽限速。

带宽限速用于用户访问URL、应用程序等内容时，基于策略对带宽速率进行全局控制，对未命中策略的Web访问不进行带宽控制。

1. 选择SWG管理 > 策略元素 > 带宽限速进入带宽限速页面。
2. 点击添加，新建带宽限速规则。
3. 填写带宽限速规则名称，说明其用途。
4. 填写带宽限速规则描述，详细说明其用途。
5. 设置由客户端到目标服务器的最大上传速率。
6. 设置由目标服务器到客户端的最大下载速率。
7. 点击保存，新增策略模板添加于列表。

表 37: 页面图标和行间操作按钮功能

图标	解释
	编辑带宽限速规则，可查看最后修改时间，创建者信息和URL分类使用情况。
	删除策略模板。使用中的策略模板不可以删除。
删除	批量删除所选带宽限速规则。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

### 管理策略模板

介绍管理策略模板的步骤。

在SWG管理 > 策略元素 > 策略模板页面管理Web安全策略的策略模板。

策略模板用于管理员快速生成相似策略。系统预置2个策略模板：仅监控策略模板和基本安全策略模板。

- 基本安全策略模板不允许用户访问安全风险分类里的网站，包括代理规避，钓鱼，动态DNS，恶意软件，恶意网站，间谍软件，可疑内容，帐号密码和自定义加密传输等。
- 仅监控策略模板则允许用户访问所有网站。

1. 选择SWG管理 > 策略元素 > 策略模板进入策略模板配置页面。

2. 点击添加，新建策略模板：

- 填写策略模板名称，说明其用途。
- 填写策略模板描述，详细说明其用途。
- 设置来源Risk Level，如果用户的来源Risk Level评分高于设置值，将使用该策略匹配动作进行拦截保护。

 注：该功能需购买ITM License并授权激活。

3. 点击检测内容选项卡，设置策略检测匹配/例外的内容。详细信息请参考[添加检测内容](#)。

4. 点击通道选项卡，

- 配置网络通道，目前支持HTTP协议、HTTPS加密协议和FTP协议的网络通道内容检查，默认为HTTP和HTTPS协议。选择HTTP或HTTPS协议时，同时可配置控制阶段和请求方法的高级设置。
- 配置终端通道，目前支持HTTP协议、HTTPS加密协议和FTP协议的网络通道内容检查，默认为HTTP和HTTPS协议。选择HTTP或HTTPS协议时，同时可配置控制阶段和请求方法的高级设置。

5. 点击动作选项卡，ASWG策略所支持的动作如下：

计时	控制用户访问网络的时间。
提示	提示用户在进行风险网络访问，管理员可定义风险网站。
阻止	阻止用户的网络访问行为。
放行	允许用户的网络访问行为。

a. 设置在不同的时段执行不同的动作类型（所设置的时间段不能重复）。

b. 选择是否开启内容分析，将ASWG获取的用户网络请求提交给数据防泄漏（DLP）引擎做进一步的内容分析，ASWG会根据其分析结果控制员工的网络访问。

 注：本设置对阻止动作不生效。

c. 选择是否启用安全扫描，启用后对命中该策略的用户做Web安全病毒检测。安全扫描开关与设置安全扫描相关联。若安全扫描开关开启，会对命中策略的数据做病毒扫描。

- d. 选择是否启用带宽限速，并选择带宽控制对象，控制其网络访问的带宽速率。
6. 点击保存，新增策略模板添加于列表。



注：

- 导入模板里用户自定义的名称和内容与当前UCSS已有文件类型或URL分类内容不重复时，直接导入并增加新引入的元素内容；如果名称重复，则需用户选择是否覆盖当前UCSS设备上的元素内容；
- 导入模板里用户自定义的名称和内容与当前UCSS已有文件类型或URL分类内容不重复并包含时段规则时，需新增时段；如果名称重复但内容不重复，则去重名称后新增时段元素。

表 38: 页面图标和行间操作按钮功能

图标	解释
	编辑策略模板。
	删除策略模板。使用中的策略模板不可以删除。
删除	批量删除所选策略模板。
	从本地导入策略模板。
	导出策略模板到本地。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

## 规则元素

在SWG管理 > 规则元素页面管理Web安全规则元素。

Web安全规则元素是策略分析的内容依据，包括云应用程序Cloud App、风险类别、风险级别和文件类型。

规则元素对应内容是策略中的检测内容的匹配项，规则元素是预先定义的各种规则对象，方便在策略的匹配项中引用。

用户场景 1: 管理不允许员工访问带宽占用率较高的网站或者风险级别是高的网站，防止给内网引入病毒或漏洞；

用户场景 2: 禁止员工外发文档类型或压缩类型的文件，防止员工通讯录、财务等数据被泄漏出去；

### 管理Cloud App

介绍管理云应用Cloud App的步骤。

安全管理员可以查看增强型Web安全网关ASWG预制的云应用Cloud Application的详细信息，也可以对预制的云应用Cloud Application快速添加安全策略。

在SWG管理 > 规则元素 > Cloud App页面查看云应用的详细描述，并对安全风险云应用采取安全策略措施。

- 查看云应用详情：点击云应用名称后的按钮，即可进入云应用详情页面，查看该应用的详细信息，包括名称，描述，分类，信任级别，发布者，风险因子和使用详情等。
- 快速添加策略：勾选云应用名称前的复选框后，可点击快速添加策略按钮，进入添加策略页面，所选择的云应用将显示在默认匹配规则中。可通过这种方式检测特定云应用并制定安全策略。关于策略定制，请参考[Web安全策略](#)获取更多相信信息。

相关概念

[Cloud App](#) on page 85



介绍检测条件中的云应用Cloud App及其相关知识。


### 管理风险类别

介绍管理风险类别的步骤。

管理员可以对ASWG设置的URL分类划分风险类别，系统预置风险类别包括宽带风险、带宽占用、生产力损失、法律责任、商业用途和Web2.0。风险类别的数据用于ASWG报告的统计。





在SWG管理 > 规则元素 > 风险类别页面管理Web安全策略的风险类别。

有关ASWG报告的详细信息请参考[ASWG用户行为报告](#)和[ASWG用户安全报告](#)。

1. 按照以下步骤添加自定义风险类别。
2. 选择ASWG管理 > 规则元素 > 风险类别设置。
3. 点击添加，添加自定义风险类别。
4. 输入自定义风险类别名称，点击确定。
5. 点击风险类别名称可显示该风险类别包含的URL分类，点击添加，可添加系统中预置或自定义URL分类；点击  删除所选URL分类。

 提示：将鼠标悬浮于风险类别名称，出现详情图标 ，点击后可显示该风险类别的使用详情。

表 39: 页面图标和行间操作按钮功能

图标	解释
	编辑自定义风险类别名称。
删除	批量删除所选风险类别或URL分类，使用中的风险类别或URL分类不能被删除。
	从本地导入风险类别文件，会完全覆盖系统中的风险分类。
	导出风险类别和对应的URL分类信息到本地，不包含自定义URL分类里的URL信息。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。
	恢复初始，此操作会丢失所有风险类别中添加的自定义URL分类和自定义风险类别。

### 管理风险级别

介绍管理风险级别的步骤。

在SWG管理 > 规则元素 > 风险级别页面管理Web安全策略的风险级别。





ASWG预置高、中和低三种风险级别，未被划分的URL默认为安全，用户可根据应用场景将URL分类进行风险级别的划分。系统统计风险级别信息并呈现于ASWG报告中。

选择ASWG管理 > 规则元素 > 风险级别设置，点击风险级别可显示该风险级别包含的URL分类。

点击添加可添加系统中预置或自定义的URL分类；点击删除删除所选URL分类。

 提示：将鼠标悬浮于风险级别名称，出现详情图标 ，点击后可显示该风险级别的使用详情。

表 40: 页面图标和行间操作按钮功能

图标	解释
	批量删除所选风险类别或URL分类，使用中的风险类别或URL分类不能被删除。
	从本地导入风险类别文件。
	导出风险类别文件到本地。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。
	恢复初始，此操作会丢失所有风险类别中添加的自定义URL分类和自定义风险类别。

### 管理文件类型

介绍管理文件类型的步骤。

在SWG管理 > 规则元素 > 文件类型页面管理Web安全策略的文件类型。



**扩展名类型：**文件类型基于文件扩展名对文件进行分类，用于管理URL请求中包含的文件，或对指定类型的文件进行病毒扫描。

**MIME类型**MIME (Multipurpose Internet Mail Extensions)为多用途互联网邮件扩展类型。它是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。

管理员可以增加新的扩展名类型和MIME类型。，也可以在预置的新的扩展名类型和MIME类型中添加新的文件类型。

1. 选择SWG管理 > 策略元素 > 文件类型，进入文件类型配置页面。
2. 点击扩展名类型或MIME类型标题栏。
3. 点击添加，新建文件类型。
4. 输入名称和描述，说明文件类型的用途。
5. 对于扩展名文件类型，输入自定义文件扩展名。对于MIME类型，输入自定义MIME类型。
6. 点击保存，新增文件类型添加到列表。

表 41: 页面图标和行间操作按钮功能

图标	解释
	编辑文件类型，可查看最后修改时间，创建者信息和文件类型使用情况。
	删除文件类型。
删除	批量删除所选文件类型。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

### 相关概念

[文件类型](#) on page 160

介绍检测条件中的文件类型及其相关知识。

## 全局控制

介绍全局控制的相关信息。

在SWG管理 > 全局控制页面管理Web安全全局控制。

Web安全全局控制主要用来配置ASWG的全局白名单功能与全局黑名单功能，支持在特殊情况下放行或阻止指定的客户访问请求。



注：

全局黑名单的优先级高于全局白名单，即针对一个用户访问请求，系统会优先处理黑名单，再处理白名单（如果此访问请求没有被黑名单阻止）。

### 白名单

介绍全局白名单设置页面。

### 功能介绍

全局白名单，对满足名单的来源或目标请求直接放行，并根据设置决定是否记录用户行为日志，对符合条件的请求不进行任何策略判断。

在ASWG 管理 > 全局控制 > 白名单页面管理Web安全的全局白名单。

来源/目标的逻辑关系为"或"，即只要任意一个条件匹配，名单即生效。

### 配置项介绍

来源可配置项包含：

- 用户：
  - 用户目录中的用户/OU/Group
  - 组织架构中的用户/部门
  - 自定义用户组中的用户/OU/Group
- IP（段）：例如192.168.0.0-192.168.0.255

目标可配置项包含URL、IP（段）

### 注意事项





配置白名单需注意以下事项：

- 全局白名单，优先于除黑名单以外的所有策略。
- 如对某全局来源IP(段)设置白名单 - 则该来源IP(段)发起的请求直接被放行，例如通过白名单放行公司Web服务器发起的所有请求
- 如对某全局来源用户设置白名单 - 则用户目录中对应的用户、用户组、组织单元，所有白名单用户发起的请求均被放行
- 如对某全局目标URL设置白名单 - 则所有访问白名单URL的请求均被放行。例如任何人访问白名单网站[www.12306.com](http://www.12306.com)直接被放行
- 如对某全局目标IP（段）设置白名单 - 则所有访问白名单IP（段）的请求均被放行。
- 全局白名单支持是否记录日志操作。如选择记录日志，则请求被放行的同时记录用户行为日志；如选择不记录日志，则请求被放行且不记录用户行为日志。

### 页面图标按钮

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。

图标	解释
	点击按钮将选择的匹配条件移至左侧，未选择的条件。
	点击按钮清除所有的匹配条件。
	<p>点击按钮进入匹配条件导入对话框。</p> <p>导入的名单需符合一定的格式，按照以下步骤导入匹配条件。</p> <ol style="list-style-type: none"> <li>1. 点击下载模板文件至本地。</li> <li>2. 编辑模板文件，将需要匹配的项目填入模板文件中，并保存。</li> <li>3. 点击选择，找到编辑后的模板文件。</li> <li>4. 选择对应的编码格式。</li> <li>5. 点击导入。</li> </ol>
	点击按钮将配置的匹配条件导出至本地。

记录白名单日志：拉动记录日志状态条，可以选择是否记录白名单里的用户日志。

### 黑名单

介绍全局黑名单设置页面。

### 功能介绍

全局黑名单，对满足名单的来源或目标请求直接阻断，并记录日志，对符合条件的请求不进行任何策略判断。

在SWG 管理 > 全局控制 > 黑名单页面管理Web安全的全局黑名单。

### 配置项介绍

来源可配置项包含：

- 用户：
  - 用户目录中的用户/OU/Group
  - 组织架构中的用户/部门
  - 自定义用户组中的用户/OU/Group
- IP ( 段 )：例如192.168.0.0-192.168.0.255

目标可配置项包含URL、IP ( 段 )








### 注意事项

配置黑名单需注意以下事项：

- 全局黑名单，优先于白名单和所有策略
- 如对某来源IP(段)设置黑名单 - 则该来源IP(段)发起的请求直接被阻断，例如阻断IP：172.1.1.1发起的所有网络请求
- 如对某来源用户设置黑名单 - 则用户目录中对应的用户、用户组、组织单元，所有黑名单用户发起的请求均被阻断
- 如对某目标URL设置黑名单 - 则所有访问黑名单URL的请求均被阻断。例如任何人访问黑名单网站[www.gambling.com](http://www.gambling.com)直接被阻断
- 如对某目标IP ( 段 ) 设置黑名单 - 则所有访问黑名单IP ( 段 ) 的请求均被阻断。

## 页面图标按钮

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。
	点击按钮清除所有的匹配条件。
	<p>点击按钮进入匹配条件导入对话框。</p> <p>导入的名单需符合一定的格式，按照以下步骤导入匹配条件。</p> <ol style="list-style-type: none"> <li>1. 点击下载模板文件至本地。</li> <li>2. 编辑模板文件，将需要匹配的项目填入模板文件中，并保存。</li> <li>3. 点击选择，找到编辑后的模板文件。</li> <li>4. 选择对应的编码格式。</li> <li>5. 点击导入。</li> </ol>
	点击按钮将配置的匹配条件导出至本地。

## 设置

在**SWG管理 > 设置**页面管理Web安全设置。

Web安全的其他相关设置。

### 基本设置

介绍配置Web安全基本设置的步骤。

### 基本信息

在**SWG管理 > 设置 > 基本设置**页面管理Web安全的基本设置。

ASWG基本设置包括设置策略动作以及URL和CGI检测范围。

### 策略动作

计时动作和提示动作是ASWG策略的动作项，策略动作配置可以限制用户访问网络的次数、时长和提示间隔时长。

设置项	介绍
计时动作每天分配次数	设置策略计时动作的每天访问次数配额，默认6次。
计时动作每次时长	设置策略计时动作的每天访问次数时长，默认10次。
提示动作间隔时长	设置策略提示动作的间隔时长，在间隔时间内不再进行提示，默认30次。

### URL和CGI检测范围

设置URL和CGI匹配关键字或正则表达式的范围。

设置项	介绍
URL和CGI	检测整个URL的所有字符是否包含关键字或正则表达式。
仅URL	只检测CGI查询串问号“?”前的字符是否包含关键字或正则表达式。
仅CGI	只检测CGI查询串问号“?”后的字符是否包含关键字或正则表达式。

### 安全设置

介绍Web安全扫描设置的步骤。

在SWG管理 > 设置 > 安全扫描页面管理Web安全扫描设置。

ASWG内置集成的杀毒引擎对用户访问的URL内容进行安全扫描。

在页面顶端滑动状态条启用ASWG安全扫描功能，默认启用。

### URL安全扫描

1. 设置URL安全扫描，根据以下扫描类型进行配置：


选项	介绍
对Web2.0网站进行安全扫描	使用集成的杀毒引擎对未分类的网站进行安全扫描。
对未分类的网站进行安全扫描	使用集成的杀毒引擎对Web2.0网站进行安全扫描。
对指定URL分类进行安全扫描	使用集成的杀毒引擎对指定URL分类进行安全扫描。点击  选择系统中已有的URL分类，添加到扫描列表；点击  删除所选URL分类。


### 透传扫描

设置透传扫描，勾选后使用集成的杀毒引擎对透传的流量进行安全扫描。

### 文件扫描

设置文件扫描：

1. 设置扫描时限和扫描文件大小的阈值，当文件达到阈值时，系统不对文件进行扫描。
2. 系统预置扫描可执行文件和不能识别的文件，点击可添加列表中的文件类型，文件类型与策略元素中的文件类型同步。

 提示：“不能识别的文件”是指不包含在预置和自定义的文件类型之外的文件。


### 云端查询

启用云端查询后，企业本地安全设备可以连接至天空卫士™云端URL分类数据库和安全URL分类数据库，随时查询URL分类和安全URL分类库的最新数据。

配置完成后，点击保存，安全扫描设置生效。

### 高级检测

点击页面右上角的高级检测，可进入高级检测配置页面。

 注：高级检测选项推荐使用默认设置，如需修改，请在天空卫士™技术支持人员的帮助下进行，切勿擅自修改。

## 日志设置

介绍管理Web安全日志设置的步骤。

在SWG管理 > 设置 > 设置日志页面管理Web安全日志设置。

ASWG日志记录用户的上网行为。有关日志的详细信息请参考[Web安全监控](#)。

1. 设置数据库分区阈值，包括分区容量最大值和分区活跃时长。

分区容量最大值	设置分区容量最大值，如果达到此阈值，自动将分区设为“只读”状态，并自动创建新分区。
分区活跃时长	设置分区活跃时限，如果达到此阈值，自动将分区设为“只读”状态，并自动创建新分区。

2. 设置数据库维护计划，包括自动删除分区时间和优化分区中的索引。

自动删除分区时间	删除指定时间之前的分区。
优化分区中的索引	启用优化分区中的索引，可提高报表生成速度。需要设置维护开始的时间点，默认凌晨1点。

3. 设置URL记录方式，可选择仅记录URL域名部分（包括端口）或记录完整URL内容。

仅记录URL域名部分（包括端口）	勾选此项后，仅日志中记录URL域名和端口。
记录完整URL内容	勾选此项后，记录用户访问页面的完整URL路径。

4. 设置网站浏览时长，包括任务开始时间和平均网站浏览时长。

任务开始时间设置	设置计算用户访问网站浏览时长任务的开始时间。
平均网站浏览时长	设置平均浏览网站的时限。

5. 设置日志缓存相关项。




创建缓存日志的频率	设置创建缓存日志的频率。
缓存日志条目数	设置创建缓存日志的数量，转发至UCSS管理平台生成实时日志。
日志合并	开启日志合并后，在日志入库时，将在指定时间范围内，合并相同用户在相同IP地址产生的相同URL域名的请求日志。

## Cloud App分类更新

介绍云应用Cloud App更新的步骤。

ASWG预置的云应用Cloud Application支持动态更新。

在SWG管理 > 设置 > Cloud App更新页面的Cloud App更新栏查看最新的云应用分类库版本。

- 如页面显示有可用的新版本，可直接点击立即更新下载更新并应用。
- 如页面显示当前版本已是最新，则无需更新。
- 点击页面内容右上角的按钮，您也可以通过导入ext后缀名的云应用分类库文件的方式进行更新。
- 在自动更新栏，您可以设置云应用更新的更新计划和代理服务器。
- 更新计划：勾选更新计划后按照页面设置更新时间和更新间隔。
  -  提示：建议选择系统空闲时间进行更新，以免更新占用系统和网络资源，影响工作效率。
- 代理服务器：勾选代理服务器设置后按照页面设置代理服务器。
  -  注意：确保代理服务器和需要更新的ASWG设备之间网络连接通畅。

## Web安全监控

介绍Web安全监控相关信息。

ASWG监控并统计用户上网行为，并支持实时日志，实时显示当前上网的用户行为信息。管理员可快速了解内网用户的在线情况、带宽使用情况等。

Web安全监控相关页面集中位于菜单栏的监控 > SWG监控选项下。

通过在这些页面上的操作，管理员可以：

- 审查实时用户行为状况日志
- 审查实时在线用户状况日志
- 审查实时网络日志

### 用户行为统计

介绍用户行为统计监控的相关信息。

#### 简介

用户行为统计以不同的维度统计和展示与Web相关的用户访问活动，通过递进的统计排名方式，详细了解某一用户的行为信息。

在监控 > SWG监控 > 用户行为统计页面管理实时监控到的用户行为统计信息。

#### 页面介绍

监控页面包含以下快速按钮。

表 42: 快速按钮功能介绍

按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

监控页面的筛选条件如[筛选条件](#)所示。

页面支持如下操作：

- 点击用户行为柱状统计图或二维统计的对象时跳转至用户行为日志，详细信息请参考[查看用户行为日志](#)。

#### 高级统计

按照如下步骤执行高级统计操作，对监控数据进行二维统计并排名。

1. 勾选高级统计对监控数据进行二维统计。
2. 选择排名方式和排名数。
3. 点击查询。
4. 查看显示的二维统计数据，快速确认安全隐患。


#### 报告筛选条件/显示列


介绍适用的筛选条件/显示列。

下表罗列了适用的筛选条件/显示列，并逐条介绍其含义。



表 43: 筛选条件/显示列

筛选条件/显示列	解释
用户	<p>用户的显示名称，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）</p> <ol style="list-style-type: none"> <li>1. AD 中的用户的Display Name</li> <li>2. 自定义组织机构中的名称</li> <li>3. 其它的显示IP地址（DC Agent、Logon Agent、其它）</li> </ol>
登录名	<p>用于用户身份识别，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）：</p> <ol style="list-style-type: none"> <li>1. AD 中用户的Logon Name</li> <li>2. 自定义组织机构中的用户名</li> <li>3. DC Agent、Logon Agent 中的名称</li> <li>4. 其它为空</li> </ol>
唯一识别名	<p>标识用户的唯一身份ID。</p> <p>比如AD用户CN=haha,OU=QA,OU=R&amp;D,OU=Staff,DC=skyguardmis,DC=com，或者DC Agent、Logon Agent中的FQDN名称</p>
源IP	客户端IP地址
通道	事件所发生的通道或协议类型，比如 HTTP、HTTPS、FTP
动作	<p>策略所对应的动作</p> <p>动作包含：阻止、计时、提示、放行，每条策略只对应一个动作</p> <p>动作优先级为：阻止 &gt; 计时 &gt; 提示 &gt; 放行</p>
域名	用户所在的域，可以为空
部门	用户所在的部门，可以为空
策略名称	<p>事件命中的安全策略名称。</p> <p>命中多个策略时，系统记录所有命中的策略名，包含内置的策略名称（策略名称是固定的）</p>
URL分类	URL 所属的分类，比如：购物、IT等
URL风险类别	URL对应的风险类别
安全威胁类型	安全URL扫描的结果，比如挂马、网页篡改，或者内容扫描的病毒结果
文件类型	事件涉及的文件类型（扩展名、MIME TYPE），包含请求和应答中的文件类
URL主机名	用户访问的URL主机名，比如： <a href="http://www.skyguard.com.cn">www.skyguard.com.cn</a>
完整URL	<p>完成的URL，包括协议和主机名</p> <p>系统根据用户日志设置中的URL记录类型，决定是否记录部分或完整URL地址</p> <p>设置方式：SWG管理 &gt; 设置 &gt; 日志设置 &gt; URL记录方式</p> <p> 注：动作是阻止的访问，忽略此设置，始终记录完整的URL</p>

目标IP	访问目标的IP地址，可能为空（原因是被阻止的请求，没有进行DNS解析）
端口	访问目标的端口号
设备名称	安全监控设备名称，如果是终端，则名称固定为：“注册终端”
关键字	记录命中策略中的关键字，可能有多个
文件名称	事件涉及的文件名称，可能有多个
浏览时长	访问该URL的时间，默认每个页面算为20秒
是否安全	根据风险级别的结果记录，风险级别为高、中、低，显示为不安全；风险级别为安全的情况下，显示为安全；
URL安全级别	自定义的风险级别
病毒名称	访问的内容被病毒引擎发现的病毒名称
城市	根据IP的经纬度，解析得到目标站点所在的城市
国家	根据IP的经纬度，解析得到目标站点所在的国家
位置	目标IP所在的的经纬度
发送字节数	通过浏览器或其他方式访问网络发送的请求字节数
接收字节数	目标服务器对用户的响应字节数
总字节数	发送字节数和接收字节数的总和
应用类型	网络应用类型 应用类型目前包含浏览器、客户端、P2P、即时消息、流媒体应用类型5种。不在预置类型的，默认为空
应用名称	应用程序的名称，这些是厂家自身定义的
阻止类型	<p>动作被阻止的原因：阻止类型包含以下类型：</p> <ul style="list-style-type: none"> <li>• 黑名单阻止：因为命中了黑名单被阻止（全局策略）</li> <li>• URL阻止：因URL分类或自定义URL被阻止（策略）</li> <li>• 文件类型阻止：URL里因包含文件类型被阻止（策略）</li> <li>• 关键字阻止：URL里因包含关键字被阻止（策略）</li> <li>• 计时阻止：用户被分配了上网时间配额，上网配额被用完时被阻止（策略）</li> <li>• 安全威胁阻止：网页内容由于含有病毒、或者因为安全URL检测，发现包含木马等安全风险内容而被阻止。（比如：挂马，篡改网页，钓鱼、病毒等）</li> <li>• SSL事件阻止：因为访问的网站证书不合法被阻止(非策略动作，不用记录用户行为日志)</li> <li>• DLP阻止：因为用户的访问数据命中DLP策略，并且被阻止</li> </ul> <p> 注：阻止类型记录的优先级：黑名单 &gt; SSL事件阻止 &gt; 安全威胁（安全URL检测） &gt; 计时 &gt; 关键字 &gt; 文件类型 &gt; URL &gt; 安全威胁（病毒） &gt; DLP阻止</p>
来源Risk Level	用户行为所属的Risk Level(高危、危险、严重、普通和较低)
方法	HTTP请求的方法
响应码	HTTP响应码

Cloud App	Cloud App名称
Cloud App分类	Cloud App 所属分类
Cloud App 信任级别	Cloud App 的信任级别 ( 由后台给出, 用户不可更改 )
Cloud App 分值	Cloud App 的信用分值
Referrer URL	记录当前页面的来源地址, 即是由哪个页面定向过来的
User Agent	HTTP报文中UserAgent信息, 比如浏览器类型、版本, 操作系统类型、版等
会话阶段	用户行为日志生成时所在的HTTP会话阶段

### 用户行为日志

介绍用户行为日志监控的相关信息。

### 简介



用户行为日志记录详细的用户行为信息, 用户行为日志内容依据用户行为统计的已选条件筛选获得。


在监控 > SWG监控 > 用户行为统计页面管理实时监控到的用户行为日志信息。

### 页面介绍

监控页面包含以下快速按钮。

表 44: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框, 可选择筛选条件, 查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息, 通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项, 将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表, 可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

 注: 不同的管理员登陆同一UCSS设备可以通过调整显示列设置各自的显示列条目。


### 报告筛选条件/显示列

介绍适用的筛选条件/显示列。

下表罗列了适用的筛选条件/显示列, 并逐条介绍其含义。

表 45: 筛选条件/显示列

筛选条件/显示列	解释

用户	<p>用户的显示名称，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）</p> <ol style="list-style-type: none"> <li>1. AD 中的用户的Display Name</li> <li>2. 自定义组织机构中的名称</li> <li>3. 其它的显示IP地址（DC Agent、Logon Agent、其它）</li> </ol>
登录名	<p>用于用户身份识别，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）：</p> <ol style="list-style-type: none"> <li>1. AD 中用户的Logon Name</li> <li>2. 自定义组织机构中的用户名</li> <li>3. DC Agent、Logon Agent 中的名称</li> <li>4. 其它为空</li> </ol>
唯一识别名	<p>标识用户的唯一身份ID。</p> <p>比如AD用户CN=haha,OU=QA,OU=R&amp;D,OU=Staff,DC=skyguardmis,DC=com，或者DC Agent、Logon Agent中的FQDN名称</p>
源IP	客户端IP地址
通道	事件所发生的通道或协议类型，比如 HTTP、HTTPS、FTP
动作	<p>策略所对应的动作</p> <p>动作包含：阻止、计时、提示、放行，每条策略只对应一个动作</p> <p>动作优先级为：阻止 &gt; 计时 &gt; 提示 &gt; 放行</p>
域名	用户所在的域，可以为空
部门	用户所在的部门，可以为空
策略名称	<p>事件命中的安全策略名称。</p> <p>命中多个策略时，系统记录所有命中的策略名，包含内置的策略名称（策略名称是固定的）</p>
URL分类	URL 所属的分类，比如：购物、IT等
URL风险类别	URL对应的风险类别
安全威胁类型	安全URL扫描的结果，比如挂马、网页篡改，或者内容扫描的病毒结果
文件类型	事件涉及的文件类型（扩展名、MIME TYPE），包含请求和应答中的文件类
URL主机名	用户访问的URL主机名，比如： <a href="http://www.skyguard.com.cn">www.skyguard.com.cn</a>
完整URL	<p>完成的URL，包括协议和主机名</p> <p>系统根据用户日志设置中的URL记录类型，决定是否记录部分或完整URL地址</p> <p>设置方式：SWG管理 &gt; 设置 &gt; 日志设置 &gt; URL记录方式</p> <p> 注：动作是阻止的访问，忽略此设置，始终记录完整的URL</p>
目标IP	访问目标的IP地址，可能为空（原因是被阻止的请求，没有进行DNS解析）
端口	访问目标的端口号

设备名称	安全监控设备名称，如果是终端，则名称固定为：“注册终端”
关键字	记录命中策略中的关键字，可能有多个
文件名称	事件涉及的文件名称，可能有多个
浏览时长	访问该URL的时间，默认每个页面算为20秒
是否安全	根据风险级别的结果记录，风险级别为高、中、低，显示为不安全；风险级别为安全的情况下，显示为安全；
URL安全级别	自定义的风险级别
病毒名称	访问的内容被病毒引擎发现的病毒名称
城市	根据IP的经纬度，解析得到目标站点所在的城市
国家	根据IP的经纬度，解析得到目标站点所在的国家
位置	目标IP所在的的经纬度
发送字节数	通过浏览器或其他方式访问网络发送的请求字节数
接收字节数	目标服务器对用户的响应字节数
总字节数	发送字节数和接收字节数的总和
应用类型	网络应用类型 应用类型目前包含浏览器、客户端、P2P、即时消息、流媒体应用类型5种。不在预置类型的，默认为空
应用名称	应用程序的名称，这些是厂家自身定义的
阻止类型	<p>动作被阻止的原因：阻止类型包含以下类型：</p> <ul style="list-style-type: none"> <li>• 黑名单阻止：因为命中了黑名单被阻止（全局策略）</li> <li>• URL阻止：因URL分类或自定义URL被阻止（策略）</li> <li>• 文件类型阻止：URL里因包含文件类型被阻止（策略）</li> <li>• 关键字阻止：URL里因包含关键字被阻止（策略）</li> <li>• 计时阻止：用户被分配了上网时间配额，上网配额被用完时被阻止（策略）</li> <li>• 安全威胁阻止：网页内容由于含有病毒、或者因为安全URL检测，发现包含木马等安全风险内容而被阻止。（比如：挂马，篡改网页，钓鱼、病毒等）</li> <li>• SSL事件阻止：因为访问的网站证书不合法被阻止(非策略动作，不用记录用户行为日志)</li> <li>• DLP阻止：因为用户的访问数据命中DLP策略，并且被阻止</li> </ul> <p> 注：阻止类型记录的优先级：黑名单 &gt; SSL事件阻止 &gt; 安全威胁（安全URL检测） &gt; 计时 &gt; 关键字 &gt; 文件类型 &gt; URL &gt; 安全威胁（病毒） &gt; DLP阻止</p>
来源Risk Level	用户行为所属的Risk Level(高危、危险、严重、普通和较低)
方法	HTTP请求的方法
响应码	HTTP响应码
Cloud App	Cloud App名称
Cloud App分类	Cloud App 所属分类

Cloud App 信任级别	Cloud App 的信任级别 ( 由后台给出, 用户不可更改 )
Cloud App 分值	Cloud App 的信用分值
Referrer URL	记录当前页面的来源地址, 即是由哪个页面定向过来的
User Agent	HTTP报文中UserAgent信息, 比如浏览器类型、版本, 操作系统类型、版等
会话阶段	用户行为日志生成时所在的HTTP会话阶段

## 在线用户

介绍查看在线用户的步骤。


### 简介

在线用户实时显示活跃的用户信息, 查看和管理连接到ASWG设备 ( 注册于UCSS ) 的用户或IP。系统在每日零时清除已有数据并重新统计活跃用户信息。

在监控 > SWG监控 > 在线用户页面管理实时监控到的在线用户信息。

### 页面介绍

页面提供如下功能：


- 若有多台注册的设备, 通过选择监控设备, 分别显示连接到每个设备的活跃用户信息。
- 监控设备功能显示连接到该设备的所有活跃用户信息。
- 可选择页面刷新信息频率 ( 10秒/20秒/30秒 )。
- 若某个用户发送字节数异常, 比如总字节比较多, 可点击  拉入黑名单, 阻止该用户之后的上网请求。详细信息请参考[全局控制](#)。

## 实时日志

介绍实时日志监控的相关信息。

实时日志用于实时查看监控网络中经由代理设备处理过的用户行为信息, 展现用户上网记录的日志数据。




在监控 > SWG监控 > 实时日志页面管理监控到的实时日志信息。

 提示: 通过页面刷新频率(10/20/30)设置定时刷新, 方便查看用户的上网轨迹等。

### 页面介绍

监控页面包含以下操作按钮和图标。

表 46: 按钮和按钮功能介绍

图标和按钮	功能
添加筛选	点击按钮显示所有筛选条件列表, 可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。
	开始刷新日志。
	暂停刷新日志, 保留当前页面以便于记录信息。
缓存记录数	选择每页显示的缓存记录数(100/200/500/1000)。   提示: 如果用户环境有多台Web安全设备时, 可以通过调整页面的“缓存记录”来控制每台设备定时刷新的用户日志最大数量。

## Web安全报告

介绍Web安全报告相关信息。

Web安全报告包括用户行为报告和用户安全报告，统计用户的上网行为数据，排查安全隐患。

Web安全报告相关页面集中位于菜单栏的报告 > SWG报告选项下。

通过页面上的操作，管理员可以：

- 查看用户行为报告
- 查看用户安全报告

### 用户行为报告

介绍Web安全用户行为报告的相关信息。

#### 简介

在报告 > SWG报告 > 用户行为报告页面管理用户行为报告。

用户行为报告用于统计某一段时间或某一个时间点的用户上网行为数据。

用户行为报告信息包括用户登录名、源IP、策略名称和完整URL等，报告类型包括列表报告、图表报告和趋势报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

#### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

#### 页面图标

报告列表页面包含以下操作按钮。

表 47: 页面图标功能介绍



图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

#### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

点击报告名称进入报告页面，报告页面包含以下操作按钮。

表 48: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相应步骤信息。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相应步骤信息。

下表显示报告支持的类型和对应解释。

表 49: 用户行为图表报告类型

报告类型	解释
网站-访问量排名	统计不同网站访问量，并排名前N位（最多显示30名）。
网站分类排名	统计不同URL分类的访问量，并排名前N位（最多显示30名）。
关键字命中排名	统计不同违规用户命中关键字的次数，并排名前N位（最多显示30名）。
上网行为活动排名	统计不同上网行为活动的次数并，排名前N位（最多显示30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相应步骤信息。

下表显示报告支持的类型和对应解释。

表 50: 用户行为趋势报告类型

报告类型	解释
网站访问趋势	统计不同网站的访问量并排名前N位（最多显示30名）。
网站分类访问趋势	统计不同URL分类的访问量并排名前N位（最多显示30名）。
FTP访问趋势	分别统计不同网站、URL分类和FTP的访问量并排名前N位（最多显示30名）。
网络访问趋势	分别统计不同网站、URL分类和FTP的访问量并排名前N位（最多显示30名）。



## 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

## 报告筛选条件/显示列


介绍适用的筛选条件/显示列。

下表罗列了适用的筛选条件/显示列，并逐条介绍其含义。

表 51: 筛选条件/显示列

筛选条件/显示列	解释
用户	用户的显示名称，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3） <ol style="list-style-type: none"> <li>1. AD 中的用户的Display Name</li> <li>2. 自定义组织机构中的名称</li> <li>3. 其它的显示IP地址（DC Agent、Logon Agent、其它）</li> </ol>
登录名	用于用户身份识别，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）： <ol style="list-style-type: none"> <li>1. AD 中用户的Logon Name</li> <li>2. 自定义组织机构中的用户名</li> <li>3. DC Agent、Logon Agent 中的名称</li> <li>4. 其它为空</li> </ol>
唯一识别名	标识用户的唯一身份ID。 比如AD用户CN=haha,OU=QA,OU=R&D,OU=Staff,DC=skyguardmis,DC=com，或者DC Agent、Logon Agent中的FQDN名称
源IP	客户端IP地址
通道	事件所发生的通道或协议类型，比如 HTTP、HTTPS、FTP
动作	策略所对应的动作 动作包含：阻止、计时、提示、放行，每条策略只对应一个动作 动作优先级为：阻止 > 计时 > 提示 > 放行
域名	用户所在的域，可以为空
部门	用户所在的部门，可以为空
策略名称	事件命中的安全策略名称。 命中多个策略时，系统记录所有命中的策略名，包含内置的策略名称（策略名称是固定的）
URL分类	URL 所属的分类，比如：购物、IT等
URL风险类别	URL对应的风险类别
安全威胁类型	安全URL扫描的结果，比如挂马、网页篡改，或者内容扫描的病毒结果

文件类型	事件涉及的文件类型 ( 扩展名、MIME TYPE ) , 包含请求和应答中的文件类
URL主机名	用户访问的URL主机名, 比如: <a href="http://www.skyguard.com.cn">www.skyguard.com.cn</a>
完整URL	完成的URL, 包括协议和主机名 系统根据用户日志设置中的URL记录类型, 决定是否记录部分或完整URL地址 设置方式: SWG管理 > 设置 > 日志设置 > URL记录方式  注: 动作是阻止的访问, 忽略此设置, 始终记录完整的URL
目标IP	访问目标的IP地址, 可能为空 ( 原因是被阻止的请求, 没有进行DNS解析 )
端口	访问目标的端口号
设备名称	安全监控设备名称, 如果是终端, 则名称固定为: “注册终端”
关键字	记录命中策略中的关键字, 可能有多个
文件名称	事件涉及的文件名称, 可能有多个
浏览时长	访问该URL的时间, 默认每个页面算为20秒
是否安全	根据风险级别的结果记录, 风险级别为高、中、低, 显示为不安全; 风险级别为安全的情况下, 显示为安全;
URL安全级别	自定义的风险级别
病毒名称	访问的内容被病毒引擎发现的病毒名称
城市	根据IP的经纬度, 解析得到目标站点所在的城市
国家	根据IP的经纬度, 解析得到目标站点所在的国家
位置	目标IP所在的的经纬度
发送字节数	通过浏览器或其他方式访问网络发送的请求字节数
接收字节数	目标服务器对用户的响应字节数
总字节数	发送字节数和接收字节数的总和
应用类型	网络应用类型 应用类型目前包含浏览器、客户端、P2P、即时消息、流媒体应用类型5种。不在预置类型的, 默认为空
应用名称	应用程序的名称, 这些是厂家自身定义的

阻止类型	<p>动作被阻止的原因：阻止类型包含以下类型：</p> <ul style="list-style-type: none"> <li>• 黑名单阻止：因为命中了黑名单被阻止（全局策略）</li> <li>• URL阻止：因URL分类或自定义URL被阻止（策略）</li> <li>• 文件类型阻止：URL里因包含文件类型被阻止（策略）</li> <li>• 关键字阻止：URL里因包含关键字被阻止（策略）</li> <li>• 计时阻止：用户被分配了上网时间配额，上网配额被用完时被阻止（策略）</li> <li>• 安全威胁阻止：网页内容由于含有病毒、或者因为安全URL检测，发现包含木马等安全风险内容而被阻止。（比如：挂马，篡改网页，钓鱼、病毒等）</li> <li>• SSL事件阻止：因为访问的网站证书不合法被阻止(非策略动作，不用记录用户行为日志)</li> <li>• DLP阻止：因为用户的访问数据命中DLP策略，并且被阻止</li> </ul> <p> 注：阻止类型记录的优先级：黑名单 &gt; SSL事件阻止 &gt; 安全威胁（安全URL检测） &gt; 计时 &gt; 关键字 &gt; 文件类型 &gt; URL &gt; 安全威胁（病毒） &gt; DLP阻止</p>
来源Risk Level	用户行为所属的Risk Level(高危、危险、严重、普通和较低)
方法	HTTP请求的方法
响应码	HTTP响应码
Cloud App	Cloud App名称
Cloud App分类	Cloud App 所属分类
Cloud App 信任级别	Cloud App 的信任级别（由后台给出，用户不可更改）
Cloud App 分值	Cloud App 的信用分值
Referrer URL	记录当前页面的来源地址，即是由哪个页面定向过来的
User Agent	HTTP报文中UserAgent信息，比如浏览器类型、版本，操作系统类型、版本等
会话阶段	用户行为日志生成时所在的HTTP会话阶段

## 用户安全报告

介绍Web安全用户安全报告的相关信息。

### 简介

在报告 > SWG报告 > 用户安全报告页面管理用户安全报告。

用户安全报告用于统计某一段时间或某一个时间点的用户上网安全数据。

用户安全报告包括用户登录名、源IP、命中策略名称、完整URL和安全等级等信息，报告的类型包括列表报告、图表报告和趋势报告。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

## 图标和按钮

报告列表页面包含以下操作按钮。

表 52: 页面图标功能介绍



图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

## 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

点击报告名称进入报告页面，报告页面包含以下操作按钮。

表 53: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相信步骤信息。

## 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示用户安全图表报告支持的类型和对应解释。

表 54: 用户安全图表报告类型

报告类型	解释
风险网站-拦截数量排名	统计不同风险网站被拦截的数量，并排名前N位（最多显示30名）。
病毒-拦截数量排名	统计不同病毒被拦截的数量，并排名前N位（最多显示30名）。
威胁类型-拦截数量	统计不同威胁类型被拦截的数量，并排名前N位（最多显示30名）。

报告类型	解释
上网安全活动排名	统计不同上网安全活动的数量，并排名前N位（最多显示30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示用户安全趋势报告支持的类型和对应解释。

表 55: 用户安全趋势报告类型

报告类型	解释
病毒趋势	统计不同病毒被拦截的数量，并排名前N位（最多显示30名）。
威胁类型排名	统计不同威胁类型被拦截的数量，并排名前N位（最多显示30名）。
上网安全趋势	分别统计不同病毒和威胁类型被拦截的数量，并排名前N位（最多显示30名）。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 报告筛选条件/显示列

介绍适用的筛选条件/显示列。

下表罗列了适用的筛选条件/显示列，并逐条介绍其含义。

表 56: 筛选条件/显示列

筛选条件/显示列	解释
用户	<p>用户的显示名称，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）</p> <ol style="list-style-type: none"> <li>1. AD 中的用户的Display Name</li> <li>2. 自定义组织机构中的名称</li> <li>3. 其它的显示IP地址（DC Agent、Logon Agent、其它）</li> </ol>
登录名	<p>用于用户身份识别，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）：</p> <ol style="list-style-type: none"> <li>1. AD 中用户的Logon Name</li> <li>2. 自定义组织机构中的用户名</li> <li>3. DC Agent、Logon Agent 中的名称</li> <li>4. 其它为空</li> </ol>

唯一识别名	标识用户的唯一身份ID。 比如AD用户CN=haha,OU=QA,OU=R&D,OU=Staff,DC=skyguardmis,DC=com，或者DC Agent、Logon Agent中的FQDN名称
源IP	客户端IP地址
通道	事件所发生的通道或协议类型，比如 HTTP、HTTPS、FTP
动作	策略所对应的动作 动作包含：阻止、计时、提示、放行，每条策略只对应一个动作 动作优先级为：阻止 > 计时 > 提示 > 放行
域名	用户所在的域，可以为空
部门	用户所在的部门，可以为空
策略名称	事件命中的安全策略名称。 命中多个策略时，系统记录所有命中的策略名，包含内置的策略名称（策略名称是固定的）
URL分类	URL 所属的分类，比如：购物、IT等
URL风险类别	URL对应的风险类别
安全威胁类型	安全URL扫描的结果，比如挂马、网页篡改，或者内容扫描的病毒结果
文件类型	事件涉及的文件类型（扩展名、MIME TYPE），包含请求和应答中的文件类
URL主机名	用户访问的URL主机名，比如： <a href="http://www.skyguard.com.cn">www.skyguard.com.cn</a>
完整URL	完成的URL，包括协议和主机名 系统根据用户日志设置中的URL记录类型，决定是否记录部分或完整URL地址 设置方式：SWG管理 > 设置 > 日志设置 > URL记录方式  注：动作是阻止的访问，忽略此设置，始终记录完整的URL
目标IP	访问目标的IP地址，可能为空（原因是被阻止的请求，没有进行DNS解析）
端口	访问目标的端口号
设备名称	安全监控设备名称，如果是终端，则名称固定为：“注册终端”
关键字	记录命中策略中的关键字，可能有多个
文件名称	事件涉及的文件名称，可能有多个
浏览时长	访问该URL的时间，默认每个页面算为20秒
是否安全	根据风险级别的结果记录，风险级别为高、中、低，显示为不安全；风险级别为安全的情况下，显示为安全；
URL安全级别	自定义的风险级别
病毒名称	访问的内容被病毒引擎发现的病毒名称
城市	根据IP的经纬度，解析得到目标站点所在的城市

国家	根据IP的经纬度，解析得到目标站点所在的国家
位置	目标IP所在的的经纬度
发送字节数	通过浏览器或其他方式访问网络发送的请求字节数
接收字节数	目标服务器对用户的响应字节数
总字节数	发送字节数和接收字节数的总和
应用类型	网络应用类型 应用类型目前包含浏览器、客户端、P2P、即时消息、流媒体应用类型5种。不在预置类型的，默认为空
应用名称	应用程序的名称，这些是厂家自身定义的
阻止类型	<p>动作被阻止的原因：阻止类型包含以下类型：</p> <ul style="list-style-type: none"> <li>• 黑名单阻止：因为命中了黑名单被阻止（全局策略）</li> <li>• URL阻止：因URL分类或自定义URL被阻止（策略）</li> <li>• 文件类型阻止：URL里因包含文件类型被阻止（策略）</li> <li>• 关键字阻止：URL里因包含关键字被阻止（策略）</li> <li>• 计时阻止：用户被分配了上网时间配额，上网配额被用完时被阻止（策略）</li> <li>• 安全威胁阻止：网页内容由于含有病毒、或者因为安全URL检测，发现包含木马等安全风险内容而被阻止。（比如：挂马，篡改网页，钓鱼、病毒等）</li> <li>• SSL事件阻止：因为访问的网站证书不合法被阻止(非策略动作，不用记录用户行为日志)</li> <li>• DLP阻止：因为用户的访问数据命中DLP策略，并且被阻止</li> </ul> <p> 注：阻止类型记录的优先级：黑名单 &gt; SSL事件阻止 &gt; 安全威胁（安全URL检测） &gt; 计时 &gt; 关键字 &gt; 文件类型 &gt; URL &gt; 安全威胁（病毒） &gt; DLP阻止</p>
来源Risk Level	用户行为所属的Risk Level(高危、危险、严重、普通和较低)
方法	HTTP请求的方法
响应码	HTTP响应码
Cloud App	Cloud App名称
Cloud App分类	Cloud App 所属分类
Cloud App 信任级别	Cloud App 的信任级别（由后台给出，用户不可更改）
Cloud App 分值	Cloud App 的信用分值
Referrer URL	记录当前页面的来源地址，即是由哪个页面定向过来的
User Agent	HTTP报文中UserAgent信息，比如浏览器类型、版本，操作系统类型、版等
会话阶段	用户行为日志生成时所在的HTTP会话阶段

## 创建定时任务报告

### 如何创建定时任务报告

管理员可以定制任务报告，定期将其以邮件形式发送给指定的收件人。定制内容包括，报告类型（网络事件报告，数据发现报告，综合邮件报告等）、报告类型（列表，图标，趋势）和选择现有的报告等。

以下步骤描述了如何创建一个定时任务报告：

1. 选择报告 > 报告类型，在某一报告类型页面，比如 **DLP**报告 网络事件报告页面，点击右上角 定时任务报告链接。进入定时任务报告页面。
2. 点击添加按钮进入定时任务报告页面。
3. 输入名称和描述信息。
4. 在发送报告选项行，点击请选择图标，在弹出的选项框，选择报告的分类，类型等信息。点击保存。
5. 选择以什么文档格式发送报告，目前有PDF和Excel格式。
6. 勾选启用。
7. 在邮件设置部分设置邮箱相关信息。
8. 在任务定时计划部分设置执行周期。
9. 点击保存。

## Web安全设备监控

介绍Web安全设备监控的相关信息。

在监控 > 设备监控页面查看Web安全设备监控信息。

ASWG设备监控信息包括系统资源、服务状态和代理状态，并支持三种数据统计时段（1小时/24小时/7天）。

表 57: ASWG系统资源信息

系统资源	解释
设备信息统计	统计当前设备的基本信息，如主机名称、IP地址、系统类型、CPU、物理内存、硬盘容量和网卡数量等。
CPU资源利用率	统计当前设备CPU使用率，包括用户占用、系统占用和空闲的CPU的比例。
网卡资源利用率	统计当前网卡的发送和接收速率，以及总速率。
内存资源利用率	统计当前内存用于系统及应用、缓存的使用情况。
硬盘资源使用情况	统计系统硬盘和数据硬盘的使用情况。

表 58: ASWG服务状态信息

服务状态	解释
设备版本信息对比	当前UCSS作为基准设备，将注册设备各功能模块的版本信息与基准设备版本信息同步。可选同时同步或单独同步。
安全引擎负载统计	统计安全分析引擎(CAE)的负载状况。
请求数量统计	统计设备接收到的需要进行分析的请求数量。
命中事件统计	统计设备接收到的请求命中DLP策略产生事件的数量。
OCR引擎负载统计	统计OCR图像识别引擎的负载情况。
OCR队列状态统计	统计OCR图像识别引擎队列中等待分析和扫描超时的图片数量。



表 59: ASWG代理状态信息

ASWG代理状态		解释
连接状态	客户端并发连接数	当前客户端与设备并发的数量。
	活动客户端数	当前通过代理上网的客户端数量 ( 以IP客户端计算 ) 。
	使用过代理客户端数	从开始时间累计使用过代理的客户端IP数量 ( 连接过ATS的客户端 )
	关闭连接的客户端数	使用过代理的客户端数量 ( 活动客户端 ) 。
	当前客户端状态统计	统计当前使用代理的客户端最多的前10个IP。
	连接数量(CPS)统计	统计最大CPS、最小CPS、平均CPS和当前CPS。
	客户端并发	客户端访问代理服务器的并发数量。
	服务器并发	代理访问目标的并发数量。
	总并发数	客户端并发与服务器并发的总数。
HTTP	请求流量	客户端或服务端发起的HTTP请求流量累计值，服务重启后清零。
	响应流量	客户端或服务端发起的HTTP响应流量累计值，服务重启后清零。
	请求头流量	客户端或服务端发起的HTTP请求头流量累计值，服务重启后清零。
	响应头流量	客户端或服务端发起的HTTP响应头流量累计值，服务重启后清零。
	连接数量	客户端或服务端发起的HTTP连接数量累计值，服务重启后清零。
	当前连接数	客户端或服务端与代理服务器连接数量。
	客户端并发	客户端访问代理服务器的HTTP并发数量。
	服务器并发	代理访问目标的HTTP并发数量。
	总并发数	客户端并发与服务器并发的总数。
	发送带宽	客户端使用HTTP发送的字节数。
	总带宽	发送带宽和接收带宽的总字节数。
	带宽使用排名	统计带宽使用最多的前10或前5个带宽分类。
SSL	当前连接数量	客户端或服务端与代理服务器的当前连接数。
	请求完成数量	客户端或服务端与代理服务器成功建立握手的连接数量累计值，服务重启后清零。
	SSL Cache命中	客户端发起的SSL请求命中代理设备上的SSL缓存的数量累计值，服务重启后清零。
	SSL Cache未命中	客户端发起的SSL请求没有命中代理设备上的SSL缓存的数量累计值，服务重启后清零。

ASWG代理状态	解释	
	SSL Cache超时	代理设备查询SSL缓存超时的数量累计值，服务重启后清零。
	CRL证书数量	代理设备上证书吊销列表上的证书数量。
	OCSP有效证书数量	代理设备上可以被验证有效的证书数量。
	OCSP未验证证书数量	代理设备上不可以被验证有效的证书数量
	OCSP撤销证书数量	代理设备上已经被吊销的证书数量。
	客户端并发	客户端访问代理服务器的SSL并发数量。
	服务器并发	代理访问目标的SSL并发数量。
	总并发数	客户端并发与服务器并发的总数。
	发送带宽	客户端使用SSL发送的字节数。
	接收带宽	客户端使用SSL接收的字节数。
	总带宽	发送带宽和接收带宽的总字节数。
FTP	连接数量	客户端或服务器与代理间建立过的连接数量累计值，服务重启后清零。
	当前连接数	客户端或服务器与代理当前建立连接的数量。
	发送字节	客户端或服务器发送的字节数量累计值，服务重启后清零。
	接收字节	客户端或服务器接收的字节数量累计值，服务重启后清零。
	客户端并发	客户端访问代理服务器的FTP并发数量。
	服务器并发	代理访问目标的FTP并发数量。
	总并发数	客户端并发和服务器并发数量。
	发送带宽	客户端使用FTP发送的字节数。
	接收带宽	客户端使用FTP接收的字节数。
	总带宽	发送带宽和接收带宽的总字节数。
SOCKS	当前连接数量	客户端或服务器端与代理服务器之间的当前SOCKS连接数。
	总连接数量	客户端或服务器端与代理服务器之间的SOCKS连接数累计值，服务重启后清零，数据为通过SOCKS Tunnel转入HTTP的连接数。
	成功连接数量	客户端或服务器与代理设备连接建立成功的SOCKS的连接数。
	失败连接数量	客户端或服务器与代理设备连接建立失败的SOCKS的连接数。
	客户端并发	客户端访问代理服务器的SOCKS并发数量。
	服务器并发	代理访问目标的SOCKS并发数量。
	总并发数	客户端并发与服务器并发的总数。

ASWG代理状态		解释
	发送带宽	客户端使用SOCKS发送的字节数。
	接收带宽	客户端使用SOCKS接收的字节数。
	总带宽	发送带宽和接收带宽的总字节数。
DNS	解析总次数	设备收到的所有DNS请求次数 ( 成功和失败 ) 的累计值, 服务重启后清零。
	解析成功次数	设备对收到的DNS解析成功的次数累计值, 服务重启后清零。
	解析失败次数	设备对收到的DNS解析失败的次数累计值, 服务重启后清零。
	平均解析时间	设备对收到的DNS解析平均时长 ( 解析总时长除以解析总次数 ) 。
	DNS Hostdb查询次数	设备查询Hostdb的次数 ( 成功和失败 ) 累计值, 服务重启后清零。
	DNS Hostdb命中次数	设备查询Hostdb命中的次数累计值, 服务重启后清零。
	DNS Hostdb平均TTL	设备查询Hostdb的平均TTL。
WCCP	WCCP统计	统计自定义WCCP的规则名称、状态、ID、路由器ID、发送数据包和接收数据包数量。
ICAP	阻止请求	发给ICAP Server后被阻止的所有数据, 包括大文件阻断、异常阻断和ICAP Server阻断的请求数量总和。
	放行请求	通过ASWG的ICAP Clients发送的所有被放行的请求, 包括异常放行和ICAP Server检查后安全放行。
	失败请求	所有请求失败的数据, 包括异常阻断、超时和ICAP Sever阻断的请求数量总和。
	超大请求	超过超大传输大小的请求数量。
	解密请求	HTTPS解密成功后转给ICAP Sever的请求数量。
	发送POST	统计发送的POST请求数量。
	分析POST	统计分析的POST请求的数量。
	客户端并发	浏览器与ASWG的ICAP Client建立连接的数量 ( 目前不区分协议, 包含所有协议的连接总数量 ) 。
	服务端并发	ASWG的ICAP Client与ICAP Server间的所有连接。
	总并发	客户端并发与服务端并发总数。
缓存	缓存空间大小	缓存占用磁盘空间的总大小。
	已使用缓存	已使用的缓存空间大小。
	缓存对象	缓存中保存的对象个数。
	缓存命中	用户请求命中缓存的次数累计值, 服务重启后清零。

ASWG代理状态		解释
	缓存未命中	用户请求未命中缓存的次数累计值，服务重启后清零。
认证状态	认证服务器	认证服务器名称。
	类型	认证服务器类型，比如LDAP、Windows集成、自定义等。
	缓存用户数量	在当前认证服务器上缓存的认证用户数。
	认证成功（次）	认证服务器上认证成功的次数累计值，服务重启后清零。
	认证失败（次）	认证服务器上认证失败的次数累计值，服务重启后清零。
带宽	带宽分类	自定义的带宽分类。
	当前带宽速率	当前的数据传输速率。
	流量类型	流出或流入ASWG设备的流量。
	字节	带宽传输的字节数。
	带宽使用排名	统计带宽使用最多的前10或前5个带宽分类

## Web安全管理

管理注册于UCSS的Web安全设备。

管理注册于UCSS的Web安全设备的功能、配置，以及设备、服务的启动、停止和重启等操作。Web安全设备目前支持的设备有ASWG。

### 设备

配置设备相关的选项页面。

该菜单包含设备相关的选项页面。

#### 系统信息

介绍设备的系统信息界面。

系统信息包括设备的基本信息和服务状态信息。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 系统信息菜单。

系统信息页面支持查看以下信息。

#### 设备信息

设备信息包括主机名称，IP地址，系统类型等只读的信息。

在此栏中，可以一键重启或关闭设备。

#### 系统信息

系统信息包括系统负载状态和各种系统服务的运行状态。

参考[系统服务介绍](#)，可以获得各种系统服务的基本介绍。

在此栏中，可以选择对某项服务进行重启、停止或启动，或对所有服务进行批量操作。

## ASWG基本设置

介绍配置ASWG基本设置的步骤。

在系统 > 设备管理页面进行ASWG的基本设置。

ASWG基本设置包括设备工作模式、安全模式和同步设置。


1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 基本设置，对ASWG进行基本配置。
2. 选择是否启用该设备，默认开启。
3. 输入设备名称和描述，说明其用途。
4. 选择ASWG的分析引擎：

本机内容分析	使用内置的分析引擎，可以进行内容分析和安全扫描功能。
第三方内容分析	需要开启ICAP客户端配置，会将数据传送给第三方的ICAP服务器。

5. 选择ASWG的工作模式：

代理模式	通过指定代理或透明代理方式检测流量，对网络流量进行监控或阻断等控制。
旁路监控模式	通过连接在网络设备的SPAN口将镜像的流量还原分析，仅支持审计功能。
串行模式	串行于企业内网与外网之间的链路并对流量进行监控、阻止和检测。

6. 设置不同安全级别下的引擎和透传对应的安全模式。
7. 选择手动或自动设置时间，自动从配置的时间服务器同步时间，需输入时间服务器域名。
8. 设置重定向主机，将需要重定向的URL（如认证页面、证书验证页面、策略的提示和计时页面）中的主机名/IP重定向到指定主机名/IP（请确保主机名可以被DNS解析）。
9. 点击保存,设置生效。

 注：高级设置请务必在在天空卫士™技术支持工程师的指导下修改。

## 授权许可

介绍如何管理设备的授权许可设置。

在系统 > 设备管理页面进行设备授权许可。

1. 选择系统 > 设备管理进入设备管理页面。点击要查看的设备，进入设备 > 授权许可页面。
2. 选择以下授权方式：

项目	描述
授权码	在线授权需输入授权码。
授权文件	离线授权需上传授权文件。


授权成功后，在当前页面显示授权信息如下：

表 60: 当前授权状态

设备编号	显示当前设备编号
授权号	显示当前设备所使用的授权号。

用户名称	显示License授予时的用户名称，一般为企业名称。
工作模式	显示当前设备工作模式，支持阻断和审计。
授权类型	显示授权类型，包括正式版本和测试版本。
功能模块列表	显示授权的功能模块，每个功能模块的已授权数量，当前状态和使用的有效期。

3. 点击保存，设置生效。

 提示：点击下载设备ID可下载设备ID信息为记事本格式，查询和授权License时可以使用该文件。

## 网络

配置网络相关的选项页面。






该菜单包含网络相关的选项页面。

### ASWG网卡配置

介绍ASWG网卡配置的步骤。

在系统 > 设备管理页面配置ASWG网卡。


ASWG设备的网卡包括Mgmt负责管理设备，MTA提供邮件服务，P1和P2提供代理服务。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 网络 > 网卡配置页面。
2. 在网卡信息显示列表，点击  查看Mgmt网卡的配置信息。
3. 点击  编辑MTA、P1和P2的网卡设置，可更改网卡的IP地址、子网掩码和适配模式，Mgmt网卡不可编辑。  
 注：在串行模式下，网卡P1和P2显示为Br0，提供桥接服务。
4. 点击确定，网卡设置完成。
5. 选择设备网卡并输入网卡的默认网关。
6. 输入DNS服务器IP，点击  添加于列表；点击  删除列表中所选的DNS服务器。
7. 设置重定向主机，将需要重定向的URL（如认证页面、证书验证页面、策略的提示和计时页面）中的主机名/IP重定向到指定主机名/IP（请确保主机名可以被DNS解析）。
8. 点击保存，设置生效。

### 路由设置

介绍管理路由设置的步骤。




在系统 > 设备管理页面设置路由。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 网络 > 路由页面。
2. 点击  添加静态路由或策略路由：

静态路由	添加静态路由到主路由表中，不对源IP做限制，所有从本设备发起或者转发的数据包都将遵循此路由规则。
策略路由	只有本设备发起的数据包匹配此规则。

3. 输入目标网络IP地址、子掩码和网关（网关需要跟选中网卡的地址在同一个子网内）。
4. 选择网卡类型：Mgmt负责管理设备，MTA提供邮件服务，P1和P2提供代理服务（仅ASWG设备），Br0提供桥接服务（仅UCSG-DSG设备）。
5. 点击确认，添加路由到列表中。
6. 点击保存，设置生效。

表 61: 页面图标和行间操作按钮功能

	导出路由配置。
	导入路由配置。
	删除所选路由。

### 网卡绑定


介绍配置网卡绑定设置的步骤。

在系统 > 设备管理页面选择您需要管理的设备后进行网卡绑定设置。

网卡绑定功能将两个或者更多的物理网卡绑定成一个虚拟网卡，以提供负载均衡或者冗余。

1. 选择系统 > 设备管理进入设备管理页面。
2. 点击要查看的设备。
3. 点击进入网络 > 网卡绑定页面

网卡绑定页面支持对以下参数进行修改和设置：

字段	解释
网卡管理	选择要绑定的网卡。
网卡绑定状态	滑动状态条开启网卡绑定。
工作模式	<ul style="list-style-type: none"> <li>• Active-Standby模式：主备方式，当一个网卡故障时另一个网卡接管所有工作。</li> <li>• Active-Active模式：双活方式，两个网卡同时工作，增加带宽的同时实现冗余。需要交换机支持聚合功能。</li> </ul> <p> 注：Bypass 网卡仅支持 Active-Active 模式。</p>

## 功能

配置功能相关的选项页面。

该菜单包含功能相关的选项页面。

### 代理服务

介绍设置SWG代理服务的步骤。

ASWG设备支持配置各种代理服务，用于设置在特定IP和端口处理通过显式代理 或者透明代理或者反向代理方式转发到ASWG设备上的特定协议的流量（比如：HTTP、HTTPS、FTP等协议）；

代理服务页面采用列表的方式管理SWG支持的代理服务相关基本操作，包括增加，删除，修改，查询，搜索，排序以及启用和通用代理服务等功能。

ASWG支持HTTP、FTP、POP3、IMAP、SMTP、SMB协议和自定义协议，通过配置各种代理协议的内容分析和安全分析项，检测并分析用户的访问内容或访问请求。

代理服务器列表可以包含以下筛选项，名称，状态，描述，协议，代理类型和监听IP或端口。

系统预制代理服务如下表所示。


表 62: 预制代理服务器

名称	状态	描述	代理类型	协议	监听IP或端口
HTTPS透明代理	不启用	HTTPS透明代理服务	透明代理	HTTPS	443
HTTP显式代理	启用	HTTP显式代理服务	显式代理	HTTP	0.0.0.0:8080
HTTP透明代理	不启用	HTTP透明代理服务	透明代理	HTTP	80

### 进入代理服务配置页面

按照以下步骤进入代理服务配置页面。

1. 选择系统 > 设备管理进入设备管理的总页面。
2. 点击要查看的设备，进入该设备的设备管理页面。
3. 点击设备 > 功能 > 代理服务进入代理服务设置页面。
4. 将鼠标移至添加按钮系统将显示设备支持的代理服务。

或点击  对现有的代理进行编辑。

### HTTP协议配置


介绍HTTP协议配置的步骤。

选择HTTP协议，进入代理服务编辑页面。配置以下信息。


#### 基本信息


配置以下协议的基本信息。

1. 名称 - 注意填写区别于其他条目的名称。

 注：名称支持中英文，数字，以及部分特殊符号，输入系统不支持的特殊符号将导致策略保存失败。

2. 描述 - 需说明其用途。

 提示：描述需包含安全管理员对条目进行长期管理所需的必要信息。


 注：不能与现有或内置的条目名称相同。

3. 启用状态 - 是否启用该项目。
4. 代理类型 - 选择需要配置的代理类型。

选择以下代理模式：

显式代理	输入显示代理的IP与端口号，默认IP与端口号为0.0.0.0:8080。输入在显式代理模式下，允许通过HTTP请求的端口号、允许通过Connect请求的端口号和Connect透传端口。
透明代理	输入HTTP透明代理端口号，不能和其它协议的显示代理端口重复。
反向代理	选择反向代理的主机组，输入提供反向代理服务的IP与端口号，默认值为空。配置参数不能与其他协议相同。

5. 输入类型所对应的端口号。

 重要：务必确认该端口未被其他协议占用。

以下表格列出了显示代理和透明代理下用于HTTP协议的默认端口。



协议	显示代理	透明代理
HTTP	8080	80
FTP	2120	21

## 基本设置



基本选项卡支持以下设置。

- 仅允许HTTP端口 - 设置在仅允许HTTP端口。在显式代理模式下，该端口仅允许HTTP请求，其他请求将被阻断。

### 提示:

- 当设置“仅允许HTTP端口”为“所有”，则客户端以HTTP方式访问目标域名端口为\*\*\*\*的请求时，可以成功代理。
- 当设置“仅允许HTTP端口”为某一具体的端口号，则客户端以HTTP方式访问目标域名中的该端口号请求时，系统可以成功代理此请求；如果客户端以HTTP方式访问目标域名中的其他端口的请求时，系统将无法代理此请求。
- 允许Connect端口 - 设置允许Connect端口。在显式代理模式下，该端口允许Connect请求，其他端口拒绝接受Connect请求。


### 注:

- 当设置“允许Connect端口”为所有时，ASWG设备可以代理客户端向目标服务任意端口的connect请求。
- 当设置“允许Connect端口”为指定端口时，ASWG系统只可以代理客户端向目标服务指定端口的connect请求。
- Connect透传端口 - 设置Connect透传端口。在显式代理模式下，透传对该端口的Connect请求。
  -  提示: 当设置“Connect透传端口”为指定端口时，ASWG设备将不代理客户端向目标服务指定端口的connect请求，而是直接转发到服务器而是直接转发到服务器。
  -  重要: 请确保“Connect透传端口”属于“允许Connect端口”的子集。
- 仅发送HTTP1.1请求 - 选择是否启用仅发送HTTP1.1请求。启用功能后，代理服务器将发送HTTP1.1与目标服务器进行通信。
- 域名扩展 - 选择是否启用域名扩展。启用功能后，当请求地址为非域名时，如domain，代理服务器自动补充www.和.com，即请求www.domain.com。

## FTP over HTTP

按照以下步骤配置FTP over HTTP设置。

1. 设置匿名用户密码（默认为“空”）。

 注: 当客户端通过HTTP方式访问FTP资源时，系统可使用该密码匿名登录FTP服务器。

2. 选择传输模式，支持先被动模式、仅主动模式和仅被动模式三种模式。
3. 设置连接FTP服务器后无访问请求的时限，超时后会断开连接。

## 隐私

按照以下步骤配置隐私设置。

1. 选择插入的header类型，支持插入Via和X-Forward-For。
2. 选择移除的header类型，支持移除客户端IP、Cookie、From、Referer、User-Agent或自定义。

## 超时

按照以下步骤配置超时设置。

1. 分别设置代理服务器与客户端、目标服务器的Keep-Alive超时时限，超时时断开连接。
2. 分别设置代理服务器与客户端、目标服务器的无活动Inactivity超时时限，超时时断开连接。
3. 分别设置代理服务器与客户端、目标服务器的活动Activity超时时限，超时时断开连接。
4. 设置代理服务器等待目标服务器响应时限，超时时断开连接。

## 内容分析

按照以下步骤配置内容分析设置。

1. 滑动状态条，开启内容分析功能。
2. 配置检测内容的最小字节数。

**Ⓡ** 切记：检测内容字节数允许修改，但请注意系统将不对少于此字节数的内容进行安全检测。

3. 选择工作模式。
  - 监控：当请求的内容违反数据防泄漏DLP策略，系统将记录违规事件，但是用户仍然可以正常进行HTTP访问。
  - 阻断：当请求的内容违反数据防泄漏DLP策略，系统将记录违规事件，同时，用户的访问请求将被阻断。
4. 选择当请求或响应被策略阻断时，显示默认提示页面或定向到公司自定义阻断提示网页。
5. 选择来源、目标和分析内容。根据用户定义的网段范围对用户的访问进行内容分析。

## 安全分析

按照以下步骤配置安全分析设置。

1. 滑动状态条，开启安全分析功能。
2. 配置检测内容的最小字节数。

**Ⓡ** 切记：检测内容字节数允许修改，但请注意系统将不对少于此字节数的内容进行安全检测。

3. 选择工作模式为监控或阻断。监控模式下用户的HTTP访问不受安全分析的结果影响。
4. 选择当请求或响应被策略阻断时，显示默认提示页面或定向到公司自定义阻断提示网页。
5. 分别选择来源、目标和分析内容。根据用户定义的网段范围对用户的访问进行安全分析。

## 应用配置


按照以下步骤保存和应用您的配置。

1. 点击保存，配置完成。
2. 点击重启服务，重启后配置生效。

## HTTPS协议配置

介绍HTTPS协议配置的步骤。

1. 选择HTTPS协议，进入代理服务编辑页面。
2. 点击基本选项卡，滑动状态条选择开启或关闭HTTP协议。开启后，如果在旁路模式和串联模式下，配置端口号；如果在代理模式下选择以下代理模式：

透明代理	输入HTTPS透明代理端口号。用于设置对外提供显示代理服务的端口，不能和其它协议的显示代理端口重复。
反向代理	输入提供反向代理服务的IP与端口号，点击  添加到列表，默认值为空。配置参数不能与其他协议相同。

- a) 选择入站的客户端与代理服务器进行加密连接所使用的协议版本和加密算法的强度。
- b) 选择出站的代理服务器与目标服务器进行加密连接所使用的协议版本和加密算法的强度。
3. 点击内容分析选项卡，选择是否开启内容分析，开启后进行如下配置：
  - a) 配置检测内容的最小字节数，少于此字节数不检测。
  - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受内容分析的结果影响。
  - c) 选择被策略阻断时显示默认阻断页或定向到公司自定义阻断提示网页。
  - d) 选择来源、目标和分析内容。根据用户定义的网段范围对用户Web访问的请求、响应进行内容分析。
4. 点击安全分析选项卡，选择是否开启安全分析，开启后进行如下配置：
  - a) 配置检测的最小字节数，少于此字节数的内容不被检测。
  - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受安全分析的结果影响。
  - c) 选择被策略阻断时显示默认阻断页或定向到公司自定义阻断提示网页。
  - d) 选择来源、目标和分析内容。根据用户定义的网段范围对用户Web访问的请求或响应进行安全分析。
5. 点击保存，设置生效。

### FTP协议配置

介绍FTP协议配置的步骤。

#### 基本信息

配置以下协议的基本信息。

1. 名称 - 注意填写区别于其他条目的名称。



注：名称支持中英文，数字，以及部分特殊符号，输入系统不支持的特殊符号将导致策略保存失败。

2. 描述 - 需说明其用途。



提示：描述需包含安全管理员对条目进行长期管理所需的必要信息。



注：不能与现有或内置的条目名称相同。

3. 启用状态 - 是否启用该项目。
4. 代理类型 - 选择需要配置的代理类型。

选择以下代理模式：

显式代理	输入显示代理的IP与端口号，默认IP与端口号为0.0.0.0:8080。输入在显式代理模式下，允许通过HTTP请求的端口号、允许通过Connect请求的端口号和Connect透传端口。
透明代理	输入HTTP透明代理端口号，不能和其它协议的显示代理端口重复。
反向代理	选择反向代理的主机组，输入提供反向代理服务的IP与端口号，默认值为空。配置参数不能与其他协议相同。

