

# 数据外泄管理系统(Leak Proof)

# Data Loss Prevention 5.5

# 产品安装标准程序(SOP)



趋势科技技术支持部

唐寅如

2011年01月



目 录

1	什么是 DATA LOSS PREVENTION?	. 4
1	1 DATA LOSS PREVENTION 产品体系结构和机制	. 4
1	2 DATA LOSS PREVENTION (DLP) 5.5 系列的各个组件	. 5
	1.2.1 Data Loss Prevention Server (服务端)	5
	1.2.2 Data Loss Prevention Endpoint (客户端)	5
	1.2.3 Data Loss Prevention Network Monitor 2.0 (网络监控)	6
1	3 DATA LOSS PREVENTION (DLP) 5.5 新功能一部分	. 6
2	DATA LOSS PREVENTION 产品系统需求	. 7
2	1 DIP 5 5 服务端 (DATA LOSS PREVENTION SERVER)	7
2	2 DIP 5.5 客户端(ENTR POINT AGENT)	. 8
2	3 DLP REMOTE CRAWLER	.9
2	4 TMDLPNM 2. 0 (Network Monitor Agent)	.9
3	标准安装流程....................................	10
0		10
3	I 女袋 DLP 5.5 服务辆	10
	5.1.1	10
	5.1.2	10
9	3.1.5 _ 又农口的忉知化癿且(里安)	19
	2 <b>父农 DLI 5.5 在广调</b> 3 2 1 <i>字</i>	20
	3.2.1	20
3	3.2.2 又农廷住	30
J	3	30
	3.3.1     又农前口作留       3.3.2     安装的讨程	30
	333 安装后的初始化配置	30
3	4 如何检查标准安装是否成功	33
-	3.4.1 DLP 5.5 服务端	33
	3.4.2 DLP 5.5 客户端	33
	3.4.3 TMDLPNM2.0	35
4	DLP 的基本配置	37
4	1 DLP 服务端的基本配置	37
	4.1.1 DLP 产品激活	37
	4.1.2 DLP 策略设置	37
	4.1.3 DLP 策略部署	45
	4.1.4 DLP 设备管控	51
4	2   DLP 服务端的其他设定	52
	4.2.1 Data Discovery	52
	4.2.2 Reports 报表生成	54
	4.2.3 DLP 产品补丁更新/安装	57
	4.2.4 DLP 的 Administration 设定	58
	4.2.5 各尸端收集 Debug 日志万式	64
5	通信端口列表	65
6	趋势科技厂商资源	66



趋势科技Leak Proof是一种数据丢失预防(DLP) 解决方案。凭借最广泛的覆盖范围,最出色的性能 和灵活部署而降低了其复杂性和成本.Leak Proof 通过保护员工和客户数据以帮助企业用户符合监管 需求,还能提供用户保护知识产权的DataDNA指纹技 术。此版本包括DLP客户端和DLP服务器。

数据丢失预防特征在于:成本和复杂性更低、 增强的隐私保护、数据发现和扫描、高级知识产权

保护、互动性员工教育和补救。

注意:由于DLP产品在整个安装、配置过程中,有一些需要注意的配置设定,在此SOP标准操作手册中会指导如何设定,建议部署/测试之前,仔细阅读。

版本	更新内容	日期	作者
1.0	initial	2011-01-06	Mac Tang

TREND

# 1 什么是 Data Loss Prevention?

数据丢失预防(DLP)是防止意外和恶意数据泄漏的关键所在---不论是客户信息, 财务数据,知识产权还是商业机密。一次事故可能导致品牌声誉受损、丢失业务、 罚款或法律诉讼从而造成数百万元的损失。

数据丢失面临的难题就是如何识别,跟踪并保护所处于闲置、使用和移动状态的 机密数据。这项工作正在因为风险因素的增加而变得日益困难,包括陷入失业恐慌 的失业员工,移动工作人员以及USB驱动器,网络电子邮件,即时通讯和CD/DVD之类 的泄漏渠道。

## 1.1 Data Loss Prevention 产品体系结构和机制

Data Loss Prevention (DLP) 系列产品体系整体架构如下:





	指纹匹配能够对非结构化的内容文档进行最佳操作,DLP 提取并存储敏感	
	文档后 , 如果终端用户尝试传输一个文件 , DLP 会提取传输的文件指纹信	
Fingerprint Matching	息与已保存的指纹库进行匹配。如果两者具有相同点,DLP将计算两者之	
(指纹匹配)	间的相同点的比例.DLP 设定匹配等级分为高、中、低 , 相同越高匹配等	
	级越高,一旦匹配等级达到 DLP 设定的等级,DLP 则把此文件视为敏感	
	文件。DLP 存储的指纹大小取决于文件的数量和大小。	
Dattarn Matching	DLP 基于用户自定义的样式进行匹配,例如身份证号等,DLP 能够与非	
	结构化的内容文档进行最佳操作,例如信用卡号、身份证信息、电话号码	
	等。管理员可以通过正则表达式自定义 Pattern	
Keyword Matching		
(关键字匹配)	DLP可以根据大键子进行匹配	
File Attribute Matching (文件扩展名匹配 )	DLP 可以根据文件的类型进行匹配,特别的是 DLP 具有真实文件类型的 检测能力,即时文件扩展名已经被更改或者无扩展名的文件。 Compliance template 匹配	

## 1.2 Data Loss Prevention(DLP) 5.5 系列的各个组件

Trendmicro<sup>™</sup> Data Loss Prevention (DLP) 是一套全面的解决方案,帮助企业组 织敏感信息被意外的泄漏和恶意的盗窃。DLP Agent 客户端使用独一无二的高准确的 数据指纹技术和内容匹配技术防止数据泄密。

### 1.2.1 Data Loss Prevention Server (服务端)

DLP 服务端是一款硬件设备,提供集中控制管理、策略配置和下发、产品组件更 新、日志查询、报表生成、数据指纹获取等中央控制管理操作平台。

### 1.2.2 Data Loss Prevention Endpoint (客户端)

DLP客户端可以检测数字资产并自动根据公司策略设定对泄密的操作做出阻止、 日志记录、加密、警告等操作。

支持终端用户设备访问控制,支持USB, CD/DVD,COM&LPT端口, IEEE 1394,USB 存储设备,Floppy, 红外设备,图像设备,Windows自带Print截图工具,Modems, PCMCIA适配。

扩大隐私保护,支持MSN、Skype, P2P, Windows<sup>™</sup> 局域网文件共享SMB协议, ActiveSync, 剪贴板,本地/网络共享打印机。

覆盖广阔的通信系统保护,包括: Email客户端(例如Outlook、Lotus Notes),



Webmail, HTTP/HTTPS, FTP 支持终端输入输出设备,包括:USB存储设备,CD\DVD刻录 与Active Directory集成 敏感文件扫描,以发现终端笔记本、台式机、服务器上存有的敏感文件。 支持超过300种以上的文件类型,并支持自定义扩展名文件属性。

### 1.2.3 Data Loss Prevention Network Monitor 2.0 (网络监控)

TMDLPMN 是一款基于扫描网络镜像数据,通过监控网络数据流量来检测数据威胁的产品:

- •Sensitive data
- •IP address
- •Regulatory compliance
- •Data stealing malware

DLP Netork Monitor(TMDLPMN)与DLP服务端集成,接受DLP服务端的管理和策略 下发、产品组件更新、Pattern更新等操作,并将检测到的事件日志传给DLP服务端。

- 通过扫描数据,检测内网与外网的敏感信息数据传输,包括: SMTP, HTTP, FTP,
- IM (AIM/AOL, MSN, Yahoo Messenger), and Webmail (Hotmail, Gmail, Yahoo) 支持最常用的局域网文件共享SMB协议。 注意:此款产品需要单独购买

备注: DLP Network Monitor在扫描网络镜像口流量之前,必须先注册到DLP服务端上,并激活

## 1.3 Data Loss Prevention (DLP) 5.5 新功能—部分

- 1) Web 控制台界面进一步优化
- 2) 增加 TMDLPMN2.0 网络监控产品(需要单独购买)
- 3) Remote Crawler 工具: 支持 Windows 64 位操作系统
- 4) 高级日志管理
- 5) 增加数据防偷窃 Pattern 病毒码组件-- Network Content Correlation Pattern (NCCP): Data Stealing Malware (DSM)/botnet detection
- 6) 基于不同策略设定黑白名单
- 7) 基于不同策略设定不同弹出警告框内容

# 2 Data Loss Prevention 产品系统需求

## 2.1 DLP 5.5 服务端(Data Loss Prevention Server)

### 硬件平台(DELL OEM)

产品类型:	Data Loss Prevention Server Appliance
设备规格:	Dell R610 1U2P DxWxH(30.39"x18.99"x1.68") Weight: 17.69Kgs
设备型号:	R610 : Dell PowerEdge R610 Rack Mount Server
CPU:	Xeon E5506, 2.13GHz
内存:	6GB, 6*1G UDIMM,1333 MHZ
Hard Drive Controller	SAS 6/iR Controller Card
硬盘:1st Hard Drive	2.5 SATA(7.2K RPM): 250GB
硬盘:2nd Hard Drive	2.5 SATA(7.2K RPM): 250GB
光驱:	DVD ROM, SATA
网口:	Four embedded Broadcom® NetXtreme II™ 5709c Gigabit Ethernet NIC
External NIC card	no
PSU	1x 717W
Misc	Rapid/Versa Rails
操作系统版本	CentOS version 4.6 operating system(DLP 系统自带, 无需单独安装)

### Vmware 虚拟机平台(最低需求)

产品类型:	Data Loss Prevention Server(DLP)
CPU:	最低: Intel(TM) Pentium(TM) 1024MHz (建议: Intel(TM) Pentium(TM) 2048MHz 或更高)



内存:	最低: 2048MB RAM (建议: 4096MB 或更高)
硬盘:	最低: 30G 可用空间 (建议: 200G 或更高)
网卡:	10/100 Mbps NIC (建议: 1000Mbps千兆网卡)

# 2.2 DLP 5.5 客户端(End Point Agent)

### DSA 最低硬件配置需求:

产品类型:	Data Loss Prevention Agent(DLP)	
CPU: 最低: Intel(TM) Pentium(TM) 300MHz (建议: Intel(TM) Pentium(TM) 1024MHz 或更高)		
内存:	最低: 128MB RAM (建议: 1024MB 或更高)	
硬盘: 最低: 300M 可用空间 (建议: 1G 或更高)		
网卡:	10/100 Mbps NIC (建议: 1000Mbps千兆网卡)	

### DSA 支持的操作系统

注意: (目前 DSA 只支持 Windows 操作系统平台 32bit 的客户端,)

Windows 7 Professional
Windows 7 Ultimate
Windows 7 Enterprise
Windows 7 Starter
Windows 7 Home Basic
Windows 7 Home Premium
Windows 2008 Datacenter SP1/SP2
Windows 2008 Enterprise SP1/SP2
Windows 2008 Standard SP1/SP2
Windows 2003 Enterprise SP1/SP2
Windows 2003 Datacenter SP2
Windows 2003 Standard SP1/SP2

Windows	2003 Web Edition SP2
Windows	2003 Standard R2 SP1/SP2
Windows	2003 Enterprise R2 SP1/SP2
Windows	Vista Enterprise SP1/SP2
Windows	Vista Business SP1/SP2
Windows	Vista Home Premium SP1/SP2
Windows	Vista Ultimate SP1/SP2
Windows	Vista Home Basic SP1/SP2
Windows	XP Professional SP2/SP3
Windows	XP Tablet 2005
Windows	XP Home SP2/SP3
Windows	XP Media Center SP2/SP3



## 2.3 DLP Remote Crawler

备注: Remote Crawler 是一种获取指纹的工具(在 DLP 服务端安装后的 web 管理控制台中可以下载获取到)。

DLP 服务器获取文件指纹信息提供两种方法,

1)通过共享方式访问用户存放敏感文件的服务器,以抓取文件的指纹。

2) 在文件服务器上安装 Remote Crawler 工具,安装后,通过此工具的 UI 界面,执 行需要抓取指纹目录,抓取指纹后传给 DLP 服务端.

此处是第 2 种方法,适用于需要被 DLP 服务端采集数据指纹的文件服务器上的文件 目录未被共享,即 DLP 服务端无法通过共享方式访问具有敏感文件的服务器,以获取 到这些文件的数据指纹。

#### Remote Crawler 支持的操作系统

备注:除了 DSA 支持的所有操作系统外,还额外支持以下的 64bit 操作系统:

64 bit Windows 2003	Enterprise SP1/SP2
64 bit Windows 2003	Enterprise R2 SP1/SP2
64 bit Windows 2008	Enterprise SP1/SP2

## 2.4 TMDLPNM 2.0 (Network Monitor Agent)

#### 硬件平台(DELL OEM)

产品类型:	Data Loss Prevention Network Monitor Appliance (Dell R710)
CPU:	2 x Intel® Quad Core X5550 Xeon® CPU, 2.66GHz
内存:	8GB Memory (4x2GB)
硬盘:	300GB
网卡:	Gigabit NIC
操作系统版本	CentOS version 5.3 operating system(DLP 系统自带, 无需单独安装)

# 3标准安装流程

3.1 安装 DLP 5.5 服务端

### 3.1.1 安装前的准备

1) DLP5.5 服务端 ISO 文件下载: 注意:下载完毕后,请使用 MD5 工具进行校验,确保下载的文件完整(非常重要!)

