**北京协和医院计算机终端安全配置基线**

**（讨论稿）**

**2018年12月4日**

目录

[一、 概述 4](#_Toc531719353)

[二、 操作系统配置要求 4](#_Toc531719354)

[2.1 账号与审计 4](#_Toc531719356)

[2.1.1. 设置密码策略 4](#_Toc531719360)

[2.1.2. 设置帐号锁定 5](#_Toc531719361)

[2.1.3. 设置必要的审核 6](#_Toc531719362)

[2.1.4. 设置审核日志策略 7](#_Toc531719363)

[2.1.5. 设置NTP 8](#_Toc531719364)

[2.2 资源控制 8](#_Toc531719365)

[2.2.1. 登录超时管理 8](#_Toc531719367)

[2.2.2. 远程登录超时配置 9](#_Toc531719368)

[2.2.3. 远程维护 9](#_Toc531719369)

[2.2.4. 屏保密码保护 9](#_Toc531719370)

[2.3 安全策略设置 10](#_Toc531719371)

[2.3.1. 禁止远程枚举帐号与共享 10](#_Toc531719373)

[2.3.2. 设置登录消息提示标题 11](#_Toc531719374)

[2.3.3. 设置登录消息提示正文 12](#_Toc531719375)

[2.3.4. 禁止自动登录 13](#_Toc531719376)

[2.3.5. 禁止自动执行系统调试器 14](#_Toc531719377)

[2.3.6. 禁止磁盘自动运行 14](#_Toc531719378)

[2.3.7. 重命名管理员账户 15](#_Toc531719379)

[2.3.8. 禁用Guest账户 16](#_Toc531719380)

[2.3.9. 文件所有权授权 16](#_Toc531719381)

[2.3.10. 设置试图登录的用户的消息文本、标题 16](#_Toc531719382)

[2.3.11. 可远程访问的注册表路径 18](#_Toc531719383)

[2.3.12. 远程强制关机授权 19](#_Toc531719384)

[2.3.13. 无须按 Ctrl+Alt+Del 19](#_Toc531719385)

[2.4 后台服务设置 20](#_Toc531719386)

[2.4.1. 禁用telnet服务 20](#_Toc531719388)

[2.4.2. 禁用Alert服务 20](#_Toc531719389)

[2.4.3. 降低PowerShell的执行权限 21](#_Toc531719390)

[2.4.4. 禁用Clipbook 21](#_Toc531719391)

[2.4.5. 禁止Computer Browser 22](#_Toc531719392)

[2.4.6. 禁止Remote Registry Service服务 22](#_Toc531719393)

[2.4.7. 禁止Print spooler服务 22](#_Toc531719394)

[2.4.8. 禁止RunAs Service服务 23](#_Toc531719395)

[2.4.9. 禁止Distributed File System服务 23](#_Toc531719396)

[2.4.10. 禁止Messenger服务 23](#_Toc531719397)

[2.4.11. 加强snmp community复杂度 24](#_Toc531719398)

[2.4.12. 禁用无线服务 24](#_Toc531719399)

[2.4.13. 禁用Help and Support服务 25](#_Toc531719400)

[2.5 注册表安全 25](#_Toc531719401)

[2.5.1. 关闭无用的默认端口 25](#_Toc531719403)

[2.5.2. 关闭操作系统默认共享 26](#_Toc531719404)

[2.6 剩余信息保护 27](#_Toc531719405)

[2.6.1. 不显示上次的用户名 27](#_Toc531719407)

[2.6.2. 清除虚拟内存页面文件 28](#_Toc531719408)

[2.6.3. 前次登录个数缓存 28](#_Toc531719409)

[2.7 其它安全设置 29](#_Toc531719410)

[2.7.1. 安装防火墙和杀毒软件 29](#_Toc531719412)

[2.7.2. 高危漏洞的及时修复 29](#_Toc531719413)

[2.7.3. 病毒库的及时更新 30](#_Toc531719414)

[2.7.4. USB存储介质的管控 30](#_Toc531719415)

[2.7.5. 禁用NetBIOS 30](#_Toc531719416)

[三、 终端安全管理系统 31](#_Toc531719417)

[3.1 桌面终端安全管理 31](#_Toc531719419)

[3.1.1. 常规功能的实现 31](#_Toc531719422)

[3.1.2. 外联的审计 31](#_Toc531719423)

[3.2 移动存储介质管理 32](#_Toc531719424)

[3.2.1. 移动存储介质的登记与审计 32](#_Toc531719426)

[3.2.2. 移动存储介质的管理 32](#_Toc531719427)

[3.2.3. 管理规则的支持 32](#_Toc531719428)

[3.2.4. 管理策略的支持 32](#_Toc531719429)

[3.3 终端数据防泄漏管理 33](#_Toc531719430)

[3.4 防病毒软件 33](#_Toc531719432)

