

趋势科技

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	DLP 5.5 服务端 (DATA LOSS PREVENTION SERVER)	7
2.2	DLP 5.5 客户端 (END 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
3.1	安装 DLP 5.5 服务端.....	10
3.1.1	安装前的准备	10
3.1.2	安装的过程	11
3.1.3	安装后的初始化配置 (重要)	19
3.2	安装 DLP 5.5 客户端.....	26
3.2.1	安装前的准备	26
3.2.2	安装过程	26
3.3	安装 TMDLPNM 2.0 (可选)	30
3.3.1	安装前的准备	30
3.3.2	安装的过程	30
3.3.3	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	客户端收集 Debug 日志方式	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

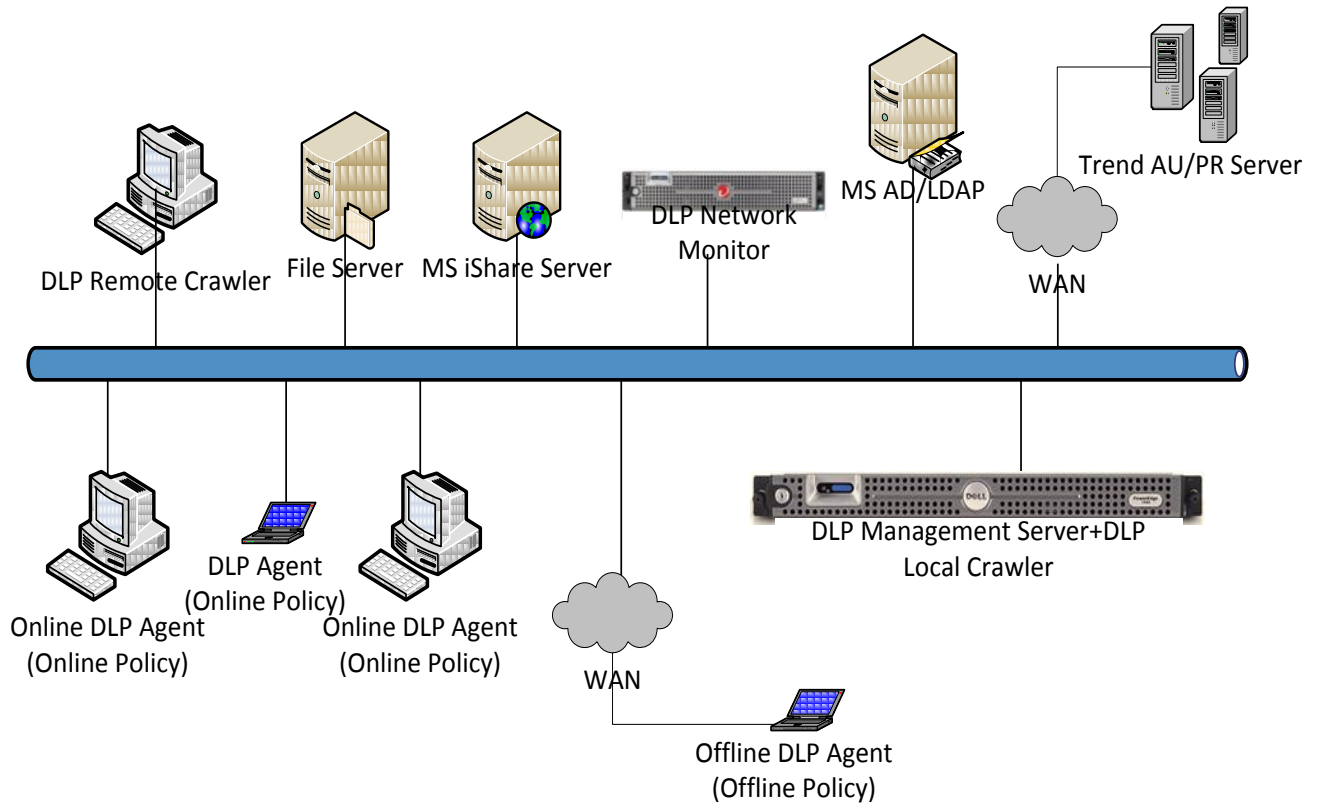
1 什么是 Data Loss Prevention?

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:



Fingerprint Matching (指纹匹配)	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。
Pattern Matching (模板匹配)	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 可以根据关键字进行匹配
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™ 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™ 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 Network 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 新功能一部分

- 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 2003 Web Edition SP2
Windows 7 Ultimate	Windows 2003 Standard R2 SP1/SP2
Windows 7 Enterprise	Windows 2003 Enterprise R2 SP1/SP2
Windows 7 Starter	Windows Vista Enterprise SP1/SP2
Windows 7 Home Basic	Windows Vista Business SP1/SP2
Windows 7 Home Premium	Windows Vista Home Premium SP1/SP2
Windows 2008 Datacenter SP1/SP2	Windows Vista Ultimate SP1/SP2
Windows 2008 Enterprise SP1/SP2	Windows Vista Home Basic SP1/SP2
Windows 2008 Standard SP1/SP2	Windows XP Professional SP2/SP3
Windows 2003 Enterprise SP1/SP2	Windows XP Tablet 2005
Windows 2003 Datacenter SP2	Windows XP Home SP2/SP3
Windows 2003 Standard SP1/SP2	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 TMDLPM 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!)

2) **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。

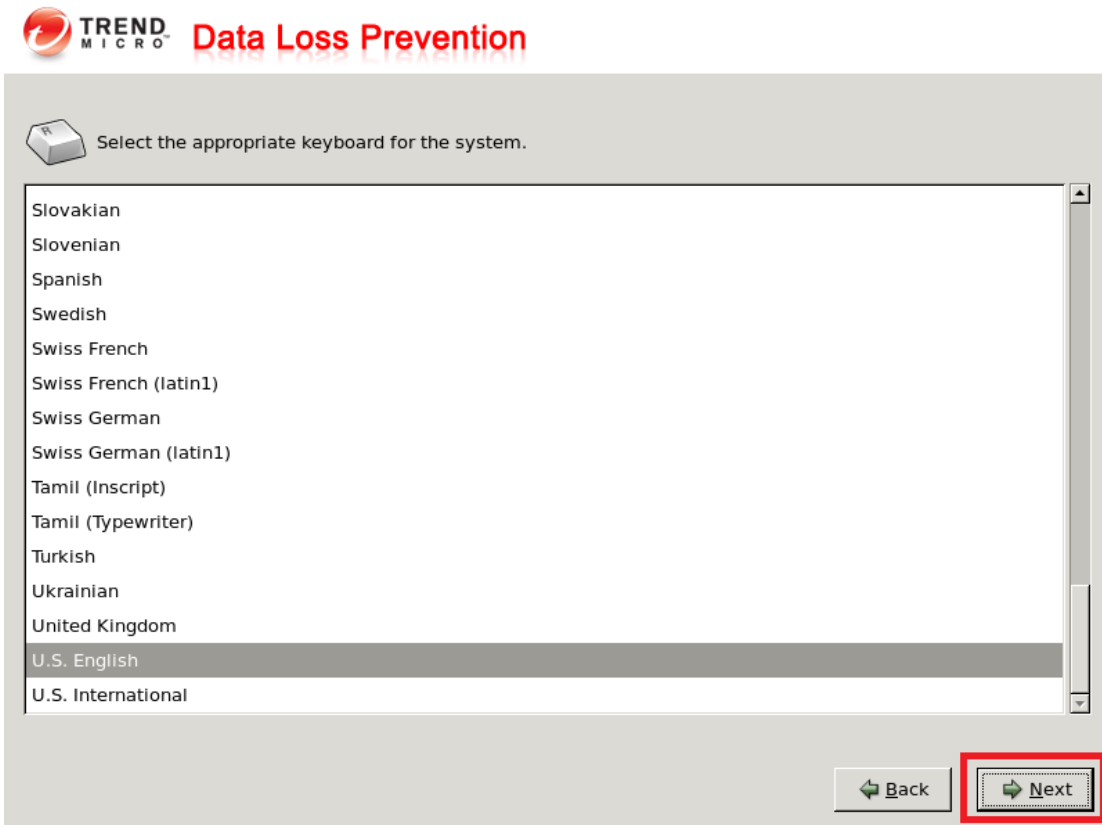


注意: 此操作仅供测试使用.

