

# ANYSEC 行为管理 AD SSO 配置手册



版权所有：深圳市中科网威科技有限公司

# 一、手册说明

## 1.1. 场景说明

该手册只针对“域控制器策略派发模式”有效。

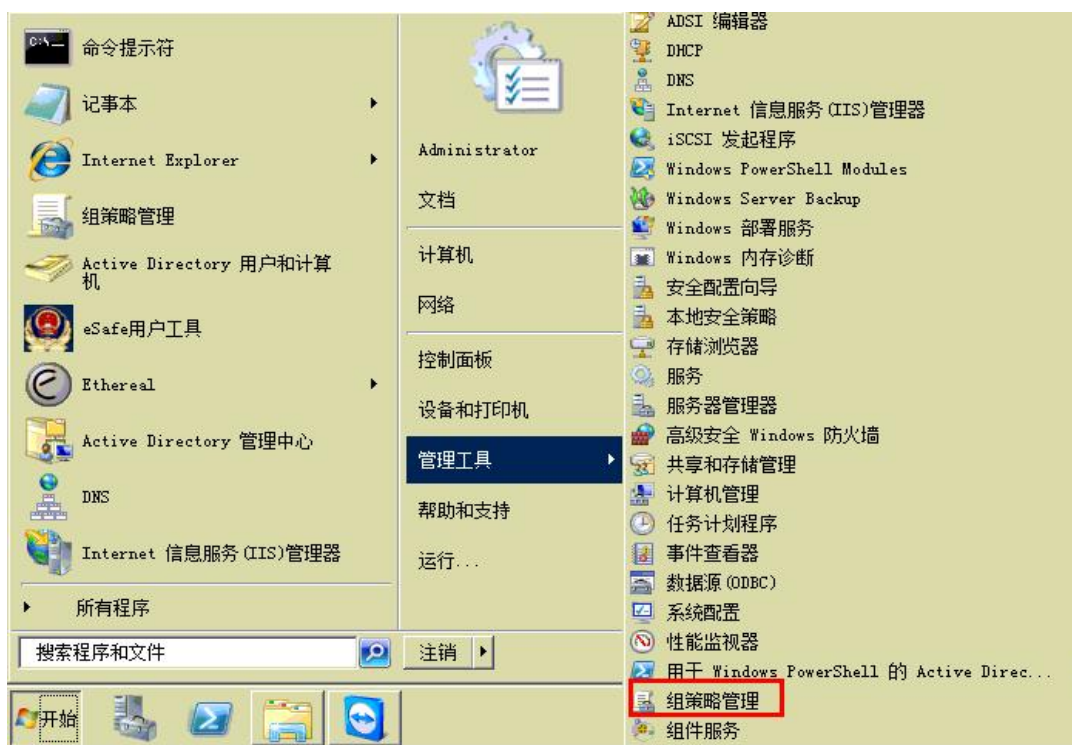
## 1.2. 域控制器策略派发模式

“域控制器策略派发模式”通过域控制器的组策略来实现单点登录。可实现域用户登录到域时自动完成到行为管理网关设备的 WEB 认证，在域用户从域注销出来时自动注销在行为管理网关设备的登录。