# 概述

本配置基线适用于北京协和医院终端计算机，包括但不限于：医院信息系统终端、联网办公电脑，不包括：涉密计算机、接入内网但不能加固的医疗设备、不联网的个人电脑。

本配置基线主要涉及终端安全配置方面的基本要求，用于指导终端安全加固工作。主要参考依据：

全国医院信息化建设标准与规范（试行） 2018.4

GB/T 22239 网络安全等级保护基本要求（试行稿）2017.12

GB/T 28448 网络安全等级保护测评要求（试行稿）2017.12

GB/T 32925 政府联网计算机终端安全管理基本要求 2016.8

# 操作系统配置要求



## 账号与审计

**注意：如果系统加入域，可以使用域控制器上的策略覆盖本地策略**



### 设置密码策略

* + - 描述

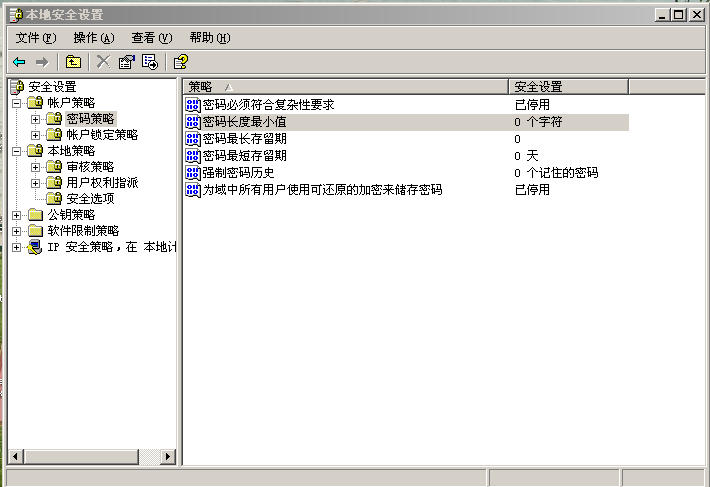
密码策略包括密码长度，密码复杂度和密码的使用周期， 好的密码策略应该满足不易猜解，定期更换原则，这将大大增加针对密码攻击的难度。

* + - 风险

无

* + - 操作

1. 点击“运行”-〉输入secpol.msc,进入本地安全策略，点击“账号策略”-〉“密码策略”，如下：



1. 设置“密码长度最小值”为8，“密码最长存留期”为180，“密码必须符合复杂性要求”启用

### 设置帐号锁定

* + - 描述

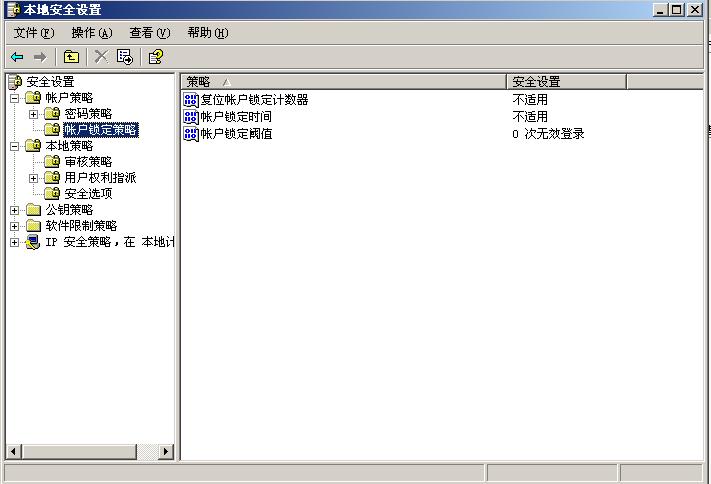
当无效登录次数达到规定的次数后，我们可以选择锁定此帐号，这可以有效的防御简单的猜解攻击。

* + - 风险

无

* + - 操作

点击“运行”-〉输入secpol.msc,进入本地安全策略，点击“账户策略”-〉“账户锁定策略”，如下：



设置“账户锁定阀值”为10，账户锁定时间与复位时间都是15分钟

### 设置必要的审核

* + - 描述

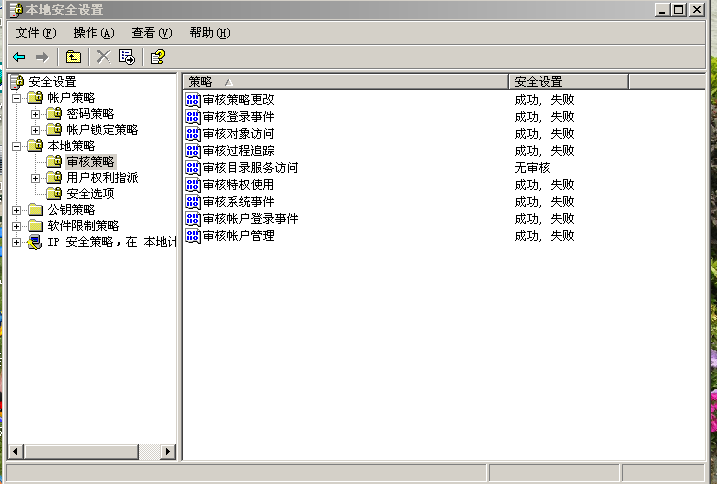
审核是针对系统事件的跟踪，可以提供诸如帐号管理，帐号登录，系统事件等方面详尽的信息，可以为发生安全事件的时候提供必要的原始日志。