3. 接受许可协议, 点击 Accept

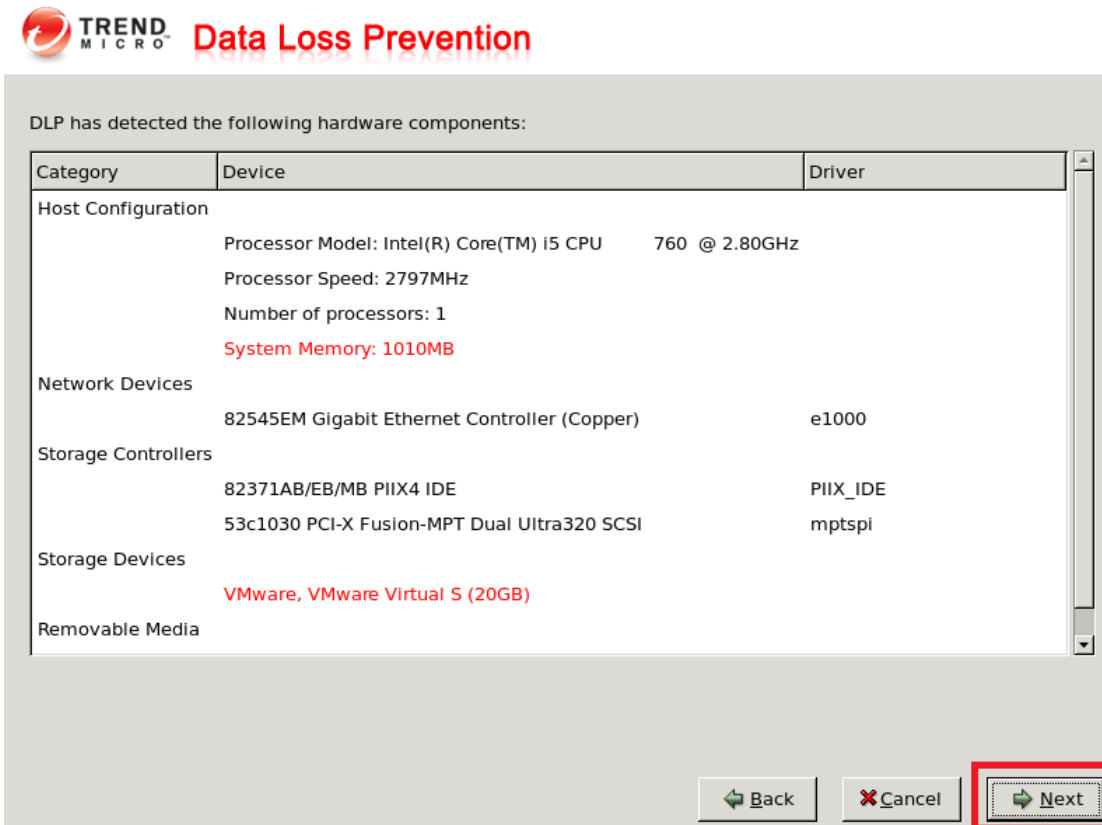


4. 选择安装向导语言类型，选择默认，点击 Next

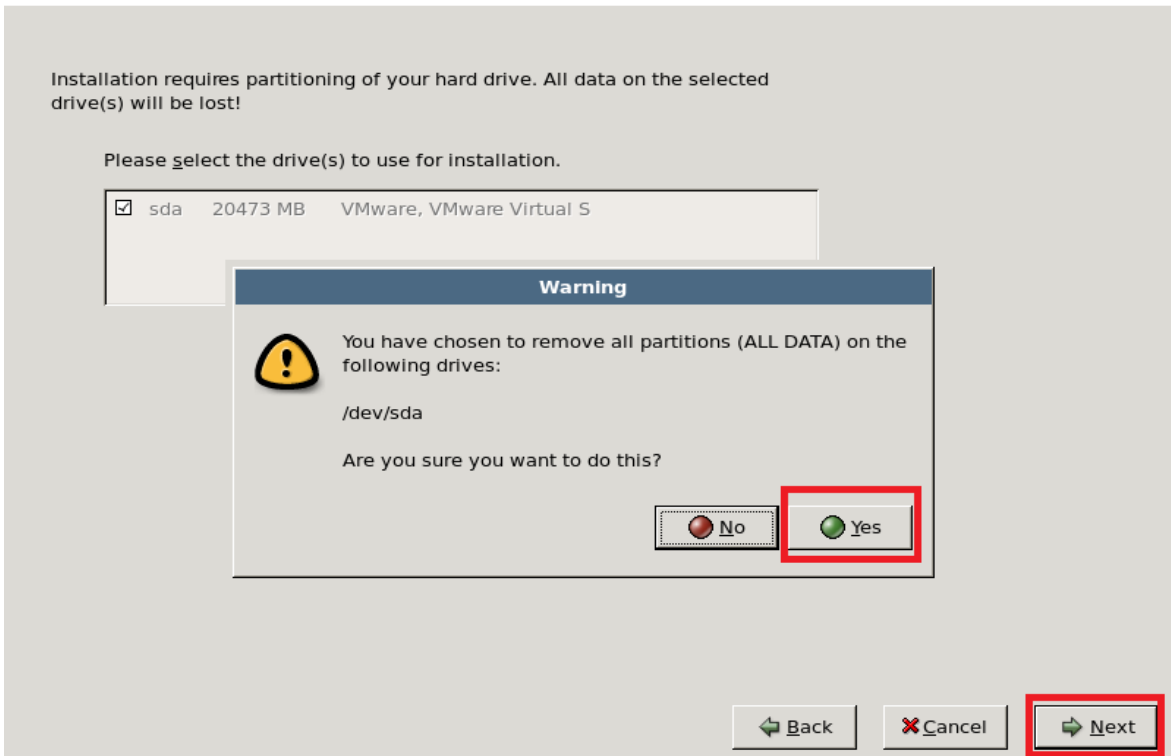


5. 安装系统检测的当前配置概要，点击 Next

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

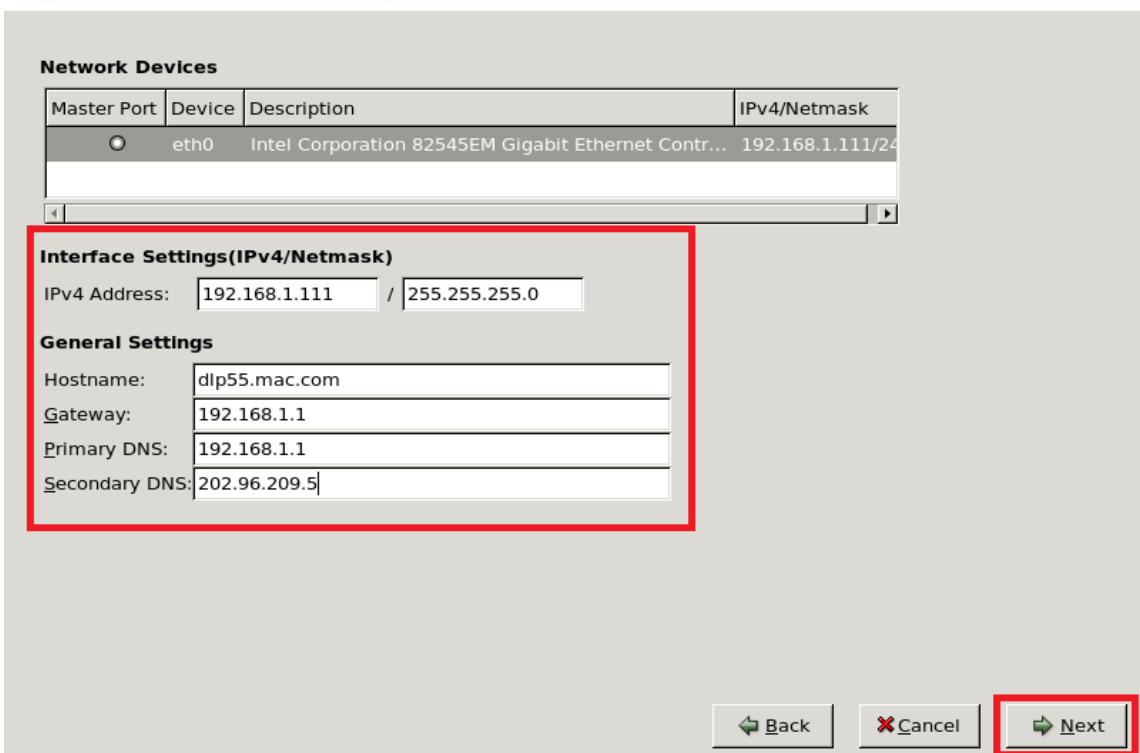


6. 提示是否全部擦除当前硬盘上的所有文件，点击 Next

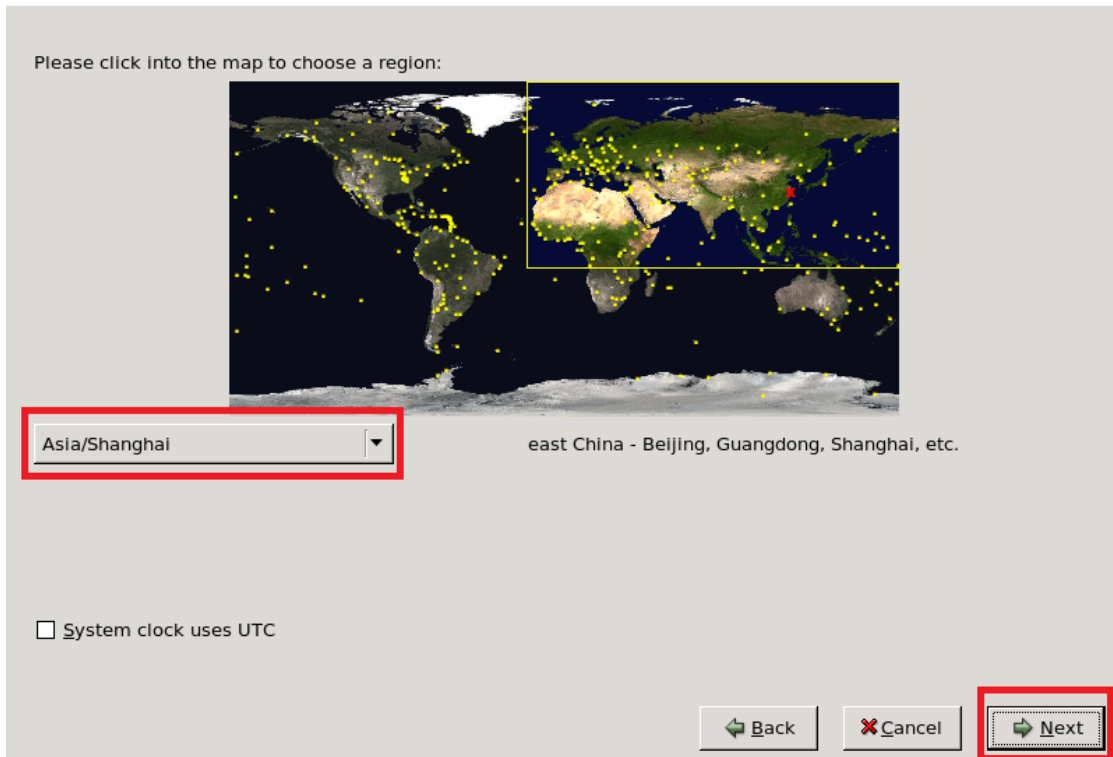
 **Data Loss Prevention**

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**

8. 选择当前所在地的时区，例如选择 Asia/Shanghai，点击 Next



9. 设定系统账号密码，设置完毕后，点击 Next

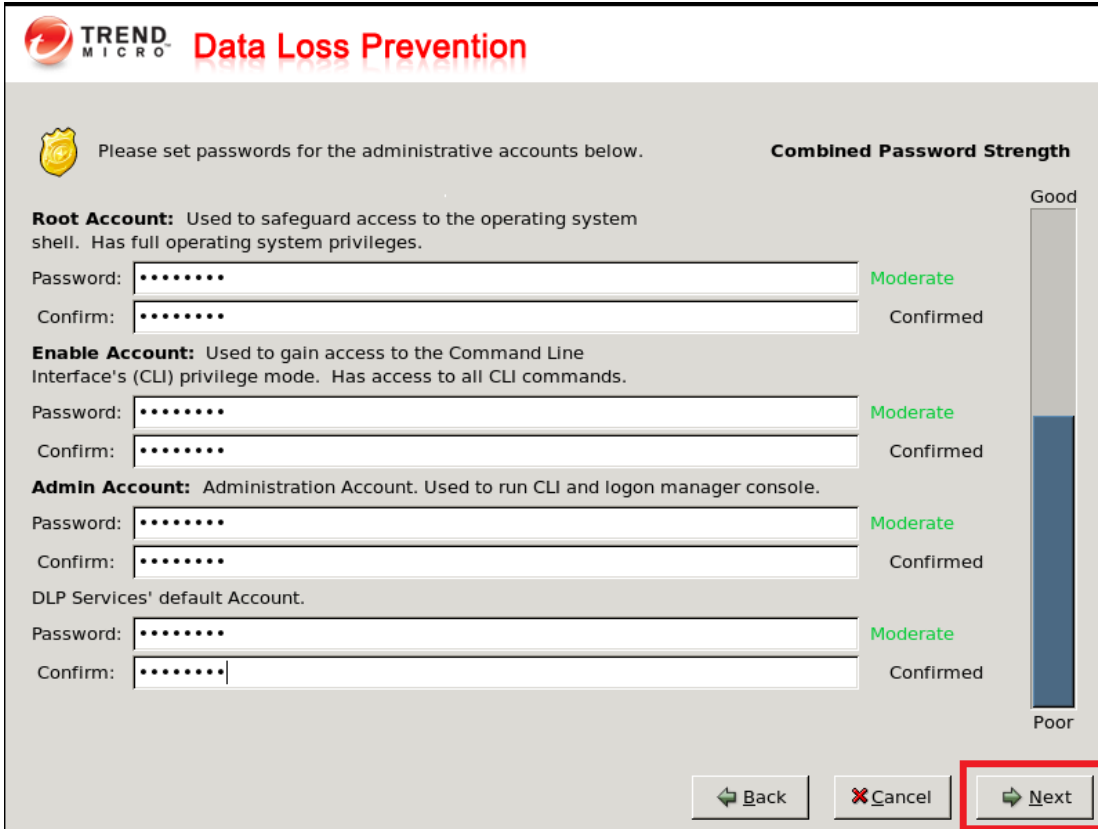
注意：Root Account：为安装完后 Linux 系统 Root 账号密码（Root 账号为最高权限）

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



TREND MICRO Data Loss Prevention

Please set passwords for the administrative accounts below. **Combined Password Strength**

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: [Moderate] Confirmed

Confirm: [Confirmed]

Enable Account: Used to gain access to the Command Line Interface's (CLI) privilege mode. Has access to all CLI commands.

Password: [Moderate] Confirmed

Confirm: [Confirmed]

Admin Account: Administration Account. Used to run CLI and logon manager console.

Password: [Moderate] Confirmed

Confirm: [Confirmed]

DLP Services' default Account.

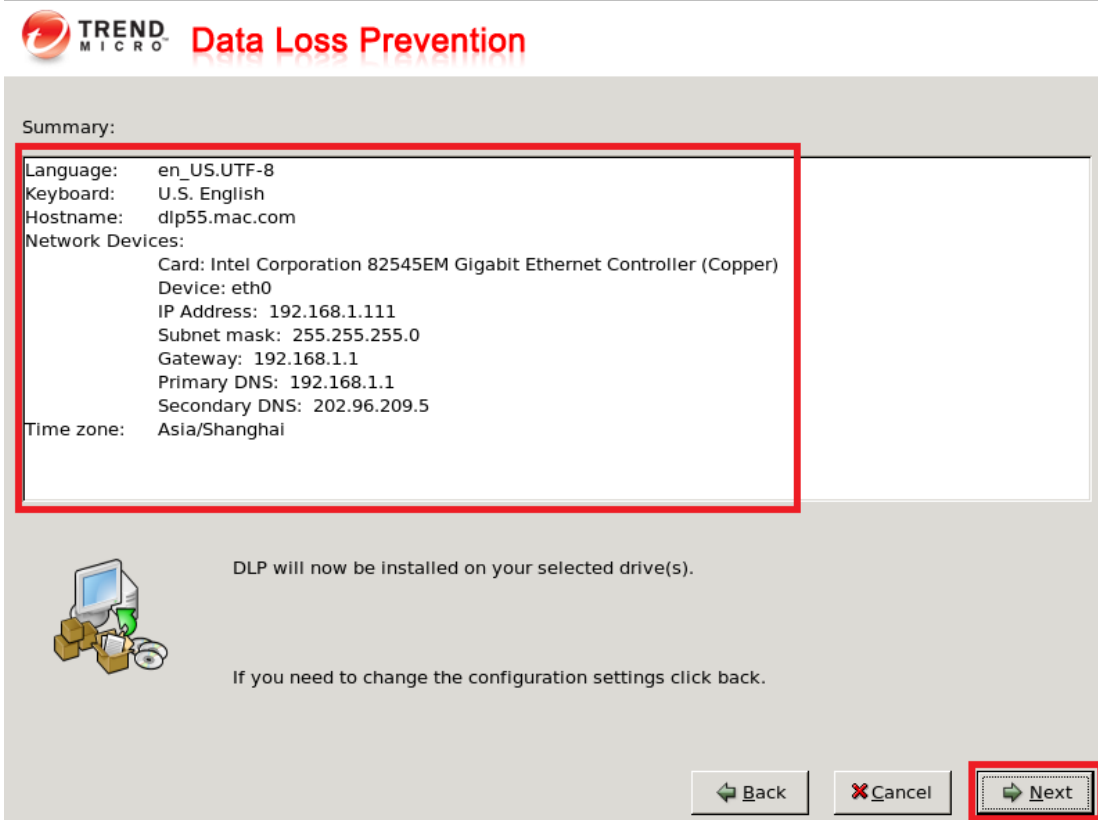
Password: [Moderate] Confirmed

Confirm: [Confirmed]

Good
Poor

Back Cancel Next

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



TREND MICRO Data Loss Prevention

Summary:

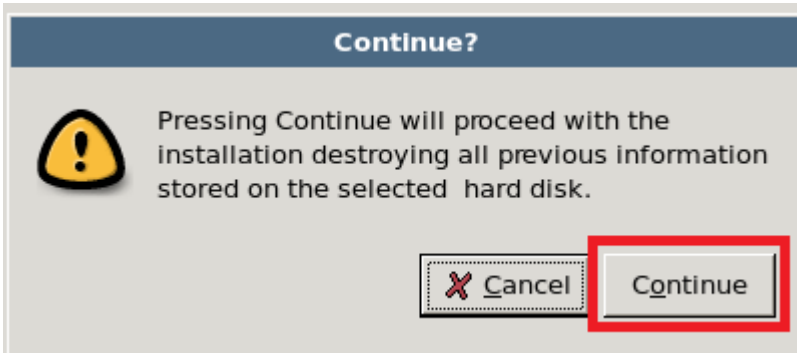
Language: en_US.UTF-8
Keyboard: U.S. English
Hostname: dlp55.mac.com
Network Devices:
Card: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
Device: eth0
IP Address: 192.168.1.111
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
Primary DNS: 192.168.1.1
Secondary DNS: 202.96.209.5
Time zone: Asia/Shanghai

DLP will now be installed on your selected drive(s).

If you need to change the configuration settings click back.

Back Cancel Next

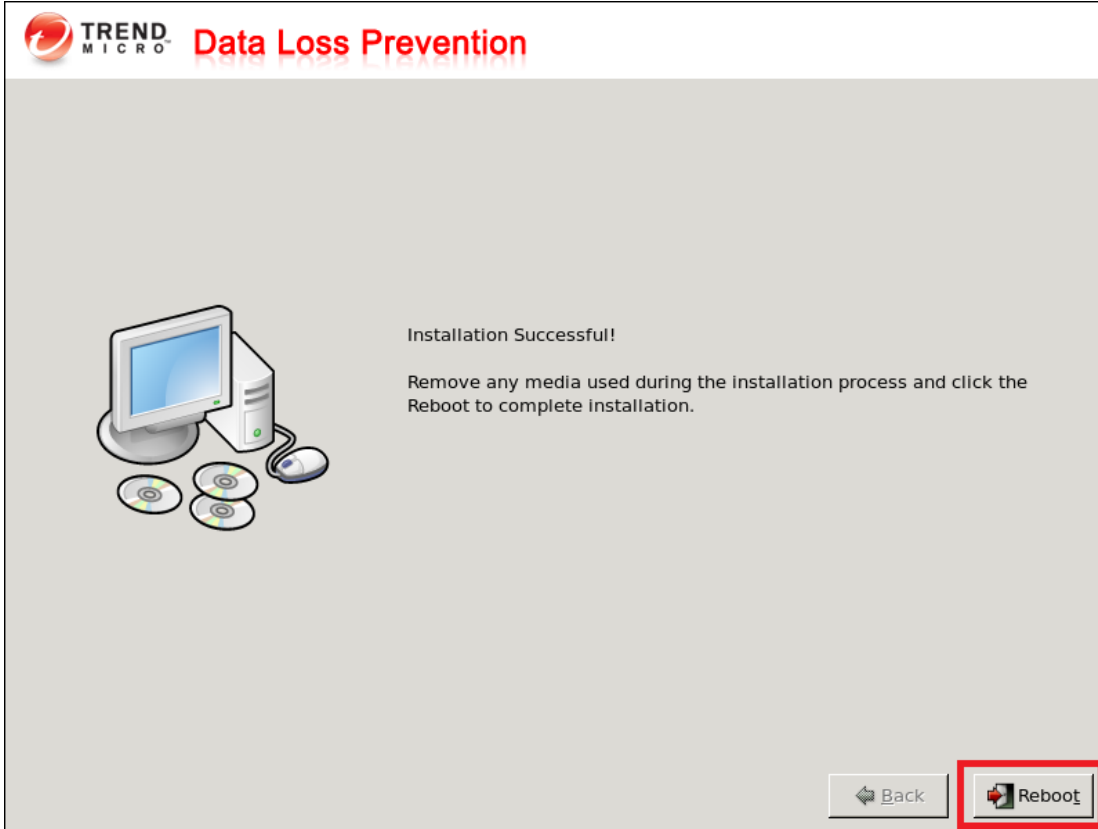
11. 安装前的最后确认，请点击 Next



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



13. 安装完毕后，提示需要重启，请点击 Reboot 按钮，以重启 DLP 系统



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）

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



Logon

Type your user name and password to access the web console.

User name:

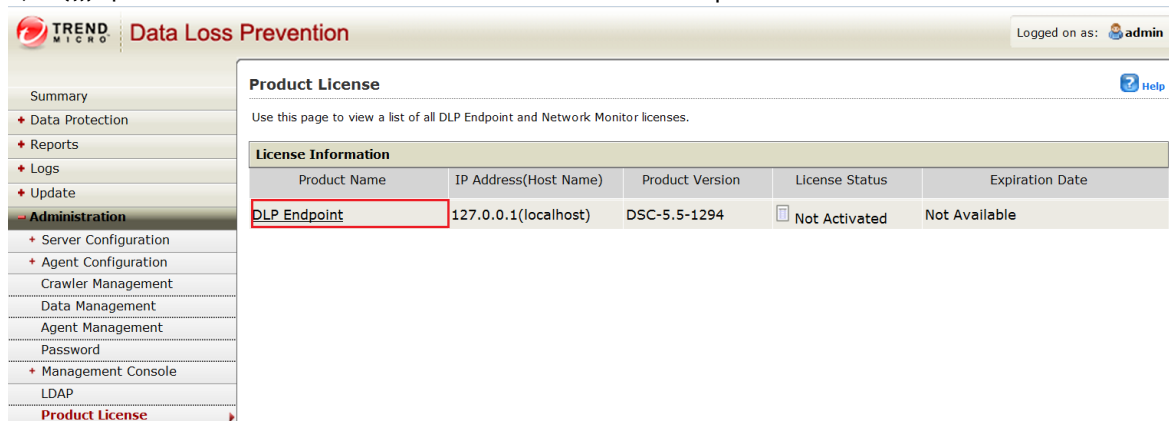
Password:

© 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 Administration---Product license---DLP Endpoint




Product License

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	<input type="checkbox"/> Not Activated	Not Available

Product License [Help](#)

Product License > License Details

 The product has not been activated.

[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 Prevention Endpoint		View detailed license online
Product:	Trend Micro™ Data Loss Prevention Endpoint (DSC-5.5-1294)	
Version:	Full	
Activation code:	██	Enter a new code
Seats:	████	
Status:	Activated	
Maintenance expiration:	Jan 6, 2011	
		<input type="button" value="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

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
[root@dlp55 ~]# clish
```

```
*****
*                               *
*      Trend Micro Data Loss Prevention (DLP)      *
*                               *
*                               *
*      WARNING: Authorized Access Only              *
*                               *
*****

Welcome to DLP UA 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

```

[root@dlp55 ~]# clish

*****
*                Trend Micro Data Loss Prevention (DLP)                *
*                                                                 *
*                WARNING: Authorized Access Only                       *
*                                                                 *
*****

Welcome to DLP UA 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       route          timezone
# configure DLP _
    
```

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

```

*****Configuration*****
* 1. System Configuration *
* 2. 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，在最后的确认信息后，按 y

```

The Network Configuration

The IP for eth0: [192.168.1.111]
The netmask for eth0: [255.255.255.0]
The gateway for eth0: []
The onboot for eth0: [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，在最后的确认信息后，按 y

```
Is the setting right (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 list:          192.168.1.1 202.96.209.5
  DNS search suffix:   mac.com
Is the setting right (type 'q' to quit from config)? (y/n/q): y
Network configuration has been done. press any key to continue...
```

验证完毕后，请按任意键进行 DLP 服务端安全配置, 很重要!