5. 输入类型所对应的端口号。



重要：务必确认该端口未被其他协议占用。

以下表格列出了显示代理和透明代理下用于HTTP协议的默认端口。

协议	显示代理	透明代理
HTTP	8080	80
FTP	2120	21

## 基本设置

1. 设置FTP代理服务器的欢迎信息。
2. 选择是否启用共享连接。启用后，多个匿名FTP客户端可共享服务器连接。
3. 选择代理建立连接的模式为主动模式或被动模式。
4. 选择数据的传输端口为默认（由操作系统选择端口）或指定端口范围（系统只监听指定范围内的端口）。

## 隐私

按照以下步骤配置隐私设置。

1. 选择插入的header类型，支持插入Via和X-Forward-For。
2. 选择移除的header类型，支持移除客户端IP、Cookie、From、Referer、User-Agent或自定义。

## 超时

按照以下步骤配置超时设置。

1. 分别设置代理服务器与客户端、目标服务器的Keep-Alive超时时限，超时后断开连接。
2. 分别设置代理服务器与客户端、目标服务器的无活动Inactivity超时时限，超时后断开连接。
3. 分别设置代理服务器与客户端、目标服务器的活动Activity超时时限，超时后断开连接。
4. 设置代理服务器等待目标服务器响应时限，超时后断开连接。

## 内容分析

按照以下步骤配置内容分析设置。

1. 滑动状态条，开启内容分析功能。
2. 配置检测内容的最小字节数。  
R 切记：检测内容字节数允许修改，但请注意系统将不对少于此字节数的内容进行安全检测。
3. 选择工作模式。
  - 监控：当请求的内容违反数据防泄漏DLP策略，系统将记录违规事件，但是用户仍然可以正常进行HTTP访问。
  - 阻断：当请求的内容违反数据防泄漏DLP策略，系统将记录违规事件，同时，用户的访问请求将被阻断。
4. 选择当请求或响应被策略阻断时，显示默认提示页面或定向到公司自定义阻断提示网页。
5. 选择来源、目标和分析内容。根据用户定义的网段范围对用户的访问进行内容分析。

## 安全分析

按照以下步骤配置安全分析设置。

1. 滑动状态条，开启安全分析功能。
2. 配置检测内容的最小字节数。  
R 切记：检测内容字节数允许修改，但请注意系统将不对少于此字节数的内容进行安全检测。
3. 选择工作模式为监控或阻断。监控模式下用户的HTTP访问不受安全分析的结果影响。
4. 选择当请求或响应被策略阻断时，显示默认提示页面或定向到公司自定义阻断提示网页。
5. 分别选择来源、目标和分析内容。根据用户定义的网段范围对用户的访问进行安全分析。

## 应用配置

按照以下步骤保存和应用您的配置。

1. 点击保存，配置完成。


2. 点击重启服务，重启后配置生效。







### SMTP协议配置

介绍ASWG SMTP协议在Proxy接入模式下的配置步骤。

在ASWG为代理模式下以Proxy接入时，按照以下步骤配置ASWG SMTP协议。

1. 选择SMTP，进入SMTP协议代理服务编辑页面。
2. 点击基本选项卡，开启或关闭协议分析。开启后进行如下配置：
  - a) 选择协议接入方式为SMTP Proxy。
  - b) 配置透传代理端口，端口与协议相对应并作相应的流量处理。
  - c) 启用SMTP加密支持功能。启用SMTP加密支持功能后需配置加密端口号。


 注：在旁路模式和串联模式下，接入方式为SMTP监控，而没有SMTP Proxy,此时只需配置端口号。

3. 选择是否启用SMTP加密支持。
  4. 点击内部域名选项卡：
    - a) 输入公司内部域名，用来区分邮件方向，点击 添加到列表。
    - b) 选择需要分析的邮件方向。
    - c) 添加不需要检测的邮件来源邮箱地址和域名，点击 添加到列表。点击 可删除所选来源。
  5. 点击内容分析选项卡，选择是否开启内容分析，开启后进行如下配置：
    - a) 配置检测内容的最小字节数，少于此字节数的内容不检测。
    - b) 选择工作模式为监控或阻断。
      -  提示：监控模式下用户的Web访问不受内容分析的结果影响。
    - c) 选择来源、目标和分析内容。根据用户定义的网段范围对用户SMTP Proxy访问的发送邮件进行内容分析。
    - d) 选择是否开启自动识别邮件服务器，开启后作如下配置：
      1. 选择是否启用全邮件记录，即可记录全部邮件原文。
      2. 指定MTA投递邮件的下一跳，可以选择DNS解析投递也可设置指定接收地址。如果开启高级邮件路由，则高级路由中配置的投递地址优先级最高。
      3. 选择TLS传输安全机制为强制明文、自适应或强制TLS。
      4. 选择是否开启高级路由，可以指定DNS，定向投递。
        -  提示：配置路由时可以设置优先级，如果同一个域名定义了多个邮件路由而对应多个服务器IP地址，系统会尝试按照路由的优先级来发送邮件。当多条路由的优先级相同时，系统会使用轮询发送机制。
    5. 选择是否发送邮件退信，可选择退信收件人为源发件人或指定收件人。
    6. 选择是否添加邮件声明，可自定义邮件声明，表明邮件已经过检测等。
    7. 设置加密邮件的网关的主机名/IP和端口号。
      -  提示：支持设置加密标识，主体加密标识用户可见，X-Header加密标识用于服务器解析。
6. 点击安全分析选项卡，选择是否开启安全分析，开启后进行如下配置：
  - a) 配置检测的最小字节数，少于此字节数不检测。
  - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受安全分析的结果影响。
  - c) 选择被策略阻断时显示默认阻断页或定向到公司自定义阻断提示网页。
  - d) 选择来源、目标和分析内容。根据用户定义的网段范围对用户SMTP Proxy访问的发送邮件进行内容分析。
7. 点击保存,设置生效。

### POP3协议配置

介绍POP3协议配置的步骤。

1. 选择POP3协议，进入代理服务编辑页面。
2. 点击基本选项卡，滑动状态条选择开启或关闭协议。开启后，如果在旁路模式和串联模式下，配置端口号；如果在代理模式下选择以下代理模式：


透明代理	输入HTTPS透明代理端口号。用于设置对外提供显示代理服务的端口，不能和其它协议的显示代理端口重复。
反向代理	输入提供反向代理服务的IP与端口号，点击  添加到列表，默认值为空。配置参数不能与其他协议相同。

- a) 选择是否启用POP3加密支持功能，启用后需配置加密端口号。
3. 点击内容分析选项卡，选择是否开启内容分析，开启后进行如下配置：
    - a) 配置检测内容的最小字节数，少于此字节数不检测。
    - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受内容分析的结果影响。
    - c) 选择来源、目标和分析内容。根据用户定义的网段范围对用户POP3访问的接收邮件进行内容分析。
  4. 点击安全分析选项卡，选择是否开启安全分析，开启后进行如下配置：
    - a) 配置检测的最小字节数，少于此字节数不检测。
    - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受安全分析的结果影响。
    - c) 选择来源、目标和分析内容。根据用户定义的网段范围对用户POP3访问的接收邮件进行内容分析。
  5. 点击保存，设置生效。

#### IMAP协议配置

介绍IMAP协议配置的步骤。

1. 选择IMAP协议，进入代理服务编辑页面。
2. 点击基本选项卡，滑动状态条选择开启或关闭协议。开启后，如果在旁路模式和串联模式下，配置端口号；如果在代理模式下选择以下代理模式：

透明代理	输入HTTPS透明代理端口号。用于设置对外提供显示代理服务的端口，不能和其它协议的显示代理端口重复。
反向代理	输入提供反向代理服务的IP与端口号，点击  添加到列表，默认值为空。配置参数不能与其他协议相同。

- a) 选择是否启用IMAP加密支持功能，启用后需配置加密端口号。
3. 点击内容分析选项卡，选择是否开启内容分析，开启后进行如下配置：
    - a) 配置检测内容的最小字节数，少于此字节数不检测。
    - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受内容分析的结果影响。
    - c) 选择来源、目标和分析内容。根据用户定义的网段范围对用户IMAP访问的接收邮件进行内容分析。
  4. 点击安全分析选项卡，选择是否开启安全分析，开启后进行如下配置：
    - a) 配置检测的最小字节数，少于此字节数不检测。
    - b) 选择工作模式为监控或阻断。监控模式下用户的Web访问不受安全分析的结果影响。
    - c) 选择来源、目标和分析内容。根据用户定义的网段范围对用户IMAP访问的接收邮件进行内容分析。
  5. 点击保存，设置生效。

#### 主机/主机组

介绍设置主机/主机组功能的步骤。

主机/主机组功能支持在开启反向代理的情况下，及时获取主机设备的健康状态等运行状况以及多台设备之间的流量负载均衡。

主机功能支持ASWG可以获取代理主机的健康状态，从而及时的将有故障的主机，以报警或日志的方式进行记录，从而方便管理员了解代理的运行情况。

主机组功能则针对多台主机提供相同服务的情况，ASWG可以以主机组的方式管理这些主机。可以设置这些主机处理流量的负载方式，以达到负载均衡。

## 主机

主机功能支持以发送ping包进行网络连接状况探测的方式，获取主机设备的健康状态。

- 探测包将按照设置的间隔时间进行发送。
- 在设定的响应时间范围内收到主机的一次响应，就认为主机处于健康状态，如超时后仍没有响应，则判断主机处于宕机状态。
- 系统将宕机状态下的主机通过通知和告警等方式告知安全管理员。

## 主机组

主机组功能支持在反向代理的情况下，设置多台主机设备之间的负载均衡方式，以确保在大流量通信的情况下，后台服务器设备能够正常提供服务。

安全管理员可以在负载均衡选项框设置用户请求的分流方式，并通过设置会话保持，在处理负载均衡时，将同一用户的多个连接保持在一台主机上处理。

系统支持以下负载方法：

- 轮询方式（Round Robin）：即由系统随机选择一台主机来处理用户请求。
- 最少连接（Least Connection）：即由系统统计和判定，选择当前连接数最少的主机来处理用户请求。

系统支持以下会话保持方法：

- 不支持（None）：主机不支持会话保持
- 客户端IP（Client IP）：同一客户的IP连接保持在一台主机上处理。


## ICAP功能

介绍设置ICAP功能的步骤。

在系统 > 设备管理页面设置ICAP功能。

ASWG设备可以作为ICAP Server 接收第三方的HTTP、HTTPS数据进行DLP内容分析；ASWG设备也可作为ICAP Client，将HTTP、HTTPS数据转给第三方的ICAP Server进行处理。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备。
2. 进入设备 > 功能 > ICAP页面，设置ICAP功能。
3. 点击客户端选项卡，滑动状态条开启或关闭ICAP客户端功能。开启后做如下配置：
  - a) 输入ICAP服务器URI。点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
  - b) 设置用户请求处理超时时间，超过此时间后将返回超时提示页面。
  - c) 设置向ICAP服务器发送请求的最大并发数量。
  - d) 选择是否启用连接异常阻断。启用后，当代理服务器与ICAP服务器连接失败或出现错误时，阻断所有请求。
  - e) 选择是否启用阻断大文件。启用后，通过代理服务器的请求如果包含大文件，将会被阻断。
  - f) 选择分析的协议（HTTP或HTTPS），代理服务器会分析该协议数据。
4. 点击服务器选项卡，滑动状态条开启或关闭ICAP服务器功能。开启后做如下配置：
  - a) 设置代理服务器提供ICAP服务的端口，以处理第三方转给代理服务器的HTTP、HTTPS流量。
  - b) 选择ICAP服务器的工作模式为监控模式和阻断模式。在阻断模式下，当数据被策略阻断时可选择显示默认提示页面或定向到公司自定义阻断提示网页；当发生错误（如系统连接错误或文件错误）时，可以选择放行或阻断（可由数据的安全性判断是否放行）。
  - c) 配置检测的最小字节数，少于此字节数不检测。

d) 设置发送数据的来源IP，可选接收任何IP发送的数据，或只接收指定IP发送的数据。添加指定IP时，输入指定IP地址，点击添加到列表中。

5. 点击保存，设置生效。



注：在所应用的ASWG策略中启用内容分析后，ICAP才会将HTTP、HTTPS的数据送给本机ICAP Server或者第三方的ICAP server。

## WCCP功能

介绍设置WCCP功能的步骤。

在系统 > 设备管理页面设置WCCP功能。

WCCP为网页缓存通信协议，用户通过开启路由器的WCCP功能将HTTP、HTTPS的流量透明转发到代理服务器。






1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 协议页面，设置WCCP。
2. 滑动状态条开启或关闭WCCP功能。开启后，点击，添加WCCP规则。
3. 点击基本配置选项卡，进行如下配置：
  - a) 输入WCCP协议的规则名称，说明其用途。
  - b) 选择是否启用该规则。
  - c) 设置该WCCP服务规则ID（自定义）。
  - d) 设置该WCCP服务规则的优先级。
  - e) 选择传输协议UDP或TCP。
  - f) 配置协议及端口，支持来源端口、目标端口设置与协议相对应并作相应的流量处理。
  - g) 选择用于路由器通信的网卡。
  - h) 选择转包方式。路由器发送包给ASWG代理的转包方式包括GRE和L2。GRE用于缓存服务器与路由器的跨网络连接，而L2用于缓存服务器与路由器的直连网络。
  - i) 选择回包方式。ASWG代理发送包给路由器的回包方式包括GRE和L2。GRE用于缓存服务器与路由器的跨网络连接，而L2用于缓存服务器与路由器的直连网络。
  - j) 选择是否启用路由安全密钥。开启后，设置ASWG代理与路由器通信密码。
  - k) 点击添加WCCP路由，配置路由器IP地址、内部网络（企业内网）、本地GRE隧道IP、掩码和下一跳的路由地址。
4. 点击高级配置选项卡，进行如下配置：
  - a) 选择路由器分发流量到多个代理服务器的方式，可选HASH或MASK。
  - b) 选择多个代理服务器进行负载均衡的分配依据，包括目标IP、来源IP、目标端口和源端口。
  - c) 配置多个代理服务器的负载均衡权重，数值越大权重越高，代理服务器的处理效率越高。
5. 点击保存，规则添加成功。
6. 再次点击保存，设置生效。

表 63: 页面图标和行间操作按钮功能

	禁用所选WCCP规则。
	启用所选WCCP规则。
	删除所选WCCP规则。



## 网络对象

介绍设置网络对象功能的步骤。

在系统 > 设备管理页面设置网络对象功能。

在设置协议时可直接引用网络对象，过滤出需要检测的流量或过滤掉不需要检测的流量。



1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 网络对象页面。
2. 点击添加，新建网络对象。
3. 输入网络对象名称。
4. 输入网络对象包含的IP或IP段，点击  添加到列表。
5. 输入排除在网络对象外的IP或IP段，点击  添加到列表。
6. 点击确定，添加成功。

表 64: 页面图标和行间操作按钮功能


	修改网络对象。
	删除所选网络对象。


## 带宽管理

介绍设置带宽管理功能的步骤。

在系统 > 设备管理页面设置带宽管理功能。

带宽管理可以对流入或流出ASWG设备的流量，基于来源、目标、协议（端口方式）和带宽分类进行管理和分配。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 带宽管理页面。
2. 滑动状态条开启带宽管理功能。
3. 分别设置P1、P2网口带宽。
4. 点击  添加带宽分类，标识带宽的用途，管理划分的带宽，步骤如下：
  - a) 输入带宽类别名称。
  - b) 选择父分类即带宽管理层级。
  - c) 设置可以为该分类提供的最小带宽，最小带宽不能小于父类的最小带宽。
  - d) 设置允许该分类使用的最大带宽。
  - e) 设置同一层级中多个带宽分类之间的相对优先级，优先级越高则优先获取带宽资源。
  - f) 选择生效线路，指定该分类使用P1或P2网卡进行接收或发送流量，子分类必须和父分类使用相同的网卡。
  - g) 选择流量类型为服务器流出或服务器端流入。
  - h) 点击保存，带宽分类添加成功。
5. 点击保存，设置生效。

 提示：点击设置规则，跳转至全局控制列表，添加带宽控制规则，详细信息请参考[全局例外功能设置](#)。

。

## IP伪装

介绍设置IP伪装功能的步骤。

在系统 > 设备管理页面设置IP伪装功能。

IP伪装会模拟客户端的IP或使用代理服务器的地址与目标服务器进行通信，用户也可以通过规则使用指定IP与目标服务器进行通信，可以避免内网客户端和ASWG设备的信息（如IP）暴露给外部网站带来的安全隐患。

1. 选择选择系统 > 设备管理进入设备管理页面后，点击要查看的设备。进入设备 > 功能 > IP伪装页面，选择开启以下功能：

显示代理IP伪装	开启此功能后，代理服务器使用客户端IP与目标服务器进行通信时对IP地址进行伪装。
透明代理IP伪装	开启此功能后，代理服务器使用客户端IP与目标服务器进行通信时对IP地址进行伪装。

2. 点击保存，设置生效。

#### 自动配置脚本

介绍设置自动配置脚本的步骤。

在系统 > 设备管理页面进行自动配置脚本。

客户端浏览器访问自动配置脚本文件自动配置脚本内容和端口，实现代理功能。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备。进入设备 > 功能 > IP伪装页面。
2. 拉动状态条开启自动配置脚本功能。
3. 输入设备用于监听脚本的端口号。
4. 系统自动生成脚本路径，客户端浏览器从此路径获取配置的脚本。
5. 编辑PAC脚本文件内容。
6. 点击保存，脚本内容设置成功。

#### 邮件队列

介绍设置邮件队列的步骤。

在系统 > 设备管理页面设置邮件队列。

邮件队列统计MTA中邮件队列中的邮件总数、等待处理的邮件数量、等待策略分析的邮件数量和等待投递的邮件数量，并可以筛选不同的邮件状态（等待处理/等待投递/等待分析）。

选择选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 邮件队列页面，点



击立即投递手动投递邮件。点击  将所选邮件从列表中删除。



#### ASWG证书

介绍设置ASWG证书的步骤。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 证书页面。

ASWG证书包括企业证书、受信证书和服务器证书，同时支持证书验证和证书事件功能。管理员可以分别点击各选项卡进行如下操作：

- 企业证书：企业证书为一个CA证书，作为客户端和原始服务器站点之间的中转站，保证与客户端的正常进通信。
  - 点击导入证书按钮导入已有的企业证书。
  - 点击创建证书按钮在线创建企业证书。
  - 点击下载证书按钮下载证书到本地。
- 受信证书：受信证书由所信任的原始服务器提供。
  - 点击  按钮导入受信证书。
  - 点击  按钮删除所选受信证书。

- 点击悬浮图标  查看证书信息。
- 点击备份全部按钮备份受信证书列表中的全部受信证书到本地。
- 点击恢复按钮按钮恢复本地备份的受信证书，执行恢复操作将覆盖所有受信证书。
- 证书验证：验证证书的合法性，保障用户访问的网站安全可信。证书验证功能默认关闭，滑动状态条可以开启证书验证功能，并进行相关设置。
  1. 设置证书验证内容。
  2. (选填) 选择是否启用绕过证书验证。启用后，当请求被证书验证引擎阻止时，允许用户确认证书警告后继续访问站点。
  3. (选填) 选择是否启用CRL更新。启用后，可设置证书吊销列表(CRL)每天的更新时间，或点击立即更新按钮更新CRL。点击查看状态阿牛可查看CRL更新状态的记录。
  4. 设置客户端证书获取方式为透传或创建证书事件。
  5. 点击保存，设置生效。
- 证书事件：将有问题的证书添加为证书事件，用于策略匹配。
  1. 点击  对有问题的证书手动添加为证书事件。
  2. 输入证书事件名称。
  3. 输入目标服务器的域名或IP地址，形成证书事件URL。
  4. (选填) 输入对该证书事件的备注。
  5. 选择对该证书事件执行的动作。
 










透传	URL被透传，代理服务器不验证证书，不解密用户发送的请求。
阻止	URL被阻拦，用户不能做任何操作。
放行	即使URL不合法，用户依然可以访问URL且请求会被解密。
警告	证书验证失败时，用户访问URL被阻断，用户确认后可以继续访问URL。
  6. 点击保存，新建证书事件添加于列表，点击证书项对应的URL可查看证书详情。
- 服务器证书：服务器证书用于存储需要进行反向代理的目标站点证书。
  - 点击  按钮添加服务器证书。在启用反向代理功能时，客户端在连接服务器时返回此证书来标识服务器。
    1. 输入服务器证书的名称。
    2. (选填) 输入服务器证书的描述信息。
    3. 点击选择，从本地上传被保护站点的服务器证书，格式为PEM。
    4. 输入证书的密钥，或点击选择从本地上传密钥。
    5. (选填) 输入该证书的密码。
    6. 选择证书的目标站点类型，并输入该证书对应的站点域名或IP。
    7. 点击保存按钮，服务器证书添加成功。
  - 点击  按钮删除所选服务器证书。
  - 点击  按钮导出所选证书到本地。

表 65: 页面图标和行间操作按钮功能

	编辑受信证书(可以修改动作并编辑CRL URI和OCSP URI)、证书事件。
---	---

	阻止所选受信证书运行。
	运行所选受信证书。
	删除所选受信证书、证书事件。
	执行动作，批量透传、放行、阻止所选受信证书、证书事件或设置警告。
	恢复本地备份的受信证书，执行恢复操作将覆盖所有受信证书。

### OCR功能

介绍管理OCR功能的步骤。

在系统 > 设备管理页面设置OCR功能。

OCR识别图像功能支持本地和外置OCR服务器，外置OCR服务器可以解析网络流量中的图片内容并进行DLP分析，提高了对大量图片内容的处理速率，减轻系统资源消耗。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > OCR页面。
2. 滑动状态条，开启OCR功能。
3. 选择OCR工作的精确度，平衡系统资源消耗：

快速	效率高但是精确度低。
平衡	兼顾效率和精确度。
精确	精确度高但是效率低。


4. 选择OCR识别的语言，包括简体中文、繁体中文和英文。
5. 设置OCR图像识别引擎检测文件的大小限制，0表示不限制大小。
6. 选择OCR服务器，包括本地OCR引擎和远程OCR引擎。
7. 点击保存，设置生效。

### 全局例外

介绍设置全局例外功能的步骤。

在系统 > 设备管理页面设置全局例外功能。

全局例外针对不同协议进行集中配置来源和目标，代理服务器透传列表中的相关配置。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 全局例外页面，点击  新建全局例外并添加规则。
2. 输入全局例外名称，说明其作用。
3. 选择是否启用该全局例外功能。
4. 输入来源IP/IP段，如果设置全部来源即为0.0.0.0-255.255.255.255。

 注：ICAP Server的全局例外使用的来源IP/IP段为172.16.1.1, 192.168.0.1-192.168.0.200。

5. 输入目的IP/IP段或域名，全部域名即为“所有”。

 注：

- 域名方式仅适用于HTTP和HTTPS协议。
- ICAP Server的全局例外使用的目的IP/IP段为220.181.112.244, 220.181.113.100-220.181.113.120。也支持正则表达式的添加方式。

6. 根据应用场景，选择相应的传输协议。

7. 点击保存，设置生效。

表 66: 页面图标和行间操作按钮功能

图标	解释
	启用所选全局例外。
	禁用所选全局例外。
	删除所选全局例外。
	导入全局例外文件，可以参考模板生成，导入文件样例文件名称为“全局例外.json”。
	导出全局例外文件到本地。

### 缓存

介绍设置缓存功能的步骤。

在系统 > 设备管理页面设置缓存功能。

缓存功能通过设置缓存对象的大小和缓存的规则，统计缓存的命中率，启用高速缓存等功能提高了设备的快速响应能力。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 缓存页面，滑动状态条开启缓存功能。
2. 设置缓存对象，即选择要缓存的内容。
3. 选择是否启用高速缓存。启用后，需要设置最大缓存数据量。
4. 选择是否启用动态缓存设置。启用后，需要设置Cookie的缓存内容。
5. 点击保存，设置生效。



提示：点击设置规则跳转到全局控制列表 > 缓存规则，设置缓存规则，滑动状态条可开启缓存功能。详细信息请参考[缓存规则](#)。







### 全局控制列表


介绍设置全局控制列表的步骤。

在系统 > 设备管理页面设置全局控制列表。

全局控制用于设置代理服务器的代理规则功能。

表 67: 页面图标和行间操作按钮功能




	编辑缓存规则。
	禁用所选缓存规则。
	启用所选缓存规则。
	删除所选缓存规则。
	通过上下箭头调整规则优先级。
	导入JSON格式的全局控制列表规则，可以参考模板生成导入文件。

	导出JSON格式的全局控制列表规则到本地。
---	-----------------------

### 连接控制规则

介绍连接控制规则的设置步骤。



客户端用于正向代理时，设置客户端到ASWG设备间的并发连接数限制；服务器端用于反向代理时，设置ASWG设备到服务器端的并发连接数限制，监控或阻断超限连接的客户端请求，防止Web服务器过载。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 全局控制列表页面，点击  进入连接控制规则编辑界面。
2. 滑动状态条开启或关闭所有连接控制规则。
3. 选择客户端选项卡，点击  添加规则信息：
  - a) 输入规则名称，表明其用途。
  - b) 选择是否启用该规则。
  - c) 输入来源的IP或IP段用作规则匹配。
  - d) 选择是否设置连接数值。如果选择限制，需输入最大连接数，当达到上限时对用户请求执行监控或阻止动作。
  - e) 点击确定，客户端连接控制规则设置成功。
4. 选择服务器选项卡，点击  添加规则信息：
  - a) 输入规则名称，表明其用途。
  - b) 选择是否启用该规则。
  - c) 输入来源的IP或域名用作规则匹配。
  - d) 选择是否设置连接数值。如果选择限制，需输入最大连接数，当达到上限时对用户请求执行监控或阻止动作。
  - e) 点击确定，服务器连接控制规则设置成功。
5. 点击保存，设置成功。

### 带宽控制规则

介绍带宽控制规则的设置步骤。



带宽规则基于源IP / IP段、源端口、目标IP / IP段和端口对设备流量进行控制。

1. 选择系统 > 设备管理进入设备管理页面。
2. 点击要查看的设备。
3. 进入设备 > 功能 > 全局控制列表页面。
4. 点击  进入带宽控制规则编辑界面。
5. 滑动状态条开启或关闭所有带宽控制规则。
6. 点击  添加规则。
7. 输入规则名称，表明其用途。
8. 选择启用或禁用该规则。
9. 输入作为来源的IP或IP段，用作规则匹配。
10. 设置来源端口用作规则匹配，可选所有端口或指定端口。
11. 输入作为目标的IP或IP段，用作规则匹配。
12. 设置目标端口用作规则匹配，可选所有端口或指定端口。
13. 选择带宽分类用作规则匹配。添加带宽分类请参考[带宽管理功能设置](#)。
14. 点击确定，规则添加成功。
15. 点击保存，设置生效。

### 代理访问规则

介绍代理访问规则的设置步骤。



代理访问规则可以控制客户端能否通过代理服务器进行网络访问。

1. 选择系统 > 设备管理进入设备管理页面后。
2. 点击要查看的设备。
3. 进入设备 > 功能 > 全局控制列表页面。
4. 点击  进入代理访问规则编辑界面。
5. 滑动状态条开启或关闭所有代理访问规则。
6. 点击  添加规则。
7. 输入规则名称，表明其用途。
8. 选择启用或禁用该规则。
9. 输入作为来源的IP或IP段，用作规则匹配。
10. 选择匹配规则后执行的动作为放行或阻止。放行即允许访问，阻止即不允许访问。
11. 点击确定，规则添加成功。
12. 点击保存，设置生效。

### Socks访问规则

介绍Socks访问规则的设置步骤。



代理访问规则可以控制客户端能否访问Socks代理服务。

1. 选择系统 > 设备管理进入设备管理页面。
2. 点击要查看的设备。
3. 进入设备 > 功能 > 全局控制列表页面。
4. 点击  进入Socks访问规则编辑界面。
5. 滑动状态条开启或关闭所有Socks访问规则。
6. 点击  添加规则。
7. 输入规则名称，表明其用途。
8. 选择启用或禁用该规则。
9. 输入作为来源的IP或IP段，用作规则匹配。
10. 选择匹配规则后执行的动作为放行或阻止。放行即允许访问，阻止即不允许访问。
11. 点击确定，规则添加成功。
12. 点击保存，设置成功。

### 缓存规则

介绍缓存规则的设置步骤。

缓存规则用于控制代理服务器对不同目标站点的缓存设置。



1. 选择系统 > 设备管理进入设备管理页面。
2. 点击要查看的设备。
3. 进入设备 > 功能 > 全局控制列表页面。
4. 点击  进入缓存规则编辑界面。
5. 滑动状态条开启规则，点击  添加规则。
6. 选择基本设置选项卡：
  - a) 输入规则名称，说明其用途。
  - b) 选择启用或禁用该规则。


- c) 选择缓存规则类型：永不缓存、忽略no\_cache头、忽略客户端请求中的no\_cache头、忽略服务器响应中的no\_cache头、保留在缓存中、重新验证和强制缓存。
  - d) 选择目标类型（域名、主机名、IP/IP段或URL正则）用作规则匹配。
7. 选择高级设置选项卡：
- a) 设置缓存功能生效时间段。
  - b) 输入URL前缀用作规则匹配。
  - c) 输入URL后缀用作规则匹配。
  - d) 输入目标的端口号用作规则匹配。
  - e) 输入作为来源的IP/IP段用作规则匹配。
  - f) 选择请求方法：GET、POST、PUT、TRACE。
  - g) 选择协议类型（HTTP、HTTPS）用作规则匹配。
8. 点击确定，规则添加成功。
9. 点击保存。

### URL重定向规则

介绍URL重定向规则的设置步骤。

URL重定向规则支持HTTP、HTTPS协议的映射、重定向和URL应答改写功能。

1. 选择系统 > 设备管理进入设备管理页面，点击要查看的设备。
2. 进入设备 > 功能 > 全局控制列表页面。
3. 点击  进入URL重定向规则编辑界面。
4. 滑动状态条开启或关闭列所有表中已有的规则。
5. 点击  添加新规则。
6. 选择基本设置选项卡，进行如下配置：
  - a) 输入规则名称，说明其用途。
  - b) 选择启用或禁用该规则。
  - c) 选择如下规则类型：
    - URL映射：URL映射直接定向为地址栏里的URL。
    - URL重定向：URL重定向地址栏里的URL会变成目标的URL路径。
    - URL反向映射：URL反向映射支持映射关系为HTTP反射为HTTP/HTTPS，HTTPS反向映射为HTTP/HTTPS，FTP反射为FTP，TCP反射为TCP。
    - URL应答改写：修改目标站点包含的绝对路径，使用SWG服务器进行反向代理。
  - d) 选择原访问协议用作规则匹配，对于URL映射只支持HTTP协议，URL重定向可以支持HTTP、HTTPS。
  - e) 输入原访问主机IP或URL用作规则匹配。
 



 注：URL反向映射规则的原访问主机支持使用正则表达式实现域名映射。在主机名下拉菜单中选择正则表达式。
  - f) 选择目标访问协议用作规则匹配，对于URL映射只支持HTTP协议，URL重定向可以支持HTTP、HTTPS。
  - g) 输入目标主机的IP或URL用作规则匹配。
7. 选择高级设置选项卡，进行如下配置：
  - a) 输入原访问端口号用作规则匹配，不支持多个端口。
  - b) 输入原访问路径前缀用作规则匹配。
  - c) 输入目标端口号用作规则匹配。
  - d) 输入目标路径前缀用作规则匹配。
8. 点击确定，规则添加成功。
9. 点击保存，设置生效。



### 上游代理规则

介绍上游代理规则的设置步骤。



上游代理规则将ASWG收到的所有或指定的代理请求发送至所配置的上游代理服务器，需开启缓存功能。缓存功能的详细信息请参考[缓存功能设置](#)。

1. 选择系统 > 设备管理进入设备管理页面。
2. 点击要查看的设备。
3. 进入设备 > 功能 > 全局控制列表页面。
4. 点击  进入上游代理规则编辑界面。
5. 滑动状态条开启或关闭所有上游代理规则。
6. 点击  添加规则。
7. 选择基本设置选项卡，进行如下配置：
  - a) 输入规则名称，说明其用途。
  - b) 选择启用或禁用该规则。
  - c) 选择目标类型（域名、主机名、IP/IP段或URL正则）用作规则匹配，输入相应的地址或内容。
  - d) 输入上游代理IP地址。
  - e) 选择轮询方式：按源IP轮播、按请求轮询和不轮询。
  - f) 选择是否直出。
8. 选择高级设置选项卡：
  - a) 设置缓存功能生效时间段。
  - b) 输入URL前缀用作规则匹配。
  - c) 输入URL后缀用作规则匹配。
  - d) 输入目标的端口号用作规则匹配。
  - e) 输入来源的IP/IP段用作规则匹配。
  - f) 选择请求方法：GET、POST、PUT、TRACE。
  - g) 选择协议类型（HTTP/HTTPS）用作规则匹配。
9. 点击确定，规则添加成功。
10. 点击保存，设置生效。

### DNS分离解析规则

介绍DNS分离解析规则的设置步骤。

DNS分离解析可以基于用户的网络请求的来源或目标，使用不同的DNS服务器进行解析。

1. 选择系统 > 设备管理进入设备管理页面。
2. 点击要查看的设备。
3. 进入设备 > 功能 > 全局控制列表页面。
4. 点击  进入DNS分离解析规则编辑界面。
5. 滑动状态条开启或关闭所有DNS分离解析规则。
6. 点击  添加规则。
7. 输入规则名称，表明其用途。
8. 选择启用或禁用该规则。
9. 输入访问目标的DNS服务器。
10. 输入目标的域名、主机名或URL正则用作规则匹配。
11. 指定用于解析主机的默认域名。
12. 点击确定，规则添加成功。
13. 点击保存，设置生效。

## SOCKS代理

介绍设置SOCKS代理的步骤。

在系统 > 设备管理页面设置SOCKS代理。

通过内置SOCKS代理服务器或配置第三方SOCKS服务器，实现对任何TCP协议的代理功能。



1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > SOCKS代理页面，滑动状态条开启SOCKS代理服务器。
2. 输入SOCKS显式代理端口号。
3. 选择SOCKS服务器端版本：V4或V5。
4. 选择是否启用集成AD/LDAP认证，支持的认证服务器类型：AD、LDAP、本地（自定义）。
5. 选择SOCKS服务器为内置SOCKS代理服务器或第三方服务器。如果选择第三方SOCKS代理服务器，需输入IP、端口、用户名和密码。
6. 设置连接时限，超时后会断开连接。
7. 点击保存，SOCKS代理设置成功。

点击设置规则设置SOCKS访问规则，详细信息请参考[Socks访问规则](#)。

## DNS解析

介绍设置DNS解析的步骤。

在系统 > 设备管理页面设置DNS解设置的步骤。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > DNS解析页面。
2. 设置代理等待DNS服务器查询的超时时间。
3. 设置代理查询DNS解析结果缓存的超时时间。
4. 设置DNS代理DNS解析结果缓存记录域名的条数。
5. 指定用于DNS分离解析的域名。当请求仅包含主机名时，在进行DNS分离解析前，服务器自动补充该域名。
6. 输入可用的DNS服务器IP和优先级，点击 添加到列表，点击 将所选DNS服务器从列表中删除。
7. 点击保存，DNS解析设置成功。

## 网络抓取文件

介绍设置网络抓取文件配置的步骤。

在系统 > 设备管理页面设置网络抓取文件功能。

系统自动收集网络传输的文件放于指定目录，包括web流量中的文件、邮件中的附件等，为数据聚类提供文件样本。


1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 功能 > 网络抓取文件。
2. 滑动状态条启用自动抓取网络文件功能。
3. 选择远程存储文件的共享方式，支持SMB和NFS。
4. 输入远程服务器的IP或主机名。
5. 输入存储文件样本的文件夹路径，存储的文件包括web上传、下载的文件和邮件接收、发送的附件。
6. 输入登录共享服务器用户名称、密码或域名。
7. 点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
8. 点击保存，网络抓取文件设置成功。


## SMTP MTA





介绍ASWG SMTP协议在MTA介入模式下的配置步骤。

按照以下步骤在MTA接入模式下的配置ASWG SMTP协议。

1. 点击功能 > SMTP MTA，SMTP MTA服务编辑页面。
2. 点击基本选项卡，开启或关闭协议分析。开启协后进行如下配置：
  - a) 选择协议接入方式为SMTP MTA。
  - b) 选择工作模式：监控或阻断。
 

 提示：监控不会干扰邮件的正常处理和投递，阻断即当邮件触发策略时根据策略动作放行、隔离、删除邮件附件或加密等。
  - c) 配置检测的最大字节数，大于此字节数的内容不检测。
  - d) 选择是否启用全邮件记录，可记录全部邮件原文。
  - e) 设置FQDN信息。
 

安全管理员可按照需要自定义FQDN信息。
  - f) 设置SMTP欢迎信息。
  - g) 输入受信IP地址和子网掩码，点击添加为受信地址，MTA只接受此列表中来源发起的SMTP连接。
  - h) 选择是否开启高级路由，设置SMTP邮件投递路由规则。
 

 提示：配置路由时可以设置优先级，如果同一个域名定义了多个邮件路由而对应多个服务器IP地址，系统会尝试按照路由的优先级来发送邮件。当多条路由的优先级相同时，系统会使用轮询发送机制。
  - i) 指定MTA投递邮件的下一跳，可以选择DNS解析投递也可设置指定接收地址。如果开启高级邮件路由，则高级路由中配置的投递地址优先级最高。
  - j) 选择TLS传输安全机制为强制明文、自适应或强制TLS。
  - k) 选择是否发送邮件退信，可选择退信收件人为源发件人或指定收件人。
  - l) 选择是否添加邮件声明，可自定义邮件声明，表明邮件已经通过检测等。
  - m) 设置加密邮件的网关的主机名/IP和端口号。支持设置加密标识，主题加密标识用户可见，X-Header加密标识用于服务器解析。
  - n) 选择是否启用邮件恶链扫描，启用后，当邮件正文包含的URL属于列表中的分类时，对邮件执行相关操作。同时支持设置接受恶链扫描的文件大小。
3. 点击内部域名选项卡，进行如下配置：
  - a) 输入公司内部域名，用来区分邮件方向，点击添加到列表。
  - b) 选择需要分析的邮件方向。
  - c) 添加不需要检测的邮件来源邮箱地址和域名，勾选源选项，输入邮箱地址和域名后，点击添加到列表。点击可删除所选来源。
4. 点击保存,设置生效。

## 认证

介绍认证设置的步骤。

在系统 > 设备管理页面进行认证设置。

ASWG认证功能可以更准确的识别上网用户的身份，用户的上网请求会匹配合适的认证规则完成认证。目前ASWG支持的认证方式有：本地认证、AD LDAP、Open LDAP、IWA等认证方式。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证页面，基本配置如下：

- 认证失败设置
- 认证冲突设置
- 认证缓存设置
- 认证缓存时间设置
- 其它设置

## 认证服务器

介绍认证服务器的配置步骤。

ASWG支持以下认证服务器类型：


- Active Directory
- GENERIC LDAP
- Radius
- Integrated Web Auth (即集成WEB认证, 用户通过自己的WEB服务器认证后, ASWG可以识别到该IP的用户信息, 不需要进行二次认证)。
- OAuth2.0



注: 如果您选择的了某种类型的WebAuth认证, 需要添加相应全局例外URL地址, 以确保认证页面可访问。

1. 选择系统 > 设备管理进入设备管理页面后, 点击要查看的设备, 进入设备 > 认证 > 认证服务器页面, 点击 添加认证服务器。
2. 选择基本设置选项卡, 进行如下配置:
  - a) 输入认证服务器名称。
  - b) 选择启用或禁用该认证服务器。
  - c) 选择认证服务器类型。
  - d) 选择服务器来源, 用户可新建服务器或从用户目录中选择服务器。
    - 新建服务器 (仅Active Directory和GENERIC LDAP), 配置如下信息:
      1. 输入LDAP认证服务器的地址。
      2. 设置LDAP认证服务器的端口号。
      3. 输入登录服务器的用户名。
      4. 输入登录服务器的密码。
      5. 输入目录根节点。
      6. 选择是否使用SSL安全连接, SSL安全连接提高数据传输的安全性。
      7. 点击测试连接, 系统会尝试使用提供的信息检测与服务器的连通性。
    - 新建用户目录服务器 (Active Directory和GENERIC LDAP), 配置如下信息:
      1. 选择已配置好的用户目录。
      2. 系统自动获取认证服务器的主机名/IP和端口号。
      3. 输入目录根节点。系统会自动读取此用户目录的根节点。
      4. 选择是否启用SSL安全连接。
      5. 点击测试连接, 系统会尝试使用提供的信息检测与服务器的连通性。
    - 新建Radius认证服务器, 配置如下信息:
      1. 输入认证服务器的地址。
      2. 设置认证服务器的端口号。
      3. 输入共享密钥。
      4. 点击测试连接, 系统会尝试使用提供的信息检测与服务器的连通性。
    - 新建Integrated Web Auth服务器, 配置如下信息:
      1. 输入Web认证服务器的URL。
      2. 设置用户进行Web认证时, 向服务器提交的表单名称。
      3. 选择登录成功或失败的识别方式。
      4. 设置验证登录Web成功的关键字。
      5. 设置验证登录Web失败的关键字。
      6. 点击测试连接, 系统会尝试使用提供的信息检测与服务器的连通性。
    - 新建OAuth2.0服务器, 配置如下信息:

1. 点击选项卡选择服务类型，目前支持腾讯QQ、微信、钉钉和新浪微博。
  2. 勾选复选框启用该服务。
  3. 输入申请认证时的域名或回调地址。
  4. 输入反馈给用户的认证AppID。
  5. 输入反馈给用户的认证口令AppKey。
3. 选择高级设置选项卡，进行如下配置：

 注：高级配置项适配基本设置中的不同服务器类型如下。

**Active Directory和GENERIC LDAP高级配置如下：**

- a. 选择启用自定义过滤。
- b. 选择登录名类型，即设置首要过滤条件。
- c. 设置显示列，即填写显示名、姓、名和描述。
- d. 根据用户项进行过滤，即根据组织单元、组和成员过滤用户。

**Radius高级配置如下：**

- a. 设置认证请求的超时时间。
- b. 设置与Radius服务器进行协商的协议。
- c. 选择服务器编码，以指定字符集向认证服务器发送认证或凭证。
- d. 设置根据RFC 2865搜索用户组信息时所检索的属性的代码值。
- e. 设置在搜索用户组信息时所需的供应商ID。
- f. 设置供应商属性中包含的子属性类型的代码值。



**Integrated Web Auth高级配置**

- a. 自动获取或者手动设置用于提交用户认证信息的URL地址。
- b. 勾选启用复选框开启认证超时设置功能，开启后进行如下配置：
  1. 设置Web Auth 反给用户浏览器的Cookie名称，用于识别Web Auth认证服务器。
  2. 设置Cookie方式返回的关键字或状态码。
- c. 点击确定，保存高级设置。

**OAuth2.0高级配置**

- a. 选择启用欢迎页面。
  - b. 输入欢迎页面的URL地址。
  - c. 点击确定，保存高级设置。
4. 点击保存，认证服务器设置生效。

表 68: 页面图标和行间操作按钮功能

	编辑认证服务器配置信息。
	删除所选认证服务器。

## Windows集成

介绍Windows集成的配置步骤。

ASWG支持Windows集成身份认证。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证 > windows集成页面，配置Windows集成身份认证。
2. 设置设备所要加入域的用户目录。
3. 输入Windows域名。


4. 输入用户登陆域账号。
5. 输入用户登陆域账号密码。
6. 连接域控制的主机，可通过DNS查询或指定主机IP。
7. 点击加入按钮加入所配置的Windows域，点击退出域按钮退出所在的Windows域。

#### 认证规则

介绍认证规则设置的步骤。


认证规则可以控制内网的某个IP或网段的计算机的认证方式。目前代理服务器支持Windows集成认证、本地认证、AD / LDAP认证、Radius认证或者不认证。其中Windows集成认证不支持备用认证服务器认证。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证 > 认证规则页面。


2. 滑动状态条可开启全部认证规则，点击添加认证规则。

3. 选择基本配置选项卡，进行如下配置：

- a) 输入规则名称，说明其用途。
- b) 选择启用或者禁用该规则。
- c) 输入需要匹配的来源IP或IP段。
- d) 选择主要认证服务器的认证方式为不认证或本地认证。

 注：当服务器选择本地认证时需要设置认证窗口，目前支持本地认证页面或标准弹窗认证。

- e) 选择次要认证服务器的认证方式为不认证或本地认证。

 注：

- 如果主要认证服务器选择本地认证，则次要服务器不可选本地认证。
- 当服务器选择本地认证时需要设置认证窗口，目前支持本地认证页面或标准弹窗认证。





4. 选择高级配置选项卡，进行如下配置：

- a) 选择需要匹配的访问目标的类型（域名、主机名、IP/IP段或URL正则）并输入相应地址或内容。
- b) 输入需要匹配的访问目标端口号。
- c) 设置该规则生效的时间段。
- d) 输入需要匹配的目标User-Agent信息。

5. 点击保存，认证规则添加成功。

6. 再次点击保存，认证规则设置生效。

表 69: 页面图标功能

	禁用所选规则。
	启用所选规则。
	删除所选规则。
	通过上下箭头调整规则优先级，点击保存后生效。


#### 帐号绑定规则

介绍帐号绑定规则的配置步骤。

帐号绑定规则可以限制同一认证账号的认证次数，并对认证账号和IP进行绑定管理，预防认证账号被盗用等安全隐患。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证 > 帐号绑定规则页面。

2. 滑动状态条可开启所有帐号绑定规则，点击添加帐号绑定规则。

3. 输入规则名称，说明其用途。
4. 选择启用或者禁用该规则。
5. 点击  从已有的用户目录中添加绑定账号。
6. 选择以下绑定类型：

绑定IP地址	输入要绑定的IP地址。
绑定认证次数	输入绑定的认证次数，控制同一账号同时在线的数量。

7. 点击确定，账号绑定规则添加成功。
8. 点击保存，账号绑定规则设置生效。

## 其他

其他的选项页面。

该菜单包含其他的选项页面。

### SNMP功能

介绍管理SNMP功能设置的步骤。

在系统 > 设备管理页面设置SNMP功能。

设备支持外部应用访问SNMP服务器来收集设备信息。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > SNMP页面，设置SNMP功能。
2. 滑动状态条，开启SNMP功能。
3. 选择SNMP query版本，可以设置为v1或v2c。
4. 输入SNMP的团体名，即SNMP的用户名或密码，只允许使用此团体名访问SNMP服务器。
5. 选择以下SNMP的连接方式：

任何IP	任何IP地址都可访问SNMP。
仅限于下列IP	输入IP地址，点击  添加到可访问SNMP的IP列表。

6. 点击保存，设置生效。


### 收集日志

介绍配置收集日志功能的步骤。

在系统 > 设备管理页面设置收集日志功能。

设备支持收集系统日志信息，了解系统运行状态。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 收集日志页面，设置收集日志功能。
2. 选择收集日志的时间段。
3. 选择收集日志的类型。
4. 点击收集日志，收集所设定日期和指定类型的日志，显示于日志收集历史列表中。

点击  可将得收集得日志文件下载到本地；点击  可删除所选日志文件。

### 备份和恢复

介绍备份/恢复功能设置的步骤。

在系统 > 设备管理页面设置备份和恢复功能。

UCSS设备支持立即备份和立即恢复系统配置，包括配置信息、证据文件、邮件、网络及主机信息等，并支持定期备份功能。

1. 选择设备 > 其他 > 备份,进入备份或恢复页面。
2. 点击定期备份启动定期备份，设置定期备份的时间。
3. 点击备份设置，选择以下备份方式和备份内容：

备份至本地	选择备份至本地设备，设置备份日志数量的最大值，若本地保存数量大于设置的最大值则会删除最早的备份。
备份至远程	支持备份至Samba服务器和NFS服务器，需输入服务器的IP/主机名、文件夹路径和用户信息，并进行测试连接。

备份记录会出现在备份历史中，点击删除可删除所选备份。

4. 点击保存，设置生效。

### 升级和补丁

介绍升级/补丁功能设置的步骤。

在系统 > 设备管理页面设置升级和补丁功能。

设备支持在线版本升级和补丁安装，但升级不支持版本回退。选择系统 > 设备管理进入设备管理页面后。点击要查看的设备，进入设备 > 其他 > 升级/补丁页面，然后进行升级或补丁设置。

#### • 升级

选择升级选项卡，点击检查更新连接天空卫士的安装包服务器，获取安装包列表，选择安装包下载并安装。如果用户设备无法直接访问互联网，可通过代理服务器配置使用代理进行检查更新，点击代理服务器配置代理服务器。

点击上传安装包从本地上传升级安装包。

#### • 补丁

选择不定选项卡，查看当前版本和可用补丁。点击上传安装包从本地上传补丁安装包，安装之后可以选择卸载。

### 远程控制

介绍远程控制功能设置的步骤。

在系统 > 设备管理页面设置远程控制功能。

设备启用SSH连接后，可通过SSH执行远程设备故障排查。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 远程控制页面。
2. 选择是否启用以下功能：

启用远程控制	启用远程控制以后可以开启SSH端口并使用设备管理账号（例如ucssadmin帐号）登录设备进行命令操作。
启用技术支持模块	启用技术模块之后，获取6位密码。该密码需要提供给天空卫士进行解密后使用。
启用超时限制	设置在指定时间之后自动关闭远程控制。

3. 点击保存，设置生效。



注：



远程访问记录可在远程访问历史中查询。

### 自定义页面

介绍设置自定义页面的步骤。

在系统 > 设备管理页面设置自定义页面。

设备支持用户自定义显示界面，当网络请求被设备阻断时，展示给用户此提示页面。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，选择如下页面定义方式：

默认页面	使用系统默认页面。
自定义LOGO和公司名称	输入公司名称，上传公司Logo，自定义具有公司标识的显示页面。
定制页面	下载预置页面模板或下载当前自定义页面，本地设计修改后上传至系统。

2. 点击保存，设置生效。

### 系统工具

介绍系统工具设置的步骤。

在系统 > 设备管理页面设置系统工具。

系统工具预置多条CLI命令，即使不连接后台时也可以使用系统工具进行故障排查，并显示执行结果。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，从下拉框中选择索要执行的命令。
2. 输入出现故障的设备主机名或IP，点击执行开始运行故障排查命令，点击停止可终止执行命令。执行结果显示于黑色屏幕中。

### 库更新



介绍设置库更新配置的步骤。

ASWG设备支持URL分类库、病毒库和Cloud App分类库的手动和自动更新。


选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面。

 注：库更新的状态在ASWG license有效期内显示激活或停用。

在版本列表中显示URL分类库、Cloud App分类库和病毒库等更新更新时间、当前版本和最新版本等信息。


如果有新的库版本更新，点击可手动下载最新版本。或者点击按钮，通过导入ext后缀名的云应用分类库文件的方式进行更新。

还可以根据以下步骤设置库自动更新计划：

1. 点击设置库更新计划：

下载计划	选择下载时间和版本检查的时间间隔。
更新计划	设置更新时间。
缓存超时设置	设置清除缓存的时间。

2. 点击确定，设置成功。

 提示：在下载及更新历史栏，可查看库版本、升级包大小、状态和更新结果的历史记录。


## 设置设备高可用


介绍设置设备高可用的步骤。




在系统 > 设备管理页面配置设备高可用。

设备高可用是将两台或多台同类型设备 ( DSG/ASWG/SEG/UCWI ) 互作备份，当其中某台出现故障时同组设备可以立即替代该设备，保证MTA、ICAP Server、代理服务业务的正常进行。

当设备出现硬件故障 ( 断电、网卡等出现问题 ) ，网络故障 ( 网线连接问题、其他网络设备出现故障 ) 等情况无法实现设备切换。

 提示：高可用仅支持同类型设备的同类型网卡间的切换，ASWG设备的P1和P2网口只能在代理模式下支持高可用切换。

 注：启用了配置同步功能后，当配置了高可用的设备组之中的任意一台设备变更了配置 ( 如HTTP里的参数变更 ) ，安全管理员无需重复操作，该设备的配置改动能自动同步到高可用组内的其他设备中。

1. 选择系统 > 设备管理，点击高可用，在下拉菜单中选择设备型号，配置设备高可用。
2. 输入设备组名称，如北京UCSG-ASWG设备。
3. 点击  从已注册设备列表中选择设备。点击  删除所选设备。设备不能被重复添加到不同的分组。
4. 开启虚拟IP，进行如下配置：
  - a) 输入虚拟IP地址 ( 虚拟IP数量不能大于组内的设备数量并且IP地址与在设备需在同一IP段 ) 。
  - b) 选择网卡类型：Mgmt管理接口，MTA邮件接口，P1/P2代理接口 ( 仅UCSG-ASWG设备 ) 。
  - c) 设置子网卡序号 ( 用于标记，数字不重复即可 ) 。
  - d) 点击  添加于列表。
5. 点击保存，添加完成。

---

# 第 5 章

---

## 数据安全

---

内容:

- [数据安全检测条件](#)
- [数据安全治理](#)
- [数据安全监控](#)
- [数据安全报告](#)
- [数据安全设备监控](#)
- [数据安全设备管理](#)
- [数据安全日志](#)

介绍天空卫士™数据防泄漏DLP解决方案。

在天空卫士™安全鳄®统一内容安全UCS解决方案中，数据安全网关DSG(以下简称UCSG-DSG)融合数据防泄漏DLP技术，作为方案的数据安全模块，防范任何可能造成敏感信息丢失或泄露的风险，以保护企业内部的信息安全。

UCSG-DSG以集中策略为基础，采用高精度的深层内容分析技术，对静态数据、传输中的数据及使用中的数据进行识别、监控、保护。采用最先进的自然语言处理、指纹扫描、智能学习、图像识别技术，对网络、终端、本地存储的数据进行全方位多层次的分析和保护，防止企业核心数据以违反安全策略规定的方式流出而泄密。

## 数据安全检测条件

介绍数据安全检测条件的相关信息。

天空卫士™安全鳄®统一内容安全UCS解决方案中的数据安全模块在安全策略中运用多种检测条件检测违反企业安全制度的内容和行为，并在有必要的情况下，采取对应的策略行为，限制或阻断通信，确保企业数据安全。

数据安全解决方案支持以下检测条件。

- 关键字
- 正则表达式
- 脚本
- 文件指纹
- 数据库指纹
- 字典
- 文件名称
- 文件类型
- 文件大小
- 附件数量
- 智能学习
- ITM模板
- 文件属性
- 数据分类
- 标签

### 关键字

介绍检测条件中的关键字及其相关知识。

#### 检测条件介绍

关键字是指在用户请求的文件中或用户请求的URL等用户请求内容中的一个关键字串，如词语，短语或缩写等。



统一内容安全UCS解决方案支持对内容中的关键词进行检测，通过在企业安全策略中定义常用安全的关键字和期望排除的关键字，安全管理员可定义关键字检测，即按照请求中包含的关键字进行检测。

关键字不需要预定义，在添加策略时如果类型是关键字则直接输入多个关键字即可（逗号分隔），可以在策略中选择设置大小写是否敏感（默认不敏感）。

#### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择关键字，即可将关键字检测条件应用至策略。

页面包含以下配置项。

- 任意关键字 - 支持输入任意关键字，即可对用户请求包含的关键字进行检测，如“机密信息”等。
- 关键字对 - 输入要检测的关键字对，点击  添加到列表。  
 注：一对关键字必须同时出现，且匹配两者的间隔字符数，才会命中策略。
- 匹配条件 - 可选择如下匹配条件。


配置项	解释
最少匹配	填写最小匹配阈值，当分析内容匹配次数达到阈值，才会命中策略。

配置项	解释
不匹配	当分析内容与关键字不同的时候，会命中策略。
统计重复内容	关键字匹配记录统计重复次数。如果不选择此项，每个关键字最大匹配次数为1。
精确匹配	不进行分词检测，进行全文正则检测。精确匹配可以检测示例检测内容包含的符号字符。
自动匹配简体/繁体中文	同时支持繁简体检测。

- Email匹配属性 - 可配置以下Email匹配属性。

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

- 文档匹配位置 - 选择文档匹配的位置，包括页眉，正文和页脚。

 注：文档匹配位置检测仅适用于包含页眉、页脚类型的文件，如Word、Excel、PPT等Office类型文件。

## 正则表达式

介绍检测条件中的正则表达式及其相关知识。

### 检测条件介绍

正则表达式是指一种可用于匹配多个字符串和文字搭配组合的模板，或常用的固定表达形式。

假设有这样一条简单的正则表达式：`skyguard.(com|org|net)`。

这个正则表达式可以匹配以下的URL。

- `skyguard.com`
- `skyguard.org`
- `skyguard.net`

需谨慎使用正则表达式。正则匹配内容中效果突出，但是需要良好的设计。缺乏良好设计的正则表达式可能导致大量漏报，大量错报，以及系统资源占用过高。将正则表达式应用为策略匹配条件可能会增加内存占用。

如需了解更多关于正则的信息，请参考以下外部链接。


- [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression)
- <http://www.regular-expressions.info/>

统一内容安全UCS解决方案支持对内容中的正则表达式进行检测，通过在企业安全策略中定义常用安全的正则和期望排除的正则，安全管理员可定义正则表达式检测，即按照请求中包含的正则进行检测。




### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择正则表达式，可应用正则表达式检测条件。

在拥有多条正则匹配规则的情况下，为正则表达式添加适当便于区分的名称以便统一管理。

 注：多条正则表达式规则时，匹配一条即为命中策略。

## 应用至Web安全策略

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮清除所有的匹配条件。

## 应用至数据安全策略

参照以下章节将正则表达式检测条件应用于数据安全策略。

[正则表达式匹配/例外](#) on page 175

## 脚本

介绍检测条件中的脚本及其相关知识。

### 检测条件介绍

脚本是指自然语言脚本，是一种使用python或C++语言开发的，可用于匹配自然语言表达的匹配条件。


统一内容安全UCS解决方案预置了大量的自然语言脚本检测条件，可用于检测数字类型的数据，例如信用卡号码以及身份证号码等。脚本检测条件为此做了大量优化，因此它通常比正则表达式更加精准。脚本整合了统计学分析和决策树等技术可同时分析内容及其关联的上下文。

脚本也可用于检测软件开发设计文档以及各种源代码文件。

### 检测条件配置

在策略配置页面，点击添加匹配或添加例外，选择脚本，可将脚本检测条件应用至策略。

脚本检测条件可配置以下项目。

- 脚本 - 点击 ，从弹出的列表中选择策略中引用的脚本。

如需了解预置脚本模板的更多信息，参考[预置数据模板](#) on page 213章节。

启用脱敏数据 - 选择是否启用脱敏数据，启用后，匹配信息部分数据将以\*代替，并在事件、报告和通知中展示。匹配详情及证据显示将对敏感数据信息增加干扰，不能查看脱敏数据。

- 匹配条件 - 可选择以下匹配条件。

配置项	解释
最少匹配	填写最小匹配阈值，当分析内容匹配次数达到阈值，才会命中策略。
不匹配	当分析内容与正则表达式不同时命中策略。
统计重复内容	关键字匹配记录统计重复次数。如果不选择此项，每个关键字最大匹配次数为1。

- Email匹配属性 - 可配置以下Email匹配属性。

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。

匹配	介绍
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

- 文档匹配位置 - 选择文档匹配的位置，包括页眉，正文和页脚。



注：文档匹配位置检测仅适用于包含页眉、页脚类型的文件，如Word、Excel、PPT等Office类型文件。

## 文件指纹

介绍检测条件中的文件指纹及其相关知识。

### 检测条件介绍

文件指纹是针对部分文件和目录进行文件指纹扫描，或扫描移动中的文件，以获取完整的文件指纹信息。

天空卫士™安全鳄®数据安全解决方案支持安全管理员使用指纹爬虫工具*DSA*扫描文件内容，并运用相关技术做成指纹信息，用于相似度匹配。

如：从一个10页的文件中，取出其中的2页，系统同样可以检出，在这2页里加入一些其它的混淆的文字系统也可以检出。

天空卫士™安全鳄®数据安全解决方案利用文件指纹作为检测条件，可有效帮助组织阻断发往外部收件人的特定文件。文件指纹也可用于保护SharePoint目录，网络文件系统，和文件共享服务器等。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择文件指纹，可将文件指纹检测条件应用至策略。

## 数据库指纹

介绍检测条件中的数据库指纹及其相关知识。

### 检测条件介绍

数据库指纹是指针对部分数据库进行数据库指纹扫描，以获取完整的数据库指纹信息。

天空卫士™安全鳄®数据安全解决方案支持安全管理员使用指纹爬虫工具*DSA*扫描数据库表里的每个单元格信息，并运用相关技术做成指纹信息，用于对外传的内容进行数据库指纹匹配。

数据库指纹检测条件对受保护的数据库中的每一个对象进行完整的，全面的数据库指纹记录。例如，可检测数据库中的姓名，登录名，身份证号码等在一条消息中同时出现的各种信息，以及在企业数据库中与其关联的某条特定记录。

数据库指纹检测条件还可以对基于云端的数据库进行数据库指纹检测。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择数据库指纹，可将数据库指纹检测条件应用至策略。

## 字典

介绍检测条件中的字典及其相关知识。

### 检测条件介绍

字典是一个容器，主要用于存放同一种语言中的多个关键字和正则表达式及其对应的权重。

统一内容安全*UCS*解决方案预置了大量的字典检测条件，包括财务方面的词汇，违禁药品相关的词汇，合同相关词汇，机密相关的词汇等。

安全管理员也可以自定义创建新的字典，或编辑现有字典，并将改动应用至你的安全策略中。

字典中的每一个关键字都可以分配权重，权重之和满足策略阈值时，将视为策略匹配或策略例外，以确保对内容中包含的所有关键信息进行安全策略检测。

权重是指关键字在整体检测中的相对重要程度，例如：策略阈值为5，字段a权重为3，字段b权重为2，字段c权重为1，a+b会命中策略，a+c和b+c不会命中策略。

#### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择字典，可将字典检测条件应用至策略。

## 文件名称

介绍检测条件中的文件名称及其相关知识。

#### 检测条件介绍

文件名称检测条件可用于检测文件名称和附件名称及其后缀名。

天空卫士™安全鳄®数据安全解决方案支持运用各种通配符自定义文件名称。

- ? 可用于单一字符匹配，如设置条件为file\_?.txt, 可检出名为file\_1.txt, file\_2.txt等文件。
- \* 可用于任意字符匹配，如设置条件为file\*.docx, 可检出名为file\_secret.docx, file\_nda.docx等文件。

文件名称检测条件基于文件后缀名进行检测，是一种初级检测手段，例如设置检测条件为\*.docx，则名为file.docx的文件会被检出，而名为file.doc.zip的文件不会被检出。

因为机密数据通常以特定的格式进行保存，例如加密的PGP格式或非开源的Excel格式。安全管理员可以将文件类型和文件名检测条件同时应用于企业安全策略，以确保某些包含文件名的，某种格式的机密文件不会外流导致企业信息资产流失。

#### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择文件名称，可将文件名称检测条件应用至策略。

## 文件类型

介绍检测条件中的文件类型及其相关知识。

#### 检测条件介绍

文件类型检测条件可检测某一特定文档类型，如Microsoft Word文档，或者基于文件内部的特征码检测一系列相似的文件类型，如各种压缩文件。

天空卫士™安全鳄®数据安全解决方案中包含了文件类型库中，其中包含了系统预置的大量文件类型，其中包括：

- 风险文件
- 文本文件
- 多媒体文件
- 图像文件
- 可执行文件
- 文档文件
- 压缩文件
- 不可识别的文件类型
- 等。。。

注：这些预置的类型中包含预置的扩展名

文件类型可编辑，系统支持在预置类型文件中添加扩展名称，也支持添加新的文件类型。





注：将文件类型应用至检测条件之前，务必确认以下注意事项。

- 一个扩展名文件可以属于不同的文件类型，比如doc 可以属于文档文件，也可以同时属于同文本文件
- 不可识别的文件类型用于标识不在文件类型定义（预置和自定义）的扩展名，内容为空，用户不能添加

### 基于文件标识的文件类型识别

天空卫士™安全鳄®数据安全解决方案可以识别文件的标识，即使该文件被压缩、删除或更改扩展名也可以被正常识别。





如：被RAR压缩后的word文件则被识别为RAR压缩和word两种格式，安全策略引擎SPE会对压缩的文件自动解压以后分析。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择文件类型，可将文件类型检测条件应用至策略。

系统支持文件的扩展名类型和MIME类型检测。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。



注：当匹配多条文件类型规则时，匹配一条即为命中策略。

### 相关信息

[管理文件类型](#) on page 98

介绍管理文件类型的步骤。

## 文件大小

介绍检测条件中的文件大小及其相关知识。

### 检测条件介绍

文件大小检测条件通过获取文件大小的方式对文件进行检测。

天空卫士™安全鳄®数据安全解决方案可以识别文件的大小和邮件中附件的大小，安全管理员可以选择文件大小1的范围，并对符合该范围的文件或邮件附件进行检测。

例如，设置检测范围为大于等于10 MB，可检测大小为10 MB或10 MB以上的文件，或邮件中包含的附件，但是大小为10 MB以下文件，或邮件中包含的附件将会被忽略，即使其中可能包含机密信息。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择文件大小，可将文件大小检测条件应用至策略。

## 附件数量


介绍检测条件中的附件数量及其相关知识。

### 检测条件介绍

附件数量检测条件可检测邮件中包含的附件的具体数量。

天空卫士™安全鳄®数据安全解决方案可以识别邮件中的附件数量，安全管理员可以选择邮件数量的范围，并对符合该范围的邮件进行检测。

例如，设置检测范围为大于等于10，可检测附带10个或10个以上附件的邮件，但是附带10个以下附件的邮件将会被忽略，即使其中可能包含机密信息。

 注：附件数量检测条件只能对邮件内容中的附件进行匹配。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择附件数量，可将附件数量检测条件应用至策略。

## 智能学习

介绍检测条件中的智能学习及其相关知识。

### 检测条件介绍


智能学习检测条件是一种高级检测工具，它可通过智能学习获得的内容模板应用于内容检测，用于检测与智能学习结果相类似的文件。

天空卫士™安全鳄®数据安全解决方案支持安全管理员在管理平台页面中执行智能学习操作，并将结果运用于安全策略检测。例如：

- 将一批相似的文件交给数据防泄漏DLP系统学习，如一系列禁止外传的机密文件，系统学习以后会提炼出这些文件的共同点，如果有类似的文件外传则会命中策略。
- 将一些容易与这些文件产生混淆的内容交给系统做反向学习，如一系列与机密文件相同格式但无需保护的常规公开文件，这样可以提高智能学习的精确度。

不同于文件指纹的是，提交智能学习的样例文件无需包含需要保护的机密内容的具体信息，而仅需与机密文件相似，或与机密文件服务于同一个主题。系统可以学习这些文件，并识别其中复杂的正则表达式和上下文关联，并基于此进行内容检测，而文件指纹检测条件则要求内容在很大程度上的完全匹配。因此，智能学习可用于检出新型的，零日病毒文件。

因为智能学习检测条件无需完全匹配，相比文件指纹检测条件，它往往可以检出更多的文件。

 注：智能学习检测条件仅可用于非结构数据。它不可用于数据库，以及SharePoint和IBM Domino中的非结构数据。

### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择智能学习，可将智能学习检测条件应用至策略。

## ITM模板

介绍检测条件中的ITM模板及其相关知识。

### 检测条件介绍

ITM模板检测条件可以基于ITM模板检测包含内部威胁风险的文件。

天空卫士™安全鳄®数据安全解决方案利用其存储于ITM服务器中的的ITM模板检测条件，支持检测个人简历，企业通讯录，客户信息表等各种由于内部员工管理不慎或恶意泄露，导致流出企业的企业重要信息资产。

ITM模板检测条件可检测文件和邮件头中的各种信息，以及邮件附件等。

#### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择ITM模板，可将ITM模板检测条件应用至策略。

## 文件属性

介绍检测条件中的文件属性及其相关知识。

#### 检测条件介绍

天空卫士™安全鳄®数据安全解决方案已将文件名称，文件类型和文件大小定义为特有的安全策略检测条件，除了这些属性之外，安全管理员还可定义以下文件属性。

- 文件所有者
- 修改日期
- 创建日期
- 访问日期
- 等

以上文件属性可检测文件和邮件头中的各种信息，以及邮件附件。

#### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择文件属性，可将文件属性检测条件应用至策略。

## 数据分类

介绍检测条件中的数据分类及其相关知识。

#### 检测条件介绍

数据分类功能使得安全管理员能够基于用户生成的数据分类信息来制定数据安全策略。

天空卫士™提供的数据分类功能使得企业安全管理员获得一种超越当前策略规则的数据安全解决方案 - 基于数据分类的数据安全解决方案。

数据分类元数据来自企业安全管理员和涉及企业安全的最终用户，在制定企业安全策略时，这可以基于数据分类进行识别和保护，确保数据安全解决方案的落实准确而具有针对性，有效提高检出率和减少误报。

#### 应用检测条件

在策略配置页面，点击添加匹配或添加例外，选择数据分类，可将数据分类检测条件应用至策略。

## 标签

介绍检测条件中的标签及其相关知识。

#### 标签

天空卫士™统一内容安全UCS解决方案提供了分类标签的功能，支持对组织内部的非结构化数据包括各种类型的非结构化文件，以及邮件内容进行标签分类，并可通过已分类的标签识别标记的文件数据，以对其进行检测防护。

标签可应用于以下场景：

- 通过标签识别实现内容的权限控制：结合现有的用户目录、用户目录组及组织架构，安全管理员可以定义标签使用的范围。
- 通过标签识别区分内容的机密级别：支持安全管理员以数字等级定义标签分类的安全级别，高于机密等级的文件如果发生数据泄露事件，安全管理员可以通过标签对事件进行迅速的检索和定位。

用户对文件进行手动标签

组织内的用户可以在安装了带有数据防泄漏DLP授权的统一内容安全终端UCSC应用程序的终端设备上，查看文件已有标签和创建新的分类标签。

将标签应用于安全策略

标签功能支持将标签作为一个内容规则被数据分类引用或者直接被策略引用。

数据防泄漏DLP策略根据设置标签规则或者分类标签规则检测外发数据，当外发数据匹配上指纹标签或者分类标签后，根据策略动作实施放行或者阻断，同时记录日志事件。

将标签应用于事件

标签功能支持对数据防泄漏DLP事件增加标签属性，并支持根据标签属性的进行事件的筛选和统计，以快速发现和定位关于标签文件的数据安全事件。

## 数据安全 管理

---

介绍数据安全 管理相关功能。

天空卫士™安全鳄®数据防泄漏DLP产品，以集中策略为基础，采用深层内容分析，对静态数据、传输中的数据及使用中的数据进行识别、监控、保护的相关机制；采用最先进的自然语言处理、指纹扫描、智能学习、图像识别等技术，对网络、终端、存储的数据进行全方位多层次的分析和保护，防止企业核心数据以违反安全策略规定的方式而泄密。

数据防泄漏DLP产品需要注册至UCSS进行交互和管理。


### 数据安全策略

介绍数据安全策略，即DLP页面的页面信息。

DLP策略用于监控通过Web、Email、数据发现等通道发送的信息，确保所有通信均符合适用的法规和条例；并且监控发送至用户移动设备的电子邮件，并根据策略规则执行相应的策略动作。如果系统注册ITM License，系统将预置17条安全策略用于ITMS中的ERS专家模型及ITM报告可视化统计展现。详细信息请参考[查看预置DLP策略模板](#)。

DLP策略目前支持自定义策略，通过预置/自定义模板添加策略和通过初始化向导添加策略。

在DLP管理 > 策略页面管理DLP策略。

点击  选择显示上级策略、下级策略、本级策略及预置安全策略。默认只显示上级策略和本级策略。下层分级对象没有权限查看上级策略，只能查看下级策略和本级策略。上层分级对象拥有所有策略的查看权限。

策略基本信息


在DLP管理 > 策略页面添加新的DLP策略。

进入页面

在DLP管理 > 策略页面管理数据安全策略。

策略配置页面包括新策略页面和策略编辑页面。

在页面按钮中点击添加 > 新策略进入创建新策略页面。

在页面显示的策略列表中，点击某一现有策略名称，或点击现有策略名称后的  按钮，进入策略编辑页面。

点击保存至策略模板按钮，可以将当前配置保存为策略模板，复用当前策略内容项。

创建新策略需要经过配置检测内容、传输通道、来源/目标和动作四大步骤。

## 策略基本信息

策略配置页面的策略基本信息部分可配置以下信息。

- 名称 - 注意填写区别于其他条目的名称。



注：名称支持中英文，数字，以及部分特殊符号，输入系统不支持的特殊符号将导致策略保存失败。

- 描述 - 需说明其用途。



提示：描述需包含安全管理员对条目进行长期管理所需的必要信息。



注：不能与现有或内置的条目名称相同。

- 来源Risk Level - Risk Level 1-5，分别对应“较低、普通、严重、危险、高危”。
- 策略组 - 策略所属的策略组，用于策略的分类管理和统计报告。
- 策略等级 - 策略所属策略等级，即将策略分级。
- 启用状态 - 是否启用该项目。
- 策略类型 - 策略类型包括以下选项。
  - DLP > 常规策略 - 用于检测常规数据防泄漏DLP事件的安全策略。
  - DLP > ITM策略 - 用于检测由内部威胁引起的内部威胁管理ITM事件的安全策略。
  - 数据发现策略 - 用于检测数据发现事件的安全策略。