* + - 风险

无

* + - 操作

1. 点击“运行”-〉输入secpol.msc,进入本地安全策略，点击“本地策略”-〉“审核策略”，如下：



1. 设置“审核策略更改”，“审核登录事件”，“审核账户登录事件”，“审核账户管理”为成功与失败

### 设置审核日志策略

* + - 描述

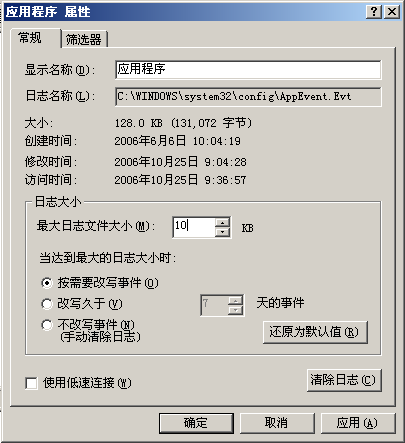
日志系统包括系统日志，应用日志与安全日志，详细的记录系统日常发生的事件，发生安全事件的时候可以提供必要的原始日志。

* + - 风险

无

* + - 操作

1. 进入“控制面板”-〉“管理工具”-〉事件查看器，如下：



1. 设置最大日志文件大小为80M，按需要改写日志文件

### 设置NTP

* + - 描述

windows time 服务设为自动。

* + - 风险

无

* + - 操作

进入“开始->管理工具->服务”：

启动“Windows Time 服务”，并设置为自动。

## 资源控制



### 登录超时管理

* + - 描述

启用超过登录时间后强制注销。

* + - 风险

无

* + - 操作

进入“开始->管理工具->本地安全策略->本地策略->安全选项”：

“网络安全: 在超过登录时间后强制注销” 设置为“已启用”。

### 远程登录超时配置

* + - 描述

检查设置：对于远程登录的帐号，设置不活动断连时间 15 分钟。

* + - 风险

无

* + - 操作

进入“开始->管理工具->本地安全策略->本地策略->安全选项”：“Microsoft 网络服务器：暂停会话前所需的空闲时间数量”为 15分钟。

### 远程维护

* + - 描述

终端计算机如无特别需要，关闭远程协助，关闭远程桌面。

* + - 风险

中

* + - 操作

鼠标右键点击“我的电脑”，选择“属性”，选中“远程设置”，在“远程协助”的下方查看，取消勾选“允许远程协助连接这台计算机”，在“远程桌面”的下方查看，勾选“不允许连接到这台计算机”。

### 屏保密码保护

* + - 描述

设置带密码的屏幕保护，并将时间设定为 5 分钟。

* + - 风险

无

* + - 操作

进入“控制面板－>外观显示－>更改屏幕保护程序”：启用屏幕保护程序，设置等待时间为“5 分钟”，启用“在恢复时使用密码保护。

## 安全策略设置

**注意：如果系统加入域，可以使用域控制器上的策略覆盖本地策略**

**回退方法：开启对应的安全设置。**



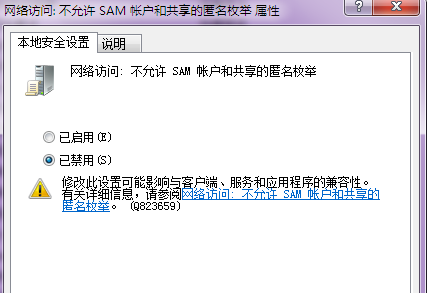
### 禁止远程枚举帐号与共享

* + - 描述

远程枚取帐号与共享是在不用任何用户名与密码的情况下，通过网络使用匿名身份进行帐号与共享与猜解，这通常会作为攻击的前奏。禁止远程枚取帐号与共享可以更好的保护系统信息的保密性，减少威胁的可能性。

* + - 风险

无



* + - 操作

1. 进入到“本地组策略标记器”，“计算机配置”->“Windows设置”->“安全设置”->“本地策略-安全选项”->“网络访问：不允许SAM账户和共享的匿名枚举”。
2. 设置“网络访问：不允许SAM账户和共享的匿名枚举”的安全策略为“已启用”。
3. Gpupdate更新策略后生效。

### 设置登录消息提示标题

* + - 描述

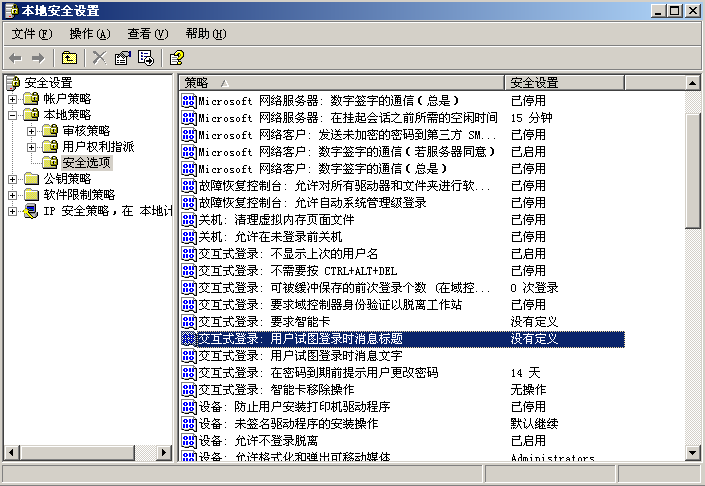
登录消息提示标题是用户登录系统时弹出授权说明的窗口标题，设置合理的标题可以对未授权访问者产生威慑作用。