- 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): [192.168.1.111/255.255.255.0] ANY
The ports to listen agents: [8804 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, 在最后的的信息确认后, 按 y

```
The subnet/ip list from which you can access DLP Management(UI)(ip or subnet list/ANY): [192.168.1.111/255.255.255.0] ANY
The ports for manager: [8080 8443]

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, 在最后的的信息确认后, 按 y

```
The subnet/ip list from which sysadmin can remote logon to system(ip or subnet list/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_
```

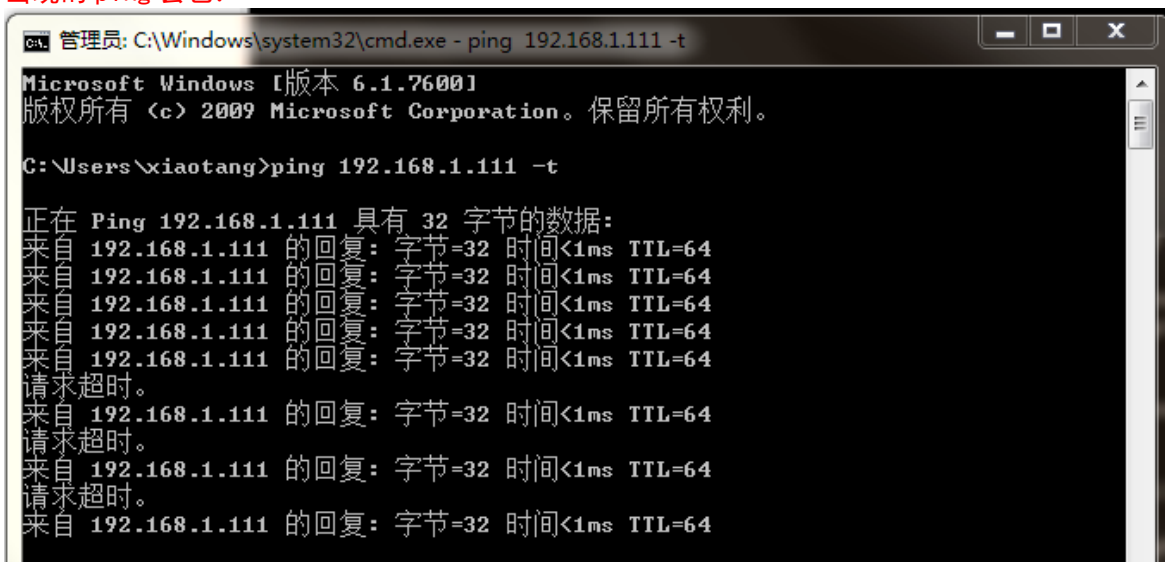
4. 更改默认防火墙配置, 允许 ping

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
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
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
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
```

如果需要修改, 我们可以做如下修改:

- 1) 进入 DLP 的 Linux 内核
- 2) vi /etc/sysconfig/iptables

```
[root@d1p55 ~]# 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《[客户端系统需求](#)》

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

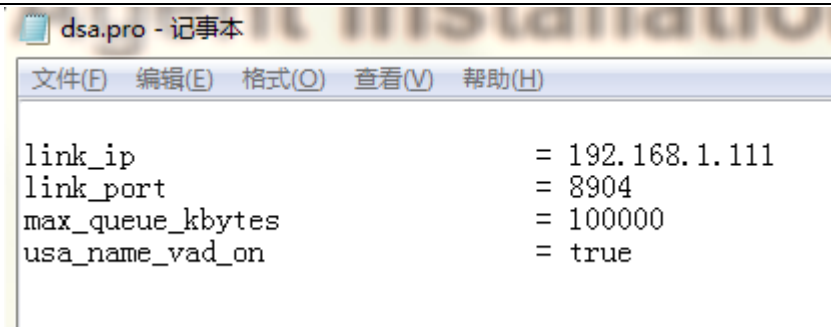
这里只介绍 dtool 工具本地安装

1. 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

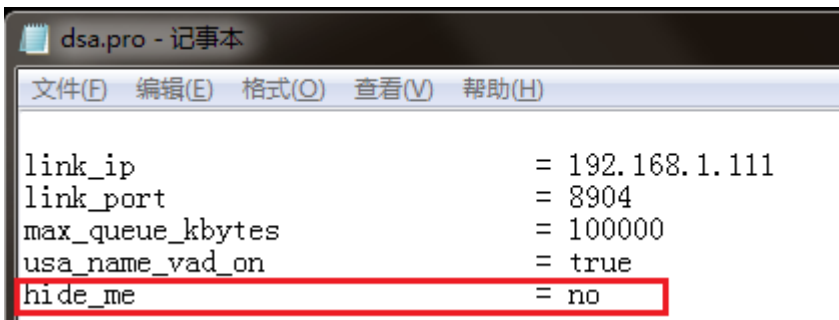


```
dsa.pro - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

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 = no

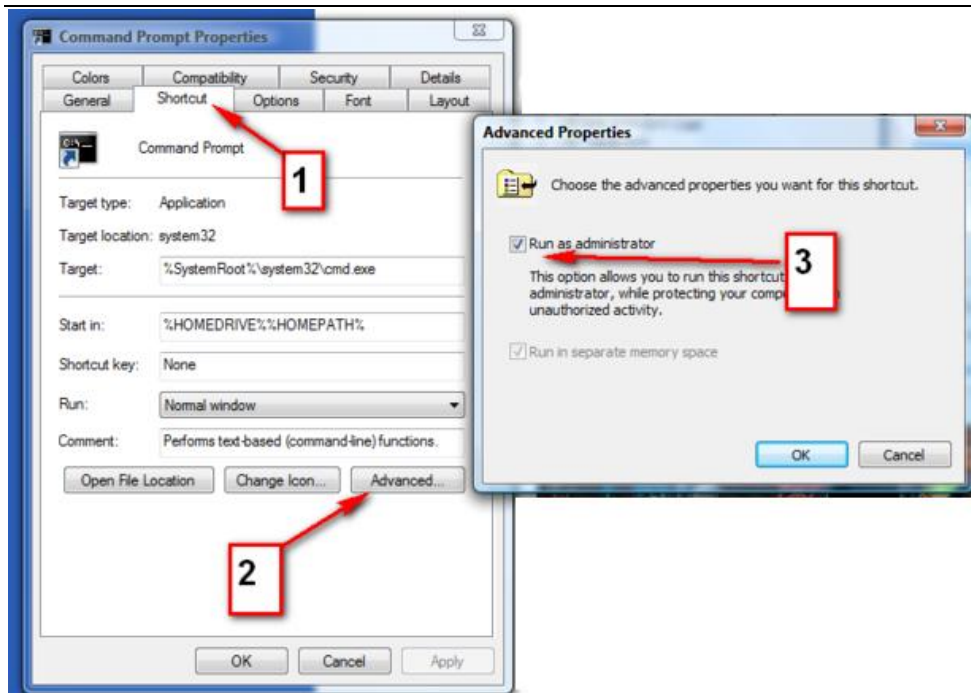


```
dsa.pro - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

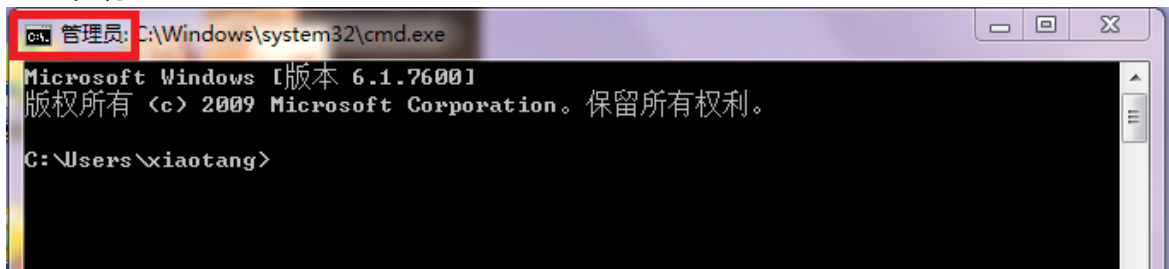
link_ip           = 192.168.1.111
link_port        = 8904
max_queue_kbytes = 100000
usa_name_vad_on  = true
hide_me          = no
```

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”。

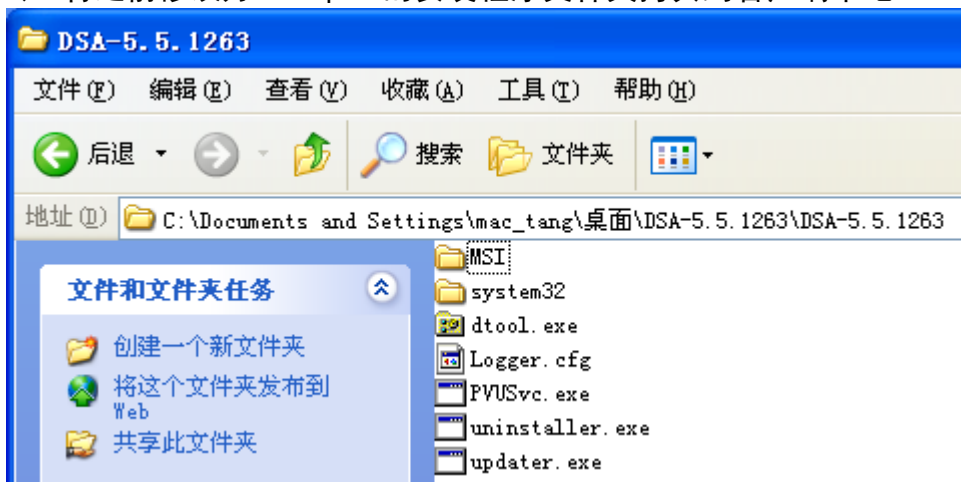


4. 检查是否“命令提示符”是否以管理员模式运行（只针对 Vista 及其以后的操作系统）



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。

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

常见使用方法:

```
dtool.exe -i          ---安装 DSA
dtool.exe -u          ---卸载 DSA
dtool.exe -i -sb      ---安装 DSA, 并支持安全模式下数据防泄密
dtool.exe -i -n       ---安装 DSA, 并暂时不重启操作系统
dtool.exe -i -s -d10 ---安装 DSA, 并 10 分钟后再重启操作系统
dtool.exe -l -p123    ---安装 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 -l -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

```
C:\Documents and Settings\mac_tang>"C:\Documents and Settings\mac_tang\桌面\DSA-
5.5.1263\DSA-5.5.1263\dtool.exe" -i -sb
Info: reboot machine localhost success!
Info: install <localhost> success.
C:\Documents and Settings\mac_tang>_
```



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 TMDLPM 2.0（可选）

注意：Trendmicro Data Loss Prevention Network Monitor (TMDLPM) 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 TMDLPM2.0 的安装程序，并刻录成 DVD 光盘

注意：目前 TMDLPM2.0 版本为 DLPMN-2.0-1135

2) 检查 TMDLPM2.0 客户端的硬件和系统配置要求。

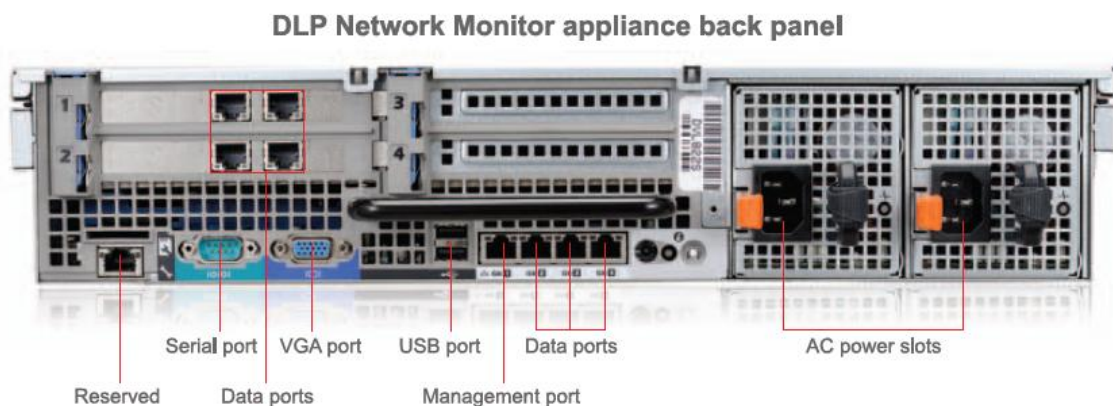
注意：参见《[TMDLPM 系统需求](#)》

3) TMDLPM 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：TMDLPM 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 TMDLPM 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 TMDLPM 的管理口。



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 TMDLPM 注册到 DLP 服务端上

注意：TMDLPM 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 TMDLPM 的 linux 内核
输入 clish

```
tmdlpmn login: root
Password:
[root@tmdlpmn ~]# clish

*****
*      Trend Micro Data Loss Prevention Network Monitor 2.0      *
*                                                                *
*      WARNING: Authorized Access Only                          *
*                                                                *
*****

Welcome to DLPNM CLI. it is Sun Dec 26 15:35:23 CST 2010
> _
```

输入 enable 进入特权模式

```
> enable
Entering privileged mode...
# _
```

输入 configure dglink IP

注意：此处的 IP 地址为 DLP 服务端的 IP 地址

```
# configure
dglink      dns      gateway      hostname      interface
max_file_size password
# configure dglink ^
ip IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
# configure dglink 192.168.1.111_
```

注册成功时，命令行中的显示：

```
Ok to create fpga pattern : /tmp/fpga.tcp.ptn.raw
Ok 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

Agent Management

Agent Management allows the user to browse and edit agents or groups.

Agents	IP Address	Status	Policy Status	Fingerprints	Agent	Last Modified
MAC-COMPUTER	192.168.1.5	Disconnected	N/A	0	5.5.1263	12/26/10 3:10:34 ...
tmdlpm.mac.com	192.168.1.104	Online	N/A	0	2.0.1135	12/26/10 3:40:50 ..

2. 输入激活码，激活 TMDLPM

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.

Product Name	IP Address(Host)	Product Version	License Status	Expiration Date
DLP Endpoint	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 > License Details

The product has not been activated. View renewal instructions

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

激活以后显示的状态

Product License

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

Product Name	IP Address(Host)	Product Version	License Status	Expiration Date
DLP Endpoint	127.0.0.1(localhost)	DSC-5.5-1294	Activated	██████████
DLP Network Monitor	172.16.4.242(TMDLP...)	2.0.1135	Activated	██████████

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 TMDLPM 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


```
> enable
Entering privileged mode...
# _
```

输入 `configure max_file_size 3000000` （单位为 字节）

3.4 如何检查标准安装是否成功

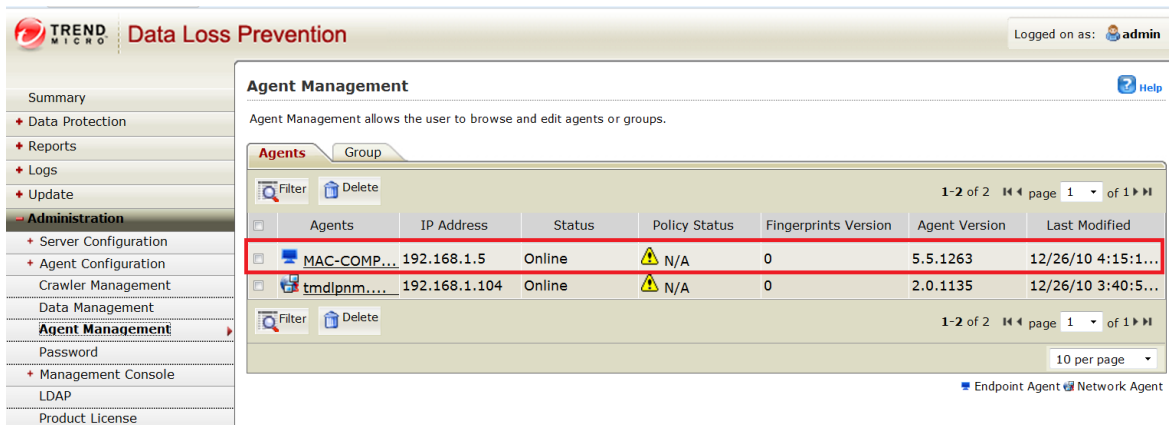
3.4.1 DLP 5.5 服务端

- 1、检查是否可以打开控制台
打开方式：<http://ip:8443/dsc>
- 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 MICRO Data Loss Prevention Logged on as: admin

Agent Management Help

Agent Management allows the user to browse and edit agents or groups.

Agents Group

Agents	IP Address	Status	Policy Status	Fingerprints Version	Agent Version	Last Modified
<input type="checkbox"/> MAC-COMP...	192.168.1.5	Online	N/A	0	5.5.1263	12/26/10 4:15:1...
<input type="checkbox"/> tmdlpm...	192.168.1.104	Online	N/A	0	2.0.1135	12/26/10 3:40:5...