DLP5.5 安装在 DELL R610 OEM 的 DLP 服务器上
 显示器、USB 键盘、ISO 光盘
 注意: DLP5.5 的 ISO 文件目前已超过 700M,请使用 DVD 刻录机刻录 DVD 光盘。

 3) DLP5.5 安装在 Vmware 虚拟机上
 硬件配置请参考《DLP5.5 服务端系统需求》章节
 注意:如果硬件达不到硬件配置需要,在引导界面按 TAB 键,增加参数: nohwfail 此参数仅适用于测试时使用。



## 3.1.2 安装的过程

1. 在 DLP 服务器光驱中放入刻录好的光盘或者 Vmware 上引导 ISO 镜像



2. 如果您的硬件/Vmware 配置不满足 DLP 服务端硬件要求,按 TAB 键,输入 nohwfail 注意: 趋势科技强烈建议使用满足硬件配置的设备安装 DLP 服务端。





3. 接受许可协议,点击 Accept

TREND Data Loss Prevention
License Agreement
IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS
Trend Micro License Agreement
Trial and Paid Use License - Enterprise and SMB Software and Services Personal Use License - Trend Micro Email Encryption Client Date: February 2009 English/Multi-country
<ol> <li>Scope. This Agreement applies to all Trend Micro software ("Software"), services sold as standalone products ("Standalone Services") and service components of Software ("Service Components") sold to small and medium business ("SMB") and large enterprises ("Enterprise"). Standalone Services and Service Components are collectively referred to as "Services". This Agreement shall also apply to Trend Micro Email Encryption Client ("TMEEC") for personal use. The term "Software" as used herein shall include TMEEC. Professional or expert service offerings are governed by other agreements.</li> <li>Binding Contract. This License Agreement ("Agreement") is a binding contract between Trend Micro Incorporated or a licensed affiliate ("Trend Micro") and the legal entity that will be using Trend Micro Software or Services on a paid or trial use basis or individuals who will be using TMEEC on a personal use <b>v</b></li> </ol>
<b>X</b> <u>D</u> ecline <b>√</b> <u>A</u> ccept



4. 选择安装向导语言类型,选择默认,点击 Next

## Data Loss Prevention

Select the appropriate keyboard for the system.	
Slovakian	<b>_</b>
Slovenian	
Spanish	
Swedish	
Swiss French	
Swiss French (latin1)	
Swiss German	
Swiss German (latin1)	
Tamil (Inscript)	
Tamil (Typewriter)	
Turkish	
Ukrainian	
United Kingdom	
U.S. English	
U.S. International	-
⇔ <u>B</u> ack	xt

### 5. 安装系统检测的当前配置概要,点击 Next

注意: 红色为提示当前不满足建议需求的硬件配置, 如没有 Next 按钮, 则参考第 2 步

## **Data Loss Prevention**

Category	Device		Driver	
Host Configuration				
	Processor Model: Intel(R) Core(TM) i5 CPU	760 @ 2.80GHz		
	Processor Speed: 2797MHz			
	Number of processors: 1			
	System Memory: 1010MB			
Network Devices				
	82545EM Gigabit Ethernet Controller (Copper)		e1000	
Storage Controllers				
	82371AB/EB/MB PIIX4 IDE		PIIX_IDE	
	53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI		mptspi	
Storage Devices				
	VMware, VMware Virtual S (20GB)			
Removable Media				



6. 提示是否全部擦除当前硬盘上的所有文件,点击 Next



7. 配置 DLP 网络信息,配置完后,点击 Next 注意: hostname 需要填写 FQDN 形式,否则会提示错误。

## Data Loss Prevention

• eth0         Intel Corporation 82545EM Gigabit Ethernet Contr 192.168.1.111/           terface Settings(IPv4/Netmask)           v4 Address:         192.168.1.111 / 255.255.255.0           aneral Settings           ostname:         dlp55.mac.com           ateway:         192.168.1.1           imary DNS:         192.168.1.1           condary DNS:         202.96.209.5	laster Port	Device	Description	IF	Pv4/Netma	sk
Terface Settings(IPv4/Netmask)         v4 Address:       192.168.1.111       /       255.255.255.0         Ineral Settings         ostname:       dlp55.mac.com         ateway:       192.168.1.1         mary DNS:       192.168.1.1	0	eth0	Intel Corporation 82545EM Gigabit Ethernet Con	tr 1	192.168.1.1	111/24
terface Settings(IPv4/Netmask)         v4 Address:         192.168.1.111       /         /         aneral Settings         ostname:         dlp55.mac.com         ateway:       192.168.1.1         imary DNS:       192.168.1.1         2condary DNS:       202.96.209.5						
terface Settings(IPv4/Netmask)         v4 Address:       192.168.1.111       /       255.255.0         eneral Settings         ostname:       dlp55.mac.com         ateway:       192.168.1.1       -         imary DNS:       192.168.1.1       -         condary DNS:       202.96.209.5       -						<b>▶</b>
v4 Address:       192.168.1.111       /       255.255.0         eneral Settings       ostname:       dlp55.mac.com         ateway:       192.168.1.1       -         rimary DNS:       192.168.1.1       -         econdary DNS:       202.96.209.5       -	nterface Se	ettings(I	Pv4/Netmask)			
eneral Settings ostname: dlp55.mac.com ateway: 192.168.1.1 rimary DNS: 192.168.1.1 econdary DNS: 202.96.209.5	Pv4 Address	: 192.	168.1.111 / 255.255.255.0			
ostname: dlp55.mac.com ateway: 192.168.1.1 rimary DNS: 192.168.1.1 econdary DNS: 202.96.209.5	eneral Set	tinas				
ateway: 192.168.1.1 rimary DNS: 192.168.1.1 econdary DNS: 202.96.209.5	lostname:	dlp5	5.mac.com			
rimary DNS: 192.168.1.1 econdary DNS: 202.96.209.5	Gateway:	192.	168.1.1			
econdary DNS: 202.96.209.5	rimary DNS	: 192.	168.1.1			
	econdary D	NS: 202.9	96.209.5			
			·			
				4	<b>∃</b> <u>B</u> ack	×
<b>⊉</b> <u>B</u> ack						_

8. 选择当前所在地的时区,例如选择 Asia/Shanghai,点击 Next **② TRENS** Data Loss Prevention



- 9. 设定系统账号密码,设置完毕后,点击 Next
- 注意: Root Account: 为安装完后 Linux 系统 Root 账号密码(Root 账号为最高权限) Enable Account: 为在 Linux 命令行模式下进入 CLI 菜单配置模式账号密码 Admin Account: 为 DLP 服务端 Web 控制台的密码,默认用户名为:admin DLP Service' default Account: 为 DLP 服务关联需要的密码
- 备注: 密码长度最小需要 8 位

## Data Loss Prevention

逫 Plea	ase set passwords for the administrative accounts below. Combi	ned Password St	rength
Root Acco shell. Has	unt: Used to safeguard access to the operating system full operating system privileges.		Good
Password:	•••••	Moderate	
Confirm:	•••••	Confirmed	
Enable Ac Interface's	count: Used to gain access to the Command Line (CLI) privilege mode. Has access to all CLI commands.		
Password:	•••••	Moderate	
Confirm:	•••••	Confirmed	
Admin Ac	count: Administration Account. Used to run CLI and logon manager console.		
Password:	•••••	Moderate	
Confirm:	•••••	Confirmed	
DLP Service	es' default Account.		
Password:	•••••	Moderate	
Confirm:	•••••	Confirmed	
			Poor
		XCancel	<b>⊳</b> <u>N</u> ext

### 10. 显示之前配置总概况信息,如确定,请点击 Next,需要更改点击 Back

## **Data Loss Prevention**

Summary:		
Language: Keyboard: Hostname: Network Dev	en_US.UTF-8 U.S. English dlp55.mac.com rices: Card: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) Device: eth0 IP Address: 192.168.1.111 Subnet mask: 255.255.255.0 Gateway: 192.168.1.1 Primary DNS: 192.168.1.1 Secondary DNS: 202.96.209.5	
Time zone:	Asia/shanghai	
	DLP will now be installed on your selected drive(s).	
	ack	<b>X</b> <u>C</u> ancel



11. 安装前的最后确认,请点击 Next



12. DLP 系统开始安装,所需时间因系统配置不同而不同,大约 10-20 分钟







14. 待出现此界面, DLP 服务端安装完毕。

CentOS release 4.6 (Final) Kernel 2.6.18-92.el5 on an i686 dlp55 login: CentOS release 4.6 (Final) Kernel 2.6.18-92.el5 on an i686 dlp55 login: \_

15. 安装完毕后,请继续参考一下部分的 DLP 服务端初始化配置。 注意:为确保正常使用,强烈建议执行初始化操作。

## 3.1.3 安装后的初始化配置(重要)

 打开控制台,输入用户名和密码 打开方式: <u>https://ip:8443/dsc</u> 用户名: admin 密码: 为安装时自定义

# TREND Data Loss Prevention

Type your user name and password to access the web console.	
User name:	
Password: Log On	

© Copyright 2005-2010 Trend Micro Incorporated. All rights reserved.

#### 2. 输入产品许可证,激活 DLP 服务端 注意:如果 DLP 不输入激活码,将无法使用 Fingerprints 指纹获取功能

#### 1) 点击 Adminisratrion---Product license---DLP Endpoint

Data Loss	Prevention				Logged on as:	<sup>8</sup> admin
Summary	Product License					🕜 Help
+ Data Protection	Use this page to view a list of a	all DLP Endpoint and Network Mo	nitor licenses.			
+ Reports	License Information					
+ Logs	Product Name	IP Address(Host Name)	Product Version	License Status	Expiration Date	
+ Update	i roduce nume		rioduce version	Electibe blacks	Expiration bate	
- Administration	DLP Endpoint	127.0.0.1(localhost)	DSC-5.5-1294	Not Activated	Not Available	
<ul> <li>Server Configuration</li> </ul>						
+ Agent Configuration						
Crawler Management						
Data Management						
Agent Management						
Password						
<ul> <li>Management Console</li> </ul>						
LDAP						
Product License						



#### Product License

Product License > License Details

X The product has not been activate	ed.	View renewal instructions	
Trend Micro™ Data Loss Prevention Endpoint			
Product:	Trend Micro™ Data Loss Prevention Endpoint (DSC-5.5-1294)		
Version:	N/A		
Activation code:	N/A	Enter a new code	
Seats:	N/A		
Status:	Not Activated		
Maintenance expiration:	N/A		

#### 2) 激活后的状态

Trend Micro™ Data Loss Pre	vention Endpoint	View detailed license online
Product:	Trend Micro <sup>™</sup> Data Loss Prevention Endpoint (DSC-5.5-1294)	
Version:	Full	
Activation code:		Enter a new code
Seats:	—	
Status:	Activated	
Maintenance expiration:	Jan 6, 2011	
		Check Status Online
		Last Status Check on Dec 25, 2010
Product License		🔁 Help

Use this page to view a list of all DLP Endpoint and Network Monitor licenses.

License Information				
Product Name	IP Address(Host Name)	Product Version	License Status	Expiration Date
DLP Endpoint	127.0.0.1(localhost)	DSC-5.5-1294	Activated	2011

3) 激活完毕后,注销控制台,请再次登录

🕜 Help



3. 更改 DLP 服务端访问控制配置
注意:此配置非常重要。因基于默认安全策略考虑,DLP 服务端安装完后默认限定如下:

a) DLP 服务端默认只允许与其同一网段的 DLP 客户端连接注册
b) DLP 服务端默认只允许与其同一个网段的 PC 机访问其 Web 控制台
c) DLP 服务端默认只允许与其同一个网段的 PC 机使用 SSH 远程登录 DLP 服务端所以需要根据如下步骤进行操作:

1) 使用显示器和键盘,进入 DLP 服务端的 linux 内核 输入 clish
CentOS release 4.6 (Final)
Kernel 2.6.18-92.el5 on an i686
dlp55 login: root
Password:
Last login: Sun Dec 19 19:29:10 on tty1
Iroot@dlp55 ~ ]# clish

WARNING: Authorized Access Only

Welcome to DLP VA CLI. it is Sun Dec 19 19:35:50 CST 2010

2) 输入 enable,进入特权模式后,输入 configure DLP,按回车



aliah

### 数据外泄管理系统 DLP5.5

***************************************	<del>ex</del>
* Trend Micro Data Loss Prevention (DLP)	*
*	*
<ul> <li>WARNING: Authorized Access Only</li> </ul>	*
*******************	<del>* ×</del>
Welcome to DLP VA CLI. it is Sun Dec 19 19:37:04 CST 2010 > en enable enable-shell > enable	
Entering privileged mode # configure date DLP dns hostname interface password # configure DLP	route timezone

3) 在出现的配置菜单中,选择1 System Configureation

	* <mark>**************Configuration*</mark> *********		
	<ul> <li>* 1. System Configuration</li> </ul>	*	
	* Z. Shutdown	*	
	**********	************	
Select:	1_		

 4) 在此可以再次验证之前安装时配置的 IP、掩码、网关等信息是否正确。
 注意:如需要修改则可以进行修改,如无需修改,则直接按回车。配置完毕后,在最后的信息确 认后,按 y

The	The Network Configuration					
The The The The	IP for eth0: [192 netmask for eth0: gateway for eth0: onboot for eth0:	2.168.1.111] [255.255.255.0] [] [yes]	_			
For	eth0 setting:					
	IP:	192.168.1.111				
	Netmask:	255.255.255.0				
	Gateway:					
	Onboot:	yes				
Is '	the setting right	(type 'q' to quit	from config)?	(y/n/q): y_		

5) 在此可以再次验证之前安装时配置的 DNS 信息是否正确。

注意:如需要修改则可以进行修改,如无需修改,则直接按回车。配置完毕后,在最后的信息确 认后,按 y



Is the setting r	ʻight (type 'q'	to quit from	config)? (y	/n/q): y		
The DNS server ip list: [192.168.1.1 202.96.209.5] The DNS search suffix list: [mac.com]						
The DNS setting: DNS ip I DNS sear	list: ch suffix:	192.168.1.1 mac.com	202.96.209.	5		
Is the setting r Network configur	ation has been	to quit from done. press a	config)? (y any key to c	/n/q):y ontinuc		

<u>验证完毕后,请按任意键进行 DLP 服务端安全配置,很重要!</u>









6) 此部分如[]中显示,DLP 服务端默认只允许与其同一网段的 DLP 客户端连接注册, 请改为 ANY(注意: ANY 需要全部大写)