* + - 风险

无

* + - 操作

1. 点击“运行”-〉输入secpol.msc,进入本地安全策略，点击“本地策略”-〉“安全选项”，如下：



1. 设置用户试图登录时消息标题

### 设置登录消息提示正文

* + - 描述

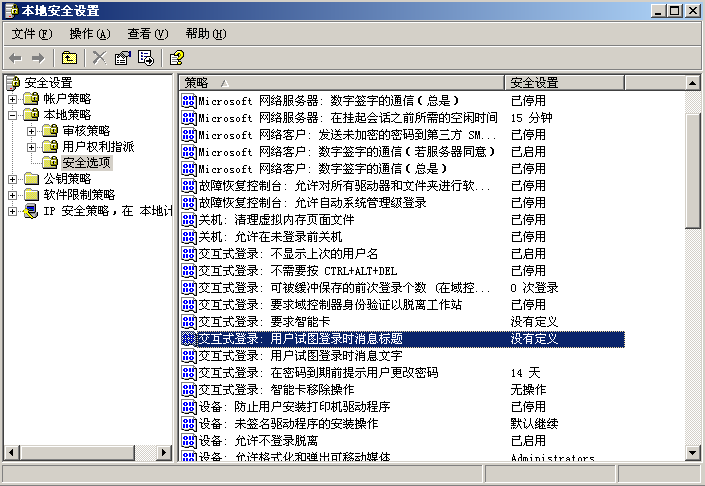
登录消息提示正文是用户登录系统时弹出授权说明的窗口正文，设置合理的正文(如访问授权)可以对未授权访问者产生威慑作用。

* + - 风险

无

* + - 操作

1. 点击“运行”-〉输入secpol.msc,进入本地安全策略，点击“本地策略”-〉“安全选项”，如下：



1. 设置用户试图登录时消息文字

### 禁止自动登录

* + - 描述

自动登录允许用户不输入用户名与密码直接进入系统，这通过在注册表中明文存放用户名与密码实现，这可能导致可以接触系统本身的任何人都可以通过重启机器进入系统。

* + - 风险

无

* + - 操作

1. 打开regedit.exe
2. 修改

HKLM\Software\Microsoft\WindowsNT\ CurrentVersion\Winlogon\AutoAdminLogon 类型: REG\_DWORD 值:0

### 禁止自动执行系统调试器

* + - 描述

系统调试器是windows处理程序异常的一种方法，当软件发生异常的时候，系统通常会提示是否使用调试器。执行系统调试器可能会导致精心构造的恶意代码在系统空间中执行，从而危害系统安全。

* + - 风险

无

* + - 操作

1. 打开regedit
2. 修改HKLM\Software\Microsoft\Window\CurrentVersion\

Windows NT\winlogon\No

类型为: REG\_DWORD 值为:0

### 禁止磁盘自动运行

* + - 描述

磁盘自动运行指当磁盘根目录如光盘F:下存在Autorun.inf的时候，当我们进入该磁盘根目录的时候，系统会自动运行Autorun.inf中指定的文件，为病毒与木马的传播带来了便捷，同样增加了安全威胁。

* + - 风险

无

* + - 操作

1. 打开regedit
2. HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Services/Cdrom。将其下Autorun字符串的值由原来的1更改为0。
3. HKLM\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriverTypeAutoRun 字符串的值

改为bd,00,00,00。

类型为: REG\_DWORD值为255

交互式登录: 之前登录到缓存的次数(域控制器不可用时) 设置为0。

重新启动。

1. 开始－运行，输入gpedit.msc，打开组策略编辑器，打开计算机配置-管理模版-Windows组件-自动播放策略-关闭自动播放。

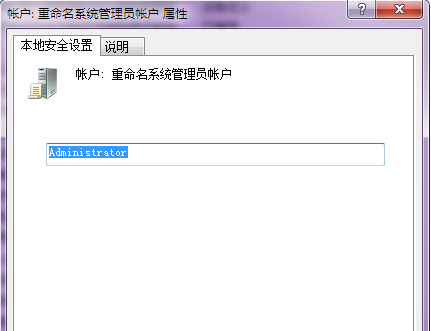
### 重命名管理员账户

* + - 描述

默认的操作系统管理员账户administrator，容易遭受账号枚举猜解攻击。

* + - 风险

无



* + - 操作

1. 进入到“本地组策略标记器”，“计算机配置”->“Windows设置”->“安全设置”->“安全选项”->“账户：重命名系统管理员账户”。
2. 修改系统默认管理员账户adminstrator。
3. Gpupdate更新策略后生效。

### 禁用Guest账户

* + - 描述

Guest账户是来宾账户，可以用它访问计算机，但是有很多入侵都是通过 Guest 账号进入系统，对Gues账户提权，并超越Administrator权限，然后进一步获得管理员密码或者权限，从而达到非法控制电脑系统的目的。