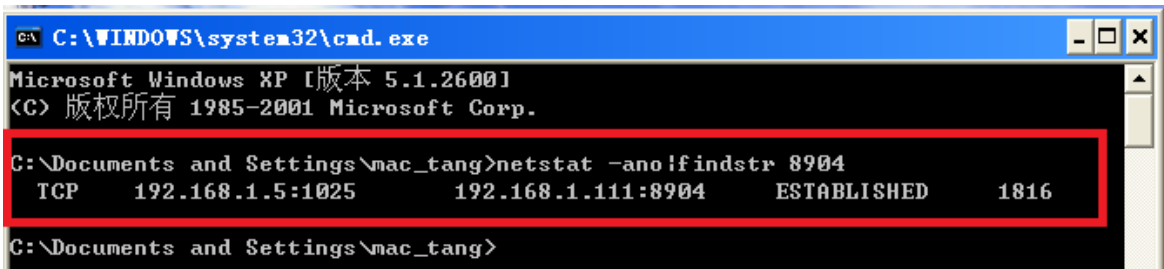
10 per page

Endpoint Agent Network Agent

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

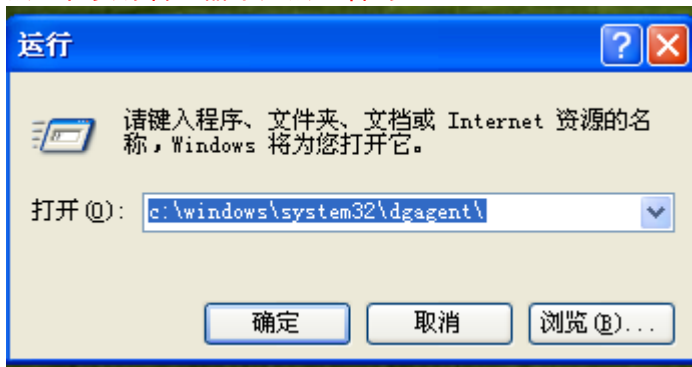


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\nac_tang>netstat -ano|findstr 8904
TCP        192.168.1.5:1025          192.168.1.111:8904      ESTABLISHED        1816
C:\Documents and Settings\nac_tang>
```

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。



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。



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 Prevention
Logged on as: **admin**

- Summary
- + Data Protection
- + Reports
- + Logs
- + Update
- Administration**
- + Server Configuration
- + Agent Configuration
- Crawler Management
- Data Management
- Agent Management**
- Password
- + Management Console
- LDAP
- Product License

Agent Management
Help

Agent Management allows the user to browse and edit agents or groups.

Agents
Group

Filter
Delete
1-2 of 2
page 1 of 1

	Agents	IP Address	Status	Policy Status	Fingerprints Version	Agent Version	Last Modified
<input type="checkbox"/>	MAC-COMP...	192.168.1.5	Online	⚠ N/A	0	5.5.1263	12/26/10 4:15:1...
<input type="checkbox"/>	tmdlpnm...	192.168.1.104	Online	⚠ N/A	0	2.0.1135	12/26/10 4:52:3...

Filter
Delete
1-2 of 2
page 1 of 1

10 per page

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`