注意:此步骤非常关键,即如果不修改,默认情况下与 DLP 服务端不同网段的客户端安装后在控制台上将不显示。

配置完毕后,在最后的信息确认后,按y Network Security Configuration : please refer to Trend Micro Data Loss Prevention (DLP) Manual The subnet/ip list where DLP agents will be deployed(ip or subnet list/ANY): [19 2.168.1.111/255.255.255.0] ANY The ports to listen agents: [18804 8904] The UDP ports to listen agents: [1558] The agents related setting: The subnet/ip list: ANY The ports: 8804 8904 The UDP ports: 1558 Is the setting right (type 'q' to quit from config)? (y/n/q): y\_

7) 此部分如[]中显示, DLP 服务端默认只允许与其同一网段的 PC 机打开 DLP 的 Web 控制台,这里请改为 ANY (注意: ANY 需要全部大写),端口无需改动

注意:此步骤非常关键,即如果不修改,默认情况下与 DLP 服务端不同网段的 PC 机将无法打开 DLP 控制台。

配置完毕后,在最后的信息确认后,按 y	
The submet/ip list from which you can access DLP Management t/ANY): [192.168.1.111/255.255.255.0] ANY The ports for manager: [8080 8443]	t(UI)(ip or submet lis
The manager related setting: The subnet/ip list: ANY The ports: 8080 8443	
Is the setting right (type 'q' to quit from config)? (y/n/	q): y_

8) 此部分如[]显示, DLP 服务端默认只允许与其同一网段的 PC 机通过 SSH 远程登录 DLP 服务端,这里请改为 ANY (注意: ANY 需要全部大写),端口无需改动

注意:此步骤非常关键,即如果不修改,默认情况下与 DLP 服务端不同网段的 PC 机将通过 SSH 协议登录 DLP 服务端。

配置完毕后,在最后的信息确认后,按y The subnet/ip list from which sysadmin can remote logon to system(ip or subnet l ist/ANY/None): [192.168.1.111/255.255.255.0] ANY The ports for sysadmin: [22] The sysadmin related setting: The subnet/ip list: ANY The ports: 22 Is the setting right (type 'q' to quit from config)? (y/n/q): y\_



9) 这里无需修改,请直接按回车,并按 y 进行确认 The ip (list) of DLP clustering machine(s)(ip list/None): [] The clustering machine(s) setting: No clustering machine Is the setting right (type 'q' to quit from config)? (y/n/q): y\_

10) 配置完毕后,需要重启服务器操作系统,按 y进行确认

Please wait....

Network security configuration has been done. press any key to continue.. System configuration has been done. The system need reboot. Reboot now?(y/n): y\_

#### 4. 更改默认防火墙配置,允许 ping

注意:默认 DLP 服务端的防火墙配置中,一分钟只允许接受 10 个 ping 包,所以会出现长 Ping 丢包的情况。----这不影响 DLP 正常运行

#### 防火墙配置:

:OUTPUT ACCEPT [0:0] -A INPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 10/min -j ACCEPT

出现的 ping 丢包:

📷 管理员: C:\Windows\system32\cmd.exe - ping 192.168.1.111 -t	x
Microsoft Windows [版本 6.1.7600] 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。</c>	* III
C:\Users\xiaotang>ping 192.168.1.111 -t	
正在 Ping 192.168.1.111 具有 32 字节的数据: 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 请求超时。 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 请求超时。 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 请求超时。 来自 192.168.1.111 的回复: 字节=32 时间<1ms TTL=64 请求超时。	

如果需要修改,我们可以做如下修改:

进入 DLP 的 Linux 内核
 vi /etc/sysconfig/iptables
 [rootOdlp55 ~]# vi /etc/sysconfig/iptables\_
 3) 找到如下内容
 -A INPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 10/min -j ACCEPT



4) 修改为如下:

-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

- 5) 保持退出
- 6) 执行防火墙重启命令:
- /etc/init.d/iptables restart
- 7) 验证 ping 包是否依旧丢弃
- 8) 如正常,还是建议再重启下 DLP 服务端。

## 3.2 安装 DLP 5.5 客户端

### 3.2.1 安装前的准备

1) 获取 DLP5.5 客户端的安装程序 注意: DLP5.5 Agent 目前 GM 的版本为: 5.5-1263

2) 检查 DLP 客户端的硬件和系统配置要求。 注意:参见<u>《客户端系统需求》</u>

- 3) 安装客户端的账号必须具有管理员权限!
- 4) 建议关闭其他所有的应用程序,安装完毕后需要重启操作系统
- 5) 如果已经安装之前的 DSA 版本,请做如下操作: 卸载旧版本 DSA---重启操作系统---安装新版本 DSA---再次重启操作系统
- 6) 确保 DLP 客户端能访问到 DLP 服务端的 8804, 8904, 1558 端口

### 3.2.2 安装过程

注意:DLP 主要安装方式分为 2 种,一种是用 dtool 工具本地安装,另一种是用 msi 安装包远程 部署 这里只介绍 dtool 工具本地安装

 更改 DLP 客户端的安装程序配置文件(重要!) 解压缩安装包,转到以下目录: DSA-5.5.1263\system32\dgagent 找到 dsa.pro 文件,用记事本打开 将 link\_ip=改为 DLP 服务端的 IP 地址



 dsa.pro - 记事本

 文件() 编辑(E) 格式(O) 查看(V) 帮助(H)

 link\_ip
 = 192.168.1.111

 link\_port
 = 8904

 max\_queue\_kbytes
 = 100000

 usa\_name\_vad\_on
 = true

注意:默认情况下,DSA 安装后,隐藏安装程序文件夹,隐藏进程,隐藏注册表。如需安装后显示,请增加如下键值(不建议操作!):

hide me

🧾 dsa.pro - 记事本	
文件(E) 编辑(E) 格式(O) 查看(	⊻) 帮助(∐)
link_ip link_port max_queue_kbytes usa_name_vad_on hide_me	= 192.168.1.111 = 8904 = 100000 = true = no

= no

保存文件

- 2. 检查操作系统当前账号是否具有管理员权限。
- 3. 设定 Windows Vista 或 Win7 操作系统的"命令提示符"增加管理员权限(只针 对 Vista 以后的操作系统)

"开始"—"所有程序"—"附件"—"命令提示符",右键"命令提示符"—"属性"—"高级"—勾选"以管理员身份运行"。



 检查是否"命令提示符"是否以管理员模式运行(只针对 Vista 及其以后的操作 系统)



- 5. 使用 dtool 工具开始安装
- 1) 将之前修改好 dsa. pro 的安装程序文件夹拷贝到客户端本地。



- 2) 打开命令提示符
- 3) 将 dtool. exe 拖入命令提示符窗口中,按回车,查看具体使用参数。



数据外泄管理系统 DLP5.5

 dtool.exe [-i|-u] [-cpara=value] [-ppwd] [-n] [-sb] [-s] [-q] [-dx] [-fx]

 [-v] [Host]

 **常见使用方法:** 

 dtool.exe - i
 ---安裝 DSA

 dtool.exe - u
 ----卸载 DSA

 dtool.exe - i - sb
 ----安裝 DSA, 并支持安全模式下数据防泄密

 dtool.exe - i - sb
 ----安裝 DSA, 并暂时不重启操作系统

 dtool.exe - i - s - d10
 ---安裝 DSA, 并10 分钟后再重启操作系统

 dtool.exe - i - p123
 ----安裝 DSA, 并设置卸载密码为 123

#### 常用并推荐使用方法:

dtool.exe - i - sb ---安装 DSA,并支持安全模式下数据防泄密 dtool.exe - I - sb - p123 ---安装 DSA,并支持安全模式下数据防泄密,并设定 卸载密码为 123(密码可以自定义)

4) 使用 dtool.exe - i - sb 进行安装。 注意:安装成功后,会有如下图显示,并会提示 30 秒后重启操作系统



 系统契机

 ●

 系统即将关机。请保存所有正在运行的工作,然后注销。未保存的改动将会丢失。关机是由 MAC-COMPUTER\mac\_tang 初始的

 富关机还有 : 00:00:14

 消息

 Shutdown Initiated by Trend Micro Data Loss Prevention Endpoint.

注意:如果需要暂时不重启,可以打开命令提示符,输入: shutdown - a 取消重启 但是只有操作系统重启后,才会注册到 DLP 的 web 控制台上,否则将不会出现。

5) 重启完操作系统后, DSA 客户端安装完毕。



## 3.3 安装 TMDLPNM 2.0 (可选)

注意: Trendmicro Data Loss Prevention Network Monitor(TMDLPNM) 是一款扫描用户网络镜 像口数据的独立产品,需要单独购买。 此为可选步骤。

### 3.3.1 安装前的准备

1) 获取 TMDLPNM2.0 的安装程序,并刻录成 DVD 光盘 注意:目前 TMDLPNM2.0 版本为 DLPMN-2.0-1135

检查 TMDLPNM2.0 客户端的硬件和系统配置要求。
 注意:参见《TMDLPNM系统需求》

3) TMDLPNM 扫描用户网络镜像口,需要用户在其交换机上配置镜像口 部署方法:TMDLPNM 需要至少连接2根网线,一根管理口,一根镜像数据口(可以多个)
1) 需要在用户交换机上制作数据镜像口,连入TMDLPNM 的镜像数据口
2) 分配一个可以与 DLP 服务端通信的 IP,并连接TMDLPNM 的管理口。



**DLP Network Monitor appliance back panel** 

## 3.3.2 安装的过程

安装过程与 DLP 服务端类似,这边不在赘述。

### 3.3.3 安装后的初始化配置

1. 将 TMDLPNM 注册到 DLP 服务端上

注意: TMDLPNM 没有单独的控制台,需要注册到 DLP 服务端控制台接受其全局管理。日志查询, 策略设定需要在 DLP 服务端上完成。



使用 root 帐号登录 TMDLPNM 的 linux 内核 输入 clish

输入 enable 进入特权模式

> enable

Entering privileged mode... # \_

注册成功时,命令行中的显示:

Dk to create fpga pattern : /tmp/fpga.tcp.ptn.raw Dk to create fpga pattern : /tmp/fpga.udp.ptn.raw

打开 DLP 服务端的 web 控制台验证,显示 online 状态



Data Loss	Preven	tion								
Summary	Agent M	lanagement								<table-cell> Help</table-cell>
+ Data Protection	Agent Ma	ant Management allows the user to browse and edit agents or groups.								
+ Reports	Agents	Group								
+ Logs										_
+ Update	QFilter	n 🛅 Delete					1-2 of 2	I4 4 page	1 -	of 1 M
- Administration		Agents	IP Address	Status	Policy Status	Fingerprints	Agent	L L	.ast Mor	dified
+ Server Configuration		-				17 N				_
+ Agent Configuration		MAC-COMPUTER	192.168.1.5	Disconnected	🗥 N/A	0	5.5.1263	12/2	26/10 3	3:10:34
Crawler Management	🗆 🚼 <u>t</u>	mdlpnm.mac.com	192.168.1.104	Online	\Lambda N/A	0	2.0.1135	12/2	26/10 3	3:40:50
Data Management	Tellton	Delete								
Agent Management	Qritter	Delete					1-2 of 2	It a page	1 1	of 1 P PI
Password										
+ Management Console								10 p	er page	<u> </u>
LDAP							= End	point Age	nt 🗐 Net	twork Agent
Product License										
	1									

### 2. 输入激活码,激活 TMDLPNM 打开 DLP 的 Web 控制台--Administration—Product License 选择 DLP Network Monitor 进行激活

#### Product License

Use this page to view a list of all DLP Endpoint and Network Monitor licenses.

License Information					
Product Name	IP Address(Host	Product Version	License Status	Expiration Date	
<u>DLP Endpoint</u>	127.0.0.1(localhost)	DSC-5.5-1294	Activated		
DLP Network Monitor	172.16.4.242(TMDLP	2.0.1135	🔲 Not Activated	Not Available	

Product License	Product	License	
-----------------	---------	---------	--

<u>Product License</u> > License Details

🔀 The product has not been activated. View renewal instructions

Trend Micro <sup>TM</sup> Data Loss Prevention Network Monitor					
Product:	Trend Micro <sup>TM</sup> Data Loss Prevention Network Monitor (2.0.1135)				
Version:	N/A				
Activation code:	N/A	<u>Enter a new code</u>			
Seats:	N/A				
Status:	Not Activated				
Maintenance expiration:	N/A				

#### 激活以后显示的状态

Product License

🔁 Help

🔁 Help

🕜 Help

Use this page to view a list of all DLP Endpoint and Network Monitor licenses.