* + - 风险

中

* + - 操作

进入“控制面板->管理工具->计算机管理”，在弹出框中选择“系统工具->本地用户和组->用户”，在右侧选择Guest，双击鼠标左键查看，勾选“账户已禁用”选项。

### 文件所有权授权

* + - 描述

“取得文件或其他对象的所有权”只指派给 Administrators组。

* + - 风险

低

* + - 操作

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权限分配->取得文件或其他对象的所有权”，鼠标右键->属性->设置为只指派给Administrators组。

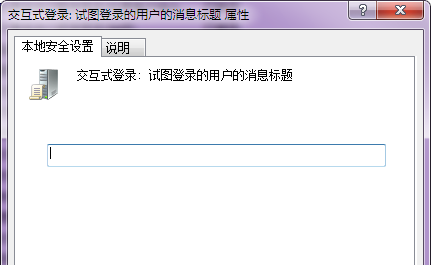
### 设置试图登录的用户的消息文本、标题

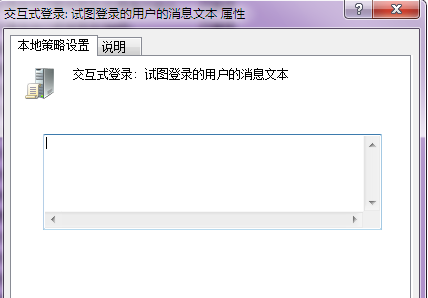
* + - 描述

试图登录的用户的消息文本、标题安全策略可作为机器辨识，人工辨识，信息提示使用。

* + - 风险

无





* + - 操作

1. 进入到“本地组策略标记器”，“计算机配置”->“Windows设置”->“安全设置”->“安全选项”->“交互式登录：试图登录的用户的消息标题”和“交互式登录：试图登录的用户的消息文本”。
2. 在“交互式登录：试图登录的用户的消息标题”和“交互式登录：试图登录的用户的消息文本”的本地安全策略设置框中输入要标识的信息
3. Gpupdate更新策略后生效。

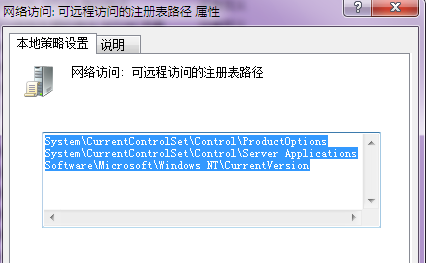
### 可远程访问的注册表路径

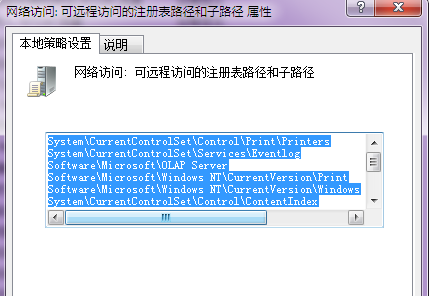
* + - 描述

该安全设置确定在网络上可访问的注册表路径和子路径，无论 **winreg** 注册表项的访问控制列表 (ACL) 中列出的是用户还是组。

* + - 风险

无





* + - 操作

1. 进入到“本地组策略标记器”，“计算机配置”->“Windows设置”->“安全设置”->“安全选项”->“网络访问：可远程访问的注册表路径”和“网络访问：可远程访问的注册表路径和子路径”。
2. 删除“网络访问：可远程访问的注册表路径”和“网络访问：可远程访问的注册表路径和子路径”的内容。
3. Gpupdate更新策略后生效。

### 远程强制关机授权

* + - 描述

非域环境的计算机，“从远程系统强制关机”的权限只指派给 Administrators 组。

* + - 风险

无

* + - 操作

进入“开始→管理工具→本地安全策略”

进入“安全设置→本地策略→用户权限分配”

配置“从远程系统强制关机”指派给“Administrators”组。

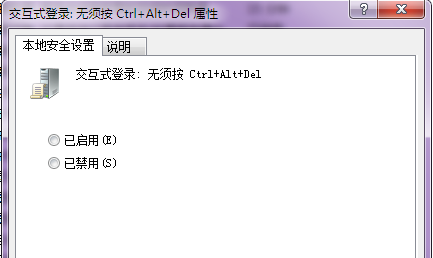
### 无须按 Ctrl+Alt+Del

* + - 描述

禁用“Ctrl+Alt+Del”三键重启，可以防止老版本Windows系统在本地采用热键非法重启和部分空密码终端按三键后自动进入到系统内。

* + - 风险

无



* + - 操作

1. 进入到“本地组策略标记器”，“计算机配置”->“Windows设置”->“安全设置”->“安全选项”->“交换式登录：无须按Ctrl+Alt+Del”。
2. 设置“交换式登录：无须按Ctrl+Alt+Del”的安全策略为“已启用”。
3. Gpupdate更新策略后生效。

## 后台服务设置



### 禁用telnet服务

* + - 描述

telnet服务用于系统管理员远程通过调用操作系统SHELL来管理维护终端，该协议属于明文传输，明文传输容易在网上泄露敏感信息，Windows系统默认禁止该服务。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开telnet，停止并禁用