```

Sun Dec 26 16:55:53 CST 2010
[STATISTICS]
syn_contrack:           1 (      184)
conntrack_count:       1 (      154)
nr_pkscan_tx:          0 (     1125)
nr_btscan_tx:          0 (       202)
nr_fpga_err:           (         0)
nr_btscan_err:         (         0)
free_lowmem:           648M ( 200M/1011M)
nr_packet_bytes:       464 [  OM] -\
nr_pk_bytes:           0 [  OM] |
nr_bt_bytes:           0 [  OM] |
nr_tr_bytes:           0 [  OM] +- ( 550M)
nr_pages:              0 [  OM] --- (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          14260
nr_not_a_syn:          7              7
nr_corrupt:            31              1
nr_redirect:           0              0
overloading:           0  0 (1:0 fs: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)

```

- 36 -

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。

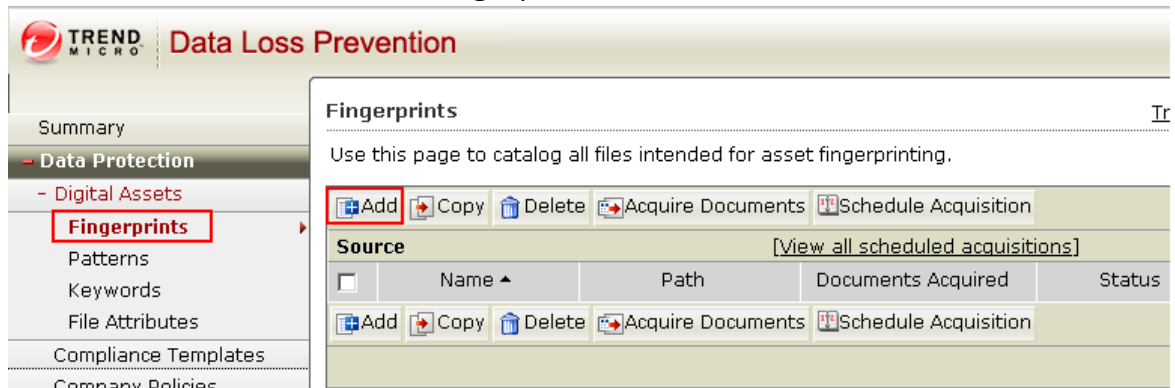
注意：如未操作进参考之前章节进行操作

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



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

Fingerprints > Adding Fingerprints

Source

Name:*

Description:

Repository Type:

Host:*
Example: server1.example.org or 123.123.123.123

Path:* Include sub-directories
Example: /documents/sensitive files

User ID:

Password:

Source connection test 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

Crawler Management Help

Crawler Management allows you to scan for confidential data stored on desktops and laptops whether users are connected or not connected to the company's network. Use this page to manage or deploy the Remote Crawler agent.

Filter Delete **Download Remote Crawler** 1-1 of 1 page 1 of 1

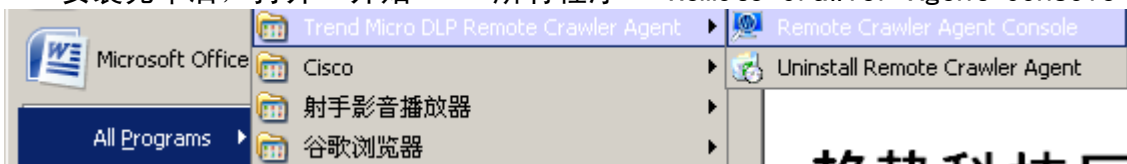
<input type="checkbox"/>	Host	IP Address	Status	Crawler Version	Last Modified
<input type="checkbox"/>	mac	172.16.4.230	Connected	5.5.1069	12/29/10 2:45:33 PM CST

Filter Delete Download Remote Crawler 1-1 of 1 page 1 of 1

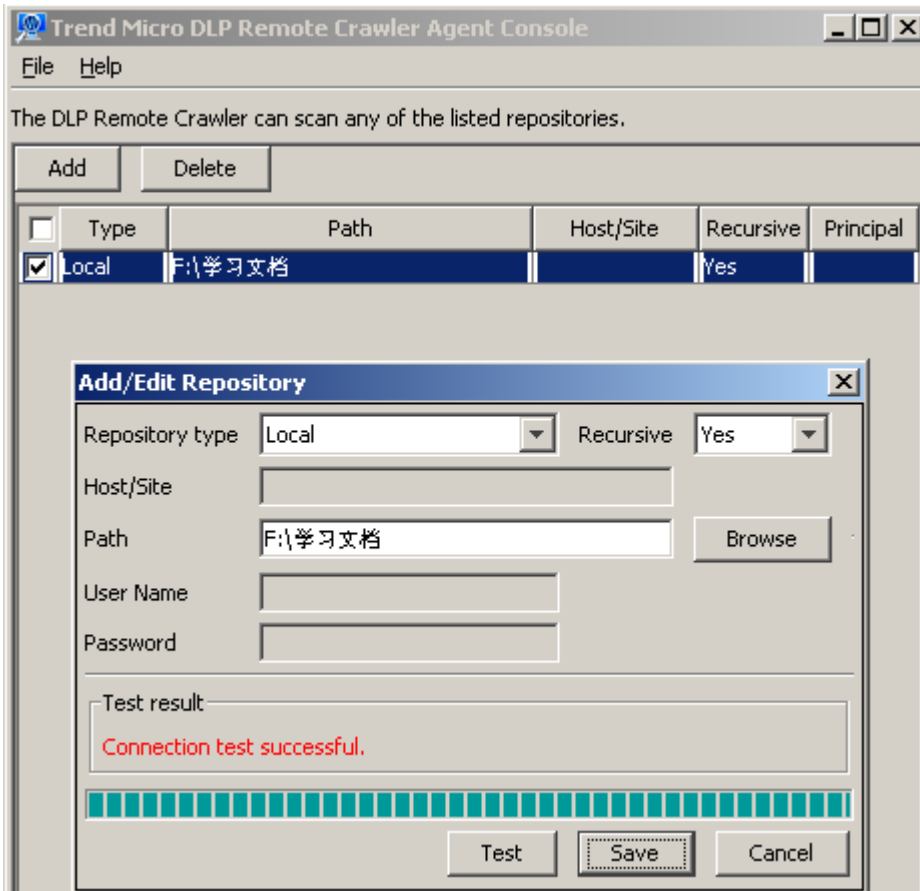
200 per page

✓ 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---Remote Crawler Agent Console



- ✓ 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。



- ✓ 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

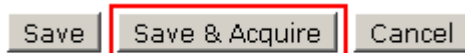
Fingerprints

[Help](#)

Fingerprints > Adding Fingerprints

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。

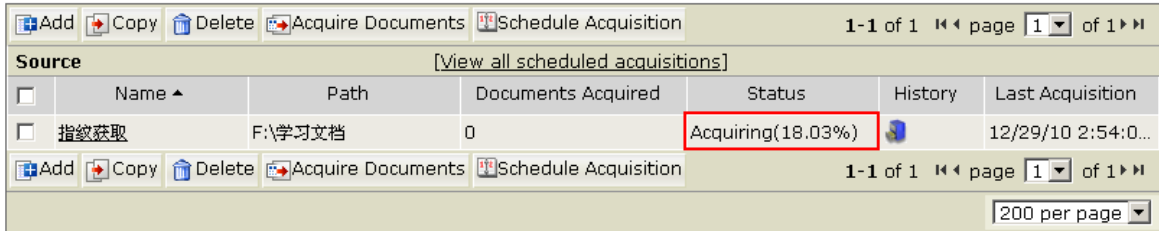



Acquire 的过程可以查看 Status 页面。

Fingerprints

Trend Micro™ DLP Workflow [Help](#)

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



Name	Path	Documents Acquired	Status	History	Last Acquisition
指纹获取	F:\学习文档	0	Acquiring(18.03%)		12/29/10 2:54:0...

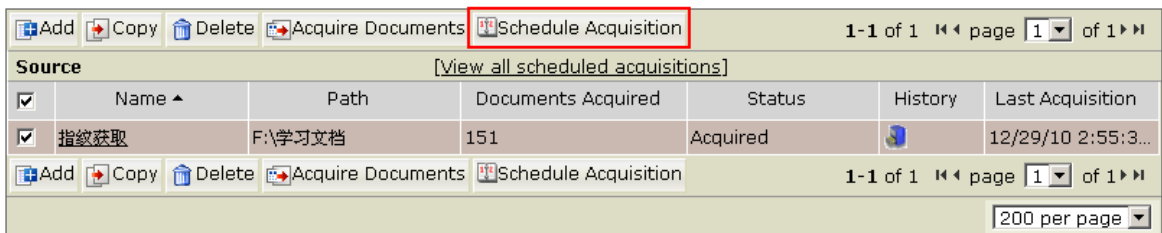
注意：Acquire 的时间取决于服务器的性能和文件的数量。建议如在测试过程中，当 DLP 服务端运行在 Vmware 平台上，请选择少量数据进行获取。


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

Fingerprints

Trend Micro™ DLP Workflow [Help](#)

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



Name	Path	Documents Acquired	Status	History	Last Acquisition
指纹获取	F:\学习文档	151	Acquired		12/29/10 2:55:3...

进行预设 Acquire 的设置。

Scheduling SensitiveDocAcquisitionJobType

[Help](#)

Scheduling Jobs for [指纹获取].

Schedule

One-time
 Daily
 Weekly
 Monthly

Date: 12-29-2010
mm-dd-yyyy

Time: 16:00
hh mm

Acquire fingerprints for all locations defined in the Remote Crawler side

Select all file locations

F:\学习文档 (includes sub-directories)

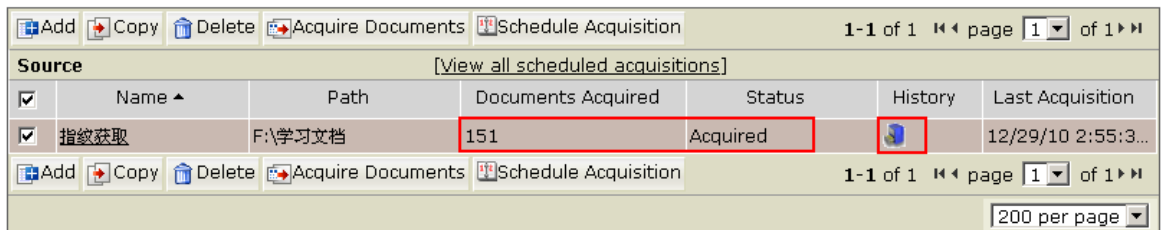
Save Cancel


6) Acquire 获取完毕后，Status 会显示 Acquired

Fingerprints

Trend Micro™ DLP Workflow [Help](#)

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



Name	Path	Documents Acquired	Status	History	Last Acquisition
指纹获取	F:\学习文档	151	Acquired		12/29/10 2:55:3...

7) 点击 History, 可以查看此次 Acquire 的显示具体信息

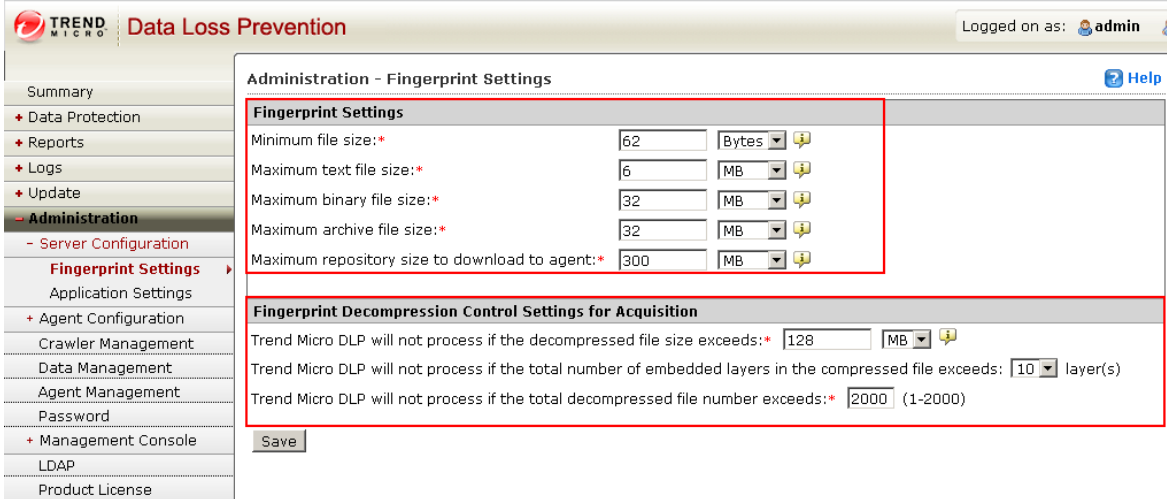
注意：如出现下图所示信息，则检查此文件是否过小，或者过大。

Acquisition Detail

2010-12-29 14:55:39 - F:\学习文档\Favorites\cnBeta.COM_网友媒体与言论平台.url: Empty fingerprints will be extracted from 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

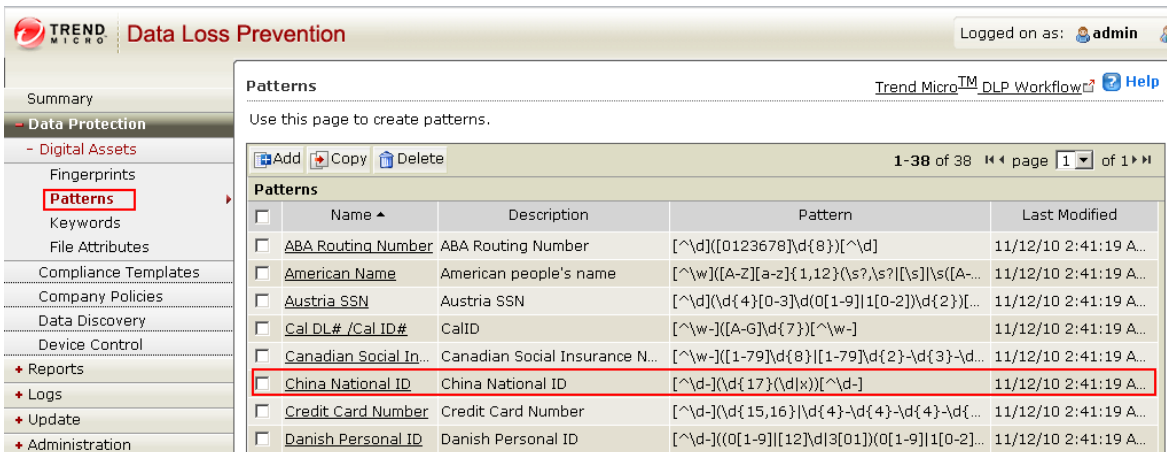
注意：趋势科技不建议进行修改，DLP Acquire 过大的文件将会影响性能。



(二) Pattern 设定

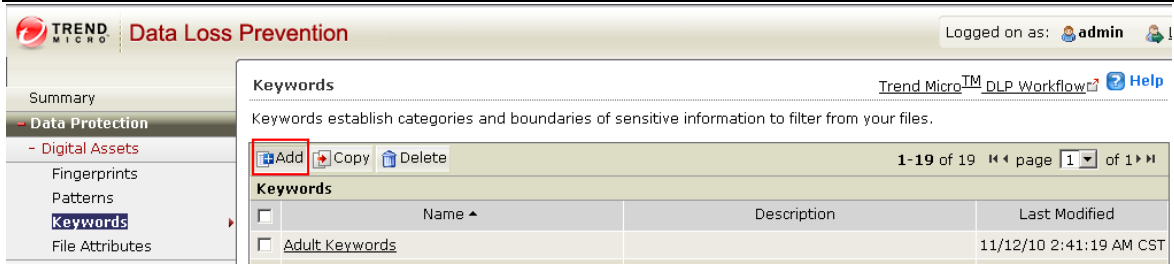
Pattern 设定是基于正则表达式完成。使 DLP 可以检测一些诸如身份证 ID，银行卡号、家庭住址、电话号码等敏感信息外泄。默认已经设定一些条目，但大部分是参照国外使用方式进行设定，一般建议不使用此功能。

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



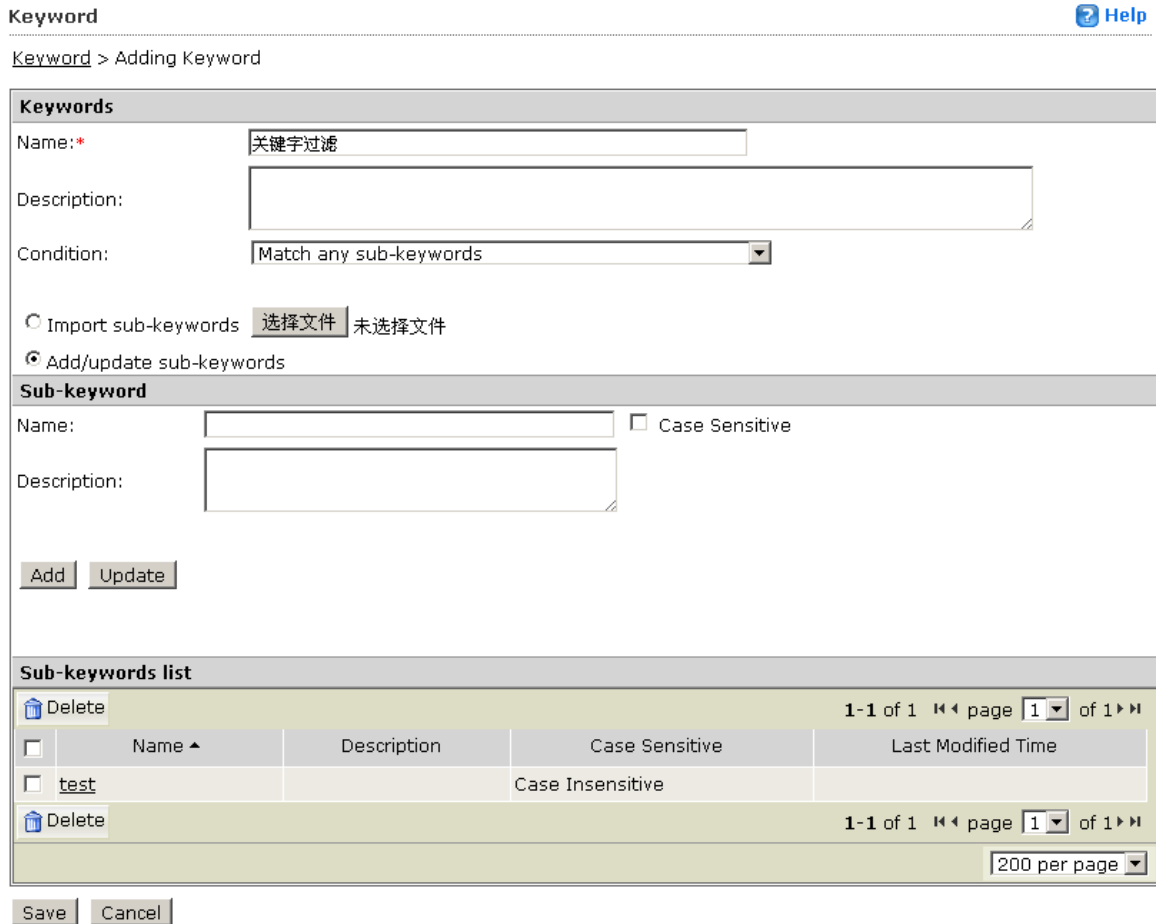
(三) 关键字设定

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



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

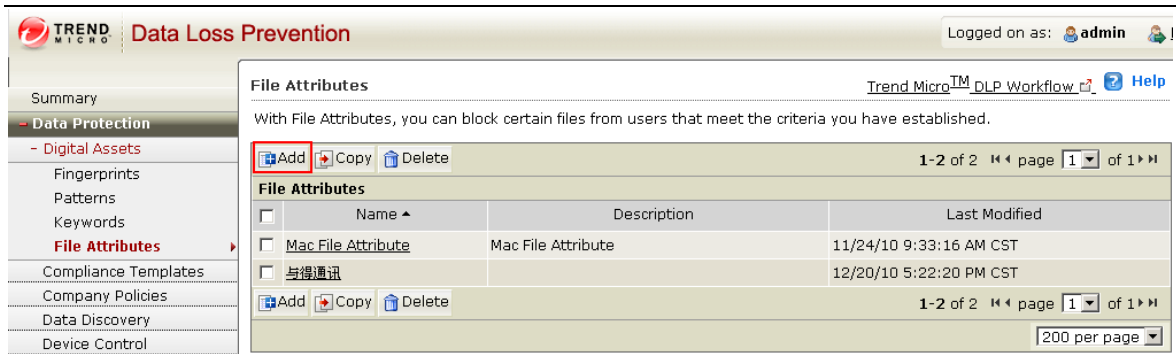


(四) 文件属性设定

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 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



Data Loss Prevention | Logged on as: admin

File Attributes | Trend Micro™ DLP Workflow | Help

With File Attributes, you can block certain files from users that meet the criteria you have established.

1-2 of 2 page 1 of 1

Name	Description	Last Modified
Mac File Attribute	Mac File Attribute	11/24/10 9:33:16 AM CST
与得通讯		12/20/10 5:22:20 PM CST

200 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

File Attributes > Adding File Attributes

File Attribute Information	
Name:*	<input type="text" value="Mac 文件类型"/>
Description:	<input type="text"/>
File Attributes	
<input checked="" type="checkbox"/> File type:	<input type="text" value="[Edit]"/>
<input type="checkbox"/> File size:	From <input type="text"/> Bytes To <input type="text"/> 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:

- Executable ▾
- Document ▾
- Image Document ▾