License Information				
Product Name	IP Address(Host	Product Version	License Status	Expiration Date
<u>DLP Endpoint</u>	127.0.0.1(localhost)	DSC-5.5-1294	Activated	
DLP Network Monitor	172.16.4.242(TMDLP	2.0.1135	Activated	04022222000

#### 3. 配置最大扫描文件大小

# 注意: 默认 DLP Network Monitor 扫描最大的文件为 20MB 趋势科技不建议修改默认值,过大的设定值会影响 TMDLPNM 的产品性能!

如需修改,可以做如下操作:

输入 enable 进入特权模式



输入 configure max\_file\_size 30000000 (单位为 字节)

## 3.4 如何检查标准安装是否成功

## 3.4.1 DLP 5.5 服务端

1、检查是否可以打开控制台 打开方式: <u>http://ip:8443/dsc</u> 2、检查是否可以 SSH 远程登录

### 3.4.2 DLP 5.5 客户端

1、 检查安装 DSA 客户端后,是否在 DLP 服务端上显示 打开 Web 控制台—Summary—Violation 页面—Agent Status 标签

Agent Status		
Status	Endpoint Agent	Network Agent
Online	1	1

TREND Data Loss	Prevention					L	.ogged on as:   🔒 adm	in
Summary	Agent Manageme	nt					2 н	elp
<ul> <li>Data Protection</li> </ul>	Agent Management allow	is the user to browse	and edit agents or	groups.				
+ Reports	Agents Group							
+ Logs								
+ Update	Tilter Delete					1-2 of 2 14	∮page 1 🔹 of 1 ► ►	1
- Administration	Agents	IP Address	Status	Policy Status	Fingerprints Version	Agent Version	Last Modified	
<ul> <li>Server Configuration</li> </ul>	_			A.		-		
<ul> <li>Agent Configuration</li> </ul>	MAC-COMP	<u>.</u> 192.168.1.5	Online	🗥 N/A	0	5.5.1263	12/26/10 4:15:1.	••
Crawler Management	🗉 👹 tmdlpnm	192.168.1.104	Online	\Lambda N/A	0	2.0.1135	12/26/10 3:40:5.	
Data Management	Elter Delete							
Agent Management 🛛 🖡						1-2 of 2 14	∮page 1 ▼ of 1 ▶ ▶	'
Password							10 per page	
+ Management Console						= Cadaata		
LDAP						Endpoin	t Agent on Network Age	3UC
Product License	1							



2、 检查 DSA 客户端是否有与 DLP 侦听

打开客户端的命令提示符, 输入:netstat - ano|findstr 8904 正常连接将有如下显示



#### 3、 客户端程序目录可以访问

开始—运行—输入:c:\windows\system32\dgagent\

注意:最后一个"\"不要忘记,由于 DSA 默认安装程序为隐藏,所以此为唯一打开程序目录方法,在资源管理器中无法查看到。

运行 ? 🔀
请键入程序、文件夹、文档或 Internet 资源的名 称,Windows 将为您打开它。
打开@): c:\windows\system32\dgagent\ 💽
确定 取消 浏览(B)

#### 4、 查看是否有 ShowMsg. exe 进程存在

注意:此进程不是 DSA 的主进程,而是弹出警示框等进程。用户即使手动 kill 此进程, DSA 也 是可以正常工作。

DSA 的主进程为隐藏进程,任务管理器将无法看到。

₩ I S R O <sup>推 サ A 技</sup> 可信赖的网络安全专家	数据外泄管理系统 DLP5.5
📕 Windows 任务管理器	
文件(E)选项(E)查看(Y)关机(U)帮助(H)	
应用程序 进程 性能 联网 用户	
映像名称	月户名 🔼
alg. exe	LOCAL SERVIC
cmd. exe	mac_tang
conime. exe	mac_tang
CSTSS. exe	SISIEM
evplorer eve	mac_tang
lsass exe	SYSTEM
services. exe	SYSTEM
ShowMsg. exe	mac_tang
smss.exe	SYSTEM
spoolsv.exe	SYSTEM
svchost.exe	SYSTEM
svchost.exe	NETWORK SERV
svchost.exe	SISIEM NETWORK SER.
sychost exe	LOCAL SERVIC
svchost. exe	LOCAL SERVIC
□显示所有用户的进程 (S)	结束进程 (2)
」 进程数:30 CPU 使用:100% 提び更改。	156M / 2526M

## 3.4.3 TMDLPNM2.0

 1、检查安装 TMDLPNM Agent 安装后,是否在 DLP 服务端上显示 打开 Web 控制台—Summary—Violation 页面—Agent Status 标签

Agent Status								
Status	Endpoint Agent	Network Agent						
Online	1	1						



Data Loss	L	ogged on as: 🙈 admin								
Summary	Age	ent Manageme		🕑 Help						
+ Data Protection	Agen	nt Management allow								
+ Reports	Ag	Agents Group								
+ Logs										
+ Update	Q	Filter 🛅 Delete					1-2 of 2 14 4	page 1 ▼ of 1 ► ►		
- Administration		Agents	IP Address	Status	Policy Status	Fingerprints Version	Agent Version	Last Modified		
+ Server Configuration		_			•					
+ Agent Configuration		MAC-COMP	<u>.</u> 192.168.1.5	Online	🗥 N/A	0	5.5.1263	12/26/10 4:15:1		
Crawler Management		tmdlpnm	192.168.1.104	Online	\Lambda N/A	0	2.0.1135	12/26/10 4:52:3		
Data Management		Filter 🚔 Delete					1.0 (0.11)			
Agent Management		l'inter					1-2 of 2 14 4	page 1 • of 1 • M		
Password								10 per page •		
+ Management Console							Endacia	t Agent 🕮 Network Agent		
LDAP							= Endpoint	r Agent 🐨 Network Agent		
Product License										

### 2、检查是否有流量通过

转到如下目录: cd /opt/TrendMicro/ndlp/platform/QA\_TOOLS/ 执行 /toe sh

汎行./toe.sh					
Sun Dec 26 16:55:53	CST 2010				
[STATISTICS]					
syn_conntrack:	1	(		184)	
conntrack_count:	1	(		154)	
nr_pkscan_tx:	0	(	1	125)	
nr_btscan_tx:	0	(		202)	
nr_fpga_err:		(		0)	
nr_btscan_err:		(		0)	
free_lowmem:	648M	( 2)	00M/1	L011M	)
<pre>nr_packet_bytes:</pre>	464	[	0M]	-\	
nr_pk_bytes:	0	[	0M]		
nr_bt_bytes:	0	[	0M]		
nr_tr_bytes:	0	[	0M]	-+-	( 550M)
nr_pages:	0	[	0M]		(4096M)
nr_sb_drop:	0				
nr_tr_drop:	0				
nr_result_vy:	0			0	
nr_result_vn:	202				
nr_result_more:	0				
nr_both_vn:	137				
nr_timeout_hole:	0				
nr_split:	0			0	
nr_nonsplit:	91311				
nr_flow_packets:	0				
nr_flow_fifo:	0				
nr_flow_pkscan:	0				
nr_flow_btscan:	0				
nr_in_conn:	1143		14	1260	
nr_not_a_syn:	7			7	
nr_corrupt:	31			1	
nr_redirect:	0			0	
overloading: 0	0 (1:0 f	s:0	f:0	d:0)	
[TCP_	_STATE]===				
SYN_SENT:	1	(		0)	
SYN_RECV:	0	(		0)	
ESTABLISHED:	0	(		0)	
FIN_WAIT:	0	(		0)	
CLOSE_WAIT:	0	(		0)	
LAST_ACK:	1	(		0)	
TIME_WAIT:	0	(		0)	
CLOSE:	0	(		0)	

# 4 DLP 的基本配置

## 4.1 DLP 服务端的基本配置

### 4.1.1 DLP 产品激活

DLP 服务端和 TMDLPNM(可选)需要使用激活码单独激活,在之前初始化配置操作步骤中已经完成。 注意:如未操作进参考之前章节进行操作

### 4.1.2 DLP 策略设置

- 注意:这里只做简单策略设定介绍。具体策略可以根据实际需求进行调整
- (一) Fingerprints 指纹获取
- 1) 点击 Data Protection---Fingerprints

Data Loss	Prever	ntion				
Summary – Data Protection	Fingerprints Use this page to catalog all files intended for asset fingerprinting.					<u>Tr</u>
- Digital Assets Fingerprints Datacres	Add Source	🔁 Сору	前 Delete	Acquire Documents	Schedule Acquisition     w all scheduled acquisitio	<u>ns]</u>
Keywords		Name	•	Path	Documents Acquired	Status
File Attributes	∎Add	🔁 Сору	💼 Delete	Acquire Documents	ESchedule Acquisition	
Compliance Templates				·		
Comnany Policies						

- 2) 常用方式一: 共享方式访问需要获取指纹的数据目录
  - ✓ Name:设定一个名字
  - ✓ Repository Type: 选择获取方式, 如 windows 共享,请选择 File system/Windows Share
  - ✓ Path:设定具体共享文件夹。如需包括子文件夹,请勾选 include sub-directories
  - ✓ 并输入目标服务器的管理员账号和密码。
  - ✓ 点击 Test Connection,如连接正常,会显示 Successfully



Fingerprints

🕑 Help

<u>Fingerprints</u> > Adding Fi	ngerprints	
Source		
Name:*	指纹获取	
Description:		
Repository Type:	File system / Windows Share 💌	
Host:*	172.16.4.230	
	Example: server1.example.org or 123.123.123.123	
Path:*	/学习文档	Include sub- directories
	Example: /documents/sensitive files	
User ID:	administrator	
Password:	•••••	Test Connection
Source connection tes	t successfully.	

#### 3) 常用方式二: 通过 Remote Crawler 工具进行获取指纹 注意: 此方式适用于存放需要保护数据目录未被共享。

在 DLP 控制台上,下载 Remote Crawler 工具,访问 Administration---Crawler Management

(								-		
Summary	Crawle	rawler Management								
+ Data Protection	Crawle or not (	rawler Management allows you to scan for confidential data stored on desktops and laptops whether users are connected r not connected to the company's network. Use this page to manage or deploy the Remote Crawler agent.								
+ Reports										
+ Logs	QFilte	er 🛅 Delete	Dowr	nload Remote Crawl <mark>er</mark>		1-1 of 1 ዞ∢ page 1 ▼ of 1 ⊧ ዞ				
+ Update		Host 4		IP Address		Status	Crawler Version	Last Modified		
- Administration		11050		In Address		ocacao		Laberhoamoa		
<ul> <li>Server Configuration</li> </ul>	🗆 <u>ma</u>	<u>ac</u>		172.16.4.230	C	Connected	5.5.1069	12/29/10 2:45:33 PM CST		
+ Agent Configuration	<b>Q</b> Filte	er 💼 Delete	Dowr	nload Remote Crawl <mark>er</mark>			1-	1 of 1 ↔ page 1 • of 1 → H		
Crawler Management 🍑								200 per page 💌		
Data Management								,,		

### ✓ 下载后拷贝到存放需要获取指纹的敏感数据的服务器上安装(需 Windows 平台)

✓ 安装完毕后,	打开"开始"所有程序R	Remot	e Crawler Agent Console
	🛅 Trend Micro DLP Remote Crawler Agent	- 🕨 🏓	🦉 Remote Crawler Agent Console
Microsoft Office	🛅 Cisco	• 🧕	🖞 Uninstall Remote Crawler Agent
	🛅 射手影音播放器	- ▶ [	
All <u>P</u> rograms 🕨	💼 谷歌浏览器	•	+# ++ ** ++



🔁 Help

✓ 点击 Add,选择 Local,并添加需要保护的路径。点击 Test,如出现 Connection test Successful, 后点击 Save 保存。

👰 Tr	end Micr	o DLP R	emote Crawler A	gent Con	sole		
Eile	<u>H</u> elp						
The DL	P Remote	Crawler	can scan any of the	listed repo	sitories.		
Ad	d	Delete					
	Туре		Path		Host/Site	Recursive	Principal
	ocal	F:(学习3	【档			Yes	
	Add/Edit	t Reposi	tory				×
	Repositor	ry type	Local	-	Recursive	Yes	
	Host/Site		<u> </u>				
	Path		F:\学习文档			Browse	
	User Nam	ne			-		
	Password	ł			-		
	Test re	sult					
	Connec	tion test	successful.				
				Test	Save	Cance	

✓ 转到 Fingerprints 页面,在 Repository Type 中选择 Remote Crawler,则会自 动显示之前添加的目录

Fingerprints		💽 Help
<u>Fingerprints</u> > Adding Fi	ngerprints	
Source		
Name:*	指纹获取	
Description:		
Repository Type:	Remote Crawler	
Host:*	mac 💌	
Path:	F:\学习文档 (includes sub-directories)	

4) 分别点击 Save & Acquire 进行保存并获取指纹。

Save Save & Acquire Cancel

Acquire 的过程可以查看 Status 页面。



Trend MicroTM <u>DLP Workflow</u> 2 记 Help

Fingerprints

Use this page to catalog all files intended for asset fingerprinting.

<b>D</b> A	dd 💽 Copy 💼 Dele	te 🕞 Acquire Document	s 🖽Schedule Acquisition	1-1	.of1 ₩∢p	age 🚺 ▼ of 1 ↦ ⊨			
Sou	Source [View all scheduled acquisitions]								
	Name 🔺	Path	Documents Acquired	Status	History	Last Acquisition			
	指纹获取	F:\学习文档	0	Acquiring(18.03%)	3	12/29/10 2:54:0			
<b>D</b> A	Add      Copy      Delete      Acquire Documents      Schedule Acquisition     1-1 of 1      1 → page      1 → of 1 →								
	200 per page 💌								

注意: Acquire 的时间取决于服务器的性能和文件的数量。建议如在测试过程中,当 DLP 服务端 运行在 Vmware 平台上,请选择少量数据进行获取。

### 5) 如需预设获取,请选择 Source 后,点击 Schedule Acquisition

Fingerprints <u>Trend Micro<sup>IM</sup> DLP Workflow</u> 2 2 Help					
] of 1 ► ₩					
quisition					
) 2:55:3					
of 1►►					
rpage 💌					

#### 进行预设 Acquire 的设定。

Scheduling SensitiveDocAcquisitionJobType

🔁 Help

Scheduling Jobs for [指纹获取].

Schedule	
<ul> <li>One-time</li> <li>Daily</li> <li>Weekly</li> <li>Monthly</li> </ul>	Date: 12-29-2010 mm-dd-yyyy Time: 16 hh mm
🗆 Acquire finge	prints for all locations defined in the Remote Crawler side
🗹 Select all file	ocations
☑ F:\学习文档	(includes sub-directories)
Save Cancel	

# 6) Acquire 获取完毕后, Status 会显示 Acquired Fingerprints

<u>Trend Micro IM</u> DLP Workflow 🗗 😈 Help

Use this page to catalog all files intended for asset fingerprinting.

<b>B</b> A	dd 💽 Copy	💼 Deleti	e 🕞 Acquire Document:	s 🖽 Schedule Acquisition		1-1	of 1	и∢ р	age <mark>1 ▼</mark> of 1 ► ►
Source [View all scheduled acquisi					ions]				
	Name	•	Path	Documents Acquired	Status		Hist	tory	Last Acquisition
	指纹获取		F:\学习文档	151	Acquired		3		12/29/10 2:55:3
∎A	dd 💽 Copy	💼 Deleti	e 💽 Acquire Document:	s 🖺 Schedule Acquisition		1-1	of 1	и∢ р	age <mark>1 ▼</mark> of 1 ► ►
									200 per page 💌

7) 点击 History, 可以查看此次 Acquire 的显示具体信息

注意:如出现下图所示信息,则检查此文件是否过小,或者过大。



Acquisition Detail

2010-12-29 14:55:39 - F:\学习文档\Favorites\cnBeta.COM\_网发媒体与言论平台.ur<mark>l: Empty fingerprints will be extracted from</mark> the file.