### 禁用Alert服务

* + - 描述

Alerter服务用于通知用户与计算机有关系统管理方面的事件，如服务启动失败等，通常这都可以在系统日志中出现，Windows系统默认禁止该服务。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Alerter,停止并禁用

### 降低PowerShell的执行权限

* + - 描述

为防止恶意脚本的执行，PowerShell有一个执行策略，默认情况下，这个执行策略被设为受限的（Restricted），意味着PowerShell脚本无法执行。

* + - 风险

中

* + - 操作

在“开始”搜索“powershell”程序，右键“以管理员身份运行”，在命令行输入“Get-ExecutionPolicy”，反馈结果若是“Restricted”表示符合退出即可；反馈结果若不是“Restricted”，在命令行输入“Set-ExecutionPolicy Restricted”后选择“Y”退出即可。

### 禁用Clipbook

* + - 描述

Clipbook服务用于在网络上的机器间共享剪贴板上的信息，通常在交互式中应用比较多，因为信息在网络中传播，可能造成信息泄露，Windows系统默认禁止该服务。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Clipbook,停止并禁用

### 禁止Computer Browser

* + - 描述

Computer Browser服务用于跟踪网络上一个域内的机器.它允许用户通过网上邻居来发现他不知道确切名字的共享资源.它可以不通过任何授权就允许任何人浏览这些资源.，通常在交互式应用中使用较多。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Computer Browser，停止并禁用

### 禁止Remote Registry Service服务

* + - 描述

远程注册表服务用于允许匿名用户通过网络获取一定的注册表信息，这通常会暴露系统的一些敏感信息，增加安全威胁。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Remote Registry Service,停止并禁用

### 禁止Print spooler服务

* + - 描述

Print spooler服务用于将多个请求打印的文档统一进行保存和管理，待打印机资源空闲后，再将数据送往打印机处理。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Print spooler,停止并禁用；

### 禁止RunAs Service服务

* + - 描述

RunAs Service用于在不同用户身份下启动过程。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开RunAs Service停止并禁用；

### 禁止Distributed File System服务

* + - 描述

Distributed File System服务管理分布于局域网或广域网的逻辑卷，通常Windows的文件系统很少跨系统分布。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Distributed File System停止并禁用；

### 禁止Messenger服务

* + - 描述

Messenger服务用于发送net send消息或传递Alerter终端的消息，该功能通常比较少用，Windows系统默认禁止该服务。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开Messenger,停止并禁用；

### 加强snmp community复杂度

* + - 描述

snmp服务提供了远程监控终端的功能，默认snmp允许所有IP地址使用public读取所有的资源，给攻击者暴露了许多有用的系统信息(如系统进程 文件系统 网卡等)。

* + - 风险

无

* + - 操作

默认snmp服务没有安装，如果已经安装，操作如下:

1. 打开“控制面板”－>管理工具->服务，打开SNMP Service->属性－>安全，修改public为复杂的字符串，选择”接收来自这些主机的SNMP包”,添加信任的需要查询信息的主机
2. 如果不需要使用snmp服务，停止并禁用该服务，停止并禁用SNMP Trap Service服务

### 禁用无线服务

* + - 描述

无线服务用于支持操作系统接受无线信号上互联网或企业内部网络，如果不用，会影响系统性能并给系统带来一定风险，可以禁用。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，选择到wired Autoconfig 和Wireless Zero Configuration服务项，默认状态设置为启动，设置停止并禁用。

### 禁用Help and Support服务

* + - 描述

HELP服务用于支持操作系统为用户提供关于系统的资料查询，疑问解答的服务，一般终端上无需用到该服务，该服务的开启，会影响系统性能并给系统带来一定风险。

* + - 风险

无

* + - 操作

打开“控制面板”－>管理工具->服务，打开help and support，停止并禁用；

## 注册表安全



### 关闭无用的默认端口

* + - 描述

Windows操作系统在安装的时候默认会开启一些端口，如果这些端口不用，但是一直对外开放，会对操作系统的安全带来一定的风险和威胁，所以如果不用，建议，在不影响业务应用的情况下，选择性的关闭一些无用的默认端口。

* + - 风险

中

* + - 操作

1. 关闭7.9等等端口：关闭Simple TCP/IP Service,支持以下 TCP/IP服务：Character Generator, Daytime, Discard, Echo, 以及 Quote of the Day。
2. 关掉21端口：关闭FTP Publishing Service,它提供的服务是通过 Internet 信息服务的管理单元提供 FTP 连接和管理。
3. 关掉23端口：关闭Telnet服务，它允许远程用户登录到系统并且使用命令行运行控制台程序。
4. 关掉25端口：关闭Simple Mail Transport Protocol (SMTP)服务，它提供的功能是跨网传送电子邮件。
5. 关闭80口：关掉WWW服务。在“服务”中显示名称为"World Wide Web Publishing Service"，通过 Internet 信息服务的管理单元提供 Web 连接和管理。
6. 关闭139端口：139端口是NetBIOS Session端口，用来文件和打印共享，注意的是运行samba的unix机器也开放了139端口，功能一样。关闭139口听方法是在“网络和拨号连接”中“本地连接”中选取“Internet协议(TCP/IP)”属性，进入“高级TCP/IP设置”“WINS设置”里面有一项“禁用TCP/IP的NETBIOS”，打勾就关闭了139端口。
7. 关闭445端口：修改注册表，添加一个键值。修改[HKEY[\_](http://www.pconline.com.cn/pcjob/system/microsoft/article/0412/507334.html)LOCAL[\_](http://www.pconline.com.cn/pcjob/system/microsoft/article/0412/507334.html)MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]  
   为"SMBDeviceEnabled"=dword:00000000