- Graphic Document ▾
- Multimedia ▾
- Encapsulation Format ▾
- 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

Data Protection

- Digital Assets

Fingerprints

Patterns

Keywords

File Attributes

Compliance Templates

Company Policies

Data Discovery

Device Control

+ Reports

+ Logs

+ Update

+ Administration

Trend Micro™ DLP Workflow [Help](#)

Keywords establish categories and boundaries of sensitive information to filter from your files.

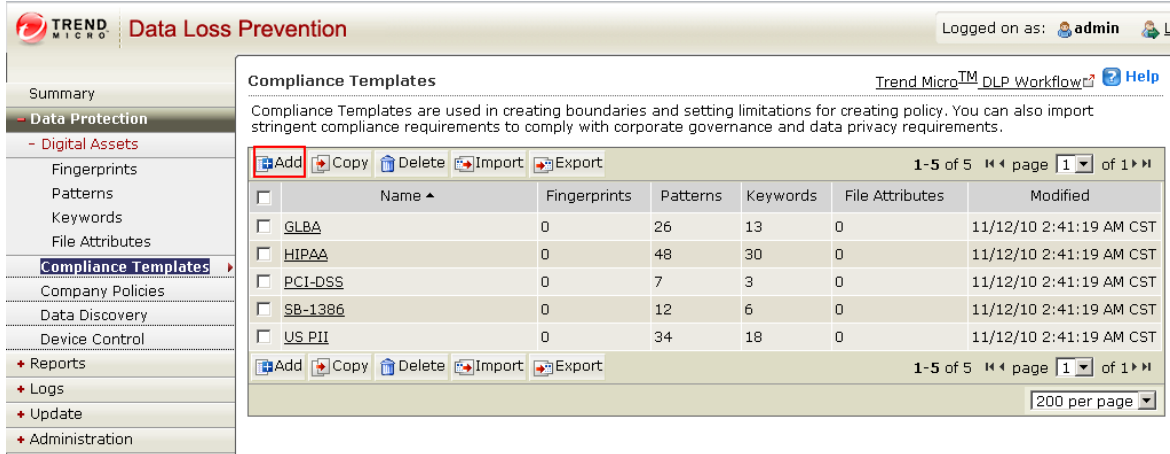
1-19 of 19 page 1 of 1

	Name ▲	Description	Last Modified
<input type="checkbox"/>	Adult Keywords		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	American-Name-Keyword1		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	American-Name-Keyword2		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	C and C++ Source Code		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	C# Source Code		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	COBOL-Source-Code		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	Common Medical Terms		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	HCFA (CMS) 1500 Form		11/12/10 2:41:19 AM CST
<input type="checkbox"/>	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



2. 设定方式如下:

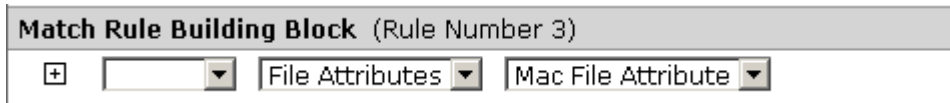
- ✓ Name: 输入模板名称
- ✓ 如需添加之前获取的指纹, 选择 Fingerprints, 并选择 High-Level Match



如需添加之前设定的关键字, 选择 Keywords



如需添加之前设定的 File Attributes, 选择 File Attributes



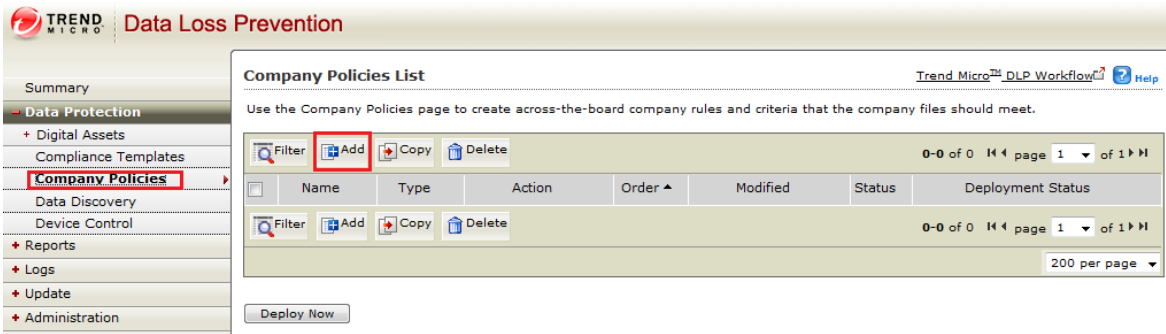
- ✓ 可以同时添加多个, 也可以单独创建模板。

注意: 请区分 OR 与 And 以及 Except 的区别

Match Rules		
1	<input type="checkbox"/>	指纹获取 (High-level Match)
2	Or	Mac Keyword
3	Or	Mac File Attribute

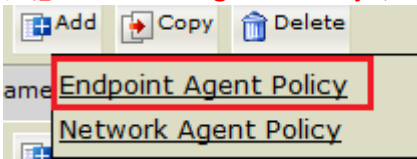
(二) 建立策略及部署

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



2. 点击 Add 后，选择 Endpoint Agent Policy

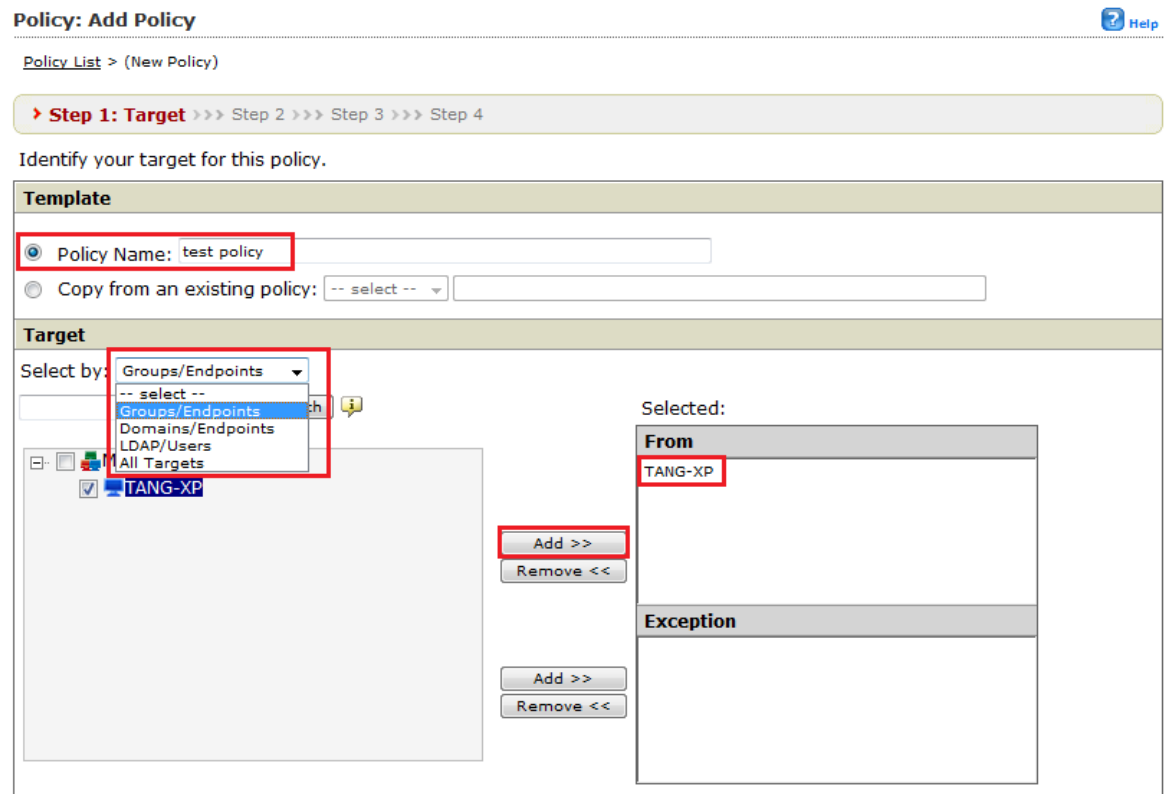
注意：Network Agent Policy 是针对 TMDLPMN 产品，此处选择 Endpoint Agent Policy



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

小贴士：有 4 种方式选择客户端，分别是：

- 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 Workgroup）
- LDAP/Users -----基于 LDAP 中用户信息的客户端
- All Targets -----所有客户端



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
<input checked="" type="checkbox"/> ActiveSync filter
<input checked="" type="checkbox"/> CD/DVD
<input checked="" type="checkbox"/> Clipboard
<input checked="" type="checkbox"/> Email
<input checked="" type="checkbox"/> Removable Storage (FileWrite)
<input checked="" type="checkbox"/> FTP
<input checked="" type="checkbox"/> HTTP
<input checked="" type="checkbox"/> HTTPS
<input checked="" type="checkbox"/> Instant Messengers
<input checked="" type="checkbox"/> P2P
<input checked="" type="checkbox"/> PGP Encryption
<input checked="" type="checkbox"/> Printer
<input checked="" type="checkbox"/> SMB
<input checked="" type="checkbox"/> 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 (OU 信息) : /O=Trend/OU=USA, /O=Trend/OU=CHINA (逗号分隔)

Email

Exchange Client Email
Lotus Notes Email
SMTP Email

Approved domain names

Separate multiple domain names with a comma. (Example: /O=Trend/OU=USA,/O=Trend/OU=CHINA)

Blocked domain names

Separate multiple domain names with a comma. (Example: /O=Trend/OU=USA,/O=Trend/OU=CHINA)

b) USB 存储设备例外

输入格式: vendor Name 1-model-Serial ID

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

TREND MICRO Data Loss Prevention

Summary

Data Protection

+ Digital Assets

Compliance Templates

Company Policies

Data Discovery

Device Control

+ Reports

+ Logs

+ Update

+ Administration

Device Control Help

Device control allows you to limit specific user access to specific devices and network shared folders.

Endpoints **Groups**

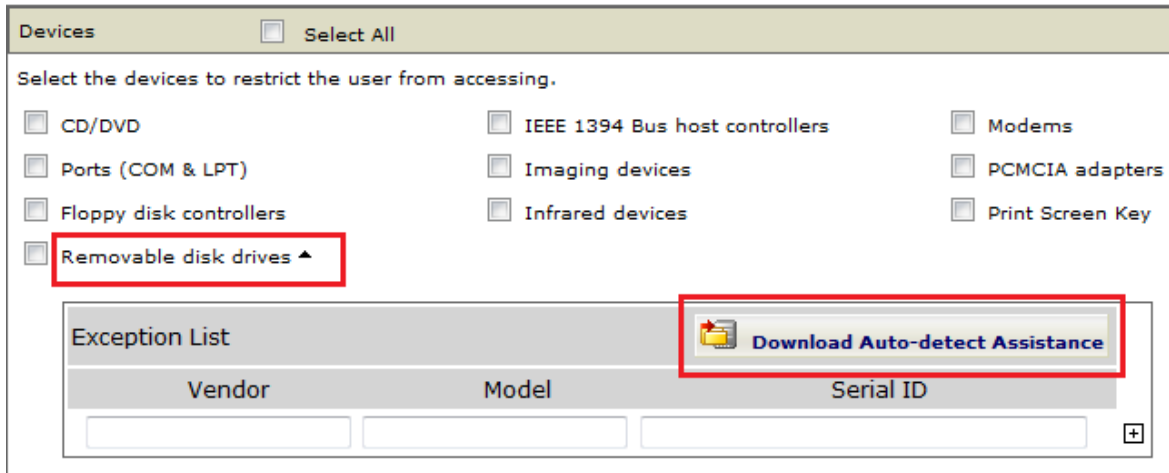
Filter 1-3 of 3 page 1 of 1

Endpoints	IP Address	Disabled Devices	Domain	Last Modified
JASON_ZHOU-PC	10.28.132.63		WORKGROUP	
MAC-XP	10.28.132.21		WORKGROUP	
TANG-XP	10.28.132.19		WORKGROUP	

Filter 1-3 of 3 page 1 of 1

200 per page

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

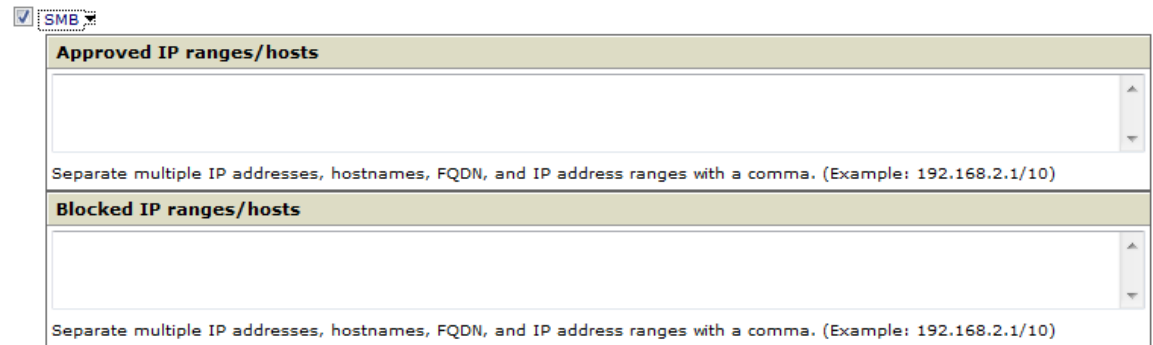


下载完毕后在插上需要允许使用 U 盘电脑上运行, 会自动弹出一个网页, 将以下信息记录, 例如: 可移动磁盘 (仅限于 闪存盘/U盘):

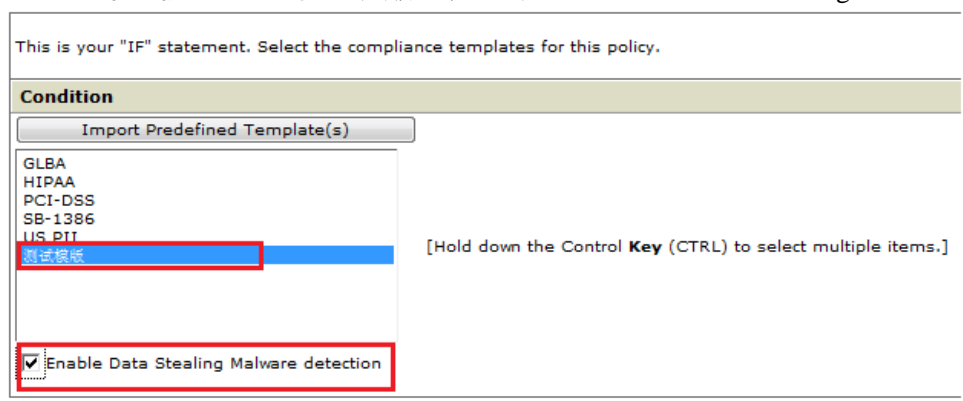
计算机	用户	端口	描述	供应商	型号	序号
XIAOTANG-PC	xiaotang-PC\xiaotang	USB	SanDisk Cruzer Color+ USB Device	SANDISK	5170	08775018AF42845D

c) SMB 协议共享

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



5. 选择之前配置的策略模版, 并建议勾选 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	
Online Agents <ul style="list-style-type: none"> <input checked="" type="radio"/> Local Area Network (recommended) <input type="radio"/> Local Machine (strict filtering) 	Offline Agents <ul style="list-style-type: none"> <input type="radio"/> Local Area Network <input checked="" type="radio"/> Local Machine (recommended)
System Action When Online	
Restrictions: <ul style="list-style-type: none"> <input type="radio"/> Pass <input checked="" type="radio"/> Block 	Actions to take: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Log <input checked="" type="checkbox"/> Client side alerting Customizable message URL: 很抱歉，您违反了公司的安全策略！ <input checked="" type="checkbox"/> Server side alerting <input type="checkbox"/> Forensic data capturing <input type="checkbox"/> Prompt user to enter justification when blocked <input type="checkbox"/> Encrypt (USB devices only) <input type="checkbox"/> Prompt user to enter justification
System Action When Offline <input checked="" type="checkbox"/> Same as Online Action	