## 页面图标按钮



提示：点击保存至策略模板可保存当前配置为策略模板，复用当前策略内容项。

图标	解释
	启用所选策略，启用状态栏显示为启用。
	禁用所选策略，启用状态栏显示为禁用。
	删除所选策略。
	编辑所选策略并显示当前策略信息。
	禁用所选策略。
	添加MRS任务，针对每个用户或者IP进行回溯得到DLP安全风险模式相似分值MRS。详细信息请参考 <a href="#">添加定时报告</a> 。
	克隆策略，基于已有策略快速创建新策略，策略名称默认为“原策略名称_副本”。
	按照策略名称、策略上次修改时间、所属策略组、策略等级对当前策略进行排序。
	将所选策略的内容导出为PDF文件。

## 策略检测内容


介绍配置策略检测内容页面。

### 简介


在策略配置页面，点击检测内容选项卡即可配置匹配和例外的检测内容。


数据安全解决方案中策略的检测内容包括以下匹配选项。

- 名称 - 注意填写区别于其他条目的名称。


 注：名称支持中英文，数字，以及部分特殊符号，输入系统不支持的特殊符号将导致策略保存失败。

- 描述 - 需说明其用途。

 提示：描述需包含安全管理员对条目进行长期管理所需的必要信息。

 注：不能与现有或内置的条目名称相同。


- 必现 - 即策略命中前提是必须命中该规则，再继续匹配其它规则。

 注：DLP策略支持M选N的功能，丰富配置检测内容。即数据必须匹配N个规则才满足记录事件的条件，如果规则中应用了DLP策略规则必现，则N的数值不小于必现规则项的数量。如：“员工信息”策略包含4个规则，中国手机号码、中国大陆二代身份证、普通证书和合同，设置4选3，即3项员工信息同时匹配才为命中策略。

- 条件 - 策略检测条件，即该策略引用的策略检测条件。

以下列表显示所有可选的检测条件。点击链接进入相关章节获取更多信息。

- [关键字](#)
- [正则表达式](#)
- [脚本](#)
- [文件指纹](#)
- [数据库指纹](#)
- [字典](#)
- [文件名称](#)
- [文件类型](#)
- [文件大小](#)
- [附件数量](#)
- [智能学习](#)
- [ITM模板](#)
- [文件属性](#)
- [数据分类](#)
- [标签](#)

- 同时匹配内容 - 点击  同一规则设置多个同时匹配内容。配置多条同时匹配内容后，数据必须匹配所有规则才达到记录事件的条件。

## 策略通道

通道用于设置策略可以识别的协议以及方法，方便安全管理对其关注的代理协议进行管理。

策略通道可应用的常见场景包括：

- 出于安全需要，禁止员工向论坛、贴吧发表评论或上传文件
- 出于安全需要，禁止员工访问返回内容包含可执行文件的下载操作

在策略配置页面，点击通道选项卡即可配置策略适用的通道。

通道页面分为网络和终端两个部分。

- 网络通道所支持的通道类型如下：

网络通道	解释
HTTP	支持HTTP协议的Web网络通道内容检查。
HTTPS	支持HTTPS加密协议的Web网络通道内容检查。
FTP	支持FTP协议的网络通道内容检查。

网络通道	解释
IM	支持明文即时通信协议通道内容检测，如Skype、yahooschat。
自定义协议	支持对终端自定义协议进行内容检测。
网络打印	支持网络打印通道内容检测（安装打印代理SPA）。
云应用APP	支持通过第三方以API方式上传数据的云应用APP通道内容检测。
POP3	支持POP3接收邮件协议通道内容检测。
IMAP	支持IMAP接收邮件协议通道内容检测。
文件共享	支持通过数据发现方式主动扫描指定目录和文件，查找敏感数据源。
ActiveSync	支持ActiveSync协议对敏感数据检测。例如客户端通过MAG接收企业电子邮件。
邮件SMTP	支持SMTP协议通道的内容检测。可以指定邮件方向检测，例如入向邮件、出向邮件和内部邮件。 邮件中又包括： <ul style="list-style-type: none"> <li>• 入向邮件 - 发件人邮箱域名为非内部域名。</li> <li>• 出向邮件 - 发件人邮箱域名为内部域名。</li> <li>• 内部邮件 - DSG/SWG设备通过MTA设置的内部域名。</li> </ul>

- 终端通道所支持的通道类型如下：

终端通道	解释
HTTP	支持HTTP协议的Web终端通道内容检查。
HTTPS	支持HTTPS加密协议的Web终端通道内容检查。
FTP	支持FTP协议的终端通道内容检查。
IM	支持加密即时通信协议通道内容检测，如QQ、微信。
应用程序	支持指定应用程序做内容检测。应用程序中又包括 <ul style="list-style-type: none"> <li>• 拷贝剪切</li> <li>• 粘贴</li> <li>• 水印</li> <li>• 文件访问</li> <li>• 截屏</li> <li>• 下载</li> </ul>
终端打印	支持打印通道做内容检测，无需安装打印代理。
网络共享	支持通过数据发现方式主动扫描主机指定目录和文件，查找敏感数据源。
移动存储	支持对移动存储进行内容检测。
刻录	支持对刻录通道进行内容检测。
蓝牙	支持对蓝牙协议进行内容检测。
自定义协议	支持对终端自定义协议进行内容检测。
本地存储	控制终端用户下载服务器上的文件存储到本地。
邮件SMTP	支持SMTP协议通道的内容检测。可以指定邮件方向检测为出向邮件或内部邮件。

终端通道	解释
	邮件中又包括： <ul style="list-style-type: none"> <li>• 出向邮件 - 发件人邮箱域名为内部域名。</li> <li>• 内部邮件 - DSG/SWG设备通过MTA设置的内部域名。</li> </ul>

### 策略来源目标

点击来源/目标选项卡,在匹配或例外区域选择目标或来源，设置作用于策略的来源/目标。


- 1. 输入来源或目标的名称，可以用部门、用户名称、区域等命名。
- 2. 输入来源或目标的描述，详细描述此来源或目标项目的、作用范围等。
- 3. 添加来源/目标，可选择已添加于列表的目标或来源或手动添加。

#### 添加来源

选项	解释
电子邮件地址	输入发送者的电子邮件地址，多个电子邮件地址以逗号分隔。当类型为目标时，如果是选择文件中的邮件地址，支持UTF-8编码的CSV格式的文件导入目标电子邮件地址。
IP/IP段	输入发送者/接收者的IP地址或IP段，多个IP或IP段以逗号分隔。
用户目录	用户目录支持选择AD服务器或自定义用户目录，类型为用户、组、OU、计算机、自定义组织架构。支持在用户目录中搜索查询特定的用户、组织或计算机，默认检测所有用户。
终端属性	当终端作为来源时，请选择终端类型或位置进行内容分析。

#### 添加目标

选项	解释
电子邮件地址	输入发送者的电子邮件地址，多个电子邮件地址以逗号分隔。当类型为目标时，如果是选择文件中的邮件地址，支持UTF-8编码的CSV格式的文件导入目标电子邮件地址。
IP/IP段	输入发送者/接收者的IP地址或IP段，多个IP或IP段以逗号分隔。
域名	如果是输入域名，多个域名间以逗号分隔；如果是选择文件，支持UTF-8编码的CSV格式的文件导入目标电子邮件地址。
URL分类	设置访问的URL类别。可针对指定访问的URL分类进行DLP检测。
应用程序类别	设置访问的应用程序类别。可针对指定目标应用程序类别进行DLP检测。
终端设备	设置访问的终端设备。可针对指定目标终端进行DLP检测。
WebService应用	设置访问的云应用App类别。可针对指定云应用APP进行DLP检测。请参考 <a href="#">WebService应用</a> 。
用户目录	用户目录支持选择AD服务器或自定义用户目录，类型为用户、组、OU、计算机、自定义组织架构。支持在用户目录中搜索查询特定的用户、组织或计算机，默认检测所有用户。

4. 添加来源/目标的双向匹配，选择列表中已有项，点击进行添加。



注：当设置多个来源/目标项时，必须同时满足规则才可触发策略。



## 策略动作

点击动作选项卡，设置事件命中策略后，对其所执行的动作。

## 默认动作

1. 配置策略安全等级，指定命中策略时的事件严重程度，在事件及统计报告中可显示事件安全级别的详细数据。指定命中策略的事件安全级别为高、中、低和信息，用户可根据命中策略内容的敏感级别来定义。
2. 在命中策略后，配置不同协议通道对事件执行不同的动作。详细信息请参考[管理策略动作](#)。

选项	解释
审计	检测所有监控通道。
保护	检测所有保护通道。

3. 设置高级项，设置同一个用户/IP在一段时间内的不同阶梯触发敏感策略内容的执行行为。高级动作项支持三个阶梯段的动作项设置。

选项	解释
至少命中n次	设置触发策略次数，只有在累计到触发次数后，开始记录事件。
策略安全级别	指定触发策略内容的安全级别（高/中/低/信息）。
策略执行动作	指定触发策略内容后执行的动作，默认为审计。

## 零星式泄露防护

DLP系统零星式泄露防护针对某段时间内持续泄露内容的行为进行防护，当某一用户行为单次或一段时间内累计匹配策略或内容时，将根据规则创建事件。

配置零星式泄露防护时，对于不同触发条件（时间段）触发策略或匹配内容的数量，时间段长的必须多于时间段短的；同一时间段内最多可配置三条规则，且触发触发策略或匹配内容的数量需依次增加。当多个条件里的事件等级冲突时，则合并冲突等级，记录最高事件等级。

1. 计算匹配的方式，指定零星式防护类型，包含策略和内容。

选项	解释
选择策略	统计触发策略的次数。
选择内容	统计触发内容的次数。

2. 指定触发时段，设置零星式防护统计时段（5分钟/15分钟/30分钟/每1小时/每4小时/每8小时/每24小时），最多可选5个时段。
3. 设置触发策略/内容次数，只有在累计到触发次数后，开始记录事件。
4. 指定触发策略内容的安全级别（高/中/低/信息）。
5. 指定触发策略内容后执行的动作，默认为审计。

## 根据向导创建策略

在DLP管理 > 策略页面基于向导快速创建策略。

向导页面包含组织所属行业，想要保护的敏感数据和触发规则时处理动作，帮助用户快速创建策略。

1. 选择DLP管理 > 策略，点击添加，选择从向导添加，配置所需策略。
2. 根据用户自身实际情况，选择组织所属行业。
3. 根据用户自身实际情况，组织所属的国家或地区。
4. 根据用户自身实际情况，选择想要保护的内容和发现违规时的处理动作。



注：要保护的内容这一项对应系统预置的DLP策略模板，启用后根据策略对企业数据执行扫描检测，对命中策略的事件执行策略动作。

5. 点击确定，新建策略模板保存于策略列表中。

通过向导创建策略模板


字段	解释		
行业	保护内容	策略名称	描述
一般企业/互联网软件/金融/保险	机密信息	并购信息	检测有数据泄露风险的并购信息
		专利信息	检测有数据泄露风险的专利信息
		帐号密码信息	检测有数据泄露风险的帐号密码信息
		企业信息	检测有数据泄露风险的企业信息
		战略计划	检测有数据泄露风险的战略计划信息
		机密信息	检测有数据泄露风险的机密信息
一般企业/互联网软件/金融/保险	人事信息	社会保障号码	检测有数据泄露风险的社会保障号码
		求职信息	检测求职相关词汇的使用
		员工信息	检测有数据泄露风险的员工信息
		薪酬信息	检测有数据泄露风险的薪酬信息
一般企业/互联网软件/金融/保险	可疑数据	未知类型文件	检测有数据泄露风险的未知类型文件
		压缩文件	检测有数据泄露风险的压缩文件
		MicrosoftOffice文件	检测有数据泄露风险的Microsoft Office文件
		多个邮件地址	检测有数据泄露风险的多个收件人的邮件通信
		加密文件	检测有数据泄露风险的加密文件
一般企业/互联网软件/金融/保险	财务数据	财务信息	检测有数据泄露风险的财务信息
		价格信息	检测有数据泄露风险的价格信息
		薪酬信息	检测有数据泄露风险的薪酬信息
一般企业/互联网软件/金融/保险	IT数据	帐号密码信息	检测有数据泄露风险的帐号密码信息
		网络拓扑图	检测有数据泄露风险的网络拓扑图
		网络地址信息	检测有数据泄露风险的网络地址信息
		密码文件	检测有数据泄露风险的密码文件
一般企业/互联网软件/金融/保险	客户和员工数据	员工信息	检测有数据泄露风险的员工信息
		客户数据	检测有数据泄露风险的客户数据

字段	解释		
一般企业/互联网软件 /金融/保险	支付数据	中国PII	检测中国PII(Personally identifiable information)个人识别信息
		支付卡行业数据安全标准PCI-DSS	检测标准的信用卡数据，支付卡行业 (PCI) 数据安全标准 (DSS) 由主要支付卡公司 (示例 Visa、MasterCard、American Express ) 联合确定
		SWIFT代码	检测SWIFT代码的使用，SWIFT(环球同业银行金融电讯协会) 代码标识所涉及的银行、位置和分支机构，在各银行之间转帐 (主要是跨国转帐) 时使用
		信用卡磁条	检测有数据泄露风险的信用卡磁条信息
		银行卡号	检测有数据泄露风险的银行卡号
互联网软件	恶劣词汇	成人信息	检测成人信息的使用
		暴力与武器	检测暴力与武器词汇的使用
		种族歧视	检测种族歧视语言的使用
		攻击性语言	检测攻击性语言的使用
保险	保险数据	药品编码	检测国家药品编码的使用
		保险信息	检测有数据泄露风险的保险信息
		理赔信息	检测有数据泄露风险的理赔信息
		客户数据	检测有数据泄露风险的客户数据
联网软件	软件开发	项目数据	检测有数据泄露风险的项目数据
		产品设计文档	检测有数据泄露风险的产品设计文档
		计算机辅助设计文档	检测有数据泄露风险的设计文档
		源代码	检测有数据泄露风险的源代码

#### 根据模板创建策略

在DLP管理 > 策略页面基于预置模板快速创建策略。

DLP系统预置大量常用合规性策略模板，可以快速有效的创建策略，检测敏感内容。

1. 选择DLP管理 > 策略，点击添加，选择从模板添加，配置所需策略。
2. 点击 选择所需策略模板：预置策略模板或自定义模板。支持同时选中多个模板添加策略，每个模板会创建一条策略。预置策略模板的详细信息请参考[查看预置DLP策略模板](#)。
3. 选择策略归属的策略组，默认为默认策略组。策略组由管理员自定义，详细信息请参考[添加策略组](#)。
4. 设置策略所属的策略等级，即将策略分级。DLP策略支持30个等级和默认等级，数值越小等级越高，默认设置为默认等级。



注：

- 一个策略只能属于一个策略等级，一个策略等级可以包含多个策略；

- 策略根据策略等级由高到低进行执行，同一等级下的策略均会被扫描执行；本等级出现策略命中后，不会再扫描执行下一等级策略；本等级没有命中任何策略时，则会继续扫描执行下一等级策略。
- 系统支持三层分级对象，一层分级对象有权限设置的策略等级为1-30和默认等级；二层分级对象有权限设置的策略等级为11-30和默认等级；三层分级对象有权限设置的策略等级为21-30和默认等级。

5. 设置命中策略后，执行的动作项。

审计	检测所有监控通道。
保护	检测所有保护通道。

6. 点击确定，新建策略模板保存于策略列表中。

#### DLP策略必现

在创建DLP策略时可配置策略必现功能。

DLP策略规则必现项功能，丰富配置检测内容的匹配项，即该规则必须命中策略，再匹配其它规则。

例如：“员工信息”策略包含多个规则，中国手机号码、中国大陆二代身份证、普通证书和合同。其中，大陆身份证号(二代)和合同两项规则设置为必现，则必须匹配大陆身份证号(二代)和合同规则，剩余其它2条规则再任意匹配1条即为命中策略。

如果同时应用DLP策略M选N（数据必须匹配N个规则才达到记录事件的条件）和DLP策略规则必现两项功能，则N不能小于必现规则的数量。

例如：“员工信息”策略包含多个规则，中国手机号码、中国大陆二代身份证、普通证书和合同。其中大陆二代身份证和合同这两项规则设置为必现，如果应用DLP策略M选N，则N可选数值不能小于2。如果DLP策略M选N的规则是4选3，则必选匹配大陆身份证号(二代)和合同两项规则外，剩余其它2条规则再任意匹配1条即为命中策略。

#### 策略批量管理

在DLP管理 > 策略页面进行策略批量管理。

DLP策略支持批量修改、添加和删除已设置的策略。

- 选择DLP管理 > 策略，点击批量修改，批量修改策略。
- 从已有的策略列表中，勾选需要批量管理的策略项。
- 选择以下策略配置项进行修改：

策略组	点击策略组，批量修改策略组。
策略等级	点击策略等级，批量修改策略等级。支持管理员调整预置ITM安全策略的等级。
策略类型	批量编辑/添加策略类型。非批量添加的策略，不会更改原有策略类型设置。
检测内容	批量添加、修改、删除检测内容。非批量添加的策略，添加、修改不会更改原有策略类型设置。支持批量删除功能。
通道	批量添加、修改策略通道。非批量添加的策略，不会更改原有策略类型设置。
来源/目标	批量添加、修改、删除来源/目标项。非批量添加的策略，添加、修改不会更改原有策略类型。
动作	批量修改策略动作项。支持批量删除功能。

4. 修改完成后，点击保存。

## 查看预置DLP策略模板


介绍查看DLP预制策略模板的步骤。

### 数据安全预制策略模板

天空卫士™ 安全鳄® 统一内容安全UCS 数据安全解决方案提供了预制的策略模板，以帮助安全管理员用于创建和编辑数据安全策略。

#### 查看策略模板

按照以下步骤查看数据安全策略模板。

1. 点击进入DLP管理 > 策略 > 根据模板创建策略页面。
2. 点击  按钮，进入选择策略模板对话框。

系统预制的数据安全策略模板显示在对话框的左侧。

### DLP策略内容匹配和例外

创建和修改策略时，在检测内容选项卡下，可以添加匹配和添加例外。天空卫士™数据安全支持一下内容匹配和例外项。参考对应的自章节查看具体的设置信息。

- 关键字
- 正则表达式
- 脚本
- 文件指纹
- 数据库指纹
- 字典
- 文件名称
- 文件类型
- 文件大小
- 附件数量
- 智能学习
- ITM模板
- 文件属性
- 分类
- 标签


#### 关键字匹配/例外


描述要保护数据的关键字信息。

策略添加关键字匹配可以保护和分析内部数据，例如识别公司员工发往外部的数据包含“最高机密”、“保密”、“内部机密”和“营业执照号”等关键信息。

关键字不需要预定义，直接输入一个或多个关键字即可。

1. 输入关键字规则项名称和描述，表明其作用。
2. 设置规则是否必现，策略命中前提是该规则必须命中，再匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 设置关键字匹配方式，可选择如下匹配方式：

匹配	介绍
任意关键字	输入要检测的关键字信息，可输入多个。
关键字对	输入要检测的关键字对，点击  添加到列表。

匹配	介绍
	 注：一对关键字必须同时出现，且匹配两者的间隔字符数，才会命中策略。

4. 设置匹配条件，可选择如下匹配条件：

匹配	介绍
最少匹配	填写最小匹配阈值，当分析内容匹配次数达到阈值，才会命中策略。
不匹配	当分析内容与关键字不同的时候，会命中策略。
统计重复内容	关键字匹配记录统计重复次数。如果不选择此项，每个关键字最大匹配次数为1。
精确匹配	不进行分词检测，进行全文正则检测。精确匹配可以检测示例检测内容包含的符号字符。
自动匹配简体/繁体中文	同时支持繁简体检测。

5. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。


6. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。

7. 点击确定保存设置。

#### 脚本匹配/例外

用系统预置脚本描述要保护的数据。


系统预置脚本描述要保护的数据，并支持在所有策略中复用。

1. 输入脚本名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 点击，从弹出的列表中选择策略中引用的脚本。
4. 选择是否启用脱敏数据。启用后，匹配信息部分数据将以\*代替，并在事件、报告和通知中展示。匹配详情及证据显示将对敏感数据信息增加干扰，不能查看脱敏数据。
5. 设置匹配条件，可选择如下匹配条件：

最少匹配	填写最小匹配阈值，当分析内容匹配次数达到阈值，才会命中策略。
不匹配	当分析内容与正则表达式不同时命中策略。
统计重复内容	关键字匹配记录统计重复次数。如果不选择此项，每个关键字最大匹配次数为1。

6. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

7. 从同时匹配下拉框中选择其他内容匹配项，点击为也可以不设置同时匹配。
8. 点击确定保存设置。

#### 正则表达式匹配/例外

用正则表达式模型描述要保护的数据。

用正则表达式模型描述要保护的数据，分为预定义和自定义正则表达式，并支持在所有策略中复用。正则表达式最多可设置1000条。

 注：

- 使用中的正则表达式和预置正则表达式不可被删除，删除时会提示报错；
- 预置正则默认不显示，预置的正则表达式默认排序位于自定义正则表达式之后。

1. 输入正则表达式规则名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 设置正则表达式匹配方式，从下拉菜单选择新建正则或选用预置正则：


选择预置	从列表中选择策略中引用的正则表达式。
新建	在显示的添加正则表达式框内添加定义的正则表达式。

4. 选择是否启用脱敏数据。启用后，匹配信息部分数据将以\*代替，并在事件、报告和通知中展示。匹配详情及证据显示将对敏感数据信息增加干扰，不能查看脱敏数据。
5. 设置匹配条件，可选择如下匹配条件：

最少匹配	填写最小匹配阈值，当分析内容匹配次数达到阈值，才会命中策略。
不匹配	当分析内容与正则表达式不同时命中策略。
统计重复内容	关键字匹配记录统计重复次数。如果不选择此项，每个关键字最大匹配次数为1。

6. 设置Email匹配属性，可选择如下属性：


匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

7. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
8. 点击确定保存设置。


#### 文件指纹匹配/例外

用文件指纹信息来描述需要保护的数据。

文件指纹使用爬虫工具扫描文件内容，形成指纹信息做相似度匹配。文件指纹支持本地上传和两种文件共享方式（Samba和NFS）。DLP策略引用的文件指纹需预置。

1. 输入文件指纹名称和描述，表明其作用。
2. 设置该规则是否必现，策略命中前提是该规则必须命中，再匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 点击，从弹出的列表中选择策略中引用的文件指纹。
4. 设置文件指纹中指纹相似度阈值（范围为10%、20%、30%、40%、50%、60%、70%、80%、90%），当指纹匹配的相似度大于等于设定的阈值时被认为与策略相匹配。
5. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

6. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
7. 点击确定保存设置。

#### 数据库指纹匹配/例外

用数据库指纹信息来描述需要保护的数据。

数据指纹由爬虫工具扫描数据库表里的每个单元格信息获取，与向外传送的数据内容做数据库指纹匹配。数据库指纹支持的数据库类型有SQLserver、Oracle、MySQL、Postgresql和DB2等。DLP策略引用的数据库指纹需预先设置。


1. 输入数据库指纹名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 设置数据库指纹匹配条件，从下拉框中选择指定引用的数据库类型。
4. 选择是否启用脱敏数据。启用后，匹配信息部分数据将以\*代替并在事件、报告和通知中展示。匹配详情及证据显示将对敏感数据信息增加干扰，因此不支持查看脱敏数据。
5. 设置匹配条件，可选择如下匹配条件：

最少匹配	填写最小匹配阈值，当分析内容匹配次数达到阈值，才会命中策略。
不匹配	当分析内容与正则表达式不同时命中策略。

6. 设置Email匹配属性，可选择如下属性：



匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。


7. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
8. 点击确定保存设置。

#### 字典匹配/例外

用关键字和权重结合的方式描述要保护的数据。

字典匹配就是按照关键字和权重结合的方式描述要保护的数据，权重是指字典在整体检测中相对重要程度。

1. 输入字典规则项名称和描述，表明其作用。
2. 设置规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 设置字典匹配方式，从下拉菜单选择新建或选用预置字典：

选择预置	点击  ，从弹出的列表中选择策略中引用的字典。
新建	在添加框内添加定义的字典。

4. 设置匹配条件，可选择如下匹配条件：

触发阈值	当分析内容匹配次数达到阈值，才会命中策略。
不匹配	当分析内容与关键字不同的时候，会命中策略。
统计重复内容	关键字匹配记录统计重复次数。如果不选择此项，每个关键字最大匹配次数为1。
精确匹配	不进行分词检测，进行全文正则检测。精确匹配可以检测示例检测内容包含的符号字符。
自动匹配简体/繁体中文	同时支持繁简体检测。

5. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

6. 从同时匹配下拉框中选择其他内容匹配项，点击设置多个同时匹配内容。也可以不设置同时匹配。
7. 点击确定保存设置。


### 文件名称匹配/例外

以自定义方式添加文件或附件名称。

DLP策略支持检测文件和附件名称，并支持多个文件或附件名称检测。

1. 输入文件名称规则的名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 输入需要检测的文件或附件名称。
4. 设置Email匹配属性，可选择如下属性：


匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

5. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
6. 点击确定保存设置。


### 文件类型匹配/例外

用文件类型描述要保护的数据。

文件类型可预置也可在创建策略时自定义，并支持在所有策略中复用。文件类型最多可设置1000条。

1. 输入文件类型规则的名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 点击，从弹出的列表中选择策略中引用的文件类型。
4. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封（收件人地址）、首部（用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject）、正文（发送方发给接收方的内容，如body、attachment）。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

5. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
6. 点击确定保存设置。

### 文件大小匹配/例外

用文件或附件的大小描述需要保护的数据。

DLP策略支持检测文件大小和附件大小，并支持检测多个文件或附件的大小，但总大小不能超过2GB。

1. 输入检测规则的名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。

3. 设置检测文件大小范围 ( 大于/小于/介于 ) ，单位可选B/KB/MB/GB。
4. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封 ( 收件人地址 ) 、首部 ( 用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject ) 、正文 ( 发送方发给接收方的内容，如body、attachment ) 。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

5. 从同时匹配下拉框中选择其他内容匹配项，允许为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
6. 点击确定保存设置。


#### 附件数量匹配/例外

用附件数量描述需要保护的数据。

DLP策略支持检测附件数量，并支持检测多个附件数量。

1. 输入检测规则的名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 设置检测附件数量范围 ( 大于/小于/介于 ) ，数量范围为1~9999。
4. 设置Email匹配属性，可选择如下属性：


匹配	介绍
全部内容	检测Email所有属性，包含信封 ( 收件人地址 ) 、首部 ( 用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject ) 、正文 ( 发送方发给接收方的内容，如body、attachment ) 。
指定内容	指定Email检测属性，可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

5. 从同时匹配下拉框中选择其他内容匹配项，点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
6. 点击确定保存设置。

#### 智能学习匹配/例外


使用智能学习任务检测并保护数据。

智能学习通过正向学习受保护数据的样例，提炼相似信息形成策略规则元素，并在所有策略复用。智能学习支持导出和导入已有的智能学习任务。

1. 输入检测规则的名称和描述，表明其作用。
2. 设置该规则是否必现，即策略命中前提是必须命中该规则，再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 设置智能学习匹配条件。点击，从弹出的列表中选择策略中引用的智能学习任务。
4. 设置Email匹配属性，可选择如下属性：

匹配	介绍
全部内容	检测Email所有属性，包含信封 ( 收件人地址 ) 、首部 ( 用户代理或者邮件服务器添加的信息，如Received、Message-ID、From、Data、Reply-

匹配	介绍
	To、X-Phone、X-Mailer、To和Subject)、正文(发送方发给接收方的内容,如body、attachment)。
指定内容	指定Email检测属性,可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。


5. 从同时匹配下拉框中选择其他内容匹配项,点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
6. 点击确定保存设置。

### ITM模板匹配/例外

应用ITM模板检测并保护数据。

在ITP防护中,系统预置ITM压缩文件深度模板和ITM实际文件类型策略模板,分别检测压缩文件的压缩层数和实际文件类型。


- ITM压缩文件深度模板检测压缩文件的压缩层数,默认检测超过3层的压缩文件,检测范围为3~20层;
- ITM实际文件类型模板检测实际文件类型,判断扩展名与实际类型不匹配的文件,默认检测文件类型:Office办公、压缩和图像文件。

1. 输入ITM模板规则项名称和描述,表明其作用。
2. 设置该规则是否必现,即策略命中前提是必须命中该规则,再继续匹配其它规则。详细信息请参考[DLP策略必现](#)。
3. 点击,从弹出的列表中选择策略中引用的ITM模板。
4. 设置匹配条件,可选择如下匹配条件:

最少匹配	填写最小匹配阈值,当分析内容匹配次数达到阈值,才会命中策略。
不匹配	当分析内容与正则表达式不同时命中策略。
统计重复内容	关键字匹配记录统计重复次数。不选择此项,每个关键字最大匹配次数为1。

5. 设置Email匹配属性,可选择如下属性:

匹配	介绍
全部内容	检测Email所有属性,包含信封(收件人地址)、首部(用户代理或者邮件服务器添加的信息,如Received、Message-ID、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject)、正文(发送方发给接收方的内容,如body、attachment)。
指定内容	指定Email检测属性,可选择正文、附件、主题、收件人、发件人、抄送接收方、密送接收方、所有邮件头或自定义邮件头。

6. 从同时匹配下拉框中选择其他内容匹配项,点击为同一规则设置多个同时匹配内容。也可以不设置同时匹配。
7. 点击确定保存设置。

### 分类匹配/例外

应用数据分类匹配和例外。


DLP策略支持检测数据分类。参考[管理数据分类](#) on page 181获取详细的数据分类介绍。

1. 输入名称和描述,表明其作用。
2. 选择是否必现。

3. 在条件框里，点击  选择已有的数据分类。
4. 点击确定保存。

标签匹配/例外  
应用标签匹配和例外。

DLP策略支持检测标签。参考[标签管理](#) on page 214获取详细的标签介绍。

1. 输入名称和描述，表明其作用。
2. 选择是否必现。
3. 在条件框里，点击  选择已有的标签。
4. 在条件框里，选择匹配Email的全部内容或者根据需要自定义指定内容。
5. 点击确定保存。

## 数据分类

介绍检测条件中的数据分类及其相关知识。

数据分类功使得安全管理员能够基于用户生成的数据分类信息来制定数据安全策略。

天空卫士™提供的的数据分类功能使得企业安全管理员获得一种超越当前策略规则的数据安全解决方案 - 基于数据分类的数据安全解决方案。

数据分类元数据来自企业安全管理员和涉及企业安全的最终用户，在制定企业安全策略时，这可以基于数据分类进行识别和保护，确保数据安全解决方案的落实准确而具有针对性，有效提高检出率和减少误报。

### 管理数据分类

在DLP管理 > 数据分类 > 分类页面管理数据分类的规则信息。

数据分类配置页面，用于定义数据分类包含的规则项，数据分类定义由现有的规则类型及标签组成。

页面支持的定义数据分类的规则包含：

- 关键字
- 正则表达式
- 脚本
- 文件指纹
- 数据库指纹
- 字典
- 文件名称
- 文件类型
- 文件大小
- 附件数量
- 智能学习
- ITM模板
- 文件属性
- 标签

### 创建一条分类

以下步骤介绍了如何创建一条分类级别：

1. 进入DLP管理 > 数据分类 > 分类页面，点击添加按钮。
2. 在添加分类页面，输入新建分类的名称和描述信息。
3. 在分类级别下拉选项框选则其归属的分类级别。
4. 在检测内容标签下面，设置匹配项。
5. 点击保存。

### 管理分类级别

在DLP管理 > 数据分类 > 分类级别页面管理数据分类的级别以及相关信息。

分类级别支持新建、编辑、删除等操作，被某一分类引用中的分类级别不可被删除。

分类级别页面显示以下项目。

- 名称：显示预置或者自定义的分类级别，如普通商密、机密、核心商密、内部公开、外部公开等。
- 描述：分类级别的描述信息。
- 上次更新时间：显示数据分类创建或最近一次变更时间。
- 使用状态：展示分类级别被数据“分类”引用状态。
- 创建者：显示分类的创建者。

### 创建一条分类级别

以下步骤介绍了如何创建一条分类级别：

1. 进入DLP管理 > 数据分类 > 分类级别页面，点击添加按钮。
2. 在添加分类级别页面，输入新建分类的名称和描述信息。点击保存。
3. 返回分类级别页面，

查看分类级别的使用情况

1. 进入DLP管理 > 数据分类 > 分类级别页面，在使用状态一栏，可以查看该条分类级别是否被使用。
2. 点击进入该分类级别，在使用详情一栏，可以查看使用了该分类级别的分类名称和类型。

## 策略元素

在DLP管理 > 策略元素页面管理数据安全策略元素。

数据安全策略预定义多种策略元素用于创建策略时配置检测内容。

数据安全策略包含以下元素：


- 策略组
- 来源/目标
- Webservice应用
- 策略动作
- 策略通知
- 动作脚本
- 数据聚类
- 策略模板

系统初始化时，每个策略元素都包含有预置内容，管理员可以调整策略元素中的内容。

### 策略组

在DLP管理 > 策略元素 > 策略组页面管理策略组。

策略组将多个相关联的策略分组，用于事件管理、监控及报告统计的配置。

 注：一个策略组里可以包含多个策略，一个策略仅能归于一个策略组。

1. 选择DLP管理 > 策略元素 > 策略组，策略组列表包含预置的默认策略组，新建策略会默认分配给默认策略组。
2. 点击添加，新建策略组，输入策略组名称和描述。
3. 点击保存，新建策略组显示在列表中。

表 70: 页面图标和行间操作按钮功能

图标	解释
	编辑策略组，可查看策略组最后修改时间，创建者信息和策略组使用情况。默认策略组不可编辑。
	删除策略组。使用中的策略组不可以删除。

## 来源和目标

在DLP管理 > 策略元素 > 来源/目标页面管理来源和目标。



根据用户、IP地址、Email地址及域名，设置指定的策略源或目标的匹配或者例外。

1. 选择DLP管理 > 策略元素 > 来源/目标，点击添加，分别新建来源或目标。
2. 输入策略来源或目标名称和描述，表明其用于检测匹配或例外。
3. 选择类型，指定策略源（发送者），或者策略目标（接收者）。根据需要进行以下配置：

电子邮件地址	输入发送者的电子邮件地址，多个电子邮件地址以逗号分隔。当类型为目标时，支持UTF-8编码的CSV格式的文件导入目标电子邮件地址。
IP/IP段	输入发送者/接收者的IP地址或IP段，多个地址以逗号分隔。
用户目录	添加AD服务器或自定义用户目录，类型可以为用户、组、OU、计算机或自定义组织架构。支持在用户目录中搜索查询特定的用户、组织或计算机，并默认检测所有用户。
终端属性	当终端作为来源时，请选择指定类型或位置的终端进行内容分析。
域名	输入域名，多个域名间以逗号分隔；如果是选择文件，支持UTF-8编码的CSV格式的文件导入域名。
URL分类	设置访问的URL类别。可针对指定访问的URL分类进行DLP检测。
应用程序类别	设置访问的应用程序类别。可针对指定目标应用程序类别进行DLP检测。
终端设备	设置访问的终端设备。可针对指定目标终端进行DLP检测。
WebService应用	设置访问的云应用App类别。可针对指定云应用App进行DLP检测。请参考 <a href="#">WebService应用</a> 。

4. 点击保存，新建来源和目标显示在列表中。

表 71: 页面图标和行间操作按钮功能

图标	解释
	编辑来源/目标，可查看来源/目标最后修改时间，创建者信息和策略使用情况。
	删除来源/目标。



## WebService应用

在DLP管理 > 策略元素 > WebService应用页面管理WebService应用，检测第三方敏感内容。

DLP预先定义WebService应用通道后，将WebService应用通道唯一ID同步到第三方，第三方绑定此WebService应用通道ID向DLP系统发送敏感文件，对其进行内容检测。

1. 选择DLP管理 > 策略元素 > WebService应用，点击添加，新建WebService应用。
2. 输入WebService应用名称和描述信息，表明该WebService应用的作用。
3. 点击保存，新建WebService应用显示在列表中，并显示WebService应用唯一ID（添加时ID由系统自动生成）。

表 72: 页面图标和行间操作按钮功能

图标	解释
	编辑WebService应用，可查看最后修改时间，创建者信息和动作脚本使用情况。
	删除WebService应用。使用中的云应用APP不可以删除。

## 策略动作

在DLP管理 > 策略元素 > 策略动作页面管理策略动作。

事件命中策略后，对所有协议通道指定不同的动作，这些动作组合称为策略动作。系统包含的预置策略动作有保护（检测所有保护通道）和审计（检测所有监控通道）。

1. 选择DLP管理 > 策略元素 > 策略动作，列表包含预置的策略动作，点击添加，新建策略动作。
2. 输入策略动作名称和描述，表明该策略动作的作用。
3. 为网络通道和终端通道协议配置动作：

策略动作	解释
阻止	阻断网络传输（对邮件通道无效，邮件通道类似阻止的动作是隔离）。
放行	对命中策略后的事件做日志记录，不影响用户访问网络，对所有通道有效。
删除附件	只适用于邮件通道，邮件附件被删除，收件人不会收到附件。
隔离	只适用于邮件通道，隔离的邮件和事件一起被存储到证据文件中，管理员可手动释放或在邮件审核后释放。在隔离条件下，邮件支持不审批、一级审批和二级审批，每一级的审批流程将被管理平台记入事件历史。
内容加密	只适用于邮件通道，命中策略后由SMTP模块加密传输。
第三方加密	只适用于邮件通道，命中策略后发给第三方加密网关加密。
水印	只适用于终端通道，命中策略的文件会包含水印信息。



4. 在命中DLP策略后，选择是否记录事件及其证据文件和发送邮件通知。



记录事件	选择是否记录事件信息，默认启用。启用后，可选择记录证据文件或将事件信息发送到指定收件人。
记录证据文件	对命中策略的事件的原文内容进行证据记录，默认不启用。
发送邮件通知	选择发送邮件通知模板，默认支持4种预置通知模板发送到指定的收件人。启用后，策略匹配后将根据模板发送策略通知。自定义策略通知请参考 <a href="#">管理策略通知</a> 。

5. 点击保存，新建策略动作显示在列表中。

表 73: 页面图标和行间操作按钮功能

图标	解释
	编辑策略动作，可查看最后修改时间，创建者信息和策略动作使用情况。
	删除策略动作。已使用的策略动作不可以删除。


#### 策略通知

在DLP管理 > 策略元素 > 策略通知页面管理策略通知。

事件命中策略之后，在执行动作的同时发送通知。

系统预置4类通知模板，也可以自定义通知模板供管理员选择，通知的邮件内容可以定制，包括Logo、公司名称、主题和正文内容等。

1. 选择DLP管理 > 策略元素 > 策略通知，点击添加，新建策略通知。
2. 输入策略通知名称和描述，表明该策略动通知的作用。
3. 设置以下通知属性：

发件人名称	输入发件人名称，默认为事件通知。
发件人Email	设置事件通知的发件人邮箱。若要通过回复通知邮件释放被隔离的邮件，可设置一个不存在的外部邮箱地址，系统默认添加Notification@company-release.com，并且确保该回复的邮件投递经过DSG。
邮件服务器	设置发现策略通知的邮箱服务器。
选择收件人	选择策略通知的接收方，直接勾选来源、策略所有者、主管、目标(仅SMTP事件)或审批员，也可点击  按钮通过AD信息和自定义组织架构添加通知的接收方。 或者自定义接收邮件通知的接收方的地址。
邮件格式	设置发送策略通知格式，支持HTML和纯文本格式。

4. 设置通知模板，并勾选策略通知可选内容，包括LOGO、公司名称、动作、事件详细信息、邮件原文、邮件审核（仅网络邮件）、邮件 workflow 和审批平台等。

主题	设置通知模板主题。默认主题变量为%策略名称%；点击添加主题变量%策略名称%%规则名称%%动作%%策略所有者%%事件ID%%来源%%目标%%安全级别%%检测时间%%事件时间%%详细信息%%通道%。
正文	设置通知模板主题。默认为%规则名称%；点击添加正文 %规则名称%%策略名称%%动作%%策略所有者%%事件ID%%来源%%目标%%安全级别%%检测时间%%事件时间%%详细信息%%通道%。

5. 点击保存，新建策略通知显示在列表中

表 74: 页面图标和行间操作按钮功能

图标	解释
	编辑策略通知模板，可查看最后修改时间，创建者信息和使用的动作。
	删除策略通知模板。已使用的策略通知模板不可以删除。

#### 动作脚本

在DLP管理 > 策略元素 > 动作脚本页面管理动作脚本。

动作脚本仅在数据发现下面的网络任务和终端任务使用，在命中策略后，网络任务或终端任务执行指定的脚本。点击[数据发现](#) on page 215获取更详细的数据发现介绍。

下面步骤描述了如何创建一个动作脚本，并且应用在数据发现任务中：

1. 选择DLP管理 > 策略元素 > 动作脚本，点击添加，新建动作脚本。
2. 输入动作脚本名称和描述，以表明该动作脚本的作用。
3. 点击选择文件，上传所创建的脚本文件。
4. 输入脚本执行参数。
5. 点击保存，新建动作脚本显示在列表中。此时的脚本使用状态是未使用
6. 选择DLP管理 > 数据发现 > 终端任务。在任务列表里，点击进入一个任务进行编辑。
7. 在编辑终端任务页面，点击动作选项卡，启用保护。
8. 选中补充脚本，在选择脚本的下拉菜单中，选择刚刚创建的动作脚本。点击保存
9. 回到DLP管理 > 策略元素 > 动作脚本页面，可以看到动作脚本的使用状态为是使用中。

#### 策略模板

在DLP管理 > 策略元素 > 策略模板页面管理策略模板。

策略模板可用于快速部署策略，有效避免策略中的错误和信息漏洞。策略模板支持导入和导出功能。预置模板通过配置策略检测内容匹配项和例外项作为模板。

1. 选择DLP管理 > 策略元素 > 策略模板，点击添加，新建策略模板：
2. 输入策略模板名称和描述，以表明该策略模板的作用。
3. 设置来源Risk Level，如果用户的来源Risk Level评分高于设置值，将使用该策略匹配动作进行拦截保护。

 注：配置前需要开启ITM功能。

4. 设置策略模板检测匹配项或例外项。
5. 点击保存，新建策略模板显示在列表中。



表 75: 页面图标和行间操作按钮功能

图标	解释
	编辑策略模板，可查看最后修改时间和创建者信息。
	删除策略模板。使用中的策略模板不可以删除。
	导入从其它环境导出的策略模板或者自定义的策略模板文件。
	导出策略模板到本地。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

### 数据聚类

在DLP管理 > 策略元素 > 数据聚类页面管理数据聚类。

UCSS管理平台整合聚类工具，提取数据样本的语义信息生成分类结果，可用于创建智能学习任务。新建数据聚类需要选择文件来源，配置过文件过滤器过滤影响聚类结果的文件，在获取的文件中排除干扰文字信息来增强精准度。

- 选择DLP管理 > 策略元素 > 数据聚类，点击添加，新建数据聚类。
- 输入数据聚类名称和描述，以表明其作用。
- 选择样本语言，即选择检测文档样本的语言为中文或者英文。
- 点击文件来源选项卡，配置远程服务器获取检测文件：
  - 选择以哪种网络共享方式获取用于数据聚类的文件，支持SMB和NFS。
  - 输入共享服务器用户名称、密码或域名。
  - 输入所获取文件在远程服务器的存放目录。该文件夹必须真实存在，且具备可写权限。
  - 输入共享服务器用户名称、密码或域名。
  - 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
  - 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。
  - 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。
- 点击过滤器选项卡，配置如下参数，过滤出所需文件：
  - 选择过滤的文件类型，按照过滤设置的文件类型进行指纹识别。
    - 包括文件类型：列出要识别的文件类型。单击从预定义文件类别中选择要过滤的文件类型。如：  
\*.doc; \*.xls; \*.ppt; \*.pdf;
    - 排除文件类型：列出要排除的文件类型。单击从预定义文件类别中选择不进行过滤的文件类型。如：  
\*.doc; \*.xls; \*.ppt; \*.pdf;









 注：如果包括文件类型和排除文件类型存在相同内容，采用排除优先原则。
  - 选择文件大小进行过滤(0~999 B/KB/MB)，大于100MB的文件直接放行。
  - 选择文件的生成日期进行过滤，即只采集设定日期的文件。
- 点击排除语义选项卡，输入不用于数据聚类分析关键字，点击添加到排除语义列表。点击批量导入关键字，支持UTF-8编码的txt文件。点击删除列表中所选的关键字。
- 点击保存，新建策略模板显示在列表中。

表 76: 页面图标和行间操作按钮功能

图标	解释
	查看数据聚类任务运行详情。详细信息请参考 <a href="#">查看数据聚类任务详情</a> 。
	删除数据聚类任务。运行中的数据聚类不可以删除。
	运行数据聚类任务，任务状态为运行中。
	停止运行中的数据聚类任务，任务状态显示为已停止。

查看数据聚类任务详情

在DLP管理 > 策略元素 > 数据聚类页面查看数据聚类任务详情。


点击，进入数据聚类任务详情查看页面。属性信息如下：

表 77: 数据聚类任务详情

基本信息	
任务名称	显示数据聚类任务名称。
任务状态	显示该数据聚类任务状态，包含空闲/运行中/已完成/失败/已停止。
聚类结果	
文件总数	显示数据聚类任务扫描的文件总数。
扫描文件大小	显示扫描的文件总大小。
分类数量	显示数据聚类任务中文件的分类数量。
当前聚类状态	
扫描文件数量	显示数据聚类任务扫描的文件总数。
扫描文件大小	显示扫描的文件总大小。
扫描进度	显示实时扫描进度 ( 0%-100% ) 。
扫描完成的文件数量	显示实时扫描文件完成的数量。
扫描失败的文件数量	显示实时扫描失败的文件数量，如文件过小或无法提取文件内容。
过滤掉文件数量	显示过滤器过滤掉的文件数量。
聚类详细列表	
相似度	选择扫描文件的相似度阈值，高于该相似度阈值的文件归为一类，说明每组分类中文件间的相似度大于等于该阈值。
分类	根据相似度动态显示文件分类。点击  修改文件名称；点击分类名称显示语义和文件。
语义	数据聚类任务提取出的关键字及其所占权重、本分类中关键字计数和在其他分类中该关键字的计数。

文件	显示该分类包含的文件信息。
创建智能学习	点击创建智能学习跳转至智能学习页面，根据数据聚类的文件分类来创建智能学习（配置页面仅支持智能学习的导出设置项）。详细信息请参考 <a href="#">智能学习任务</a> 。
排除语义	点击排除语义选择要排除的关键字，不作为分类依据。重新运行聚类任务后生效。

## 规则元素

在DLP管理 > 规则元素页面管理数据安全规则元素。

策略规则元素用于创建策略检测内容。

DLP规则元素包含关键字、正则表达式、字典(权重)、模板、文件类型、文件内容、文件大小、附件内容、附件数量、附件大小、文件指纹、数据库指纹、智能学习和ITM模板等。

### 管理正则表达式

在DLP管理 > 规则元素 > 正则表达式页面添加正则表达式。

正则表达式用来检索、替换符合某个模式（规则）的文本。DLP系统预置17条正则表达式规则，勾选显示预置正则即可显示。预置正则可在策略中直接引用，详细信息请参考[附录：预置正则表达式模板](#)。




1. 选择DLP管理 > 策略元素 > 正则表达式，点击添加，新建正则表达式。
2. 输入正则表达式名称和描述，表明该正则表达式的作用。
3. 输入正则表达式，如：`(?<=\\D|^)(1/358/d{9})(?=\\D|$)`。可点击，选择正则表达式测试进行验证。
4. 点击保存，新建正则表达式添加到列表中。

表 78: 页面图标和行间操作按钮功能

图标	解释
	编辑正则表达式，可查看最后修改时间，创建者信息和哪些策略引用该正则表达式。
	删除正则表达式。使用中的正则表达式不可以删除。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a>

### 预置正则表达式模板

预置正则模板	解释
页眉页脚信息	匹配页眉页脚内的所有词汇信息。
账户信息(英文)	匹配5-9位英文账户信息:，如："account: 123456"。
港澳通行证	
香港商业登记证16位(宽)	匹配香港商业登记证号码(16位)，如："01912151-000-07-15-1"， "01912151 000 07 15 1"
邮箱	匹配邮箱格式信息:，如："test@skyguard.com.cn"

IPv4地址(普通)	匹配两种格式的IPv4地址： <ul style="list-style-type: none"> <li>严格符合IP格式的地址,且至少有一个地址段为以数字1开头的三位地址 如："192.168.1.1"，不需要同时匹配相关词汇信息；</li> <li>格式不严格符合IP格式的地址(每段最长两位数字)，且地址附近同时匹配相关词汇信息，如："gateway：00.68.1.1"</li> </ul>
账户信息(中文)	匹配5-9位中文账户信息，如："账户：123456"
页眉页脚机密信息	匹配页眉页脚内的机密相关词汇信息，如："<header footer>机密</header footer>"
中国手机号码(宽)	匹配中国移动、中国联通、中国电信、虚拟运营商电话号码，即：13x，144，145，147，15x(154除外)，17x(174，175，179除外)，18x手机号码，不需要同时匹配相关词汇信息，更多手机号模板请见脚本类型
电子证书	匹配crt格式的电子证书文件。
自杀倾向(英文)	匹配自杀倾向相关英文词汇信息，如："The world would be better off without me"等。
香港商业登记证11位(宽)	匹配香港商业登记证号码(11位)，如："01912151-000"、"01912151 000"
IPv4地址(宽)	匹配有效的IPv4地址，如："192.168.1.1"，不需要同时匹配相关词汇信息
常用密码(宽)	匹配常用密码信息，如："a\$c1X"，不需要同时匹配相关词汇信息。
网络恐吓(英文)	匹配网络恐吓相关英文词汇信息，如："I am really gonna kill you"
Swift代码	匹配世界主要银行的Swift代码，如："BKCHCNBJ"，"ICBKCNBJ"
IPv4地址(窄)	匹配有效的IPv4地址，且地址附近同时匹配相关词汇信息，如："gateway：192.168.1.1"，"IP 192.168.1.1"
一般密码(窄)	匹配一般密码信息，且密码附近同时匹配相关词汇信息，如："password a\$c1X"、"密码 a\$c1X"
车辆识别码	检测车辆识别码：，如："LFV2B21K7A3253274."

#### 管理字典

在DLP管理 > 规则元素 > 字典页面添加字典。

字典是一个容器，用于储存属于同一种语言的词语和表达式。自定义字典可预先定义，也可在创建策略时直接定义。勾选显示预置字典即可显示预置字典。字典可在所有策略中复用。自定义字典可预先定义，也可在创建策略时直接定义。

1. 选择DLP管理 > 策略元素 > 字典，点击添加，新建字典。




2. 输入字典名称和描述，表明该字典的作用。
3. 点击导入以UTF-8编码的txt格式导入字典，每行一条。或直接输入关键字和权重（权重即该关键字在整体检测中的相对重要程度。），点击添加到关键字列表。
4. 点击保存，新建字典添加到列表中。

表 79: 页面图标和行间操作按钮功能

图标	解释
	编辑字典，可查看最后修改时间，创建者信息和哪些策略引用该字典。
	删除字典。使用中的字典不可以删除。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

## 预置字典模板

预置字典名称	解释
淫秽下流信息 (中文)	匹配淫秽下流相关中文词汇信息，如：“去年买个表”、“草泥马”、“滚犊子”等。
淫秽下流信息 (英文)	匹配淫秽下流相关英文词汇信息，如：“whore”、“virgin”、“cybersex”等。
攻击性语言	匹配攻击性语言相关简体中文、繁体中文、英文词汇信息，如：“笨蛋”、“同性恋”、“terrorist”。
成人信息	匹配成人信息相关简体中文、繁体中文、英文、日文词汇信息，如：“成人”、“无码”、“adult”等。
非法药品	匹配违禁药品相关中文、英文词汇信息，如：“三甲利定”、“alprazolam”、“3-Methylfentanyl”等。
暴力/武器	匹配暴力武器相关简体中文、繁体中文、英文词汇信息，如：“炸药”、“子弹”、“explosion”等。
赌博	匹配赌博相关简体中文、繁体中文、英文词汇信息，如：“赛马”、“赌注”、“poker”等。
酒精毒品(中文)	匹配酒精病毒相关中文词汇信息，如：“威士忌”、“吗啡”、“大麻”等。
种族歧视(中文)	匹配种族歧视相关中文词汇信息，如：“阿三”、“老毛子”、“棒子”等。
种族歧视(英文)	匹配种族歧视相关英文词汇信息，如：“spick”、“negro”、“cracker”等。

法轮功(中文)	匹配法轮功相关中文词汇信息，如：“李洪志”、“法轮功”、“法轮大法”等
中国国家领导人	匹配2016年中国国家领导人姓名
政治言论	匹配政治言论相关词汇信息，如：“台独”、“藏独”等
机密信息(中文)	匹配机密相关中文词汇信息，如：“机密”、“保密”、“绝密”等
机密信息(英文)	匹配机密相关英文词汇信息，如：“confidential”、“private”、“classified”等
机密信息(中文繁体)	匹配机密相关繁体中文词汇信息，如：“收購”、“機密”、“機密性”等
理赔记录(中文)	匹配保险理赔相关中文词汇信息，如：“出险人”、“出险日期”、“理赔日期”等
保险种类(中文)	匹配保险险种相关中文词汇信息，如：“强制保险”、“人身保险”、“商业保险”等
赔偿	匹配赔偿相关中文、英文词汇信息，如：“赔偿”、“赔款”、“compensation”等
应急方案(中文)	匹配应急方案相关词汇信息，如：“处置方案”、“安全主管”、“应急预案”等
简历	匹配简历相关中文、英文词汇信息，如：“学历”、“教育程度”、“major”等
合同	匹配合同相关词汇信息，如：“甲方”、“乙方”、“违约”等
工资奖金(中文)	匹配工资奖金相关中文词汇信息，如：“奖金”、“红利”、“工资”等
求职(中文)	匹配工作搜索相关中文词汇信息，如：“职位”、“面试”、“教育程度”等
投资信息(英文)	匹配投资相关英文词汇信息，如：“registered bond”、“stock split”、“discount broker”等
并购条款	匹配并购条款相关的中文、英文词汇信息，如：“common stock”、“回收策略”、“重整计划”等
贷款存款	匹配贷款和存款相关中文、英文词汇信息，如：“存款单”、“借款额度”、“mortgage”等



价格信息	匹配价格相关中文、英文词汇信息如：“零售价”、“批发价”、“original price”等
专利信息	匹配专利相关中文、英文词汇信息，如：“专利”、“发明”、“patent”、“invention”等
一般财务信息	匹配财务相关简体中文、繁体中文、英文词汇信息，如：“资金”、“存款”、“economy”等
财务预算(中文)	匹配财务预算相关中文词汇信息，如：“基本工资”、“材料费”、“人工费”等
财务报表(中文)	匹配财务报表相关中文词汇信息，如：“预付账款”、“应收票据”、“业务支出”等
高管职位名称	匹配高管职位相关中文、英文词汇信息，如：“总裁”、“CEO”、“Vice President”等
产品设计文档(中文)	匹配产品设计文档相关中文词汇信息，如：“功能分解”、“技术调研”、“详细设计”等
战略规划(中文)	匹配战略规划相关词汇信息如：“战略目标”、“竞争对手”、“市场潜力”等
需求文档(中文)	匹配需求文档相关中文词汇信息，如：“功能概述”、“外部接口需求”、“安全性需求”等
测试方案(中文)	匹配测试方案相关中文词汇信息，如：“性能测试”、“回归测试”、“压力测试”等
会议纪要(中文)	匹配会议纪要相关中文词汇信息，如：“会议强调”、“会议决定”、“达成一致”等
技术方案(中文)	匹配技术方案相关中文词汇信息，如：“设计依据”、“选型方案”、“实施计划”等
项目方案(中文)	匹配项目方案相关中文词汇信息，如：“设计方案”、“项目规划”、“工程文件”等
人事任免(中文)	匹配人事任免相关中文词汇信息，如：“人事任免”、“研究决定”、“任命”等
网络拓扑信息	匹配网络拓扑相关中文、英文词汇信息，如：“节点”、“网关”、“NAT”等

网络安全	匹配网络安全相关中文、英文词汇信息，如："肉鸡"、"xscan"、"hacktool"等
数据备份策略(中文)	匹配数据备份相关中文词汇信息，如："备份方式"、"备份计划"、"备份位置"等
健康病症(中文)	匹配身体状况相关中文词汇信息，如："肌腱炎"、"神经炎"、"偏头痛"等。
网络安全	匹配网络安全相关中文、英文词汇信息，如："肉鸡"、"xscan"、"hacktool"等。
项目方案(中文)	匹配项目方案相关中文词汇信息，如："设计方案"、"项目规划"、"工程文件"等。
投资信息(英文)	匹配投资相关英文词汇信息，如："registered bond"、"stock split"、"discount broker"等

### 管理指纹

在DLP管理 > 规则元素 > 字典页面添加指纹任务。

DLP系统指纹识别功能支持结构化指纹和非结构化指纹。


非结构指纹是由爬虫工具扫描共享文件服务器或者文件网站服务器，根据一定算法生成文件指纹库，做精确匹配或相似度匹配来保护数据，阻止分发受保护的信息。如：Sharepoint、Lotus Domino和文件共享方式的非结构化指纹任务。

结构化指纹是连接到数据库，依据检测记录和识别记录形成的结构化指纹，从受保护的数据库中精确检测到敏感字段。DLP支持的数据库类型

有SQLServer、Oracle、Mysql、POSTGRES、DB2、Hiveodbc、Informix、Sybase\_ase、Sybase\_iq、Teradata、CSV、Salefor

表 80: 页面图标和行间操作按钮功能

图标	解释
	编辑指纹信息，可查看最后修改时间，创建者信息和该指纹任务被策略引用状态。
	查看指纹运行详情。详细信息请参考 <a href="#">查看指纹运行详情</a> 。
	运行指纹任务，任务状态为运行中。
	暂停运行中的指纹任务，任务状态显示为已暂停。
	停止运行中的指纹任务，任务状态显示为已停止。
	删除指纹。被策略引用的指纹任务不可以删除。
快速添加策略	快速创建策略，跳转至添加策略页面，新创建的策略规则名称和策略名称以指纹任务名称命名，指纹规则被快速添加到检测匹配内容项。详细信息请参考 <a href="#">添加新策略</a> 。
	仅针对单条任务进行导出操作，导出内容包含指纹任务配置及每次运行指纹库版本信息。

	导入文件指纹和导入数据库指纹。详细信息请参考 <a href="#">添加文件共享指纹</a> 和 <a href="#">添加数据库指纹</a> 。
---	---


### 添加文件共享指纹

添加文件共享指纹库任务保护共享文件。

文件共享指纹是由爬虫工具扫描共享文件或文件网站服务器，根据一定算法生成文件指纹库，并做精确匹配或相似度匹配来保护数据，阻止分发受保护的信息。

1. 选择DLP管理 > 规则元素 > 指纹，点击添加，在下拉列表中选择文件共享，添加文件共享指纹。
2. 输入指纹的名称和描述，表明该指纹的作用。
3. 选择收集器扫描文档，查找敏感性数据。默认收集器为UCSS上的DSA。
4. 选择扫描模式：

- 敏感内容：扫描需要执行数据安全保护的敏感信息。
- 忽略内容：扫描不需要执行数据安全保护的非敏感信息，比如：免责声明、版权声明等。


 注：忽略内容会在安全策略引擎进行指纹内容匹配之前被自动过滤，无需将忽略内容的指纹添加到规则或策略。


5. 选择扫描方法：


- 相似度匹配：检测文档的各个部分，查找已扫描的内容与文件之间的相似特征，只要存在一定相似度即会被策略命中，安全性较高。
- 完全匹配：文件和指纹文件只有在完全匹配的情况下才会被策略命中，检测到任何微小差异都不会再继续扫描文件。

6. 点击文件来源选项卡，选择本地上传检测文件或远程共享检测文件：


- 本地上传压缩文件：将文件压缩为zip格式上传至DLP服务器，进行DLP指纹扫描分析。默认勾选扫描完成后删除zip文件。
- 使用远程文件共享，需配置远程共享服务器：
  - a. 选择网络共享方式扫描文件，支持SMB和NFS。
  - b. 输入共享服务器的IP或主机名。
  - c. 输入共享服务器的用户信息，包括用户名称、密码或域名。也可以匿名登录。
  - d. 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


 提示：如果尝试连接失败，系统将会给出提示信息。

e. 添加扫描内容，点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。

f. 添加排除内容，点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。

7. 点击过滤器选项卡，配置如下参数进行指纹识别，过滤出所需文件：

文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
----------	--

真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p> 注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB )，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。


## 8. 点击计划选项卡，设置扫描计划：

## a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

## b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。

时间选项	描述
	 提示: 如果选定每小时扫描, 时间段为一个月。如果想在上班期间暂停扫描, 可选择周一至周五9:00~18:00暂停扫描。

 注:

- 任务开始时间不能小于系统时间, 否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到, 不会重新运行该扫描任务。

9. 点击导出选项卡, 选择是否开启导出指纹文件功能, 开启后进行如下配置:

- 选择网络共享方式导出文件, 支持SMB和NFS。
- 输入导出指纹文件时可访问共享服务器IP或主机名。
- 输入所导出的指纹文件的存放目录。该文件夹必须真实存在, 且具备可写权限。
- 输入登录共享服务器的用户信息, 包括用户名称、密码或域名(若共享服务器账户属于某一AD域, 须填写域名)。也可以匿名登录。
- 点击测试连接, 系统会尝试使用提供的信息检测与共享服务器的连通性。

10. 点击保存, 新建指纹任务将被添加到任务列表页。


#### 添加SharePoint指纹

添加SharePoint指纹库任务保护SharePoint共享文件。

当用户帐户具有SharePoint站点内容的访问和浏览权限, 并具有调用Web服务和获取访问控制列表(ACL)的权限时, 可使用DLP扫描SharePoint服务器上泄露的机密数据。


- 选择DLP管理 > 规则元素 > 指纹, 点击添加, 在下拉列表中选择SharePoint添加SharePoint指纹。
- 输入指纹的名称和描述, 表明该指纹的作用。
- 选择收集器扫描文档, 查找敏感性数据。默认收集器为UCSS上的DSA。
- 选择扫描模式:

- 敏感内容: 扫描需要执行数据安全保护的敏感信息。
- 忽略内容: 扫描不需要执行数据安全保护的非敏感信息, 比如:免责声明、版权声明等。

 注: 忽略内容会在安全策略引擎进行指纹内容匹配之前被自动过滤, 无需将忽略内容的指纹添加到规则或策略。


5. 选择扫描方法:

- 相似度匹配: 检测文档的各个部分, 查找已扫描的内容与文件之间的相似特征, 只要存在一定相似度即会被策略命中, 安全性较高。
- 完全匹配: 文件和指纹文件只有在完全匹配的情况下才会被策略命中, 检测到任何微小差异都不会再继续扫描文件。

 注: 对于包含许多文件的大型目录结构, 建议首先设置完全匹配扫描, 然后返回并将其更改为相似度匹配扫描。


6. 点击文件来源选项卡, 配置远程服务器获取检测文件:


- 填写站点路径, 即输入SharePoint站点根目录的主机名, 如http://gumby/site\_name。在SharePoint中, 站点路径不同于文件夹路径, 系统仅支持此字段的站点级URL。


 注: 若输入IP地址, 则SharePoint管理员必须将该IP地址添加到备用访问映射表。在SharePoint 2010中, 选择 Central Administration (中央管理) > AlternateAccess Mapping (备用访问映射); 单击 Add InternalURLs (添加内部URL)。SharePoint 指纹识别将连接到站点集合(如http://intranet/sites/HR:8080), 而不会连接到 Web 应用程序。

- 输入共享服务器用户名称、密码或域名。
- 输入所导出的指纹文件的存放目录。该文件夹必须真实存在, 且具备可写权限。
- 输入共享服务器用户名称、密码或域名。

e) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

f) 添加扫描内容，点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。

g) 添加排除内容，点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。

7. 点击过滤器选项卡，配置如下参数进行指纹识别，过滤出所需文件：


过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p> 注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB)，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。

8. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

9. 点击导出选项卡，选择是否开启导出指纹文件功能，开启后进行如下配置：

- 选择网络共享方式导出文件，支持SMB和NFS。
- 输入导出指纹文件时可访问共享服务器IP或主机名。
- 输入所导出的指纹文件的存放目录。该文件夹必须真实存在，且具备可写权限。
- 输入登录共享服务器的用户信息，包括用户名称、密码或域名（若共享服务器账户属于某一AD域，须填写域名）。也可以匿名登录。
- 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


10. 点击保存，新建指纹将被添加指纹任务列表页。

#### 添加Lotus Domino指纹

生成Lotus Domino指纹库保护Lotus Domino数据管理系统的文件。


DLP支持指纹扫描识别存储于IBM Lotus Domino数据管理系统上的文档。一般情况下，Domino环境部署一个或多个协同工作的服务器，并将数据存储于Notes Storage Format (NSF) 文件中。任何给定的Domino服务器上通常有许多NSF，NSF中的每个条目可能有一个标题、一个或多个正文字段以及附件。

- 选择DLP管理 > 规则元素 > 指纹，点击添加，在下拉列表中选择**Lotus Domino**，添加Lotus Domino指纹。
- 输入指纹的名称和描述，表明该指纹的作用。
- 选择收集器扫描文档，查找敏感性数据。默认收集器为UCSS上的DSA。
- 选择扫描模式：
  - 敏感内容：扫描需要执行数据安全保护的敏感信息。
  - 忽略内容：扫描不需要执行数据安全保护的非敏感信息，如：免责声明、版权声明等。

 注：忽略内容会在安全策略引擎进行指纹内容匹配之前被自动过滤，无需将忽略内容的指纹添加到规则或策略。


#### 5. 选择扫描方法：



- 相似度匹配：检测文档的各个部分，查找已扫描的内容与文件之间的相似特征，只要存在一定相似度即会被策略命中，安全性较高。
- 完全匹配：文件和指纹文件只有在完全匹配的情况下才会被策略命中，检测到任何微小差异都不会再继续扫描文件。

 注：对于包含许多文件的大型目录结构，建议首先设置完全匹配扫描，然后返回并将其更改为相似度匹配扫描。


#### 6. 点击文件来源选项卡，配置远程服务器获取检测文件：

- 输入要扫描的IBM Lotus Domino服务器的IP地址。
- 输入要扫描的IBM Lotus Domino服务器的主机名称。
- 点击选择文件，上传IBM Lotus Domino服务器的访问用户ID和密码。
- 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- 输入包含文档正文文本的字段。如：Body, Content, Main。
- 添加扫描内容，点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。选择是否扫描文档正文(需输入存有文档正文文本的一个或多个字段的名称，默认情况下选择“Body”)和文档附件。
- 添加排除内容，点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。

#### 7. 点击过滤器选项卡，配置如下参数进行指纹识别，过滤出所需文件：

过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB)，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。
附件大小过滤	选择附件的大小进行过滤(范围0~999 B/KB/MB)，大于100MB的文件直接放行。
附件类型过滤	<p>选择附件类型过滤。</p> <p>过滤：预定义文件类别中选择要进行过滤识别的附件文件类型。如：*设计；</p>




排除：从预定义文件类别中选择选择不进行过滤识别的附件文件类型。

8. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

9. 点击导出选项卡，选择是否开启导出指纹文件功能，开启后进行如下配置：

- 选择网络共享方式导出文件，支持SMB和NFS。
- 输入导出指纹文件时可访问共享服务器IP或主机名。
- 输入所导出的指纹文件的存放目录。该文件夹必须真实存在，且具备可写权限。
- 输入登录共享服务器的用户信息，包括用户名称、密码或域名（若共享服务器账户属于某一AD域，须填写域名）。也可以匿名登录。
- 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


10. 点击保存，新建指纹任务将被添加指纹任务列表页。


## 添加CSV指纹

添加CSV数据库指纹任务保护CSV数据库的文件。

CSV指纹数据来源使用文件共享方式选择CSV过滤文件。CSV数据库指纹过滤不支持SQL语句展示和查询。

1. 选择DLP管理 > 规则元素 > 指纹，点击添加，在下拉列表中选择CSV，添加CSV指纹。
2. 输入指纹的名称和描述，表明该指纹的作用。
3. 选择收集器扫描文档，查找敏感性数据。默认收集器为UCSS上的DSA。
4. 点击数据来源选项卡，可通过支持本地上传或远程文件共享获取CSV文件，配置如下：
  - a) 选择CSV编码格式，支持GBK、BIG5、UTF8和UTF16。
  - b) 选择本地上传检测文件或远程共享检测文件：
    - 本地上传压缩文件：将文件压缩为zip格式上传至DLP服务器，进行DLP指纹扫描分析。默认勾选扫描完成后删除zip文件。
 

 注：如果选择扫描完成后删除CSV文件，扫描完成后再次编辑/保存该任务时，可能会提示找不到CSV源文件，需要再次上传；如果该指纹被策略使用，请先删除策略和指纹的引用关系，才能再次上传。
    - 使用远程文件共享，需配置远程共享服务器：
      1. 选择网络共享方式扫描文件，支持SMB和NFS。
      2. 输入共享服务器的IP或主机名。
      3. 输入要扫描的文件和文件夹所在的根文件夹或根目录。
      4. 输入共享服务器的用户信息，包括用户名称、密码或域名。也可以匿名登录。
      5. 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。
 

 提示：如果尝试连接失败，系统将会给出提示信息。
  6. 在数据来源中选择CSV文件后，在此显示CSV文件名称。如：FileType.csv。


5. 点击过滤器选项卡，配置如下参数进行指纹识别，过滤出所需文件：

CSV文件名称	在数据来源中选择CSV文件后，在此显示CSV文件名称。如：FileType.csv。
通过列表选择需要指纹的名称	选择需要扫描的CSV数据库表列项。点击列名显示其在CSV文件中所包含的前10个数据。
单元格内容长度过滤	设置单元格扫描的字节数，进行数据库过滤。

6. 点击计划选项卡，设置扫描计划：


- a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

 注：选择对比扫描后，需指定扫描字段用于记录比较。收集器会核对指定的字段是否已更改。如果已更改，它会在此字段和所有新字段之前重新识别上一个字段的指纹；如果未更改，收集器将忽略该表。如果此字段不存在，则系统会执行全面指纹识别扫描。

- b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	设置执行扫描任务运行的频率。

时间选项	描述
	<ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

7. 点击导出选项卡，选择是否开启导出指纹文件功能，开启后进行如下配置：

- 选择网络共享方式导出文件，支持SMB和NFS。
- 输入导出指纹文件时可访问共享服务器IP或主机名。
- 输入所导出的指纹文件的存放目录。该文件夹必须真实存在，且具备可写权限。
- 输入登录共享服务器的用户信息，包括用户名称、密码或域名（若共享服务器账户属于某一AD域，须填写域名）。也可以匿名登录。
- 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


8. 点击保存，新建指纹任务将被添加指纹任务列表页。

#### 添加数据库指纹

添加数据库指纹任务保护数据库的文件。


DLP可快速连接到数据库、检索记录以及识别记录的数据库指纹，并使用指纹提取技术从受保护的数据库中检测精确字段，如名字、姓氏和社会保障号码等用户私有信息，若这些信息泄露于外部收件人或外发的内容中，DLP可通过定义数据库指纹来阻止此类信息的分发。DLP目前支持扫描QLServer、Oracle、MySQL、POSTGRES、DB2和其它类型数据库的敏感信息。

- 选择DLP管理 > 规则元素 > 指纹，点击添加，在下拉列表中选择数据库，添加数据库指纹。
- 输入指纹的名称和描述，表明该指纹的作用。
- 选择收集器扫描文档，查找敏感性数据。默认收集器为UCSS上的DSA。

 注：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

4. 点击数据来源选项卡，配置数据库获取检测文件：

- 选择要识别的数据库类型，以配置连接不同数据库的信息。并支持启用安全连接数据库。

 提示：目前支持SQLSERVER、MYSQL、ORACLE、POSTGRESQL、DB2及其它(Hiveodbc、Informix、Sybase\_ase、Sybase\_iq、Teradata)多种数据库类型。

- 输入连接数据库的IP地址。


## c) 配置数据库的端口号。

数据库类型	端口号
SQLSERVER	1433
MYSQL	3306
ORACLE	1521
POSTGRESQL	5432
DB2	5000

## d) 输入登录数据库的用户名称、密码或域名（如果此数据库属于某一AD域，域名为必填项）。

- 数据库类型为ORACLE时需选择登录数据库用户所属角色（DEFAULT/SYSDBA/SYSOPER）。
- 数据库类型为ORACLE/POSTGRESQL/DB2时，需要输入数据库对应实例名称。