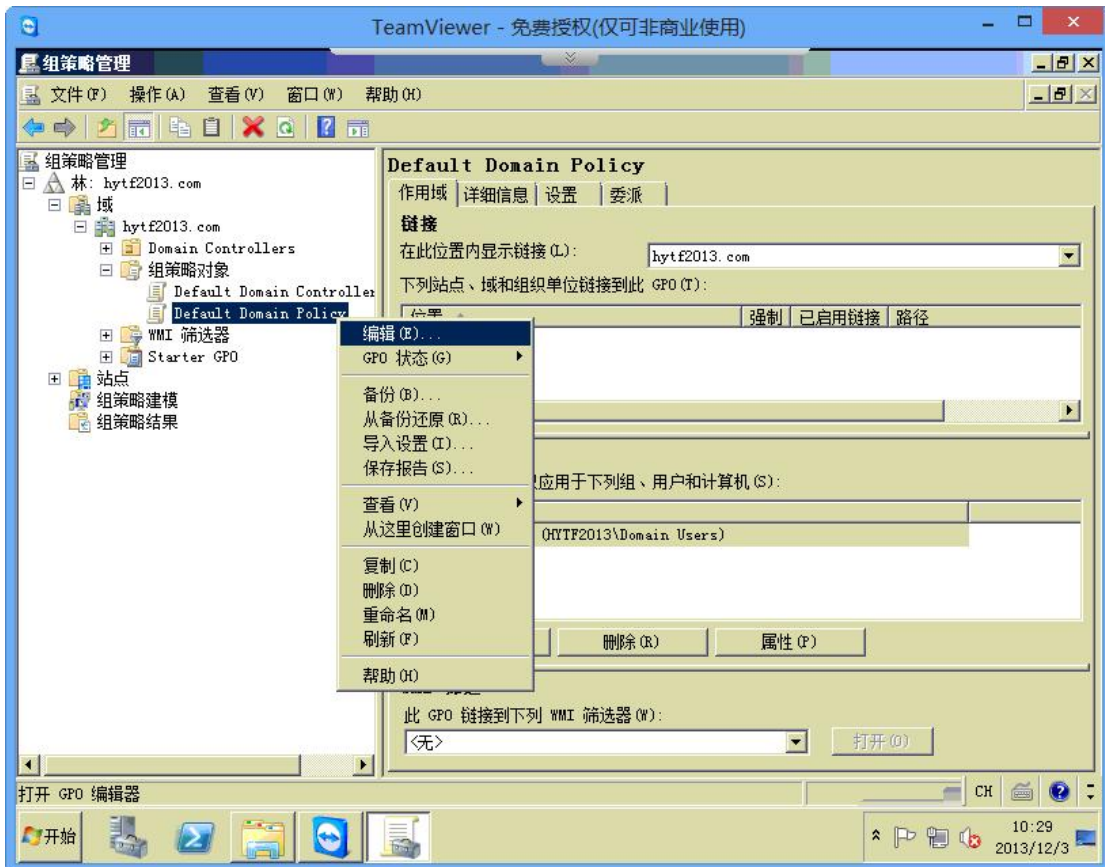
# 二、域控制器设置

## 2.1.配置与用户登录脚本

1. 利用域管理员登录域后，找到 2008 AD server ‘管理工具’ - ‘组策略管理’，如图：