Restrictions: <ul style="list-style-type: none"> <input type="radio"/> Pass <input checked="" type="radio"/> Block 	Actions to take: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Log <input checked="" type="checkbox"/> Client side alerting Customizable message URL: 很抱歉，您违反了公司的安全策略！ <input checked="" type="checkbox"/> Server side alerting <input type="checkbox"/> Forensic data capturing <input type="checkbox"/> Prompt user to enter justification when blocked <input type="checkbox"/> Encrypt (USB devices only) <input type="checkbox"/> 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

Offline 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: 10.0.0.0~10.255.255.255

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) **Encrypt** 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。

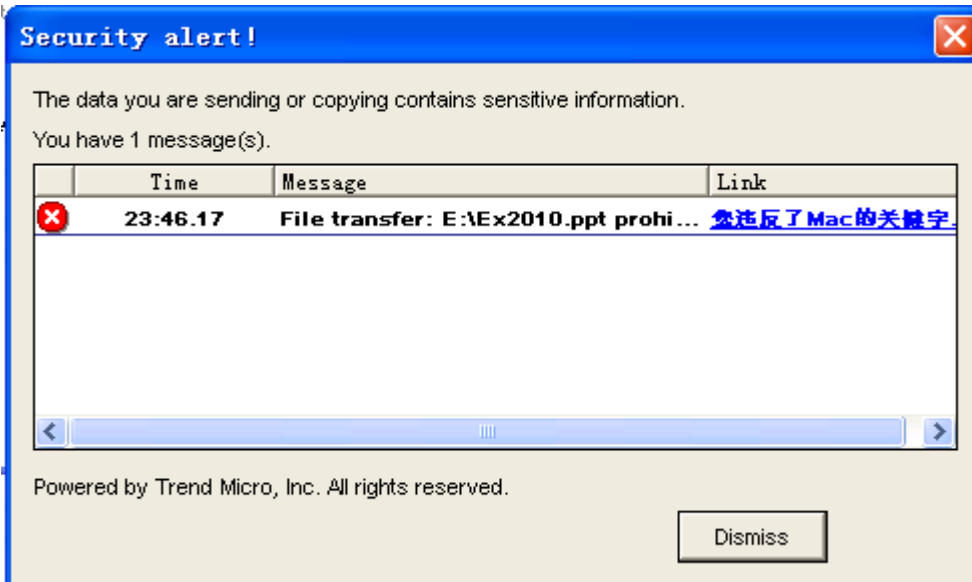
已部署将显示: Policies have been deployed

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 1 分钟后再次显示



9. 客户端验证

在确保客户端 online 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



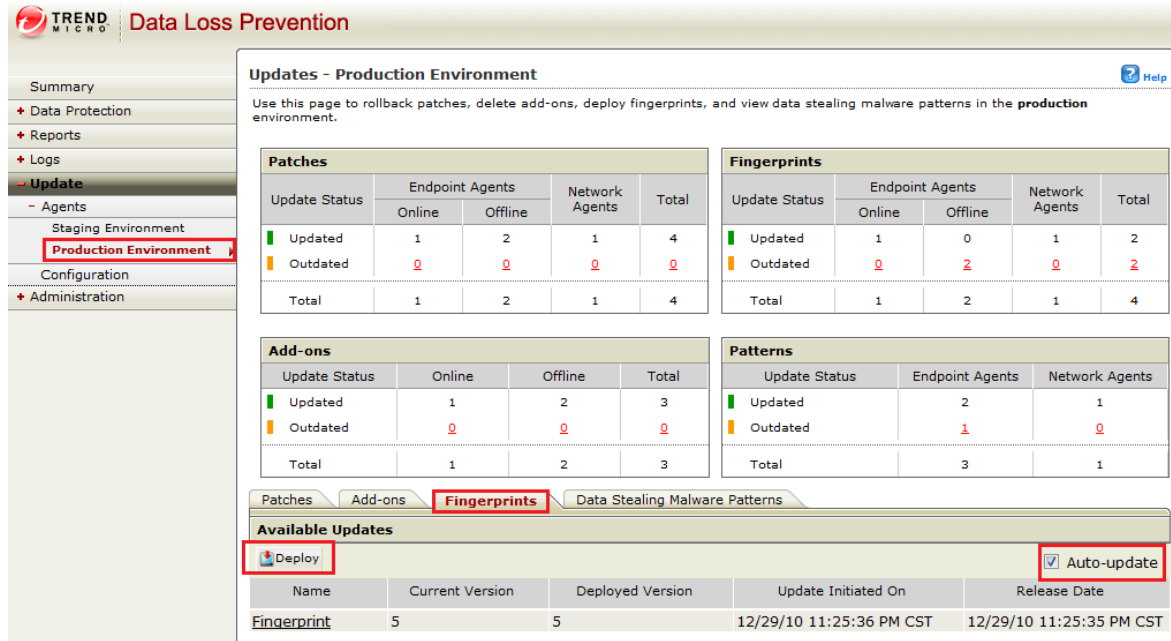
小贴士: 离线 Offline 模式下, 通过 channel 传送数据指纹的文件, 为何 DSA 不检测? 而 Online 模式下 DSA 可以检测?

如果您的客户端是 Production Environment, 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 Deploy, 过几分钟再次验证



Updates - Production Environment

Use this page to rollback patches, delete add-ons, deploy fingerprints, and view data stealing malware patterns in the **production** environment.

Update Status	Endpoint Agents		Network Agents	Total
	Online	Offline		
Updated	1	2	1	4
Outdated	0	0	0	0
Total	1	2	1	4

Update Status	Endpoint Agents		Network Agents	Total
	Online	Offline		
Updated	1	0	1	2
Outdated	0	2	0	2
Total	1	2	1	4

Update Status	Online	Offline	Total
Outdated	0	0	0
Total	1	2	3

Update Status	Endpoint Agents	Network Agents
Outdated	1	0
Total	3	1

Available Updates

Deploy Auto-update

Name	Current Version	Deployed Version	Update Initiated On	Release Date
Fingerprint	5	5	12/29/10 11:25:36 PM CST	12/29/10 11:25:35 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

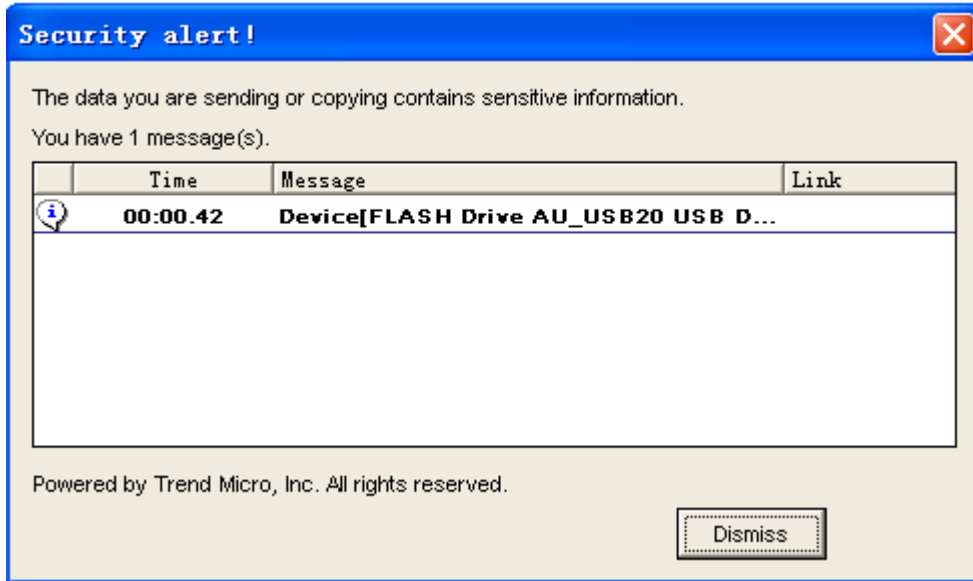
Print Screen Key

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.



Query [Hide Query]

Data Range: Last 7 days From To

Log Type: Policy Deployment **System Events** Security Audit Security Violations Server Status

[Show Log](#)

Filter Export Refresh 1-22 of 22 page 1 of 1

ID	Log Time	Severity	Description
299	12/30/10 12:07:54 AM CST	Informational	Device[FLASH Drive AU_USB20 USB Device] is disabled! @ T...

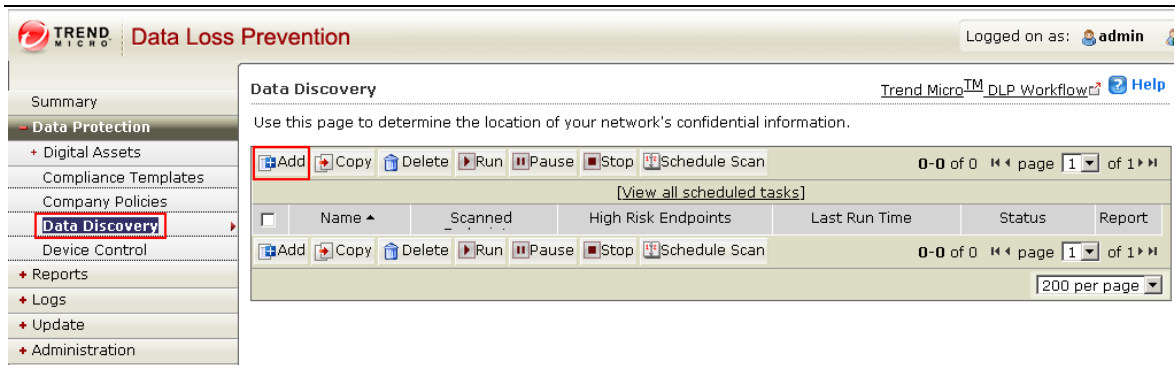
4.2 DLP 服务端的其他设定

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



Data Discovery Trend Micro™ DLP Workflow [Help](#)

Use this page to determine the location of your network's confidential information.

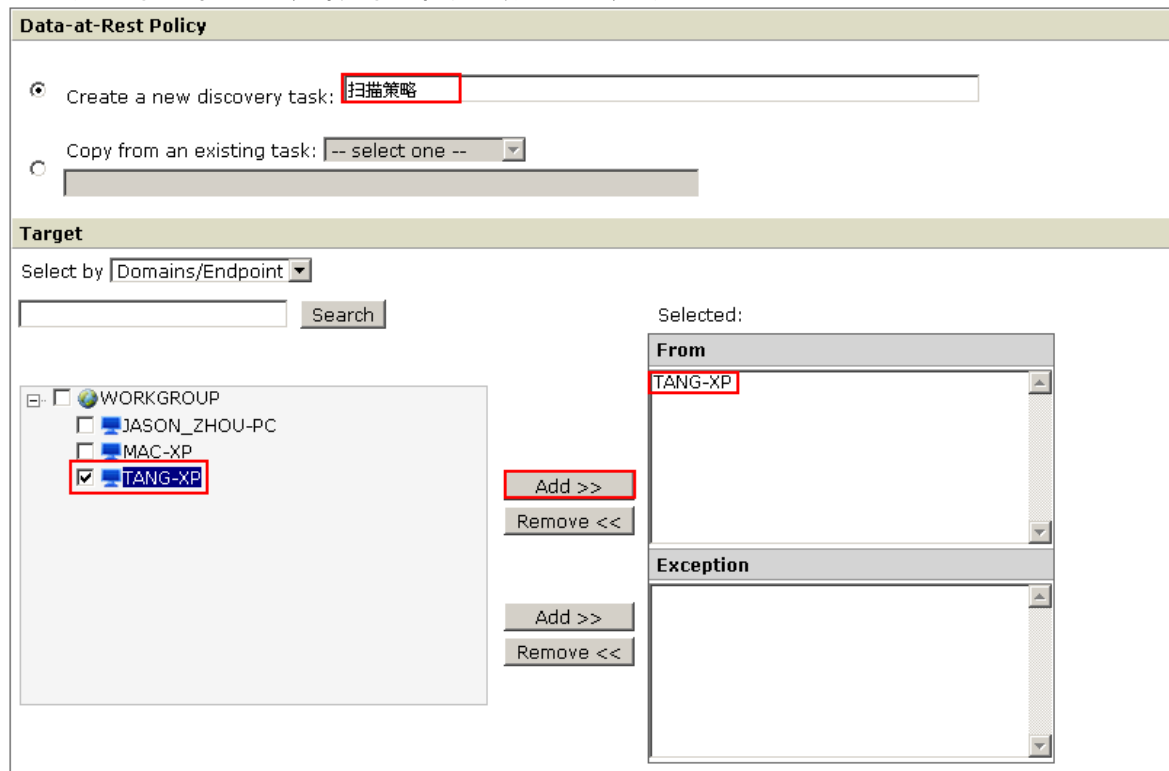
0-0 of 0 page 1 of 1

[\[View all scheduled tasks\]](#)

<input type="checkbox"/>	Name ^	Scanned	High Risk Endpoints	Last Run Time	Status	Report
<input type="button" value="Add"/>	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Pause"/>	<input type="button" value="Stop"/>	<input type="button" value="Schedule Scan"/>

200 per page

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

Create a new discovery task:

Copy from an existing task:

Target

Select by:

WORKGROUP

- JASON_ZHOU-PC
- MAC-XP
- TANG-XP

Selected:

From

TANG-XP

Exception

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 敏感文件
 Mac 文件后缀名
 PCI-DSS
 SB-1386
 US PII
 与得通讯

[Hold down the Control Key (CTRL) to select multiple items.]

Root path:

Priority:

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

Log

Other Actions

Move to security folder:

Encrypt

System Action When Offline Same as Online Action

Log

Other 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 Schedule Scan 预设扫描

Add Copy Delete Run Pause Stop Schedule Scan

1-1 of 1 page 1 of 1

[View all scheduled tasks]

	Name	Scanned	High Risk Endpoints	Last Run Time	Status	Report
<input checked="" type="checkbox"/>	扫描策略	0	0		New	

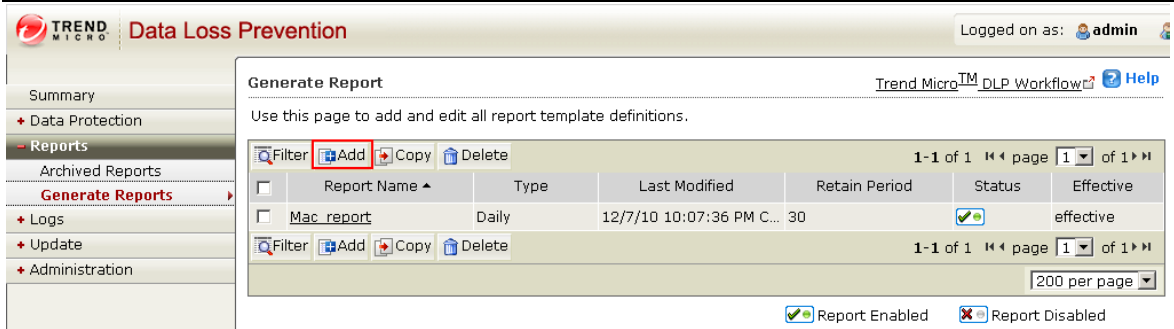
Add Copy Delete Run Pause Stop Schedule Scan

1-1 of 1 page 1 of 1

200 per page

4.2.2 Reports 报表生成

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



Generate Report Trend Micro™ DLP Workflow Help

Use this page to add and edit all report template definitions.

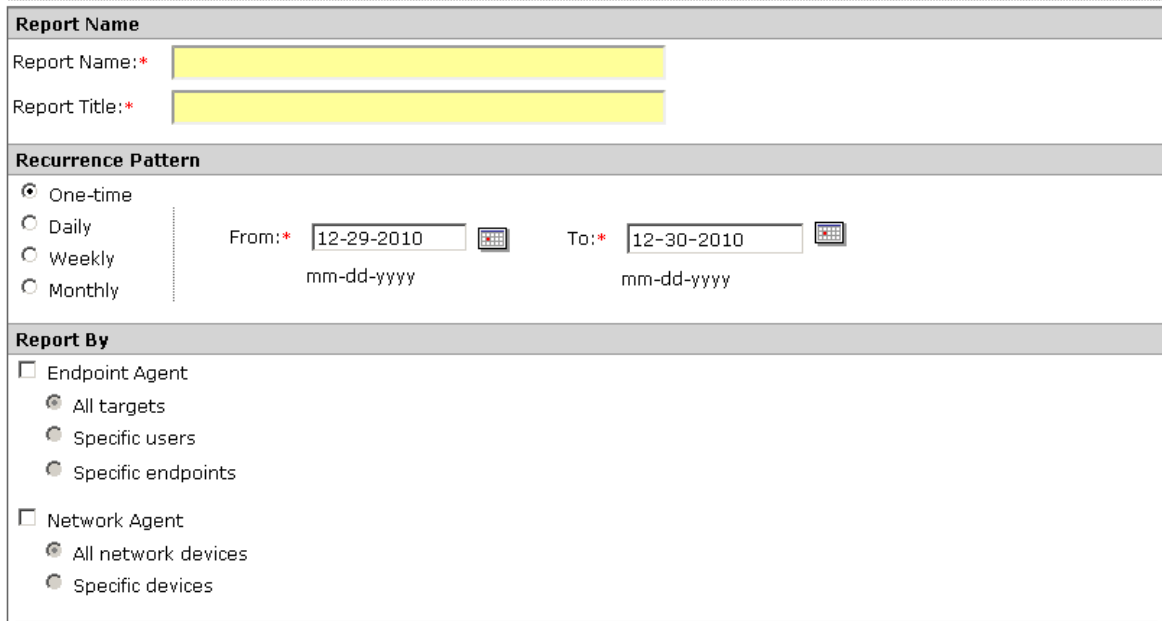
Report Name	Type	Last Modified	Retain Period	Status	Effective
Mac_report	Daily	12/7/10 10:07:36 PM C...	30	<input checked="" type="checkbox"/>	effective

Report Enabled Report Disabled

2. 设定 Report Name 名称等报表信息。

可以根据需求，设定 one-time 报表或者预设报表（每日、每周、每月）

Adding Reports (*: Required field) Help



Report Name

Report Name:*

Report Title:*

Recurrence Pattern

One-time

Daily

Weekly

Monthly

From:* To:*

mm-dd-yyyy mm-dd-yyyy

Report By

Endpoint Agent

All targets

Specific users

Specific endpoints

Network Agent

All network devices

Specific devices

3. 以及勾选报表内容需要的选项

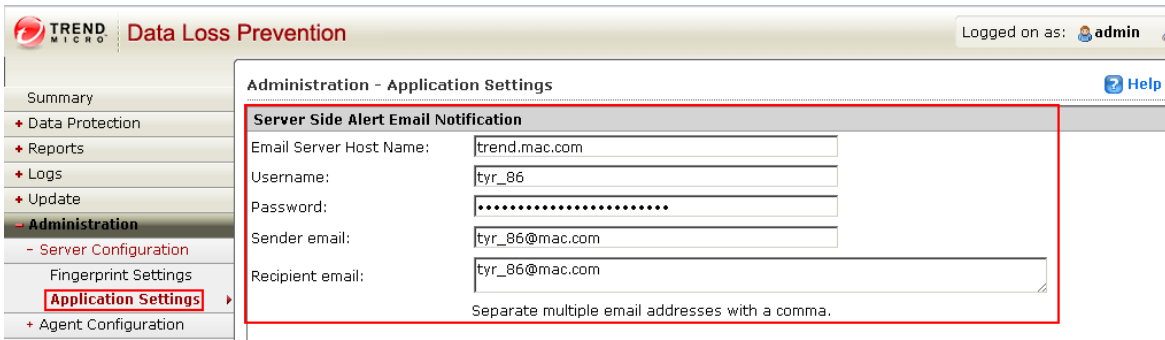