## e) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


 提示：如果尝试连接失败，系统将会给出提示信息。

## 5. 点击过滤器选项卡，配置如下参数进行指纹识别，过滤出所需文件：

## a) 选择数据库名称。在数据来源选项卡配置数据库并测试连通性后，出现于下拉菜单中。

## b) 配置选择数据库记录数据的方式：

使用列表方式选择相关记录	选择需要扫描的数据库表及其表列，并显示使用的SQL语句。
使用SQL语句选择相关记录	如果需要过滤数据库表列中的某些记录，可以手动添加SQL语句。


 注：不支持同时使用列表方式选择相关记录与使用SQL语句相关记录设置数据库指纹过滤器。

## c) 选择是否设置单元格内容长度进行数据库指纹过滤。

## 6. 点击计划选项卡，设置扫描计划：


## a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

 注：选择对比扫描后，需指定扫描字段用于记录比较。收集器会核对指定的字段是否已更改。如果已更改，它会在此字段和所有新字段之前重新识别上一个字段的指纹；如果未更改，收集器将忽略该表。如果此字段不存在，则系统会执行全面指纹识别扫描。

## b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	设置执行扫描任务运行的频率。 <ul style="list-style-type: none"> <li>• 选择执行一次，请指定运行一次扫描任务的时间；</li> <li>• 选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳</li> </ul>

时间选项	描述
	<p>扫描时间是在夜间业务高峰时间之后运行指纹扫描；</p> <ul style="list-style-type: none"> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

7. 点击导出选项卡，选择是否开启导出指纹文件功能，开启后进行如下配置：

- 选择网络共享方式导出文件，支持SMB和NFS。
- 输入导出指纹文件时可访问共享服务器IP或主机名。
- 输入所导出的指纹文件的存放目录。该文件夹必须真实存在，且具备可写权限。
- 输入登录共享服务器的用户信息，包括用户名称、密码或域名（若共享服务器账户属于某一AD域，须填写域名）。也可以匿名登录。
- 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


8. 点击保存，新建指纹任务将被添加指纹任务列表页。

#### 添加Salesforce指纹

添加Salesforce指纹任务保护Salesforce服务器上的文件。

DLP支持指纹扫描识别存储于Salesforce服务器上的文件，防止机密数据泄漏。此功能需要用户帐户具有Salesforce站点的访问和浏览权限。


- 选择DLP管理 > 规则元素 > 指纹，点击添加，在下拉列表中选择Salesforce。
- 输入指纹的名称和描述，表明该指纹的作用。
- 选择收集器扫描文档，查找敏感性数据。默认收集器为UCSS上的DSA。
- 点击文件来源选项卡，配置Salesforce服务器：
  - 输入Salesforce登录网址，如：https://login.salesforce.com/services/oauth2/token。
  - 输入可以访问Salesforce系统的用户名称。
  - 输入登录密码。
  - 输入访问Salesforce API所需的授权令牌Token。
  - 输入访问Salesforce API所需的Consumer Key，也叫Client Secret。
  - 输入访问Salesforce API所需的Consumer Secret，服务端的安全保障凭据。
  - 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

5. 点击过滤器选项卡，配置如下参数进行指纹识别，过滤出所需文件：

- 配置选择数据库记录数据的方式：

使用列表方式选择相关记录	选择需要扫描的数据库表及其表列，并显示使用的SQL语句。
使用SQL语句选择相关记录	如果需要过滤数据库表列中的某些记录，可以手动添加SQL语句。


 注：不支持同时使用列表方式选择相关记录与使用SQL语句相关记录设置数据库指纹过滤器。

b) 选择是否设置单元格内容长度进行数据库指纹过滤。


6. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

 注：选择对比扫描后，需指定扫描字段用于记录比较。收集器会核对指定的字段是否已更改。如果已更改，它会在此字段和所有新字段之前重新识别上一个字段的指纹；如果未更改，收集器将忽略该表。如果此字段不存在，则系统会执行全面指纹识别扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：


- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

7. 点击导出选项卡，选择是否开启导出指纹文件功能，开启后进行如下配置：

- a. 选择网络共享方式导出文件，支持SMB和NFS。
  - b. 输入导出指纹文件时可访问共享服务器IP或主机名。
  - c. 输入所导出的指纹文件的存放目录。该文件夹必须真实存在，且具备可写权限。
  - d. 输入登录共享服务器的用户信息，包括用户名称、密码或域名（若共享服务器账户属于某一AD域，须填写域名）。也可以匿名登录。
  - e. 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。
8. 点击保存，新建指纹任务将被添加指纹任务列表页。

查看指纹运行详情

查看详细的指纹任务运行信息。

点击指纹任务详情图标，进入指纹任务详情查看页面，查看属性信息如下：

- 基本信息

类型	显示该指纹任务类型。
任务状态	显示该指纹任务状态，包含未开始/就绪、运行中、已完成、失败、完成/部分错误、已停止、已暂停、等待中。

- 扫描设置

上次运行时间	显示该指纹任务上次运行时间。
下次运行时间	如果设置了定时扫描，显示该指纹任务下次运行时间。如果未设置，显示N/A。
上次计划时间	显示该指纹任务计划时间。如果未设置，显示N/A。
定时扫描	显示该指纹任务的定时扫描时间。如果未设置，显示禁用。
扫描频率	显示定时扫描设置中的扫描频率，如:每天/每周/每小时。如果未设置，显示N/A。

- 扫描结果

- 结构化指纹

扫描记录数量	显示扫描数据库表的记录数量。
当前指纹库大小	显示指纹任务生成的指纹库信息大小。

- 非结构化指纹

扫描文件数量	显示扫描的文件总数。
扫描文件大小	显示扫描的文件总体大小。
当前指纹库大小	显示该指纹任务生成的指纹库信息大小。

- 当前扫描状态

- 结构化指纹

扫描进度	显示实时扫描进度（0%-100%）。
扫描完成的记录	显示扫描完成的记录数量。
预计总记录数量	显示扫描前预估数据库表的行的总数量。

- 非结构化指纹

扫描的文件数量	显示实时扫描的文件数量。
扫描的文件大小	显示实时扫描的文件大小。
扫描进度	显示实时扫描进度 ( 0%-100% )。
扫描完成的文件数量	显示实时扫描文件完成的数量。
扫描失败的文件数量	显示实时扫描文件失败的数量。
过滤掉的文件数量	显示过滤扫描文件的数量。
预计总文件数量	显示扫描前预估文件总数量。
预计总文件大小	显示扫描前预估文件总大小。


• 指纹扫描详细列表

搜索查询	显示按照目录名、文件名搜索查看指定文件的扫描详情。
目录名	显示扫描的文件所属文件目录。
文件名	显示扫描的文件名称。
文件修改时间	显示扫描的文件最后修改时间。
文件大小	显示扫描的文件大小。
任务状态	显示文件扫描结果，如：过滤、已扫描、文件太大、提取文件失败。
指纹扫描时间	显示扫描文件的完成时间。
指纹扫描详情列表翻页/跳转	显示在指纹扫描详情列表通过翻页、跳转查询扫描详情列表。

### 管理智能学习

在DLP管理 > 规则元素 > 智能学习页面添加智能学习任务。

智能学习是指DLP正向学习一批内容详细的文件，提炼相似敏感信息并被策略引用，如果有类似文件外泄，将会匹配智能学习策略。同时也可将易于与这些文件混淆的内容交给DLP做反向学习，提高智能学习的精准度。

 注：正向学习和反向学习样本数建议均不少于50个。

1. 选择DLP管理 > 规则元素 > 智能学习，点击添加，新建智能学习任务。
2. 输入智能学习任务的名称和描述，表明该任务的作用。
3. 选择该智能学习任务的类型（类型包含默认、Java源代码、C/C++源代码、Python源代码和Per源代码）。
4. 选择进行智能学习扫描的服务器名称，用于读取提供的样本文件。
5. 点击样本来源选项卡，可通过支持本地上传或远程文件共享获取CSV文件获取样本文件的来源，配置如下：

- 本地上传压缩文件：


正向学习	点击选择，上传本地压缩后的需要学习的正向文本。
反向学习	点击选择，上传本地压缩后的需要学习的负向文本。



扫描完成后删除zip文件


选择是否将学习扫描完成的压缩文件从DLP系统里删除。

- 使用远程文件共享：
  - a. 选择文件的共享类型，支持Samba和NFS。
  - b. 输入可以访问的共享服务器IP或主机名。
  - c. 输入要扫描的文件和文件夹的根文件夹或根目录。如\\Server\Public\shared。
  - d. 输入共享服务器用户名称、密码或域名（如果此数据库属于某一AD域，域名为必填项）。也可以匿名登录。
  - e. 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- f. 导入样本目录，分别点击选择目录，选择远程压缩后的需要学习的正向文本和反向文本。

6. 点击计划选项卡，选择是否开启扫描计划，开启后设置开始时间和暂停时段。


开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>• 选择执行一次，请指定运行一次扫描任务的时间；</li> <li>• 选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>• 选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>• 选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次指纹任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。


7. 点击导出选项卡，选择是否开启导出指纹文件功能，开启后进行如下配置：

- a) 选择网络共享方式导出文件，支持SMB和NFS。
- b) 输入导出指纹文件时可访问共享服务器IP或主机名。
- c) 输入所导出的指纹文件的存放目录。该文件夹必须真实存在，且具备可写权限。
- d) 输入登录共享服务器的用户信息，包括用户名称、密码或域名（若共享服务器账户属于某一AD域，须填写域名）。也可以匿名登录。
- e) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。


8. 点击保存，新建的智能学习任务将被添加任务列表页。

表 81: 页面图标和行间操作按钮功能

图标	解释
	编辑智能学习任务信息，可查看最后修改时间，创建者信息和引用了该智能学习任务的策略信息。
	查看智能学习任务详情。详细信息请参考查看智能学习任务详情。
	运行智能学习任务，任务状态为运行中。
	暂停运行中的智能学习任务，任务状态显示为已暂停。
	停止运行中的智能学习任务，任务状态显示为已停止。
	删除文件类型组。被策略引用的文件类型不能删除。
快速添加策略	快速创建策略，跳转至添加新策略页面，创建的新策略规则名称和策略名称以文件组类型名称命名，文件组类型被快速添加到检测匹配内容项。详细信息请参考 <a href="#">添加新策略</a> 。
	导出单条任务，导出内容包含智能学习任务配置、智能学习任务每次运行的智能学习库信息。
	导入智能学习任务。详细信息请参考添加智能学习。

查看智能学习任务详情

查看详细的智能学习任务运行信息。

点击智能学习详情图标 ，进入智能学习任务详情查看页面，查看属性信息如下：

- 基本信息

任务状态	显示该智能学习任务状态。
估计精准度	显示智能学习准确率。
上次运行时间	显示该智能学习任务上次运行时间。
下次运行时间	如果设置了定时扫描，显示该智能学习任务下次运行时间。如果未设置，显示N/A。

- 正向学习

路径	显示扫描文件的路径。
文件个数	显示扫描文件的数量。
文件总大小	显示扫描文件的总大小。

- 反向学习

路径	显示扫描文件的路径。
文件个数	显示扫描文件的数量。
文件总大小	显示扫描文件的总大小。

- 正向/反向学习扫描详情列表

目录名	显示扫描文件所属文件目录。
文件名	显示扫描文件名称。
文件修改时间	显示扫描文件最后修改时间。
文件大小	显示扫描文件大小。
智能学习状态	显示扫描文件扫描结果。示例:已扫描、文件太大、提取文件失败。
智能学习时间	显示扫描文件智能学习完成时间。

### 文件类型组

文件类型组将同一类型文件分组进行统一识别。

DLP系统预置500多种文件类型和28种文件类型组，文件类型组将同一类型文件分组进行统一识别，可直接在策略中引用，如Office系列，压缩文件系列、加密系列、媒体文件、制图软件等。DLP系统可识别外发文件和附件，即使该文件被压缩或者更改扩展名也可提取识别信息。详细信息请参考[附录：预置文件类型组](#)。




1. 选择DLP管理 > 规则元素 > 文件类型组，点击添加，新建文件类型组。
2. 输入自定义文件类型组名称和描述，表明文件类型组的用处。
3. 点击选择需要自定义的文件类型。
4. 点击保存，新建文件类型组被添加到列表。

表 82: 页面图标和行间操作按钮功能

图标	解释
	编辑文件类型组。
	删除文件类型组。被策略引用的文件类型不能删除。
快速添加策略	快速创建策略，跳转至添加新策略页面，创建的新策略规则名称和策略名称以文件组类型名称命名，文件组类型被快速添加到检测匹配内容项。详细信息请参考 <a href="#">添加新策略</a> 。

### 预置文件类型组

预置文件类型组	解释
办公文件	检测所有常用办公文件类型，常用办公的文件类型：Word、Excel、PPT、XML、HTML、HTM、PDF、iWork Keynote\Numbers\Pages。
SAM文件	检测所有SAM类型文件。
私钥文件	检测所有私钥文件类型，包含PEM私钥和PKCS12私钥。
证书文件	检测所有证书文件类型，包含PEM证书。
Microsoft Works文件	检测所有Microsoft Works类型的文件。
HTML文件	检测HTML文件，包括HTML，XHTML，MIME HTML，Unicode HTML，HTML Fragment。
未知类型文件	检测未知文件类型。
Microsoft数据库文件	检测Microsoft数据库类型的文件，包括Microsoft Project，Microsoft Access。

图像文件	检测图像类型的文件，包括CorelDRAW，DCX Fax System，Encapsulated PostScript，Enhanced Metafile，GIF，JPEG，AMIDraw，Lotus Pic，MacPaint，MSO，PC PaintBrush，PNG，SGI RGB Image，Sun Raster Image，TIFF，Truevision Targa，ANI，Bitmap，ICO，WMF，Word Perfect Graphics。
邮件文件	检测邮件类型的文件，包括Domino XML，Legato Extender，Lotus Notes DB，Microsoft Outlook，Microsoft Outlook Express，Microsoft Outlook Personal Folder，Text Mail (MIME)，Transport Neutral Encapsulation，Microsoft Outlook iCalendar Data File (ICS)，Microsoft Outlook vCalendar Data File (VCS)。
电子表格文件	检测电子表格类型的文件，包括Microsoft Excel，Apple iWork Numbers，Applix Spreadsheets，Comma Separated Values (CSV)，Data Interchange Format，Lotus 1-2-3，Microsoft Works Spreadsheet，Star Office Spreadsheet。
可执行文件	检测可执行文件，包括EXE，Microsoft Com executables。
文字处理文件	检测文字处理类型的文件，包括Microsoft Word，Adobe FrameMaker，Apple Pages，Applix Words，WordPerfect，Display Write，Folio Flat File，Founder E-Paper，Oasys，Haansoft Hangul，DCA/RFT，Just Systems Ichitaro，Lotus AML，Lotus Word，Microsoft Works，WordPad，XPS，XyWrite，Yahoo Messenger，Microsoft Outlook vCard Contact Files (VCF)。
文本标记文件	检测文本标记类型的文件，包括ASCII，HTML，Microsoft Excel Windows XML，Microsoft Word Windows XML，Microsoft Visio XML，MIME HTML，Rich Text Format (RTF)，Unicode Text，XHTML，XML。
计算机辅助设计文件	检测计算机辅助设计类型的文件，包括AutoCAD DXF graphics，AutoCAD Drawing，CATIA formats，Microsoft Visio，MicroStation。
Microsoft Access文件	检测所有版本的Microsoft Access类型的文件。
Microsoft Visio文件	检测所有版本的Microsoft Visio类型的文件。
Microsoft Project文件	检测所有版本的Microsoft Project类型的文件。
Microsoft Word文件	检测所有版本的Microsoft Word类型的文件。
Microsoft Excel文件	检测所有版本的Microsoft Excel类型的文件。
Microsoft PowerPoint文件	检测所有版本的Microsoft PowerPoint类型的文件。
多媒体文件	检测所有多媒体类型的文件，包括Advanced Streaming Format (ASF)，Audio Interchange File Format (AIFF)，Microsoft Wave Sound (WAV)，MIDI，MP3，Mpeg-1 Video，Mpeg-2 Audio，NeXT/Sun Audio，Quick Time Movie，Windows Video (AVI)，MPEG-4。
分片和损坏的压缩文件	检测分片和损坏的压缩类型的文件，包括PKZIP，GZ，TAR，RAR，7Z，BZIP2，XZ，未知格式。
所有压缩文件	检测所有压缩类型的文件，包括一般压缩文件、压缩加密文件、分片和损坏的压缩文件。
一般压缩文件	检测压缩类型的文件，包括CF_RAR5，Microsoft Cabinet format，7-Zip，RAR Format，UNIX Tape ARchiver。
压缩加密文件	检测压缩加密类型的文件，包括Nero Encrypted File，Encrypted files of unknown format，ZIP encrypted format，RAR Encrypted Format，Encrypted 7-Zip File。


Microsoft office加密文件	检测Microsoft office系列加密类型的文件，包括Encrypted Excel 97-2003，Encrypted Word 97-2003，Microsoft Office 2007-2010 Encrypted，Encrypted Power-Point 97-2003，Encrypted Access 97-2003。
所有加密文件	检测加密类型的文件，包括PGP Encrypted files，Microsoft Office 2007-2010，ZIP。

### 管理文件类型

在DLP管理 > 规则元素 > 文件类型组页面添加文件类型。

DLP系统预置500多种文件类型，同一类型文件被分组为同一文件类型组。


1. 选择DLP管理 > 规则元素 > 文件类型组，点击所有文件类型，进入文件类型管理页面。

 提示：勾选显示预置文件类型可显示所有预置文件类型。

2. 点击添加，新建文件类型。

3. 输入自定义文件类型名称和描述，表明文件类型的用处。

4. 输入自定义文件类型签名内容。

 提示：使用文件类型分析工具Fileformat生成的文件签名值，请到Skyguard官网下载或联系Skyguard技术支持获取签名。

5. 点击保存，新建文件类型被添加到列表。

表 83: 页面图标和行间操作按钮功能

图标	解释
	编辑文件类型。
	删除文件类型。被策略引用的文文件类型不能删除。
快速添加策略	快速创建策略，跳转至添加新策略页面，创建的新策略规则名称和策略名称以文件组类型名称命名，文件组类型被快速添加到检测匹配内容项。详细信息请参考 <a href="#">添加新策略</a> 。

### 预置数据模板

配置系统预置的字典、正则表达式、脚本等数据模板。

数据防泄漏DLP支持多种预置类型数据模板，可在DLP策略中直接引用。


点击模板名称可显示模板的详细描述和已使用该模板的策略信息。

在DLP管理 > 规则元素 > 预置数据模板页面查看系统预制的的数据模板。


数据模板包含以下类型：

- 字典 - 参考[字典检测条件](#)获取更多信息。
- 脚本 - 参考[脚本检测条件](#)获取更多信息。
- 正则表达式 - 参考[正则表达式检测条件](#)获取更多信息。
- ITM模板 - 参考[ITM模板检测条件](#)获取更多信息。

勾选预置数据模板，点击快速添加策略，跳转至添加策略页面。。

 提示：创建的新策略规则名称和策略名称以数据模板名称命名，详细信息请参考[添加新策略](#)。

### 页面图标和行间操作按钮功能

图标	解释
	从本地导入数据模板。

## 标签管理

介绍DLP标签管理的相关信息。

数据防泄漏DLP标签功能支持对组织内部的非结构化数据进行标签分类，并可通过已分类的标签对标记的文件数据进行识别检测防护。

标签分类是通过手动或者自动的方式对文件进行标记分类。

当标签防护是被标记的文件在另存、复制、修改扩展名、下载、传输（文件共享、邮件、web）后分类标签不会丢失，创建的标签分类被策略引用进行实时识别检测拦截。

### 标签

介绍创建和管理标签等相关信息。

标签管理页面提供了标签的创建、撤销、指纹标签的查看、标签权限控制等功能，用于创建/编辑管理手动指纹标签。

在DLP管理 > 标签管理 > 标签页面创建/编辑管理标签。

标签的类型包括手动标签分类和自动标签分类。

### 手动分类标签

手动分类标签是至通过终端将标签通过“元数据”的方式插入文档。一旦被标记，手动标签属性将永久跟随文档。手动分类标记可以与文档内容无关，数据防泄漏DLP检测时通过插入的标签ID判断是否触发策略。

手动标签分类又分为：

- 分类标签-单纯需要手动添加的标签分类
- 指纹标签-手动添加并可执行内容指纹探测的标签分类

在安装了数据防泄漏DLP的重大您设备上，有权限的企业终端用户，进入数据保护 > 手动标签编辑器菜单，可查看该文件的标签设置，也可在此菜单下给该文件标记其它标签，但是无权限更改其他人已标记的标签。

终端用户在标签标记文档时，该原始文件会被上传至管理平台，以确保安全管理员可进行撤销标签及查看原始标签标记的文档等统筹安全管理操作。

### 自动分类标签

自动分类标签则分为：

- 基于内容条件探测标准的标签分类
- 基于保密等级条件探测标准的标签分类

### 绑定指纹标签

管理人员创建分类标签时，可选择是否关联绑定指纹标签。

 注：

一个分类标签只能绑定一个指纹标签。

分类标签与绑定指纹标签用户使用权限配置需保持一致。

如选择关联绑定，则终端用户手动打分类标签时，自动将该分类绑定的指纹标签也打在该文档上。

### 标记文档

介绍如何查看标签标记的文档等相关信息。

标记文档页面提供了统一的报告视图页面，允许管理员快速便捷地查看标签标注的文档的流转情况。

页面默认显示最近24小时内各注册终端中所标记的文档。

### 标签设置

介绍管理标签设置的相关信息。

该功能模块用于定义标签分类、维护手动标签分类权限、设置手动分类常规设置项。定义的手动标签分类在终端可被用于文件手动分类，而定义自动标签分类被终端应用程序或者进行数据发现扫描时应用。

在DLP管理 > 标签管理 > 标签设置页面管理标签的相关设置。

## 数据发现

在DLP管理 > 数据发现页面管理数据发现任务。

DLP数据发现通过选定的收集器扫描扫描网络服务器、终端、Exchange Server、PST、数据库等，发现敏感数据后，根据策略执行数据保护或隔离。

### 数据发现任务

本节介绍数据发现任务

DLP数据发现通过创建数据发现策略，调用系统收集器扫描网络服务器、终端、Exchange Server、PST、数据库等，发现敏感数据后，根据策略执行数据保护或隔离。

DLP数据发现包括了：






- 网络任务 - 网络任务可以扫描分析存储在网络共享、Sharepoint、Domino、数据库等位置的数据，并对命中策略的内容记录为数据发现事件。
- 终端任务 - 终端任务扫描分析存储在终端所在主机的数据，并对命中策略的内容记录为数据发现事件。

### 管理网络任务

在DLP管理 > 数据发现 > 网络任务页面管理网络任务。

网络任务可以扫描分析存储在网络共享、Sharepoint、Domino、数据库等位置的数据，并对命中策略的内容记录为数据发现事件。DLP支持的网络任务类型：文件共享、Sharepoint、Lotus Domino、数据库、Exchange、Outlook PST、Exchange Online、Salesforce和邮件反查。


页面图标和行间操作按钮功能如下：




图标	解释
	编辑任务信息，可查看最后修改时间，创建者信息和该任务被策略引用状态。
	运行网络任务，任务状态为运行中。
	暂停运行中的网络任务，任务状态显示为已暂停。
	停止运行中的网络任务，任务状态显示为已停止。
	删除网络任务。运行中的网络任务不可以删除。
历史记录	查看创建网络任务的历史纪录。

### 添加文件共享扫描任务

介绍文件共享扫描任务扫描任务的添加步骤。

1. 选择DLP管理 > 数据发现 > 网络任务，点击添加，在下拉菜单中选择文件共享，添加文件共享扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。
 

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。
4. 点击文件来源选项卡，配置远程服务器获取检测文件：
  - a) 选择网络共享方式扫描文件，支持SMB和NFS。
  - b) 输入共享服务器的IP或主机名。
  - c) 输入要扫描的文件和文件夹所在的根文件夹或根目录。
  - d) 输入共享服务器用户名称、密码或域名。
  - e) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。
 

 提示：如果尝试连接失败，系统将会给出提示信息。
  - f) 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。
  - g) 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。
5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。
6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p> 注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	<p>选择文件大小进行过滤(范围0~999 B/KB/MB )，大于100 MB的文件直接放行。</p>




文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。
--------	----------------------------


7. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>


 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。


8. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。

9. 点击动作选项卡，选择是否启用保护原文、隔离原文或执行补充脚本中的保护功能。

选项	介绍
保护原文	将发现的敏感文件备份到配置的SMB/NFS服务器。
隔离原文	将敏感文件备份以后，删除原敏感文件。
补充脚本	上传系统可执行自定义的补充脚本，执行脚本所配置的动作。

 注：保护原文和隔离原文支持配置远程服务器获取检测文件：

- a. 选择网络共享方式扫描文件，支持SMB和NFS。
- b. 输入共享服务器的IP或主机名。
- c. 输入共享服务器的用户信息，包括用户名称、密码或域名。也可以匿名登录。
- d. 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


 提示：如果尝试连接失败，系统将会给出提示信息。

10. 点击保存，新建的网络任务将被添加列表页。

#### 添加SharePoint扫描任务

介绍SharePoint扫描任务扫描任务的添加步骤。

1. 选择DLP管理 > 数据发现 > 网络任务，点击添加，在下拉列表中选择SharePoint，添加SharePoint扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。


 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。



4. 点击文件来源选项卡，登录共享服务器获取检测文件：
  - a) 输入SharePoint站点根目录的主机名，如http://gumby/site\_name。


 注：


- 在SharePoint中，站点路径不同于文件夹路径，DLP系统仅支持此字段的站点级URL。
- 若输入IP地址，则SharePoint管理员必须将该IP地址添加到备用访问映射表。
- 在SharePoint 2010中，管理员应选择 Central Administration (中央管理) > AlternateAccess Mapping (备用访问映射)，然后单击 Add InternalURLs (添加内部URL)；SharePoint 指纹识别将连接到站点集合 (如http://intranet/sites/HR:8080)，而不会连接到 Web 应用程序。

- b) 输入登录共享服务器的用户名称、密码或域名。
- c) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- d) 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。
- e) 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。
5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。
6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。 如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。 如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。 如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p>


	<p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p> 注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB )，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。
附件大小过滤	选择附件的大小进行过滤(范围0~999 B/KB/MB )，大于100MB的文件直接放行。
附件类型过滤	<p>选择附件类型过滤。</p> <p>过滤：预定义文件类别中选择要进行过滤识别的附件文件类型。如：*设计；</p> <p>排除：从预定义文件类别中选择选择不进行过滤识别的附件文件类型。</p>

7. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>



注：


- 任务开始时间不能小于系统时间，否则系统将给出错误提示。

- 如果上次任务扫描未完成而下一计划的计划时间已到，不会重新运行该扫描任务。
8. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。
  9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。
  10. 点击保存，新建的网络任务将被添加列表页。


### 添加Lotus Domino扫描任务



介绍Lotus Domino扫描任务的添加步骤。


1. 选择DLP管理 > 数据发现 > 网络任务，点添加，在下拉菜单中选择**Lotus Domino**，添加Lotus Domino扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。


 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

4. 点击文件来源选项卡，登录Domino服务器获取检测文件：
  - a) 输入接受扫描的IBM Lotus Domino服务器的IP地址。
  - b) 输入接受扫描的IBM Lotus Domino服务器的主机名称。
  - c) 点击选择，上传要扫描的IBM Lotus Domino服务器的访问用户ID和密码。
  - d) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

  - e) 输入标题字段，即包含文档正文文本的字段。例如:Body, Content, Main。
  - f) 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。
  - g) 选择是否扫描文档正文（需输入存有文档正文文本的一个或多个字段的名称。默认情况下选择“Body”（正文））和文档附件。
  - h) 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。
5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。
6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p>

	<p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p> 注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB )，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。
附件大小过滤	选择附件的大小进行过滤(范围0~999 B/KB/MB )，大于100MB的文件直接放行。
附件类型过滤	<p>选择附件类型过滤。</p> <p>过滤：预定义文件类别中选择要进行过滤识别的附件文件类型。如：*设计；</p> <p>排除：从预定义文件类别中选择选择不进行过滤识别的附件文件类型。</p>

7. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。

时间选项	描述
	 提示: 如果选定每小时扫描, 时间段为一个月。如果想在上班期间暂停扫描, 可选择周一至周五9:00~18:00暂停扫描。

 注:


- 任务开始时间不能小于系统时间, 否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到, 不会重新运行该扫描任务。

8. 点击高级选项卡, 设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡, 选择是否开启动作, 执行补充脚本中的保护功能。
10. 点击保存, 新建的网络任务将被添加列表页。

#### 添加数据库扫描任务


介绍数据库扫描任务的添加步骤。

1. 选择DLP管理 > 数据发现 > 网络任务, 点添加, 在下拉菜单中选择数据库, 添加数据库扫描任务。
2. 输入网络任务名称和描述, 以表明该网络任务的作用。
3. 选择收集器扫描文档, 查找敏感性数据。默认收集器为UCSS上的DSA。

 提示: 管理较多文档时, 可部署若干个收集器(UCSS-Lite)。

4. 点击数据来源选项卡, 登录数据库获取检测文件:

a) 选择要识别的数据库类型, 以配置连接不同数据库的信息。

 提示: 目前支持SQLSERVER、MYSQL、ORACLE、POSTGRESQL、DB2、其它(Hiveodbc、Informix、Sybase\_ase、Sybase\_iq、Teradata)多种数据库类型, 并支持安全连接数据库。

b) 输入所连接数据库的IP地址。


c) 配置数据库的端口号。

数据库类型	端口号
SQLSERVER	1433
MYSQL	3306
ORACLE	1521
POSTGRESQL	5432
DB2	5000

d) 选择是否启用数据库安全连接。

e) 输入登录数据库的用户名称、密码或域名 ( 如果此数据库属于某一AD域, 域名为必填项 )。

f) 点击测试连接, 系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示: 如果尝试连接失败, 系统将会给出提示信息。

5. 点击策略选项卡, 选择列表中全部策略或部分策略执行数据发现扫描。

6. 点击过滤器选项卡, 配置如下参数, 过滤文件内容:


数据库名称	数据来源项测试数据库连通性后, 通过下拉列表选定需过滤的数据库名称。
包含表名称	点击添加, 选择需要扫描的数据库表。
排除表名称	点击添加, 选择需要排除的数据库表。

## 7. 点击计划选项卡，设置扫描计划：

## a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

## b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

## 8. 点击高级选项卡，设置每张表随机扫描的行数或选择每张表均扫描所有记录，以及每分钟最多处理的文件数量和文件大小。


## 9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。

## 10. 点击保存，新建的网络任务将被添加列表页。

## 添加Exchange扫描任务


介绍Exchange扫描任务的添加步骤。


- 选择DLP管理 > 数据发现 > 网络任务，点添加，在下拉菜单中选择Exchange，添加Exchange扫描任务。
- 输入网络任务名称和描述，以表明该网络任务的作用。
- 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

## 4. 点击文件来源选项卡，登录Exchange服务器获取检测文件：

- a) 输入连接Exchange服务器的IP/主机名。
- b) 输入登陆Exchange服务器用户名称、密码或域名。
- c) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- d) 添加扫描内容，选择扫描对象（用户）或公共文件夹，点击 添加到列表。

5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。

6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

按MailBox名称过滤	过滤：输入需要扫描的MailBox名称。 排除：输入排除扫描的MailBox名称。  提示：如果过滤和排除存在相同内容，采用排除优先原则。
按主题过滤	过滤：输入需要扫描的邮件主题。 排除：输入排除扫描的邮件主题。  提示：如果过滤和排除存在相同内容，采用排除优先原则。
按邮件大小过滤	选择邮件大小进行过滤(范围0~999 B/KB/MB)，大于100MB的邮件直接放行。
按邮件日期过滤	选择邮件日期进行过滤，指纹扫描将按照设置的邮件日期进行指纹识别。

7. 点击计划选项卡，设置扫描计划：


- a) 选择扫描类型：


计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

- b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>• 选择执行一次，请指定运行一次扫描任务的时间；</li> <li>• 选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>• 选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>• 选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>• 选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>



时间选项	描述
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：


- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

8. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。
10. 点击保存，新建的网络任务将被添加列表页。


#### 添加Outlook PST扫描任务



介绍Outlook PST扫描任务的添加步骤。

1. 选择DLP管理 > 数据发现 > 网络任务，点击添加，在下拉菜单中选择Outlook PST，添加Outlook PST扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

4. 点击文件来源选项卡，登录远程服务器获取检测文件：
  - a) 选择网络共享方式扫描文件，支持SMB和NFS。
  - b) 输入共享服务器的IP或主机名。
  - c) 输入要扫描的文件和文件夹所在的根文件夹或根目录。
  - d) 输入共享服务器用户名称、密码或域名。
  - e) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- f) 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。
  - g) 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。
5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。
  6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

按MailBox名称过滤	<p>过滤：输入需要扫描的MailBox名称。</p> <p>排除：输入排除扫描的MailBox名称。</p> <p> 提示：如果过滤和排除存在相同内容，采用排除优先原则。</p>
按主题过滤	<p>过滤：输入需要扫描的邮件主题。</p> <p>排除：输入排除扫描的邮件主题。</p> <p> 提示：如果过滤和排除存在相同内容，采用排除优先原则。</p>


按邮件大小过滤	选择邮件大小进行过滤(范围0~999 B/KB/MB ) , 大于100MB的邮件直接放行。
按邮件日期过滤	选择邮件日期进行过滤, 指纹扫描将按照设置的的邮件日期进行指纹识别。

7. 点击计划选项卡, 设置扫描计划:

a) 选择扫描类型:

计划项目	描述
增量扫描	文件扫描只有在初次扫描时, 扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划, 开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次, 请指定运行一次扫描任务的时间;</li> <li>选择每小时, 请指定运行扫描的时间及扫描截止日期, 如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描;</li> <li>选择每天/每周, 请指定运行扫描的时间及扫描截止日期, 如14:00;</li> <li>选择每月, 需要指定运行扫描的时间为某一天的某个时段及扫描截止日期;</li> <li>选择持续, 根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始, 还处于运行中的扫描任务将暂停, 此时间段结束后将继续扫描。</p> <p> 提示: 如果选定每小时扫描, 时间段为一个月。如果想在上班期间暂停扫描, 可选择周一至周五9:00~18:00暂停扫描。</p>

 注:

- 任务开始时间不能小于系统时间, 否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到, 不会重新运行该扫描任务。

8. 点击高级选项卡, 设置每分钟最多处理的文件数量和文件大小。

9. 点击动作选项卡, 选择是否开启动作, 执行补充脚本中的保护功能。


10. 点击保存, 新建的网络任务将被添加列表页。

#### 添加Exchange Online扫描任务

介绍Exchange Online扫描任务的添加步骤。


1. 选择DLP管理 > 数据发现 > 网络任务, 点击添加, 在下拉菜单中选择Exchange Online, 添加Exchange Online扫描任务。



2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

4. 点击文件来源选项卡，登录Office 365获取检测文件：

- a) 输入Office 365的网址。
- b) 输入Office 365的登录帐号。
- c) 输入Office 365的登录密码。
- d) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- e) 选择是否添加扫描对象。点击，从用户目录选择扫描对象。点击可删除所选扫描对象。

5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。

6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

按MailBox名称过滤	过滤：输入需要扫描的MailBox名称。 排除：输入排除扫描的MailBox名称。  提示：如果过滤和排除存在相同内容，采用排除优先原则。
按主题过滤	过滤：输入需要扫描的邮件主题。 排除：输入排除扫描的邮件主题。  提示：如果过滤和排除存在相同内容，采用排除优先原则。
按邮件大小过滤	选择邮件大小进行过滤(范围0~999 B/KB/MB)，大于100MB的邮件直接放行。
按邮件日期过滤	选择邮件日期进行过滤，指纹扫描将按照设置的的邮件日期进行指纹识别。


7. 点击计划选项卡，设置扫描计划：

- a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

- b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	设置执行扫描任务运行的频率。 <ul style="list-style-type: none"> <li>• 选择执行一次，请指定运行一次扫描任务的时间；</li> <li>• 选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> </ul>

时间选项	描述
	<ul style="list-style-type: none"> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：


- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

8. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。
10. 点击保存，新建的网络任务将被添加列表页。


#### 添加Salesforce扫描任务

介绍Exchange Online扫描任务的添加步骤。

1. 选择DLP管理 > 数据发现 > 网络任务，点击添加，在下拉菜单中选择Salesforce，添加Salesforce扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

4. 点击文件来源选项卡，登录Salesforce服务器获取检测文件：
  - a) 输入Salesforce登录网址，如：<https://login.salesforce.com/services/oauth2/token>
  - b) 输入可以访问Salesforce系统的用户名称。
  - c) 输入用户密码。
  - d) 输入访问Salesforce API所需的授权令牌Token。
  - e) 输入访问Salesforce API所需的Consumer Key，也叫Client Secret。
  - f) 输入访问Salesforce API所需的Consumer Secret，服务端的安全保障凭据。
  - g) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。


 提示：如果尝试连接失败，系统将会给出提示信息。

5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。
6. 点击过滤器选项卡，点击添加，选择需要排除或扫描的数据库表及数据库表列。
7. 点击计划选项卡，设置扫描计划：
  - a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。

计划项目	描述
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。


8. 点击高级选项卡，设置每张表随机扫描的行数或选择扫描所有记录，以及设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。
10. 点击保存，新建的网络任务将被添加列表页。

#### 添加邮件反查扫描任务


介绍邮件反查扫描任务的添加步骤。

数据发现的邮件反查功能对经由MTA服务器的过往邮件内容进行反查，用于定义未知敏感数据或者预防某些数据敏感度升级，帮助用户及时更新策略，防止用户通过邮件泄漏敏感内容。

1. 选择DLP管理 > 数据发现 > 网络任务，点击添加，在下拉菜单中选择邮件反查，添加邮件反查扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

4. 点击邮件来源选项卡，点击添加筛选根据下拉列表中的条件筛选要扫描的邮件。点击预览邮件列表查看所筛选邮件的详细信息。

 提示：详细信息请参考附录：邮件报告筛选条件显示列。


5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。

## 6. 点击计划选项卡，设置扫描计划：

## a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

## b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

## 7. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。

## 8. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。

## 9. 点击保存，新建的网络任务将被添加列表页。


## 添加OneDrive扫描任务

介绍OneDrive扫描任务的添加步骤。

## 1. 选择DLP管理 &gt; 数据发现 &gt; 网络任务，点击添加，在下拉菜单中选择OneDrive，添加OneDrive扫描任务。


## 2. 输入网络任务名称和描述，以表明该网络任务的作用。



## 3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。

## 4. 点击文件来源选项卡，登录OneDrive云服务获取检测文件：




- a) 输入提供OneDrive云服务所在的区域。
- b) 输入登录云服务的用户名称。
- c) 输入登录云服务的密码。
- d) 输入获取OneDrive数据的应用程序ID。
- e) 输入应用程序的密码。
- f) 输入租户的ID。
- g) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

- h) 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。
- i) 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。

5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。

6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

文件类型过滤	<p>选择文件类型进行过滤：</p> <p>过滤即包括文件类型：列出要识别的文件类型。点击从预定义文件类别中选择要过滤的文件类型。如：*.doc; *.xls; *.ppt; *.pdf；</p> <p>排除即排除文件类型：列出要排除的文件类型。点击从预定义文件类别中选择不进行过滤的文件类型。如：*.doc; *.xls; *.ppt; *.pdf；</p> <p> 注：如果包括文件类型和排除文件类型存在相同内容，采用排除优先原则。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB)，大于100MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。


7. 点击计划选项卡，设置扫描计划：

a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>• 选择执行一次，请指定运行一次扫描任务的时间；</li> <li>• 选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> </ul>

时间选项	描述
	<ul style="list-style-type: none"> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：


- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

8. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。
10. 点击保存，新建的网络任务将被添加列表页。

#### 添加SharePoint Online扫描任务


介绍SharePoint Online扫描任务的添加步骤。

1. 选择DLP管理 > 数据发现 > 网络任务，点击添加，在下拉菜单中选择SharePoint Online，添加SharePoint Online扫描任务。
2. 输入网络任务名称和描述，以表明该网络任务的作用。
3. 选择收集器扫描文档以查找敏感性数据。默认收集器为UCSS上的DSA。

 提示：管理较多文档时，可部署若干个收集器(UCSS-Lite)。


4. 点击文件来源选项卡，登录共享服务器获取检测文件：


a) 输入SharePoint站点根目录的主机名，如http://gumby/site\_name。


 注：在SharePoint中，站点路径不同于文件夹路径，DLP系统仅支持此字段的站点级URL。

b) 输入登录共享服务器的用户名称、密码或域名。

c) 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

d) 添加扫描内容。点击，弹出目录文件选择页，可选择需要扫描的文件或者文件目录。



e) 添加排除内容。点击，弹出目录文件选择页，可选择需要排除的文件或者文件目录。

5. 点击策略选项卡，选择列表中全部策略或部分策略执行数据发现扫描。

6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p>



	<p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p> <p> 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。</p>
真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件; 文字处理文件; 多媒体文件; 办公文件等</p> <p> 注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。</p>
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB )，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。


## 7. 点击计划选项卡，设置扫描计划：

## a) 选择扫描类型：

计划项目	描述
增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

## b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。

时间选项	描述
开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指数扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> </ul>

时间选项	描述
	<ul style="list-style-type: none"> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> <li>选择持续，根据持续扫描间隔时间对扫描目标进行持续增量扫描。</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p> <p> 提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。</p>

 注：

- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次任务扫描未完成而下一次的计划时间已到，不会重新运行该扫描任务。

8. 点击高级选项卡，设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡，选择是否开启动作，执行补充脚本中的保护功能。
10. 点击保存，新建的网络任务将被添加列表页。

#### 管理终端任务

在DLP管理 > 数据发现 > 终端任务页面管理终端任务。



终端任务扫描分析存储在终端所在主机的数据，并对命中策略的内容记录为数据发现事件。

1. 选择DLP管理 > 数据发现 > 终端任务，点击添加，新建终端任务。
2. 输入终端任务名称和描述，以表明该终端任务的作用。
3. 选择启用或禁用终端任务，默认为启用。
4. 点击扫描内容选项卡，选择要扫描的内容：

计算机	选择扫描所有计算机，或通过FQDN，IP地址，或唯一识别名指定要扫描的计算机。
本地磁盘	选择扫描所有磁盘目录，或输入指定磁盘目录。
排除内容	输入扫描过程中排除的磁盘目录。排除内容可识别多种环境变量，页面默认显示所有常用的需排除的变量类型，如无需排除该类型，可直接删除。

5. 点击策略选项卡，选择列表中已有的全部策略或部分策略执行数据发现扫描。
6. 点击过滤器选项卡，选择配置如下参数，过滤出所需文件：

过滤器	解释
文件扩展名过滤器	<p>按照文件扩展名进行过滤。</p> <p>过滤：从预定义文件扩展名中选择要进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等。</p> <p>排除：从预定义文件扩展名中选择不进行过滤识别的文件扩展名。</p> <p>如：*.doc; *.xls; *.ppt; *.pdf等</p>


	 注：如果过滤列表中的文件扩展名和排除列表中的文件文件扩展名存在相同，则系统选择优先排除该文件名。
真实文件类型过滤器	<p>按照真实文件类型进行过滤。</p> <p>过滤：从预定义真实文件类型中选择要进行过滤识别的文件类型。</p> <p>如：邮件文件；文字处理文件；多媒体文件；办公文件等</p> <p>排除：从预定义真实文件类型中选择不进行过滤识别的文件类型。</p> <p>如：邮件文件；文字处理文件；多媒体文件；办公文件等</p>  注：如果过滤列表中的真实文件类型和排除列表中的真实文件类型存在相同，则系统选择优先排除该文件名。
文件大小过滤	选择文件大小进行过滤(范围0~999 B/KB/MB)，大于100 MB的文件直接放行。
文件日期过滤	选择文件的生成日期进行过滤，即只采集设定日期的文件。

## 7. 点击计划选项卡，设置扫描计划：

## a) 选择扫描类型：

增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

## b) 选择是否开启扫描计划，开启后设置开始时间和暂停时段。


开始时间	<p>设置执行扫描任务运行的频率。</p> <ul style="list-style-type: none"> <li>选择执行一次，请指定运行一次扫描任务的时间；</li> <li>选择每小时，请指定运行扫描的时间及扫描截止日期，如每小时00/10/20/30/40/50分。最佳扫描时间是在夜间业务高峰时间之后运行指纹扫描；</li> <li>选择每天/每周，请指定运行扫描的时间及扫描截止日期，如14:00；</li> <li>选择每月，需要指定运行扫描的时间为某一天的某个时段及扫描截止日期；</li> </ul>
暂停时段	<p>在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。</p>  提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。

 注:


- 任务开始时间不能小于系统时间，否则系统将给出错误提示。
- 如果上次指纹任务扫描未完成而下一计划的计划时间已到，不会重新运行该扫描任务。

8. 点击高级选项卡，选择扫描条件，并设置每分钟最多处理的文件数量和文件大小。
9. 点击动作选项卡，选择是否启用保护原文、隔离原文或执行补充脚本中的保护功能。

保护原文	将发现的敏感文件备份到配置的SMB/NFS服务器。
隔离原文	将敏感文件备份以后，删除原敏感文件。
补充脚本	上传系统可执行自定义的补充脚本，执行脚本所配置的动作。

 注：保护原文和隔离原文的功能，需配置远程服务器获取检测文件：

- a. 选择以哪种网络共享方式扫描文件：SMB和NFS。
- b. 输入所访问共享服务器的IP或主机名。
- c. 输入套扫描的文件和文件夹所存放的根文件夹或根目录。
- d. 输入登录共享服务器用户名称、密码或域名。也可以匿名登录。
- e. 点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

10. 点击保存，新建的终端任务将被添加列表页。


## 邮件回溯

在DLP管理 > 邮件回溯页面管理邮件回溯。


ASEG开启记录所有邮件原文功能时，邮件回溯可以基于ASEG反查过往邮件内容，用于定义空白敏感数据或者预防已有数据敏感度升级，并标记命中策略的邮件为事件，以帮助用户及时更新策略。

 注：邮件回溯功能需要DLP和ASEG的双模块授权才可使用。

1. 选择DLP管理 > 邮件回溯，点击添加，添加邮件回溯。
2. 点击邮件来源选项卡，点击添加筛选选择要扫描分析的邮件内容；也可点击预览邮件列表，从列表中勾选已有的邮件内容进行扫描分析。

 提示：更多邮件筛选条件信息请参考[附录邮件报告筛选条件/显示列](#)。

3. 点击策略选项卡，选择列表中已有的全部策略或部分策略执行数据发现扫描。
4. 点击计划选项卡，选择是否开启扫描计划。开启后设置开始时间和暂停时段。

开始时间	选择开始扫描邮件的时间。
暂停时段	在扫描计划中停止某个时间的扫描。暂停时间段开始，还处于运行中的扫描任务将暂停，此时间段结束后将继续扫描。  提示：如果选定每小时扫描，时间段为一个月。如果想在上班期间暂停扫描，可选择周一至周五9:00~18:00暂停扫描。

- a) 选择扫描类型：

增量扫描	文件扫描只有在初次扫描时，扫描整个目录所有文件。之后扫描都将只对新增和有变化的文件进行扫描。
完整扫描	对任务设定的全部文件进行扫描。

5. 点击高级选项卡，选择扫描条件，并设置每分钟最多处理的邮件数量和文件大小。
6. 点击保存，邮件回溯任务将被添加列表页。

## 数据安全设置

介绍数据安全相关设置信息。

数据安全设置页面允许您的管理员进行数据安全相关的设置。


可选设置包括：

- 事件设置
- 移动邮件安全设置

### 事件设置

在DLP管理 > 数据发现 > 设置页面管理DLP事件设置。

DLP系统支持设置事件证据显示方式、事件详情展示内容等信息。

 提示：页面所有功能设置，在点击保存后才生效。

### 设置证据

字段	解释
使用纯文本安全取证	勾选此项，则查看事件详细信息时，证据文件的内容显示方式默认为纯文本，且不能切换为HTML。
删除已关闭事件的取证	勾选此项，则当事件状态被更改为关闭时，对应的证据文件将同时被删除。

### 设置Web邮件取证

字段	解释
证据内容表单按顺序显示下列字段	勾选此项，自定义邮件字段将从上到下依次显示于证据内容。
显示非表单格式数据	原始数据将显示在证据内容。

### 设置数据发现事件

字段	解释
最多存储发现事件数量	设置发现事件的最大存储量，超过限制时，最早的数据发现事件将会被自动删除。
锁定所有发现事件	勾选此项，当前所有发现事件将会被锁定，避免产生重复事件。

### 设置重复事件分组

勾选启用后，在30秒内由相同来源所连续产生的相同事件会被进分组显示。默认不启用。

### 设置安全策略事件

勾选启用以后可以在事件里看到命中“预置安全策略”的事件内容。




### 设置邮件 workflow

字段	解释
启用邮件 workflow 帐户安全验证	启用时，若用户在进行邮件 workflow 操作，则必须输入拥有事件管理权限的 UCSS 管理员帐号和密码。默认启用。
管理平台访问 IP	输入正确的访问管理平台的 IP 或域名。
管理平台访问端口	输入正确的访问管理平台的端口。

### 设置 WebMail

点击  添加 URL，当地址目标为此 URL 时，将 HTTP/HTTPS 网络通道事件标记为 Webmail，保存设置。


表 84: 页面图标和行间操作按钮功能

图标	解释
	删除所选的 URL。
	下载模板，导入 URL 地址。
	导出所选的 URL 地址。

### 移动邮件安全设置

在 DLP 管理 > 数据发现 > 设置页面管理 DLP 事件设置。




DLP 检测和保护通过 ActiveSync、POP3、IMAP 等方式接收到的移动端邮件，防止敏感内容被同步至移动设备而导致数据泄露。

 提示：页面所有功能设置，在点击保存后才生效。

### 设置分析内容

字段	解释
邮件	分析电子邮件的所有内容，包括主题、正文、收件人、发件人、附件等。
日程事件	分析日程项，包括主题、地点、参加者以及说明。
任务	分析待办事项列表中的内容。
联系人	分析同步的联系人内容。
便签	分析同步的笔记中的内容。

### 设置移动设备白名单

输入用户名和 User Agent，点击  添加到移动设备白名单列表中，对白名单中用户发起的任何请求全部放行。点击  编辑移动设备白名单的用户。点击  删除移动设备白名单的用户。

设置释放邮件有效期

设置释放邮件有效天数，范围为1~30天。

设置移动设备状态更新频率

设置移动安全网关MAG更新移动设备状态至管理平台的频率，范围1~60分钟。

## 数据安全监控

介绍数据安全监控相关信息。

DLP监控包括命中DLP策略的网络事件、发现事件、终端事件和移动事件，并记录流量日志。DLP监控记录包含有关事件的严重性、关联策略、匹配数量、违规内容和事件状态等多项信息，支持按照事件属性（通道/动作/策略组）查看事件，并保存为事件报告。查看详细报告信息请参考[数据安全报告](#)。

Web安全监控相关页面集中位于菜单栏的监控 > DLP监控选项下。

通过这些页面上的操作，管理员可以：

- 监控网络事件
- 监控发现事件
- 监控移动事件
- 监控回溯事件

### 网络事件

介绍网络事件实时监控的相关信息。

简介

网络事件监控功能查看所有网络通道流量命中DLP策略的事件详情和证据文件信息。



默认显示检测时间为最近3天，状态为未忽略的所有事件。

在监控 > DLP监控 > 网络事件页面管理监控到的实时网络事件信息。

页面介绍

实时监控页面包含以下快速按钮。

表 85: 快速按钮功能介绍

按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

实时监控页面包含以下操作按钮。

表 86: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 下载的文件为解密后的eml格式文件。</li> <li>• 支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>• 如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 添加的备注信息可以在历史记录中进行查看。</li> <li>• 支持为事件批量添加备注信息。</li> </ul>
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>



按钮	功能
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>支持事件的批量忽略和取消忽略。</li> </ul>
邮件审批	<p>点击按钮将所选的事件发送至安全管理员或主管进行审批。</p> <p>邮件审批包括释放和拒绝功能。</p> <ul style="list-style-type: none"> <li>选择释放则邮件会被投递给原收件人，事件动作会更新为已释放，已释放的邮件不可再次释放。</li> <li>选择拒绝则邮件不会被投递，事件动作会更新为已拒绝，已拒绝的邮件可以再次释放。</li> </ul> <p> 注：仅适用于邮件通道中的被系统隔离的事件，需事先在通知详情配置中选择邮件审核选项。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

### 事件处理 workflow

主管或相关人员通过接收的通知邮件处理事件。

在监控 > DLP监控 > 网络事件页面，管理员在列表中选择命中策略的事件后，可点击通知选择发送事件信息到相应的主管或其他收件人的邮箱。

在通知邮件页面底部点击邮件工作流的事件管理，即可跳转至事件配置界面，通过邮件更新事件属性信息并同步至UCSS网络事件页面。


事件工作流支持以下事件管理功能：

- 事件安全级别
- 事件状态
- 忽略事件
- 添加标签
- 添加备注

- 事件处理动作 ( 释放邮件/通知 )



#### 网络事件详情

查看命中策略的网络事件的详细运行信息。

选择列表中的网络事件，将鼠标悬浮于事件ID，出现事件详情图标  并点击，显示下列事件属性、命中策略详情、证据和历史记录等信息。





- 事件属性详细信息

事件属性	解释
来源	网络数据的来源信息，例如：用户名(用户识别模块)、IP地址、主机名或Email地址。如果为域账号，显示Logoname，否则显示为IP；如果发送方为邮箱用户，显示发送方邮箱地址。
TRS分值	内部用户的总风险值。
目标	网络数据的目标信息，例如：用户名(用户识别模块)、IP地址、URL地址、设备名(Endpoint USB/DVD/Printing)或Email地址。
方向	三种邮件数据流向：入向、出向和内部。
通道	检测网络数据的通道。
动作	违规后触发策略所执行的动作 ( 放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放 )。
最大匹配	触发策略规则项的最大匹配。如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
详细信息	若为HTTP/HTTPS事件，会显示URL信息；如果为邮件则显示邮件主题。
检测时间	引擎模块检测到违规事件触发策略的时间。
事件时间	管理平台收到违规事件的时间。
检测引擎	DLP检测数据的引擎模块。
分析引擎	后端分析数据的引擎ATS。
工作模式	DLP设备工作模式，支持仅监控和/阻断。

 注：点击  显示个人用户风险报告，详细信息请参考[查看个人用户风险报告](#)。

- 命中策略及详情：显示该事件命中的策略名称和详细违规内容。策略配置请参考[DLP策略](#)。
- 证据：包括事件来源和目标内容，若为HTTP/HTTPS事件，则显示URL信息。



表 87: 证据页面图标功能

图标	解释
	全屏显示证据文件。
	预览事件包含的文件。
	下载事件包含的文件。
	返回到事件列表页面。

- 历史记录：包括所有对该事件的操作信息，如果该事件被删除，则不会被记录，而显示在审计日志中。详细信息请参考[查看审计日志](#)。

### 个人用户风险报告

个人用户风险报告记录用户在最近7天、最近3天或今天所触发的网络事件和终端事件的风险详情。查看个人用户风险报告的方式有以下两种：

- 选择监控>DLP监控，点击统计，选择按来源统计，点击。
- 选择监控>DLP监控>网络事件>网络事件详情，点击。

个人用户风险报告页面详细信息如下：

- 显示来源IP地址及其他用户信息。括号内的数值表示来源事件数，点击数值跳转至网络事件或终端事件页面。
- 统计来源事件数和事件总数，并显示阻止和放行两种动作的比值。
- 显示来源事件数的当前排名。
- 显示来源事件的风险比例。
- 统计命中最多的策略名称和命中数量。
- 统计最多的发送目标和事件数量。
- 统计使用最多的通道和使用次数。
- 显示事件趋势图，展示不同时间点导入的策略和数量。
- 按策略排名展示事件命中四个安全级别（高/中/低/信息）的数量并排名。
- 按目标排名展示事件发送目标的数量并排名，并显示安全级别（高/中/低/信息）。
- 按通道排名展示事件使用通道的数量并排名，并显示安全级别（高/中/低/信息）。

## 发现事件

介绍发现事件实时监控的相关信息。

### 简介

发现事件监控功能记录所有数据发现流量(包括网络和终端)命中数据防泄漏DLP数据发现策略的事件详情和证据文件信息。

默认显示检测时间为最近3天，状态为未忽略的所有事件。



在监控 > DLP监控 > 发现事件页面管理监控到的实时发现事件信息。

### 页面介绍

实时监控页面包含以下快速按钮。

表 88: 快速按钮功能介绍


按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

实时监控页面包含以下操作按钮。


表 89: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 下载的文件为解密后的eml格式文件。</li> <li>• 支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>• 如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 添加的备注信息可以在历史记录中进行查看。</li> <li>• 支持为事件批量添加备注信息。</li> </ul>
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>

按钮	功能
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>• 选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>• 事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>• 支持事件的批量忽略和取消忽略。</li> </ul>
锁定	<p>点击按钮将事件置为锁定状态。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 对于非数据库发现事件，当同一文件被同一发现任务扫描产生发现事件时，如果事件处于未锁定状态，则会将事件记录的所有内容（除事件ID）更新，并产生历史记录，事件被发现任务XX更新；如果事件处于锁定状态，则事件记录的所有内容都不会更新，而是产生一条新的事件。</li> <li>• 对于数据库发现事件，当同一个数据表被同一发现任务扫描产生发现事件时，会首先清空同一数据表被同一发现任务扫描产生的所有数据库分片发现事件，然后产生新的分片事件；如果某些分片事件处于锁定状态，则这些事件不会被清除。</li> </ul> <p> 注：仅显示于发现事件报告页面。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>• 支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>• 支持删除报表中所有的事件。</li> <li>• 删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>• 如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

## 发现事件详情

查看命中策略的发现事件的详细运行信息。





选择列表中的发现事件，将鼠标悬浮于事件ID，出现事件详情图标  并点击，显示下列事件属性、命中策略详情、证据和历史记录等信息。

- 事件属性详细信息

事件属性	解释
文件路径	触发数据发现事件的文件路径。
文件名称	触发数据发现事件的文件名称。
文件夹路径	触发数据发现事件的文件夹路径。
字段名称	触发数据发现事件的列的名称。如针对hiveodbc数据库，字段名称记录了哪些列触发了数据发现事件。
文件大小	触发数据发现事件的文件大小。
文件所有者	触发数据发现事件的文件所有者。
主机名和IP地址	发现事件的主机名和IP地址。
创建日期	事件详情创建日期。
Checksum	冗余校验。
数据库名	数据库名称，适用于数据库事件。
数据表名	数据库的表名，适用于数据库事件。
事件状态	五种事件状态（新/进行中/关闭/误报/提级）。
安全级别	四种安全级别（高/中/低/信息）。
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
流量大小	数据流量的大小
检测时间	引擎模块检测到违规事件触发策略的时间。
事件时间	管理平台收到违规事件的时间。
检测引擎	DLP检测数据的引擎模块。
分析引擎	后端分析数据的引擎ATS。

- 命中策略及详情：显示该事件命中的策略名称和详细违规内容。策略配置请参考[DLP策略](#)。
- 发现任务，包含任务名称和任务类型。

## 证据页面图标功能

图标	解释
	全屏显示证据文件。
	预览事件包含的文件。
	下载事件包含的文件。
	返回到事件列表页面。

- 历史记录包括所有对该事件的操作信息，若该事件被删除，则不会记录而显示在审计日志中。详细信息请参考[查看审计日志](#)。

## 回溯事件


介绍发现回溯事件实时监控的相关信息。

### 简介

回溯事件监控记录所有由邮件回溯任务标记的事件信息详情和证据文件信息。

默认显示检测时间为最近3天，状态为未忽略的所有事件。



在监控 > DLP监控 > 回溯事件页面管理监控到的实时回溯事件信息。

 注：监控回溯事件功能需要数据防泄漏DLP和增强型安全邮件网关ASEG的双模块授权才可使用。

### 页面介绍

实时监控页面包含以下快速按钮。

表 90: 快速按钮功能介绍

按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

实时监控页面包含以下操作按钮。

表 91: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>下载的文件为解密后的eml格式文件。</li> <li>支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>添加的备注信息可以在历史记录中进行查看。</li> <li>支持为事件批量添加备注信息。</li> </ul>

按钮	功能
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>• 选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>• 事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>• 支持事件的批量忽略和取消忽略。</li> </ul>



按钮	功能
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

## 筛选条件/显示列

筛选条件/显示列	解释
事件ID	事件识别号
流量UUID	流量通用唯一识别码
事件时间	事件发生的时间
来源	用户名(用户识别模块)/IP地址/主机名/Email地址
目标	用户名(用户识别模块)/IP地址/URL地址/设备名(Endpoint USB/DVD/Printing)/Email地址
策略组	事件所属的策略组，支持多选。
策略名称	DLP策略名称
事件状态	五种事件状态（新/进行中/关闭/误报/提级）
安全级别	四种安全级别（高/中/低/信息）
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
事件标签	为事件添加的标签
违规内容	事件详细的违规内容，如机密等
组	组织架构定义的组名
组织单元	组织架构定义的组织单元名
来源IP	来源IP地址

筛选条件/显示列	解释
目标IP	目标IP地址
邮箱	组织架构中配置或同步AD的用户邮箱
主管	组织架构中配置或同步AD的主管信息
部门	组织架构定义的部门名称
URL分类	DLP策略定义的URL分类
国家	国家名称
城市	城市名称
位置	事件发生的位置
风险级别	事件所属的风险级别：较低、普通、严重、危险、高危。
职位	组织架构定义的职位名称

## 流量日志

介绍流量日志监控的相关信息。

### 简介

流量日志记录来自所有网络设备和所有通道的流量信息（不包含终端流量信息），包括记录并标识未命中数据防泄漏DLP策略的事件。

每个设备只支持显示200条流量日志。



默认显示检测时间为最近24小时的所有流量日志。

在监控 > DLP监控 > 流量日志页面管理实时监控的流量日志信息。

### 页面介绍

监控页面包含以下快速按钮。

表 92: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

监控页面的筛选条件如[筛选条件/显示列](#) on page 251所示。

## 筛选条件/显示列

筛选条件/显示列	解释
流量ID	各DLP模块检测到的流量的识别号
事件	流量是否命中策略产生事件
通道	网络通道和终端通道，如HTTP、FTP、SMTP等。
流量大小	以字节Byte为单位的流量大小
源	来源信息，如用户名、IP、Email等。
目标	目标信息，如IP、Email等。
动作	策略所对应的动作，如审计、阻挡等。
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
流量UUID	流量通用唯一识别码
时间	流量日志生成的时间
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称
分析状态	分析数据的状态，包括成功和失败
是否取消	显示数据分析是否取消
分析内容耗时	分析关键字、字典、指纹等所消耗的时间
排队耗时	流量在SPE队列排队等待时间
数据库指纹延迟耗时	等待分析数据库指纹的延迟时间
字典延迟耗时	等待分析字典的延迟时间
关键字延迟耗时	等待分析关键字的延迟
正则表达式延迟耗时	等待分析正则表达式的延迟
解压耗时	解压流量中的文本的时间
文件指纹延迟耗时	等待分析文件指纹的延迟时间
预定义规则检索耗时	身份证、银行卡等预置检测脚本检测时间
解析用户名耗时	解析源、目标用户名所消耗的时间
解析主机名耗时	将源IP解析为主机名所消耗的时间
总延迟耗时	分析流量的延迟时间，包含分析内容事件、创建事件时间和排队时间。
文件大小	流量中文件或附件的大小
是否超时	引擎分析是否超时
URL目录分析耗时	分析URL目录的延迟时间

## 数据安全报告

---

介绍数据安全报告相关信息。

数据安全报告整体展现命中的策略名称、策略动作和所属安全级别等事件的详细信息。

数据安全报告包括：

- 网络事件报告
- 发现事件报告
- 定时任务报告

## 网络事件报告

介绍数据安全网络事件报告的相关信息。

### 简介

网络事件报告展现命中策略的网络事件信息。网络事件报告信息包括事件来源 IP、目标、通道、动作和安全级别等，报告类型分为列表报告、图表报告和趋势报告。

用户行为报告用于统计某一段时间或某一个时间点的网络事件数据。

在报告 > DLP 报告 > 网络事件报告页面管理网络事件报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 图标和按钮

报告的设置页面包含以下操作按钮：

表 93: 页面图标功能介绍

图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。



### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

报告页面包含以下快速按钮：

表 94: 快速按钮功能介绍


按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

报告页面包含以下操作按钮：

表 95: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 下载的文件为解密后的eml格式文件。</li> <li>• 支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>• 如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 添加的备注信息可以在历史记录中进行查看。</li> <li>• 支持为事件批量添加备注信息。</li> </ul>
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>

按钮	功能
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>• 选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>• 事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>• 支持事件的批量忽略和取消忽略。</li> </ul>
邮件审批	<p>点击按钮将所选的事件发送至安全管理员或主管进行审批。</p> <p>邮件审批包括释放和拒绝功能。</p> <ul style="list-style-type: none"> <li>• 选择释放则邮件会被投递给原收件人，事件动作会更新为已释放，已释放的邮件不可再次释放。</li> <li>• 选择拒绝则邮件不会被投递，事件动作会更新为已拒绝，已拒绝的邮件可以再次释放。</li> </ul> <p> 注：仅适用于邮件通道中的被系统隔离的事件，需事先在通知详情配置中选择邮件审核选项。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>• 支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>• 支持删除报表中所有的事件。</li> <li>• 删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>• 如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相信步骤信息。

## 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示网络事件图表报告支持的类型和对应解释。

表 96: 报告类型

报告类型	解释
策略排名	统计不同策略被命中的事件数量，并排名前N位（最多30名）。
来源排名	统计不同来源所命中的策略总数，并排名前N位（最多30名）。
目标排名	统计不同目标所命中的策略总数，并排名前N位（最多30名）。
通道排名	统计不同通道处理的事件总数，并排名前N位（最多30名）。
安全级别	统计不同安全级别对应的事件总数，并排名前N位（最多30名）。
动作排名	统计不同动作类别对应的事件总数，并排名前N位（最多30名）。
策略组排名	统计不同策略组被命中的事件总数，并排名前N位（最多30名）。
事件状态	统计不同事件状态对应的事件总数，并排名前N位（最多30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

## 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。

表 97: 报告类型

报告类型	解释
安全级别趋势	统计不同安全级别对应的事件数量。
策略趋势	统计策略被命中的事件数量，并排名前N位（最多30名）。
全部属性	统计以上全部属性的趋势信息。

## 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

## 相关概念

[移动邮件报告](#) on page 344

介绍移动邮件报告的相关信息。

## 筛选条件/显示列

介绍数据安全报告的筛选条件/显示列。

下表罗列了数据安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
事件ID	事件识别号
流量UUID	流量通用唯一识别码
事件时间	事件发生的时间
检测时间	检测事件的时间
来源	用户名(用户识别模块)/IP地址/主机名/Email地址
目标	用户名(用户识别模块)/IP地址/URL地址/设备名(Endpoint USB/DVD/Printing)/Email地址
策略组	事件命中策略的组，支持多选。
策略名称	DLP策略名称
通道	事件所发生的通道 ( HTTP/HTTPS/FTP/IM/SMTP/自定义协议/网络打印/IMAP/POP3/"WebService应用/文件共享 )。
动作	策略所对应的动作 ( 放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放/水印 )。
事件状态	五种事件状态 ( 新/进行中/关闭/误报/提级 )
安全级别	四种安全级别 ( 高/中/低/信息 )
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称
释放状态	事件是否被手动释放
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
事件标签	为事件添加的标签
忽略状态	事件状态为已忽略或未忽略
工作模式	支持仅监控/阻断
违规内容	事件详细的违规内容，如机密等
组	组织架构定义的组名
组织单元	组织架构定义的组织单元名
来源IP	来源IP地址
目标IP	目标IP地址
邮箱	组织架构中配置或同步AD的用户邮箱
主管	组织架构中配置或同步AD的主管信息
部门	组织架构定义的部门名称
URL分类	DLP策略定义的URL分类
国家	国家名称



城市	城市名称
位置	事件发生的位置
释放者	邮件的释放者
释放时间	释放邮件的时间
职位	组织架构定义的职位名称
发现任务	发现任务名称
主机名	生成发现/移动事件的主机名
IP地址	生成发现事件的IP地址
文件路径	触发发现事件的文件路径
文件夹路径	触发发现事件的文件夹路径
文件大小	触发发现事件的文件大小
文件所有者	触发发现事件的文件所有者
文件夹所有者	触发发现事件的文件夹所有者
文件扩展名	触发发现事件的文件扩展名
锁定状态	发现事件是否被锁定
发现类型	发现任务类型，包括文件共享、SharePoint、Lotus Domino、Exchange、Outlook PST终端、数据库、邮件、Exchange Online、Salesforce、Salesforce Online、OneDrive、SharePoint Online。
设备类型	终端设备类型
操作系统	终端的操作系统
终端位置	终端属于公司内部或外部
来源RiskLevel	事件来源的RiskLevel ( 较低、普通、严重、危险、高危 )
匹配总数	事件命中所有规则的匹配数量总和

## 发现事件报告

介绍数据安全发现事件报告的相关信息。

### 简介

发现事件报告展现触发数据发现策略的事件信息。发现事件报告信息包括事件来源IP、目标、通道、动作和安全级别等，报告类型包括列表报告和图表报告。

发现事件报告用于统计某一段时间或某一个时间点的数据发现事件数据。

发现事件报告是基于数据发现事件的统计报告，故不提供趋势报告。

在报告 > **DLP**报告 > 发现事件报告页面管理发现事件报告。

如需配置发现事件，请参考[DLP数据发现](#)。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。

- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。





### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相应步骤信息。



报告列表页面包含以下操作按钮。

表 98: 页面图标功能介绍

图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

报告页面包含以下快速按钮。

表 99: 快速按钮功能介绍

按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

报告页面包含以下操作按钮。

表 100: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 下载的文件为解密后的eml格式文件。</li> <li>• 支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>• 如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 添加的备注信息可以在历史记录中进行查看。</li> <li>• 支持为事件批量添加备注信息。</li> </ul>
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>

按钮	功能
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>支持事件的批量忽略和取消忽略。</li> </ul>
锁定	<p>点击按钮将事件置为锁定状态。注意以下事项：</p> <ul style="list-style-type: none"> <li>对于非数据库发现事件，当同一文件被同一发现任务扫描产生发现事件时，如果事件处于未锁定状态，则会将事件记录的所有内容（除事件ID）更新，并产生历史记录，事件被发现任务XX更新；如果事件处于锁定状态，则事件记录的所有内容都不会更新，而是产生一条新的事件。</li> <li>对于数据库发现事件，当同一个数据表被同一发现任务扫描产生发现事件时，会首先清空同一数据表被同一发现任务扫描产生的所有数据库分片发现事件，然后产生新的分片事件；如果某些分片事件处于锁定状态，则这些事件不会被清除。</li> </ul> <p> 注：仅显示于发现事件报告页面。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

## 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示发现事件图表报告支持的类型和对应解释。

表 101: 发现事件图表报告类型

报告类型	解释
策略排名	统计不同策略被命中的事件数量，并排名前N位（最多30名）。
任务类型排名	统计不同任务类型对应的事件总数，并排名前N位（最多显示30名）。

报告类型	解释
安全级别	统计不同安全级别对应的事件总数，并排名前N位（最多30名）。
任务排名	统计不同任务对应的事件总数，并排名前N位（最多显示30名）。
扫描量排名	统计不同事件的扫描量，并排名前N位（最多显示30名）。
事件状态	统计不同事件状态对应的事件总数，并排名前N位（最多30名）。
数据发现任务策略统计	统计数据发现任务的策略数量，并排名前N位（最多显示30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 相关概念

[移动邮件报告](#) on page 344

介绍移动邮件报告的相关信息。

### 筛选条件/显示列

介绍数据安全报告的筛选条件/显示列。

下表罗列了数据安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
事件ID	事件识别号
流量UUID	流量通用唯一识别码
事件时间	事件发生的时间
检测时间	检测事件的时间
来源	用户名(用户识别模块)/IP地址/主机名/Email地址
目标	用户名(用户识别模块)/IP地址/URL地址/设备名(Endpoint USB/DVD/Printing)/Email地址
策略组	事件命中策略的组，支持多选。
策略名称	DLP策略名称
通道	事件所发生的通道（HTTP/HTTPS/FTP/IM/SMTP/自定义协议/网络打印/IMAP/POP3/”WebService应用/文件共享）。
动作	策略所对应的动作（放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放/水印）。
事件状态	五种事件状态（新/进行中/关闭/误报/提级）
安全级别	四种安全级别（高/中/低/信息）
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。