以下为默认情况下 DLP 服务端 Acquire 指纹信息的配置,可以根据实际需求进行修改

#### 注意: 趋势科技不建议进行修改, DLP Acquire 过大的文件将会影响性能。

TREND Data Loss		Logged on as: 🤮 admin 🛛 🌡		
Summary	Administration - Fingerprint Settings			🔁 Help
+ Data Protection	Fingerprint Settings			
+ Reports	Minimum file size:*	62	Bytes 💌 🏓	
+ Logs	Maximum text file size:*	6	MB 💌 🏓	
+ Update	Maximum binary file size:*	32	MB 💌 🏓	
- Administration	Maximum archive file size *	32	MB V	
- Server Configuration		52	···· ··· ··· ··· ··· ··· ··· ··· ··· ·	
Fingerprint Settings 🕠	Maximum repository size to download to agent:*	300	IMB 🔽 🏓	
Application Settings				
+ Agent Configuration	Fingerprint Decompression Control Settings for	· Acquisition		
Crawler Management	Trend Micro DLP will not process if the decompres	sed file size e>	ceeds:* 128	MB 🗾 🦊
Data Management	Trend Micro DLP will not process if the total numb	er of embedde	d layers in the compress	ed file exceeds: 10 💌 layer(s)
Agent Management	Trend Micro DLP will not process if the total decor	noressed file n	umber exceeds:* 2000	(1-2000)
Password	······································			_ (= ====;
+ Management Console	Save			
LDAP				
Product License				

#### (二) Pattern 设定

Pattern 设定是基于正则表达式完成。使 DLP 可以检测一些诸如身份证 ID,银行卡 号、家庭住址、电话号码等敏感信息外泄。默认已经设定一些条目,但大部分是参 照国外使用方式进行设定,一般建议不使用此功能。

在 DLP5.5 中,如测试需要,可以勾选 China National ID,即身份证号码。

Data Loss Prevention Logged on as: Sadmin								
Summary – Data Protection	Summary Data Protection Trend Micro <sup>TM</sup> DLP Workflow C							
- Digital Assets Fingerprints	Pat	Add 💽 Copy 💼 Delet	e	1-38 of 38	K∢ page 1 ▼ of 1 ► H			
Keywords		Name 🔺	Description	Pattern	Last Modified			
File Attributes		ABA Routing Number	ABA Routing Number	[^\d]([0123678]\d{8})[^\d]	11/12/10 2:41:19 A			
Compliance Templates		<u>American Name</u>	American people's name	$^{(A-Z][a-z]{1,12}(s?,s?[[s]](A)}$	11/12/10 2:41:19 A			
Company Policies		<u>Austria SSN</u>	Austria SSN	[^\d](\d{4}[0-3]\d(0[1-9] 1[0-2])\d{2})[	11/12/10 2:41:19 A			
Data Discovery		Cal DL# /Cal ID#	CalID	[^\w-]([A-G]\d{7})[^\w-]	11/12/10 2:41:19 A			
Device Control		Canadian Social In	Canadian Social Insurance N	[^\w-]([1-79]\d{8} [1-79]\d{2}-\d{3}-\d.	. 11/12/10 2:41:19 A			
+ Reports		<u>China National ID</u>	China National ID	[^\d-](\d{17}(\d x))[^\d-]	11/12/10 2:41:19 A			
+ Undate		Credit Card Number	Credit Card Number	[^\d-](\d{15,16} \d{4}-\d{4}-\d{4}-\d{4}-	. 11/12/10 2:41:19 A			
Administration		Danish Personal ID	Danish Personal ID	[^\d-]((0[1-9] [12]\d 3[01])(0[1-9] 1[0-2].	11/12/10 2:41:19 A			

#### (三) 关键字设定

1) 点击 Data Protection--- Digital Assets--- Keywords, 右边点击 Add



#### 数据外泄管理系统 DLP5.5

Data Loss	TREND. Data Loss Prevention					
Summary	Keywords	<u>Trend Micro<sup>II</sup></u>	M <u>DLP Workflow</u> d 记 Help			
- Data Protection	Keywords establish categories and boundaries of sensitive information to filter from your files.					
- Digital Assets	🔁 Add 💽 Copy 🕋 Delete	<b>1-19</b> of 19	I K∢ page 1 ▼ of 1 ► M			
Fingerprints	Keywords					
Keywords	Name 🔺	Description	Last Modified			
File Attributes	Adult Keywords		11/12/10 2:41:19 AM CST			

- 2) 设定方式如下
- ✓ Name 设定此条规则的名称
- ✓ Condition:选择 Match any Sub-keywords
- ✓ 选择 Add/update Sub-keywords
- ✓ 在 Sub-Keyword 列表中, Name 中输入需要保护的"keyword"
- ✓ 如需要大小写敏感,请勾选 Case Sensitive
- ✓ 点击 Add, (可以同时添加多个关键字)
- ✓ 点击保存

Keyword					🕄 Help		
<u>Keyword</u> > Adding Ke	yword						
Keywords							
Name:*	关键	建字过滤					
Description:							
Condition:	Ma	atch any sub-keywords	5	•			
C Import sub-keyw	ords 选 <eywords< td=""><td>择文件 <sub>5</sub></td><td></td><td></td><td></td></eywords<>	择文件 <sub>5</sub>					
Sub-keyword							
Name:			L Case Sensi	itive			
Description:							
Add Update							
Sub-keywords list							
💼 Delete					1-1 of 1 🛤 page 🚺 💌 of 1 ► M		
🗖 📃 Name 🔺		Description	Case Sensitive		Last Modified Time		
🗖 <u>test</u>			Case Insensitive				
🗎 Delete					1-1 of 1 🛤 page 🚺 💌 of 1 ► M		
	200 per page 🔻						

Save Cancel

#### (四) 文件属性设定

注意: True file Attributes 采用识别真实文件类型属性,不是单纯的基于扩展名检测。目前 支持常见的 300 多余种文件类型。

当 DLP 识别某种类型的文件,即使更改扩展名或者去除扩展名,DLP 依旧可以有效的识别和检测。 1) 点击 Data Protection--- Digital Assets---File Attributes,右边点击 Add



### 数据外泄管理系统 DLP5.5

Data Loss	Pre	evention		Logged on as: 💩 admin 🛛 🎄 !			
Summary – Data Protection	File Attributes         Trend Micro <sup>TM</sup> DLP Workflow i           tion         With File Attributes, you can block certain files from users that meet the criteria you have established.						
- Digital Assets	Add Copy Delete 1-2 of 2 H4 page 1						
Fingerprints	File Attributes						
Patterns Keywords	Г	Name      Description     Last Mod					
File Attributes 🔹 🕨	Г	Mac File Attribute	Mac File Attribute	11/24/10 9:33:16 AM CST			
Compliance Templates	Г	与得通讯		12/20/10 5:22:20 PM CST			
Company Policies		Add 🕞 Copy 🕋 Delete		1-2 of 2 M < page 1 ▼ of 1 ► M			
Data Discovery	. –						
Device Control				1200 per page 💌			

#### 2) 设定方法如下:

Name: 中设定规则名称

- ✓ 如需针对文件类型控制,请勾选 File type, 点击 Edit
- ✓ 如下针对文件大小控制,请勾选 File Size,并直接设定大小即可,范围: Bytes、 KB、MB、GB
- File Attributes

<u>File Attributes</u> > Adding File Attributes

File	Attribute Information							
Nam	e:* Mac文	ac 文件类型						
Desc	ription:							
File	Attributes							
	File type:	[Edit]						
File size:		From Bytes To Bytes						

3) 当选择 File type 后,在如下页面可以根据实际需求进行设定。



File Attributes

File Attributes > Adding File Attributes

Select:
Selected types

Executable

Document

Image Document

Graphic Document

Graphic Document

Multimedia

Multimedia

Encapsulation Format

Database Document

Database Document

Spreadsheet Document

Presentation Document

Desktop Publishing

General Purpose Document

Obfuscated File (Encrypted File)

Others

**注意:** File Type 中的检测是针对常见的文件类型而不是单纯的基于文件扩展名,对于一些编译 程序生成的一些文件,比如使用 C++程序的源代码扩展名为.c 的文件,此类文件与扩展名为.txt 和.ini 一样,不属于真实文件类型,所以可以在 Others 中添加,或者可以使用 keywords 进行 设定。

#### 在 Keywords 中的设定,

Summary	Ke	Keywords <u>Trend Micro</u> TM_DLP Workflowd 2 Help			
– Data Protection	Key	words establish categories and boundaries of s	ensitive information to filter from your files.		
- Digital Assets	T.	Add 🕞 Copy 🕋 Delete	1-19	of 19 M∢ page 1 ▼ of 1▶M	
Fingerprints	Ke	wwords			
Patterns		Namo A	Description	Last Medified	
Keywords		Name -	Description	Lasc Modified	
File Attributes		Adult Keywords		11/12/10 2:41:19 AM CST	
Compliance Templates		American-Name-Keyword1		11/12/10 2:41:19 AM CST	
Company Policies	🗖	American-Name-Keyword2		11/12/10 2:41:19 AM CST	
Data Discovery		C and C++ Source Code		11/12/10 2:41:19 AM CST	
Device Control		C# Source Code		11/12/10 2·41·19 AM CST	
<ul> <li>Reports</li> </ul>					
+ Logs		COBOL-Source-Code		11/12/10 2:41:19 AM CST	
+ Update		Common Medical Terms		11/12/10 2:41:19 AM CST	
+ Administration		HCFA (CMS) 1500 Form		11/12/10 2:41:19 AM CST	
		Java Source Code		11/12/10 2:41:19 AM CST	

## 4.1.3 DLP 策略部署

### (一) 建立合规模板

1. 点击 Data Protection--- Compliance Templates, 右边点击 Add

Data Loss Prevention Logged on as: Sadmin						gged on as: 🤱 admin 🛛 🙈 L
Summary – Data Protection – Digital Assets	Compliance Templates Compliance Templates are used in stringent compliance requirements	creating boundaries to comply with corp	and setting orate govern	limitations fo ance and da	<u>Trend Micro</u> or creating policy. Yi ta privacy requirem	M_DLP Workflowr ? Help ou can also import nents.
Fingerprints Patterns	Add 🕒 Copy 📷 Delete 🕞 Imp	Fingerprints	Patterns	Keywords	1-5 of File Attributes	5 K ← page   1 ▼ of 1 ► Modified
Keywords File Attributes		0	26 48	13 30	0	11/12/10 2:41:19 AM CST
Compliance Templates > Company Policies	□ PCI-DSS	0	7	3	0	11/12/10 2:41:19 AM CST
Data Discovery Device Control	US PII	0	12 34	6 18	0	11/12/10 2:41:19 AM CST 11/12/10 2:41:19 AM CST
<ul> <li>Reports</li> <li>Logs</li> </ul>	Image: The second s					
+ Update     + Administration						

- 2. 设定方式如下:
- ✓ Name: 输入模板名称
- ✓ 如需添加之前获取的指纹,选择 Fingerprints,并选择 High-Level Match

Match Rule Building Block
田 ▼ Fingerprints ▼ 指纹获取 ▼ High-level Match ▼
如需添加之前设定的关键字,选择 Keywords
Match Rule Building Block
🛨 🔽 Keywords 💌 Mac Keyword
如需添加之前设定的 File Attributes.洗择 File Attributes
Match Rule Building Block (Rule Number 3)
Ŧ 🛛 🔽 File Attributes 💌 Mac File Attribute 💌

## ✓ 可以同时添加多个,也可以单独创建模板。

E	注意:请区分 OR 与 And 以及 Except 的区别							
N	Match Rules							
1	<b>•</b>	指纹获取 (High-level Match)	ŵ					
2	Or 💌	Mac Keyword	Î					
3	Or 💌	Mac File Attribute	Î					

### (二) 建立策略及部署

1. 点击 Data Protection---Company Polices, 右边点击 Add



TREND Data Loss Prevention							
Summary - Data Protection	Company Policies List <u>Trend Micro<sup>22</sup> DLP Workflow</u> <sup>22</sup> Rep Use the Company Policies page to create across-the-board company rules and criteria that the company files should meet.						
+ Digital Assets Compliance Templates Company Policies	Filter     Image Copy     Image Delete     0-0 of 0     H ≤ page 1     of 1 > H						
Data Discovery	Name Type Action Order▲ Modified Status Deployment Status						
+ Reports	O-0 of 0 H 4 page 1 v of 1 M						
+ Logs + Update	200 per page 🔻						
+ Administration	Deploy Now						

#### 2. 点击 Add 后,选择 Endpoint Agent Policy

注意: Network Agent Policy 是针对 TMDLPNM 产品,此处选择 Endpoint Agent Policy 📑 Add 🕞 Copy 🕋 Delete

		_
ame	Endpoint Agent Policy	
	<u>Network Agent Policy</u>	

"Policy Name"中输入设定策略名称,"Target"中选择此条需应用此策略的 3. Agent 客户端。设定完毕, 点击 Next

<b>e</b>		
小贴士:有4种方式选择零	客户端,分别是 <b>:</b>	
Groups/Endpoints	基于分组中的客户端(可以手动分组)	
Domains/Endpoints	基于 Domains/Endpoints 中的客客户端(例如 Workgrou	p)
LDAP/Users	基于 LDAP 中用户信息的客户端	
All Targets	所有客户端	
Policy: Add Policy		🔁 Help

Policy: Add Policy

Policy List > (New Policy)

> Step 1: Target >>> Step 2 >>> Step 3 >>> Step 4

Identify your target for this policy.