### 关闭操作系统默认共享

* + - 描述

在Windows 2000以上版本，有一个“默认共享”，这是在安装终端的时候，把系统安装分区自动进行共享，虽然对其访问还需要超级用户的密码，但这是潜在的安全隐患，从终端的安全考虑，最好关闭这个“默认共享”，以保证系统安全。

* + - 风险

中

* + - 操作

关闭默认共享的方法是：单击“开始/运行”，在运行窗口中输入“Regedit”， “HKEY[\_](http://www.pconline.com.cn/pcjob/system/microsoft/article/0412/507334.html)LOCAL[\_](http://www.pconline.com.cn/pcjob/system/microsoft/article/0412/507334.html)MACHINE\SYSTEM\CurrentControlSet\Lanmanworkstation\parameters”，在右侧窗口中创建一个名为“AutoShareWks”的双字节值，将其值设置为0，(win2000专业版 win xp)；

[HKEY[\_](http://www.pconline.com.cn/pcjob/system/microsoft/article/0412/507334.html)LOCAL[\_](http://www.pconline.com.cn/pcjob/system/microsoft/article/0412/507334.html)MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]

"AutoShareServer"=dword:00000000这样就可以彻底关闭“默认共享”。(在DOS下运行net share c$Content$nbsp;/del，有几个默认共享就执行几次)

## 剩余信息保护



### 不显示上次的用户名

* + - 描述

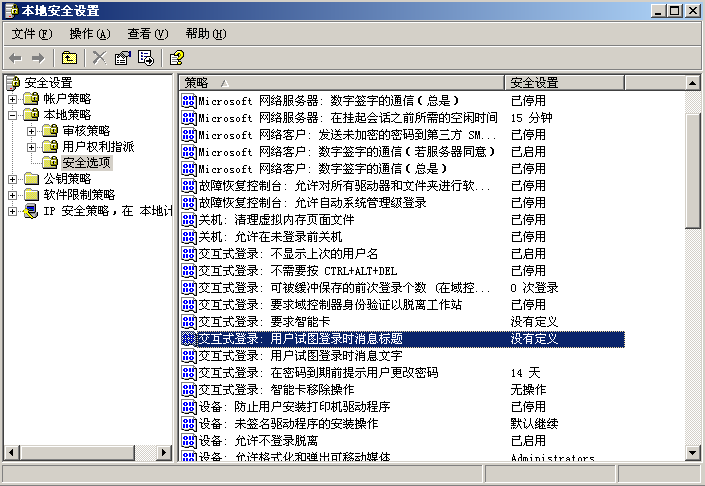
默认登录的时候，系统会使用上一次登录使用的用户名，这给我们带来了方便，但是如果攻击着有权连接系统，同样可以给他减少猜解用户名的麻烦。