流量大小	数据流量的大小。
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称
释放状态	事件是否被手动释放
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
事件标签	为事件添加的标签
忽略状态	事件状态为已忽略或未忽略
工作模式	支持仅监控/阻断
违规内容	事件详细的违规内容，如机密等
组	组织架构定义的组名
组织单元	组织架构定义的组织单元名
来源IP	来源IP地址
目标IP	目标IP地址
邮箱	组织架构中配置或同步AD的用户邮箱
主管	组织架构中配置或同步AD的主管信息
部门	组织架构定义的部门名称
URL分类	DLP策略定义的URL分类
国家	国家名称
城市	城市名称
位置	事件发生的位置
释放者	邮件的释放者
释放时间	释放邮件的时间
职位	组织架构定义的职位名称
发现任务	发现任务名称
主机名	生成发现/移动事件的主机名
IP地址	生成发现事件的IP地址
文件路径	触发发现事件的文件路径
文件夹路径	触发发现事件的文件夹路径
文件大小	触发发现事件的文件大小
文件所有者	触发发现事件的文件所有者
文件夹所有者	触发发现事件的文件夹所有者
文件扩展名	触发发现事件的文件扩展名
锁定状态	发现事件是否被锁定

发现类型	发现任务类型，包括文件共享、SharePoint、Lotus Domino、Exchange、Outlook PST终端、数据库、邮件、Exchange Online、Salesforce、Salesforce Online、OneDrive、SharePoint Online。
设备类型	终端设备类型
操作系统	终端的操作系统
终端位置	终端属于公司内部或外部
来源RiskLevel	事件来源的RiskLevel ( 较低、普通、严重、危险、高危 )
匹配总数	事件命中所有规则的匹配数量总和

## 终端事件报告

介绍终端安全事件报告的相关信息。

### 简介

终端事件报告展现命中策略的终端事件信息。

终端事件报告信息包括事件来源IP、目标、通道、动作和安全级别等，报告类型包括列表报告、图表报告和趋势报告。

在报告 > **DLP报告** > 终端事件报告页面管理终端事件报告。

如需配置发现事件，请参考[DLP数据发现](#)。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 页面图标

报告列表页面包含以下操作按钮。

表 102: 页面图标功能介绍



图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

报告页面包含以下快速按钮。

表 103: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

报告页面包含以下操作按钮。

表 104: 报告按钮

按钮	
启用	点击按钮启用选中的终端设备。
禁用	点击按钮禁用选中的终端设备。
更多操作	点击按钮可选择对终端进行升级等更多操作。
终端数据发现	点击按钮对终端执行 <a href="#">数据发现</a> 任务。
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
申请禁用	点击按钮显示申请禁用的终端设备。
离线	点击按钮显示离线的终端设备。
在线	点击按钮显示在线的终端设备。
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。



下表显示网络事件图表报告支持的类型和对应解释。

表 105: 图表报告类型

报告类型	解释
策略排名	统计不同策略被命中的事件数量，并排名前N位（最多30名）。
任务排名	统计不同任务对应的事件总数，并排名前N位（最多显示30名）。
扫描量排名	统计不同事件的扫描量，并排名前N位（最多显示30名）。
来源排名	统计不同来源所命中的策略总数，并排名前N位（最多30名）。
目标排名	统计不同目标所命中的策略总数，并排名前N位（最多30名）。
通道排名	统计不同通道处理的事件总数，并排名前N位（最多30名）。
安全级别	统计不同安全级别对应的事件总数，并排名前N位（最多30名）。
动作排名	统计不同动作类别对应的事件总数，并排名前N位（最多30名）。
策略组排名	统计不同策略组被命中的事件总数，并排名前N位（最多30名）。
事件状态	统计不同事件状态对应的事件总数，并排名前N位（最多30名）。
终端位置	统计不同位置的终端安装数量，并排名前N位（最多显示30名）。
终端设备类型	统计不同终端类型的数量，并排名前N位（最多显示30名）。
终端操作系统	统计不同终端操作系统的数量，并排名前N位（最多显示30名）。
注册终端类型	统计不同终端注册类型的数量，并排名前N位（最多显示30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。

表 106: 报告类型

报告类型	解释
安全级别趋势	统计不同安全级别对应的事件数量。
策略趋势	统计策略被命中的事件数量，并排名前N位（最多30名）。
全部属性	统计以上全部属性的趋势信息。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 相关概念

[移动邮件报告](#) on page 344

介绍移动邮件报告的相关信息。

事件筛选条件/显示列

介绍终端安全事件报告的筛选条件/显示列。

下表罗列了终端安全事件报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
事件ID	事件识别号
流量UUID	流量通用唯一识别码
事件时间	事件发生的时间
检测时间	检测事件的时间
来源	用户名(用户识别模块)/IP地址/主机名/Email地址
目标	用户名(用户识别模块)/IP地址/URL地址/设备名(Endpoint USB/DVD/Printing)/Email地址
策略组	事件命中策略的组，支持多选。
策略名称	DLP策略名称
通道	事件所发生的通道 ( HTTP/HTTPS/FTP/IM/SMTP/自定义协议/网络打印/IMAP/POP3/"WebService应用/文件共享 )。
动作	策略所对应的动作 ( 放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放/水印 )。
事件状态	五种事件状态 ( 新/进行中/关闭/误报/提级 )
安全级别	四种安全级别 ( 高/中/低/信息 )
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
事件标签	为事件添加的标签
忽略状态	事件状态为已忽略或未忽略
违规内容	事件详细的违规内容，如机密等
终端位置	终端属于公司内部或外部
操作系统	终端的操作系统
设备类型	终端设备类型
工作模式	
组	组织架构定义的组名
组织单元	组织架构定义的组织单元名
来源IP	来源IP地址

目标IP	目标IP地址
邮箱	组织架构中配置或同步AD的用户邮箱
主管	组织架构中配置或同步AD的主管信息
部门	组织架构定义的部门名称
URL分类	DLP策略定义的URL分类
国家	国家名称
城市	城市名称
位置	事件发生的位置
主机名	生成发现/移动事件的主机名
来源RiskLevel	事件来源的RiskLevel ( 较低、普通、严重、危险、高危 )
职位	组织架构定义的职位名称
匹配总数	事件命中所有规则的匹配数量总和
终端服务器	

## 创建定时任务报告

### 如何创建定时任务报告


管理员可以定制任务报告，定期将其以邮件形式发送给指定的收件人。定制内容包括，报告类型（网络事件报告，数据发现报告，综合邮件报告等）、报告类型（列表，图标，趋势）和选择现有的报告等。

以下步骤描述了如何创建一个定时任务报告：

1. 选择报告 > 报告类型，在某一报告类型页面，比如 DLP报告 网络事件报告页面，点击右上角 定时任务报告链接。进入定时任务报告页面。
2. 点击添加按钮进入定时任务报告页面。
3. 输入名称和描述信息。
4. 在发送报告选项行，点击请选择图标，在弹出的选项框，选择报告的分类，类型等信息。点击保存。
5. 选择以什么文档格式发送报告，目前有PDF和Excel格式。
6. 勾选启用。
7. 在邮件设置部分设置邮箱相关信息。
8. 在任务定时计划部分设置执行周期。
9. 点击保存。

## 数据安全设备监控

在监控 > 设备监控页面查看设备监控信息。

在设备监控页面，将鼠标悬浮于DSG设备名称之上，出现  图标并点击，可查看设备监控信息。

DSG设备监控信息包括系统资源和服务状态，并支持三种数据统计时段（1小时/24小时/7天）。

表 107: DSG系统资源信息

设备信息统计	解释
设备基本信息	统计当前设备的基本信息，如主机名称、IP地址、系统类型、CPU、物理内存、硬盘容量和网卡数量等。

设备信息统计	解释
CPU资源利用率	统计当前设备CPU使用率，包括用户占用、系统占用和空闲的CPU的比例。
网卡资源利用率	统计当前网卡的发送和接收速率，以及总速率。
内存资源利用率	统计当前内存用于系统及应用、缓存的使用情况。
硬盘资源使用情况	统计系统硬盘和数据硬盘的使用情况。

表 108: DSG服务状态信息

服务状态	解释
设备版本信息对比	当前UCSS作为基准设备，将注册设备各功能模块的版本信息与基准设备版本信息同步。可选同时同步或单独同步。
安全引擎负载统计	统计安全分析引擎(CAE)的负载状况。
请求数量统计	统计设备接收到的需要进行分析的请求数量。
命中事件统计	统计设备接收到的请求命中DLP策略产生事件的数量。
OCR引擎负载统计	统计OCR图像识别引擎的负载情况。
OCR队列状态统计	统计OCR图像识别引擎队列中等待分析和扫描超时的图片数量。

## 数据安全设备管理

管理注册于UCSS的Web安全设备。

管理注册于UCSS的DSG设备的功能、配置，以及设备、服务的启动、停止和重启等操作。

### 设备

配置设备相关的选项页面。

该菜单包含设备相关的选项页面。

#### 系统信息

介绍设备的系统信息界面。

系统信息包括设备的基本信息和服务状态信息。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 系统信息菜单。

系统信息页面支持查看以下信息。

#### 设备信息

设备信息包括主机名称，IP地址，系统类型等只读的信息。

在此栏中，可以一键重启或关闭设备。

#### 系统信息

系统信息包括系统负载状态和各种系统服务的运行状态。

参考[系统服务介绍](#)，可以获得各种系统服务的基本介绍。

在此栏中，可以选择对某项服务进行重启、停止或启动，或对所有服务进行批量操作。

## UCSG-DSG基本设置

介绍配置UCSG-DSG基本设置的步骤。

在系统 > 设备管理页面配置设备的基本信息。基本设置包括设备工作模式、安全模式和同步设置。


1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 基本设置，对UCSG-DSG设备进行基本配置。
2. 选择是否启用UCSG-DSG设备，默认开启。
3. 输入设备名称和描述，说明其用途。
4. 选择UCSG-DSG设备的工作模式：

旁路监控模式	在网络设备（例如交换机）上对网络流量镜像(SPAN/MIRROR)至UCSG-DSG设备进行分析，只支持明文协议，并且无法阻断数据，只支持审计功能。
串行模式	串行部署于网络设备之间，对网络流量进行分析。支持明文和加密协议，并支持阻断。

5. 设置不同安全级别下的引擎和透传对应的安全模式。
6. 选择手动或自动同步系统时间：

自动同步	自动与UCSS设备同步系统时间，需设定每天的同步时间。
手动同步	点击立即同步，立刻触发一次与UCSS设备同步系统时间。

7. 点击保存，配置生效。

 注：高级设置请务必在在天空卫士™技术支持工程师的指导下修改。

## 授权许可

介绍如何管理设备的授权许可设置。

在系统 > 设备管理页面进行设备授权许可。

1. 选择系统 > 设备管理进入设备管理页面。点击要查看的设备，进入设备 > 授权许可页面。
2. 选择以下授权方式：


项目	描述
授权码	在线授权需输入授权码。
授权文件	离线授权需上传授权文件。

授权成功后，在当前页面显示授权信息如下：

表 109: 当前授权状态

设备编号	显示当前设备编号
授权号	显示当前设备所使用的授权号。
用户名称	显示License授予时的用户名称，一般为企业名称。
工作模式	显示当前设备工作模式，支持阻断和审计。
授权类型	显示授权类型，包括正式版本和测试版本。
功能模块列表	显示授权的功能模块，每个功能模块的已授权数量，当前状态和使用的有效期。

3. 点击保存，设置生效。

 提示：点击下载设备ID可下载设备ID信息为记事本格式，查询和授权License时可以使用该文件。

## 网络

配置网络相关的选项页面。


该菜单包含网络相关的选项页面。


### UCSG-DSG网卡设置


介绍设备网卡的设置步骤。



在系统 > 设备管理页面进行设备授权许可。

UCSG-DSG的网卡包括Mgmt网卡负责管理设备，MTA网卡提供邮件服务，Br0网卡提供桥接服务。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 网络 > 网卡配置页面。
2. 点击  编辑MTA和P1/P2网卡（Br0）的网卡设置，Mgmt网卡不可编辑。

 提示：


- 在旁路模式下，UCSG-DSG的网卡显示为P1和P2；在串行模式下，网卡显示为Br0，提供桥接服务。
- 点击  查看Mgmt网卡的配置信息。

3. 点击确定，网卡设置完成。
4. 选择设备网卡并输入网卡的默认网关。
5. 输入DNS服务器IP，点击  添加于列表；点击  删除列表中所选的DNS服务器。
6. 点击保存，配置生效。

### 路由设置

介绍管理路由设置的步骤。




在系统 > 设备管理页面设置路由。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 网络 > 路由页面。
2. 点击  添加静态路由或策略路由：

静态路由	添加静态路由到主路由表中，不对源IP做限制，所有从本设备发起或者转发的数据包都将遵循此路由规则。
策略路由	只有本设备发起的数据包匹配此规则。

3. 输入目标网络IP地址、子掩码和网关（网关需要跟选中网卡的地址在同一个子网内）。
4. 选择网卡类型：Mgmt负责管理设备，MTA提供邮件服务，P1和P2提供代理服务（仅ASWG设备），Br0提供桥接服务（仅UCSG-DSG设备）。
5. 点击确认，添加路由到列表中。
6. 点击保存，设置生效。

表 110: 页面图标和行间操作按钮功能

	导出路由配置。
	导入路由配置。
	删除所选路由。

## 网卡绑定

介绍网卡绑定设置的步骤。

在系统 > 设备管理页面设置网卡绑定。

网卡绑定功能将两个或者更多的物理网卡绑定成一个虚拟网卡以提供负载均衡或者冗余。

1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 网络 > 网卡配置页面，选择要绑定的网卡，滑动状态条开启网卡绑定。
2. 选择绑定网卡的工作模式：

Active-Standby模式	主备方式，当一个网卡故障时另一个网卡接管所有工作。
Active-Active模式	双活方式，两个网卡同时工作，增加带宽的同时实现冗余。需要交换机支持聚合功能。

➔ 注意：Bypass网卡仅支持Active-Active模式。

3. 点击保存，网卡绑定生效。

## 功能

配置功能相关的选项页面。


该菜单包含功能相关的选项页面。

### UCSG-DSG协议配置

介绍UCSG-DSG协议配置的步骤。


在系统 > 设备管理页面配置UCSG-DSG协议。

UCSG-DSG支持HTTP、FTP、POP3、IMAP、SMTP协议和自定义协议，检测并分析各协议流量。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 协议页面。
2. 选择要编辑的协议，鼠标悬浮于协议名称上方，点击  编辑所选协议。

 提示：点击  图标可停用该协议。

3. 滑动状态条开启或关闭协议分析。
4. 配置协议端口号，端口与协议相对应并作相应的流量处理。
5. 配置检测的最小字节数，少于此字节数的内容不被检测。
6. 选择串行工作模式下UCSG-DSGD的工作模式为监控或阻断。


 提示：

- 串行模式在设备 > 基本设置页面进行配置。默认设置为旁路模式。
  - HTTP协议在阻断模式下可设置阻断页面提示信息，可选择默认提示页面或定向到公司自定义阻断提示网页。
7. 选择来源、目标和分析内容。根据用户定义的网段范围对HTTP请求或响应流量、FTP和SMTP的上传或下载流量、POP3和IMAP接收邮件流量进行内容分析。
  8. 点击保存，设置生效。

### UCSG-DSG自定义协议配置

介绍如何配置UCSG-DSG自定义协议。

在系统 > 设备管理页面配置UCSG-DSG协议。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 协议页面。
2. 点击  添加自定义协议。

3. 输入自定义协议名称，说明其作用。
4. 滑动状态条开启或关闭协议分析。
5. 配置协议端口号，端口与协议相对应并作相应的流量处理。
6. 配置检测的最小字节数，少于此字节数的内容不被检测。
7. 选择串行工作模式下UCSG-DSGD的工作模式为监控或阻断。

 提示：


- 串行模式在设备 > 基本设置页面进行配置。默认设置为旁路模式。

8. 选择来源、目标和分析内容。根据用户定义的网段范围对自定义协议请求或响应流量进行内容分析。
9. 点击保存，设置生效。

### SMTP协议配置(串行模式)

介绍SMTP协议支持的接入方式。

在串行模式下，SMTP协议支持SMTP Proxy和SMTP MTA两种接入方式。


 提示：





- 串行模式在设备 > 基本设置页面进行配置。默认设置为旁路模式。

#### UCSG-DSG SMTP Proxy

介绍UCSG-DSG的SMTP协议在Proxy接入模式下的配置步骤。

SMTP Proxy模式下的配置步骤如下：


1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 功能 > 协议，点击  编辑SMTP协议。
2. 点击基本选项卡，开启或关闭协议分析。开启后进行如下配置：
  - a) 选择协议接入方式为SMTP Proxy。
  - b) 选择是否开启SMTP加密支持。
  - c) 配置透传代理端口端口，端口与协议相对应并作相应的流量处理。
  - d) 配置检测的最小字节数，少于此字节数的内容不被检测。
  - e) 选择工作模式为监控或阻断。
 

 提示：监控不会干扰邮件的正常处理和投递，阻断即当邮件触发策略时根据策略动作放行、隔离、删除邮件附件或加密等。
  - f) 选择来源、目标和分析内容进行流量分析。例如分析SMTP发送邮件的流量内容。
  - g) 选择是否开启自动识别邮件服务器。开启后，DSG网关会自动识别邮件的来源是邮件服务器还是客户端。如果来源是邮件服务器，则邮件由内部的MTA模块直接进行分析处理，不需要在邮件服务器上做任何配置变更，并可以实现对此类邮件的隔离、加密、释放等功能。该功能启用后需要重启相关服务。
3. 点击内部域名选项卡：
  - a) 输入公司内部域名，用来区分邮件方向，点击  添加。
  - b) 选择需要分析的邮件方向。
  - c) 添加不需要检测的邮件来源邮箱地址和域名，点击  添加。点击  删除所选来源。
4. 点击保存，设置生效。

#### UCSG-DSG SMTP MTA

介绍UCSG-DSG SMTP协议在MTA接入模式下的配置步骤。


SMTP MTA模式下的配置步骤如下：


1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 功能 > 协议。
2. 点击  编辑SMTP协议。



### 3. 点击基本选项卡，开启或关闭协议分析。开启协后进行如下配置：

- a) 选择协议接入方式为SMTP MTA。
- b) 选择工作模式为监控或阻断。




 提示：监控不会干扰邮件的正常处理和投递，阻断即当邮件触发策略时根据策略动作放行、隔离、删除邮件附件或加密等。

- c) 配置检测的最大字节数，大于此字节数的内容不被检测。
- d) 选择是否启用全邮件记录，可记录全部邮件原文。
- e) 设置FQDN信息。  
安全管理员可按照需要自定义FQDN信息。
- f) 设置SMTP欢迎信息。
- g) 输入受信IP地址和子网掩码，点击添加为受信地址，MTA只接受此列表中来源发起的SMTP连接。
- h) 开启高级路由，设置SMTP邮件投递路由规则。配置路由时可以设置优先级，如果同一个域名定义了多个邮件路由而对应多个服务器IP地址，系统会尝试按照路由的优先级来发送邮件。当多条路由的优先级相同时，系统会使用轮询发送机制。
- i) 指定MTA投递邮件的下一跳，可以选择DNS解析投递也可设置指定接收地址。如果开启高级邮件路由，则高级路由中配置的投递地址优先级最高。
- j) 选择TLS传输安全机制：

强制明文	强制使用明文，如果对方不支持明文，邮件将不能完成投递。
自适应	优先使用TLS，如果对方支持TLS，则使用TLS进行投递，否则使用非TLS进行投递。
强制TLS	强制使用TLS，如果对方不支持TLS，邮件将不能完成投递。

- k) 选择是否发送邮件退信，可选择退信收件人为源发件人或指定收件人。
- l) 选择是否添加邮件声明，可自定义邮件声明，表明邮件已经过检测等。
- m) 设置加密邮件的网关的主机名/IP和端口号。支持设置加密标识，主题加密标识用户可见，X-Header加密标识用于服务器解析。

### 4. 点击内部域名选项卡：

- a) 输入公司内部域名，用来区分邮件方向，点击添加。
- b) 选择需要分析的邮件方向。
- c) 添加不需要检测的邮件来源邮箱地址和域名，点击添加。点击删除所选来源。

### 5. 点击保存，设置生效。

## ICAP功能

介绍设置ICAP功能的步骤。

在系统 > 设备管理页面设置ICAP功能。

第三方代理可以通过ICAP协议将数据传输到UCSG-DSG进行DLP检测。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > ICAP页面。
2. 滑动状态条选择开启或关闭ICAP功能。
3. 配置协议端口，端口与协议相对应并作相应的流量处理。
4. 选择ICAP服务器的工作模式为监控模式和阻断模式。在阻断模式下，当数据被策略阻断时可选择显示默认提示页面或定向到公司自定义阻断提示网页；当发生错误（如系统连接错误或文件错误）时，可以选择放行或阻断（可由数据的安全性判断是否放行）。
5. 配置最小检测流量，少于此流量的内容不被检测。
6. 设置发送数据的来源IP。可选接收任何IP发送的数据，或只接收指定IP发送的数据。

7. 点击保存，设置生效。

### 网络对象

介绍设置网络对象功能的步骤。

在系统 > 设备管理页面设置网络对象功能。

在设置协议时可直接引用网络对象，过滤出需要检测的流量或过滤掉不需要检测的流量。



1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 网络对象页面。
2. 点击添加，新建网络对象。
3. 输入网络对象名称。
4. 输入网络对象包含的IP或IP段，点击  添加到列表。
5. 输入排除在网络对象外的IP或IP段，点击  添加到列表。
6. 点击确定，添加成功。

表 111: 页面图标和行间操作按钮功能

	修改网络对象。
	删除所选网络对象。

### 邮件队列

介绍设置邮件队列的步骤。

在系统 > 设备管理页面设置邮件队列。

邮件队列统计MTA中邮件队列中的邮件总数、等待处理的邮件数量、等待策略分析的邮件数量和等待投递的邮件数量，并可以筛选不同的邮件状态（等待处理/等待投递/等待分析）。

选择选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 邮件队列页面，点




击立即投递手动投递邮件。点击  将所选邮件从列表中删除。




### UCSG-DSG证书设置

介绍证书设置的步骤。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 证书页面。

DSG证书包括企业证书、受信证书和服务器证书。管理员可以分别点击各选项卡进行如下操作：

- 企业证书：企业证书为一个CA证书，作为客户端和原始服务器站点之间的中转站，保证与客户端的正常进通信。
  - 点击导入证书按钮导入已有的企业证书。
  - 点击创建证书按钮在线创建企业证书。
  - 点击下载证书按钮下载证书到本地。
- 受信证书：受信证书由DSG所信任的原始服务器提供。
  - 点击  按钮导入受信证书。
  - 点击  按钮删除所选受信证书。
  - 点击悬浮图标  查看证书信息。
  - 点击备份全部按钮备份受信证书列表中的全部受信证书到本地。
  - 点击恢复按钮按钮恢复本地备份的受信证书，执行恢复操作将覆盖所有受信证书。
- 服务器证书：服务器证书用于存储需要进行反向代理的目标站点证书。

- 点击  按钮添加服务器证书。在启用反向代理功能时，客户端在连接服务器时返回此证书来标识服务器。
  1. 输入服务器证书的名称。
  2. (选填) 输入服务器证书的描述信息。
  3. 点击选择，从本地上传被保护站点的服务器证书，格式为PEM。
  4. 输入证书的密钥，或点击选择从本地上传密钥。
  5. (选填) 输入该证书的密码。
  6. 选择证书的目标站点类型，并输入该证书对应的站点域名或IP。
  7. 点击保存按钮，服务器证书添加成功。
- 点击  按钮删除所选服务器证书。
- 点击  按钮导出所选证书到本地。

### OCR功能

介绍管理OCR功能的步骤。

在系统 > 设备管理页面设置OCR功能。

OCR识别图像功能支持本地和外置OCR服务器，外置OCR服务器可以解析网络流量中的图片内容并进行DLP分析，提高了对大量图片内容的处理速率，减轻系统资源消耗。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > OCR页面。
2. 滑动状态条，开启OCR功能。
3. 选择OCR工作的精确度，平衡系统资源消耗：

快速	效率高但是精确度低。
平衡	兼顾效率和精确度。
精确	精确度高但是效率低。


4. 选择OCR识别的语言，包括简体中文、繁体中文和英文。
5. 设置OCR图像识别引擎检测文件的大小限制，0表示不限制大小。
6. 选择OCR服务器，包括本地OCR引擎和远程OCR引擎。
7. 点击保存，设置生效。

### 全局例外

介绍设置全局例外功能的步骤。

在系统 > 设备管理页面设置全局例外功能。

全局例外针对不同协议进行集中配置来源和目标，代理服务器透传列表中的相关配置。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 全局例外页面，点击  新建全局例外并添加规则。
2. 输入全局例外名称，说明其作用。
3. 选择是否启用该全局例外功能。
4. 输入来源IP/IP段，如果设置全部来源即为0.0.0.0-255.255.255.255。

 注：ICAP Server的全局例外使用的来源IP/IP段为172.16.1.1, 192.168.0.1-192.168.0.200。

5. 输入目的IP/IP段或域名，全部域名即为“所有”。

 注：

- 域名方式仅适用于HTTP和HTTPS协议。

- ICAP Server的全局例外使用的目的IP/IP段为220.181.112.244, 220.181.113.100-220.181.113.120。也支持正则表达式的添加方式。
6. 根据应用场景，选择相应的传输协议。
  7. 点击保存，设置生效。

表 112: 页面图标和行间操作按钮功能

图标	解释
	启用所选全局例外。
	禁用所选全局例外。
	删除所选全局例外。
	导入全局例外文件，可以参考模板生成，导入文件样例文件名称为“全局例外.json”。
	导出全局例外文件到本地。

### 抓取网络文件设置

介绍设置抓取网络文件功能的步骤。


在系统 > 设备管理页面设置抓取网络文件功能。

系统自动收集网络传输的文件放于指定目录，包括web流量中的文件、邮件中的附件等，为数据聚类提供文件样本。

1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 功能 > 抓取网络文件,选择是否启用自动抓取网络文件功能。

如果选择开启抓取网络文件功能，需要配置远程服务器如下：

- a. 选择远程存储的共享方式，支持SMB和NFS。
- b. 输入远程服务器的IP或主机名。
- c. 输入存储文件样本的文件夹路径。
- d. 输入共享服务器用户名、密码和域名，或选择已保存的用户凭证登录。
- e. 点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。

 提示：如果尝试连接失败，系统将会给出提示信息。

2. 点击保存，设置生效。

## 其他

其他的选项页面。

该菜单包含其他的选项页面。

### SNMP功能

介绍管理SNMP功能设置的步骤。

在系统 > 设备管理页面设置SNMP功能。

设备支持外部应用访问SNMP服务器来收集设备信息。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > SNMP页面，设置SNMP功能。。
2. 滑动状态条，开启SNMP功能。
3. 选择SNMP query版本，可以设置为v1或v2c。

4. 输入SNMP的团体名，即SNMP的用户名或密码，只允许使用此团体名访问SNMP服务器。
5. 选择以下SNMP的连接方式：

任何IP	任何IP地址都可访问SNMP。
仅限于下列IP	输入IP地址，点击  添加到可访问SNMP的IP列表。

6. 点击保存，设置生效。

#### 收集日志

介绍配置收集日志功能的步骤。

在系统 > 设备管理页面设置收集日志功能。

设备支持收集系统日志信息，了解系统运行状态。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 收集日志页面，设置收集日志功能。
2. 选择收集日志的时间段。
3. 选择收集日志的类型。
4. 点击收集日志，收集所设定日期和指定类型的日志，显示于日志收集历史列表中。

点击 可将得收集得日志文件下载到本地；点击 可删除所选日志文件。

#### 备份和恢复

介绍备份/恢复功能设置的步骤。

在系统 > 设备管理页面设置备份和恢复功能。

UCSS设备支持立即备份和立即恢复系统配置，包括配置信息、证据文件、邮件、网络及主机信息等，并支持定期备份功能。

1. 选择设备 > 其他 > 备份,进入备份或恢复页面。
2. 点击定期备份启动定期备份，设置定期备份的时间。
3. 点击备份设置，选择以下备份方式和备份内容：

备份至本地	选择备份至本地设备，设置备份日志数量的最大值，若本地保存数量大于设置的最大值则会删除最早的备份。
备份至远程	支持备份至Samba服务器和NFS服务器，需输入服务器的IP/主机名、文件夹路径和用户信息，并进行测试连接。

备份记录会出现在备份历史中，点击删除可删除所选备份。

4. 点击保存，设置生效。

#### 升级和补丁

介绍升级/补丁功能设置的步骤。

在系统 > 设备管理页面设置升级和补丁功能。

设备支持在线版本升级和补丁安装，但升级不支持版本回退。选择系统 > 设备管理进入设备管理页面后。点击要查看的设备，进入设备 > 其他 > 升级/补丁页面，然后进行升级或补丁设置。

- 升级

选择升级选项卡，点击检查更新连接天空卫士的安装包服务器，获取安装包列表，选择安装包下载并安装。如果用户设备无法直接访问互联网，可通过代理服务器配置使用代理进行检查更新，点击代理服务器配置代理服务器。

点击上传安装包从本地上传升级安装包。

- 补丁

选择不定选项卡，查看当前版本和可用补丁。点击上传安装包从本地上传补丁安装包，安装之后可以选择卸载。

### 远程控制

介绍远程控制功能设置的步骤。

在系统 > 设备管理页面设置远程控制功能。

设备启用SSH连接后，可通过SSH执行远程设备故障排查。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 远程控制页面。
2. 选择是否启用以下功能：

启用远程控制	启用远程控制以后可以开启SSH端口并使用设备管理账号（例如ucssadmin帐号）登录设备进行命令操作。
启用技术支持模块	启用技术模块之后，获取6位密码。该密码需要提供给天空卫士进行解密后使用。
启用超时限制	设置在指定时间之后自动关闭远程控制。

3. 点击保存，设置生效。



注：

远程访问记录可在远程访问历史中查询。

### 自定义页面

介绍设置自定义页面的步骤。

在系统 > 设备管理页面设置自定义页面。

设备支持用户自定义显示界面，当网络请求被设备阻断时，展示给用户此提示页面。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，选择如下页面定义方式：

默认页面	使用系统默认页面。
自定义LOGO和公司名称	输入公司名称，上传公司Logo，自定义具有公司标识的显示页面。
定制页面	下载预置页面模板或下载当前自定义页面，本地设计修改后上传至系统。

2. 点击保存，设置生效。

### 系统工具

介绍系统工具设置的步骤。

在系统 > 设备管理页面设置系统工具。

系统工具预置多条CLI命令，即使不连接后台时也可以使用系统工具进行故障排查，并显示执行结果。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，从下拉框中选择索要执行的命令。
2. 输入出现故障的设备主机名或IP，点击执行开始运行故障排查命令，点击停止可终止执行命令。执行结果显示于黑色屏幕中。


### 设置设备高可用


介绍设置设备高可用的步骤。




在系统 > 设备管理页面配置设备高可用。

设备高可用是将两台或多台同类型设备（DSG/ASWG/SEG/UCWI）互作备份，当其中某台出现故障时同组设备可以立即替代该设备，保证MTA、ICAP Server、代理服务业务的正常进行。

当设备出现硬件故障（断电、网卡等出现问题），网络故障（网线连接问题、其他网络设备出现故障）等情况无法实现设备切换。

 提示：高可用仅支持同类型设备的同类型网卡间的切换，ASWG设备的P1和P2网口只能在代理模式下支持高可用切换。

 注：启用了配置同步功能后，当配置了高可用的设备组之中的任意一台设备变更了配置（如HTTP里的参数变更），安全管理员无需重复操作，该设备的配置改动能自动同步到高可用组内的其他设备中。

1. 选择系统 > 设备管理，点击高可用，在下拉菜单中选择设备型号，配置设备高可用。
2. 输入设备组名称，如北京UCSG-ASWG设备。
3. 点击  从已注册设备列表中选择设备。点击  删除所选设备。设备不能被重复添加到不同的分组。
4. 开启虚拟IP，进行如下配置：
  - a) 输入虚拟IP地址（虚拟IP数量不能大于组内的设备数量并且IP地址与在设备需在同一IP段）。
  - b) 选择网卡类型：Mgmt管理接口，MTA邮件接口，P1/P2代理接口（仅UCSG-ASWG设备）。
  - c) 设置子网卡序号（用于标记，数字不重复即可）。
  - d) 点击  添加于列表。
5. 点击保存，添加完成。

## 数据安全日志

---

### 流量日志

监控-DLP监控-流量日志

### 系统日志

监控--系统日志

### 审计日志

监控--审计日志

### 数据安全设备日志

系统-设备管理-dsg-其他-收集日志





---

# 第 6 章

---

## 邮件安全

---

内容:

- [邮件安全检测条件](#)
- [邮件安全管理](#)
- [邮件安全监控](#)
- [邮件安全报告](#)
- [邮件安全设备监控](#)
- [邮件安全设备管理](#)

介绍天空卫士™邮件安全解决方案。

在天空卫士™安全鳄®统一内容安全UCS解决方案中，增强型安全邮件网关ASEG作为方案中的邮件安全模块，保护您的邮件用户远离任何邮件通道中的安全威胁。

## 邮件安全检测条件

介绍邮件安全检测条件的相关信息。

天空卫士™安全鳄®统一内容安全UCS解决方案中的邮件安全模块在安全策略中运用多种检测条件检测违反企业安全制度的内容和行为，并在有必要的情况下，采取对应的策略行为，限制或阻断通信，确保企业邮件安全。

邮件安全解决方案支持以下检测条件。

- 反病毒
- 反垃圾
- 反欺诈
- URL分类
- 安全URL分类

### 反病毒

介绍检测条件中的反病毒检测条件及其相关知识。

反病毒检测条件可检测邮件及其任意附件中所包含的利用邮件进行传播的病毒等安全威胁。

### 反垃圾

介绍检测条件中的反垃圾检测条件及其相关知识。

反垃圾检测条件可运用多种特征检测手段识别垃圾邮件。

### 反欺诈

介绍检测条件中的反欺诈检测条件及其相关知识。

反欺诈检测条件可验证邮件发送者身份是否真实有效，并且通过一系列的邮件头中的发送者比对，发件人策略框架SPF，域名密钥识别邮件#DKIM#和发送者ID分析，检测盗用他人身份或冒名顶替的发送者。

### URL分类

介绍检测条件中的URL分类及其相关知识。

#### URL分类

浏览网页已经是员工日常主要的互联网访问行为。每天都有大量的新增网站以及网页产生，随着大量的社交型网站出现，员工在公工作时间访问这些互联网站点，不仅降低了员工的工作效率，同时也可能会一些潜在的安全隐患，甚至可能会给公司造成信息资产流失等巨大的损失。天空卫士™通过对海量的互联网站点进行静态分类和云端智能分类结合的方式，帮助管理员通过URL分类配置访问策略，从而规范员工的上网行为，将潜在的安全风险拒之门外。

天空卫士™提供业界领先的分类工具和流程，以及人工监控和分类技术，为企业安全管理员提供最精准的，最及时的，和覆盖最完整的URL分类库。

天空卫士™安全鳄®统一内容安全UCS解决方案运用URL分类检测条件，结合系统预置的URL分类库和自定义分类，对用户的网络访问请求中的URL进行分析，并基于分析结果，结合管理员设置的策略，控制用户的访问请求操作。

- URL分类包含预置分类和自定义分类，URL分类匹配的顺序为：自定义优先预置分类。

比如：用户将原本属于搜索引擎分类的 <https://www.baidu.com> 添加到购物分类，那么用户访问 <https://www.baidu.com> 时，就总是属于购物分类，如果策略不允许访问购物分类，那么用户访问 <https://www.baidu.com> 时，就会被阻止。

- 一些URL会属于多个分类（预置URL分类库或者在不同URL分类中添加了一些正则表达式），安全管理员对这些分类均可进行策略匹配。

- 自定义URL支持正则表达式，URL地址。支持在预置分类和自定义分类中添加URL地址、正则表达式，天空卫士™统一内容安全UCS解决方案对这些添加的自定义URL能够保持自动同步。
- URL分类可以划分到不同的URL风险级别和URL风险类别。

### URL风险级别

员工通过网络访问不同的网站或应用时，可能给企业引入不同的风险。天空卫士™借助自身强大的URL分类库，对潜在的风险网站进行了风险级别划分。一方面有助于帮助管理员定制有效的安全访问策略，另一方面管理员可以根据风险级别统计内网用户的上网行为。

风险级别分为以下四个等级：

- 高
- 中
- 低
- 安全

风险级别有2种来源

- 系统预置的风险级别，系统根据现有URL类别库、Cloud App 分类，进行风险级别的划分。
- 管理员也可以根据URL分类、Cloud App 分类重新定义。

命中安全URL扫描：自定义安全URL黑名单、云端安全URL黑名单（如：挂马，篡改网页、钓鱼、恶意软件下载、木马等恶意网址），都归类到高风险级别；

风险级别冲突时的优先原则：当风险级别冲突时，处理原则，就高不就低

比如：用户访问某网站时，预置库里对于该网站定义的风险级别为低，但该访问同时命中了安全URL检测（风险级别为：高），那么最终的日志记录风险级别为高

比如管理员可以对风险级别为“高”的风险URL访问行为进行阻断。

### URL风险类别

在Web安全用户场景中，安全管理员会对不同的URL分类进行风险类别划分，从而方便管理员按照风险类别配置策略或统计员工的上网活动，生成不同的风险类别报告。



- 增强型Web安全网关ASWG预置了6种风险类别，分别为：安全风险、带宽占用、商业用途、法律责任、生产力损失、Web2.0，用户也可以添加自定义的风险类别
- 一个URL分类、Cloud App 分类可以属于不同的风险类别，比如流媒体URL分类，可以属于带宽占用，也可以属于生产力损失
- Web安全策略可以根据风险类别配置，比如安全管理员可以通过预置或自定义的风险类别对带宽占用、生产力损失的URL访问行为进行阻断





应用检测条件


URL分类，URL风险级别和URL风险类别均可被策略引用。

在策略配置页面，点击添加匹配或添加例外，选择URL分类，可应用URL分类检测条件。

所涉及页面包含如下按钮和图标。

图标	解释
URL分类	在该栏下点击  进入URL分类对话框，在系统预置和自定义的数据库中选择需要检测的URL分类。
URL风险级别	在该栏下点击  进入URL风险级别对话框，在高中低三个级别中选择需要检测的风险级别。

图标	解释
URL风险类别	在该栏下点击  进入URL风险类别对话框，在系统预置和自定义的数据库中选择需要检测的风险类别。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。

 注：设置多条URL分类规则时，匹配一条即为命中策略。

## 安全URL分类

介绍检测条件中的安全URL分类及其相关知识。

### 检测条件介绍

为了灵活的控制对URL的安全进行检测（不再默认对安全URL分类访问进行阻断），安全管理员可以通过定义该检测条件对指定类别的安全URL类型进行检测（比如：挂马、网页篡改、钓鱼等类型等），并且结合策略的动作控制员工的网络访问。

是否允许包含安全风险的URL访问，取决于策略的动作，如果动作是阻止，则无法访问，并触发阻断页面。

如URL分类中包含安全分类，比如用户访问购物网站被阻止，同时也被安全URL分类中的“钓鱼”分类命中，那么在阻断页面的URL分类显示为“购物,钓鱼”。

### URL沙箱检测





沙箱用于对可疑文件进行深入分析，提供了对高级持续威胁APT，零日威胁和的额外安全防护。

天空卫士™安全设备通过在虚拟环境中运行并分析这些可疑的文件，以检测恶意行为。

### 检测条件配置

在策略配置页面，点击添加匹配或添加例外，选择安全URL分类，可配置安全URL分类检测条件。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。

## 邮件安全管理

介绍邮件安全管理相关功能。

邮件安全管理相关页面集中位于菜单栏的SEG管理选项下。

通过在这些页面上的操作，管理员可以：


- 管理邮件安全策略
- 管理邮件安全策略元素
- 管理全局控制设置
- 管理PEM设置
- 管理其他邮件安全设置

## 邮件安全策略

介绍邮件安全策略的相关信息。


在SEG管理 > 策略页面管理邮件安全策略。



1. 选择SEG管理 > 策略，进入策略页面。
2. 光标悬空放在添加按钮上，点击新策略选项，进入添加策略页面。

 注：如果你已经定义了策略模板，也可以选择添加 > 通过模板添加基于现有的策略模板添加策略。关于更多策略模板的设置，参阅[策略模板](#)。

3. 输入策略模板名称和描述，表明该策略的作用。
4. 设置来源Risk Level，如果来源Risk Level达到阈值，将使用该策略匹配动作进行拦截保护。

 注：配置前需要开启ITM功能。

5. 设置策略所属的策略等级，即将策略分级，支持30个等级和默认等级，数值越小等级越高，默认等级优先级最低。
  - 一个策略只能属于一个策略等级，一个策略等级可以包含多个策略；策略根据策略等级由高到低进行执行，同一等级下的策略均会被扫描执行；本等级出现策略命中后，不会再扫描执行下一等级策略；本等级没有命中任何策略时，则会继续扫描执行下一等级策略。
  - 系统支持三层分级对象，一层分级对象有权限设置的策略等级为1-30和默认等级；二层分级对象有权限设置的策略等级为10-30和默认等级；三层分级对象有权限设置的策略等级为20-30和默认等级。
6. 选择是否启用该策略。
7. 点击检测内容选项卡，点击添加匹配，在下拉菜单中选择反病毒、反垃圾、反欺诈，URL分类或安全URL分类创建检测内容，也可以自定义检测内容：
  - a) 输入检测内容匹配规则名称和描述，表明其作用。
  - b) 点击 设置匹配条件。
 

 注：反病毒和反垃圾的匹配条件由全局控制，详细配置步骤请参考[检测设置](#)。
  - c) 勾选是否启用URL沙箱检测。  
启用该功能后ASEG会检测邮件里嵌入URL所包含的网页内容，如果发现安全风险则识别为恶链邮件。
  - d) 设置同时匹配条件。点击 为URL分类、安全URL分类和自定义检测内容设置多个同时执行的检测内容，也可选择不添加同时匹配。
  - e) 点击确定，保存检测内容的设置。
8. 点击方向选项卡，选择检测的邮件方向，默认检测入向、出向、内部和开放转发四个邮件方向。
9. 点击来源/目标选项卡。点击添加匹配分别创建新的来源和目标策略。关于更多来源/目标的设置，参阅[来源和目标](#)。
10. 点击动作选项卡，设置策略执行动作，并选择是否启用内容分析功能，启用后对投递的邮件进行DLP检测。
11. 点击保存，新策略添加成功。

## 邮件策略元素

介绍邮件策略元素。

在SEG管理 > 策略元素页面管理邮件安全策略元素。

SEG策略元素作为策略属性用于创建策略，包括来源/目标、策略动作和策略模板。

### 来源和目标

介绍配置来源和目标的步骤。

在SEG管理 > 策略元素 > 来源/目标页面管理邮件安全的来源和目标。

根据用户目录、IP地址或者是Email地址，设置指定的策略源或目标匹配或者例外。

1. 选择SEG管理 > 策略元素 > 来源/目标，点击添加，分别新建来源或目标。
2. 输入策略来源或目标名称和描述，表明其用于检测匹配或例外。
3. 选择类型，指定策略源（发送者），或者策略目标（接收者），根据需要进行配置：e

电子邮件地址	输入发送者的电子邮件地址，多个电子邮件地址以逗号分隔。当类型为目标时，支持将UTF-8编码的CSV格式的文件导入目标电子邮件地址。
IP/IP段	输入发送者/接收者的IP地址或IP段，多个地址以逗号分隔。
用户目录	输入发送者/接收者的IP地址或IP段，多个地址以逗号分隔。

4. 点击保存，新建来源和目标显示在列表中。

表 113: 页面图标和行间操作按钮功能

图标	解释
	编辑来源/目标，可查看来源/目标最后修改时间，创建者信息和策略使用情况。
	删除来源/目标。


### 策略动作

介绍管理策略动作的步骤。

在SEG管理 > 策略元素 > 策略动作页面管理邮件安全的策略动作。

事件命中策略后，对所有协议通道指定不同的动作，这些动作组合称为策略动作。

按照以下步骤添加新的策略动作。

1. 选择SEG管理 > 策略元素 > 策略动作。
  -  提示：初始页面的列表包含了预置的策略动作：放行和隔离。
2. 点击添加，新建策略动作。
3. 输入策略动作名称和描述，表明该策略动作的作用。
4. 从下拉菜单选择动作类型，并对相应类型的参数做设置：

策略动作	解释
阻止	阻断网络传输（对邮件通道无效，邮件通道类似阻止的动作是隔离）。

策略动作	解释
放行	对命中策略后的事件做日志记录，不影响用户访问网络，对所有通道有效。
删除附件	只适用于邮件通道，邮件附件被删除，收件人不会收到附件。
隔离	只适用于邮件通道，隔离的邮件和事件一起被存储到证据文件中，管理员可手动释放或在邮件审核后释放。在隔离条件下，邮件支持不审批、一级审批和二级审批，每一级的审批流程将被管理平台记入事件历史。
内容加密	只适用于邮件通道，命中策略后由SMTP模块加密传输。
第三方加密	只适用于邮件通道，命中策略后发给第三方加密网关加密。

ASEG的各策略动作分别附带了以下邮件通道中的附加策略动作：

动作	邮件功能
放行	<ul style="list-style-type: none"> <li>记录邮件原文</li> <li>添加/修改/删除邮件头</li> <li>邮件投递至指定主机/IP</li> <li>邮件密送至指定邮箱</li> <li>添加邮件声明，即命中该策略以后添加指定的声明信息。</li> <li>发送邮件通知至指定收件人</li> </ul>
删除附件	<ul style="list-style-type: none"> <li>记录邮件原文</li> <li>发送邮件通知至指定收件人</li> </ul>
隔离	<ul style="list-style-type: none"> <li>记录邮件原文</li> <li>邮件密送至指定邮箱</li> <li>发送邮件通知至指定收件人</li> </ul>
内容加密	<ul style="list-style-type: none"> <li>记录邮件原文</li> <li>邮件密送至指定邮箱</li> <li>发送邮件通知至指定收件人</li> </ul>
第三方加密	<ul style="list-style-type: none"> <li>记录邮件原文</li> <li>邮件密送至指定邮箱</li> <li>发送邮件通知至指定收件人</li> </ul>

5. 点击保存，新建策略动作显示在列表中。

### 策略通知



介绍管理策略通知的步骤。

在SEG管理 > 策略元素 > 策略通知页面管理邮件安全的策略通知。


策略通知与策略动作配合使用，在命中策略执行动作的同时来选择是否发送通知。

按照以下步骤添加一个新的策略通知。

1. 选择SEG管理 > 策略元素 > 策略通知。
2. 点击添加，新建策略通知。
3. 输入策略通知名称和描述，表明该策略通知的作用。
4. 设置通知属性。
  - a) 设置策略通知的默认发件人名称。
  - b) 设置策略通知的默认发件人地址。
  - c) 设置邮件服务器。
  - d) 设置收件人。

 提示：可选择收件人为来源，策略所有者，主管或目标地址，也可点击进入选择用户对话框，在组织架构中或用户目录中选择需要的收件人。

- e) 设置邮件格式为HTML或纯文本格式。
5. 设置通知模板。
  - a) 设置通知模板的主题。  
[违规事件：%事件ID%] - %来源%违反数据防泄漏策略
  - b) 设置通知模板的正文。  
您好，%来源%发送的邮件包含敏感内容触发数据防泄漏策略%策略名称%。邮件已被%动作%。
  - c) 勾选是否在通知邮件正文中添加以下内容：
    - 是否显示公司LOGO标志
    - 是否显示公司名称
    - 是否显示对邮件执行的策略动作
    - 是否包含违规的数据原文
    - 是否执行邮件审核，是否允许安全管理员即通过邮件工作流放行或拒绝邮件。

 注：拒绝后系统将发送通知邮件给原发件人，事件动作更新为“已拒绝”，并记录事件历史和审计日志。

    - 是否显示审批历史。
    -

6. 点击保存，将新建的策略通知添加至列表，

### 策略模板


介绍配置策略模板的步骤。

在SEG管理 > 策略元素 > 策略模板页面管理邮件安全的策略模板。

预置模板通过配置策略检测内容匹配项和例外项作为模板。

策略模板可用于快速部署策略，有效避免策略中的错误和信息漏洞。策略模板支持导入和导出功能。

1. 选择SEG管理 > 策略元素 > 策略模板，点击添加，新建策略模板。
2. 输入策略模板名称和描述，以表明该策略模板的作用。
3. 设置来源Risk Level，如果来源Risk Level达到阈值，将使用该策略匹配动作进行拦截保护。


 注：配置前需要开启ITM功能。

4. 设置策略所属的策略等级，即将策略分级，支持30个等级和默认等级，数值越小等级越高，默认等级优先级最低。
  - 一个策略只能属于一个策略等级，一个策略等级可以包含多个策略；策略根据策略等级由高到低进行执行，同一等级下的策略均会被扫描执行；本等级出现策略命中后，不会再扫描执行下一等级策略；本等级没有命中任何策略时，则会继续扫描执行下一等级策略。
  - 系统支持三层分级对象，一层分级对象有权限设置的策略等级为1-30和默认等级；二层分级对象有权限设置的策略等级为10-30和默认等级；三层分级对象有权限设置的策略等级为20-30和默认等级。
5. 选择是否启用该策略。







6. 点击检测内容选项卡，点击添加匹配，在下拉菜单中选择反病毒、反垃圾或URL分类创建检测内容，也可以自定义检测内容：
  - a) 输入检测内容匹配规则名称和描述，表明其作用。
  - b) 设置匹配条件：

 注：

- 反病毒、反垃圾、反欺诈和URL分类的匹配条件由全局控制，详细配置步骤请参考[检测设置](#)。
- 添加自定义检测内容匹配时，点击 添加邮件属性。以下0个规则必须同时匹配是指数据必须匹配N个规则才达到记录事件的条件。

7. 点击保存，新建策略模板显示在列表中。

表 114: 页面图标和行间操作按钮功能

图标	解释
	编辑策略模板，可查看最后修改时间和创建者信息。
	删除策略模板。使用中的策略模板不可以删除。
	导入从其它环境导出的策略模板或者自定义的策略模板文件。
	导出策略模板到本地。
快速添加策略	快速创建策略，跳转至添加策略页面。详细信息请参考 <a href="#">添加新策略</a> 。

## 全局控制

介绍邮件安全中的全局控制配置。

在SEG管理 > 全局控制页面管理邮件安全的全局控制。

邮件安全全局控制主要用来配置SEG的全局白名单功能与全局黑名单功能，支持在特殊情况下放行或阻止指定的邮件发送请求。

 注：



全局黑名单的优先级高于全局白名单，即针对一个用户访问请求，系统会优先处理黑名单，再处理白名单（如果此访问请求没有被黑名单阻止）。

### 白名单

介绍白名单设置的步骤

在SEG管理 > 全局控制 > 白名单页面管理邮件安全的白名单。

邮件安全白名单支持放行指定用户或来源的邮件发送请求。

1. 进入白名单页面。
2. 添加用户白名单。
  - a) 点击 进入选择用户对话框。
  - b) 在用户目录组中选择用户。
  - c) 点击确定添加用户到白名单。
3. 添加来源白名单。
  - a) 点击 进入添加白名单对话框。

- b) 输入来源名称。
- c) 选择来源类型。可选类型包括：

IP/IP段	来源的IP地址或IP段。
邮件地址	来源的邮件地址。
域名	来源的域名。

- d) 输入所选类型的值。
  - e) 点击确定添加来源到白名单。
4. 点击保存，白名单添加成功。


### 黑名单

介绍配置黑名单的步骤。


在SEG管理 > 全局控制 > 黑名单页面管理邮件安全的黑名单。

邮件安全黑名单支持阻断指定用户或来源的邮件发送请求。

1. 选择SEG管理 > 全局控制 > 黑名单，进入黑名单页面。
2. 添加用户黑名单。

- a) 点击  进入选择用户对话框。
- b) 在用户目录组中选择用户。
- c) 点击确定添加用户到黑名单。

3. 添加来源白名单。

- a) 点击  进入添加黑名单对话框。
- b) 输入来源名称。
- c) 选择来源类型。可选类型包括：

IP/IP段	来源的IP地址或IP段。
邮件地址	来源的邮件地址。
域名	来源的域名。

- d) 输入所选类型的值。
  - e) 点击确定添加来源到黑名单。
4. 点击保存，黑名单添加成功。

## PEM管理

介绍PEM管理的相关设置。

在SEG管理 > PEM管理页面管理个人用户邮件设置。

增强型安全邮件网关ASEG会对邮件进行垃圾、病毒、恶链等自定义策略的检测，而个人邮件管理是指允许员工使用自己的邮件地址、密码登录SEG的页面来查看自己被隔离的垃圾、病毒、恶链邮件。

另外当一些员工的邮件被垃圾、病毒、恶链阻止时员工可以在一天的某几个设置的时间点收到通知摘要邮件，以防止有误判的情况影响到正常业务工作。

摘要的内容是一段时间内（可配置）被SEG拦截的邮件列表，员工可以查看这些列表里的邮件有没有误判，可以对这些邮件进行删除、投递、加入白名单、加入黑名单等操作。

### 管理SSL证书

介绍管理邮件安全SSL证书的步骤。

在SEG管理 > PEM管理 > SSL证书页面管理SSL证书设置。

为了防范垃圾和广告邮件及诈骗、钓鱼、勒索病毒邮件等问题，同时为了保障邮件账号的安全以及邮件内容在传输过程中不被非法窃取和篡改，企业邮件服务器通常要求安装SSL安全证书。

天空卫士™安全鳄®增强型安全邮件网关ASEG邮件安全解决方案提供的电子邮件服务器SSL安全证书确保客户端设备到邮件服务器端数据传输为加密方式。

在SSL证书管理页面，您可以完成以下操作。

- 导入证书：点击按钮进入导入证书对话框，导入系统可识别的证书文件，并添加证书密码和私钥。
- 创建证书：点击按钮进入创建证书对话框，输入地理位置和组织架构，并添加证书秘钥。
- 下载证书：点击按钮将创建的SSL证书 - pemmanager.crt 下载到本地。

### PEM基本设置


介绍管理邮件安全基本设置的步骤。

在SEG管理 > PEM管理 > 基本设置页面管理个人邮件设置基本设置。

天空卫士™安全鳄®增强型安全邮件网关ASEG邮件安全解决方案提供了个人邮件基本安全设置选项，用于检测病毒，垃圾邮件和邮件中包含的恶意URL链接。

在基本设置页面，您可以管理以下个人邮件管理的设置。

设置项	介绍
启用状态	点击滑动按钮启用PEM管理系统。
隔离邮件	勾选后，在PEM管理系统或在个人用户的邮件摘要通知里可见所选的隔离邮件类型。默认选中垃圾邮件。
个人对隔离邮件的操作权限	个人用户对隔离邮件可以行使的操作权限包括投递、删除和下载。
PEM管理设置	设置显示于PEM管理系统页面的公司Logo和企业名称。
其他功能设置	<ul style="list-style-type: none"> <li>• 勾选黑名单或白名单后，在PEM管理系统中可见个人黑/白名单操作按钮和页面。</li> <li>• 勾选启用反馈误判邮件后，个人用户可在个人邮件管理列表中对系统分析结果为垃圾的邮件进行反馈误判邮件操作，将邮件反馈至天空卫士™安全运营中心，确保此误判不会再次发生，以免影响正常的业务进展。</li> </ul>

 提示：用户可通过PEM管理平台管理个人邮件，详细信息请参考[PEM管理平台](#)。

### 邮件摘要管理

介绍设置邮件摘要管理的步骤。

在SEG管理 > PEM管理 > 邮件摘要管理页面管理邮件摘要设置。

增强型安全邮件网关ASEG在每天固定时间点发送一封“隔离邮件摘要”，摘要的内容包括被隔离的邮件列表，用户可以根据这个摘要邮件列表来查看是否有误判，并对发件人加入黑名单、加入白名单、放行、删除、误判等操作。


1. 选择PEM管理 > 邮件摘要，进入邮件摘要管理页面。
2. 点击启用状态滑框启用设置。
3. 设置邮件摘要计划。
  - a) 选择发送周期。
  - b) 选择发送时间，点击确定。
4. 设置邮件摘要模板。
  - a) 输入发件人名称。

- b) 输入发件人邮件地址。
  - c) 输入邮件主题。
  - d) 输入尾部声明。
  - e) 输入邮件数量。
5. 设置邮件摘要收件人为所有个人均可收到邮件摘要，或是仅指定人可收到邮件摘要。
  6. 设置PEM管理系统超链接。个人用户在收到邮件通知后，该点击该链接可以跳转到PEM管理平台登录页面。
  7. 点击保存，设置成功。

## PEM管理平台

介绍PEM管理平台的相关信息。

PEM管理平台是个人邮件管理工具，即允许员工使用自己的邮件地址和密码登录平台页面，查看并管理本人由于触发邮件安全策略而被增强型安全邮件网关ASEG隔离的垃圾邮件、病毒邮件和恶链邮件等。如果增强型安全邮件网关ASEG发生误判，员工可以执行继续投递和误判反馈等操作，以保证业务的正常进行。

 注：管理员统一管理PEM管理平台的登录权限，并拥有对所有用户的邮件操作权限。

PEM管理平台以支持下功能操作：

### 登陆管理平台

用户可以通过以下两种方式登录PEM管理系统：

- 点击邮件摘要通知中的查看摘要详情链接跳转到PEM管理平台登录界面。对通知摘要邮件的设置请参考[邮件摘要管理](#)。
- 通过浏览器，输入网页地址<https://UCSS IP址:8448/pemManager/pages/login>前往PEM管理平台登录页面。

输入邮箱和密码，验证成功后，即可登录到PEM管理系统界面。

登录PEM管理平台前可到通过UCSS对其进行基本设置。详细信息请参考[PEM基本设置](#)。

### 切换界面语言

PEM管理平台界面默认为中文（简体）。用户可以点击菜单顶部的下拉框可切换为英文语言。

### 隔离邮件管理


点击左侧菜单栏的个人邮件管理选项卡，显示当前用户所有被隔离的邮件。邮件根据接收时间由上到下排序，并显示邮件ID，发件地址，接收地址，邮件主题，邮件大小和分析结果等信息。

用户可以对隔离的邮件进行如下操作：

- 点击列表中的邮件ID查看邮件原文。
- 点击添加筛选，根据筛选条件显示被隔离的邮件信息。
- 对隔离邮件进行投递、删除、下载添加至黑、白名单等操作。


### 个人黑名单


获得管理员的授权后，按照以下步骤设置个人黑名单。用户将不会收到黑名单中的邮件地址发送来的邮件。

1. 点击左侧菜单栏的个人黑名单选项卡。
2. 点击弹出添加黑名单窗口。
3. 输入邮件地址，点击确定。

## 个人白名单

获得管理员的授权后，按照以下步骤设置个人白名单。白名单中的邮件地址发送来的邮件会绕过垃圾邮件检测。

1. 点击左侧菜单栏的个人白名单选项卡。
2. 点击弹出添加白名单窗口。
3. 输入邮件地址，点击确定。

 注：个人用户的个人黑/白名单功能权限可以由管理员在SEG管理 > PEM管理 > 基本设置页面启用。

## 设置

介绍邮件安全的其他相关设置。

在SEG管理 > 设置页面管理邮件安全相关设置。

本章介绍邮件安全的其他相关设置。

### 检测设置

介绍配置检测设置的步骤。

#### 简介

在SEG管理 > 设置 > 检测设置页面管理邮件安全检测的相关设置。

检测设置支持设置反病毒、反垃圾邮件、URL的全局检测配置，用于配置策略的检测内容。

#### 反病毒设置

- 设置邮件大小检测，当邮件过大时，不做病毒检测。
- 设置压缩层数检测，当附件压缩层数过大时，不做病毒检测。
- 设置收件人病毒提示，输入提示信息并选择提示位置。


#### 反垃圾设置

- 设置邮件大小检测，当邮件过大时，不做反垃圾扫描。
- 选择是否启用垃圾指纹库功能。启用后，SEG基于垃圾邮件的明显特征进行垃圾邮件的识别。
- 选择是否启用启发式垃圾检测。启用后，SEG将基于垃圾邮件的疑似可能性进行垃圾邮件的识别。
- 选择是否启用标记邮件。启用后，SEG将误判和漏判的非垃圾邮件进行标记，并提交给智能分析库学习。
- 选择是否启用域名黑名单#DBL#。启用后，在方框中输入域名黑名单，SEG可以分析用户邮件的RDNS、HELO、Mail From、From、Reply-To、Message-ID、Body里包含的域名是否属于黑名单中的垃圾域名。
- 选择是否启用动态白名单#Dynamic Whitelist#。当发件人与收件人之间的正常邮件通信（不触发防垃圾邮件过滤）达到指定次数之后，该发件人/收件人地址对将被添加到动态白名单。启用后，来自动态白名单中的邮件地址的邮件可绕过垃圾邮箱检测。
- 选择是否启用禁止词汇检测并设置禁止词汇。当邮件的主题或正文中的词汇匹配禁止词汇列表，或正则表达式时，邮件被判定为危险邮件。
- 选择是否启用安全词汇检测并设置安全词汇。当邮件的主题或正文中的词汇匹配安全词汇列表，或正则表达式时，邮件被判定为安全邮件。

#### 内嵌URL检测设置


- 设置URL跳转次数，超过此限制将被识别为恶意链接。同时支持根据邮件大小做检测限制并设置相应的处理动作。
- 选择放行邮件操作，当放行包含内嵌URL的邮件时，可将嵌入的URL链接删除，替换，或忽略。

- 启用URL跳转功能后，每一个跳转URL的页面内容都会进行Web内容安全检测。

 注：以上功能设置完成后，请点击确定按钮，及时保存设置。

### 高级检测

点击页面右上角的高级检测，可进入高级检测配置页面。

 注：高级检测选项推荐使用默认设置，如需修改，请在天空卫士™技术支持人员的帮助下进行，切勿擅自修改。

## 邮件安全监控

介绍邮件安全监控相关信息

邮件监控记录所有通过SMTP MTA组件的邮件日志信息（不包含通过SMTP Proxy的日志），包括邮件日志和邮件连接日志。

### 监控邮件日志


介绍查看邮件日志的步骤。


#### 简介

邮件日志记录SMTP MTA模块从接收邮件至投递邮件整个过程的详细日志。

默认显示最近3天所接收到的邮件日志列表。

在监控 > 邮件监控 > 邮件日志页面管理监控到的实时邮件日志信息。



 提示：页面支持如下操作：

- 点击邮件ID的悬浮图标  可以查看完整的邮件详情信息，包括邮件原文和邮件头信息等。
- 点击分析结果中的命中DLP策略可以查看DLP事件详情。
- 标记邮件-当出现漏判或误判邮件时，管理员可以进行手动标记为垃圾邮件并送至后台分析，或取消标记。这一操作会影响标记正常和标记垃圾的统计数量。

#### 页面介绍

监控页面包含以下快速按钮。

表 115: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

监控页面包含以下操作按钮。


表 116: 按钮功能介绍


按钮	功能
下载	<p>点击按钮下载.eml格式的邮件证据文件到本地。</p> <p> 提示: 支持从各不同增强型安全邮件网关ASEG上下载打包的文件再重新打包后下载, 下载后的文件为zip格式。</p>
投递	<p>点击按钮将邮件直接投递至原收件人。注意以下事项:</p> <ul style="list-style-type: none"> <li>• 支持所有类型的邮件, 不论邮件分析结果、邮件状态如何。</li> <li>• 支持重复投递, 不限次数。</li> <li>• 支持批量操作, 包括已选择邮件和已过滤邮件</li> <li>• 投递的邮件不会经过任何策略扫描</li> <li>• 投递会产生新的邮件日志, 且永远不会包含邮件原文。新的邮件日志将在分析结果字段标记为正常(投递)。</li> </ul>
添加至	<p>点击按钮选择将邮件发件人添加至全局白名单或黑名单。</p> <p> 注: 不适用于数据安全网关DSG和增强型Web安全网关ASWG在邮件转发MTA部署下所产生的邮件日志, 管理平台在没有SEG license授权时隐藏该操作菜单。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件: 直接删除已选项目。</p> <p>删除过滤事件: 标记原因(误报/已解决/不相关)后删除当前页面所有筛选后的项目。</p> <p>注意以下事项:</p> <ul style="list-style-type: none"> <li>• 支持项目的批量删除, 需先选中需要删除的项目。如果删除失败, 则会提示错误信息, 并显示失败的原因。</li> <li>• 支持删除报表中所有的项目。</li> <li>• 删除项目时, 会弹出确认对话框, 其中显示删除项目的数量, 并选择需要删除项目的原因。选择其他原因时, 需要说明具体原因。</li> <li>• 如果事件被成功删除, 存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表, 快速对多条事件进行归类排列, 并呈现柱状图排序。</p>

#### 查看邮件日志详情

介绍查看邮件日志详情的步骤。

在监控 > 邮件监控 > 邮件日志页面查看邮件日志详情。

1. 进入邮件日志页面。
2. 点击  查看邮件日志详情, 显示邮件详情和邮件原文。
3. 按照需要您可选择下载, 投递或删除邮件日志详情。

 注: 邮件详情记录邮件接受方的接收状态和重新投递的状态。若投递失败, 一天内会重新投递, 间隔最长为1小时。邮件原文可作为附件下载到本地。

邮件日志包括以下信息:

表 117: 邮件日志详情

邮件日志详情	解释
邮件ID	发送邮件的ID。
SMTP-ID	邮件唯一标识 ( Postfix系统后台邮件队列里的文件名称, 如 : 2D6B8ADE34)。
Message-ID	邮件头里的Message-ID字段
接受时间	邮件到达UCSG设备的时间
发送IP	发件人IP地址
发件人	发件人邮箱地址
收件人	收件人邮箱地址
抄送	抄送的邮件地址
密送	密送地址
主题	邮件主题
邮件大小	邮件大小 ( B/KB/MB )
附件数量	邮件中包含的附件数量
附件名称及大小	每个附件的名称及大小
发送时间	UCSG发送邮件的时间
设备	处理邮件的UCSG设备主机名
分析结果	邮件扫描结果 ( 正常/垃圾/病毒/恶链邮件/命中DLP策略/异常 )
状态	邮件投递状态 ( 放行/阻止 ( Proxy模式 ) /隔离 ( MTA模式 ) /已释放/失败 )
恶链数量	邮件内包含恶链的数量
恶链分类	邮件内包含恶链对应的URL分类信息

## 邮件日志筛选条件/显示列

筛选条件/显示列	解释
邮件ID	邮件识别号
Message-ID	邮件头里的Message-ID字段
SMTP-ID	邮件唯一标识 ( Postfix系统后台邮件队列里的文件名称, 如 : 2D6B8ADE34 )
接收时间	邮件到达接收设备的时间
发送IP	发件人IP地址
发件人	发件人邮箱地址
收件人	收件人邮箱地址
主题	邮件主题
邮件大小	邮件大小



附件名称	每一个附件的名称
附件数量	邮件里包含的附件数量
状态	邮件投递状态，包括放行、阻止（Proxy模式）、隔离（MTA模式）、已释放、失败等。
检测设备	处理邮件的设备主机名
URL数量	邮件内包含恶意链接的数量
URL分类	邮件内包含恶链对应的URL分类信息
分析结果	邮件扫描结果，包括正常、垃圾、病毒、恶链邮件、命中DLP策略、异常等。
投递者	在UCSS执行投递操作的管理员
投递时间	在UCSS执行投递操作的时间
邮件方向	邮件检测方向为开放转发、内部、出向或内部。
病毒名称	邮件携带的病毒名称
策略名称	邮件触发的策略名称
安全威胁类型	邮件所属的安全威胁类型
来源Risk Level	发件人所属的Risk Level(高危、危险、严重、普通和较低)
响应码	记录在邮件日志中的错误代码
TLS	是否启用了TLS
真实源IP	真实的发件人IP地址
标记状态	邮件被标记为正常邮件或垃圾邮件

## 监控邮件连接日志

介绍查看邮件连接日志的步骤。

### 简介

邮件连接日志记录SMTP MTA模块收到的源IP发起的邮件连接日志，包含连接成功和连接失败的日志信息。

在监控 > 邮件监控 > 邮件连接日志页面管理监控到的实时邮件连接日志信息。

在监控 > 邮件监控 > 邮件连接日志页面查看邮件连接日志。

点击邮件IP地址，可跳转至此IP发送的相同时间点的邮件日志页面。

### 页面介绍

监控页面包含以下快速按钮。

表 118: 快速按钮功能介绍

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

监控页面包含以下操作按钮。

表 119: 按钮功能介绍

按钮	功能
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的项目。</li> <li>删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

## 创建定时任务报告

### 如何创建定时任务报告

管理员可以定制任务报告，定期将其以邮件形式发送给指定的收件人。定制内容包括，报告类型（网络事件报告，数据发现报告，综合邮件报告等）、报告类型（列表，图标，趋势）和选择现有的报告等。

以下步骤描述了如何创建一个定时任务报告：

1. 选择报告 > 报告类型，在某一报告类型页面，比如 DLP 报告 网络事件报告页面，点击右上角 定时任务报告链接。进入定时任务报告页面。
2. 点击添加按钮进入定时任务报告页面。
3. 输入名称和描述信息。
4. 在发送报告选项行，点击请选择图标，在弹出的选项框，选择报告的分类，类型等信息。点击保存。
5. 选择以什么文档格式发送报告，目前有 PDF 和 Excel 格式。
6. 勾选启用。
7. 在邮件设置部分设置邮箱相关信息。
8. 在任务定时计划部分设置执行周期。
9. 点击保存。

## 邮件安全报告

介绍邮件安全报告相关信息。

邮件报告包括综合邮件报告、入向邮件报告和出向邮件报告。

邮件报告统计接收和发送的邮件详情用于分析和预测风险，包括相应的邮件 ID、收/发件人、恶链数量和恶链类型等信息。

邮件安全报告包括：

- 综合邮件报告
- 入向邮件报告
- 出向邮件报告
- 连接日志报告

## 综合邮件报告

介绍综合邮件报告的相关设置。

### 简介

邮件报告统计接收和发送的邮件详情用于分析和预测风险。

综合邮件报告包括相应的邮件ID、收/发件人、恶链数量和恶链类型等信息。

在报告 > 邮件报告 > 综合邮件报告页面管理综合邮件报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 页面图标

报告列表页面包含以下操作按钮。

表 120: 页面图标功能介绍



图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

报告页面包含以下快速按钮。

表 121: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

报告页面包含以下操作按钮。

表 122: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载.eml格式的邮件证据文件到本地。</p> <p> 提示：支持从各不同增强型安全邮件网关ASEG上下载打包的文件再重新打包后下载，下载后的文件为zip格式。</p>
投递	<p>点击按钮将邮件直接投递至原收件人。注意以下事项：</p> <ul style="list-style-type: none"> <li>支持所有类型的邮件，不论邮件分析结果、邮件状态如何。</li> <li>支持重复投递，不限次数。</li> <li>支持批量操作，包括已选择邮件和已过滤邮件</li> <li>投递的邮件不会经过任何策略扫描</li> <li>投递会产生新的邮件日志，且永远不会包含邮件原文。新的邮件日志将在分析结果字段标记为正常（投递）。</li> </ul>
添加至	<p>点击按钮选择将邮件发件人添加至全局白名单或黑名单。</p> <p> 注：不适用于数据安全网关DSG和增强型Web安全网关ASWG在邮件转发MTA部署下所产生的邮件日志，管理平台在没有SEG license授权时隐藏该操作菜单。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的项目。</li> <li>删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

## 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示报告支持的类型和对应解释。

表 123: 综合邮件图表报告类型

报告类型	解释
邮件大小排名	统计某段时间每天发送和接收的邮件字节数，并排名前N位（最多30名）。
邮件数量排名	统计某段时间每天发送和接收的邮件数量，并排名前N位（最多30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。

表 124: 综合邮件趋势报告类型

报告类型	解释
邮件大小趋势	统计某段时间每天接收和发送的邮件字节数，并形成趋势图。
邮件数量趋势	统计某段时间每天接收和发送的邮件数量，并形成趋势图。
全部属性	统计以上全部属性的趋势信息。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 邮件报告筛选条件/显示列

介绍邮件安全报告的筛选条件/显示列。

下表罗列了邮件安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
邮件ID	邮件识别号
Message-ID	邮件头里的Message-ID字段
SMTP-ID	邮件唯一标识（Postfix系统后台邮件队列里的文件名称，如：2D6B8ADE34）
接收时间	邮件到达接收设备的时间
发送IP	发件人IP地址
发件人	发件人邮箱地址
收件人	收件人邮箱地址
主题	邮件主题
邮件大小	邮件大小
附件名称	每一个附件的名称
附件数量	邮件里包含的附件数量

状态	邮件投递状态，包括放行、阻止（Proxy模式）、隔离（MTA模式）、已释放、失败等
检测设备	处理邮件的设备主机名
恶链数量	邮件内包含恶意链接的数量
恶链类型	邮件内包含恶链对应的URL分类信息
分析结果	邮件扫描结果，包括正常、垃圾、病毒、恶链邮件、命中DLP策略、异常等。
投递者	在UCSS执行投递操作的管理员
投递时间	在UCSS执行投递操作的时间
邮件方向	邮件检测方向为开放转发、内部、出向或内部。
病毒名称	邮件携带的病毒名称
策略名称	邮件触发的策略名称
安全威胁类型	邮件所属的安全威胁类型
来源Risk Level	发件人所属的Risk Level(高危、危险、严重、普通和较低)
响应码	显示SEG返回给发件方的代码，即代表连接成功或失败的response code（响应码）
TLS	显示该连接是否使用了TLS加密
标记状态	显示邮件的标记状态