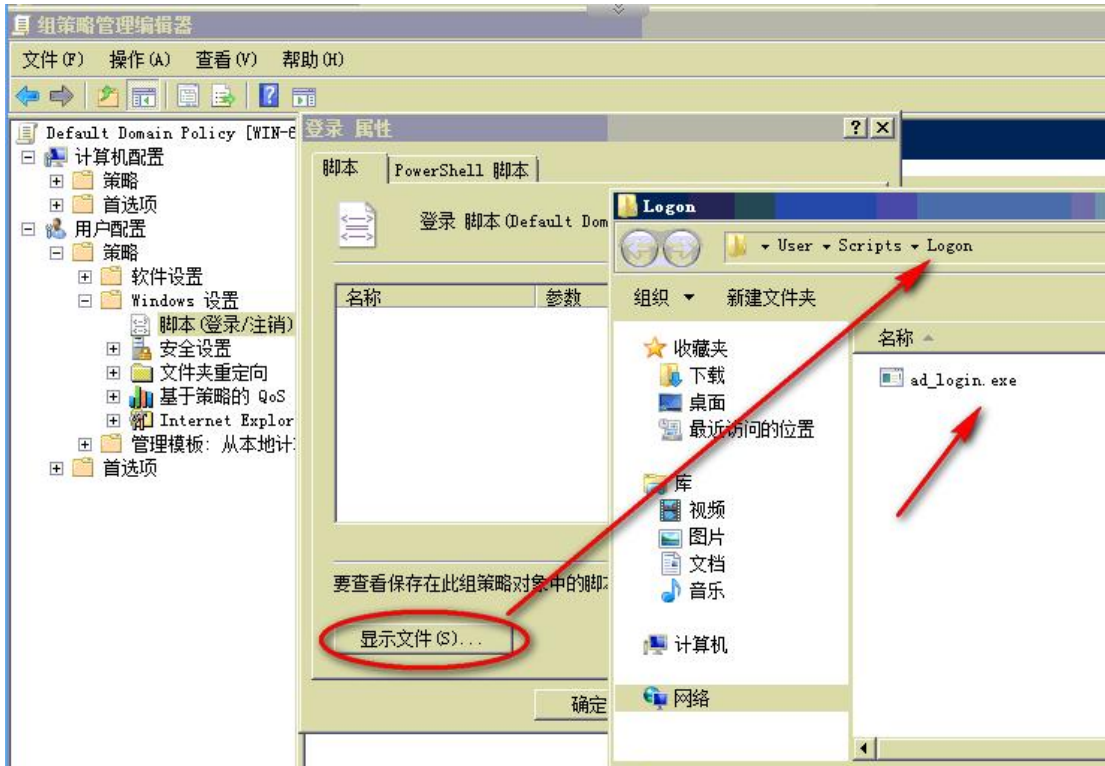
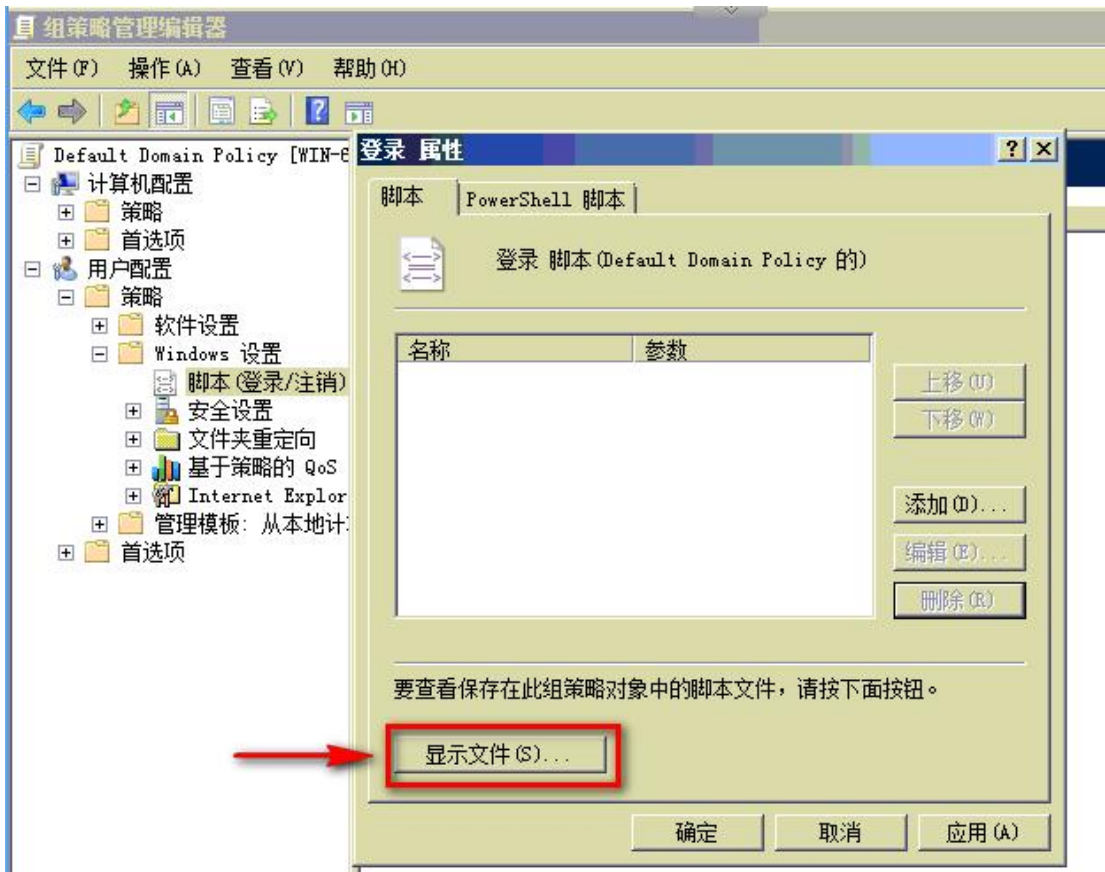
2. 右键点击组策略选项，“Default Domain Policy”，选择编辑