Template							
Policy Name: test policy     Copy from an existing policy: select							
Target							
Select by: Groups/Endpoints  Groups/Endpoints  Groups/Endpoints  Domains/Endpoints  Domai							

4. 管道 Channels 中,选择全部,即所有 DLP 支持的 Channels



Check to prevent users from accessing sensitive information with the following:

Channels
ActiveSync filter
CD/DVD
Clipboard
<u> Email</u> ▼
Removable Storage (FileWrite)
FTP
🕅 нттр
V HTTPS
Instant Messengers -
<u><u>▼ p2p</u> ▼</u>
V PGP Encryption
V Printer
SMB S
Web Mail -

## 小贴士: 此处为单条策略中的黑白名单设定

## 注意:黑白名单的优先级为:黑名单、白名单、网络边界(Bondary)

#### a) "Email"管道中,可以单独设定黑白名单。

输入格式(0U信息):/0=Trend/0U=USA,/0=Trend/0U=CHINA(逗号分隔)

122		۰.
	Empail	
	Engli	ei,
		۰.

Email		
Exchange Client Email	Approved domain names	
Lotus Notes Email		1
SMTP Email		
	Separate multiple domain names with a comma. (Example: /O=Trend/OU=USA,/O=Trend/OU	U=CHINA)
	Blocked domain names	
	A	
	Separate multiple domain names with a comma. (Example: /O=Trend/OU=USA,/O=Trend/OU	U=CHINA)

#### b) USB 存储设备例外

输入格式: vendor Name 1-model-Serial ID

<b>V</b>	Removable Storage (FileWrite) 🗷			
Approved USB Devices				
		*		
		-		
	Separate multiple USBs with a comma. Asterisk (*) is supported. Format: vendor Name 1-model-Serial ID, Vendor Name 2-model-Serial ID Example: ZTE-6025-301011006703D310,GENERIC-8012-*,GENERIC-*-*,*-*-*			

#### 小帮助:如何获取每个 USB 的 ID 编号?

方法: 打开 Data Protection---Device Control---选择任意 Agent

Data Loss Prevention							
Summary — Data Protection	Device Control Device control allows you to limit specific user access to specific devices and network shared folders.						
+ Digital Assets Compliance Templates Company Policies	Endpoints Groups			1-3 of 3	8 K∢page 1 ▼ of 1 ► M		
Data Discovery Device Control	Endpoints 🔺	IP Address	Disabled Devices	Domain	Last Modified		
+ Reports	JASON ZHOU-PC	10.28.132.63		WORKGROUP			
+ Logs	MAC-XP	10.28.132.21		WORKGROUP			
+ Update	TANG-XP	10.28.132.19		WORKGROUP			
+ Administration	QFilter			1-3 of 3	3 M∢ page 1 👻 of 1 → M		
					200 per page 👻		



点开 Remove disk Drives,下载 Download Auto-detect Assistance 工具

Devices	Select All			
Select the devices to restric	t the user from acc	essing.		
CD/DVD		IEEE 1394 Bus	host controllers	Modems
Ports (COM & LPT)		Imaging device	25	PCMCIA adapters
Floppy disk controllers		Infrared devices		Print Screen Key
🔲 Removable disk drives				
Exception List			🔄 Download Auto-de	etect Assistance
Vendor		Model	Serial ID	
				÷

下载完毕后在插上需要允许使用 U 盘电脑上运行, 会自动弹出一个网页, 将以下信息记录, 例如: 可移动磁盘(仅限于 IA存盘/U盘):

计算机	用户	端口	描述	供应商	型号	序号	
XIAOTANG-PC	xiaotang-PC\xiaotang	USB	SanDisk Cruzer Colors+ USB Device	SANDISK	5170	08775018AF42845D	

#### c) SMB 协议共享

输入格式: IP addresses, hostnames, FQDN, and IP address ranges (逗号分隔。)

manual "	
Approved IP ranges/hosts	
	4
Separate multiple IP addresses, hostnames, FQDN, and IP address ranges with a comma. (Example: 192.168.2.1/10)	)
Blocked IP ranges/hosts	
	-
	,
Separate multiple IP addresses, hostnames, FQDN, and IP address ranges with a comma. (Example: 192.168.2.1/10)	)

#### 5. 选择之前配置的策略模版,并建议勾选 Enable Data Stealing Malware detection

This is your "IF" statement. Select the compliance templates for this policy.							
Condition							
Import Predefined Template(s)							
GLBA HIPAA PCI-DSS SB-1386 US PII 题试模纸	[Hold down the Control <b>Key</b> (CTRL) to select multiple items.]						
Enable Data Stealing Malware detection							

6. 设定网络边界和检测后的处理措施,建议选择如下图所示



Specify the online and offline actions for this policy. **Network Boundary** Offline Agents 부 Online Agents 🡎 🔘 Local Area Network 🏓 Iccal Area Network (recommended) Local Machine (recommended) Local Machine (strict filtering) System Action When Online Restrictions: Actions to take: √ Log Pass Block Client side alerting Customizable message URL: <sup>很抱歉,</sup>您违反了公司的安全策略! Server side alerting Forensic data capturing Prompt user to enter justification when blocked Encrypt (USB devices only) Prompt user to enter justification System Action When Offline Same as Online Action Restrictions: Actions to take: Pass √ Log Block Client side alerting Customizable message URL: 很抱歉, 您违反了公司的安全策略! ✓ Server side alerting Forensic data capturing Prompt user to enter justification when blocked Encrypt (USB devices only) Prompt user to enter justification 相关说明:

a) Online 和 Offline Online Agent: 与服务端正常通信的客户端 Offiline Agent: 与服务端断开连接的客户端

b) Local Area Network 和 Local Machine

Local Area Network: DLP 只检测出 LAN 的信息,不会对公司局域网 LAN 之间敏感信息传输 进行检测。(适合 Online)

Local Machine: DLP 针对出本机的任何敏感信息都进行检测(适合 Offline)

```
DLP 如何区分 LAN?
```

答: DLP 自动检测私有地址段:

- A: 10.0.0.0<sup>~</sup>10.255.255.255
- B: 172. 16. 0. 0~172. 31. 255. 255
- C: 192. 168. 0. 0~192. 168. 255. 255
- c) Client Side alerting 和 Server Side alerting (建议都勾选上)

勾选 Client Side alerting,当触发策略时,客户端将弹出提示框。DLP5.5 可以自定义每 条策略弹出内容

勾选 Server Side alerting,当触发策略时,如需要邮件通知管理员,需启用此功能

d) Prompt user to enter justification 当触发策略时,会弹出框提示输入传送次敏感信息的缘由,当用户输入缘由后即可将次信息 传送出去。管理员也可以在 DLP 控制台的 Log 中查询到此缘由。 为了方便使用,此后的默认 30 秒内再次传送的文件不再需要输入申辩缘由,但日志中都会 记录 在 Administration---Agent Configuration---Agent Setting 中可以修改默认时间

e) Forensic Data Capture(不建议勾选) DLP 客户端当检测到违反策略的文件传出时,会同时备份此文件上传到 DLP 服务端上。



不建议使用此功能,因为过多的文件,过大的文件会影响 DLP 服务器性能并占用 LAN 的流量。 f) Encrpty 和 Prompt user to enter justification

此功能仅当 Channel 单独只选择 Removable Storage (FileWrite)时有效

7. 配置完毕点击 Save 进行保存

#### 8. 勾选策略, 点击 Deploy Now 部署策略到客户端。

已部署将显示: Policies have been deployed

注意:基于产品性能的考虑,默认1分钟建议只部署1次策略。在此情况下,"Policies have been deployed"信息也只会在1分钟后再次显示

**Company Policies List** 

<u>Trend Micro<sup>™</sup> DLP Workflow</u>⊡ 🔂 <sub>Help</sub>

Use the Company Policies page to create across-the-board company rules and criteria that the company files should meet.

Q	Grilter       Image       Image									
	Name	Туре	Action	Order 🔺	Modified	Status	De	eployment Statı	IS	
	Mac 网络防	Network	Log/Server side al	1 -	12/29/10 11:36:13	<b>*</b> •		Deployed		
	<u>Mac 文件扩</u>	Endpoint	Online: Log/Client	2 🔻	12/29/10 11:36:13	<b>*</b> •		Deployed		
	<u>Mac 关键字</u>	Endpoint	Online: Log/Client	3 🔻	12/29/10 11:36:13	<b>*</b> =		Deployed		
	<u>Mac 敏感文件</u>	Endpoint	Online: Log/Client	4 🔹	12/29/10 11:36:13	<b>*</b> •		Deployed		
Q	□ Filter     □ Add     □ Delete     1-4 of 4     I < page 1									
	200 per page									

## 9. 客户端验证

Deploy Now Policies have been deployed.

在确保客户端 on l ine 并接收到 DLP 服务端的策略下发后。违反策略后,DLP 将会弹 出警告框

ĺ	Security alert!		
	The data you are sendir You have 1 message(s)	ng or copying contains sensitive information. I.	
	Time	Message	Link
	23:46.17	File transfer: E:\Ex2010.ppt prohi	参违反了Mac的关键字。
	<		>
	Powered by Trend Micr	o, Inc. All rights reserved.	
			Dismiss



#### 数据外泄管理系统 DLP5.5

小贴士:离线 Offline 模式下,通过 channel 传送数据指纹的文件,为何 DSA 不检测?而 Online 模式下 DSA 可以检测?

如果您的客户端是 Production Evironment,则需要做如下操作:

打开 DLP 控制台----Update---Agents---Product Environment

转到 Fingerprints 页面, 勾选 Auto-Update (很重要!)

点击 Dep loy,过几分钟再次验证

2										
Summany	Updates - Produ	iction Env	ironment							🕜 Help
b Data Bratactica	Use this page to rol	lback patches	s, delete add	-ons, deploy f	fingerprints,	and view data stea	ling malwa	re patterns in the	production	
+ Data Protection	environment.									
+ Reports										
+ Logs	Patches					Fingerprints				
- Update	Undete Otature	Endpoint	t Agents	Network	Tabal	Undete Chature	Endp	oint Agents	Network	Tabal
- Agents	Update Status	Online	Offline	Agents	Total	Update Status	Online	Offline	Agents	Iotai
Staging Environment	Updated	1	2	1	4	Updated	1	0	1	2
Configuration	Outdated	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	Outdated	<u>0</u>	2	<u>0</u>	2
+ Administration	Total	1	2	1	4	Total	1	2	1	4
	Add-ons					Patterns				
	Update Status	Onlin	ne (	Offline	Total	Update Sta	Endpoint Agen	int Agents Network Agent		
	Updated	1		2	3	Updated		2		1
	Outdated	<u>0</u>		<u>0</u>	<u>0</u>	Outdated		1		<u>o</u>
	Total	1		2	3	Total		3		1
	Patches Add	ons Fi	ngerprints	Data Ste	aling Malwa	are Patterns				
	Available Update	es								
	Deploy								🔽 Auto	o-update
	Name	Current	Version	Deploye	d Version	Update I	nitiated Or	n	Release Dat	e
	<u>Fingerprint</u>	5		5		12/29/10 11:	25:36 PM	CST 12/29	/10 11:25:3	5 PM CST

## 4.1.4 DLP 设备管控

除了策略部署外,DLP 还支持对客户端进行设备管控。 支持如下设备管控: CD/DVD IEEE 1394 Bus host controllers Modems Floppy disk controllers Ports (COM & LPT) Infrared devices Imaging devices Print Screen Key PCMCIA adapters Removable disk drives (支持设定认证 USB)

注意: 当勾选 Removable disk drives 后,当用户插入一个 USB 设备时, DLP 将做如下操作:

- 禁止此 USB 设备
- 弹出警告框.
- DLP 服务端上记录日志.



Sec	urity a	lert!				Þ	<
The	data you a	are sending	g or copying con	tains sensitive inform	nation.		
You	have 1 me	ssage(s).					
	Ti	me	Message			Link	]
9	00:0	0.42	Device[FLAS	H Drive AU_USI	820 USB D		
Pow	ered by Tr	end Micro	, Inc. All rights re	served.			
	,		,		Diemies		
					Distilise	<u></u>	
							_
Quer	y						[ <u>Hide Query</u> ]
Data	Range:	Last 7	days 🔻				
		From	[	12:00 To		12:00	
Log I	ype:	Policy D	eployment Violations	System	Events		
		<ul> <li>Server S</li> </ul>	Status	Securit	y Audit		
Sh	ow Log						
<b>Filte</b>	er <b>F</b> xport	nefresh 🔁				1-22 of 22	
Syster	m Events	-				1 11 51 22	page 1 t ol 1770
ID -		Log Tim	e	Severity		Description	
299	12/30/10	L2:07:54 AM	1 CST	Informational	Device[FLASH Driv	e AU_USB20 USB D	evice] is disabled! @ T

## 4.2 DLP 服务端的其他设定

## **4.2.1 Data Discovery**

DLP 可以提供扫描装有 DSA 客户端的 PC 客户端,扫描电脑上是否存有基于定义的敏感文件。

(此功能默认一般不启用,如需启用,请根据实际情况进行设定)

1. 点击 Data Protection---Data Discovery, 右边点击 Add



### 数据外泄管理系统 DLP5.5

Data Loss	Prevention	Logged on as: 🤱 admin 🔏						
Summary — Data Protection	Data Discovery         Trend           Use this page to determine the location of your network's confidential information.	MicroTM DLP Workflow 🗗 记 Help						
+ Digital Assets	Add Copy Delete Run Pause Stop Schedule Scan	J-O of 0 H∢ page 1 ▼ of 1 ► H						
Compliance Templates	[View all scheduled tasks]							
Data Discovery	□ Name ▲ Scanned High Risk Endpoints Last Run Time	Status Report						
Device Control	GAdd      Copy      Delete      Run      IIIPause      Stop      Schedule Scan     Copy	)-O of 0 ዞ∢ page 🔟 💌 of 1 ↦ ዞ						
+ Reports		200 per page 💌						
+ Logs								
+ Update								
+ Administration								

### 2. 设定策略名称,并将目标客户端选中,并添加到右边。点击 Next

Data-at-Rest Policy	
<ul> <li>Create a new discovery task: 扫描策略</li> <li>Copy from an existing task: select one </li> </ul>	
Target	
Select by Domains/Endpoint 💌	
Search Selected:     From     TANG-XP     MAC - XP     Add >>   Remove <<	