## 入向邮件报告

介绍入向邮件报告的相关信息。

### 简介

入向邮件报告统计所有入向邮件的信息并生成报告。

入向邮件报告包括收发件人、接收时间、检测设备和恶链类型等信息。入向邮件报告类型包括列表类、图表类和趋势类。

在报告 > 邮件报告 > 入向邮件报告页面管理入向邮件报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 页面图标

报告列表页面包含以下操作按钮。

表 125: 页面图标功能介绍



图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。


报告页面包含以下快速按钮。


表 126: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

报告页面包含以下操作按钮。

表 127: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载.eml格式的邮件证据文件到本地。</p> <p> 提示: 支持从各不同增强型安全邮件网关ASEG上下载打包的文件再重新打包后下载，下载后的文件为zip格式。</p>
投递	<p>点击按钮将邮件直接投递至原收件人。注意以下事项：</p> <ul style="list-style-type: none"> <li>支持所有类型的邮件，不论邮件分析结果、邮件状态如何。</li> <li>支持重复投递，不限次数。</li> <li>支持批量操作，包括已选择邮件和已过滤邮件</li> <li>投递的邮件不会经过任何策略扫描</li> <li>投递会产生新的邮件日志，且永远不会包含邮件原文。新的邮件日志将在分析结果字段标记为正常（投递）。</li> </ul>

按钮	功能
添加至	<p>点击按钮选择将邮件发件人添加至全局白名单或黑名单。</p> <p> 注：不适用于数据安全网关DSG和增强型Web安全网关ASWG在邮件转发MTA部署下所产生的邮件日志，管理平台在没有SEG license授权时隐藏该操作菜单。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的项目。</li> <li>删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示报告支持的类型和对应解释。

表 128: 入向邮件图表报告类型

报告类型	解释
外部来源发送邮件数量排名	统计发送恶链邮件数量最多的外部来源，并排名前N位（最多30名）。
外部来源发送邮件大小排名	统计发送邮件数量最多的外部来源，并排名前N位（最多30名）。
内部收件人接收邮件数量排名	统计内部收件人接收邮件数量，并排名前N位（最多30名）。
内部收件人接收邮件大小排名	统计内部收件人接收邮件字节数，并排名前N位（最多30名）。
内部域名接收邮件数量排名	统计内部域名接收邮件数量，并排名前N位（最多30名）。
内部域名接收邮件大小排名	统计内部域名接收邮件字节数，并排名前N位（最多30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。



表 129: 入向邮件趋势报告类型

报告类型	解释
邮件大小趋势	统计某段时间每天接收和发送的邮件字节数并形成趋势图。
邮件数量趋势	统计某段时间每天接收和发送的邮件数量并形成趋势图。
全部属性	统计以上全部属性的趋势信息。

#### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

#### 邮件报告筛选条件/显示列

介绍邮件安全报告的筛选条件/显示列。

下表罗列了邮件安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
邮件ID	邮件识别号
Message-ID	邮件头里的Message-ID字段
SMTP-ID	邮件唯一标识 ( Postfix系统后台邮件队列里的文件名称，如：2D6B8ADE34)
接收时间	邮件到达接收设备的时间
发送IP	发件人IP地址
发件人	发件人邮箱地址
收件人	收件人邮箱地址
主题	邮件主题
邮件大小	邮件大小
附件名称	每一个附件的名称
附件数量	邮件里包含的附件数量
状态	邮件投递状态，包括放行、阻止 ( Proxy模式 )、隔离 ( MTA模式 )、已释放、失败等
检测设备	处理邮件的设备主机名
恶链数量	邮件内包含恶意链接的数量
恶链类型	邮件内包含恶链对应的URL分类信息
分析结果	邮件扫描结果，包括正常、垃圾、病毒、恶链邮件、命中DLP策略、异常等。
投递者	在UCSS执行投递操作的管理人员
投递时间	在UCSS执行投递操作的时间
邮件方向	邮件检测方向为开放转发、内部、出向或内部。

病毒名称	邮件携带的病毒名称
策略名称	邮件触发的策略名称
安全威胁类型	邮件所属的安全威胁类型
来源Risk Level	发件人所属的Risk Level(高危、危险、严重、普通和较低)
响应码	显示SEG返回给发件方的代码，即代表连接成功或失败的response code ( 响应码 )
TLS	显示该连接是否使用了TLS加密
标记状态	显示邮件的标记状态

## 出向邮件报告

介绍出向邮件报告的相关信息。

### 简介

出向邮件报告统计所有出向邮件的信息并生成报告。

出向邮件报告包括收发件人、接收时间、检测设备和恶链类型等信息。出向邮件报告类型包括列表类、图表类和趋势类

在报告 > 邮件报告 > 出向邮件报告页面管理出向邮件报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 页面图标

报告列表页面包含以下操作按钮。

表 130: 页面图标功能介绍



图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

报告页面包含以下快速按钮。

表 131: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

报告页面包含以下操作按钮。

表 132: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载 .eml 格式的邮件证据文件到本地。</p> <p> 提示: 支持从各不同增强型安全邮件网关 ASEG 上下载打包的文件再重新打包后下载，下载后的文件为 zip 格式。</p>
投递	<p>点击按钮将邮件直接投递至原收件人。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 支持所有类型的邮件，不论邮件分析结果、邮件状态如何。</li> <li>• 支持重复投递，不限次数。</li> <li>• 支持批量操作，包括已选择邮件和已过滤邮件</li> <li>• 投递的邮件不会经过任何策略扫描</li> <li>• 投递会产生新的邮件日志，且永远不会包含邮件原文。新的邮件日志将在分析结果字段标记为正常（投递）。</li> </ul>
添加至	<p>点击按钮选择将邮件发件人添加至全局白名单或黑名单。</p> <p> 注: 不适用于数据安全网关 DSG 和增强型 Web 安全网关 ASWG 在邮件转发 MTA 部署下所产生的邮件日志，管理平台在没有 SEG license 授权时隐藏该操作菜单。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>• 支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>• 支持删除报表中所有的项目。</li> <li>• 删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>• 如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>

按钮	功能
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示报告支持的类型和对应解释。

表 133: 图表报告类型

报告类型	解释
内部来源发送邮件数量排名	统计发送恶链邮件数量最多的内部来源，并排名前N位（最多30名）。
内部来源发送邮件大小排名	统计发送邮件数量最多的内部来源，并排名前N位（最多30名）。
外部邮箱接收邮件数量排名	统计内部收件人接收邮件数量，并排名前N位（最多30名）。
外部邮箱接收邮件大小排名	统计内部收件人接收邮件字节数，并排名前N位（最多30名）。
外部域名接收邮件数量排名	统计内部域名接收邮件数量，并排名前N位（最多30名）。
外部域名接收邮件大小排名	统计内部域名接收邮件字节数，并排名前N位（最多30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。

表 134: 趋势报告类型

报告类型	解释
邮件大小趋势	统计某段时间每天接收和发送的邮件字节数并形成趋势图。
邮件数量趋势	统计某段时间每天接收和发送的邮件数量并形成趋势图。
全部属性	统计以上全部属性的趋势信息。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 邮件报告筛选条件/显示列

介绍邮件安全报告的筛选条件/显示列。

下表罗列了邮件安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
邮件ID	邮件识别号
Message-ID	邮件头里的Message-ID字段
SMTP-ID	邮件唯一标识 ( Postfix系统后台邮件队列里的文件名称 , 如 : 2D6B8ADE34)
接收时间	邮件到达接收设备的时间
发送IP	发件人IP地址
发件人	发件人邮箱地址
收件人	收件人邮箱地址
主题	邮件主题
邮件大小	邮件大小
附件名称	每一个附件的名称
附件数量	邮件里包含的附件数量
状态	邮件投递状态 , 包括放行、阻止 ( Proxy模式 )、隔离 ( MTA模式 )、已释放、失败等
检测设备	处理邮件的设备主机名
恶链数量	邮件内包含恶意链接的数量
恶链类型	邮件内包含恶链对应的URL分类信息
分析结果	邮件扫描结果 , 包括正常、垃圾、病毒、恶链邮件、命中DLP策略、异常等。
投递者	在UCSS执行投递操作的管理员
投递时间	在UCSS执行投递操作的时间
邮件方向	邮件检测方向为开放转发、内部、出向或内部。
病毒名称	邮件携带的病毒名称
策略名称	邮件触发的策略名称
安全威胁类型	邮件所属的安全威胁类型
来源Risk Level	发件人所属的Risk Level(高危、危险、严重、普通和较低 )
响应码	显示SEG返回给发件方的代码 , 即代表连接成功或失败的response code ( 响应码 )
TLS	显示该连接是否使用了TLS加密
标记状态	显示邮件的标记状态

## 连接日志报告

介绍连接日志报告的相关信息。

### 简介

连接日志可以记录发送方IP的发起SMTP连接 , 并显示连接的成功或失败结果。而且针对连接失败的情况 , 例如由于连接控制被阻断 , 需要记录是什么原因引起的连接失败。

连接日志报告统计所有邮件连接并生成报告。

连接日志报告包括收发送IP、连接时间、连接结果和连接内邮件数量等信息。连接日志报告类型包括列表类、图表类和趋势类。

在报告 > 邮件报告 > 连接日志报告页面管理出向邮件报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 页面图标

报告列表页面包含以下操作按钮。

表 135: 页面图标功能介绍

图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

报告页面包含以下快速按钮。

表 136: 快速按钮功能介绍

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

报告页面包含以下操作按钮。

表 137: 报告按钮

按钮	
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的项目。</li> <li>删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示报告支持的类型和对应解释。

表 138: 图表报告类型

报告类型	解释
连接数量排名	统计邮件连接日志记录的发送连接请求数量最多的来源，并排名前N位（最多30名）。
连接结果排名	统计邮件连接日志记录的收到连接结果最多的来源，并排名前N位（最多30名）。
响应码排名	统计邮件连接日志记录的收到响应码最多的来源，并排名前N位（最多30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。

表 139: 趋势报告类型

报告类型	解释
连接数量趋势	统计某段时间每天发送的连接请求数量，并形成趋势图。
连接结果趋势	统计某段时间每天收到的连接结果反馈数量，并形成趋势图。

报告类型	解释
全部属性	统计以上全部属性的趋势信息。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 连接报告筛选条件/显示列

介绍连接日志报告的筛选条件/显示列。

下表罗列了连接日志报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
发送IP	发件人IP地址
连接内邮件数量	显示该连接内发送的邮件总数
响应码	显示SEG返回给发件方的代码，即代表连接成功或失败的response code ( 响应码 )
详情	SEG返回给发件方的响应详情信息
TLS	显示该连接是否使用了TLS加密
设备名称	显示连接至SEG/DSG/ASWG设备的主机名

## 邮件安全设备监控

介绍如何监控您的邮件安全设备。

在[监控](#) > 设备监控页面实时监控邮件安全设备。

ASEG设备监控信息包括系统资源和服务状态，并支持三种数据统计时段（1小时/24小时/7天）。

表 140: ASEG系统资源信息

设备信息统计	解释
设备基本信息	统计当前设备的基本信息，如主机名称、IP地址、系统类型、CPU、物理内存、硬盘容量和网卡数量等。
CPU资源利用率	统计当前设备CPU使用率，包括用户占用、系统占用和空闲的CPU的比例。
网卡资源利用率	统计当前网卡的发送和接收速率，以及总速率。
内存资源利用率	统计当前内存用于系统及应用、缓存的使用情况。
硬盘资源使用情况	统计系统硬盘和数据硬盘的使用情况。



表 141: ASEG服务状态信息

服务状态	解释
设备版本信息对比	当前UCSS作为基准设备，将注册设备各功能模块的版本信息与基准设备版本信息同步。
队列状态统计	统计邮件队列中分别处于待处理，处理中，投递中和延迟等各种队列状态下的邮件数量。
邮件数量统计	统计各种情况下的邮件数量，包括出向和入向的邮件数量，内部和开放转发的邮件数量，以及总的邮件数量。
邮件流量统计	统计各种情况下的邮件流量，包括出向和入向的邮件流量，内部和开放转发的邮件流量，以及总的邮件流量。

## 邮件安全设备管理

### 设备

配置设备相关的选项页面。

该菜单包含设备相关的选项页面。

#### 系统信息

介绍设备的系统信息界面。

系统信息包括设备的基本信息和服务状态信息。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 系统信息菜单。

系统信息页面支持查看以下信息。

#### 设备信息

设备信息包括主机名称，IP地址，系统类型等只读的信息。

在此栏中，可以一键重启或关闭设备。

#### 系统信息

系统信息包括系统负载状态和各种系统服务的运行状态。

参考[系统服务介绍](#)，可以获得各种系统服务的基本介绍。

在此栏中，可以选择对某项服务进行重启、停止或启动，或对所有服务进行批量操作。

#### 邮件安全基本设置

介绍配置邮件安全基本设置的步骤。

在系统 > 设备管理页面进行邮件安全的基本设置。

邮件安全基本设置包括设备安全模式和同步设置。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 基本设置页面。
2. 选择是否启用设备（默认开启），对设备进行基本配置。
3. 输入设备名称和描述，说明其用途。
4. 设置设备工作模式为旁路监控模式或邮件网关模式。

参考[邮件安全部署介绍](#)获取更多信息。


### 5. 设置不同安全级别下的引擎安全模式。

即出错或超时的情况下，是否需要放行邮件。具体设置包括：

- 反病毒引擎超时或出现错误的情况下是否需要放行邮件。
- 安全策略引擎CAE引擎超时或出现错误的情况下是否需要放行邮件。
- 增强型安全邮件网关ASEG策略引擎分析超时的情况下是否需要放行邮件。

### 6. 选择手动或自动设置时间，自动从配置的时间服务器同步时间，需输入时间服务器域名。

### 7. 点击保存，设置生效。

 注：高级设置请务必在在天空卫士™技术支持工程师的指导下修改。

## 授权许可

介绍如何管理设备的授权许可设置。

在系统 > 设备管理页面进行设备授权许可。

1. 选择系统 > 设备管理进入设备管理页面。点击要查看的设备，进入设备 > 授权许可页面。
2. 选择以下授权方式：


项目	描述
授权码	在线授权需输入授权码。
授权文件	离线授权需上传授权文件。

授权成功后，在当前页面显示授权信息如下：

表 142: 当前授权状态

设备编号	显示当前设备编号
授权号	显示当前设备所使用的授权号。
用户名称	显示License授予时的用户名称，一般为企业名称。
工作模式	显示当前设备工作模式，支持阻断和审计。
授权类型	显示授权类型，包括正式版本和测试版本。
功能模块列表	显示授权的功能模块，每个功能模块的已授权数量，当前状态和使用的有效期。

### 3. 点击保存，设置生效。

 提示：点击下载设备ID可下载设备ID信息为记事本格式，查询和授权License时可以使用该文件。

## 网络

配置网络相关的选项页面。


该菜单包含网络相关的选项页面。




### 网卡配置

在系统 > 设备管理页面配置AESG网卡。

ASEG设备的网卡包括Mgmt负责管理设备，MTA提供邮件服务。

### 1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 网络 > 网卡配置页面。


2. 在网卡信息显示列表，光标悬停在Mgmt网卡文字上，点击  图标查看Mgmt网卡的配置信息。Mgmt网卡不可编辑。

- 光标悬停在MTA网卡文字上，点击图标编辑MTA网卡设置。可更改网卡的IP地址、子网掩码和适配模式。
- 点击确定，网卡设置完成。
- 选择设备网卡并输入网卡的默认网关。
- 输入DNS服务器IP，点击添加于列表；点击删除列表中所选的DNS服务器。
- 设置重定向主机，将需要重定向的URL（如认证页面、证书验证页面、策略的提示和计时页面）中的主机名/IP重定向到指定主机名/IP（请确保主机名可以被DNS解析）。
- 点击保存，设置生效。

### 路由设置

介绍管理路由设置的步骤。




在系统 > 设备管理页面设置路由。

- 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 网络 > 路由页面。
- 点击添加静态路由或策略路由：

静态路由	添加静态路由到主路由表中，不对源IP做限制，所有从本设备发起或者转发的数据包都将遵循此路由规则。
策略路由	只有本设备发起的数据包匹配此规则。

- 输入目标网络IP地址、子掩码和网关（网关需要跟选中网卡的地址在同一个子网内）。
- 选择网卡类型：Mgmt负责管理设备，MTA提供邮件服务，P1和P2提供代理服务（仅ASWG设备），Br0提供桥接服务（仅UCSG-DSG设备）。
- 点击确认，添加路由到列表中。
- 点击保存，设置生效。

表 143: 页面图标和行间操作按钮功能

	导出路由配置。
	导入路由配置。
	删除所选路由。

### 网卡绑定

介绍网卡绑定设置的步骤。

在系统 > 设备管理页面设置网卡绑定。

网卡绑定功能将两个或者更多的物理网卡绑定成一个虚拟网卡以提供负载均衡或者冗余。

- 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 网络 > 网卡配置页面，选择要绑定的网卡，滑动状态条开启网卡绑定。
- 选择绑定网卡的工作模式：

Active-Standby模式	主备方式，当一个网卡故障时另一个网卡接管所有工作。
Active-Active模式	双活方式，两个网卡同时工作，增加带宽的同时实现冗余。需要交换机支持聚合功能。

➔ 注意：Bypass网卡仅支持Active-Active模式。

3. 点击保存，网卡绑定生效。

## 功能


配置功能相关的选项页面。

该菜单包含功能相关的选项页面。


### SMTP协议

介绍配置SMTP协议设置的步骤。

在系统 > 设备管理页面设置SMTP协议。

1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 功能 > SMTP协议页面，编辑SMTP协议。
2. 点击基本选项卡，开启或关闭协议分析。开启后后进行如下配置：
  - a) 选中启用全邮件记录。开启后可记录全部邮件原文。
  - b) 设置FQDN信息。  
安全管理员可按照需要自定义FQDN信息。
  - c) 设置SMTP欢迎信息。
  - d) 输入受信IP地址和子网掩码，点击  添加为受信地址，MTA只接受此列表中来源发起的SMTP连接。
  - e) 开启高级路由，设置SMTP邮件投递路由规则。配置路由时可以设置优先级，如果同一个域名定义了多个邮件路由而对应多个服务器IP地址，系统会尝试按照路由的优先级来发送邮件。当多条路由的优先级相同时，系统会使用轮询发送机制。
  - f) 指定投递邮件的下一跳，可以选择DNS解析投递也可设置指定接收地址。如果开启高级邮件路由，则高级路由中配置的投递地址优先级最高。
  - g) 选择TLS传输安全机制：


强制明文	强制使用明文，如果对方不支持明文，邮件将不能完成投递。
自适应	优先使用TLS，如果对方支持TLS，则使用TLS进行投递，否则使用非TLS进行投递。
强制TLS	强制使用TLS，如果对方不支持TLS，邮件将不能完成投递。

- h) 选择是否发送邮件退信，可选择退信收件人为源发件人或指定收件人。
  - i) 设置加密邮件的网关的主机名/IP和端口号。支持设置加密标识，主题加密标识用户可见，X-Header加密标识用于服务器解析。
3. 点击内部域名选项卡：
    - a) 输入公司内部域名，用来区分邮件方向，点击  添加。
  4. 点击保存，设置生效。


### TCP代理协议

介绍配置TCP代理协议的步骤。

ASEG通过TCP代理协议，将客户端发过来的POP3、IMAP和自定义协议的数据透传给内部的邮件服务器，进行邮件同步。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > TCP代理协议页面。
2. 点击  按钮添加POP3、IMAP或者自定义协议。
3. 输入协议名称。
4. 滑动状态条，可以开启代理协议功能。开启后，继续进行如下配置步骤。
5. 输入协议的端口号。

协议名称	端口号
POP3	默认110
IMAP	默认143
自定义协议	默认为空

6. 输入内部邮件服务器IP地址，点击  按钮添加到IP列表。
7. 点击保存，设置生效。

### 接收和发送

介绍配置接收和发送功能的步骤。

在系统 > 设备管理页面设置接收和发送功能。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 接收/发送页面。
2. 选择连接控制选项卡，选择以下功能项进行设置：

- 连接控制

参数	解释
单个IP并发	设置SEG服务器允许的单个IP最大并发连接数。
连接超时时间	设置SEG服务器连接断开之前允许的最大空闲时长。

- RBL实时黑名单

参数	解释
启用状态	勾选复选框可以启用实时黑名单功能。
RBL服务器	设置RBL服务器，用于识别拦截第三方发布的已知垃圾邮件。

- 动态白名单

参数	解释
启用状态	勾选复选框可以启用动态白名单功能，名单中的邮件地址将绕过垃圾邮件检测。
邮件交换次数	指定将发件人/收件人无垃圾邮件的交换次数。
超时时间	设置超时时间。当名单中的发件人/收件人在指定的时间范围内没有邮件收发时，将被自动移除。

- 信誉检测

参数	解释
启用状态	勾选复选框可以启用信誉检测功能，拦截信誉风险程度较高的垃圾邮件。
信誉阻断设置	设置信誉阈值，超过该阈值的邮件将被阻断。

- 反向域名解析

参数	解释
启用状态	勾选复选框可以启用反向域名解析功能，识别发送方是否来自合法的域。
断开连接设置	选择触发断开连接的条件。

- RMX接收验证

参数	解释
启用状态	勾选复选框可以启用RMX接收验证功能，识别发送方是否带有合法的MX记录，是否伪造域名。

- 灰名单

参数	解释
启用状态	勾选复选框可以启用灰名单功能，拦截可疑的垃圾邮件。
生存周期	指定动态灰名单的生存周期。
延迟间隔	设置触发灰名单生效的最大延迟时间。


- SPF检测

参数	解释
启用状态	勾选复选框可以启用SPF检测功能，拦截通过伪造域名发送的垃圾邮件。
拒接邮件设置	选择触发拒接邮件的条件。

- DKIM域名密钥识别邮件

参数	解释
启用状态	勾选复选框可以启用DKIM域名密钥识别邮件功能，拦截诈骗类垃圾邮件。

- DMARC验证

参数	解释
启用状态	勾选复选框可以启用DMARC验证功能，拦截诈骗钓鱼类垃圾邮件。  注：DMARC功能在DKIM域名密钥识别邮件和SPF检测功能同时启用后才生效。

- SMTP问候延迟

参数	解释
启用状态	勾选复选框可以启用SMTP问候延迟功能，拦截短时间内发送大量垃圾邮件的邮件源。
延迟间隔	设置延迟间隔，如果在此间隔内，客户端频繁发送数据，则会断开连接。

- 目录攻击控制

参数	解释
启用状态	勾选复选框可以启用目录攻击控制功能，防范垃圾邮件发送者通过用电子邮件轰炸方式来获取合法电子邮件地址的行为。
统计间隔	设置目录攻击的间隔时间段，并设置满足触发目录攻击控制的最大邮件数量或连接数量。
阻断目录攻击IP总时长	勾选复选框后，设置当以上条件都满足时，阻断目录攻击IP总时长。

3. 选择邮件控制选项卡，选择以下功能项进行设置：


- 邮件控制：设置邮件大小，收件人数量，连接数据大小等参数用以控制SEG邮件转发。
- 反弹地址标记验证

参数	解释
启用状态	勾选复选框可以启用反弹地址标记验证功能，识别反弹邮件地址的合法性。
BATV检测例外	输入接收或发送方的发件人IP/IP段，将不做BATV检测。

- 内部发件人验证

参数	解释
启用状态	勾选复选框可以启用内部发件人验证功能，识别发件人账号和认证账号一致性。

4. 选择例外选项卡，选择以下功能项进行设置：

- 点击  按钮，添加例外的IP或IP段。
  - 点击保存，添加例外成功。
- 列表中的IP/IP段将绕过以下连接限制功能：

- 并发连接控制
- 灰名单
- SPF检测
- 延迟响应
- 实时黑名单
- 反向域名解析
- 目录攻击控制
- BATV验证
- DKIM验证
- DMARC验证







注：以上连接控制、邮件控制和例外选项卡中的功能项设置完成后，请及时点击保存按钮，保存并应用相应的设置。

### 真实源IP



介绍配置真实源IP功能的步骤。


真实源 IP 检测 ( Original Source IP ) 使用邮件头信息和到达增强型安全邮件网关 ASEG 设备的网络活跃点数来确定网络外围第一个发件人的 IP 地址。此功能可以识别真实的发件人 IP 地址，即使该邮件经过了 NAT 或是多重 MTA 转发以后也可以识别真实的发件人 IP 地址，并且该真实 IP 地址可以应用于 RBL、全局黑名单等连接状态 IP 层的控制。

页面包含以下图标和操作按钮。

图标按钮	解释
	点击按钮添加项目
	点击按钮启用规则
	点击按钮禁用规则
	点击按钮删除选中的规则
调整优先级	点击按钮进入规则列表，并在列表中调整规则的优先级，排在顶部的规则优先处理。

页面包含以下配置项。


配置项	说明
名称	规则名称
启用状态	是否启用规则
直连网关	与增强型安全邮件网关ASEG设备直连的网关设备的IP地址。  注：直连网关与增强型安全邮件网关ASEG设备之间的跳数固定为1。
边界网关	增强型安全邮件网关ASEG设备途径的网关设备的IP地址。  注：边界网关与ASEG之间的跳转次数由安全管理员自行设置，范围是2-32。不同边界网关的跳转次数可以重复，相同边界网关的跳转次数不能相同，建议设置的过程中按跳转次数排序。

 注：直连网关和边界网关的IP地址不能相同。

### 流量整形规则

介绍设置流量整形规则的步骤。

流量整形控制基于域、组或用户目录对邮件传输数量进行限制，以防止其触犯黑名单规则。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 流量整形规则页面。
2. 点击  按钮添加流量整形规则。
3. 输入规则名称。
4. 选择是否启用该规则（启用后继续进行以下设置）。
5. 选择流量整形参数选项卡，设置如下邮件发送限制：
  - 最大并发连接数：ASEG向某一个目标服务器发送的最大并发连接数。
  - 每个连接限制：指定时间段内一个连接的最大邮件数量。
  - 每封邮件的最大收件人数量：如果邮件数量超过阈值则分批发送。
6. 选择来源选项卡，选择全部邮件来源或指定邮件来源。

ASEG支持配置以下参数用于对指定来源的发件人或域名发送的邮件频率进行控制。

- 邮件地址
- 域名
- 用户目录



## 7. 选择目标选项卡，选择全部邮件目标或指定邮件目标。

ASEG支持配置以下参数用于对指定来源的发件人或域名发送的邮件频率进行控制。




- 邮件地址
- 域名
- 用户目录

 注:

- 只有同时命中了来源和目标后，流量整形参数的设置才能生效。
- 支持来源与目标与的关系设置，比如user1@company1.com发给user2@company2.com的邮件频率需要控制。
- 流量整形的匹配顺序按照规则的优先级匹配。

## 8. 点击确定，新建规则添加到列表。

在主页面，对列表中的规则可执行如下操作：

- 点击全局设置按钮，选择是否启用 SMTP 会话缓存以减少SEG同目标服务器之间的连接次数。启用后配置如下参数：
  - 连接重用次数：指定SMTP会话在关闭之前可能被重用的次数。
  - 连接重用总时长：指定 SMTP会话连接被重复使用总时长。
- 点击调整优先级按钮，设置规则匹配的优先级。
- 点击悬浮图标  编辑所选规则。
- 点击  按钮运行所选规则。
- 点击  按钮停止运行所选规则。

### 邮件地址改写功能设置


介绍邮件地址改写功能设置的步骤。

增强型安全邮件网关ASEG支持改写邮件的信封收件人地址，将邮件传送重定向至其他地址；也可以改写信封发件人和邮件头地址，从而向邮件收件人隐藏邮件地址详细信息。


该功能可应用于以下场景。

- 安全管理员期望隐藏真实邮箱。
- 安全管理员期望在一个邮箱中查看写给多个收件人的邮件。
- 当有多个邮件域名的情况下，安全管理员期望终端用户维护一个邮箱地址即可。

### 发件人改写规则

1. 选择发件人改写规则选项卡，点击  进入添加页面。
2. 输入规则名称，表明规则的用途。
3. 选择改写类型为邮件或域名。
4. 根据步骤2所选改写类型填写原始值。
5. 根据步骤2所选改写类型填写改写值。
6. 点击确定保存改写规则。

### 收件人改写规则

7. 选择收件人改写规则选项卡，点击  进入添加页面。
8. 输入规则名称，表明规则的用途。
9. 选择改写类型为邮件或域名。
10. 根据步骤2所选改写类型填写原始值。
11. 根据步骤2所选改写类型填写改写值。

12. 点击确定保存改写规则。
13. 点击保存，邮件地址改写规则生效。

#### 邮件队列功能设置

介绍邮件队列功能设置的步骤。

正常情况下增强型安全邮件网关ASEG可及时处理电子邮件的发送，不会出现邮件延迟堆积等。在无法找到收件方域名导致重试、SEG资源紧张等情况下，可能出现邮件队列积压现象。安全鳄®增强型安全邮件网关ASEG支持对因各种原因导致暂时没有完成传送而暂存在邮件队列里的邮件进行展示、筛选、删除、立即投递等操作。

用户发送的邮件一直无法到达发件人方，通过邮件队列可以查询该邮件是否在队列中等待以及当前处理状态，用户可以选择该邮件进行立即投递处理。

操作过程中需注意以下事项。

- 可按筛选条件过滤邮件，筛选条件包含：邮件ID，时间，大小，收发件人和邮件状态。初始页面默认无筛选条件。
- 点击删除按钮，您可选择删除已选邮件或删除过滤邮件（未选中的邮件）。

#### TLS证书设置

介绍管理TLS证书设置的步骤。


在系统 > 设备管理页面设置TLS证书。

SEG证书包括企业证书。

企业证书为一个TLS证书，作为客户端和原始服务器站点之间的中转站，保证与客户端的正常进通信。

选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 功能 > 证书页面。点击导入证书按钮导入已有的企业证书，也可点击创建证书按钮在线创建企业证书。

受信证书由SEG所信任的原始服务器提供。

点击  导入受信证书。点击  删除所选受信证书。

#### OCR功能

介绍管理OCR功能的步骤。

在系统 > 设备管理页面设置OCR功能。

OCR识别图像功能支持本地和外置OCR服务器，外置OCR服务器可以解析网络流量中的图片内容并进行DLP分析，提高了对大量图片内容的处理速率，减轻系统资源消耗。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > OCR页面。
2. 滑动状态条，开启OCR功能。
3. 选择OCR工作的精确度，平衡系统资源消耗：

快速	效率高但是精确度低。
平衡	兼顾效率和精确度。
精确	精确度高但是效率低。

4. 选择OCR识别的语言，包括简体中文、繁体中文和英文。
5. 设置OCR图像识别引擎检测文件的大小限制，0表示不限制大小。
6. 选择OCR服务器，包括本地OCR引擎和远程OCR引擎。
7. 点击保存，设置生效。

## 认证

介绍认证设置的步骤。

在系统 > 设备管理页面进行认证设置。

ASWG认证功能可以更准确的识别上网用户的身份，用户的上网请求会匹配合适的认证规则完成认证。目前ASWG支持的认证方式有：本地认证、AD LDAP、Open LDAP、IWA等认证方式。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证页面，基本配置如下：

- 认证失败设置
- 认证冲突设置
- 认证缓存设置
- 认证缓存时间设置
- 其它设置


### 认证服务器设置

介绍认证服务器设置的步骤。

在系统 > 设备管理页面设置认证服务器。

SEG支持四种认证服务器类型：Active Directory、GENERIC LDAP和ESMTP。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证 > 认证服务器页面。

2. 点击  添加认证服务器。：

- a) 输入认证服务器名称。
- b) 选择启用或禁用该认证服务器。
- c) 选择认证服务器类型：Active Directory、GENERIC LDAP和ESMTP。
- d) 选择服务器来源，用户可新建服务器或从用户目录中选择服务器。



Active Directory和GENERIC LDAP支持UCSS用户目录，即调用UCSS系统的用户目录，主机名/IP和端口不可更改。Active Directory和GENERIC LDAP也支持新建服务器，配置如下信息：

1. 输入主机名或者IP地址。
2. 设置LDAP认证服务器的端口号。
3. 输入登录服务器的用户名。
4. 输入登录服务器的密码。
5. 输入目录根节点。如果服务器来源选择的是用户目录，若此用户目录设置了根节点，系统会自动读取。
6. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
7. 选择是否使用SSL安全连接，SSL安全连接提高数据传输的安全性适合于外部网络传输。
8. 输入标准LDAP查询过滤器。例如用户可以通过标准LDAP查询语句快速过滤出期望的对象。
9. 输入邮件字段。例如用户LDAP服务器自定义了邮件字段emailbox，通过邮件字段设置可以告知SEG该字段也代表邮箱地址。

当认证服务器是ESMTP时，只需填写SEG向用户目录进行ESMTP验证使用的邮箱地址。

3. 点击保存，认证服务器设置生效。

表 144: 页面图标和行间操作按钮功能

	编辑认证服务器配置信息。
	删除所选认证服务器。

## 认证规则

介绍管理认证规则的步骤。

在系统 > 设备管理页面设置认证服务器。

认证规则可以控制内网的某个IP或网段的计算机的认证方式。目前代理服务器支持Windows集成认证、本地认证、AD / LDAP认证、Radius认证或者不认证。其中Windows集成认证不支持备用认证服务器认证。






1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证 > 认证规则页面。
2. 滑动状态条全局开启认证规则，点击  添加认证规则。
3. 在弹出的添加规则窗口：
  - a) 输入规则名称，说明其用途。
  - b) 选择启用或者禁用该规则。
  - c) 输入需要匹配的域名。
  - d) 从下拉菜单中选择认证服务器。
  - e) 选择认证功能，支持用户认证和收件人地址验证。
  - f) 点击保存，认证规则添加成功。
4. 再次点击保存，认证规则设置生效。

表 145: 页面图标功能

	禁用所选规则。
	启用所选规则。
	删除所选规则。
	通过上下箭头调整规则优先级，点击保存后生效。

## 其他

其他的选项页面。

该菜单包含其他的选项页面。

### SNMP功能

介绍管理SNMP功能设置的步骤。

在系统 > 设备管理页面设置SNMP功能。

设备支持外部应用访问SNMP服务器来收集设备信息。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > SNMP页面，设置SNMP功能。。
2. 滑动状态条，开启SNMP功能。
3. 选择SNMP query版本，可以设置为v1或v2c。
4. 输入SNMP的团体名，即SNMP的用户名或密码，只允许使用此团体名访问SNMP服务器。
5. 选择以下SNMP的连接方式：

任何IP	任何IP地址都可访问SNMP。
仅限于下列IP	输入IP地址，点击  添加到可访问SNMP的IP列表。

6. 点击保存，设置生效。



## 收集日志

介绍配置收集日志功能的步骤。

在系统 > 设备管理页面设置收集日志功能。

设备支持收集系统日志信息，了解系统运行状态。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 收集日志页面，设置收集日志功能。
2. 选择收集日志的时间段。
3. 选择收集日志的类型。
4. 点击收集日志，收集所设定日期和指定类型的日志，显示于日志收集历史列表中。

点击  可将得收集得日志文件下载到本地；点击  可删除所选日志文件。

## 备份和恢复

介绍备份/恢复功能设置的步骤。

在系统 > 设备管理页面设置备份和恢复功能。

UCSS设备支持立即备份和立即恢复系统配置，包括配置信息、证据文件、邮件、网络及主机信息等，并支持定期备份功能。

1. 选择设备 > 其他 > 备份,进入备份或恢复页面。
2. 点击定期备份启动定期备份，设置定期备份的时间。
3. 点击备份设置，选择以下备份方式和备份内容：

备份至本地	选择备份至本地设备，设置备份日志数量的最大值，若本地保存数量大于设置的最大值则会删除最早的备份。
备份至远程	支持备份至Samba服务器和NFS服务器，需输入服务器的IP/主机名、文件夹路径和用户信息，并进行测试连接。

备份记录会出现在备份历史中，点击删除可删除所选备份。

4. 点击保存，设置生效。

## 升级和补丁

介绍升级/补丁功能设置的步骤。

在系统 > 设备管理页面设置升级和补丁功能。

设备支持在线版本升级和补丁安装，但升级不支持版本回退。选择系统 > 设备管理进入设备管理页面后。点击要查看的设备，进入设备 > 其他 > 升级/补丁页面，然后进行升级或补丁设置。

### • 升级

选择升级选项卡，点击检查更新连接天空卫士的安装包服务器，获取安装包列表，选择安装包下载并安装。如果用户设备无法直接访问互联网，可通过代理服务器配置使用代理进行检查更新，点击代理服务器配置代理服务器。

点击上传安装包从本地上传升级安装包。

### • 补丁

选择不定选项卡，查看当前版本和可用补丁。点击上传安装包从本地上传补丁安装包，安装之后可以选择卸载。

### 远程控制

介绍远程控制功能设置的步骤。

在系统 > 设备管理页面设置远程控制功能。

设备启用SSH连接后，可通过SSH执行远程设备故障排查。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 远程控制页面。
2. 选择是否启用以下功能：

启用远程控制	启用远程控制以后可以开启SSH端口并使用设备管理账号（例如ucssadmin帐号）登录设备进行命令操作。
启用技术支持模块	启用技术模块之后，获取6位密码。该密码需要提供给天空卫士进行解密后使用。
启用超时限制	设置在指定时间之后自动关闭远程控制。

3. 点击保存，设置生效。



注：

远程访问记录可在远程访问历史中查询。

### 系统工具

介绍系统工具设置的步骤。

在系统 > 设备管理页面设置系统工具。

系统工具预置多条CLI命令，即使不连接后台时也可以使用系统工具进行故障排查，并显示执行结果。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，从下拉框中选择索要执行的命令。
2. 输入出现故障的设备主机名或IP，点击执行开始运行故障排查命令，点击停止可终止执行命令。执行结果显示于黑色屏幕中。

### 垃圾病毒库更新

介绍垃圾库和病毒库更新的步骤。

在其他 > 垃圾病毒库更新页面管理版本库更新设置。

增强型安全邮件网关ASEG可以自动按照设定时间从天空卫士™官网进行最新版本的URL分类库、病毒库版本、垃圾库版本下载和更新。

页面显示了当前的版本库状态，包括版本信息和下载及更新历史信息。

版本库包含反垃圾数据库，反病毒数据库和URL分类数据库。

按照以下步骤管理版本库更新设置。

1. 点击其他 > 垃圾病毒库更新进入版本库更新页面。
2. 点击设置按钮进入版本库更新设置对话框。
3. 点击勾选框激活下载计划设置。



注：下载将导致带宽占用，请选择系统空闲的时间下载。

- a) 设置更新时段，点击配置框设置具体的日期和时间。
- b) 在下拉菜单中选择版本检查时间间隔。

4. 点击勾选框激活更新计划设置。



注：更新后设备将自动重启，请选择系统空闲的时间更新。

- a) 设置更新时段，点击配置框设置具体的日期和时间。
5. 点击勾选框激活缓存超时设置，并输入过期时间。  
缓存超时设置后，系统将清除指定时间前缓存在本地的URL记录。
6. 点击确认完成设置。


### 设置设备高可用


介绍设置设备高可用的步骤。




在系统 > 设备管理页面配置设备高可用。

设备高可用是将两台或多台同类型设备（DSG/ASWG/SEG/UCWI）互作备份，当其中某台出现故障时同组设备可以立即替代该设备，保证MTA、ICAP Server、代理服务业务的正常进行。

当设备出现硬件故障（断电、网卡等出现问题），网络故障（网线连接问题、其他网络设备出现故障）等情况无法实现设备切换。

 提示：高可用仅支持同类型设备的同类型网卡间的切换，ASWG设备的P1和P2网口只能在代理模式下支持高可用切换。

 注：启用了配置同步功能后，当配置了高可用的设备组之中的任意一台设备变更了配置（如HTTP里的参数变更），安全管理员无需重复操作，该设备的配置改动能自动同步到高可用组内的其他设备中。

1. 选择系统 > 设备管理，点击高可用，在下拉菜单中选择设备型号，配置设备高可用。
2. 输入设备组名称，如北京UCSG-ASWG设备。
3. 点击  从已注册设备列表中选择设备。点击  删除所选设备。设备不能被重复添加到不同的分组。
4. 开启虚拟IP，进行如下配置：
  - a) 输入虚拟IP地址（虚拟IP数量不能大于组内的设备数量并且IP地址与在设备需在同一IP段）。
  - b) 选择网卡类型：Mgmt管理接口，MTA邮件接口，P1/P2代理接口（仅UCSG-ASWG设备）。
  - c) 设置子网卡序号（用于标记，数字不重复即可）。
  - d) 点击  添加于列表。
5. 点击保存，添加完成。





---

# 第 7 章

---

## 移动安全

---

内容:

- 移动安全检测条件
- 移动安全管理
- 移动安全监控
- 移动安全报告
- 移动安全设备监控
- 移动安全设备管理

介绍天空卫士™移动安全解决方案。

天空卫士™安全鳄®统一内容安全UCS ( UCS ) 解决方案采用移动安全网关MAG作为其移动安全解决方案，以帮助您的企业和机构应对散布在移动应用设备及其通信通道中的各种安全威胁。

在移动互联网日益发展的新形势下，个人智能移动设备越来越多的开始被企业和组织用于承载关键业务和核心应用。企业和组织需要一个具备高安全性，高可用性的移动安全解决方案，用于完善企业和组织的应用程序安全以及企业数据安全。

天空卫士™移动安全产品解决方案-移动安全网关MAG以虚拟安全域为技术为核心，从移动设备监控，企业移动应用管理，移动设备中的企业数据存储和移动设备在网络中的传输4个角度出发，采用终端安全域作为应用载体，基于统一的企业数据安全策略平台，实现对企业移动安全的全面覆盖。同时，结合天空卫士™其他安全产品，为企业移动应用的运行和控制提供统一的安全管理环境，实现内容安全有效落地。

### 产品特点

天空卫士™移动安全产品解决方案-移动安全网关MAG产品具有如下特点：

- 将企业移动应用与个人移动应用完全隔离开来，其中包括数据隔离。
- 企业移动应用程序的数据受到严格控制，包括下载，上传，复制，粘贴，截屏，以及数据存储和加密以实现移动终端数据防泄密。
- 企业移动应用程序通过专门的加密通道访问企业内部服务器。企业移动应用的数据采用安全方式加密，确保攻击者难以破解非法获得的数据。
- 集成内容分析引擎，支持针对移动设备安全域中的企业应用数据发现任务，保证移动设备的数据存储符合企业的安全合规性要求。
- 员工完全无需更改个人移动应用程序以及使用习惯。

## 移动安全检测条件

介绍检测条件中的移动应用及其相关知识。

天空卫士™安全鳄®统一内容安全UCS解决方案中的移动安全模块在安全策略中运用多种检测条件检测违反企业安全制度的内容和行为，并在有必要的情况下，采取对应的策略行为，限制或阻断通信，确保企业移动安全。

移动安全解决方案支持以下检测条件。

- 移动应用

### 应用

介绍检测条件中的移动应用及其相关知识。

应用检测条件针对企业的内部应用程序，企业根据自身的安全性要求，可通过应用策略，针对对应用、用户、时间、位置维度等进行安全性限制。

通过添加应用检测匹配，安全管理员可以配置APP应用策略并下发至移动安全网关MAG，在指定的时间和指定地址范围对企业应用的敏感操作进行限制，以防止用户通过复制、截屏、分享、蓝牙、应用内打开等方式泄露企业机密信息，或通过水印操作在用户拍照泄密后可以溯源。

## 移动安全管理

介绍移动安全管理相关功能。

移动安全管理相关页面集中位于菜单栏的**Mobile**管理选项下。

通过这些页面上的操作，管理员可以：

- 管理移动安全策略
- 管理移动应用
- 管理移动客户端
- 管理其他移动安全设置

### 移动安全策略

介绍移动安全策略管理的相关信息。





统一内容安全UCS解决方案支持企业安全管理员企业IT管理员可以对企业应用下发应用策略，保证应用符合企业的安全性要求。

在**Mobile**管理 > 策略页面添加移动安全策略。

策略检测内容

在策略配置页面，点击检测内容选项卡后，选择**匹配 > 应用**选项即可配置移动应用所匹配的用户。

所涉及页面包含如下图标。

图标	解释
	点击按钮进入匹配条件配置对话框。
	点击按钮删除选择的匹配条件。
	点击按钮将选择的匹配条件移至左侧，未选择的条件。
	点击按钮将选择的匹配条件移至右侧，已选择的条件。

## 移动应用

在**Mobile管理** > 应用页面管理企业移动应用。

统一内容安全UCS解决方案提供统一的企业级应用市场，可以对企业应用进行添加、编辑、启用、禁用、删除和重新打包等操作。

1. 选择**Mobile管理** > 应用，进入应用管理页面。
2. 点击添加按钮，进入添加应用页面。
3. 输入应用名称，表明该应用的用途。
4. 点击选择上传应用。并选择是否填写对该应用的描述。
5. 择是否启用该应用。如果不启用，新添加的应用不被启用，但将显示于应用列表中。
6. 设置该应用程序的可被下载的次数，不设置数值即为无限制。
7. 点击确定，保存对该应用的设置。



提示：点击启用、禁用、重新打包和删除按钮可对列表中已选的应用进行一键操作。

## 移动客户端

移动安全网关MAG支持对移动客户端进行统一配置和管理。主要包含以下部分：

- 客户端配置
- 安全域配置
- 客户端安装包

### 配置客户端

介绍客户端配置页面

在**Mobile管理** > 客户端管理 > 客户端配置页面对移动安全网关MAG所管理的移动客户端进行统一配置。

### MAG服务器外网设置

在此栏查看移动安全网关MAG服务器的外网连接状态。

### 连接频率

在此栏设置策略同步频率、设备同步频率和清除未同步移动端的时间。

具体描述和限制如页面信息所示。

### 客户端磁盘空间占用

在此栏设置日志文件、事件证据和临时文件的存储空间大小限制，并显示总的存储空间占用限制。

具体描述和限制如页面信息所示。

### 使用限制

在此栏选择是否支持越狱或ROOT设备。

具体描述和限制如页面信息所示。

### 水印

在此栏设置水印显示颜色和透明度，以及水印显示内容。

- 水印显示：设置字体颜色和透明度。字体颜色以RGB表示。
- 水印内容：包括登录账号，日期时间，和公司名称。

具体描述和限制如页面信息所示。

## 客户端升级

在此栏选择是否启用客户端升级包的自动推送提示，以及是否启用强制升级。

当客户端启用时会收到提示信息，用户确认后下载升级包。

具体描述和限制如页面信息所示。

## 配置安全域

介绍安全域配置页面。

在**Mobile管理** > **客户端管理** > **安全域配置**页面对安全域内的所有企业应用进行统一配置。

移动安全网关MAG支持虚拟安全域，将移动客户端的所有企业级应用归属一个安全域，方便统一管理。

1. 选择**Mobile管理** > **客户端管理** > **安全域配置**，进入安全域配置页面。
2. 点击添加，进入编辑安全域配置 页面。
3. 输入安全域名称和描述（选填）。
4. 选择是否启用该安全域配置。
5. 在管理移动安全客户端区域，选择需要管理的移动终端用户。
6. 在移动安全网关区域，选择移动安全配置服务器并设置优先级。
7. 在安全配置区域，配置客户端空闲时长限制。



提示：勾选禁用客户端时，清除安全域数据选项后，客户端在收到服务器禁用指令后会清除安全域内的数据。

8. 在网络配置区域，选择网络传输机制。

请根据网络配置设置相应的硬件部署：

- 安全传输和DLP检测：

- 设置安全传输功能，详细配置信息请参考[安全传输功能设置](#) on page 360。
- 部署ASWG设备并进行相关配置，详细信息请参考天空卫士™安全鳄®统一内容安全UCS部署指南。
- 仅安全传输：设置安全传输功能，详细配置信息请参考[安全传输功能设置](#) on page 360。
- 不保护网络：无需额外设置。

9. 在设备存储配置区域，选择是否对安全域内的数据进行加密存储。
10. 点击保存，安全域配置生效。

## 客户端安装包

在**Mobile管理** > **客户端管理** > **客户端安装包**页面对移动客户端安装包进行统一管理。

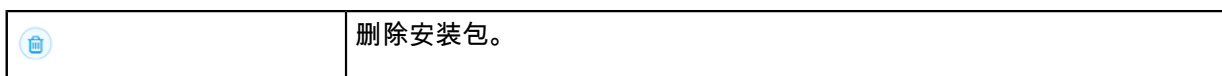
管理员可通过UCSS上传、创建和删除客户端安装包，实现客户端的安装、升级和部署。

1. 选择**Mobile管理** > **客户端管理** > **客户端安装包**，进入客户端安装包页面。
2. 点击上传按钮将本地的安装包添加至列表。  
上传类型一栏显示手动上传。
3. 选中安装包，点击创建按钮，指定移动安全网关后开始创建安装包。  
创建状态一栏显示创建中。
4. 创建状态一栏显示已完成时，安装包创建成功。

将鼠标悬浮于所创建的安装包名称，出现悬浮图标及其解释如下：

表 146: 页面图标和行间操作按钮功能

	编辑安装包。
	下载安装包。



## 移动安全设置

介绍移动安全相关设置信息。

移动安全设置页面允许您的管理员进行移动安全相关的设置。

可选设置包括：



- 基本设置
- 证书管理

### 基本设置

介绍配置移动安全基本设置的步骤。

基本设置包含管理员在UCSS设置内网目标服务器，保证移动客户端的访问遵循企业统一的SWG策略管理，对其从内网下载的数据进行DLP检测并执行安全操作。

在基本设置页面，管理员可以配置移动安全高级设置。高级设置主要提供给管理员做一些针对Mobile的不常用但是必须的设置管理。如果高级设置的信息发生变化，基本设置版本号需要发生相应修改。

1. 选择**Mobile管理** > **设置** > **基本设置**，进入基本设置页面。
2. 在内网服务器区域添加内网服务器：
  - a) 在下拉菜单中选择IP、IP段、主机名或子网掩码，并输入相应数值。
  - b) 点击  添加到列表。点击  可删除列表中选中的内网服务器。
  - c) 点击保存，内网服务器配置生效。

### 证书管理

在**Mobile管理** > **设置** > **证书管理**页面管理移动安全证书。

移动安全网关MAG支持代码签名证书和凭证证书，并由UCSS进行统一管理。

- 代码签名证书为企业重新发布应用的必要条件，需要在使用前进行配置，否则无法打包应用。
- 凭证证书用于安全传输过程中的授权需要，用户可按需配置。

### 代码签名证书

在代码签名证书选项卡下，

在iOS区域，点击导入证书和描述文件按钮。在弹出的页面进行如下配置：

1. 点击选择按钮，从本地导入证书文件。
2. 输入证书密码。
3. 点击选择按钮，从本地导入证书描述文件。
4. 点击确定导入，证书导入成功。

在Android区域，点击导入证书和描述文件按钮。在弹出的页面进行如下配置：

1. 点击选择按钮，从本地导入证书文件。
2. 输入证书密码。
3. 点击确定导入，证书导入成功后显示详细的信息。

### 凭证证书

在凭证证书选项卡下，点击添加，在弹出的页面进行如下配置：

1. 点击选择按钮，从本地导入证书文件。
2. 点击选择按钮，从本地导入证书私钥。

3. 输入证书密码。
4. 点击导入，证书导入到列表。

## 移动安全监控

介绍如何监控您的移动安全设备。

移动设备监控记录所有注册到移动安全网关MAG服务器的客户端信息，并对其进行控制。

### 移动邮件事件

介绍监控移动邮件事件的相关信息。



#### 简介

移动邮件事件监控功能记录所有移动端发送和接受的邮件流量命中DLP策略的事件详情和证据文件信息。在监控 > 移动监控 > 移动邮件事件页面管理监控到的实时移动邮件事件信息。

#### 页面介绍

实时监控页面包含以下快速按钮。

表 147: 快速按钮功能介绍


按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

实时监控页面包含以下操作按钮。

表 148: 按钮功能介绍


按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 下载的文件为解密后的eml格式文件。</li> <li>• 支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>• 如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>

按钮	功能
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 添加的备注信息可以在历史记录中进行查看。</li> <li>• 支持为事件批量添加备注信息。</li> </ul>
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>• 选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>• 事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>• 支持事件的批量忽略和取消忽略。</li> </ul>

按钮	功能
邮件审批	<p>点击按钮将所选的事件发送至安全管理员或主管进行审批。</p> <p>邮件审批包括释放和拒绝功能。</p> <ul style="list-style-type: none"> <li>选择释放则邮件会被投递给原收件人，事件动作会更新为已释放，已释放的邮件不可再次释放。</li> <li>选择拒绝则邮件不会被投递，事件动作会更新为已拒绝，已拒绝的邮件可以再次释放。</li> </ul> <p> 注：仅适用于邮件通道中的被系统隔离的事件，需事先在通知详情配置中选择邮件审核选项。</p>
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	<p>点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。</p>

#### 移动事件详情

查看命中策略的移动事件的详细运行信息。

选择列表中的发现事件，将鼠标悬浮于事件ID，出现事件详情图标  并点击，显示下列事件属性、命中策略详情、证据和历史记录等信息。

#### • 事件属性详细信息

事件属性	解释
全名	生成事件的用户全名，获取用户目录中的用户全名，包括用户名(用户识别模块)/IP地址/主机名/Email地址等。
登录名	生成事件的登录名，获取终端IP地址。
邮箱	生成事件的用户邮箱。
部门	生成事件的用户部门名称，获取组织架构定义或AD Department的部门名称。
职位	生成事件的用户职位，获取组织架构定义或AD Department的职位名称。
用户识别名	生成事件的用户识别名，获取组织架构定义或AD 登录名的用户识别名。
组	生成事件的用户所在组，获取组织架构定义或AD Group的组名。
TRS分值	生成事件来源的总风险值。
通道	检测网络数据的通道。
类型	生成事件的类型。



事件属性	解释
同步用户	同步该邮件的用户数，点击数值显示用户信息。
动作	违规后触发策略所执行的动作（放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放）。
事件状态	五种事件状态（新/进行中/关闭/误报/提级）。
安全级别	事件安全级别（高/中/低/信息）。
最大匹配	触发策略规则项的最大匹配。如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。
检测时间	引擎模块检测到违规事件触发策略的时间。
事件时间	管理平台收到违规事件的时间。
检测引擎	DLP检测数据的引擎模块。
分析引擎	后端分析数据的引擎ATS。
工作模式	DLP设备工作模式，支持仅监控和阻断。

- 命中策略及详情：显示该事件命中的策略名称和详细违规内容。策略配置请参考[DLP策略](#)。
- 证据：包括事件来源（终端名称\用户名）和终端设备名称。



注：若需显示证据信息，则要开启记录证据文件功能，具体操作请参考[管理策略动作](#)，通过编辑策略开启此功能。

表 149: 证据页面图标功能

图标	解释
	全屏显示证据文件。
	返回到事件列表。

- 历史记录：包括所有对该事件的操作信息，若该事件被删除，则不会记录而显示在审计日志中。详细信息请参考[查看审计日志](#)。

## 应用管理事件

介绍监控移动应用管理事件的相关信息。

### 简介

监控应用管理事件功能支持管理由企业应用触发移动策略而产生的事件。

在[监控](#) > [移动监控](#) > [应用管理事件](#)页面管理监控到的实时应用管理事件信息。



提示：除常规项目外，页面还可支持如下筛选条件：

- 通道：包括拷贝/剪切、截屏、Open-In、第三方分享和蓝牙。
- 动作：包括加密、放行和阻止。

### 页面介绍

监控页面包含以下快速按钮。

表 150: 快速按钮功能介绍

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

监控页面包含以下操作按钮。

表 151: 按钮功能介绍

按钮	功能
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>• 支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>• 支持删除报表中所有的项目。</li> <li>• 删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>• 如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

## 邮件安全移动端

介绍查看MAG邮件安全移动端监控的相关信息。

### 简介

邮件安全移动端监控功能记录所有通过移动邮件接入网关MAG同步过邮件信息的移动设备信息。

- 移动设备的邮件客户端通过MAG接收邮件时只会记录一个移动设备的信息；
- 一台移动设备上有多条邮件地址通过MAG接收邮件时会记录多条设备信息，其中的设备ID相同，邮件地址不同。
- 只有ActiveSync协议支持移动设备的监控，POP3和IMAP协议不支持。

在监控 > 移动监控 > 邮件安全移动端监控页面管理监控到的实时邮件安全移动端信息。

### 页面介绍

监控页面包含以下信息。

表 152: 页面显示列

筛选条件/显示列	解释
设备ID	移动设备的内部ID。
设备类型	设备类型名称，如Android、iPad、iPhone等。
邮箱	在邮件客户端设置的邮箱地址。

筛选条件/显示列	解释
用户	邮箱地址与用户目录关联后的用户显示名称，如张三。
部门	该邮箱地址对应的用户所在的部门。
上次同步时间	上次同步邮件的时间。
user Agent	邮件客户端类型的标识符User Agent，如：Android/7.0-Outlook-EAS。

监控页面包含以下快速按钮。

表 153: 快速按钮功能介绍

按钮	功能
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

监控页面包含以下操作按钮。

表 154: 按钮功能介绍

按钮	功能
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的项目。</li> <li>删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。


## 设备安全移动端

介绍设备安全移动端监控的相关信息。

### 简介

设备安全移动端监控功能实时展示移动端设备信息，客户端信息和邮件同步状态。

在监控 > 设备安全移动端页面管理实时监控到的设备安全移动端信息。

点击  查看移动端设备信息，客户端信息和同步状态。



筛选条件	解释
Mobile服务器	所连接的终端服务器地址
设备名称	终端设备名称

筛选条件	解释
平台类型	终端平台类型：iOS/Android
设备型号	终端设备型号
软件信息	详细终端软件平台版本号
内存大小	终端内存大小
可用空间	终端设备可用空间大小
设备序号	终端设备序列号
设备IMEI号	终端设备IMEI号
MAC地址	终端设备的MAC地址信息
蓝牙	终端设备的蓝牙地址信息
登录账号	客户端登录状态信息
终端状态	客户端状态为启用或禁用
Mobile服务器版本	客户端所连接的终端服务器版本
配置名称	同步状态下的配置名称
终端配置版本	同步状态下的配置版本
安全配置版本	安全配置的软件版本
证书配置版本	证书配置的版本
应用配置版本	应用配置的版本
同步状态	同步状态为失败或者成功
上次同步时间	上次同步的时间
安全域数据	安全域中数据的大小

### 页面介绍

监控页面包含以下快速按钮。

表 155: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示：</p> <ul style="list-style-type: none"> <li>可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

监控页面包含以下操作按钮。

表 156: 按钮功能介绍

按钮	功能
启用	点击按钮启用设备安全移动端应用程序。
禁用	点击按钮禁用设备安全移动端应用程序。
更多操作	<p>点击按钮对设备安全移动端进行进一步操作。可选的操作包括：</p> <ul style="list-style-type: none"> <li>• 擦除安全域数据，被擦除的数据不可恢复。</li> <li>• 卸载移动设备上安装的安全客户端应用程序</li> <li>• 升级移动设备上安装的安全客户端应用程序</li> <li>• 卸载移动设备上安装的安全终端客户端应用程序</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选项目。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的项目。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>• 支持项目的批量删除，需先选中需要删除的项目。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>• 支持删除报表中所有的项目。</li> <li>• 删除项目时，会弹出确认对话框，其中显示删除项目的数量，并选择需要删除项目的原因。选择其他原因时，需要说明具体原因。</li> <li>• 如果事件被成功删除，存放的证据文件也将一起删除。</li> </ul>

## 移动流量统计

介绍设置移动流量统计的步骤。

### 简介

移动流量统计功能统计企业移动应用的网络访问流量，并记录为移动流量日志。

在监控 > 移动监控 > 移动流量统计页面管理实时监控到的移动流量统计信息。



系统默认显示最近1天所接收到的移动应用访问量。

 注：移动流量监控功能需要开启安全传输和DLP检测，详细信息请参考[配置安全域](#) on page 332。

### 页面介绍

监控页面包含以下快速按钮。

表 157: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

### 高级统计

按照如下步骤执行高级统计操作，对监控数据进行二维统计并排名。

1. 勾选高级统计对监控数据进行二维统计。
2. 选择排名方式和排名数。
3. 点击查询。
4. 查看显示的二维统计数据，快速确认安全隐患。

### 筛选条件/显示列

筛选条件/显示列	解释
用户	用户名或IP地址
登录名	开启认证时的用户登录名
唯一识别名	如AD中的用户识别名
部门	组织架构的部门信息
源IP	来源的IP地址
动作	SWG策略所对应的动作
域名	用户域名
策略名称	SWG策略名称
通道	事件所发生的通道
URL分类	SWG策略定义的URL分类
URL风险类别	URL对应的风险类别
安全威胁类型	预置的安全类型
病毒名称	所中病毒的名称
关键字	配置策略时定义的关键字
URL主机名	URL的主机名
完整URL	完成的URL，包括协议和主机名
目标IP	目标IP地址

端口	目标端口号
移动设备名称	移动设备的名称
文件名称	网络传输的文件名称
浏览时长	用户浏览网页的时长
是否安全	命中威胁类型和病毒的都是不安全的
城市	根据目标IP解析的城市
国家	根据目标IP解析的国家
位置	根据目标IP解析的位置
发送字节数	发送请求字节数
接收字节数	收到响应字节数
总字节数	请求和响应的总字节数
应用类型	网络应用类型
应用名称	应用程序名称
阻止类型	自定义动作被阻止的原因类别
来源Risk Level	用户行为所属的Risk Level(高危、危险、严重、普通和较低)
方法	HTTP请求的方法
响应码	HTTP响应码
Cloud App	Cloud App名称
Cloud App分类	Cloud App 所属分类
Cloud App 信任级别	Cloud App 的信任级别 ( 由后台给出 , 用户不可更改 )
Cloud App 分值	Cloud App 的信用分值
Referrer URL	记录当前页面的来源地址 , 即定向页面的URL
User Agent	HTTP报文中UserAgent信息
会话阶段	用户行为日志生成时所在的HTTP会话阶段

### 移动流量日志

介绍移动流量日志监控的相关信息。

#### 简介

移动流量日志监控功能对移动流量日志进行实时监控。



在监控 > 移动监控 > 移动流量日志页面管理实时监控到的移动流量日志信息。

系统默认显示最近1天产生的移动流量日志。

#### 页面介绍

监控页面包含以下快速按钮。

表 158: 快速按钮功能介绍

按钮	功能
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	<p>点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p>

## 移动安全报告

介绍移动安全报告相关信息。

移动安全报告整体展现命中的策略名称、策略动作和所属安全级别等事件的详细信息。

移动安全报告包括：

- 移动邮件报告
- 应用管理报告
- 移动设备报告
- 移动流量报告

### 移动邮件报告

介绍移动邮件报告的相关信息。

#### 简介

移动邮件报告展现移动安全设备获取用户移动端的邮件信息。移动邮件报告信息包括事件来源IP、目标、通道、动作和安全级别等，报告类型包括列表报告、图表报告和趋势报告。

在报告 > 移动报告 > 移动邮件报告页面管理移动邮件报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

#### 基本操作

系统支持预置报告和自定义报告。

- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。



#### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

报告页面包含以下快速按钮。





表 159: 快速按钮功能介绍

按钮	功能
保存为报告	将当前设置的筛选条件保存为自定义报告。保存后的报告显示在报告列表中。
调整显示列	<p>点击按钮显示所有筛选条件对话框，可选择筛选条件，查看具体的报告数据。符合筛选条件的统计数据将以显示列的方式显示在报告中。</p> <p> 提示:</p> <ul style="list-style-type: none"> <li>• 可充分利用显示的列信息，通过查看、排序、分组和过滤等找到重大违规事件项</li> <li>• 可点击恢复初始按钮  可恢复为系统默认列信息</li> <li>• 可勾选保存为默认配置选项，将当前所选的列信息保存为默认显示列。</li> </ul>
添加筛选	点击按钮显示所有筛选条件列表，可添加筛选条件。符合筛选条件的统计数据将以显示列的方式显示在报告中。

报告页面包含以下操作按钮。

表 160: 按钮功能介绍

按钮	功能
下载	<p>点击按钮下载已选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 下载的文件为解密后的eml格式文件。</li> <li>• 支持事件的批量下载，批量下载的文件为zip格式，其中每个事件文件以事件ID命名。</li> <li>• 如果下载失败，则会提示错误信息，并显示失败的原因。</li> </ul>
添加备注	<p>点击按钮为所选事件添加备注信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 添加的备注信息可以在历史记录中进行查看。</li> <li>• 支持为事件批量添加备注信息。</li> </ul>
添加标签	<p>点击按钮为所选事件添加<a href="#">事件标签</a>，用于筛选事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 标签名称为必填字段，标签备注为选填字段。</li> <li>• 添加的标签信息可以在历史记录中进行查看。</li> <li>• 保存事件标签时，系统会对标签名称的唯一性进行检查。</li> </ul>
更改事件状态	<p>点击按钮更改事件状态。事件状态包括：</p> <ul style="list-style-type: none"> <li>• 新事件</li> <li>• 进行中的事件</li> <li>• 已关闭的事件</li> <li>• 被标记为误报的事件</li> <li>• 被标记为需提高安全级别的事件</li> </ul>
更改安全级别	<p>点击按钮更改事件的<a href="#">安全级别</a>。安全级别包括：高，中，低，和信息。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 从下拉列表中选择一种事件严重性，选中事件严重性后，会更新相应事件的状态信息，并刷新事件列表。</li> <li>• 支持批量更新事件的严重性，如果更新失败，则会提示错误信息，并显示失败的原因。</li> </ul>

按钮	功能
通知	<p>点击按钮将所选事件以邮件的形式向上级主管或安全管理员发送通知。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 如果需要发送副本或无信头副本，则可以添加抄送和秘密抄送。</li> <li>• 邮件主题和正文默认显示邮件模板内容，可以自定义主题和正文内容，可以通过模板变量添加更多信息。</li> <li>• 如果选择重要邮件选项，则此邮件为优先发送的邮件。</li> <li>• 可以在邮件服务器列表中选择需要通过哪个邮件服务器发送该通知邮件。</li> <li>• 通知发送成功后，会将相应事件的状态更新为已上报（提高安全级别）。</li> <li>• 支持事件的批量通知，以每个事件一封邮件的方式进行发送。如果发送失败，则会提示错误信息，并显示失败的原因。</li> <li>• 收件人可点击邮件 workflow 管理该事件。</li> </ul>
忽略设置	<p>点击按钮忽略所选事件或取消忽略该事件。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 选择忽略事件会将事件置为忽略状态，并更新事件列表，被忽略的事件不会在事件列表中显示出来。</li> <li>• 选择取消忽略事件，则将事件置为未忽略状态，并更新事件列表，显示取消忽略的事件。</li> <li>• 事件列表默认不显示被忽略的事件，除非通过高级过滤器，添加显示被忽略的事件条件。</li> <li>• 支持事件的批量忽略和取消忽略。</li> </ul>
邮件审批	<p>点击按钮将所选的事件发送至安全管理员或主管进行审批。</p> <p>邮件审批包括释放和拒绝功能。</p> <ul style="list-style-type: none"> <li>• 选择释放则邮件会被投递给原收件人，事件动作会更新为已释放，已释放的邮件不可再次释放。</li> <li>• 选择拒绝则邮件不会被投递，事件动作会更新为已拒绝，已拒绝的邮件可以再次释放。</li> </ul> <p> 注：仅适用于邮件通道中的被系统隔离的事件，需事先在通知详情配置中选择邮件审核选项。</p>
锁定	<p>点击按钮将事件置为锁定状态。注意以下事项：</p> <ul style="list-style-type: none"> <li>• 对于非数据库发现事件，当同一文件被同一发现任务扫描产生发现事件时，如果事件处于未锁定状态，则会将事件记录的所有内容（除事件ID）更新，并产生历史记录，事件被发现任务XX更新；如果事件处于锁定状态，则事件记录的所有内容都不会更新，而是产生一条新的事件。</li> <li>• 对于数据库发现事件，当同一个数据表被同一发现任务扫描产生发现事件时，会首先清空同一数据表被同一发现任务扫描产生的所有数据库分片发现事件，然后产生新的分片事件；如果某些分片事件处于锁定状态，则这些事件不会被清除。</li> </ul> <p> 注：仅显示于发现事件报告页面。</p>

按钮	功能
删除	<p>点击按钮删除选中的事件。</p> <p>删除已选事件：直接删除已选事件。</p> <p>删除过滤事件：标记原因（误报/已解决/不相关）后删除当前页面所有筛选后的事件。</p> <p>注意以下事项：</p> <ul style="list-style-type: none"> <li>支持事件的批量删除，需先选中需要删除的事件。如果删除失败，则会提示错误信息，并显示失败的原因。</li> <li>支持删除报表中所有的事件。</li> <li>删除事件时，会弹出确认对话框，其中显示删除事件的数量，并选择需要删除事件的原因。选择其他原因时，需要说明具体原因。</li> <li>如果事件删除成功，存放的证据文件也将一起删除。</li> </ul>
统计	点击按钮按照快速生成按照某一条件的进行统计的事件统计报表，快速对多条事件进行归类排列，并呈现柱状图排序。

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相信步骤信息。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示网络事件图表报告支持的类型和对应解释。

表 161: 报告类型

报告类型	解释
策略排名	统计不同策略被命中的事件数量，并排名前N位（最多30名）。
来源排名	统计不同来源所命中的策略总数，并排名前N位（最多30名）。
目标排名	统计不同目标所命中的策略总数，并排名前N位（最多30名）。
通道排名	统计不同通道处理的事件总数，并排名前N位（最多30名）。
安全级别	统计不同安全级别对应的事件总数，并排名前N位（最多30名）。
动作排名	统计不同动作类别对应的事件总数，并排名前N位（最多30名）。
策略组排名	统计不同策略组被命中的事件总数，并排名前N位（最多30名）。
事件状态	统计不同事件状态对应的事件总数，并排名前N位（最多30名）。
全部属性	统计以上全部属性的信息，并排名前N位（最多30名）。

### 趋势报告

趋势报告支持以一段时间的数据为基础展示行为和事件发生的趋势。

如需创建自定义报告，参考[创建自定义趋势报告](#)章节获取相信步骤信息。

下表显示网络事件趋势报告支持的类型和对应解释。

表 162: 报告类型

报告类型	解释
安全级别趋势	统计不同安全级别对应的事件数量。
策略趋势	统计策略被命中的事件数量，并排名前N位（最多30名）。
全部属性	统计以上全部属性的趋势信息。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 事件筛选条件/显示列

介绍数据安全报告的筛选条件/显示列。

下表罗列了数据安全报告的筛选条件/显示列，并逐条介绍其含义。

筛选条件/显示列	解释
事件ID	事件识别号
流量UUID	流量通用唯一识别码
事件时间	事件发生的时间
检测时间	检测事件的时间
来源	用户名(用户识别模块)/IP地址/主机名/Email地址
目标	用户名(用户识别模块)/IP地址/URL地址/设备名(Endpoint USB/DVD/Printing)/Email地址
策略组	事件命中策略的组，支持多选。
策略名称	DLP策略名称
通道	事件所发生的通道（HTTP/HTTPS/FTP/IM/SMTP/自定义协议/网络打印/IMAP/POP3/”WebService应用/文件共享）。
动作	策略所对应的动作（放行/阻止/删除附件/第三方加密/隔离/内容加密/已释放/水印）。
事件状态	五种事件状态（新/进行中/关闭/误报/提级）
安全级别	四种安全级别（高/中/低/信息）
最大匹配	如匹配多条策略规则，显示最大的匹配数量。
文件名称	如POST的文件，Email的附件；若为数据库文件则显示表名。
流量大小	数据流量的大小。
检测引擎	捕获数据的引擎名称
分析引擎	后端分析数据的引擎名称
释放状态	事件是否被手动释放
详细信息	若为HTTP/HTTPS事件，会显示URL信息；若为邮件则显示邮件主题。

事件标签	为事件添加的标签
忽略状态	事件状态为已忽略或未忽略
违规内容	事件详细的违规内容，如机密等
工作模式	支持仅监控/阻断
组	组织架构定义的组名
组织单元	组织架构定义的组织单元名
来源IP	来源IP地址
目标IP	目标IP地址
邮箱	组织架构中配置或同步AD的用户邮箱
主管	组织架构中配置或同步AD的主管信息
部门	组织架构定义的部门名称
国家	国家名称
城市	城市名称
位置	事件发生的位置
同步用户	移动设备上进行邮件同步操作的用户
来源RiskLevel	事件来源的RiskLevel ( 较低、普通、严重、危险、高危 )
类型	事件的类型
释放者	邮件的释放者
释放时间	释放邮件的时间
职位	组织架构定义的职位名称
匹配总数	事件命中所有规则的匹配数量总和

## 应用管理报告

介绍应用管理报告的相关信息。

通过列表/图表的方式帮助管理员快速了解如下信息：

在报告 > 移动报告 > 移动应用报告页面管理移动应用报告。

### 简介

应用管理报告展现移动安全设备获取用户移动端的移动应用信息。应用管理报告信息包括日期时间、设备名称、登录账号、应用名称、通道、动作和策略名称等，报告类型包括列表报告和图表报告。