3. 组策略编辑页面，依次点击【用户配置】-【windows 设置】-【脚本（登录/注销）】

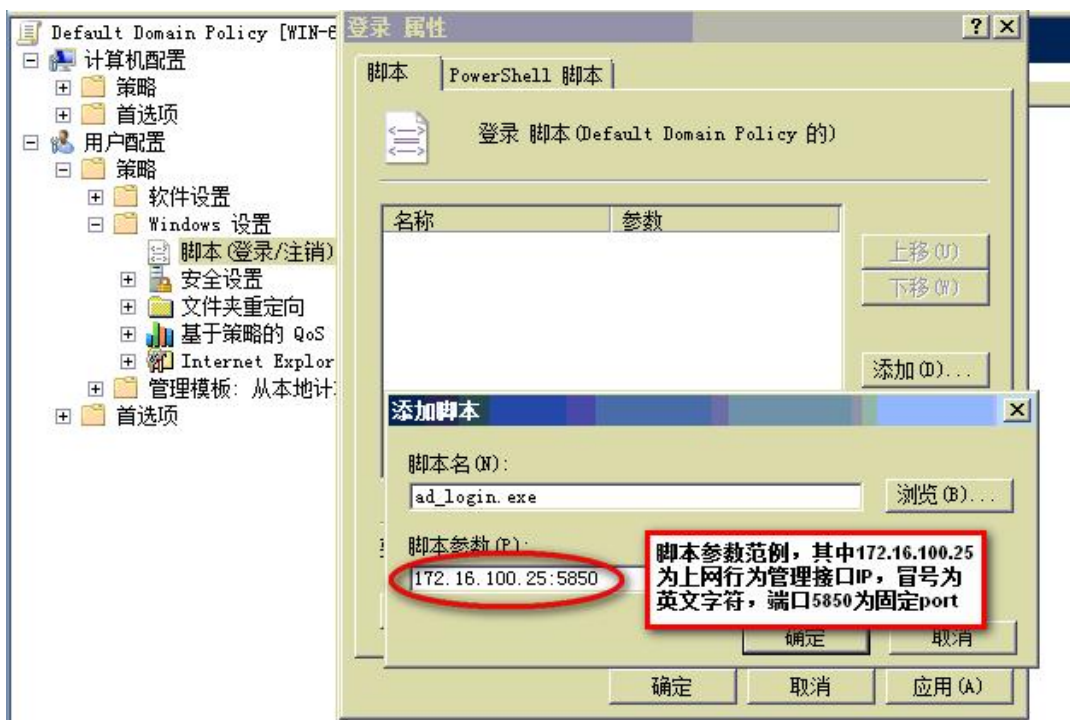
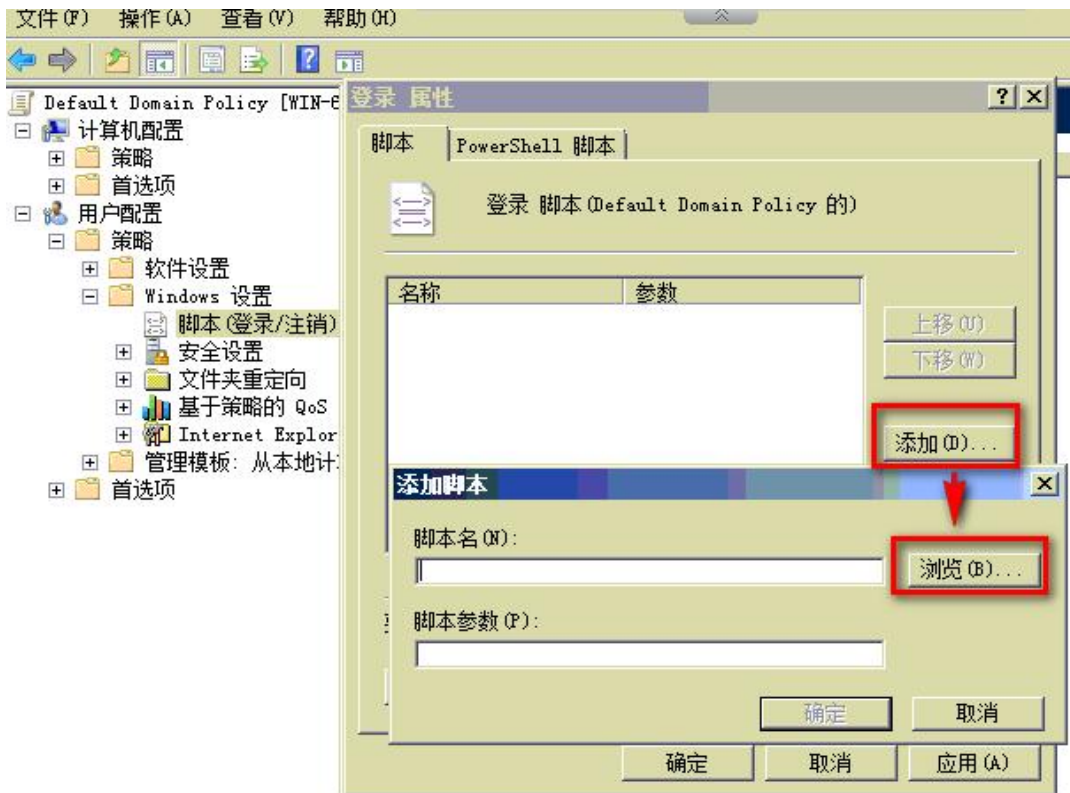