3. 选择所需要的策略模板,并设定扫描的路径例如 C:\, 点击 Next 注意: 基于系统稳定性和性能的考虑, DLP 将不会扫描以下文件或者目录: Windows Share folder (Windows 共享文件夹) Removable device (例如 USB 设备、DVD 设备). autoexec.bat 文件 \Cookies\

\Local Setting\
\Application Data\
\Program Files\
\Windows\
\WINNT\



Select the Compliance Templates								
GLBA HIPAA Mac 关键字 Mac 英键方件 Mac 文件后缀名 PCI-DSS SB-1386 US PII 与得通讯								
Root path: C:\								
Priority: Normal 💌								
Scan Exceptions								
Include:								
Exclude:								

#### 4. 选择处理措施(建议只要选择 Log)

注意:强烈建议不要使用 MOVE 和 Encrypt,以免涉及用户系统关键文件或者应用程序文件,影响操作系统运行。

System Action When Online	
M Log	
Other Actions	
Move to security folder:	
Encrypt	
System Action When Offline	
M Log	
Conter Actions	
Move to security folder:	
Encrypt	

#### 5. 配置完毕后,点击 Run 可以立即运行,或者点击 Schdule Scan 预设扫描

∎A	xdd 💽 Copy 🏦 🕻	Delete 🕨 Run 💷 Pau	se 🔳 Stop	TSchedule Scan	1-1 0	f1 🙌 page 🚺	▼ of 1 M			
	[View all scheduled tasks]									
◄	Name 🔺	Scanned	High Ris	sk Endpoints	Last Run Time	Status	Report			
	<u>扫描策略</u>	0	0			New	Q			
∎A	xdd 💽 Copy 🏦 🛙	Delete 🕨 Run 💷 Pau	se 🔳 Stop 🤇	TSchedule Scan	1-1 0	f 1 🙌 page 🚺	▼ of 1 M			
						200 p	er page 💌			

## 4.2.2 Reports 报表生成

1. 点击 Reports---Generate Reports, 右边点击 Add



### 数据外泄管理系统 DLP5.5

Data Loss	Prevention				Logged on a	as: 🧟 admin 🔏	
Summary + Data Protection	Generate Report Use this page to add and edi	t all report templ	ate definitions.	<u>Trend Micr</u>	o <sup>TM</sup> _DLP Wor	kflow 🗗 记 Help	
- Reports Archived Reports Generate Reports	©Filter			1-1 o Retain Period	1-1 of 1 ₩4 page 1  of 1 > M ain Period Status Effective		
+ Logs	Mac report	Daily	12/7/10 10:07:36 PM C	30	<b>*</b> •	effective	
+ Update	GFilter      GAdd      Copy     GDelete     1-1 of 1      H ← page     1      of 1      H						
+ Administration					2	00 per page 💌	
				🛹 Report Enabled	🗙 🔿 Report	Disabled	

2. 设定 Report Name 名称等报表信息。

可以根排	居需求,说	殳定 one-time {	报表或者	预设报表	(每日、	每周、	每月)	
Adding Reports	(*: Require	d field)						🔡 Help
Report Name								
Report Name:*								
Report Title:*								
Recurrence Patt	tern							
One-time								
O Daily O Weekly O Monthly	From:*	12-29-2010 🛛 🗷	To:*	12-30-2010 mm-dd-yyyy				
Report By								
<ul> <li>Endpoint Age</li> <li>All targets</li> <li>Specific us</li> <li>Specific en</li> <li>Network Age</li> <li>All networi</li> <li>Specific de</li> </ul>	ent eers ndpoints nt k devices evices							

3. 以及勾选报表内容需要的选项



### 数据外泄管理系统 DLP5.5

1.Top Violator Information	3.Executive Summary Information
🗹 Select All	🗹 Select All
Top 10 Data Fingerprints by Violation	Violation Summary Trend by Channel by 8 weeks
✓ Top 10 Destinations by Violation	Data Stealing Malware Violation Summary Trend by Channel by 8 weeks
Top 10 Endpoints by Violation	Violation Distribution
☑ Top 10 Users by Violation	-by Policy
Top 10 Templates by Violation	-by Channel
Top 10 Policies by Violation	-by Template
✓ Top 10 IP Addresses by Violation	-by Department(only for Endpoint Agents)
✓ Top 10 Email Addresses by Violation	✓ Top 10 Department Violations
Top 10 Endpoints infected by Data-stealing Malware	Top 10 Policy Violations
☑ Top 10 Data-stealing Malware Destinations	🔽 Top 10 High Risk Users
✓ Top 10 Email Destinations	🔽 Top 10 Users Infected by Data Stealing Malware
☑ Top 10 URL Destinations	☑ Top 10 IPs Infected by Data Stealing Malware
	✓ Top 10 Email Account Violations
2. Summary Information	4. Audit Information
🗹 Total Violations Over Time	🗖 Compliance Audit Report
Total Violations by Channel	
Total Violations by Data Fingerprint	
Total Violations by Template Name	

### 4. DLP 的报表可以发送邮件给到管理员。这边需要设定报表的格式。以及邮件收件 人等信息。

Time to K	eep This Report
30 d	ays 💌
🗆 Email	This Report
Format:	O PDF ☉ HTML O EXCEL
To:*	Separate multiple addresses with a comma.
Subject:*	

### 同时,还需要进行邮件通知设定

#### (Administration---Server configuration---Application Settings)

TREND Data Loss	Prevention		Logged on as	admin 🔏
Summary	Administration - Applicati	ion Settings		🕑 Help
+ Data Protection	Server Side Alert Email Not	tification		
+ Reports	Email Server Host Name:	trend.mac.com		
+ Logs	Username:	tyr_86		
+ Update	Password:	•••••		
– Administration	Sondor ombile	tur 96@maa.com		
- Server Configuration	Senuer email:	Lyr_so@inac.com		
Fingerprint Settings	Recipient email:	tyr_86@mac.com		
Application Settings		Senarate multiple email addresses with a comma	0	
+ Agent Configuration		coparace maraple cinar addresses with a comma.		
And the Management				

#### 注意:设定必须准确,如果通知设定出现错误,报表将不会生成。

5. 每天生成好的报表会在 Archived Reports 中查询。用户也会收到邮件。



Data Loss Prevention

### 数据外泄管理系统 DLP5.5

Loggod on act	💿 admin	1
Loggeu on as.	👸 auiiiiii	6

Summary + Data Protection	Report Data Use this page to catalog all t	he archived repo	rt data.	Trend Micro	DLP Workflow 🗗 😨 H	lelp
- Reports	🟹 Filter 🍿 Delete				H 4 page 🔽 of H	F FI
Generate Reports	🗖 🛛 Report Name 🔺	Туре	Date	Days to Save	Output	
+ Logs	Mac_report	Daily	12/7/10 10:08:27 PM CST	9	<u>html pdf excel</u>	
+ Update	Mac_report	Daily	12/7/10 11:59:07 PM CST	9	html pdf excel	
Administration	Mac_report	Daily	12/8/10 11:59:20 PM CST	10	<u>html pdf excel</u>	
	Mac_report	Daily	12/9/10 11:59:10 PM CST	11	html pdf excel	
	Mac_report	Daily	12/10/10 11:59:30 PM CST	12	<u>html pdf excel</u>	
	🗖 Mac_report	Daily	12/11/10 11:59:26 PM CST	13	html pdf excel	
	🗖 Mac_report	Daily	12/12/10 11:59:27 PM CST	14	<u>html pdf excel</u>	
	🗖 Mac_report	Daily	12/13/10 11:59:06 PM CST	15	html pdf excel	
	Mac_report	Daily	12/14/10 11:59:05 PM CST	16	<u>html pdf excel</u>	
	Mac_report	Daily	12/15/10 11:59:05 PM CST	17	html pdf excel	
	Mac_report	Daily	12/16/10 11:59:24 PM CST	18	html pdf excel	

#### 邮件通知中的内容:



Report 'Mac\_report\_DLP' is attached. Please check.

Generation time: 12-29-2010 23:59:00

## 4.2.3 DLP 产品补丁更新/安装

1. 默认情况下,趋势科技会定期出 DLP 产品的 Patch 补丁,并放在 AU 更新源上, DLP 服务端可以更新到。



Data Loss Prevention

#### 数据外泄管理系统 DLP5.5

Logged on as: 🤱 admin

~				
Summary	Configuration			🕄 He
+ Data Protection	Server Update	Source		
+ Reports	Trend Micro	Active Update Server (http://	/tmlp55-p.activeupdate.trendmicro.com	n/activeupdate)
+ Logs	O Other Upda	ite Source		
- Update	URL:			
- Agents	Broyy Sotting		🔽 Eashia Draw	
Staging Environment	FIDAy Settings		Enable Proxy	
Production Environment	Proxy Type:	HTTP 🗾		
Configuration 🕨	Server name:	10.28.129.90		
+ Administration	Port Number:	8080		
	Username:			
	Password:			Hide characters
	Download Upd	ate Schedule	🔽 Enable Schedul	ed Update
	© Daily ○ Weekly ○ Monthly	Every: <b>*</b> 1 day	Time: 01 💌 : 00 💌	AM 💌

#### 2. DLP 服务端也可以手动更新补丁。

#### 注意: DSA 客户端分为 2 中模式:

Staging Environmente ---适用于策略测试和补丁测试。

Production Environment---适用于所有客户端

默认情况下补丁安装后,先应用到 Staging Environment 模式的客户端,便于管理员在进行批量 部署到全部客户端之前,先小范围进行应用测试。测试有效后,在 Deploy to Production 模式

#### 导入部署需注意: DLP 安装补丁有先后顺序,需按顺序导入,但可以几个补丁同时进行安装。

Summary	Updates - Stagiı	ng Enviror	nment							🔁 Hel
Data Protection Reports	Use this page to t agents in the <b>stag</b>	est and rev <b>Jing</b> enviro	view new ve nment.	rsions of pa	tches, add	d-ons, fingerprints :	and data	stealing malwa	re patterns	; to
Logs	Patches					Fingerprints				
Update	Lindata Status	Endpoin	t Agents	Network	Total	Undato Status	Endpo	oint Agents	Network	Total
- Agents	opuate status -	Online	Offline	Agents	TUCAL	Opuace Status	Online	Offline	Agents	TUCAL
Staging Environment 🔸	Updated	0	0	0	0	Updated	0	0	0	0
Production Environment	l Outdated	<u>0</u>	Q	<u>0</u>	0	Outdated	<u>0</u>	D	<u>0</u>	0
Configuration	Total	0	0	0	0	Total	0	0	0	0
Auministration										
	Add-ons					Patterns				
	Update Status	Onlir	ne (	Offline	Total	Update Stat	tus	Endpoint Agent	s Network	< Agent
	Updated	0		0	0	Updated		0	1	D
	l Outdated	<u>0</u>		<u>0</u>	<u>0</u>	l Outdated		Q	1	0
	Total	0		0	0	Total		0		D
	Patches Ad	d-ons	Fingerprints	Data S	tealing Ma	alware Patterns				
	Augilable Undate									

## 4.2.4 DLP 的 Administration 设定

DLP 服务端设定, Fingerprints 指纹获取设定
 小贴士: 默认设定下: 以下情况下的文件, DLP 服务端不会获取文件指纹。
 最小文件:小于 62Bytes (特别是空文件)
 最大文本文件:大于 6M (常见为文档)



最大二进制文件: 32MB(常见为. exe 等应用程序) 最大存档的文件: 32MB(DLP 客户端触发策略后,将外泄数据存档备份到 DLP 服务端) 最大部署到客户端的指纹大小: 300MB

解压缩后文件大小:128MB(解压后文件大小超过 128M 的文件,DLP 不会去获取其指纹) 压缩层数:10(压缩超过 10 层的文件,DLP 不会去获取其指纹) 解压后的文件:2000 个(解压后文件超过 2000 个的文件,DLP 不会去获取其指纹)

Data Loss	Prevention Logged on as	: 🤮 admin 💡
Summary	Administration - Fingerprint Settings	🕑 Help
+ Data Protection		
+ Reports	BZ Bytes	
+ Logs	Maximum text file size:* 6 MB 🔽 🦊	
+ Update	Maximum binary file size:* 32 MB 🖌 🦊	
- Administration	Mayimum archive file size *	
- Server Configuration		
Fingerprint Settings 🕠	Maximum repository size to download to agent:* 300 MB 💌 🔑	
Application Settings		
+ Agent Configuration	Fingerprint Decompression Control Settings for Acquisition	
Crawler Management	Trend Micro DLP will not process if the decompressed file size exceeds:* 128 MB 🗹 🦊	
Data Management	Trend Micro DLP will not process if the total number of embedded layers in the compressed file exceeds: 10 💌	layer(s)
Agent Management	Trend Micro DLP will not process if the total decompressed file number exceeds:* 2000 (1-2000)	
Password		

### 2. 通知邮件设定 触发违规事件或者发送报表时,系统会基于设定进行发送通知邮件

TREND Data Loss	Prevention		Logged on as	admin 🔏
Summary	Administration - Applicat	tion Settings		🕑 Help
+ Data Protection	Server Side Alert Email No	otification		
+ Reports	Email Server Host Name:	trend.mac.com		
+ Logs	Username:	tyr_86		
+ Update	Password:			
– Administration	Candanamail	hun 06 @maa aam		
- Server Configuration	Sender email:	tyr_86@mac.com		
Fingerprint Settings	Recipient email:	tyr_86@mac.com		
Application Settings		L Senarate multiple email addresses with a comma	2	
+ Agent Configuration		Separate multiple email addresses with a comma.		
Crawler Management	Cauci			
Data Management	Save			
Agent Management				
Password				
+ Management Console				
LDAP				
Product License				

3. 客户端设定 Agent Settings

#### 相关说明:

a) Agent Batch Encryption Settings

如果策略设定 DLP 触发违规事件后,需要用户输入 Justification 或者针对 USB 存储进行自动加密(Encryption)

默认随后的 30 秒内将参照第一次的操作,不再提示,日志将记录。

b) Local LDAP Cache

默认 DLP 服务端与 LDAP 进行同步周期为一天。

- c) Decompression Control Settings
  - 针对部分压缩文件,DLP 不会进行检测
    - 解压缩后文件大小:128MB(解压后文件大小超过 128M 的文件, DLP 不会进行检测)
    - 压缩层数: 10(压缩超过 10 层的文件, DLP 不会进行检测)
    - 解压后的文件: 2000 个 (解压后文件超过 2000 个的文件, DLP 不会进行检测)
- d) Change password



#### 数据外泄管理系统 DLP5.5

此处为 DLP 备份用户外泄的敏感文件到 DLP 服务端时,自动进行加密备份 当从控制台下载时,自动会进行解密(默认密码:12345678)

Data Loss	Prevention Logged on as: Sadmin
Summary	Administration - Agent Settings
+ Data Protection	Agent Batch Encryption Settings
+ Reports	Agent Batch Encryption/Justification Timeout:* 30 second(s)
+ Logs	Agent Batch Encryption Filename Prefix:* dlp_encrypted_ 🤑
+ Update	Local LDAP Cache
- Administration	Time To Live (TTL): 1 🖬 day(s)
- Agent Configuration	Decompression Control Settings
Agent Settings 💦 🔸	Trend Micro DLP will not process if the decompressed file size exceeds:* 128 MB 🖃 🦊
Advanced Settings	Trend Micro DLP will not process if the total number of embedded layers in the compressed file exceeds: 10 💌 layer(s)
Global Exceptions	Trend Micro DLP will not process if the total decompressed file number exceeds:* [2000] (1-2000)
Crawler Management	
Data Management	Change password: The password is used for forensic data encryption and data discovery
Agent Management Password	Old password:*
+ Management Console LDAP	New password:*
Product License	Confirm password:*
	Passwords must be from 8-32 characters.