在报告 > 移动报告 > 应用管理报告页面管理应用管理报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。

- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

## 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

主要为企业安全管理员解读以下问题。

- 企业用户触发了哪些应用管理操作 ( 列表 )

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相信步骤信息。

## 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

主要为企业安全管理员解读以下问题。

- 企业的哪些移动用户触发管控操作 ( 图表 )
- 移动用户使用的哪些应用操作较多 ( 图表 )

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示网络事件图表报告支持的类型和对应解释。

表 163: 报告类型

报告类型	解释
用户排名	统计不同用户被命中的事件数量，并排名前N位 ( 最多30名 )。
应用排名	统计不同应用被命中的事件总数，并排名前N位 ( 最多30名 )。
通道排名	统计不同通道处理的事件总数，并排名前N位 ( 最多30名 )。
全部类型	统计以上全部属性的信息，并排名前N位 ( 最多30名 )。

## 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

## 移动设备报告

介绍移动设备报告的相关信息。

需要提供多个维度的报告，方便管理员了解企业的移动用户的移动终端设备的部署和使用情况。具体包括以下部分：

- 客户端设备平台类型: 按照设备安全移动端监控列表平台类型进行统计，帮助管理员了解企业移动设备平台比例。
- iOS客户端系统系统版本: 统计iOS设备，按照并按照设备安全移动端监控列表软件信息字段分平台进行归类。帮助管理员了解企业移动设备的系统版本信息。
- 安卓客户端系统系统版本: 统计安卓设备，并按照设备安全移动端监控列表软件信息字段分平台进行归类。帮助管理员了解企业移动设备的系统版本信息。
- 安全域数据分布: 统计汇总企业应用下载的数据量记录，帮助企业管理员调整和制度策略。

在报告 > 移动报告 > 移动设备报告页面管理移动事件报告。

## 移动流量报告

介绍移动流量报告的相关信息。

### 简介

移动流量报告帮助您的管理员掌握企业移动用户使用企业内网的信息。系统提供包括列表/图表的报告：

- 了解企业用户使用移动设备访问记录（列表）
- 了解企业用户使用移动设备访问内网信息（图表）

在报告 > 移动报告 > 移动流量报告页面管理移动流量报告。

安全管理员可以点击调整显示列按钮，运用[筛选条件](#)，查看具体的报告数据。

### 基本操作

系统支持预置报告和自定义报告。





- 预置报告支持另存和新建定时任务等操作。
- 自定义报告支持编辑、另存、添加[定时任务](#)和删除等操作。

安全管理员可以点击列表中的报告名称，进入报告查看具体信息。

### 图标和按钮

报告列表页面包含以下操作按钮。

表 164: 页面图标功能介绍

图标	功能
	编辑报告，预置报告模板不支持直接编辑。
	将报告另存到列表。另存预置报告模板后可编辑报告。
	添加定时任务并发送给指定的管理员邮箱。详细信息请参考 <a href="#">创建定时任务报告</a> 。定时任务数量和创建者显示于报告列表行信息。
	删除所选报告。

### 列表报告

列表报告支持以列表的形式展示行为和事件等信息。

如需创建自定义报告，参考[创建自定义列表报告](#)章节获取相信步骤信息。

### 图表报告

图表报告支持以图表的形式展示行为和事件的所占比例等信息。

如需创建自定义报告，参考[创建自定义图表报告](#)章节获取相信步骤信息。

下表显示用户安全图表报告支持的类型和对应解释。

表 165: 图表报告类型

报告类型	解释
用户排名	统计不同用户被拦截的数量，并排名前N位（最多显示30名）。

报告类型	解释
应用排名	统计不同应用程序被拦截的数量，并排名前N位（最多显示30名）。
网站访问量排名	统计各个网站的访问量，并排名前N位（最多显示30名）。
网站分类排名	统计不同上网安全活动的数量，并排名前N位（最多显示30名）。
全部类型	统计以上全部分类的信息，并排名前N位（最多30名）。

### 定时任务报告

定时任务报告支持按照设定时间，向主管或相关人员发送安全报告，及时汇报系统安全状况。

定时任务报告信息包括任务名称，任务状态，报告周期，下次运行时间，描述，以及最近修改时间等。

安全管理员可以点击页面右上角的定时任务报告按钮，进入定时任务报告页面并参照[创建定时任务报告](#)章节，创建新的定时任务报告。

### 报告筛选条件/显示列

介绍适用的筛选条件/显示列。


下表罗列了适用的筛选条件/显示列，并逐条介绍其含义。

表 166: 筛选条件/显示列

筛选条件/显示列	解释
用户	用户的显示名称，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3） <ol style="list-style-type: none"> <li>AD 中的用户的Display Name</li> <li>自定义组织机构中的名称</li> <li>其它的显示IP地址（DC Agent、Logon Agent、其它）</li> </ol>
登录名	用于用户身份识别，按以下优先级顺序显示：（如1为空，则显示2，如2为空，则显示3）： <ol style="list-style-type: none"> <li>AD 中用户的Logon Name</li> <li>自定义组织机构中的用户名</li> <li>DC Agent、Logon Agent 中的名称</li> <li>其它为空</li> </ol>
唯一识别名	标识用户的唯一身份ID。 比如AD用户CN=haha,OU=QA,OU=R&D,OU=Staff,DC=skyguardmis,DC=com，或者DC Agent、Logon Agent中的FQDN名称
源IP	客户端IP地址
通道	事件所发生的通道或协议类型，比如 HTTP、HTTPS、FTP
动作	策略所对应的动作 动作包含：阻止、计时、提示、放行，每条策略只对应一个动作 动作优先级为：阻止 > 计时 > 提示 > 放行
域名	用户所在的域，可以为空
部门	用户所在的部门，可以为空




策略名称	事件命中的安全策略名称。 命中多个策略时，系统记录所有命中的策略名，包含内置的策略名称（策略名称是固定的）
URL分类	URL 所属的分类，比如：购物、IT等
URL风险类别	URL对应的风险类别
安全威胁类型	安全URL扫描的结果，比如挂马、网页篡改，或者内容扫描的病毒结果
文件类型	事件涉及的文件类型（扩展名、MIME TYPE），包含请求和应答中的文件类
URL主机名	用户访问的URL主机名，比如： <a href="http://www.skyguard.com.cn">www.skyguard.com.cn</a>
完整URL	完成的URL，包括协议和主机名 系统根据用户日志设置中的URL记录类型，决定是否记录部分或完整URL地址 设置方式：SWG管理 > 设置 > 日志设置 > URL记录方式  注：动作是阻止的访问，忽略此设置，始终记录完整的URL
目标IP	访问目标的IP地址，可能为空（原因是被阻止的请求，没有进行DNS解析）
端口	访问目标的端口号
设备名称	安全监控设备名称，如果是终端，则名称固定为：“注册终端”
关键字	记录命中策略中的关键字，可能有多个
文件名称	事件涉及的文件名称，可能有多个
浏览时长	访问该URL的时间，默认每个页面算为20秒
是否安全	根据风险级别的结果记录，风险级别为高、中、低，显示为不安全；风险级别为安全的情况下，显示为安全；
URL安全级别	自定义的风险级别
病毒名称	访问的内容被病毒引擎发现的病毒名称
城市	根据IP的经纬度，解析得到目标站点所在的城市
国家	根据IP的经纬度，解析得到目标站点所在的国家
位置	目标IP所在的经纬度
发送字节数	通过浏览器或其他方式访问网络发送的请求字节数
接收字节数	目标服务器对用户的响应字节数
总字节数	发送字节数和接收字节数的总和
应用类型	网络应用类型 应用类型目前包含浏览器、客户端、P2P、即时消息、流媒体应用类型5种。不在预置类型的，默认为空
应用名称	应用程序的名称，这些是厂家自身定义的

阻止类型	<p>动作被阻止的原因：阻止类型包含以下类型：</p> <ul style="list-style-type: none"> <li>黑名单阻止：因为命中了黑名单被阻止（全局策略）</li> <li>URL阻止：因URL分类或自定义URL被阻止（策略）</li> <li>文件类型阻止：URL里因包含文件类型被阻止（策略）</li> <li>关键字阻止：URL里因包含关键字被阻止（策略）</li> <li>计时阻止：用户被分配了上网时间配额，上网配额被用完时被阻止（策略）</li> <li>安全威胁阻止：网页内容由于含有病毒、或者因为安全URL检测，发现包含木马等安全风险内容而被阻止。（比如：挂马，篡改网页，钓鱼、病毒等）</li> <li>SSL事件阻止：因为访问的网站证书不合法被阻止(非策略动作，不用记录用户行为日志)</li> <li>DLP阻止：因为用户的访问数据命中DLP策略，并且被阻止</li> </ul> <p> 注：阻止类型记录的优先级：黑名单 &gt; SSL事件阻止 &gt; 安全威胁（安全URL检测） &gt; 计时 &gt; 关键字 &gt; 文件类型 &gt; URL &gt; 安全威胁（病毒） &gt; DLP阻止</p>
来源Risk Level	用户行为所属的Risk Level(高危、危险、严重、普通和较低)
方法	HTTP请求的方法
响应码	HTTP响应码
Cloud App	Cloud App名称
Cloud App分类	Cloud App 所属分类
Cloud App 信任级别	Cloud App 的信任级别（由后台给出，用户不可更改）
Cloud App 分值	Cloud App 的信用分值
Referrer URL	记录当前页面的来源地址，即是由哪个页面定向过来的
User Agent	HTTP报文中UserAgent信息，比如浏览器类型、版本，操作系统类型、版本等
会话阶段	用户行为日志生成时所在的HTTP会话阶段

## 移动安全设备监控

在监控邮件安全移动端页面查看设备监控信息。

在设备监控页面，将鼠标悬浮于移动安全网关MAG设备名称之上，出现图标并点击，可查看设备监控信息。

移动安全网关MAG设备监控信息包括系统资源和服务状态，并支持三种数据统计时段（1小时/24小时/7天）。

表 167: MAG系统资源信息

设备信息统计	解释
设备信息统计	统计当前设备的基本信息，如主机名称、IP地址、系统类型、CPU、物理内存、硬盘容量和网卡数量等。
CPU资源利用率	统计当前设备CPU使用率，包括用户占用、系统占用和空闲的CPU的比例。

设备信息统计	解释
网卡速率	统计当前网卡的发送和接收速率，以及总速率。
内存资源利用率	统计当前内存用于系统及应用、缓存的使用情况。
IO速率	设备输入接口和输出接口的读写速率。
硬盘资源使用情况	统计系统硬盘和数据硬盘的使用情况。

表 168: MAG服务状态信息

服务状态	解释
设备版本信息对比	当前UCSS作为基准设备，将注册设备各功能模块的版本信息与基准设备版本信息同步。可选同时同步或单独同步。
安全引擎负载统计	统计安全分析引擎CAE的负载状况。
分析请求数量统计	统计设备接收到的需要进行分析的请求数量。
命中事件统计	统计设备接收到的请求命中DLP策略产生事件的数量。
OCR引擎负载统计	统计OCR图像识别引擎的负载情况。
OCR队列状态统计	统计OCR图像识别引擎队列中等待分析和扫描超时的图片数量。
移动端服务负载统计	统计邮件安全移动端和设备安全移动端的负载状态。

## 移动安全设备管理

管理注册于UCSS的移动安全设备。

移动安全服务器注册到UCSS后，可以查看基本信息和服务状态，以及远程管理的相关服务。

### 设备

配置设备相关的选项页面。

该菜单包含设备相关的选项页面。

#### 系统信息

介绍设备的系统信息界面。

系统信息包括设备的基本信息和服务状态信息。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 系统信息菜单。

系统信息页面支持查看以下信息。

#### 设备信息

设备信息包括主机名称，IP地址，系统类型等只读的信息。

在此栏中，可以一键重启或关闭设备。

#### 系统信息

系统信息包括系统负载状态和各种系统服务的运行状态。

参考[系统服务介绍](#)，可以获得各种系统服务的基本介绍。

在此栏中，可以选择对某项服务进行重启、停止或启动，或对所有服务进行批量操作。

## MAG基本设置


介绍MAG基本设置的步骤。

MAG基本设置包括设备工作模式和同步设置。

1. 选择系统>设备管理>设备名称>设备>基本设置，滑动状态条选择启用设备（默认开启），进行基本配置。
2. 输入设备名称和描述，说明其用途。
3. 选择手动或自动同步系统时间：

自动同步	自动与UCSS设备同步系统时间，需设定每天的同步时间。
手动同步	点击立即同步，立刻触发一次与UCSS设备同步系统时间。

4. 点击保存，配置生效。

 注：高级设置请务必在在天空卫士™技术支持工程师的指导下修改。

## 授权许可

介绍如何管理设备的授权许可设置。

在系统 > 设备管理页面进行设备授权许可。

1. 选择系统 > 设备管理进入设备管理页面。点击要查看的设备，进入设备 > 授权许可页面。
2. 选择以下授权方式：


项目	描述
授权码	在线授权需输入授权码。
授权文件	离线授权需上传授权文件。

授权成功后，在当前页面显示授权信息如下：

表 169: 当前授权状态

设备编号	显示当前设备编号
授权号	显示当前设备所使用的授权号。
用户名称	显示License授予时的用户名称，一般为企业名称。
工作模式	显示当前设备工作模式，支持阻断和审计。
授权类型	显示授权类型，包括正式版本和测试版本。
功能模块列表	显示授权的功能模块，每个功能模块的已授权数量，当前状态和使用的有效期。

3. 点击保存，设置生效。

 提示：点击下载设备ID可下载设备ID信息为记事本格式，查询和授权License时可以使用该文件。

## 网络





配置网络相关的选项页面。

该菜单包含网络相关的选项页面。

## MAG网卡配置

介绍配置MAG网卡的步骤。


MAG设备有四块网卡：Mgmt负责管理设备，MTA提供邮件服务，P1和P2提供代理服务。

1. 选择系统>设备管理>设备名称>设备>网络>网卡配置,点击查看网卡的配置信息。
2. 点击编辑MTA、P1和P2的网卡设置，Mgmt网卡不可编辑。
3. 点击确定，网卡设置完成。
4. 选择设备网卡并输入网卡的默认网关。
5. 输入DNS服务器IP，点击添加于列表；点击删除列表中所选的DNS服务器。
6. 点击保存，配置生效。

## 路由设置

介绍管理路由设置的步骤。




在系统 > 设备管理页面设置路由。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 网络 > 路由页面。
2. 点击添加静态路由或策略路由：

静态路由	添加静态路由到主路由表中，不对源IP做限制，所有从本设备发起或者转发的数据包都将遵循此路由规则。
策略路由	只有本设备发起的数据包匹配此规则。

3. 输入目标网络IP地址、子掩码和网关（网关需要跟选中网卡的地址在同一个子网内）。
4. 选择网卡类型：Mgmt负责管理设备，MTA提供邮件服务，P1和P2提供代理服务（仅ASWG设备），Br0提供桥接服务（仅UCSG-DSG设备）。
5. 点击确认，添加路由到列表中。
6. 点击保存，设置生效。

表 170: 页面图标和行间操作按钮功能

	导出路由配置。
	导入路由配置。
	删除所选路由。

## 网卡绑定

介绍网卡绑定设置的步骤。

在系统 > 设备管理页面设置网卡绑定。

网卡绑定功能将两个或者更多的物理网卡绑定成一个虚拟网卡以提供负载均衡或者冗余。

1. 选择系统 > 设备管理进入设备管理页面后，点击您要查看的设备，进入设备 > 网络 > 网卡配置页面，选择要绑定的网卡，滑动状态条开启网卡绑定。
2. 选择绑定网卡的工作模式：

Active-Standby模式	主备方式，当一个网卡故障时另一个网卡接管所有工作。
------------------	---------------------------

Active-Active模式	双活方式，两个网卡同时工作，增加带宽的同时实现冗余。需要交换机支持聚合功能。
-----------------	--

➔ 注意: Bypass网卡仅支持Active-Active模式。

3. 点击保存，网卡绑定生效。

## 功能


配置功能相关的选项页面。

该菜单包含功能相关的选项页面。

### MAG协议配置

介绍MAG协议配置的步骤。

MAG支持ActiveSync、POP3和IMAP协议，检测并分析收件服务器的邮件流量。

1. 选择设备 > 功能 > 协议，点击  编辑协议。
2. 滑动状态条开启或关闭代理。
3. 选择是否启用加密支持。
4. 配置协议端口，端口与协议相对应并作相应的流量处理。
5. 选择工作模式：监控或阻断。监控不会干扰邮件的处理和接收流程，阻断即当邮件触发策略时根据策略动作进行放行或隔离，需要管理员手动释放被隔离的邮件。
6. 配置检测的最小字节数，少于此字节数不检测。
7. 设置移动设备连接，选择移动设备连接到MAG设备的网卡。
8. 设置收件服务器连接：
  - a) 输入接收邮件的服务器主机名或IP地址。
  - b) 输入该服务器对应的端口号。
  - c) 选择是否启用SSL连接。
  - d) 选择来源、目标和分析内容，进行流量分析。例如分析内网和外网间的ActiveSync、POP3和IMAP接收邮件流量。
9. 点击保存，协议设置成功。

### 网络对象

介绍设置网络对象功能的步骤。

在系统 > 设备管理页面设置网络对象功能。

在设置协议时可直接引用网络对象，过滤出需要检测的流量或过滤掉不需要检测的流量。



1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 网络对象页面。
2. 点击添加，新建网络对象。
3. 输入网络对象名称。
4. 输入网络对象包含的IP或IP段，点击  添加到列表。
5. 输入排除在网络对象外的IP或IP段，点击  添加到列表。
6. 点击确定，添加成功。

表 171: 页面图标和行间操作按钮功能

	修改网络对象。
	删除所选网络对象。

## OCR功能

介绍管理OCR功能的步骤。

在系统 > 设备管理页面设置OCR功能。

OCR识别图像功能支持本地和外置OCR服务器，外置OCR服务器可以解析网络流量中的图片内容并进行DLP分析，提高了对大量图片内容的处理速率，减轻系统资源消耗。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > OCR页面。
2. 滑动状态条，开启OCR功能。
3. 选择OCR工作的精确度，平衡系统资源消耗：

快速	效率高但是精确度低。
平衡	兼顾效率和精确度。
精确	精确度高但是效率低。


4. 选择OCR识别的语言，包括简体中文、繁体中文和英文。
5. 设置OCR图像识别引擎检测文件的大小限制，0表示不限制大小。
6. 选择OCR服务器，包括本地OCR引擎和远程OCR引擎。
7. 点击保存，设置生效。

## 全局例外

介绍设置全局例外功能的步骤。

在系统 > 设备管理页面设置全局例外功能。

全局例外针对不同协议进行集中配置来源和目标，代理服务器透传列表中的相关配置。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 全局例外页面,点击  新建全局例外并添加规则。
2. 输入全局例外名称，说明其作用。
3. 选择是否启用该全局例外功能。
4. 输入来源IP/IP段，如果设置全部来源即为0.0.0.0-255.255.255.255。

 注：ICAP Server的全局例外使用的来源IP/IP段为172.16.1.1, 192.168.0.1-192.168.0.200。

5. 输入目的IP/IP段或域名，全部域名即为“所有”。

 注：

- 域名方式仅适用于HTTP和HTTPS协议。
- ICAP Server的全局例外使用的目的IP/IP段为220.181.112.244, 220.181.113.100-220.181.113.120。也支持正则表达式的添加方式。

6. 根据应用场景，选择相应的传输协议。
7. 点击保存，设置生效。

表 172: 页面图标和行间操作按钮功能

图标	解释
	启用所选全局例外。
	禁用所选全局例外。
	删除所选全局例外。

图标	解释
	导入全局例外文件，可以参考模板生成，导入文件样例文件名称为“全局例外.json”。
	导出全局例外文件到本地。

### MAG证书设置


介绍MAG证书设置的步骤。

MAG证书包括站点证书，作为客户端和原始服务器站点之间的中间站，点击导入证书按钮导入站点证书。点击下载证书按钮下载证书到本地。

### 安全传输功能设置

在系统 > 设备管理页面设置安全传输功能。

配置安全网关可以对网络传输的内容进行加密和内容分析，防止终端用户访问非法URL而引发数据泄密。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > 安全传输页面。
2. 滑动状态条开启安全传输功能。
3. 输入安全传输连接端口号。
4. 选择用户鉴定方式，支持用户名和证书两种方式。
5. 在凭证证书区域，点击  添加或编辑移动安全网关。
  - a) 输入Web安全网关IP地址。
  - b) 输入网关端口号。
  - c) 设置网关优先级。
  - d) 点击保存，Web网关添加至列表。
6. 点击保存，设置生效。

## 认证

介绍认证设置的步骤。

在系统 > 设备管理页面进行认证设置。

ASWG认证功能可以更准确的识别上网用户的身份，用户的上网请求会匹配合适的认证规则完成认证。目前ASWG支持的认证方式有：本地认证、AD LDAP、Open LDAP、IWA等认证方式。


选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证页面，基本配置如下：

- 认证失败设置
- 认证冲突设置
- 认证缓存设置
- 认证缓存时间设置
- 其它设置

### MAG认证服务器

在系统 > 设备管理页面设置移动安全网关MAG认证。



配置移动安全网关MAG认证服务器，当前版本支持Active Directory服务器类型。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 认证 > 认证服务器页面。
2. 点击  添加认证服务器。
3. 选择基本设置选项卡，进行如下配置：
  - a) 输入认证服务器名称。
  - b) 选择启用或禁用该认证服务器。



- c) 选择认证服务器类型。
- d) 选择服务器来源，用户可新建服务器或从用户目录中选择服务器。  
如果用户新建服务器，配置如下信息：
  - 1. 输入认证服务器的地址。
  - 2. 设置认证服务器的端口号。
  - 3. 输入登录服务器的用户名。
  - 4. 输入登录服务器的密码。
  - 5. 输入目录根节点。如果服务器来源选择的是用户目录，系统会自动读取此用户目录的根节点。
  - 6. 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
  - 7. 选择是否使用SSL安全连接，SSL安全连接提高数据传输的安全性。
- 4. 选择高级设置选项卡，选择是否启用自定义过滤。启用后，进行如下配置：
  - a) 选择登录名类型，即设置首要过滤条件。
  - b) 设置显示列，即填写显示名、姓、名和描述。
  - c) 根据用户项进行过滤，即根据组织单元、组和成员过滤用户。
- 5. 点击保存，认证服务器添加到列表。
- 6. 再次点击保存，认证服务器设置生效。

表 173: 页面图标和行间操作按钮功能

图标	功能
	编辑认证服务器配置信息。
	删除所选认证服务器。

## 其他

其他的选项页面。

该菜单包含其他的选项页面。

### SNMP功能

介绍管理SNMP功能设置的步骤。

在系统 > 设备管理页面设置SNMP功能。

设备支持外部应用访问SNMP服务器来收集设备信息。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > SNMP页面，设置SNMP功能。。
2. 滑动状态条，开启SNMP功能。
3. 选择SNMP query版本，可以设置为v1或v2c。
4. 输入SNMP的团体名，即SNMP的用户名或密码，只允许使用此团体名访问SNMP服务器。
5. 选择以下SNMP的连接方式：

任何IP	任何IP地址都可访问SNMP。
仅限于下列IP	输入IP地址，点击  添加到可访问SNMP的IP列表。

6. 点击保存，设置生效。



## 收集日志

介绍配置收集日志功能的步骤。

在系统 > 设备管理页面设置收集日志功能。

设备支持收集系统日志信息，了解系统运行状态。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 收集日志页面，设置收集日志功能。
2. 选择收集日志的时间段。
3. 选择收集日志的类型。
4. 点击收集日志，收集所设定日期和指定类型的日志，显示于日志收集历史列表中。

点击  可将得收集得日志文件下载到本地；点击  可删除所选日志文件。

## 备份和恢复

介绍备份/恢复功能设置的步骤。

在系统 > 设备管理页面设置备份和恢复功能。

UCSS设备支持立即备份和立即恢复系统配置，包括配置信息、证据文件、邮件、网络及主机信息等，并支持定期备份功能。

1. 选择设备 > 其他 > 备份,进入备份或恢复页面。
2. 点击定期备份启动定期备份，设置定期备份的时间。
3. 点击备份设置，选择以下备份方式和备份内容：

备份至本地	选择备份至本地设备，设置备份日志数量的最大值，若本地保存数量大于设置的最大值则会删除最早的备份。
备份至远程	支持备份至Samba服务器和NFS服务器，需输入服务器的IP/主机名、文件夹路径和用户信息，并进行测试连接。

备份记录会出现在备份历史中，点击删除可删除所选备份。

4. 点击保存，设置生效。

## 升级和补丁

介绍升级/补丁功能设置的步骤。

在系统 > 设备管理页面设置升级和补丁功能。

设备支持在线版本升级和补丁安装，但升级不支持版本回退。选择系统 > 设备管理进入设备管理页面后。点击要查看的设备，进入设备 > 其他 > 升级/补丁页面，然后进行升级或补丁设置。

### • 升级

选择升级选项卡，点击检查更新连接天空卫士的安装包服务器，获取安装包列表，选择安装包下载并安装。如果用户设备无法直接访问互联网，可通过代理服务器配置使用代理进行检查更新，点击代理服务器配置代理服务器。

点击上传安装包从本地上传升级安装包。

### • 补丁

选择不定选项卡，查看当前版本和可用补丁。点击上传安装包从本地上传补丁安装包，安装之后可以选择卸载。

## 远程控制

介绍远程控制功能设置的步骤。

在系统 > 设备管理页面设置远程控制功能。

设备启用SSH连接后，可通过SSH执行远程设备故障排查。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 远程控制页面。
2. 选择是否启用以下功能：

启用远程控制	启用远程控制以后可以开启SSH端口并使用设备管理账号（例如ucssadmin帐号）登录设备进行命令操作。
启用技术支持模块	启用技术模块之后，获取6位密码。该密码需要提供给天空卫士进行解密后使用。
启用超时限制	设置在指定时间之后自动关闭远程控制。

3. 点击保存，设置生效。



注：

远程访问记录可在远程访问历史中查询。

## 系统工具

介绍系统工具设置的步骤。

在系统 > 设备管理页面设置系统工具。

系统工具预置多条CLI命令，即使不连接后台时也可以使用系统工具进行故障排查，并显示执行结果。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，从下拉框中选择索要执行的命令。
2. 输入出现故障的设备主机名或IP，点击执行开始运行故障排查命令，点击停止可终止执行命令。执行结果显示于黑色屏幕中。



---

# 第 8 章

---

## Hybrid云安全

---

内容:

- [混合云Hybrid](#)

介绍天空卫士™云安全解决方案。

天空卫士™安全鳄®统一内容安全UCS ( UCS ) 解决方案采用云端虚拟机设备提供高性价比的Hybrid云安全解决方案。

## 混合云Hybrid

介绍混合云安全解决方案。

DLP的混合云部署，以总部的UCSS物理设备为基础，采用云端虚拟机为分支机构提供数据防泄漏保护，通过云端虚拟机同步策略和用户目录等，并将检测到的事件和证据等数据返回给总部的UCSS系统，进行统一管理。目前仅支持阿里云的部署环境。


### 配置云平台虚拟机

介绍配置云平台虚拟机的步骤。

天空卫士™统一内容安全UCS解决方案允许安全管理员在管理平台上虚拟安全设备，并进行统一的设备管理和安全策略部署。

按照如下步骤配置在云平台中创建的虚拟机设备。


1. 选择系统 > Hybrid进入虚拟机管理页面。
2. 点击阿里云图标，进入配置页面。

 提示：系统对于页面的各个配置选项提供了详细的配置项描述，点击配置项说明按钮，即可跳转至描述页面。

3. 选择以下设备类型：

设备类型	功能介绍
Hybrid UCSG	通过在路由器或防火墙配置GRE通道，将指定的流量导入阿里云虚拟机进行DLP保护。
Hybrid ASWG	通过阿里云虚拟UCSG-ASWG设备的公网IP设置显示代理，也可以通过在路由器或防火墙配置GRE通道，将指定的流量导入阿里云虚拟机。
Hybrid UCSS Lite	为漫游用户（roaming user）的终端提供实时的策略同步和事件上报。


4. 输入设备名称。
5. 输入虚拟主机实例ID，即阿里云虚拟主机的ID，通过这个ID查找用户部署于阿里云的天空卫士设备。
6. 输入阿里云API认证使用的Key和Secret。
7. 设置公网IP地址，用于云端的虚拟主机与UCSS设备通信。
8. 设备类型为Hybrid DSG和Hybrid ASWG是，需进行以下网络配置：



名称	网络名称
公司公网出口IP	输入公网出口IP地址，用于建立GRE tunnel。
内部网络	点击  添加内部网络IP地址，在云端做策略路由时，属于该网络的数据会使用与其相应的GRE tunnel。

9. 点击保存，混合云部署设置成功。

点击更多，显示混合云部署详细信息。

页面图标和行间操作按钮功能

按钮	介绍
	编辑Hybrid配置。

按钮	介绍
	跳转到设备管理页面。
	删除云端设备。





---

# 第 9 章

---

## **GatorCloud云安全**

---

内容:

- [GatorCloud云安全](#)
- [UCWI设备监控](#)
- [UCWI设备管理](#)
- [WebService API 调用指南](#)

介绍天空卫士™云安全解决方案。

天空卫士™安全鳄®统一内容安全UCS ( UCS ) 解决方案采用统一内容安全审查平台UCWI作为其云安全审查解决方案，以帮助企业和机构应对散布在企业云应用中的各种安全威胁。

## GatorCloud云安全

---

介绍GatorCloud云安全解决方案的相关信息。

### 关于GatorCloud云安全

为了提供云环境下威胁和数据安全防护，并有效地保护企业存放在云端的数据，GatorCloud云安全解决方案提供了针对云的数据保护，形成以集中的企业安全策略云平台为核心，以具有解析不同数据通道能力的各种Inspectors为安全执行者（Enforcer）的统一云安全解决方案。

### 组件介绍

GatorCloud云安全解决方案包括以下的组件：

- GatorCloud 云安全管理平台：构建多租户的GatorCloud云安全管理平台，以减少企业各种类型的安全设备复杂的维护现状，并提供最高级别的集中安全管控。
- GatorCloud 安全处理组件（Inspector）：由企业客户自主拥有并部署在云或内部网络中，从GatorCloud云安全管理平台同步该企业客户的Web安全策略、数据安全策略、威胁防护策略和UEBA用户行为分析策略。

### GatorCloud 安全处理组件

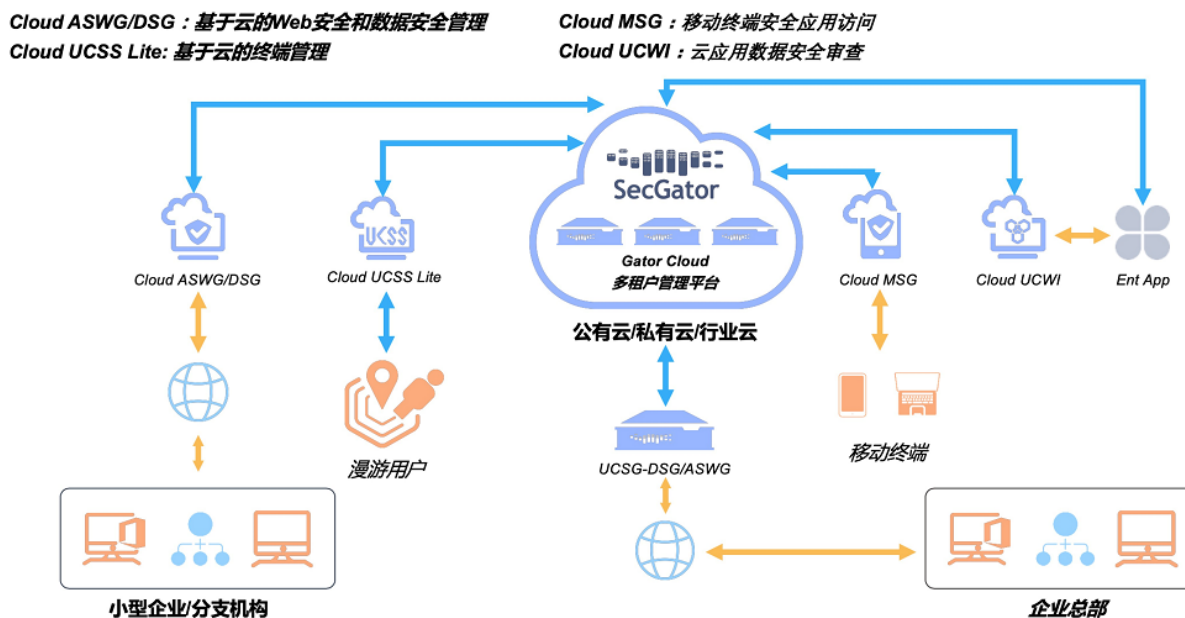
不同的安全组件（Inspector）负责分析处理不同通道的数据（Web、Email、FTP、终端、移动设备或各种云应用等），并根据安全策略执行相应的动作（允许、阻断、删除附件、通知、告警、记录日志等）。

GatorCloud 安全处理组件主要有以下几种形态。

- Cloud ASWG：为小型企业或者大型企业的分支机构提供安全互联网访问服务，包括对入向流量恶意链接、病毒、木马的查杀和出向的敏感内容检测功能。
- Cloud UCSS Lite：提供数据安全终端管理功能，每个安装了天空卫士数据安全终端软件的终端，都会在连上互联网的时候注册到Cloud UCSS Lite上，获取最新的企业数据安全策略和上传最新的数据安全事件，有效保护在互联网上散落的企业终端电脑。
- Cloud MSG：提供企业应用的移动终端安全接入功能，当使用移动终端上的APP访问企业部署在云端的内部服务时，通过Cloud MSG形成内部通道，让企业应用的后台无需暴露在互联网上，同时运行在移动终端上的安全域将会严格保护在移动端的企业数据。
- Cloud UCWI：支持对第三方应用或者设备提供内容安全技术集成，即企业部署于云端的各类应用后台都可以按照预定的Restful API接口将相关数据发送至UCWI进行内容安全检查，UCWI将向请求发起端返回内容分析结果。

### GatorCloud 网络拓扑图

下图介绍GatorCloud云安全解决方案的网络拓扑结构



## UCWI设备监控

介绍如何监控统一内容安全审查平台UCWI安全设备。

Hybrid云安全监控记录所有统一内容安全审查平台UCWI的信息。

### UCWI监控

查看UCWI监控的相关信息。

在监控 > UCWI监控页面查看UCWI监控信息。

## UCWI设备管理

介绍统一内容安全审查平台UCWI云安全设备管理。

本章介绍如何管理天空卫士™云安全设备-统一内容安全审查平台UCWI。

### 设备

配置设备相关的选项页面。

该菜单包含设备相关的选项页面。

### 系统信息

介绍设备的系统信息界面。

系统信息包括设备的基本信息和服务状态信息。

选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 系统信息菜单。

系统信息页面支持查看以下信息。

### 设备信息

设备信息包括主机名称，IP地址，系统类型等只读的信息。

在此栏中，可以一键重启或关闭设备。

### 系统信息

系统信息包括系统负载状态和各种系统服务的运行状态。

参考[系统服务介绍](#)，可以获得各种系统服务的基本介绍。

在此栏中，可以选择对某项服务进行重启、停止或启动，或对所有服务进行批量操作。


### UCWI基本设置

UCWI基本设置包括设备名称、时区和时间设置。只有UCSS设备可设置时间及时区信息，其他注册设备自动从UCSS同步时间。

1. 选择系统 > 设备管理进入设备管理页面。
2. 点击设备名称>设备>基本设置，滑动状态条启用设备（默认开启），进行基本配置。
3. 输入设备名称和描述，说明其用途。
4. 选择手动或自动同步系统时间：

自动同步	自动与UCSS设备同步系统时间，需设定每天的同步时间。
手动同步	点击立即同步，立刻触发一次与UCSS设备同步系统时间。

5. 点击保存，配置生效。

 注：高级设置请务必在在天空卫士™技术支持工程师的指导下修改。

### 授权许可

介绍如何管理设备的授权许可设置。

在系统 > 设备管理页面进行设备授权许可。

1. 选择系统 > 设备管理进入设备管理页面。点击要查看的设备，进入设备 > 授权许可页面。
2. 选择以下授权方式：

项目	描述
授权码	在线授权需输入授权码。
授权文件	离线授权需上传授权文件。

授权成功后，在当前页面显示授权信息如下：

表 174: 当前授权状态

设备编号	显示当前设备编号
授权号	显示当前设备所使用的授权号。
用户名称	显示License授予时的用户名称，一般为企业名称。
工作模式	显示当前设备工作模式，支持阻断和审计。
授权类型	显示授权类型，包括正式版本和测试版本。
功能模块列表	显示授权的功能模块，每个功能模块的已授权数量，当前状态和使用的有效期。

3. 点击保存，设置生效。



提示：点击下载设备ID可下载设备ID信息为记事本格式，查询和授权License时可以使用该文件。

## 功能

配置功能相关的选项页面。

该菜单包含功能相关的选项页面。

### OCR功能

介绍管理OCR功能的步骤。

在系统 > 设备管理页面设置OCR功能。

OCR识别图像功能支持本地和外置OCR服务器，外置OCR服务器可以解析网络流量中的图片内容并进行DLP分析，提高了对大量图片内容的处理速率，减轻系统资源消耗。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 功能 > OCR页面。
2. 滑动状态条，开启OCR功能。
3. 选择OCR工作的精确度，平衡系统资源消耗：

快速	效率高但是精确度低。
平衡	兼顾效率和精确度。
精确	精确度高但是效率低。

4. 选择OCR识别的语言，包括简体中文、繁体中文和英文。
5. 设置OCR图像识别引擎检测文件的大小限制，0表示不限制大小。
6. 选择OCR服务器，包括本地OCR引擎和远程OCR引擎。
7. 点击保存，设置生效。

## 其他

其他的选项页面。

该菜单包含其他的选项页面。

### SNMP功能

介绍管理SNMP功能设置的步骤。

在系统 > 设备管理页面设置SNMP功能。

设备支持外部应用访问SNMP服务器来收集设备信息。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > SNMP页面，设置SNMP功能。。

2. 滑动状态条，开启SNMP功能。
3. 选择SNMP query版本，可以设置为v1或v2c。
4. 输入SNMP的团体名，即SNMP的用户名或密码，只允许使用此团体名访问SNMP服务器。
5. 选择以下SNMP的连接方式：

任何IP	任何IP地址都可访问SNMP。
仅限于下列IP	输入IP地址，点击  添加到可访问SNMP的IP列表。

6. 点击保存，设置生效。

#### 收集日志

介绍配置收集日志功能的步骤。

在系统 > 设备管理页面设置收集日志功能。

设备支持收集系统日志信息，了解系统运行状态。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 收集日志页面，设置收集日志功能。
2. 选择收集日志的时间段。
3. 选择收集日志的类型。
4. 点击收集日志，收集所设定日期和指定类型的日志，显示于日志收集历史列表中。

点击 可将得收集得日志文件下载到本地；点击 可删除所选日志文件。

#### 备份和恢复

介绍备份/恢复功能设置的步骤。

在系统 > 设备管理页面设置备份和恢复功能。

UCSS设备支持立即备份和立即恢复系统配置，包括配置信息、证据文件、邮件、网络及主机信息等，并支持定期备份功能。

1. 选择设备 > 其他 > 备份,进入备份或恢复页面。
2. 点击定期备份启动定期备份，设置定期备份的时间。
3. 点击备份设置，选择以下备份方式和备份内容：

备份至本地	选择备份至本地设备，设置备份日志数量的最大值，若本地保存数量大于设置的最大值则会删除最早的备份。
备份至远程	支持备份至Samba服务器和NFS服务器，需输入服务器的IP/主机名、文件夹路径和用户信息，并进行测试连接。

备份记录会出现在备份历史中，点击删除可删除所选备份。

4. 点击保存，设置生效。

#### 升级和补丁

介绍升级/补丁功能设置的步骤。

在系统 > 设备管理页面设置升级和补丁功能。

设备支持在线版本升级和补丁安装，但升级不支持版本回退。选择系统 > 设备管理进入设备管理页面后。点击要查看的设备，进入设备 > 其他 > 升级/补丁页面，然后进行升级或补丁设置。

- 升级

选择升级选项卡，点击检查更新连接天空卫士的安装包服务器，获取安装包列表，选择安装包下载并安装。如果用户设备无法直接访问互联网，可通过代理服务器配置使用代理进行检查更新，点击代理服务器配置代理服务器。

点击上传安装包从本地上传升级安装包。

- 补丁

选择不定选项卡，查看当前版本和可用补丁。点击上传安装包从本地上传补丁安装包，安装之后可以选择卸载。

### 远程控制

介绍远程控制功能设置的步骤。

在系统 > 设备管理页面设置远程控制功能。

设备启用SSH连接后，可通过SSH执行远程设备故障排查。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 远程控制页面。
2. 选择是否启用以下功能：

启用远程控制	启用远程控制以后可以开启SSH端口并使用设备管理账号（例如ucssadmin帐号）登录设备进行命令操作。
启用技术支持模块	启用技术模块之后，获取6位密码。该密码需要提供给天空卫士进行解密后使用。
启用超时限制	设置在指定时间之后自动关闭远程控制。

3. 点击保存，设置生效。



注：

远程访问记录可在远程访问历史中查询。

### 系统工具

介绍系统工具设置的步骤。

在系统 > 设备管理页面设置系统工具。

系统工具预置多条CLI命令，即使不连接后台时也可以使用系统工具进行故障排查，并显示执行结果。

1. 选择系统 > 设备管理进入设备管理页面后，点击要查看的设备，进入设备 > 其他 > 系统工具页面，从下拉框中选择索要执行的命令。
2. 输入出现故障的设备主机名或IP，点击执行开始运行故障排查命令，点击停止可终止执行命令。执行结果显示于黑色屏幕中。

## WebService API 调用指南

本章介绍了如何用预置的Python脚本调用WebService API。

WebService API为统一内容安全审查平台UCWT调用RESTful API服务提供指导，为客户的内部业务应用程序提供数据安全API。

## 概述

介绍统一内容安全审查平台UCWI。

### 介绍

随着企业数字化转型的不断推进，各种业务逐渐被数字化。相应的，各种业务系统得到广泛应用。为了应对不断扩大的风险暴露面，企业面临经济，人员，理念等各方面的压力。

天空卫士运用其统一内容安全审查平台UCWI提供统一内容检查服务，作为天空卫士一个创新产品，给企业的信息安全建设带来了新的选择。

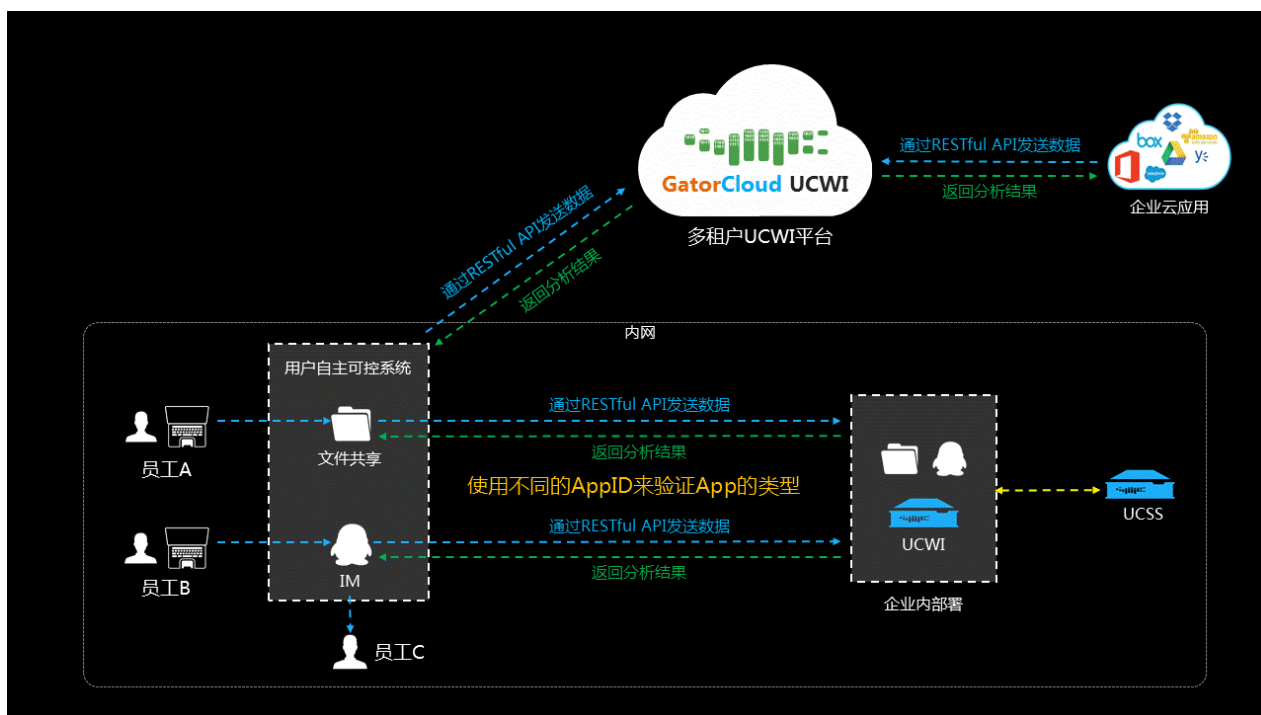
SkyGuard统一内容Web服务检测平台为客户的内部业务应用程序了提供值得信赖的数据安全API，优雅地解决了这个问题。客户自己的业务应用程序开发团队比其他人更清楚地知道他们的数据应该如何存储、移动和使用，因此他们很容易在业务应用程序中找到调用SkyGuard UCWI API的适当位置，而无需了解复杂的公司范围内数据安全策略。另一方面，客户的数据安全管理团队能够专注于数据安全和数据合规，而无需了解复杂的业务数据处理逻辑。

### 产品特点

UCWI产品主要有以特点：

- 简单但功能强大的RESTful API
- 支持同步和异步模式
- 无缝集成到业务流程中
- 共享与SkyGuard高级Web安全网关ASWG和SkyGuard数据安全网关DSG相同的数据安全策略集
- 业内最高性能: 高达600 Mbps的办公文件处理能力
- 支持多种数据检测技术: 指纹、机器学习、正则表达式、关键字和词典
- 支持上千种文件格式：包括Word，PDF，CAD等
- 快速、高精度的OCR
- 支持大多数压缩文件格式
- 内置丰富的数据模板：GDPR PII，PCI，PHI等。
- 支持结构化数据（数据库）和非结构化数据（文件）

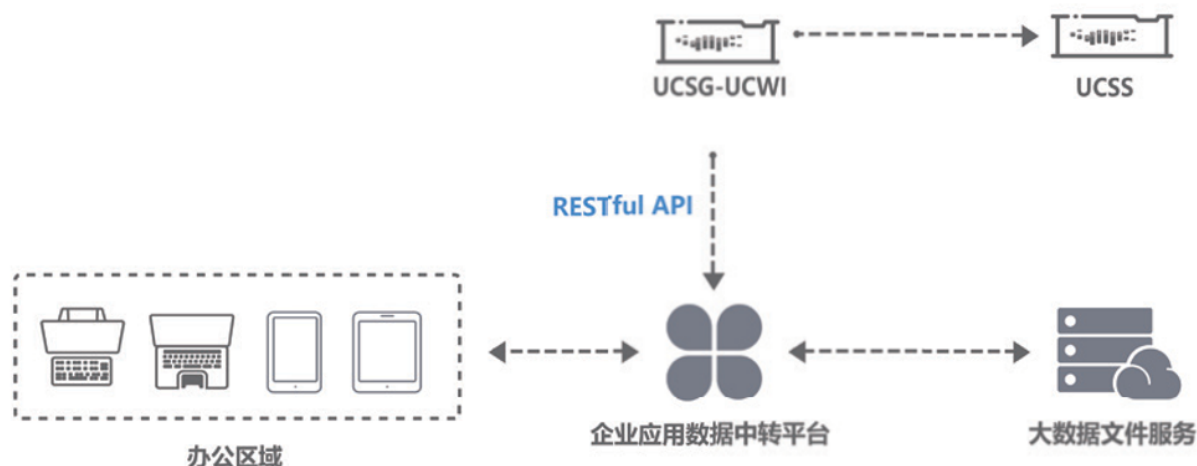




### 典型部署-大数据处理平台

介绍大数据平台部署的相关信息。

支持大数据处理平台的典型部署：



- 数据处理应用程序之一，数据收集器，从数据生成器收集数据，并将原始数据存储在一个数据存储中。另一个应用程序（数据清理器）删除敏感信息或对其进行编辑，并将经过清理的数据存储在另一个数据存储中。
- 该部署假定办公室中只有少数特权用户可以访问原始数据，而其他办公室用户只能访问经过清理的数据。此外，平台政策还规定，包含地理位置信息的数据，即使经过处理，也不应发布给非成员数据使用者。但是，由于所有应用程序都可以访问这两个数据存储，因此在处理数据时遵守上述规则成为应用程序开发人员的负担。应用程序逻辑中一旦出现错误，非特权用户长时间访问一些未经处理的原始数据，而不会触发警告，导致某些交付应用程序的数据由于无法识别地理位置信息，交付了包含外部用户数据的地理位置。
- 随着SkyGuard UCWI的部署，平台数据安全团队创建并维护UCSS上的所有数据安全策略，该团队会自动将这些策略发布到UCWI。应用程序开发人员只需在关键数据传输点提交具有适当UCWI API的数据，以确保不会向错误的收件人传递不适当的数据。因此，在一段时间内，会收到重复的DLP事件警告，当数据被传递给无特权用户时，敏感数据会被阻止，开发人员意识到他们在代码中出现了错误，并在将数据呈现给无特权用户，于是他们从原始数据存储中读取数据用户。此外，应用程序开发人员在向外部用户发送数据时，可以使用UCWI API筛选出包含地理位置信息的数据，从而消除编程错误的可能。

#### 技术功能列表

列举产品的技术功能。

#### UCWI 支持多种内容检查接口模式

- 同步接口：客户端通过 RESTful接口将内容提交到UCWI，等待UCWI分析完毕后返回检查结果
- 异步接口：客户端通过 RESTful接口将内容提交到UCWI，无需等待分析结果。事后可以通过事件查询指令查询检查结果，通过证据文件查询指令获取对应的证据文件
- 外部检测接口：对于S3类型外部存储，客户端将被检查URL提交到UCWI，UCWI主动去分析提交的 URL 所对应的数据存储，并将检查结果返回给客户端

#### UCWI 支持多种内容检测方式

- 文件解析：支持上千种文件格式解析，支持对压缩文件、嵌套文件的解析
- 图片 OCR：可以对包含在图片中的文字进行识别和分析
- 内容分析：支持关键词、字典、正则表达式、机器学习、文件指纹等多种内容对比方式

## 典型应用场景

介绍WebService API的典型应用场景。

### 数据中转平台

通过简单的接口调用，数据中转平台将业务数据通过 API 发送给 UCWI，解决了以往人工无法完成的任务：

- 海量数据的脱敏检查：审查脱敏数据内容是否脱敏合格，防止敏感 / 价值数据流入办公 / 研发区域
- 检查数据异常传输，对异常的数据下载进行监控
- 对中转数据内容进行识别，帮助管理者掌控数据资源传输情况

### 办公平台/ 业务系统对接

通过与企业系统对接，使业务系统真正有了对自身处理的数据进行内容感知的能力，使企业业务流程更加精确、合理。同时为业务部门提供了数据追踪的能力：

- 相关平台的数据传输的内容控制：避免内容与标题不一致，防止数据资产流失
- 审批可监控：检查审批事件与流转数据的真实性，避免恶意敏感数据外泄
- 流转数据监控：记录敏感数据通过业务系统通过正常通道流转，数据使用可追溯

## WebService API快速配置指南

统一内容安全审查平台UCWI为客户的内部业务应用程序提供数据安全API。

应用系统通过调用RESTful API，将需要检查的内容发送到UCWI。

UCWI通过内置的DLP数据安全策略对内容进行分析，并向应用系统返回检测内容的安全等级，命中策略等信息，应用系统可以根据这些信息对检测内容执行存储、下载或者共享等操作。

管理员可以按照如下步骤快速使用本产品：

- [创建云应用APP](#)
- [获取API认证信息](#)
- [配置DLP策略](#)
- [调用RESTful API服务](#)

### 创建WebService应用

介绍如何创建WebService应用。

创建DLP策略元素-WebService应用，并获得WebService应用的唯一ID。

1. 选择DLP管理 > 策略元素 > WebService应用，点击添加，创建WebService应用。
2. 输入WebService应用的名称和描述信息，表明WebService应用的作用。
3. 点击保存，新建的WebService应用显示在列表中，并显示该WebService应用的唯一ID（添加时ID由系统自动生成）。

### 通过管理平台获取认证信息


介绍如何通过管理平台获取认证信息。

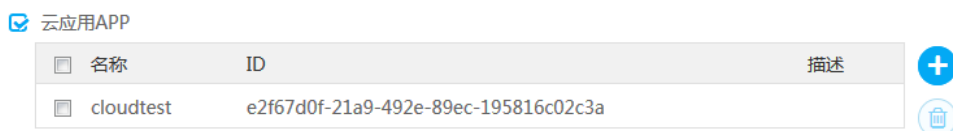
按照以下步骤在管理平台上访问UCWI设备，获取调用API所需要的 授权许可认证信息。


1. 登陆管理平台。
2. 选择系统 > 设备管理进入设备管理页面。
3. 点击已注册的UCWI设备，在左侧菜单栏选择设备 > 授权许可。
4. 点击右上角认证信息按钮，显示API需要授权许可认证信息。

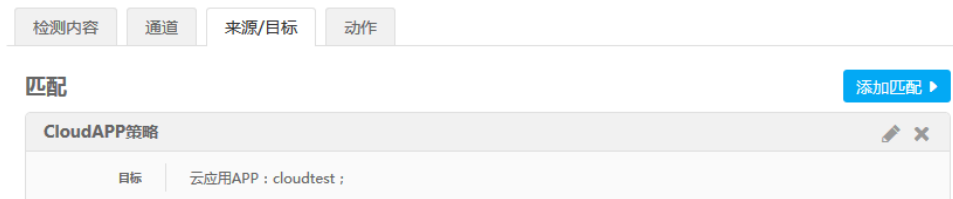
### 配置DLP策略

创建DLP策略，添加云应用APP作为策略目标。


1. 选择DLP管理 > 策略，点击添加，添加新策略。
2. 输入策略名称和描述，表明该策略用于API调用。
3. 设置策略归属的策略组，默认设置为默认策略组。
4. 设置策略所属的策略等级，即将策略分级，可设置为默认等级。
5. 启用新建策略，默认为启用。
6. 指定新建策略类型为DLP策略。
7. 点击检测内容选项卡，添加DLP规则元素的匹配或例外项。
8. 点击通道选项卡，勾选网络检测通道中的云应用APP。
9. 点击来源/目标选项卡，在匹配区域选择目标，将云应用APP设置为策略的目标。
  - a) 输入目标的名称和描述。
  - b) 添加目标，选择添加目标，勾选云应用APP。
  - c) 点击 ，弹出云应用APP选择窗口，选择创建的云应用APP。



- d) 点击  添加到右侧有效区。
- e) 点击确认添加目标列表，用于DLP检测。
- f) 点击确定，策略目标添加成功。



10. 点击动作选项卡，设置事件命中策略后，对其所执行的动作。
11. 点击保存,新建策略添加到列表中。

 提示: 如果想了解关于创建策略的详细信息，请参考《天空卫士™安全鳄®统一内容安全UCS管理指南》中DLP策略相关章节。

### 调用RESTful API服务

统一内容安全审查平台UCWI支持通过WebService API调用检测内容，并返回策略检测结果。

### WebService API调用检测内容

操作步骤如下：

1. WebService API基于密钥 HMAC (Hash Message Authentication Code) 的自定义 HTTP进行身份验证。  
用于认证的AccessKey以及Inspector ID的获取方式，请参考[获取API认证信息](#)章节的内容。
2. 发送请求至DLP数据防泄漏模块，并获取检测通道信息。
3. 发送检测内容至WebService Inspector。
4. 返回事件详情和证据文件等策略检测信息。

## 资源获取接口

介绍资源获取接口的基本信息。

请求方式

GET

URL

接口地址

使用以下URL接口地址进行调用。

URL定义规则为：

/skg/<API版本号>/<功能模块>/<资源名称>/<资源名...>

请求参数

表 175: 请求参数表

参数名称	参数位置	是否必须	描述
<API版本号>	URL参数	是	天空卫士™官方发布的RESTful API版本号。
<功能模块>	URL参数	是	当前版本支持调用的功能模块名称。详见 <a href="#">功能模块</a> 。
<资源名称>	URL参数	是	当前版本支持调用的资源名称。详见 <a href="#">资源名称</a> 。

功能模块：

- dlp - 数据防泄漏DLP服务
- swg - Web数据安全服务

资源名称：

- channel - 通道

 注：若功能模块为dlp则资源ID包括包括web, email, 和cloudapp。

- report - 报告
- incident - 事件
- forensics - 证据文件

子资源：在URL中显示为<资源名称>/<子资源名称>。资源按照级别依次排列。可通过列举资源名称获取所有资源名。

返回结果

成功调用该接口，系统将返回json格式的字符串。

获取通道

介绍获取通道的接口调用方式。

接口介绍

该接口用于获取通道类型。

获取通道类型列表后，后续可以通过获取通道详细信息接口查询某个通道类型的详细信息。具体查阅[获取通道详细信息](#)。

### 请求方式

GET  
URL

### 接口地址

使用以下URL接口地址进行调用。

GET /skg/v1/dlp/channel

### 返回结果

成功调用该接口，系统将返回以下参数。

参数	描述
channels	列表显示当前连接的所有通道
channels.name	通道名称： <ul style="list-style-type: none"> <li>web - 网络通道</li> <li>email - 邮件通道</li> <li>cloudapp - 云应用通道</li> </ul>
channels.description	通道描述 - 自定义的对于该通道的描述信息

### 返回示例

```
{
  "channels": [
    {
      "name": "web",
      "description": "Web channel"
    },
    {
      "name": "email",
      "description": "Email channel"
    },
    {
      "name": "cloudapp",
      "description": "Cloud App channel"
    }
  ]
}
```

### 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

### 获取通道详细信息

介绍获取通道详细信息的接口调用方式。

### 接口介绍

该接口用于获取某个类型通道的详细信息。

### 请求方式

GET  
URL

### 接口地址

使用以下URL接口地址进行调用。

/skg/v1/dlp/channel/<通道类型>



注：你可以使用[获取通道](#)接口查看当前连接的所有通道类型。

### 请求参数

参数名称	参数位置	是否必须	描述
<通道类型>	URL参数	是	指定一个通道类型，你可以使用 <a href="#">获取通道</a> 接口查看所有通道类型。

### 请求示例

以下示例为调用接口请求获取云应用(Cloud App)通道的详细信息。

```
GET /skg/v1/dlp/channel/cloudapp
```

### 返回结果

返回结果中包含以下参数：

名称	描述
<通道类型>	列表显示当前通道中所有的App。
<通道类型>.name	当前通道中App的名称。
<通道类型>.appid	当前通道中App的ID。
<通道类型>.description	当前通道中App的描述信息。

### 返回示例

```
{
  "cloudapp": [
    {
      "name": "cloudstorage",
      "appid": "78217a43-542d-47e2-97a5-4435bf11521d",
      "description": "Cloud storage application"
    },
    {
      "name": "cloudcrm",
      "appid": "1e99e55d-64c0-49ea-9e94-7df304e4580f",
      "description": "Cloud CRM application"
    }
  ]
}
```

## 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

## 获取事件列表

介绍获取事件列表的接口调用方式。

## 接口介绍

该接口用于获取包含所有安全违规事件的列表。

获取事件列表后，后续可以通过获取事件详情接口查询某个事件的详细信息。具体查阅[获取事件详情](#)。

## 请求方式

GET

URL

## 接口地址

/skg/v1/dlp/incident?<事件属性>



注：你可以使用[获取事件详情](#) on page 385接口查看某一事件的详细信息。

## 请求参数

参数名称	参数位置	是否必须	描述
<事件属性>	URL参数	是	指定一个通道类型。使用 <a href="#">获取通道</a> 接口查看所有通道类型。

事件属性参数列表如下：

- page\_from(可选)：事件分页起始页(默认为0)
- page\_sizetype(可选)：每页返回的事件数目(1对应20个事件，2对应50个事件，3对应100个事件。默认为1)
- start\_timestamp(可选)：事件开始时间 epoch timestamp
- end\_timestamp(可选)：事件结束时间 epoch timestamp
- user(可选)：生成事件的用户名
- action(可选)：对违规事件所采取的动作：1 - 允许 ( 审计模式 ) 2 - 阻断 ( 阻断模式 )
- source(可选)：事件来源
- dest(可选)：事件目标
- policy(可选)：策略名称
- channel(可选)：通道

## 请求示例

以下是一个请求案例。

该案例旨在通过接口获取从1484895553到1484896943阻断用户joe.doe@abc.com的所有事件。

```
GET
```



```
/skg/v1/dlp/incident?
start_timestamp=1484895553&end_timestamp=1484896943&user=abc\joe.
doe&action=2
```

## 返回结果

返回结果中包含以下参数：

名称	描述
result	请求是否成功，成功为0，失败为1
incidents	安全违规事件的事件ID号
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息

以上事件列表请求结果如下：

- 请求成功：

```
{
  "result" : 0,
  "incidents" : [ "d829cb60-1571-4c72-
b2c4-3de461698b73", "912ed858-2a6d-4faaa41e-debccf9e163c" ]
}
```

- 请求失败：

```
{
  "result" : 1,
  "errorCode" : 400,
  "message" : "Invalid parameter"
}
```

## 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

## 获取事件详情

介绍获取事件详情的接口调用方式。

## 接口介绍

该接口用于获取某一事件的详细信息。

## 请求方式

GET

URL

## 接口地址

使用以下URL接口地址进行调用。

```
/skg/v1/dlp/incident/<事件ID>
```

## 请求参数

参数名称	参数位置	是否必须	描述
<事件ID>	URL参数	是	指定一个事件。

## 请求示例

以下示例为调用接口请求获取事件ID为d829cb60-1571-4c72-b2c4-3de461698b73的事件的详细信息。

```
GET /skg/v1/dlp/incident/d829cb60-1571-4c72-b2c4-3de461698b73
```

## 返回结果

返回值包含：查询ID，检测时间，事件时间，来源，目标，策略名称，通道，动作，事件状态，安全级别，最大匹配，和文件名称。

返回值参数定义如下表所示：

参数名	类型	含义
queryID	String	查询ID，此ID与发送内容检查中metadata中传送的查询ID一致
forensicsName	String	证据文件名称
detectTime	int	监测时间戳
incidentTime	int	生成事件事件戳
source	String	生成事件源 - 如用户IP或用户名
dest	Array	生成事件目的 - 如用户访问网站或收件人列表。cloudApp通道无此项。
action	int	1 - 放行， 2- 阻断
channel	String	通道
policies	Array	配备策略名
incidentStatus	int	1- 新事件， 2 - 进行中， 3 - 关闭， 4 - 误报， 5 - 提级（可通过WebUI修改事件状态）
severityTypeCode	int	1 - 高， 2 - 中， 3 - 低， 4 - 信息
maxMatches	int	最大匹配数

## 返回示例

事件详情请求返回值案例：

- 请求成功：

```
{
```

```

"result" : 0,
"data" : {
  "queryID" : "d829cb60-1571-4c72-b2c4-3de461698b73",
  "forensicsName" : "76c68a52-dff3-47e0-b992-a3186fad2134.eml"
  "detectTime" : 1484896943,
  "incidentTime": 1484896943,
  "source" : ["abc\joe.doe"],
  "dest" : ["www.baidu.com"],
  "action" : 1/2,
  "channel" : "http",
  "policies" : ["test"],
  "incidentStatus" : 1/2/3/4/5,
  "severityTypeCode": 1/2/3/4,
  "maxMatches": 10
}
}

```

- 请求失败

```

{
  "result" : 1,
  "errorCode" : 400,
  "message" : "Invalid parameter"
}

```

### 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

### 获取证据文件

介绍获取证据文件的接口调用方式。

### 接口介绍

该接口用于发送请求获取证据文件。

### 请求方式

GET

URL

### 接口地址

使用以下URL接口地址进行调用。

```
GET /skg/v1/dlp/forensics/download?filename=<文件名称>.eml
```

## 请求参数

参数名称	参数位置	是否必须	描述
<文件名称>	URL参数	是	指定一个文件。


## 请求示例

以下示例为调用接口请求获取名称为76c68a52-dff3-47e0-b992-a3186fad2134的证据文件。

```
GET /skg/v1/dlp/forensics/download?filename=76c68a52-dff3-47e0-b992-a3186fad2134.eml
```

## 返回示例

```
stream file
```

 注：证据文件以加密eml格式存放在统一内容安全审查平台UCWT设备存储中。

## 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

## 获取报告

介绍获取报告的接口调用方式。

发送请求获取安全报告：

```
GET /skg/v1/dlp/report?type=<报告类型>&top=<排名前几>
```

URL 参数列表如下：

- type：报告类型：1 - 策略命中排名 2 - 用户命中排名 3 - 目标命中排名 4 - 通道命中排名
- top：报告排名：前x名

## 请求方式

GET  
URL

## 请求参数

参数名称	参数位置	是否必须	描述
<报告类型>	URL参数	是	获取指定类型的报告。
<排名前几>	URL参数	是	获取指定排名前几的统计信息。

## 请求示例

获取策略命中排名前3名的统计信息。

发送获取报告请求。

```
GET /skg/v1/dlp/report?type=1&top=3
```

返回结果

返回结果中包含以下参数：

名称	描述
result	请求是否成功，成功为0，失败为1
report	生成的安全报告
name	被违反的安全策略的名称
incident_number	违反该安全策略的事件号
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息

报告请求结果如下：

- 请求成功：

```
{
  "result" : 0,
  "report" :
  [
    {
      "name" : "policy1",
      "incident_number" : 20134
    },
    {
      "name" : "policy2",
      "incident_number" : 1097
    },
    {
      "name" : "policy3",
      "incident_number" : 198
    }
  ]
}
```

- 请求失败：

```
{
  "result" : 1,
  "errorCode" : 400,
  "message" : "Invalid parameter"
}
```

错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数

错误码	描述
404	未知错误，例如请求了未触发的事件等。
500	无效参数

## 内容审查接口

介绍内容审查接口的基本信息。

### 概述

第三方应用生成queryID并将queryID做为metadata的参数传送给统一内容安全审查平台UCWI，此queryID用来查询与此请求关联的事件详情。

若请求未触发事件，则通过此queryID查询将返回404。事件的生成为异步，根据流量大小入库事件略有不同，第三方应用应该在发送请求后间隔一段时间再查询事件详情。

### 接口介绍

该接口用于发送信息给统一内容安全审查平台UCWI进行内容检查。

### 请求方式

POST

URL

### 接口地址

使用以下URL接口地址进行调用。

URL定义规则为：

/skg/<API版本号>/<功能模块>/<资源名称>/<资源名...>/<请求模式>

### 请求参数

表 176: 请求参数表


参数名称	参数位置	是否必须	描述
<API版本号>	URL参数	是	天空卫士™官方发布的RESTful API版本号。
<功能模块>	URL参数	是	当前版本支持调用的功能模块名称。详见 <a href="#">功能模块</a> 。
<资源名称>	URL参数	是	当前版本支持调用的资源名称。详见 <a href="#">资源名称</a> 。
<请求模式>	URL参数	是	调用内容检查请求的请求模式。详见 <a href="#">请求模式</a> 。

功能模块：

- dlp - 数据防泄漏DLP服务
- swg - Web数据安全服务

资源名称：

- channel - 通道

 注：例：若功能模块为dlp则资源ID包括包括web，email，和cloudapp。

- protocol - 协议

请求模式：

- sync - 同步，UCWI完成扫描之后放回
- async - 异步，立即返回，所有结果都是放行

### Web通道

介绍如何调用接口在Web通道中进行内容审查。

请求方式

POST

URL

接口地址

使用以下URL接口地址进行调用。

POST /skg/v1/dlp/channel/web/<协议类型>/<请求模式>

请求参数

参数名称	参数位置	是否必须	描述
<协议类型>	URL参数	是	指定一种Web协议，如HTTP。
<请求模式>	URL参数	是	指定请求模式为同步或异步。

元数据参数

metadata元数据参数定义。

参数名	类型	适用状态	说明
sourceAddress	String(必选)	同步和异步	请求源IP地址
user	String(可选)	同步和异步	生成事件的用户名 - 支持域用户名，格式为域名/用户名。
url	String(必选)	同步和异步	请求URL
httpBodyLen	int(必选)	同步和异步	HTTP请求Body长度
queryID	String(必选)	同步和异步	与此请求关联的事件查询ID，保持唯一。若请求无事件生成则无法查询到事件详情。
httpHeader	String(必选)	同步和异步	HTTP请求的头部信息
callback_url	String(可选)	异步	只限于异步模式必须填写回调函数的url
uploadtype	String(必选)	异步	只限于异步模式必须填写-file/s3

## 请求示例

以下示例为调用接口分别在同步模式和异步模式下发送数据至统一内容安全审查平台UCWI进行内容安全检测。

- 同步状态下：

```
POST /skg/v1/dlp/channel/web/http/sync
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "sourceAddress": "123.12.12.112",
  "user": "abc\enduser1",
  "url": "http://www.sina.com.cn/forum/post.action",
  "httpBodyLen" : 10240,
  "queryID" : "1024f306-566a-415f-9ada-1be89b9f1086",
  "httpHeader": "Host: testhost.com\r\nConnection: Keep-Alive\r\nContent-
Type: text/plain\r\nContent-Length: 00000010240\r\n\r\n",
  "callback_url": "http://172.22.113.49:5000/post/http"
}
--${bound}
Content-Disposition: form-data; name="request"; filename="httpbody"
Content-Type: application/octet-stream
%HTTP BODY%
```

- 异步状态下：

```
POST /skg/v1/dlp/channel/web/http/async
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "sourceAddress": "123.12.12.112",
  "user": "abc\enduser1",
  "url": "http://www.sina.com.cn/forum/post.action",
  "httpBodyLen" : 10240,
  "queryID" : "1024f306-566a-415f-9ada-1be89b9f1086",
  "httpHeader": "Host: testhost.com\r\nConnection: Keep-Alive\r\nContent-
Type: text/plain\r\nContent-Length: 00000010240\r\n\r\n",
  "callback_url": "http://172.22.113.49:5000/post/http"
}
--${bound}
Content-Disposition: form-data; name="request"; filename="http://s3_url/
httpchannel/http/http.txt"
Content-Type: application/octet-stream
%HTTP BODY%
```

## HTTP BODY 格式：

```
Film and the City: The Urban Imaginary in Canadian Cinema.
```

## 返回示例

内容审查请求返回结果中包含以下参数：

名称	描述
result	请求是否成功，成功为0，失败为1




名称	描述
actionCode	请求成功时，用户可选择对符合请求条件的内容进行默认操作，默认操作包括1-允许数据传输和2-阻断数据传输
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息

内容审查请求的回复如下。

- 请求成功：

```
{
  "result" : 0,
  "actionCode" : 1/2
}
actionCode: 1 - allow, 2 - block
```

 注：若匹配策略，发现违规内容，系统还将返回策略匹配信息，具体请参照[送检策略匹配返回值定义](#)

- 请求失败：

```
{
  "result" : 1,
  "errorCode" : 500,
  "message" : "Invalid parameter"
}
```

#### 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

#### 邮件通道

介绍如何调用接口在邮件通道中进行内容审查。

#### 请求方式

POST

URL

#### 接口地址

使用以下URL接口地址进行调用。

POST /skg/v1/dlp/channel/email/<协议类型>/<请求模式>

## 请求参数

参数名称	参数位置	是否必须	描述
<协议类型>	URL参数	是	指定一种邮件协议，如SMTP。
<请求模式>	URL参数	是	指定请求模式为同步或异步。

## 元数据参数

metadata参数定义。

参数名	类型	适用状态	说明
sender	String(必选)	同步和异步	发件人邮箱
recipients	String(可选)	同步和异步	收件人邮箱 - 包括To, cc, bcc
queryID	String(必选)	同步和异步	与此请求关联的事件查询ID, 保持唯一。若请求无事件生成则无法查询到事件详情。
callback_url	String(可选)	异步	只限于异步模式填写回调函数的url
uploadtype	String(必选)	异步	只限于异步模式填写-file/s3
X-Auth-Token	String(必选)	异步	swift的认证token, 只限于异步模式且uploadtype为swift

## 请求示例

以下示例为调用接口分别在同步模式和异步模式下发送数据至统一内容安全审查平台UCWI进行内容安全检测。

- 同步状态下：

```
POST /skg/v1/dlp/channel/email/smtp/sync
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "sender": "joe.doe@abc.com",
  "recipients": ["john.doe@abc.com", "joe.smith@abc.com"],
  "queryID": "99b32659-1227-4745-bd72-e90406b62fa3",
}
--${bound}
Content-Disposition: form-data; name="request"; filename="email"
Content-Type: application/octet-stream
%EML%
```