<p>1. Top Violator Information</p> <p><input checked="" type="checkbox"/> Select All</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Data Fingerprints by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Destinations by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Endpoints by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Users by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Templates by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Policies by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> IP Addresses by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Email Addresses by Violation</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Endpoints infected by Data-stealing Malware</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Data-stealing Malware Destinations</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Email Destinations</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> URL Destinations</p> <p>2. Summary Information</p> <p><input checked="" type="checkbox"/> Total Violations Over Time</p> <p><input checked="" type="checkbox"/> Total Violations by Channel</p> <p><input checked="" type="checkbox"/> Total Violations by Data Fingerprint</p> <p><input checked="" type="checkbox"/> Total Violations by Template Name</p>	<p>3. Executive Summary Information</p> <p><input checked="" type="checkbox"/> Select All</p> <p><input checked="" type="checkbox"/> Violation Summary Trend by Channel by 8 weeks</p> <p><input checked="" type="checkbox"/> Data Stealing Malware Violation Summary Trend by Channel by 8 weeks</p> <p><input checked="" type="checkbox"/> Violation Distribution</p> <p>-by Policy</p> <p>-by Channel</p> <p>-by Template</p> <p>-by Department(only for Endpoint Agents)</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Department Violations</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Policy Violations</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> High Risk Users</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Users Infected by Data Stealing Malware</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> IPs Infected by Data Stealing Malware</p> <p><input checked="" type="checkbox"/> Top <input type="text" value="10"/> Email Account Violations</p> <p>4. Audit Information</p> <p><input type="checkbox"/> Compliance Audit Report</p>
---	--

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。

<p>Time to Keep This Report</p> <p><input type="text" value="30"/> <input type="text" value="days"/></p>
<p><input type="checkbox"/> Email This Report</p> <p>Format: <input type="radio"/> PDF <input checked="" type="radio"/> HTML <input type="radio"/> EXCEL</p> <p>To:* <input type="text"/></p> <p>Separate multiple addresses with a comma.</p> <p>Subject:* <input type="text"/></p>

同时，还需要进行邮件通知设定

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



Administration - Application Settings

Server Side Alert Email Notification

Email Server Host Name:

Username:

Password:

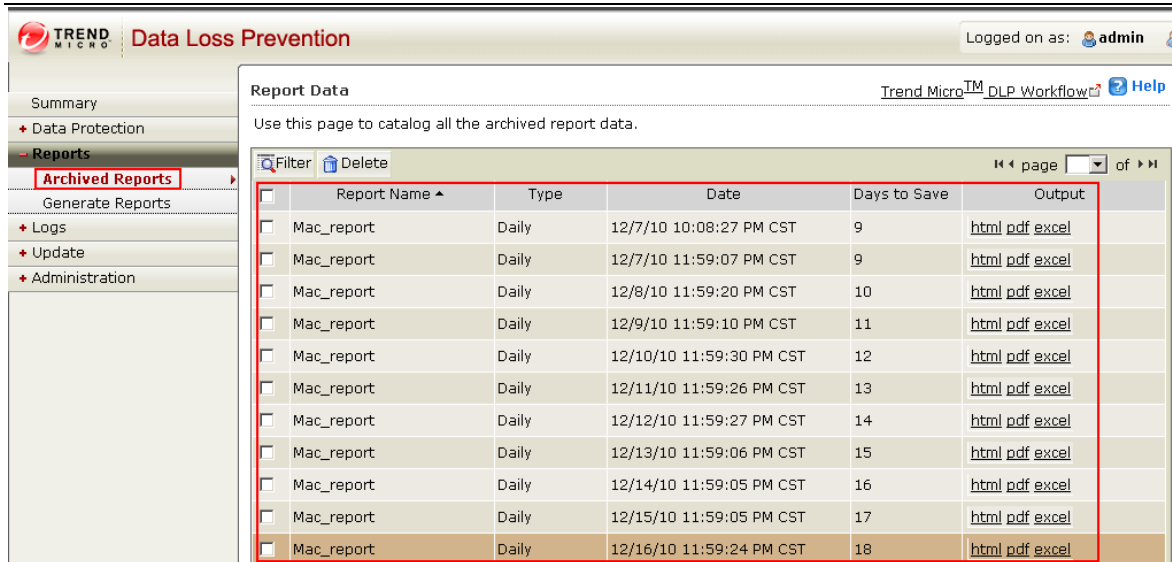
Sender email:

Recipient email:

Separate multiple email addresses with a comma.

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。

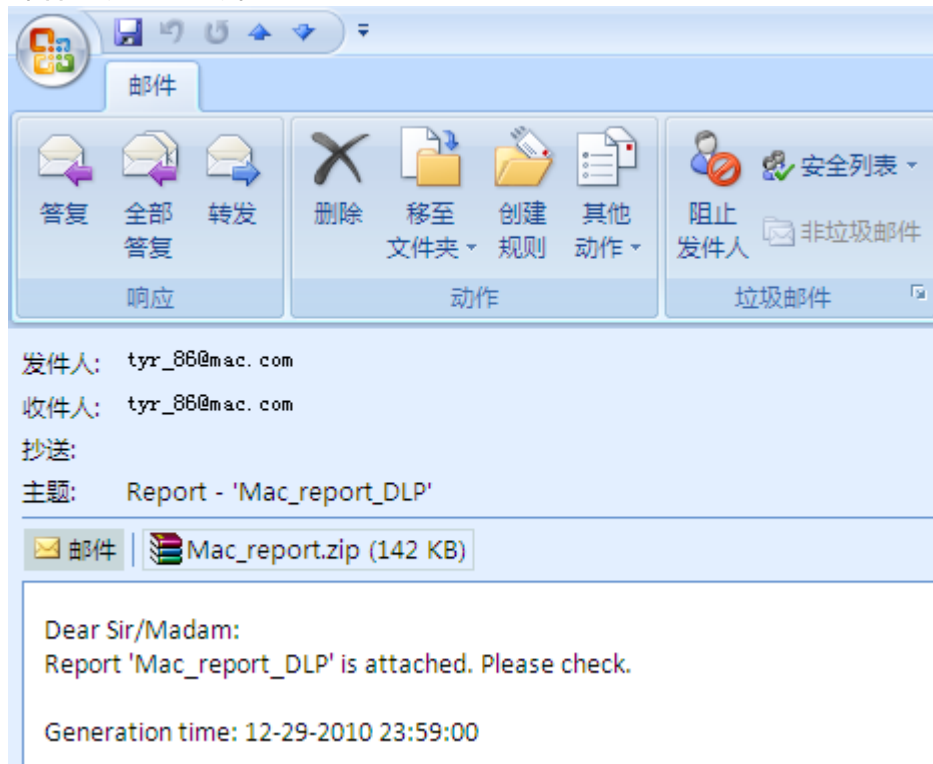


Report Data Trend Micro™ DLP Workflow [Help](#)

Use this page to catalog all the archived report data.

Report Name	Type	Date	Days to Save	Output
Mac_report	Daily	12/7/10 10:08:27 PM CST	9	html pdf excel
Mac_report	Daily	12/7/10 11:59:07 PM CST	9	html pdf excel
Mac_report	Daily	12/8/10 11:59:20 PM CST	10	html pdf excel
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	html pdf excel
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	html pdf excel
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	html pdf excel
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:



发件人: tyr_86@mac.com
 收件人: tyr_86@mac.com
 抄送:
 主题: Report - 'Mac_report_DLP'

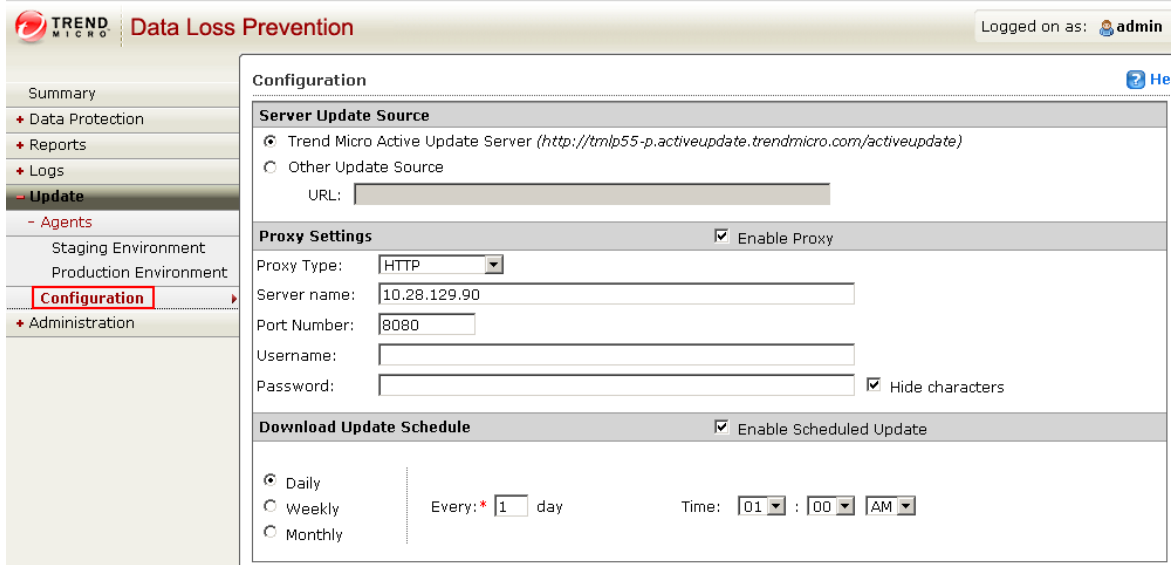
Mac_report.zip (142 KB)

Dear Sir/Madam:
 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。



2. DLP 服务端也可以手动更新补丁。

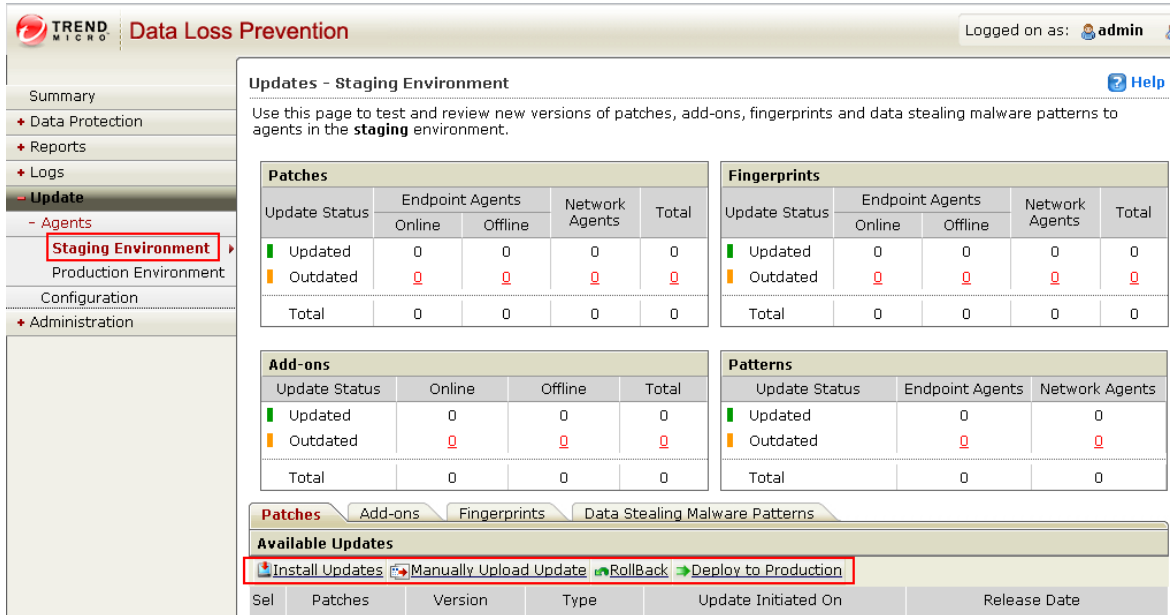
注意：DSA 客户端分为 2 中模式：

Staging Environment ——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。



4.2.4 DLP 的 Administration 设定

1. 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）

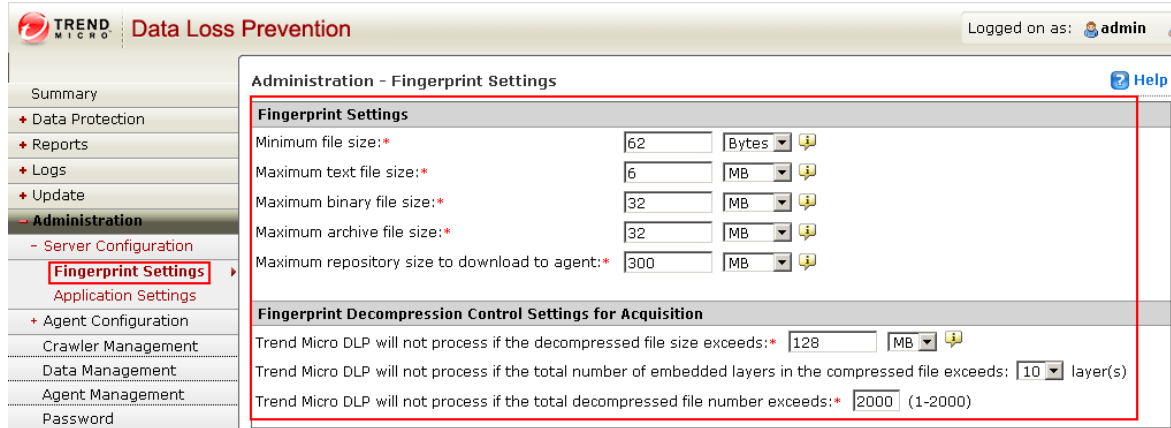
最大存档的文件：32MB（DLP 客户端触发策略后，将外泄数据存档备份到 DLP 服务端）

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）

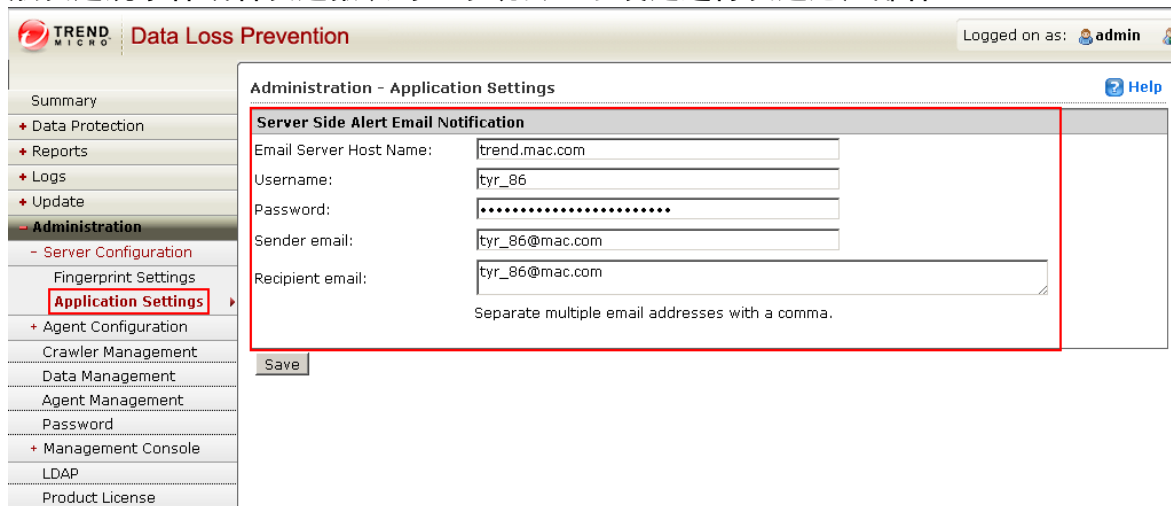
压缩层数：10（压缩超过 10 层的文件，DLP 不会去获取其指纹）

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）



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



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

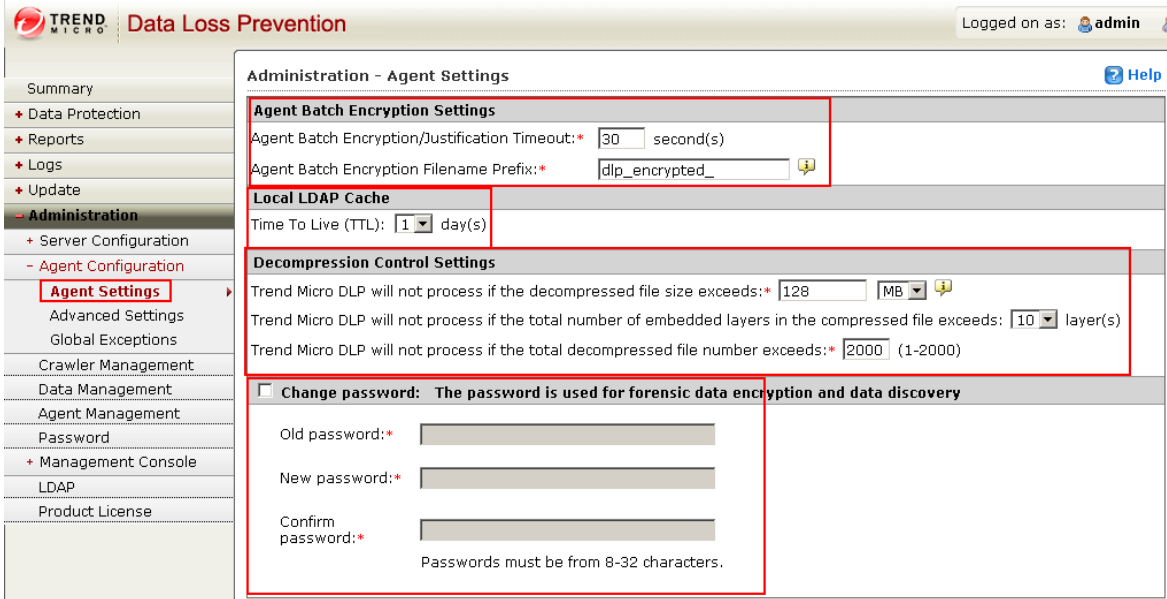
- 解压缩后文件大小：128MB（解压后文件大小超过 128M 的文件，DLP 不会进行检测）

- 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

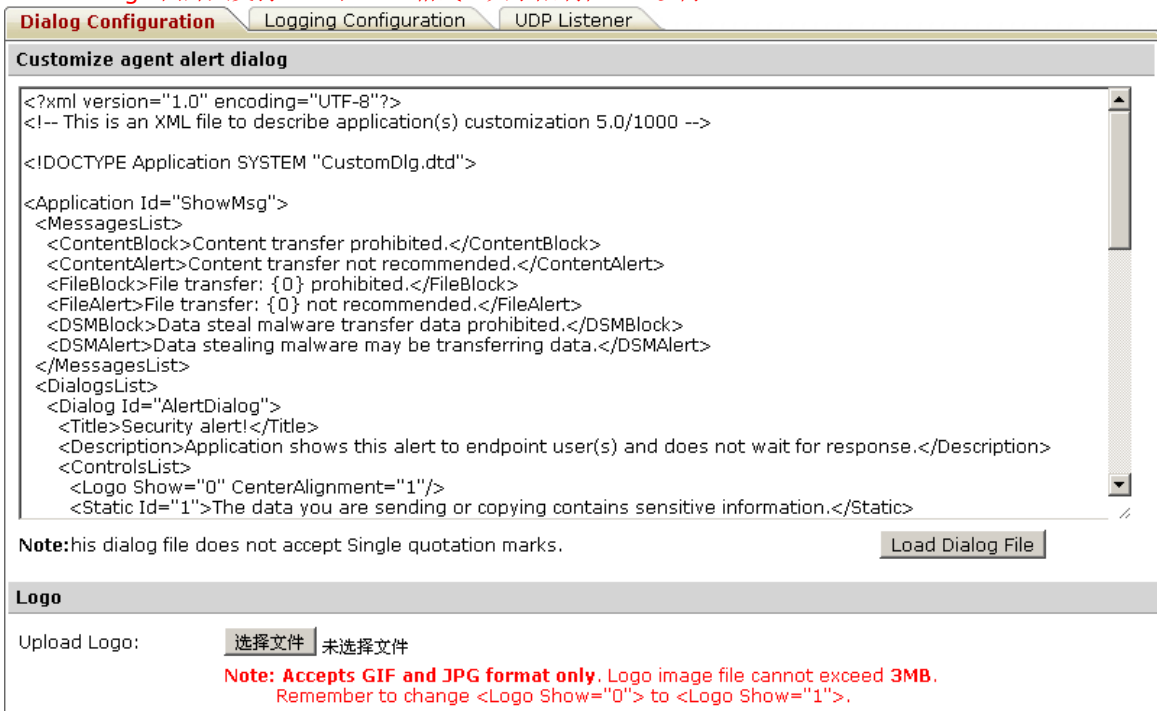
此处为 DLP 备份用户外泄的敏感文件到 DLP 服务端时，自动进行加密备份
 当从控制台下载时，自动会进行解密（默认密码：12345678）



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。



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：Blocked List -> Approved List -> Network Boundary

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

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

[Help](#)

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

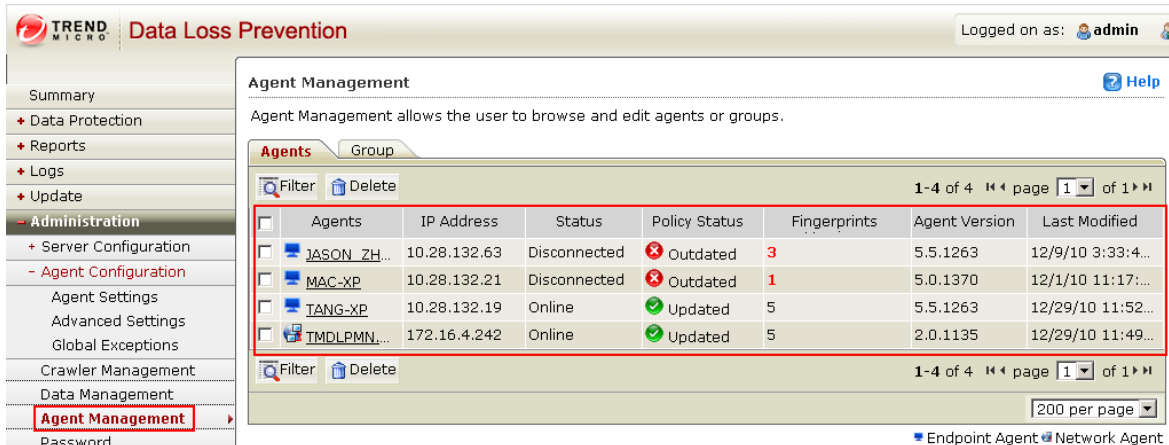
如果导出文件大于 200M, 请通过以下方式导入:

- 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

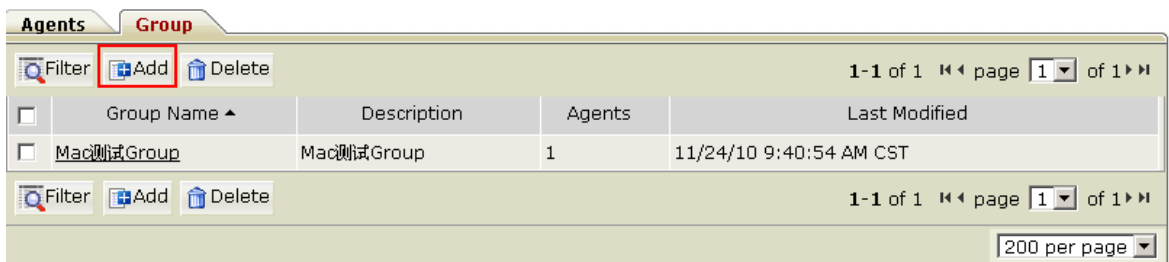


7. Agent 版本信息和组信息

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



可以创建用户组，将客户端添加至组中



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

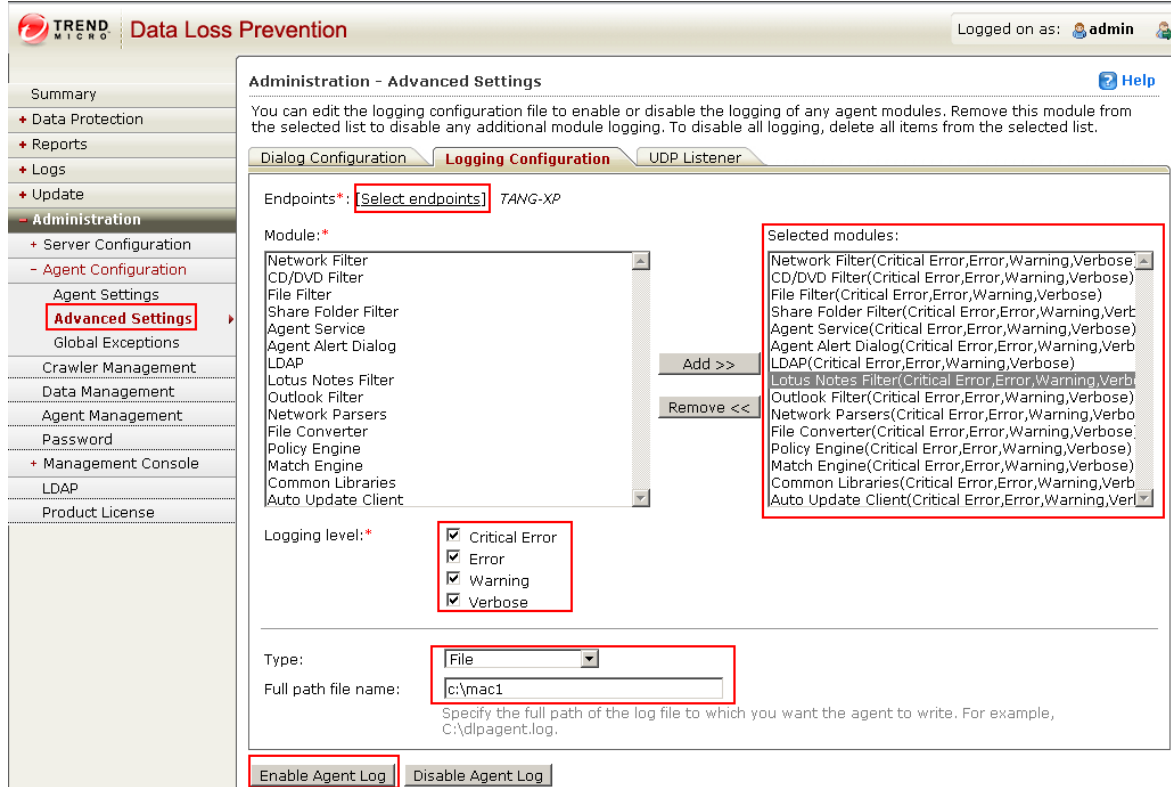
9. LDAP 的设定

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

4.2.5 客户端收集 Debug 日志方式

收集方式:

- 选中需要收集日志的客户端
- 将所对应的 Module 添加至右边
- 勾选 Logging 等级
- 设定存储位置
- 点击 Enable Agent Log
- 在客户端上重现问题。
- 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



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