#### 4. 高级设定 Advanced Setting

#### 客户端警示框特制,例如:更改图标,更改内容等等

#### 注意:在Load Dialog File 按钮后,需把<Logo Show="0"> 改为 <Logo Show="1">.

Logo 图片只支持 GIF 和 JPG 格式,大小限制在 3M 以内。

Dialog Configuration Logging Configuration UDP Listener

Customize agent alert dialog	
<pre><?xml version="1.0" encoding="UTF-8"?> <!-- This is an XML file to describe application(s) customization 5.0/1000--> <!DOCTYPE Application SYSTEM "CustomDlg.dtd">     <!--Application Id="ShowMsg"--> <!--MessagesList--> <!--ContentBlock-->Content transfer prohibited. <!--ContentBlock-->Content transfer not recommended. <!--FileBlock-->File transfer: {0} prohibited. <!--SMBlock-->Data steal malware transfer data prohibited. <!--DSMBlock-->Data stealing malware may be transferring data. <!--MessagesList--> <!--Dialog Id="AlertDialog"--> <!--Title-->Security alert! <!--ControlsList--> <!--Co</th--><th></th></pre>	
Logo	
Upload Logo: 选择文件 未选择文件 Note: Accepts GIF and JPG format only. Logo image file cannot exceed 3MB. Remember to change <logo show="0"> to <logo show="1"></logo></logo>	

5. 全局例外 Global Exceptions

相关说明:

● 黑白名单如果出现冲突,则根据以下优先级:BlockedList -> ApprovedList -> Network Boundary

格式: (IP address/subnet mask: port range)

😰 Help

例如: 10.28.0.111 10.28.0.111:80 10.28.0.111:80-90 10.28.0.111/24 (只支持/XX 格式,不支持例如 255. 255. 255. 0 等格式)

- ▶ 如果客户端上网通过代理服务器,请把代理服务器地址添加至 Blocked List
- 请把用户自己的邮件域名和 X. 400 地址输入至 Internal Email Domain 这样用户域之间邮件互发将正常,不会被 DSA 检测。
   格式:
   Global ExceptionsX400 format: "/O=Trend/OU=USA, /O=Trend/OU=China."
   Email domains: example.com.

Administration - Global Exceptions

Approved List				
Define safe services. (Example, IP address/subnet mask:port range)				
Separate multiple entries with a comma.				
Blocked List				
Define unsafe services. (Example, IP address/subnet mask:port range)				
10.28.129.90/25				
Separate multiple entries with a comma.				
Internal Email Domains				
List all internal email domains (Example, /O=trend/OU=usa).				
mac.com;/O=mac				
Separate multiple entries with a comma.				

#### 6. DLP 服务端配置文件导出/导入,支持把策略等信息可以全局导出和导入 注意:如果导出文件小于 200M,请通过 Web 页面进行导入 如果导出文件大于 200M,请通过以下方式导入:

- 1、 使用诸如 FTP 工具把之前导出的文件上传到 DLP 的 Linux 内核中(注意不要更改原文件名)
- 2、 SSH 登录 Linux 内核命令行模式(请使用 dgate 账号)
- 3、转到以下目录: /home/dgate/prod/common/scripts
- 4、 输入以下命令. /dg\_import. sh (/之前有个"."不要忘记)
- 5、 等待执行完毕后,重启 DLP 服务器

#### **Data Loss Prevention** Administration - Data Management Summary Data Management Control C Exported Files Data Protection $^{\circ}$ Import file to system data repository + Reports + Logs Select a data file to import: 选择文件 未选择文件 + Update Export file from system data repository $\odot$ Administration Full Data Export + Server Configuration O Report Definition Data Export - Agent Configuration O Security Policy Data Export Agent Settings O Data Discovery Data Export Advanced Settings O Sensitive Information Data Export Global Exceptions O User and Role Data Export Crawler Management Data Management Start Agent Management Password + Management Console LDAP Product License

#### 7. Agent 版本信息和组信息

#### 注意: 这里会显示 Agent 版本信息,特别是之后安装 Patch 补丁后,可以在此验证 Agent 的版本 是否有正确升级

Data Loss Prevention Logged on as: admin							
Summary	Agent Management  Aqent Management allows the user to browse and edit agents or groups.						
Reports     Logs	Agents Group						
+ Update - Administration	QFilter Delete	IP Address	Status	Policy Status	Fingerprints	1-4 of 4 ₩ 4 p Agent Version	Last Modified
+ Server Configuration - Agent Configuration	□ = <u>jason zh</u> □ = mac-xp	10.28.132.63 10.28.132.21	Disconnected Disconnected	Outdated Outdated	3 1	5.5.1263 5.0.1370	12/9/10 3:33:4 12/1/10 11:17:
Agent Settings Advanced Settings	□	10.28.132.19 172.16.4.242	Online Online	Updated Updated	5	5.5.1263 2.0.1135	12/29/10 11:52 12/29/10 11:49
Crawler Management	Filter 👚 Delete					1-4 of 4 ⊌∢ p	age <mark>1 ▼</mark> of 1 ► ₩
Agent Management  Password						= Endpoint Age	200 per page 💌 ent 🖲 Network Agent
可以创建用户组,将客户端添加至组中							
Tilter Add 🔒 De	lete				1-1 0	of1 ⊌∢page	1 ▼ of 1 ► ₩
🗖 🛛 Group Name 🔺	Des	cription	Agents		Last	Modified	
Mac測试Group	Mac测试Gro	oup	1	11/24/10	9:40:54 AM CS	т	
Tilter 🔁 Add 🕋 Del						1 ▼ of 1 ► ►	
						20	)0 per page 💌

8. 账号设定和密码设定,可以针对用户角色进行设定,分配给不同权限的账户



### 数据外泄管理系统 DLP5.5

Data Loss	Prevention		Logged on as:	🔒 admin 🛛 🔏
Summary	User Accounts			💽 Help
+ Data Protection	📑 Add 🍵 Delete		1-1 of 1 🛤 page 🕽	. ▼ of 1 ► ₩
+ Reports	Lisername	•	Role	Status
+ Logs	-		i colo	Status
+ Update	I <u>admin</u>	administrator sec	curity manager	<b>~</b> •
– Administration	📬 Add  🍿 Delete		1-1 of 1  ⊌∢ page 1	. ▼ of 1 ► ₩
+ Server Configuration			200	ner nage 🔳
+ Agent Configuration			1200	por page
Crawler Management			😬 Account Enabled 🛛 🗶 🖻 Acco	unt Disabled
Data Management				
Agent Management				
Password				
- Management Console				
User Accounts 🔰				
Role Management				

#### 9. LDAP 的设定

注意:目前 LDAP 设定只支持 Microsoft Active Directory 为了确保有效,设定完毕后,需重启 DLP 服务器

Data Loss	revention			
		🛛 Helo		
Summary				
+ Data Protection	ata Protection LDAP Settings			
+ Reports	LDAP Server Type: Microsoft Active Directory			
+ Logs				
+ Update	M Enable Primary LDAP server			
– Administration	Server name:  172.16.4.239			
+ Server Configuration	Example: server1.u	s.example.org or 123.123.123.123		
+ Agent Configuration	Base DN: DC=mac,DC=com			
Crawler Management	Port: 389			
Data Management	Login Llogr Name (DN) - mag) administrator	_		
Agent Management	Login Oser Name/DN: Imac\auministrator			
Password	Password:	••		
- Management Console	🗖 Enable SSL [Ce	rtificate Management]		
User Accounts	Test Connection			
Role Management	Connection success.			
	Enable Backup LDAP server			
Product License	Server name:			
	Example: server1.u	s.example.org or 123.123.123.123		
	Base DN:			
	Port: 389			
	Login User Name/DN:			
	Password:			
	🗖 Enable SSL [Cer	tificate Management]		
	Test Connection			
	LDAP Cache Expiration			
	Time to Live (TTL): 60 minute(s)			
	Save			
	CAUTION: The DLP server MUST be restarted for ar	y new changes to take effect.		



## 4.2.5 客户端收集 Debug 日志方式

#### 收集方式:

- a) 选中需要收集日志的客户端
- b) 将所对应的 Module 添加至右边
- c) 勾选 Logging 等级
- d) 设定存储位置

- e) 点击 Enable Agent Log
- f) 在客户端上重现问题。
- g) 重新问题后,收集 C:\目录下所对应的日志文件,传给趋势科技进行分析

MICRO	Data Loss	Prevention				Logged on as: 🤮 admin 🔏
C		Administration - Adva	inced Settings			
Summary	tion	You can edit the logging	configuration file to enable	or disable the logo	jing of any agent modules.	Remove this module from
Data Protect	tion	the selected list to disab	le any additional module lo	gging. To disable a	ll logging, delete all items fr	om the selected list.
+ Reports		Dialog Configuration	Logging Configuration	UDP Listener		
+ Logs			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
- Administrat	tion	Endpoints*: <u>Select en</u>	apointsj (ANG-XP			
+ Server Cor	nfiguration	Module:*			Selected modules:	
- Agent Con	figuration	Network Filter		*	Network Filter(Critical Erro	or,Error,Warning,Verbose 🔺
Aaent Se	ettinas	File Filter			File Filter(Critical Error	r,Error,Warning,Verbose) or,Warning,Verbose)
Advance	d Settings	Share Folder Filter			Share Folder Filter(Critica	l Error,Error,Warning,Verb
Global Ex	ceptions	Agent Alert Dialog			Agent Alert Dialog(Critical	Error,Error,Warning,Verbose)
Crawler Ma	anagement	LDAP		Add >>	LDAP(Critical Error,Error,V	Varning,Verbose)
Data Mana	agement	. Outlook Filter		D	Outlook Filter(Critical Erro	r,Error,Warning,Verbose)
Agent Man	agement	Network Parsers		Remove <<	Network Parsers(Critical E	Error,Error,Warning,Verbo
Password		Policy Engine			Policy Engine(Critical Erro	r,Error,Warning,Verbose)
+ Manageme	ent Console	Match Engine			Match Engine(Critical Erro	r,Error,Warning,Verbose)
LDAP		Auto Update Client		-	Auto Update Client(Critica	al Error,Error,Warning,Verl
Product Lic	cense	Logging lovels*	I oritical former			
		Logging level;	Critical Error			
			✓ Warning			
			Verbose			
		Type:	File			
		Full noth file nome	ei\mpo1			
		rui paurnie name.	Specify the full nath of th	e loa file to which y	rou want the agent to write	For example.
			C:\dlpagent.log.	o log no co milori ,	ou nunc allo agone to ninto	rror onampio,
			1			
		Enable Agent Log Di	isable Agent Log			_
🧇 本地	<u> 禰盘</u> (C:	0				
文件 (2)	) 编辑(E)	) 查看(V) 收藏	【(A) 工具(T)	帮助(H)		
-	-					
6 🜔	退 🔹 🕞	) - 🍙 💭 i	腹索 🛛 🔂 文件夹			
-						
地址(2)	🥯 C: \					
			Documents an	d Settings		_
无机	HA					
**	11.39	$\odot$	moulache			
$\sim$		99.65.65.27	🗀 Office2007			
	1236年1月1日日日日日	時的内袋	🛅 Program File	s		
12						
				m. 173 VF -		
	我亲又作或	以任天	📄 dipinstall. 1	og. TANG-XP. 1	Log	
			📕 mac1. TANG-XP	log		

# 5 通信端口列表

部署之前,请确保开启以下通信端口:

DLP 服务端控制台:	8080 (HTTP) , 8443 (HTTPS)
SSH 访问 DLP 服务端:	22
End Agent 访问 DLP 服务端:	8804(TCP), 8904(TCP).1558(UDP)
Network Agent 访问 DLP 服务端:	8804(TCP), 8904(TCP).1558(UDP)
Remote Crawlers访问DLP服务端:	8080 (HTTP), 8443 (HTTPS)



# 6 趋势科技厂商资源

800 免费技术支持热线 800-820-8839

#### 800 免费商务热线

800-820-8876

售后电子邮件地址 service@trendmicro.com.cn

#### 趋势科技中文网站

http://cn.trendmicro.com/cn/home/

#### 病毒查询

www.trendmicro.com.cn/vinfo

趋势科技英文网站 http://us.trendmicro.com/us/home/

#### 趋势科技病毒递交信箱 virus\_doctor@trendmicro.com.cn