- 异步状态下：

```
POST /skg/v1/dlp/channel/email/smtp/async
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "sender": "joe.doe@abc.com",
  "recipients": ["john.doe@abc.com", "joe.smith@abc.com"],
```

```

"queryID": "99b32659-1227-4745-bd72-e90406b62fa3",
"uploadtype": "file/s3",
"X-Auth-Token": "AUTH_tkbdac2a3474ee4d6396133c99cfd962c8",
"callback_url": "http://172.22.113.49:5000/post/email"
}
--${bound}
Content-Disposition: form-data; name="request"; filename="http://s3_url/
emailchannel/email/email.eml"
Content-Type: application/octet-stream
%EML%

```

## 返回示例

内容审查请求返回结果中包含以下参数：

名称	描述
result	请求是否成功，成功为0，失败为1
actionCode	请求成功时，用户可选择对符合请求条件的内容进行默认操作，默认操作包括1-允许数据传输和2-阻断数据传输
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息


内容审查请求的回复如下。

- 请求成功：

```

{
  "result" : 0,
  "actionCode" : 1/2
}
actionCode: 1 - allow, 2 - block

```

 注：若匹配策略，发现违规内容，系统还将返回策略匹配信息，具体请参照[送检策略匹配返回值定义](#)

- 请求失败：

```

{
  "result" : 1,
  "errorCode" : 500,
  "message" : "Invalid parameter"
}

```

## EML文件示例

EML例子如下：

```

Date: Fri, 20 Jan 2017 03:28:09 UTC
From: asmith@skg.com
To: eyee@skg.com
Subject: Normal_Mail
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="Spirent_Avalanche_SMTP"
This is a mime encoded message
--Spirent_Avalanche_SMTP
Content-Type: text/plain

```

```
Dear David and Steve,
Good morning.
This is the body of this E-Mail.Aaaaa, aaaaaaa, aaa, aaa, aa, aaaaaaaaaa,
aaaaaaaaaaaaaaaaaaaaaa.
Please contact us at any time.
Best Regards.
Someone
--Spirent_Avalanche_SMTP--
```

### 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

### CloudApp通道-明文内容

介绍如何调用接口在云应用通道中进行针对明文内容的内容审查。

#### 请求方式

POST  
URL

#### 接口地址

使用以下URL接口地址进行调用。

POST /skg/v1/dlp/channel/cloudapp/<云应用ID>/<请求模式>

#### 请求参数

参数名称	参数位置	是否必须	描述
<云应用ID>	URL参数	是	通过ID指定某云应用程序。
<请求模式>	URL参数	是	指定请求模式为同步或异步。

#### 元数据参数

支持明文内容的扫描

metadata参数定义

参数名	类型	适用状态	说明
user	String(必选)	同步和异步	生成事件的用户名 - 支持域用户，格式为域名\用户名。
filename	String(可选)	同步和异步	文件名 - 可做根据文件名设置的策略匹配
queryID	String(必选)	同步和异步	与此请求关联的事件查询ID，保持唯一。若请求无事件生成则无法查询到事件详情。
callback_url	String(可选)	异步	只限于异步模式填写，call back的监听地址

参数名	类型	适用状态	说明
encoding	String(可选)	同步和异步	文件编码
uploadtype	String(必选)	异步	只限于异步模式填写-file/s3或swift
X-Auth-Token	String(必选)	异步	swift的认证token，只限于异步模式且uploadtype为swift

#### 请求示例

以下示例为调用接口分别在同步模式和异步模式下发送明文内容至统一内容安全审查平台UCWI进行内容安全检测。

- 同步状态下：

```
POST /skg/v1/dlp/channel/cloudapp/appid/sync
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "user": "abc\enduser1",
  "filename": "confidential.doc",
  "queryID": "cd2fd109-c4d4-489f-9b27-53752f7827d6",
}
--${bound}
Content-Disposition: form-data; name="request";
  filename="confidential.doc"
Content-Type: application/pdf
%PDF FILE%
```

- 异步状态下：

```
POST /skg/v1/dlp/channel/cloudapp/appid/async
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "user": "abc\enduser1",
  "filename": "confidential.doc",
  "queryID": "cd2fd109-c4d4-489f-9b27-53752f7827d6",
  "uploadtype": "file/s3",
  "X-Auth-Token": "AUTH_tkbdac2a3474ee4d6396133c99cfd962c8",
  "callback_url": "http://172.22.113.49:5000/post/cloudapp"
}
--${bound}
Content-Disposition: form-data; name="request"; filename="http://s3_url/cloudappchannel/cloudapp/cloudapp.doc"
Content-Type: application/octet-stream
%PDF FILE%
```

#### 返回示例

内容审查请求返回结果中包含以下参数：


名称	描述
result	请求是否成功，成功为0，失败为1

名称	描述
actionCode	请求成功时，用户可选择对符合请求条件的内容进行默认操作，默认操作包括1-允许数据传输和2-阻断数据传输
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息

内容审查请求的回复如下。

- 请求成功：

```
{
  "result" : 0,
  "actionCode" : 1/2
}
actionCode: 1 - allow, 2 - block
```

 注：若匹配策略，发现违规内容，系统还将返回策略匹配信息，具体请参照[送检策略匹配返回值定义](#)

- 请求失败：

```
{
  "result" : 1,
  "errorCode" : 500,
  "message" : "Invalid parameter"
}
```

## 批量审查

介绍如何调用接口在云应用通道中进行批量内容审查。

表 177: 元数据参数

参数名	类型	说明
user	String(必选)	生成事件的用户名 - 支持域用户，格式为域名\用户名。
filename	String(可选)	文件名 - 可做根据文件名设置的策略匹配
queryID	String(必选)	与此请求关联的事件查询ID，保持唯一。若请求无事件生成则无法查询到事件详情。
callback_url	String(可选)	call back的监听地址
verbose	String(必选)	是否返回事件信息。
uploadtype	String(必选)	swift，批量上传支持的上传类型为swift。
X-Auth-User	String(必选)	swift的认证用户名。
X-Auth-Key	String(必选)	swift的认证Key。
X-Auth-Token	String(必选)	swift的认证token。
objectUrl	String(必选)	swift的认证文件的地址。

请求示例：

```
{
  "callback_url": "http://172.22.113.49:5000/post.php",
  "verbose": True, //是否返回incident_info
  "objects": [
    {
      "user": "abc\enduser1",
      "filename": "confidential.doc",
      "queryID": "cd2fd109-c4d4-489f-9b27-53752f7827d6",
      "uploadtype": "swift",
      "objectInfo": {
        "authUrl": "http://swift.example.com/auth/v1.0",
        "X-Auth-User": "testuser",
        "X-Auth-Key": "2121212",
        "X-Auth-Token": "AUTH_tkbdac2a3474ee4d6396133c99cfd962c",
        "objectUrl": "https://swift-server/confidential.doc"
      }
    },
    {
      "user": "abc\enduser2",
      "filename": "test.doc",
      "queryID": "47992d42-04b7-4860-b186-b8c11f8b2253",
      "uploadtype": "swift",
      "objectInfo": {
        "authUrl": "http://swift.example.com/auth/v1.0",
        "X-Auth-User": "testuser",
        "X-Auth-Key": "2121212",
        "X-Auth-Token": "AUTH_tkbdac2a3474ee4d6396133c99cfd962c",
        "objectUrl": "https://swift-server/confidential.doc"
      }
    }
  ]
}
```

批量审查请求返回结果中包含以下参数：

名称	描述
result	请求是否成功，成功为0，失败为1
actionCode	请求成功时，用户可选择对符合请求条件的内容进行默认操作，默认操作包括1-允许数据传输和2-阻断数据传输
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息
Incident_info	策略匹配的事件信息

返回示例：

```
{
  "cd2fd109-c4d4-489f-9b27-53752f7827d": {
    "localDetectedTime": "2019-07-29T16:17:43.079368+0800", //检测时间
    "incident_info": //事件信息
    {
      "matchedPolicies": [ //匹配策略
        {
          "numberOfMatches": 1, //匹配策略的事件数量
          "name": "abc\enduser1", //违规用户的域名和用户名
        }
      ]
    }
  }
}
```

```

    "actionSettingName": "阻断", //对违规事件执行的动作
    "matchedRules": [ //匹配的策略规则
      {
        "name": "skyguard", //规则名称
        "matchedConditions": [ //匹配的条件
          {
            "type": 5, //条件匹配类型, 包括: 1:正则, 2:字典, 3:外部脚本,
            4:文件类型组, 5:关键字, 6:脚本, 7:文件指纹, 8:机器学习, 9:终端位置, 10:文件名称,
            11:附件数量, 12:数据库指纹, 13:文件大小, 14:二进制, 15#压缩文件深度, 16:加密文件,
            17:格式不匹配文件, 18:内置模板
            "matchedElements": [ //匹配的元素
              {
                "matchedContents": [ //匹配的内容
                  {
                    "detectedValues": [ //检测到的内容
                      {
                        "text": "skyguard" //关键字
                      }
                    ],
                    "isFileSuffixMatch": true, //文件后缀名是否一致
                    "isArchiveFile": false, //是否为压缩文件
                    "isEncryptFile": false, //是否为加密文件
                    "encodeType": "UnknownEncoding", //文件编码类型, 具
                    体请参阅国际标准编码类型及其解释
                    "numberOfMatches": 1, //匹配数
                    "locationPath": "confidential.doc", //文件全路
                    径
                    "id": "0-0", //文件ID
                    "contentSize": 22 //内容大小
                  }
                ],
                "numberOfMatches": 1,
                "isTruncated": false
              }
            ],
            "isTraditionalMatching": false //是否开启繁体匹配
          }
        ]
      }
    ],
    "priority": 31, //优先级
    "groupName": "默认策略组", //策略组名称
    "severity": 3 //敏感级别 1 - 高, 2 - 中, 3 - 低, 4 - 信息
  }
],
"result": 0,
"actionCode": 2
},
"47992d42-04b7-4860-b186-b8c11f8b2253": {
  "localDetectedTime": "2019-07-29T07:52:26.423684",
  "incident_info": {},
  "result": 0,
  "actionCode": 1
}
}

```

#### 错误代码

若调用出现错误, 将返回以下错误代码:



错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

### CloudApp通道-文本内容

介绍如何调用接口在云应用通道中进行针对文本内容的内容审查。

#### 请求方式

POST  
URL

#### 接口地址

使用以下URL接口地址进行调用。

POST /skg/v1/dlp/channel/cloudapp/<云应用ID>/<文本请求模式>

#### 请求参数

参数名称	参数位置	是否必须	描述
<云应用ID>	URL参数	是	通过ID指定某云应用程序。
<文本请求模式>	URL参数	是	指定文本内容的请求模式为同步或异步。

#### 元数据参数

支持文本内容的扫描

metadata参数定义

参数名	类型	适用状态	说明
user	String(必选)	同步和异步	生成事件的用户名 - 支持域用户，格式为域名\用户名。
queryID	String(必选)	同步和异步	与此请求关联的事件查询ID，保持唯一。若请求无事件生成则无法查询到事件详情。
callback_url	String(可选)	异步	只限于异步模式填写，call back的监听地址
encoding	String(可选)	同步和异步	文件编码

#### 请求示例

以下示例为调用接口分别在同步模式和异步模式下发送文本内容至统一内容安全审查平台UCWI进行内容安全检测。

- 同步状态下：

```
POST /skg/v1/dlp/channel/cloudapp/appid/message_sync
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
```

```
{
  "user": "abc\enduser1",
  "queryID": "cd2fd109-c4d4-489f-9b27-53752f7827d6",
}
--${bound}
Content-Disposition: form-data; name="inspectContent";
Content-Type: text/plain
%Message Content%
```

- 异步状态下：

```
POST /skg/v1/dlp/channel/cloudapp/appid/message_async
Content-Type: multipart/form-data; boundary=${bound}
--${bound}
Content-Disposition: form-data; name="metadata"
Content-Type: application/json
{
  "user": "abc\enduser1",
  "queryID": "cd2fd109-c4d4-489f-9b27-53752f7827d6",
  "callback_url": "http://172.22.113.49:5000/post/cloudapp"
}
--${bound}
Content-Disposition: form-data; name="inspectContent";
Content-Type: text/plain
%Message Content%
```

#### 返回示例


内容审查请求返回结果中包含以下参数：

名称	描述
result	请求是否成功，成功为0，失败为1
actionCode	请求成功时，用户可选择对符合请求条件的内容进行默认操作，默认操作包括1-允许数据传输和2-阻断数据传输
errorCode	请求失败时返回的错误代码
message	请求失败时返回的错误消息

内容审查请求的回复如下。

- 请求成功：

```
{
  "result" : 0,
  "actionCode" : 1/2
}
actionCode: 1 - allow, 2 - block
```

 注：若匹配策略，发现违规内容，系统还将返回策略匹配信息，具体请参照[送检策略匹配返回值定义](#)

- 请求失败：

```
{
  "result" : 1,
  "errorCode" : 500,
  "message" : "Invalid parameter"
```

```
}

```

### 错误代码

若调用出现错误，将返回以下错误代码：

错误码	描述
400	无效参数
404	未知错误，例如请求了未触发的事件等。
500	无效参数

### 送检返回值定义

介绍将内容通过内容审查接口送检的返回值定义。

若匹配策略，系统将返回匹配策略信息。

以下示例为一送检返回值示例及具体注释。

```
{
  "localDetectedTime": "2017-11-02T11:06:08.408697" //检测时间
  "incident_info": //事件信息
    {
      "matchedPolicies": [ //匹配策略
        {
          "numberOfMatches": 1, //匹配策略的事件数量
          "name": "关键字策略", //匹配的策略名称
          "actionSettingName": "阻断", //对违规事件执行的动作
          "matchedRules": [ //匹配的策略规则
            {
              "name": "关键字策略", //规则名称
              "matchedConditions": [ //匹配的条
                {
                  "type": 5, //条件匹
                  "matchedElements": [ //匹配的元
                    {
                      "matchedContents": [ //匹配的內
                        {
                          "detectedValues": [ //检
                            {
                              "text": "保密"
                            }
                          ],
                          "isFileSuffixMatch": true, //文件后缀名是否一致
                          "isEncryptFile": false,
                          "encodeType": "UnknownEncoding", //文件编码类型，具体请参阅国际标准编码类型及其解释
                          "numberOfMatches": 1,
                          "locationPath": "DLP.rar || DLP.docx", //文件全路径
                        }
                      ]
                    }
                  ]
                }
              ]
            }
          ]
        }
      ]
    }
  "content": "测到的内容"
  "keyword": "关键字"
}
```

匹配类型，包括：1:正则，2:字典，3:外部脚本，4:文件类型组，5:关键字，6:脚本，7:文件指纹，8:机器学习，9:终端位置，10:文件名称，11:附件数量，12:数据库指纹，13:文件大小，14:二进制，15#压缩文件深度，16:加密文件，17:格式不匹配文件，18:内置模板

```

        "isArchiveFile":false,
        "contentSize":986637
    },
    ],
    "numberOfMatches":1,
    },
    ],
    "isTraditionalMatching":false //是
否开启繁体匹配
    }
    ],
    },
    "isTrickle":false, //是否是零星式内容检测策略
    "priority":1001, //优先级
    "groupName":"默认策略组", //策略组名称
    "severity":4 //敏感级别 1 - 高, 2 - 中, 3 - 低,
4 - 信息
},
{
    "numberOfMatches":2,
    "name":"指纹策略",
    "actionSettingName":"阻断",
    "matchedRules":[
        {
            "name":"指纹规则",
            "matchedConditions":[
                {
                    "type":7,
                    "matchedElements":[
                        {
                            "matchedContents":[
                                "detectedValues":[
                                    //当类型为文件指纹时没有text字段, 其他都有
                                ],
                                "similarity":100, //相似度
                                "isPreciseMatching":false, //是否为精确匹配
                                "filePath":"C:/
Users/admin/Desktop/101/cloudappfile/DLP.docx" //文件指纹的原始扫描文件路径
                            ],
                        }
                    ],
                }
            ],
            "similarity":100,
            "isPreciseMatching":true,
            "filePath":"C:/
Users/admin/Desktop/101/cloudappfile/DLP.docx"
        }
    ],
    "isFileSuffixMatch":true,
    "isEncryptFile":false,
    "encodeType":"UnknownEncoding",
    "numberOfMatches":2,

```

```

"locationPath": "DLP.rar || DLP.docx",
    "isArchiveFile": false,
    "contentSize": 986637
  },
  ],
  "numberOfMatches": 2,
},
],
"isTraditionalMatching": false
}
]
},
],
"isTrickle": false,
"priority": 1001,
"groupName": "默认策略组",
"severity": 1
},
{
  "numberOfMatches": 16,
  "name": "关键字策略B",
  "actionSettingName": "阻断",
  "matchedRules": [
    {
      "name": "关键字规则",
      "matchedConditions": [
        {
          "type": 5,
          "matchedElements": [
            {
              "matchedContents": [
                {
                  "detectedValues": [
                    { "text": "IP地址" },
                    { "text": "函数" },
                    { "text": "机器学习" }
                  ]
                }
              ]
            }
          ]
        }
      ]
    }
  ],
  "isFileSuffixMatch": true,
  "isEncryptFile": false,
  "encodeType": "UnknownEncoding",
  "numberOfMatches": 16,
  "locationPath": "DLP.rar || DLP.docx",
  "isArchiveFile": false,
  "contentSize": 986637
},
],
"numberOfMatches": 16,
},
],
"isTraditionalMatching": false
}
]
},
],
"isTrickle": false,
"priority": 1001,
"groupName": "默认策略组",
"severity": 2
}

```

```

    }
  ],
  "result":0,
  "actionCode":2, //可执行的动作代码, 包括-1:允许, 2:阻断, 3:确认, 4:删除附件,
  5:邮件加密, 6:邮件隔离, 7:终端系统加密, 8:邮件内容加密, 9:终端个人密钥加密, 10:水印 (仅
  限代理)
}

```

## 使用curl的示例

例举使用curl调用API及其参数的示例。

参照以下示例使用curl调用API 进行内容审查：

### 内容审查-Web通道

按照如下示例使用curl调用接口在Web通道中进行内容审查。

以下示例适用于上传类型为S3的情况：

- 带callback：

```

curl -F 'metadata={"uploadtype": "s3", "callback_url":
  "http://172.22.113.12:9999/post/http", "url": "http://172.22.78.100/
  post.php", "httpBodyLen": "987056",
  "queryID": "3d6aa370-4b4c-11e7-81f7-9ef3ee527981", "user": "hwsh1\
  \hwsh0410enduser1", "sourceAddress": "192.168.100.1",
  "httpHeader": "Host: hwbj1.com\r\nConnection: Keep-Alive\r\nContent-Type:
  multipart/form-data; boundary=-----289549027074\r
  \nContent-Length: 987056\r\n\r\n"}'
-F 'request=http://172.22.78.91:8070/test-http/home/test/http/dlp.docx'
https://172.22.78.107:5443/skg/v1/dlp/channel/web/http/async

```

- 不带callback：

```

curl -F 'metadata={"uploadtype": "s3", "url": "http://172.22.78.100/
  post.php", "httpBodyLen": "987056", "queryID":
  "66883380-4b2e-11e7-81f7-9ef3ee527981",
  "user": "hwsh1\hwsh0410enduser1", "sourceAddress": "192.168.100.1",
  "httpHeader": "Host: hwbj1.com\r\nConnection: Keep-Alive\r\nContent-Type:
  multipart/form-data; boundary=-----289549027074\r
  \nContent-Length: 987056\r\n\r\n"}'
-F 'request=http://172.22.78.91:8070/test-http/home/test/http/dlp.docx'
https://172.22.78.107:5443/skg/v1/dlp/channel/web/http/async

```

以下示例适用于上传类型为localhost的情况：

- 带callback：

```

curl -F 'metadata={"uploadtype": "localhost", "callback_url":
  "http://172.22.113.12:9999/post/http", "url": "http://172.22.78.100/
  post.php", "httpBodyLen": "987056",
  "queryID": "66883380-4b2e-11e7-81f7-9ef3ee527981", "user": "hwsh1\
  \hwsh0410enduser1", "sourceAddress": "192.168.100.1",
  "httpHeader": "Host: hwbj1.com\r\nConnection: Keep-Alive\r\nContent-Type:
  multipart/form-data; boundary=-----289549027074\r
  \nContent-Length: 987056\r\n\r\n"}'
-F 'request=@/home/test/http/dlp.docx' https://172.22.78.107:5443/skg/v1/
  dlp/channel/web/http/async

```

- 不带callback :

```
curl -F 'metadata={"uploadtype": "localhost", "url":
"http://172.22.78.100/post.php", "httpBodyLen": "987056", "queryID":
"c44604f0-4b49-11e7-81f7-9ef3ee527981",
"user": "hwsh1\hwsh0410enduser1", "sourceAddress": "192.168.100.1",
"httpHeader": "Host: hwbj1.com\r\nConnection: Keep-Alive\r\nContent-Type:
multipart/form-data; boundary=-----289549027074\r
\nContent-Length: 987056\r\n\r\n"}'
-F 'request=@/home/test/http/dlp.docx' https://172.22.78.107:5443/skg/v1/
dlp/channel/web/http/async
```

### 内容审查-邮件通道

按照如下示例使用curl调用接口在邮件通道中进行内容审查。

以下示例适用于上传类型为S3的情况 :

- 带callback :

```
curl -H "Content-Type: multipart/form-data" -F 'metadata={"uploadtype":
"s3", "callback_url": "http://172.22.113.12:9999/post/
email", "sender": "hwsh-senduser2@huawei.com",
"recipients": ["hwsh-receiveruser2@huaweicom", "external-
receiveruser2@126.com"], "queryID": "9affdc62-4b2e-11e7-81f7-9ef3ee527981"}'
-F "request=http://172.22.78.91:8070/test-email/home/test/email/
Fwdaaaa.eml" https://172.22.78.107:5443/skg/v1/dlp/channel/email/smt/
async
```

- 不带callback :

```
curl -H "Content-Type: multipart/form-data" -F 'metadata={"uploadtype":
"s3", "sender": "hwsh-senduser2@huawei.com", "recipients": ["hwsh-
receiveruser2@huaweicom", "external-receiveruser2@126.com"],
"queryID": "9affdc62-4b2e-11e7-81f7-9ef3ee527981"}' -F
"request=http://172.22.78.91:8070/test-email/home/test/email/Fwdaaaa.eml"
https://172.22.78.107:5443/skg/v1/dlp/channel/email/smt/async
```

以下示例适用于上传类型为localhost的情况 :

- 带callback :

```
curl -H "Content-Type: multipart/form-data" -F 'metadata={"uploadtype":
"localhost", "callback_url": "http://172.22.113.12:9999/post/
email", "sender": "hwsh-senduser2@huawei.com",
"recipients": ["hwsh-receiveruser2@huaweicom", "external-
receiveruser2@126.com"], "queryID": "9affdc62-4b2e-11e7-81f7-9ef3ee527981"}'
-F "request=@/home/test/email/Fwdaaaa.eml" https://172.22.78.107:5443/skg/
v1/dlp/channel/email/smt/async
```

- 不带callback :

```
curl -H "Content-Type: multipart/form-data" -F 'metadata={"uploadtype":
"localhost", "sender": "hwsh-senduser2@huawei.com", "recipients": ["hwsh-
receiveruser2@huaweicom", "external-receiveruser2@126.com"],
"queryID": "9affdc62-4b2e-11e7-81f7-9ef3ee527981"}' -F "request=@/home/
test/email/Fwdaaaa.eml" https://172.22.78.107:5443/skg/v1/dlp/channel/
email/smt/async
```

## 内容审查-Cloud App通道

按照如下示例使用curl调用接口在Cloud App通道中进行内容审查。

以下示例适用于上传类型为S3的情况：

- 带callback：

```
curl -F 'metadata={"uploadtype": "s3", "callback_url":
"http://172.22.113.12:9999/post/cloudapp", "queryID":
"000864b0-4b2c-11e7-81f7-9ef3ee527981", "user": "hwshtest1\
\hwsh0410user1", "filename": "DLPencrypt.rar"}'
-F 'request=http://172.22.78.91:8070/test-cloudapp/home/test/testfile4/
DLPencrypt.rar' https://172.22.78.107:5443/skg/v1/dlp/channel/cloudapp/
e4dbd0d7-2fc6-4034-b4d8-3807af66bf91/async
```

- 不带callback：

```
curl -F 'metadata={"uploadtype": "s3", "queryID":
"000864b0-4b2c-11e7-81f7-9ef3ee527981", "user": "hwshtest1\
\hwsh0410user1", "filename": "DLPencrypt.rar"}'
-F 'request=http://172.22.78.91:8070/test-cloudapp/home/test/testfile4/
DLPencrypt.rar' https://172.22.78.107:5443/skg/v1/dlp/channel/cloudapp/
e4dbd0d7-2fc6-4034-b4d8-3807af66bf91/async
```

以下示例适用于上传类型为localhost的情况：

- 带callback：

```
curl -F 'metadata={"uploadtype": "localhost", "callback_url":
"http://172.22.113.12:9999/post/cloudapp", "queryID":
"44130fdc-4b2e-11e7-81f7-9ef3ee527981", "user": "hwshtest1\
\hwsh0410user1", "filename": "DLPencrypt.rar"}'
-F 'request=@/home/test/testfile4/DLPencrypt.rar'
https://172.22.78.107:5443/skg/v1/dlp/channel/cloudapp/
e4dbd0d7-2fc6-4034-b4d8-3807af66bf91/async
```

- 不带callback：

```
curl -F 'metadata={"uploadtype": "localhost","queryID":
"44130fdc-4b2e-11e7-81f7-9ef3ee527981", "user": "hwshtest1\
\hwsh0601user1", "filename": "DLPencrypt.rar"}'
-F 'request=@/home/test/testfile4/DLPencrypt.rar'
https://172.22.78.107:5443/skg/v1/dlp/channel/cloudapp/
e4dbd0d7-2fc6-4034-b4d8-3807af66bf91/async
```

## 第三方志管理平台集成

介绍与第三方日志管理平台集成的信息。

天空卫士云管理平台 ( GatorCloud ) 支持将DLP事件转发到第三方syslog server或SIEM server。可通过UI配置打开与第三方日记管理平台的集成。

### 设置Syslog

介绍Syslog设置的相关信息。

UCSS使用Syslog服务器记录系统日志，管理员通过查看系统记录随时了解系统状况。

1. 选择系统 > 基本设置 > Syslog，设置Syslog。
2. 滑动状态条启用Syslog，默认不启用。
3. 输入Syslog服务器的IP地址和端口号 ( 默认端口514 )。
4. 选择Syslog模块，即日志发送格式。默认Syslog格式user-level messages。



5. 点击发送测试信息按钮，验证Syslog设置是否有效。
6. 选择是否设置自定义分隔符用于日志内容。
7. 选择是否发送空值到服务器。
8. 选择发送至Syslog服务器的内容：
  - 系统日志：勾选此项后，发送UCSS以及全部注册设备的系统日志至Syslog服务器。
  - DLP事件：勾选此项后，发送DLP事件信息至Syslog服务器。
  - ASWG代理日志：勾选此项后，发送ASWG代理日志至Syslog服务器。
  - 邮件日志：勾选此项后，发送UCSS以及全部注册设备的邮件日志至Syslog服务器。
  - 邮件连接日志：勾选此项后，发送UCSS以及全部注册设备的邮件连接日志至Syslog服务器。
  - 审计日志：勾选此项后，发送UCSS管理平台的审计日志至Syslog服务器。
9. 点击保存，Syslog设置生效。

### 设置SIEM

介绍SIEM设置的相关信息。

SIEM为网络、系统和应用产生的安全信息（包括日志、告警等）进行统一的实时监控、历史分析；对来自外部的入侵和内部的违规、误操作行为进行监控、审计分析、调查取证、出具各种报表报告。

1. 选择系统 > 基本设置 > SIEM，设置SIEM。
2. 滑动状态条启用SIEM，默认不启用。
3. 输入SIEM服务器的IP地址和端口号（默认端口514）。
4. 选择SIEM服务器的数据传输方式为UDP或TCP。
5. 点击发送测试信息验证SIEM设置是否有效。
6. 选择是否设置自定义分隔符用于日志内容。
7. 选择是否发送空值到服务器。
8. 选择发送至SIEM服务器的内容：

系统日志	勾选此项后，发送UCSS以及全部注册设备的系统日志至SIEM服务器。
DLP事件	勾选此项后，发送DLP事件信息至SIEM服务器。
ASWG代理日志	勾选此项后，发送ASWG代理日志至SIEM服务器。
邮件日志	勾选此项后，发送UCSS以及全部注册设备的邮件日志至SIEM服务器。
邮件连接日志	勾选此项后，发送UCSS以及全部注册设备的邮件连接日志至SIEM服务器。
审计日志	勾选此项后，发送UCSS管理平台的审计日志至SIEM服务器。

9. 点击保存，SIEM设置生效。



---

# 第 10 章

---

## 内部威胁防护

---

内容:

- [ITM管理](#)
- [ITM报告](#)

介绍天空卫士™内部威胁防护ITP解决方案。

关于内部威胁防护

内部威胁 是一种新兴的风险类别。内部威胁往往来自机构被授权的内部人员，他们在行使自身权限的过程中，有意地或无意地对数据进行过度传播，不当修改，甚至刻意盗取数据。。。等各种损害企业利益或危害企业安全的行为，最终导致经济损失或资源和性能受到损害。

这使得传统的由策略匹配触发的被动监控，被动阻断和被动审计等安全措施 在应对内部威胁的过程中往往束手无策。

为应对由公司内部人员不规范行为引发的各种安全隐患，天空卫士™利用其行业领先的ITM技术构建了各种行为模型并以此对您内网环境中的每一台电脑和每一个个人进行安全风险评分。基于分析结果，天空卫士™ ITM在确认发现内部威胁的情况下，将发送警告或执行安全策略行为。

## ITM管理

介绍如何进行内部威胁管理。

ITMS管理用于对ITMS设备管理、日志收集来源、运行频率、MRS任务、ERS专家模型同步、ITM报告设置等功能进行基本配置。

### 查看预置ITM安全策略模板


介绍查看预置ITM安全策略模板的步骤。

#### ITM安全预制策略模板

天空卫士™ 安全鳄® 内部威胁管理ITM 内部威胁防护ITP解决方案提供了预制的策略模板，以帮助安全管理员用于创建和编辑内部威胁防护ITP安全策略。

#### 查看策略模板

按照以下步骤查看Web安全策略模板。

1. 点击进入DLP管理 > 策略页面。
2. 将鼠标移至  按钮，勾选显示预制ITM策略选项。




系统预制的ITM安全策略模板显示在页面列表中。

### 预置ITM模板

字段	解释
压缩文件层数	检测压缩文件的压缩层数，默认检测超过3层的压缩文件。
实际文件类型	判断扩展名与实际类型不匹配的文件，默认检测Office办公（word/excel/ppt）、压缩、图片三类文件。


## ITM设置

管理设置ITMS状态、ITMS服务器连接配置及其运行频率。

1. 选择系统 > ITM管理 > ITM设置，滑动状态条启用ITM，默认不启用。
2. 选择是否上传MRS（精准威胁行为回溯）模型至SkyGuard云安全实验室，用于ITM模型优化。
3. 设置ITM服务器：
  - a) 输入ITM服务器的主机名或IP地址。
  - b) 输入ITM服务器用于日志收集服务的端口，默认为514。
  - c) 输入登陆ITM服务器的用户名。
  - d) 输入登陆ITN服务器的密码。
  - e) 设置完成后，点击测试连接，系统会尝试使用提供的信息检测与共享服务器的连通性。如果尝试连接失败，系统将会给出提示信息。
4. 日志来源服务器：输入用于收集除ITM日志以外的日志的服务器，点击  添加到服务器列表。点击  删除所选服务器IP地址。
5. 设置ITM运行频率，即ITM服务器后台进行数据分析的时间间隔，以零点或12点作为计时起点。
6. 设置ARS用户组，将行为比较类似的用户划分为组进行ARS分析，提高ITM风险行为分析准确率。点击  选择已有用户组添加到列表，如需自定义请参考[添加用户目录组](#)。
7. 点击保存，ITM设置生效。

## 启用专家模型

专家系统 ( ERS ) 结合专家经验和大数据分析结果，针对每个用户或者IP得到同已知风险模式匹配的风险概率值ERS。专家模型预置多个专家系统模型，集成ERS关键策略和分析统计技术等模型因子，根据收集到的用户行为数据评估风险并生成ITM风险报告。

选择系统 > ITM管理 > 专家模型，点击  编辑预置专家模型，显示名称、描述和模型因子不可编辑，可更改启用状态为启用或禁用。




专家模型支持用户组分析，即将行为比较类似的用户划分为组进行专家模型分析，提高ITM风险行为分析准确率。选择系统 > ITM管理 > 专家模型 > 编辑专家模型，点击  选择已有用户组添加到列表，如需自定义请参考[用户目录](#)。

表 178: 页面图标和行间操作按钮功能

图标	解释
	禁用专家模型。
	启用所选专家模型。

## MRS任务

MRS即事件行为感知泄密风险，以特定DLP安全事件为基础，针对每个用户或者IP进行回溯得到DLP安全风险模式相似分值MRS。




1. 选择系统 > ITM管理 > MRS任务，点击添加，新建MRS任务。
2. 输入MRS任务名称和描述，说明其作用。
3. 选择是否启用MRS任务。
4. 点击  从策略列表中选择相应策略应用于MRS任务，根据策略的命中信息得出安全风险模式相似分值。
5. 点击  添加用户到MRS回溯列表，得出安全风险模式相似分值。
6. 点击保存，新建MRS任务显示于列表。

表 179: 页面图标和行间操作按钮功能

	编辑MRS任务，查看应用的策略。
	运行所选的MRS任务。
	禁用所选MRS任务。
	MRS重新培训，详细信息请参考 <a href="#">MRS重新培训</a> 。
	删除所选的MRS任务。
	批量启用所选MRS任务。
	批量禁用所选MRS任务。
	批量删除所选MRS任务。

## MRS重新培训

MRS支持多用户组的安全风险建模，当某一用户组的分析结果不理想时，可点击进行重新培训并再次获取相似分值。

重新培训功能支持四种任务状态：



- 等待样本
- 开始培训
- 培训中
- 可预测

其中等待样本为缺少数据状态，需要向用户组填补数据；可预测为已经完成重新培训并获得安全风险模式相似分值。

## ITM例外

ITM例外实现对一些特定的来源IP或用户不进行ITM的统计和控制。

1. 选择系统 > ITM管理 > ITM例外，点击添加，新建ITM例外。
2. 输入ITM例外名称和描述，说明其用途。
3. 选择以下方式添加ITM例外：

自定义IP/IP段例外	在自定义下拉菜单中选择IP/IP段，并输入数值，点击  添加到自定义列表。添加多个数值时以英文逗号分隔。
自定义用户例外	在自定义下拉菜单中选择用户，并输入用户名称，点击  添加到自定义列表。支持通配符*和?，添加多个数值时以英文逗号分隔。
选择用户	点击  从系统的用户目录组或AD中选择用户，点击确定添加到例外列表。

4. 点击保存，新建ITM例外信息显示于列表。

表 180: 页面图标和行间操作按钮功能

	编辑MRS任务，查看应用的策略。
	删除所选的MRS任务。

## ITM报告设置

管理员可自定义TRS、ARS、ERS、MRS的风险模型及因子基准阈值，显示触发ITM风险阈值的用户及其详细信息，并根据统计数据进行调整，过滤出风险用户。详细信息请参考[ITM报告](#)。

表 181: ITM报告设置

字段	解释
来源Risk Level阈值	设置在ITM报告中展示的内部威胁风险级别（较低、普通、严重、危险、高危），默认级别为危险。

ARS阈值	ARS阈值：设置数据异常行为ARS的阈值，默认7.0； IRS阈值：设置事件数据异常IRS的阈值，默认7.0； DRS阈值：设置应用数据异常DRS的阈值，默认7.0； NRS阈值：设置全网流量异常NRS的阈值，默认7.0。
ERS阈值	ERS阈值：设置专家模式风险ERS的阈值，默认7.0； 员工离职泄密风险阈值：设置员工离职泄密风险的阈值，默认7.0。 感染木马泄密风险阈值：设置感染木马泄密风险的阈值，默认7.0。 恶意用户泄密风险阈值：设置恶意用户泄密风险的阈值，默认7.0。 研发数据泄密风险阈值：设置研发数据泄密风险的阈值，默认7.0。 异常传输泄密风险阈值：设置异常传输泄密风险的阈值，默认7.0。 密送转发泄密风险阈值：设置密送转发泄密风险的阈值，默认7.0。 不良信息发布风险阈值：设置不良信息发布风险的阈值，默认7.0。 MRS阈值：设置事件感知行为模式MRS的阈值，默认7.0。
MRS阈值	输入事件感知行为模式MRS的阈值，默认7.0。

## ITM异常设置

介绍配置ITM异常设置的步骤。

定义异常项分析内容，对同步至移动端的内容进行异常行为分析。

选择系统 > ITM管理 > ITM异常设置进入ITM异常设置页面。

在如下终端异常行为的输入区域，进行参数设置：

异常行为	解释
隐写工具	运行所设置的隐写工具时会触发ITM检测。
远程服务软件	出现所设置的远程服务软件进程时会触发ITM检测。
对外服务软件	出现所设置的对外服务软件进程时会触发ITM检测。
黑名单软件	出现所设置的黑名单软件进程时会触发ITM检测。
工作时间	点击  按钮添加工作时段，在此时间段内会执行ITM检测。如果不设置，系统会避开正常工作时间执行ITM检测。

## ITM报告

介绍内部安全管理报告的相关信息。

ITM报告包括ITM风险用户报告、ITM风险类型报告和ITM异常行为报告。

### ITM风险用户报告

介绍ITM风险用户报告展现风险用户、风险分值及详情。

ITM风险报告展示RiskLevel排名，通过数据异常行为风险*ARS*，事件行为感知泄密风险*MRS*、专家模型行为风险*ERS*及其异常风险评分*TRS*展现个人风险详情、个人历史趋势、各类风险类别用户数量排名及风险趋势；同时可对专家模型风险展现风险详情证据。

ITM相关配置请参考[ITM管理](#)。

#### 查看ITM风险用户报告

ITM风险用户报告用于统计用户的内部威胁风险评分。

选择报告 > ITM报告 > ITM风险用户报告，默认显示当天的RiskLevel对应的用户数量、ITM十大风险类别的风险用户数量和用户风险摘要卡片信息。

在ITM风险用户报告页面，可进行如下操作查看相关ITM风险用户报告：

- 点击柱状图显示当天各用户的内部威胁风险评分及风险排名。
- 点击左右翻页键选择日期或通过日历选择日期，查看某天的ITM报告和风险类别用户数量。
- 点击ITM风险类型显示该风险所包括的用户信息并根据TRS分值排名。ITM风险类型支持多项筛选。
- 点击添加筛选根据登录名、来源IP、来源关键字或用户以及来源Risk Level筛选特定风险用户。
- 点击ITM例外按钮将改用户添加为ITM例外，系统将不对ITM例外对象进行风险统计。详细信息请参考[ITM例外](#) on page 414。
- 点击详情按钮进入ITM风险用户报告个人详情页面，详细信息请参考[查看ITM风险用户报告个人详情](#) on page 416。

#### 查看ITM风险用户报告个人详情

1. 选择报告 > ITM报告 > ITM风险用户报告进入ITM风险用户报告页面。
2. 点击进入ITM风险用户报告个人详情页面，显示数据异常行为风险*ARS*，事件行为感知泄密风险*MRS*，和专家模型行为风险*ERS*的相关数据。

具体显示信息介绍如下：

- 显示风险用户信息属性，包含来源的详细信息、用户登录名、源IP地址、邮箱和部门等。点击ITM例外，系统将不对ITM例外对象进行风险统计。详细信息请参考[ITM例外](#)。
- 显示内部威胁RiskLevel(较低、普通、严重、危险、高危)。
- 显示数据异常风险评分数据异常行为风险*ARS*，根据监控的用户日常行为数据，统计与典型用户行为的偏差值或偏移量，包括数据异常分值 ( DRS )、事件数据异常分值 ( IRS ) 和网络数据异常分值 ( NRS )，并显示当天的ARS、DRS、IRS和NRS的最高分值。
- 显示专家模型行为风险*ERS*，根据预置的专家系统模式，结合贝叶斯算法得到与此专家模式匹配度的风险评分，显示一天内ERS及各专家风险模型最高分值。有关专家风险模型的详细信息请参考[启用专家模型](#)。点击证据详情查看专家模式行为风险证据详情。
- 显示事件行为感知泄密风险行为评分事件行为感知泄密风险*MRS*，根据DLP和ASWG策略生成机器学习模，显示一天内容MRS风险最高分值。详细信息请参考[MRS任务](#)。
- 显示风险分值详情，根据ITM运行频率，统计RiskLevel、MRS、ARS、ERS及其风险类别的分值，选择不同的检测时刻后，动态直观的展现真实的风险数据，关联图默认展示一天内TRS风险分值最高时刻的分值。设置ITM运行频率请参考[ITM管理](#)。



### 查看个人历史趋势

在ITM风险用户报告个人详情页面点击个人历史趋势可查看该用户1天、30天或1年的来源Risk Level、数据异常行为风险ARS、专家模型行为风险ERS和事件行为感知泄密风险MRS趋势图。

- 彩色圆圈代表不同风险类型，点击圆点可选择显示或者不显示该风险类型的趋势图。

## ITM 风险类型报告

介绍 ITM 风险类型报告的相关信息。

ITM风险类型报告用于统计用户的风险类型排名和风险类型趋势等。



ITM风险类型报告显示风险用户数量并展现7天、30天或1年内的高风险类型用户的风险分值排名和泄密次数排名以及趋势图。

ITM预置十大风险类型包括：网络数据异常、应用数据异常、事件数据异常、员工离职泄密、感染木马泄密、恶意用户泄密、研发数据泄密、异常传输泄密、密送转发泄密和不良信息发布。

本章介绍ITM风险类型报告显示风险用户数量，风险分值排名和泄密次数排名以及趋势。

在报告 > ITM报告 > ITM风险类型报告页面查看ITM风险类型报告。

在ITM风险类型报告页面，可进行如下操作查看相关ITM风险类型报告：

- 点击添加筛选可根据关键字或用户目录中的用户筛选出相应来源的风险信息。
- 点击排名中的用户名称或来源IP地址即可跳转至该用户的个人风险详情页面。
- 点击查看某一风险类型全部风险用户的信息。
- 点击列表中的来源IP地址即可跳转至该用户的个人风险详情页面，详细信息请参考[查看ITM风险用户报告个人详情](#)。
- 点击导出某一风险类型的全部风险用户来源、分值排名和次数排名信息。

### 查看ITM风险类型报告

## ITM异常行为报告

介绍ITM异常行为报告的相关信息。

ITM异常行为报告展示终端异常行为，并通过数据异常行为风险ARS，获取Risk Level等用户风险详情数据。

选择报告 > ITM报告 > ITM异常行为报告进入ITM异常行为报告页面，默认显示最近7天的异常行为分值排名、次数排名和数据详情。

异常行为报告提供如下丰富的页面操作按钮，便于管理员查询和管理：

- 添加筛选：根据条件筛选异常行为信息（包括异常行为名称、异常类型、异常时间、参与对象、异常分值和异常描述）、分值排名和次数排名。
- 异常行为包括如下类型，点击蓝色异常行为名称显示详细的趋势分析和原始日志：

异常行为	解释
打印异常	打印文件大小或打印文件数量出现异常
传输大量数据至移动存储	传输至移动存储的文件大小或文件数量过大
通过共享服务外发大量数据	通过共享服务向外发送大量数据
通过蓝牙外发大量数据	通过蓝牙向外发送大量数据
通过Airdrop外发大量数据	通过Airdrop向外发送大量数据
隐藏文件夹	出现隐藏文件夹的行为
更改文件扩展名	出现更改文件扩展名的行为

异常行为	解释
设置浏览器代理	出现设置浏览器代理的行为
关闭防火墙	出现关闭防火墙的行为
运行洋葱浏览器Tor	出现运行洋葱浏览器Tor的行为
运行隐写工具	出现运行隐写工具的行为
账号权限更改	出现账号权限更改的行为
异常账号登录	使用异常账号进行终端登录
异常时间登录	在异常时间进行终端登录
账号变更	创建或删除终端账号
开启本地网络共享	出现开启本地网络共享的行为
运行对外服务软件	出现运行对外服务软件的行为
运行远程服务软件	出现运行远程服务软件的行为
传输数据至本地网络共享	出现传输数据至本地网络共享的行为
应用CloudApp	出现应用CloudApp的行为
运行黑名单软件	出现运行黑名单软件的行为
监控账号状态	出现监控账号状态的行为
注册表变更异常	注册表变更出现异常
截屏异常	出现异常截屏行为
剪切板使用异常	剪切板使用出现异常
VPN使用异常	VPN使用出现异常
目标通信地理位置异常	目标通信地理位置出现异常
HTTP/FTP/Mail出向流量异常	HTTP/FTP/Mail出向流量出现异常



注：关于运行隐写工具、运行对外服务软件、运行远程服务软件、运行黑名单软件和异常时间登录等异常行为需要做相关设置才能获取分析数据，详细信息请参考[ITM异常设置](#) on page 415。

---

# 第 11 章

---

## 术语库

---

内容:

- 安全级别
- 安全策略
- AD (Active Directory)
- APT (Advanced Persistent Threat)
- ARS (Anomaly Risk Score)
- ATS (Apache Traffic Server)
- ASWG (Advanced Secure Web Gateway)
- ASEG (Advanced Secure Email Gateway)
- 必现
- 策略
- 策略匹配
- 策略类型
- 策略组
- 策略等级
- 策略路由
- 串行模式
- CGI (Common Gateway Interface)
- CSV (Comma-Separated Values)
- 对比扫描
- 动作脚本
- DNS (Domain Name System)
- DLP (Data Loss Prevention)
- DSA (Data Scraping Agent)
- DN (Distinguished Name)
- 恶链邮件
- ERS (Expert Risk Score)
- 分析
- 放行
- FPDB (Fingerprint Database)

- 管理平台
- 管理员
- 规则
- GRE (Generic Routing Encapsulation)
- 黑名单
- 忽略
- ICAP (Internet Content Adaptation Protocol )
- ICAP Proxy
- IM (Instant Messaging)
- ITM (Insider Threat Management)
- ITP (Insider Threat Protection)
- 角色
- 漏报
- LDAP (Lightweight Directory Access Protocol)
- MAG (Mobile Access Gateway)
- MIME
- MRS (Model Risk Score)
- MTA (Mail Transfer Agent)
- NFS (Network File System)
- NDR (Notification Delivery Return)
- OCR (Optical Character Recognition)
- 爬虫工具
- 匹配关键字
- 旁路模式
- PAC (Proxy Auto Configuration)
- 权限
- RMS (Microsoft Rights Management Service)
- 事件
- 事件标签
- 数据发现
- 数据聚类
- SIEM (Security Information and Event Management)
- SSL (Security Socket Layer)
- SSL 例外
- SMB (Server Message Block)
- SAM (Security Accounts Manager)
- SMTP
- SPE (Security Policy Engine)
- 通道

- 提级
- 通知
- 透明用户标识
- TRS (Threat Risk Score)
- UCSS (Unified Content Security Server)
- UCSG (Unified Content Security Gateway)
- UCSC (Unified Content Security Client)
- UCWI (Unified Content Web Inspector)
- URL 分类
- UUID (Universally Unique Identifier)
- 外部邮箱
- 误报
- 文件系统目录
- 文件指纹
- 文件类型
- 完整扫描
- 系统完整性保护SIP
- 网络任务
- 终端任务
- 用户
- 用户目录
- 智能学习
- 终端
- 阻断
- 证据
- 真实源IP地址

## 安全级别

---

根据要保护内容的敏感级别来定义安全级别，指定命中策略事件的严重程度。

## 安全策略

---

组织内部的预置策略，用户可直接应用安全策略模板对流量进行监控或拦截。

## AD (Active Directory)

---

AD存储了网络对象的相关信息，例如用户、用户组、计算机、域、组织单位 (OU) 以及安全策略等信息。

## APT (Advanced Persistent Threat)

---

APT是指组织(特别是政府)或者小团体以窃取核心资料为目的，针对客户所发动的长期持续性网络攻击和侵袭行为。

## ARS (Anomaly Risk Score)

---

异常数据风险评分从海量日志中抽取出一组最典型的特征组，并使用统计学算法对所有主机进行全天候的检测，得到每个用户或者IP的异常风险分值。

## ATS (Apache Traffic Server)

---

协议分析引擎是指高性能、模块化的HTTP代理和缓存服务器。

## ASWG (Advanced Secure Web Gateway)

---

增强型Web安全网关基于大数据和机器学习的动态分类技术，集成高级安全内容扫描引擎，跨时间、跨空间、跨计算平台，有效防范APT攻击。

## ASEG (Advanced Secure Email Gateway)

---

增强型安全邮件网关主要防范对企业入向、出向、内部邮件的攻击、垃圾、病毒、恶链和DLP数据防泄漏，以及个人邮件管理、邮件归档等。

## 必现

---

当策略配置多项匹配规则时，只有匹配标记为必现的规则后，才会继续匹配其他策略规则。

## 策略

---

天空卫士的安全策略包括DLP策略和ASWG策略，DLP策略用于监控通过Web、Email、数据发现等通道发送的信息，ASWG策略用于监控公司内部员工的Web访问行为。

## 策略匹配

---

策略匹配是指分析系统中发生的事件，并基于策略判断是授权事件还是违反政策的事件。

## 策略类型

---

将相似的策略分组形成策略类型。天空卫士UCSS支持DLP策略和数据发现策略两种策略类型。

## 策略组

---

将多个策略类型分组形成策略组，可以将这些群组分配给特定管理员，以用于事件管理和监控。通常，一个策略类别组反映与这些事项关联的公司部门，例如“财务部”或“市场部”

## 策略等级

---

策略等级即将策略分级，DLP 和ASWG 策略分别支持31 个等级（其中包含默认等级），策略等级高的优先进行内容匹配。

## 策略路由

---

策略路由通过用户制定的DLP 或ASWG 策略进行转发，且该策略优于路由表的转发，只有本设备发起的数据包匹配其策略路由规则。

## 串行模式

---

数据保护设备的部署方式，串行部署模式即设备部署在网络的数据通道上。

## CGI (Common Gateway Interface)

---

公共网关接口描述了Web 服务器与同一计算机上的软件的通信方式，可以让一个客户端从网页浏览器向在执行在Web 服务器上的程序请求数据。是互联网上网页内容生成与应用的标准技术。

## CSV (Comma-Separated Values)

---

CSV 是一种通用的、相对简单的文件格式，以纯文本形式存储表格数据（数字和文本）。广泛应用于程序之间转移表格数据。

## 对比扫描

---

对比扫描也称差示扫描，收集器只对指定的字段进行扫描，对应于完整扫描。

## 动作脚本

---

动作脚本可用于配置策略引擎和终端触发策略时的行为。

## DNS (Domain Name System)

---

万维网上作为域名和IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的IP 数串。

## DLP (Data Loss Prevention)

---

天空卫士数据防泄漏DLP 产品以集中策略为基础，采用深层内容分析，对静态、传输中及使用中的数据进行分析、识别、监控和保护，智能地管理和保护企业内部的海量的机密及关键数据。

## DSA (Data Scraping Agent)

---

DLP 使用DSA 数据收集器提取指纹规则元素用于创建策略检测内容。

## DN (Distinguished Name)

---

系统中标识用户的唯一识别名称。

## 恶链邮件

---

恶链邮件是指包含恶意网络链接的邮件。

## ERS (Expert Risk Score)

---

专家风险评分ERS 结合专家经验和大数据分析结果，针对得到每个用户或者IP 与同已知风险模式匹配的风险概率值。

## 分析

---

天空卫士UCSS 检查数据是否包含需要保护的含敏感信息的流程。

## 放行

---

对违反策略的行为进行放行操作。

## FPDB (Fingerprint Database)

---

指纹数据库服务器负责存储、管理、同步系统指纹等功能，也提供部分查询功能。

## 管理平台

---

天空卫士管理平台即UCSS，对ITM、ASWG 和DLP 等模块进行统一管理。

## 管理员

---

管理员定义安全策略，并监控安全策略在组织内的分发，以及授权将被阻止的传输内容分发到预定收件人。



## 规则

---

规则为策略提供逻辑，是约束策略行为的条件。

## GRE (Generic Routing Encapsulation)

---

通用路由封装采用Tunnel (隧道) 技术，对某些网络层协议 (如IP 和IPX) 的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议 (如IP) 中传输。

## 黑名单

---

ASWG 模块支持全局黑名单，在特殊情况下阻止指定客户的web 访问请求。

## 忽略

---

如果事件涉及的文件或附件被认为并未违规，或者并没有危害，那么它们可以被设置为忽略。理解忽略事件有助于优化策略，防止对信息流通造成非必要的阻断。天空卫士统一安全平台默认不忽略任何事件。

## ICAP (Internet Content Adaptation Protocol )

---

ICAP 是在HTTP message 上执行RPC 远程过程调用的一种轻量级的协议。

## ICAP Proxy

---

指的是代理软件或代理服务器，也可以认为是一种网络访问方式。

## IM (Instant Messaging)

---

即时通讯是一个实时通信系统，允许两人或多人使用网络，实时传递文字消息、文件、语音与视频交流。

## ITM (Insider Threat Management)

---

内部威胁管理ITM 基于海量数据对内部用户的异常行为或内部威胁进行预测，主动防御数据泄漏，为安全分析人员提供可靠的依据。

## ITP (Insider Threat Protection)

---

基于现有的统一内容安全技术和内部威胁管理技术，实现对内部异常用户行为进行主动防御的解决方案。

## 角色

---

角色拥有UCSS 系统各功能模块不同的访问和操作权限，无需为每个用户定义安全详细信息即可应用到多个用户的安全配置文件。

## 漏报

---

被判断为假的正样本。

## LDAP (Lightweight Directory Access Protocol)

---

轻量目录访问协议基于TCP/IP，提供邮件客户端查询联系人信息所使用的协议标准。天空卫士UCSS 使用LDAP 自动添加用户和用户组到数据库。

## MAG (Mobile Access Gateway)

---

移动接入网关MAG拥有Mobile Email 模块和Mobile App模块。Mobile Email 模块部署于邮件服务器和移动设备邮件客户端之间，对客户端同步的邮件进行DLP 内容检测，放行或阻断命中DLP 策略的邮件；Mobile App模块作为移动安全模块，保护移动设备用户远离任何移动设备通道中的安全威胁。

## MIME

---

MIME (Multipurpose Internet Mail Extensions)为多用途互联网邮件扩展类型。它是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。

## MRS (Model Risk Score)

---

MRS 为事件行为模式风险评分，即针对特定数据泄漏事件进行回溯得到DLP 安全风险模式相似分值。

## MTA (Mail Transfer Agent)

---

UCSS 通过MTA 模块检测和管理其收发的邮件，并记录邮件日志信息。

## NFS (Network File System)

---

UCSS 支持将样本文件存放NFS 服务器上，可以通过网络访问获取并生成指纹文件，减少本地终端存储空间的压力。

## NDR (Notification Delivery Return)

---

当发件人向限制接收该发件人邮件的收件人发送邮件时，可能会收到一个类似于以下内容的未送达报告(NDR)：邮件未送达部分或任何预期的收件人。

## OCR (Optical Character Recognition)

---

天空卫士安全鳄系列产品外置OCR 服务器，可以解析网络流量中的图片内容并进行DLP 分析。

## 爬虫工具

---

负责查找文件中的敏感数据。

## 匹配关键字

---

文档中必须受保护的预定义文本字符串，可能指示文档包含机密信息。

## 旁路模式

---

数据保护设备的部署方式，即设备部署在数据通道外，通过旁路端口连接。

## PAC (Proxy Auto Configuration)

---

PAC 为脚本文件，帮助系统判断使用哪一台代理服务器进行联机以实现代理功能。

## 权限

---

用户在 UCSS 系统中可进行操作的权限。

## RMS (Microsoft Rights Management Service)

---

RMS 是一种信息保护技术，它与启用 RMS 的应用程序配合以帮助保护数字信息避免未经授权的使用。

## 事件

---

事件是违反策略的一项或一组交易。根据配置规则的方式，可为每个策略违反或在规定时间段内发生的匹配创建事件。

## 事件标签

---

事件标签是事件的一种自定义属性，用于识别和筛选具有相似特点的事件。

## 数据发现

---

数据发现是通过扫描文件服务器，邮件服务器，数据库，终端设备和内容共享平台（Microsoft SharePoint 等），以确定敏感性内容在企业网络中的位置的行为。常见的数据发现任务显示设备中被扫描的文件数量、被过滤的文件数量、文件类型分布、敏感文件分布等信息。

## 数据聚类

---

数据聚类利用无监督智能学习对选择的文档自动聚类，提取出数据样本的语义信息生成分类结果形成策略元素。

## SIEM (Security Information and Event Management)

---

SIEM 可以过滤电子邮件，搜索关键词和发现安全缺口，为网络、系统和应用产生的安全信息（包括日志、告警等）进行统一的实时监控、历史分析。

## SSL (Security Socket Layer)

---

SSL 安全套接字层加密连接到服务器，增强外部网络传输的安全性。

## SSL 例外

---

系统对用户行为中属于SSL 例外的IP 视为安全事件，不进行策略检测。

## SMB (Server Message Block)

---

SMB 协议用于Web 连接，客户端与服务器之间的信息沟通。

## SAM (Security Accounts Manager)

---

SAM 用于存储本地用户帐户的安全信息。

## SMTP

---

SMTP 是一种TCP 协议支持的提供可靠且有效电子邮件传输的应用层协议，用于发送邮件给外网用户。

## SPE (Security Policy Engine)

---

安全策略引擎负责查杀病毒、木马、网络威胁和未知威胁等。

## 通道

---

事件所发生的通道，包括Email、Web、FTP、HTTPS、网络打印、IMAP、POP3、云应用和文件共享等。

## 提级

---

提级为DLP 事件的显示状态，其它事件状态还包括新、进行中、关闭和误报。

## 通知

---

通过邮件发送告警信息到管理员或相关人员，包括事件信息、命中策略详情等。

## 透明用户标识

---

天空卫士™统一内容安全UCS提供的一项系统服务，将用户识别代理、用户登录代理获取的IP、用户/计算机的信息传递给安全引擎，进行策略匹配。

XID

## TRS (Threat Risk Score)

---

用户风险评分TRS 是由ARS、MRS、ERS 综合得到的用户内部威胁风险评分值。

## UCSS (Unified Content Security Server)

---

UCSS 统一内容安全管理平台是天空卫士首创的基于内容安全的安全管理系统，承载安全鳄数据防泄漏系统。

## UCSG (Unified Content Security Gateway)

---

天空卫士统一内容安全网关系列产品包括ASWG、DSG 和混合云网关。

## UCSC (Unified Content Security Client)

---

天空卫士安全鳄统一内容安全终端监控终端用户的文件共享、邮件、Web、应用程序等传输的数据，并根据安全策略执行管控。

## UCWI (Unified Content Web Inspector)

---

天空卫士安全鳄统一内容Web 检测条件，与云应用实现API 对接，检测通道流量并生成事件。

## URL 分类

---

天空卫士URL 分类包含最准确，最新以及最全的URL 分类列表。

## UUID (Universally Unique Identifier)

---

流量通用唯一识别码。

## 外部邮箱

---

位于组织或域外部的邮箱账号。

## 误报

---

被判断为真的数据负样本。

## 文件系统目录

---

操作系统中存储文件信息的目录路径。

## 文件指纹

---

文件指纹是由爬虫工具扫描共享文件或文件网站服务器根据一定算法生成的。

## 文件类型

---

文件类型是指电脑为了存储信息而使用的对信息的特殊编码方式，用于识别内部储存的资料。

## 完整扫描

---

对任务设定的全部文件进行扫描，相对于对比扫描。

## 系统完整性保护SIP

---

MAC主机的*System Integrity Protection (SIP)*功能，即系统完整性保护。启用该功能后，可确保即使恶意代码以root权限运行也不会破坏核心系统文件。

## 网络任务

---

用于在网络文件系统、共享目录、Domino 服务器、数据库、Outlook PST、Exchange Online、Salesforce 和邮件反查上设置数据发现。

## 终端任务

---

用于在终端所在的主机上设置数据发现。

## 用户

---

组织内可以进行数据接收和发送的个人。

## 用户目录

---

在天空卫士统一安全系统使用LDAP 进行用户目录自动配置。

## 智能学习

---

智能学习通过正向或反向学习受保护数据的样例，提炼相似信息形成策略规则元素。

## 终端

---

终端安装于用的户计算机，监控终端用户行为。

## 阻断

---

防止需要保护的敏感信息被发送给未授权的用户。

## 证据

---

可用于法律证据的数据泄漏事件鉴定资料。

## 真实源IP地址

---

真实源 IP 检测使用邮件头信息和到达SEG的网络活跃点数来确定网络外围第一个发件人的 IP 地址。此功能可以识别真实的发件人IP地址，即使该邮件经过了NAT或是多重MTA转发以后也可以识别真实的发件人IP地址，并且该真实IP地址可以应用于RBL、全局黑名单等连接状态IP层的控制。





# 索引

## 符號

### 安全策略

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

### 安全管理员必备

#### 数据安全

标签 163

数据分类 163

#### 邮件安全

邮件二级审批 43

邮件审批 43

#### Web安全

数据分类 163

URL分类

分类错误反馈 38

## A

API定义 375

ASWG 79, 125

## B

版本 15

### 报告

发现事件报告 257

风险类型报告 417, 417

风险用户报告 416, 416, 416, 417, 417

网络事件报告 252

#### 移动报告

移动流量报告 351

移动设备报告 350

移动邮件报告 344

应用管理报告 349

用户安全报告 111

#### 邮件报告

出向邮件报告 306

连接日志报告 309

入向邮件报告 302

综合邮件报告 299

终端事件报告 263

DLP报告 251

#### SWG报告

用户安全报告 115

用户行为报告 111

### 必备知识

Web用户界面 25

标签 214, 214, 215, 215

部门 53

## C

策略动作 286

策略模板 288

策略通知 287

### 常用操作知识

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

### 出向邮件报告 306

### 创建定时任务报告

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

### 创建列表报告

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

### 创建趋势报告

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

### 创建图表报告

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

## D

### 大屏实时监控

必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

### 代理模式

反向代理 128, 130, 131, 133, 134

透明代理 128, 130, 131, 133, 134

显式代理 128, 131

登录代理安装包 46

第三方志管理平台 408

调整优先级 50

DLP, 匹配, 例外 173

DLP报告 155

### DLP管理

#### 标签管理

标记文档 215

标签 214

标签设置 215

#### 策略

动作 169

根据模板创建策略 171

根据向导创建策略 169

检测内容

例外 165

匹配 165

来源目标 168

批量管理 172

添加策略 164

通道 166

#### 策略元素

策略动作 184

策略模板 186

策略通知 185

策略组 182

动作脚本 186

来源和目标 183

数据聚类 187

WebService应用 184

#### 规则元素

文件类型组 211, 213

预制数据模板 213

正则表达式 189

指纹 194

智能学习 208

- 字典 190
- 设置
  - 事件设置 237
  - 移动安全设置 238
- 数据发现
  - 网络任务 215
  - 终端任务 234
- 数据分类
  - 分类 181
  - 分类级别 182
- 邮件回溯 236
- DLP监控 155

## F

- 发现事件 257
- 分级对象 54
- 风险类型 417, 417
- 风险用户 416, 416, 416, 417, 417
- FTP 131

## G

- 功能
  - 带宽管理 137
  - 缓存 141
  - 流量整形规则 320
  - 全局控制列表
    - 代理访问规则 143
    - 带宽规则 142
    - 连接控制规则 142
    - 上游代理规则 145
    - DNS分离解析规则 145
    - Socks访问规则 143, 143
    - URL重定向规则 144
  - 网络对象 137, 274, 358
  - 邮件地址改写 321
  - 邮件队列 322
  - 证书 138, 274, 360
  - 自动配置脚本 138
  - DNS解析 146
  - IP伪装 137
  - SOCKS代理 146
  - WCCP 136
- 管理员 55
- 归档 62
- 规则元素
  - 文件类型
    - 扩展名类型 98
    - MIME类型 98
- GatorCloud 369

## H

- 硬件型号 17
- 硬件规格 17
- HTTP 128
- HTTPS 130
- Hybrid 366
- Hybrid虚拟机 365

## I

- IMAP 134
- ITM 416, 416, 417

## J

- 计算机 54
- 监控
  - 审计日志 36
  - 系统日志 37
  - 移动监控
    - 设备安全移动端 339
    - 移动流量统计 341
    - 移动邮件事件 334
    - 应用管理事件
      - 移动流量日志 343
      - 应用管理事件统计 337
  - 移动设备
    - 邮件安全移动端 338
  - 邮件监控
    - 邮件连接日志 297
  - 终端监控 71, 76
  - DLP监控
    - 发现事件
      - 事件详情 246
    - 回溯事件 247
    - 流量日志 250
    - 网络事件
      - 事件详情 242
    - 终端事件
      - 事件详情 75
  - SWG监控
    - 实时日志 110
    - 用户行为日志 107
    - 用户行为统计 104
    - 在线用户 110
  - 监控邮件连接日志 297
  - 监控邮件日志 294
  - 监控终端事件 71
  - 检测设置 293
  - 检测条件
    - 数据安全
      - 附件数量 162
      - 关键字 156
      - 脚本 158
      - 数据库指纹 159
      - 文件大小 161
      - 文件类型 160
      - 文件名称 160
      - 文件指纹 159
      - 正则表达式 82, 157
      - 智能学习 162
      - 字典 159
      - ITM模板 162
    - 移动安全
      - 应用 330
    - 邮件安全
      - 反病毒 282
      - 反垃圾 282
      - URL分类 80, 282

**Web安全**

- 安全URL分类 86, 284
- 关键字 82
- 文件类型 83
- 应用控制 83
- 正则表达式 82, 157
- Cloud App 85
- Header控制 84
- URL分类 80, 282

- 简介 15
- 角色 56

**K****控制台**

- 初始化 20
- 命令行 20

**L**

- 来源和目标 286
- 连接日志报告 309

**M****Mobile管理**

- 策略 330
- 设置
  - 基本设置 333
  - 基本设置高级设置 333
  - 证书管理 333

**N**

- 内部威胁防护 411, 412, 413, 413, 414, 414, 415
- 内部威胁管理 411
- 内容审查
  - 邮件通道 393
  - CloudApp通道
    - 明文内容 396
    - 文本内容 401
  - Web通道 391

**P**

- PEM管理 290, 290, 291, 291
- PEM管理系统 292
- POP3 133

**Q****其他**

- 备份/恢复 61, 151, 277, 325, 362, 374
- 库更新设置 153
- 垃圾病毒库更新 326
- 升级/补丁 61, 152, 277, 325, 362, 374
- 收集日志 60, 151, 277, 325, 362, 374
- 系统工具 62, 153, 278, 326, 363, 375

**R****认证**

- 认证服务器 148, 323
- 添加规则 324
- 账号绑定规则 150
- Windows集成 149, 150
- 入向邮件报告 302

**S****设备**

- 功能
  - 协议 271

**设备管理**

- 必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35
- 基本设置 58, 313
- 授权许可 59, 125, 269, 314, 356, 372
- 网卡配置 270
- 网卡设置 314
- 网络
  - 路由 126, 270, 315, 357
  - 网卡绑定 127
  - 网卡配置 126
- 系统信息
  - 基本设置 125

**SEG**

- 接收和发送 317
- 真实源IP 319
- SMTP 316
- TCP代理 316

**设备监控**

- 必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35
- 设置 293
- 审计日志 36
- 数据安全 155, 165, 166, 168, 169
- 数据安全报告 251
- 数据安全策略 182
- 数据安全治理 164, 164, 169, 171, 172, 182, 183, 184, 184, 185, 186, 186, 187, 189, 190, 194, 208, 211, 213, 213, 215, 234, 237, 238
- 数据安全规则 189
- 数据安全监控 75, 242, 246
- 数据发现 215
- 数据防泄漏DLP 182, 189, 215, 236
- SEG 313, 314, 316, 316, 317, 319

**SEG管理**

- 全局控制
  - 白名单 289
  - 黑名单 290
- 设置
  - 检测设置 293

**PEM管理**

- 基本设置 291
- 邮件摘要管理 291
- SSL证书 290

**SMTP**

- SMTP MTA 146
- SMTP Proxy 133

**SWG**

- 其他 153, 278

自定义页面 153, 278

## SWG管理

### 策略

- 动作 90
- 根据模板创建策略 91
- 检测内容
  - 例外 89
  - 匹配 89
- 来源 90
- 批量管理 92
- 添加策略 88
- 通道 89

### 策略元素

- 策略模板 95
- 带宽限速 94
- 来源 93
- 时段 94

### 规则元素

- 风险级别 97
- 风险类别 97
- Cloud App 96

### 全局控制

- 白名单 99
- 黑名单 100

### 设置

- 安全扫描 102
- 基本设置 101
- 设置日志 103
- Cloud App更新 103

SWG监控 104

Syslog 47, 408

## T

添加策略 285

TLS证书 322

## U

URL分类 48, 49

URL分类更新 49

## W

### 网络

网卡绑定 271, 315, 357

网络事件 252

Web安全 79, 86, 87, 88, 89, 89, 90, 90, 91, 92, 93, 94, 94, 95, 96, 96, 97, 97, 98, 98, 99, 100, 101, 103

Web安全策略 93

Web安全监控 104, 110

Web安全设置 101, 102, 103

### Web用户界面

- 标题栏 25
- 菜单栏 26
- 快速跳转按钮 28
- 浏览器 28
- 设备管理页面 29
- 设置 31
- 系统健康状态 32

页面信息概述 28

## X

### 系统

归档 62

#### 基本设置

- 报告设置 40
- 存储设置 40
- 授信地址 47
- 系统通知 41
- 用户识别
  - 登录代理安装包 46

邮件服务器 41

邮件告警 41

邮件释放 42

SIEM 48, 409

SSL例外 47

Syslog 47, 408

URL分类 48

URL分类更新 49

#### 设备管理

编辑高可用 154, 279, 327

#### 功能

- 代理服务 127
- 网络抓取文件 146
- 邮件队列 138, 274
- 主机/主机组 134
- ICAP 135

基本设置 269, 356

#### 其他

- SNMP 60, 61, 151, 152, 276, 278, 324, 326, 361, 363, 373, 375
- 全局例外 140, 275, 359
- 添加高可用 154, 279, 327
- OCR 60, 140, 275, 322, 359, 373

#### 用户管理

- 分级对象 54
- 用户目录 50
- 用户目录组 53
- 用户凭证 54
- 账户管理
  - 管理员 55
  - 角色 56
- 组织架构
  - 部门 53
  - 计算机 54
  - 用户 53

#### 邮件审批

- 审批架构 44
- 审批平台设置 45

#### 终端管理

- 全局设置 65
- 终端安装包 70
- 终端白名单 68
- 终端配置 67
- 终端设备 70
- 终端协议 70

Hybrid 366

#### ITM管理

专家模型 413

- ITM报告设置 414
- ITM例外 414
- ITM设置 412
- ITM异常设置 415
- MRS任务 413
- Mobile管理
  - 客户端管理
    - 安全域配置 332
    - 客户端安装包 332
    - 客户端配置 331
- 系统服务 20
- 系统健康状态
  - 必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35
- 系统日志 37
- 协议配置 358
- 修改个人信息 26
- 修改密码 26

- 修改个人信息 26
- 修改密码 26
- 主页显示模板
  - 必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35
- 资源获取
  - 获取报告 388
  - 获取事件列表 384
  - 获取事件详情 385
  - 获取通道 381
  - 获取通道详细信息 382
  - 获取证据文件 387
- 自定义页面 153, 278
- 综合邮件报告 299
- 组件介绍 16
- 组织架构 53
- 最近访问报告
  - 必备知识 24, 25, 30, 32, 32, 32, 33, 33, 34, 34, 34, 35, 35

## Y

- 移动安全 329
- 移动安全报告 344
- 移动安全管理 330, 330, 331, 332, 332, 333
- 移动安全监控 334
- 移动流量报告 351
- 移动事件 344
- 移动应用 331
- 用户 53
- 用户目录
  - Active Directory 50
  - ADAM 51
  - CSV 52
  - Domino 52
  - LDAP 51
- 用户目录同步详情 50
- 用户目录组 53
- 用户凭证 54
- 用户识别 46
- 用户行为 111, 111, 115
- 邮件安全 281, 285, 286, 286, 287, 288, 289, 289, 290
- 邮件安全报告 298
- 邮件安全监控 295
- 邮件工作流 237
- 邮件回溯 236
- 邮件监控
  - 邮件日志
    - 邮件日志详情 295
- 云应用更新 103

## Z

- 终端安全管理 65, 67, 68, 68, 70, 70, 70
- 终端安全监控 71
- 终端管理
  - 终端应用程序类别
    - 终端应用程序 69
- 终端事件 263
- 主页
  - 设置显示模板 31
  - 系统健康状态 32