* + - 风险

无

* + - 操作

点击“运行”-〉输入secpol.msc,进入本地安全策略，点击“本地策略”-〉“安全选项”，将“交互登录：不显示上次（最后）的用户名”配置为“已启用”。



### 清除虚拟内存页面文件

* + - 描述

在每次干净关机时，清除系统页面文件。

* + - 风险

无

* + - 操作

进入“开始->管理工具->本地安全策略->本地策略->安全选项”：

将“关机：清除虚拟内存页面文件”配置为“已启用”。

### 前次登录个数缓存

* + - 描述

可被缓存的前次登录次数。

* + - 风险

无

* + - 操作

进入控制面板->管理工具->本地安全策略->安全选项->交互式登录：

设置可被缓存的前次登录个数为 5。

## 其它安全设置



### 安装防火墙和杀毒软件

* + - 描述

Windows操作系统对外提供服务，会面临互联网和企业内网内的病毒、蠕虫、木马的攻击，要全面有效的防范网内和往外的攻击，需要安装杀毒软件和防火墙。

* + - 风险；

低

* + - 操作

1. 打开“控制面板”－>管理工具->服务，打开Windows Firewall，设置为启用；
2. 在终端上安装第三方的杀毒软件和防火墙；

### 高危漏洞的及时修复

* + - 描述

Windows系统是应用最为普遍的操作系统，因其复杂性及开放性，会存在各种各样的漏洞，其中高危漏洞最容易被攻击者利用，进行破坏终端系统，病毒木马就会乘虚而入。

* + - 风险

高

* + - 操作

通过漏扫设备针对存在的漏洞进行扫描，定期修复高危项。

所有终端计算机统一部署桌面安全管理软件，由该软件统一进行系统安全补丁的更新。

### 病毒库的及时更新

* + - 描述

以往病毒利用终端没有安装杀毒软件或者终端病毒库版本较旧杀毒能力薄弱来继续进行对终端的入侵，损害终端或对终端信息进行窃取。

* + - 风险

高

* + - 操作

所有终端计算机统一部署防病毒杀毒软件，并保持病毒库的更新迭代，推荐一周进行一次病毒库版本的升级。

### USB存储介质的管控

* + - 描述

U盘、移动硬盘等移动存储介质随意介入终端，可能将其携带的病毒木马类文件感染至终端计算机，并以此传播开来造成批量终端遭受病毒木马感染受害。

* + - 风险

高

* + - 操作

所有终端计算机统一部署桌面安全管理软件，由该软件统一对终端的U口进行集中策略管控，若需要使用U盘，再另行加白操作。

### 禁用NetBIOS

* + - 描述

NetBIOS Session端口，用来文件和打印共享，注意的是运行samba的unix机器也开放了NetBIOS Session 139端口，功能一样。

* + - 风险

无

* + - 操作

关闭NetBIOS Session 139的方法是在“网络和拨号连接”中“本地连接”中选取“Internet协议(TCP/IP)”属性，进入“高级TCP/IP设置”“WINS设置”里面有一项“禁用TCP/IP的NETBIOS”，打勾就关闭了NetBIOS Session 139端口。

# 终端安全管理系统



## 桌面终端安全管理



### 常规功能的实现

* + - 描述

桌面终端安全管理系统应具备即时通讯管理、非授权外连管理、软件分发、打印管理、文件操作行为管理、补丁管理、移动介质管理、主机监控与审计、上网行为控制与审计、敏感字审计、远程协助等 11 项功能。

* + - 操作

安装用于满足终端各种安全管理和合规性需求的终端安全管理软件。

### 外联的审计

* + - 描述

桌面终端安全管理系统应支持对双网卡、WIFI、3G、蓝牙、红外等 5 种违规连接方式进行监测、审计和阻断。

* + - 操作

安装用于满足终端各种安全管理和合规性需求的终端安全管理软件。

## 移动存储介质管理



### 移动存储介质的登记与审计

* + - 描述

具备移动存储介质注册管理、接入控制、访问权限控制、安全审计等 4 项功能。

* + - 操作

安装解决医院移动存储介质非法滥用造成信息泄露安全问题的专用管理设备。

### 移动存储介质的管理

* + - 描述

支持移动硬盘、闪存、U 盘、储存卡等 4 种移动存储介质的管理。

* + - 操作

安装解决医院移动存储介质非法滥用造成信息泄露安全问题的专用管理设备。

### 管理规则的支持

* + - 描述

支持预置策略、自定义策略、预置标签及自定义标签等 4 种管理规则。

* + - 操作

安装解决医院移动存储介质非法滥用造成信息泄露安全问题的专用管理设备。

### 管理策略的支持

* + - 描述

支持内部低密、内部普密、内置高密、外部应用审计、外部文档审计、外部无审计等6种预置管理策略和预置标签管理策略。

* + - 操作

安装解决医院移动存储介质非法滥用造成信息泄露安全问题的专用管理设备。

## 终端数据防泄漏管理

* 1. + 描述

本系统应具有防止信息通过以下途径泄露的功能：

**1）使用泄露**（①操作失误导致技术数据泄漏或损坏；②通过打印、剪切、复制、粘贴、另存为、重命名等操作泄漏数据）；

**2）存储泄露**（①数据中心、服务器、数据库的数据被随意下载、共享泄漏；②离职人员通过U盘、CD/DVD、移动硬盘随意拷走机密资料；③移动笔记本被盗、丢失或维修造成数据泄漏）；

**3）传输泄露**（①通过email、QQ、MSN等轻易传输机密资料；②通过网络监听、拦截等方式篡改、伪造传输数据）等泄密途径。

* + - 操作

部署解决造成医院内部重要信息泄露安全问题的专用DLP数据泄露防护系统。

## 防病毒软件

* + - 描述

为了提高医院信息系统终端的病毒防范能力，防病毒软件应满足以下基本功能的实现：

**1）防病毒软件的安装**（防病毒软件的客户端安装后，应配置为普通用户无法删除与卸载，若需要临时卸载，可联系管理员进行卸载操作）。

**2）防病毒软件的定时扫描**（防病毒软件的客户端安装后，应当配置定时扫描策略，扫描项可分快速扫描与全盘扫描，扫描策略只能由管理员配置生效）。

**3）防病毒软件的升级更新**（防病毒软件的客户端安装后，应保证最新病毒库定义码版本与当前时间不超过七天）。

**4）防病毒软件的查杀功能**（防病毒软件的客户端安装后，应当具备联网查杀和离线查杀的两种查杀能力）。

**5）防病毒软件的误报处理**（防病毒软件的客户端安装后，对于被终端误报的文件，可以对该文件进行加白处理；若是需要加黑某个文件，同样也可以将该文件进行加黑处理）。

**6）防病毒软件的病毒分析**（防病毒软件的客户端安装后，应具备病毒分析能力，该能力是终端杀毒的日志报表体现，可包括病毒查杀趋势图、病毒种类占比、触发方式趋势、触发方式及病毒排名等为分类的图例，能够快速的帮助管理员查询统计出网内的病毒现状，以便采取相应的措施）。

* + - 操作

所有终端计算机统一部署防病毒杀毒软件。