4. 双击“登录”选项，在弹出的登录脚本编辑窗口左下角点击“显示文件”，将打开一个目录，然后将登入脚本文件（ad\_login.exe）拷贝到该目录下，关闭该目录





5. 在弹出的登录脚本编辑窗口中单击“添加”按钮，在添加脚本窗口中，点击浏览，选择步骤4操作的登入脚本文件（ad\_login.exe），并在脚本参数中输入范例 IP:5850，其中 IP 为行为管理设备接口 IP，端口固定为 5850，参数之间以英文字符的冒号分隔，点击应用，再点击确定，一次关闭登入属性页面配置。

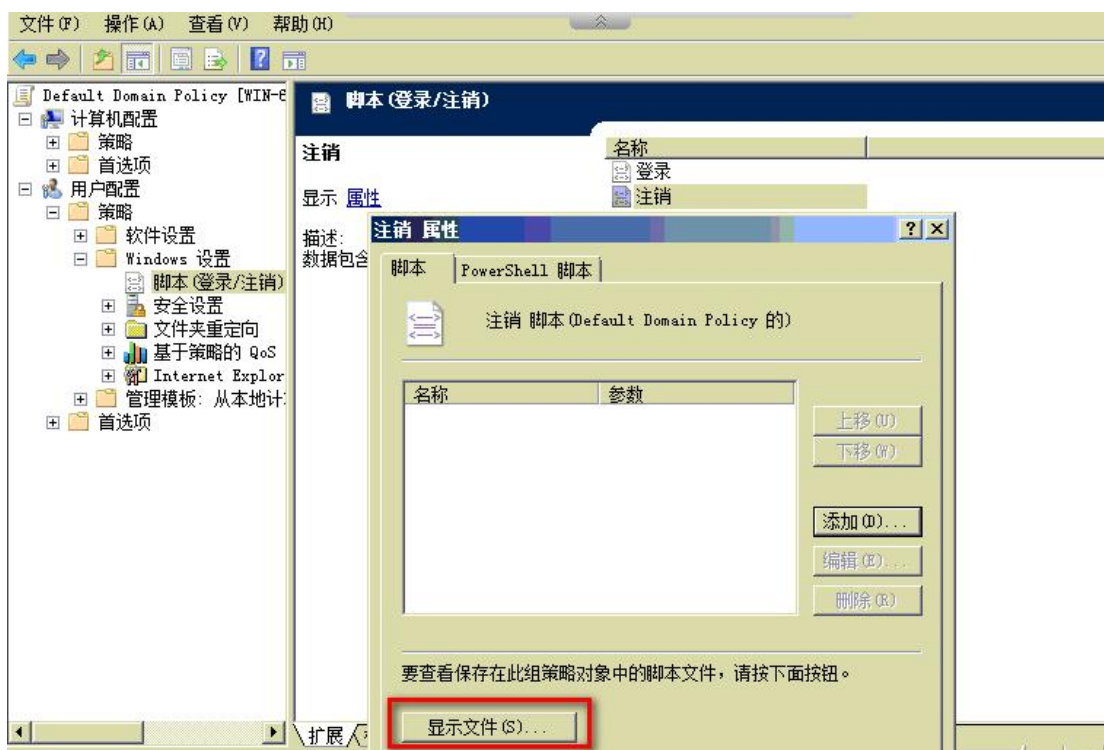


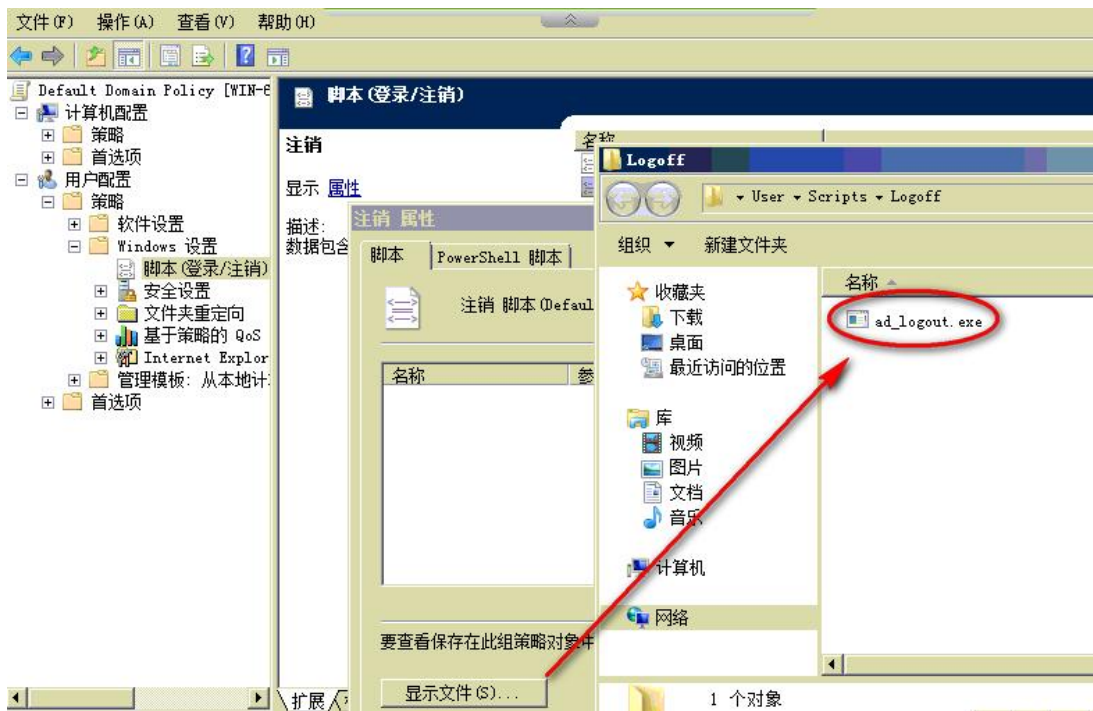
6. 配置完脚本后,依次点击 PC 桌面左下角“开始-运行”,在弹出的运行窗口中输入:“gpupdate /force”更新策略,并点击确定,配置策略生效

7. 登录脚本程序设定 OK,当域用户登录时,该脚本程序通过域下发到 PC 的启动目录,并在该 PC 执行

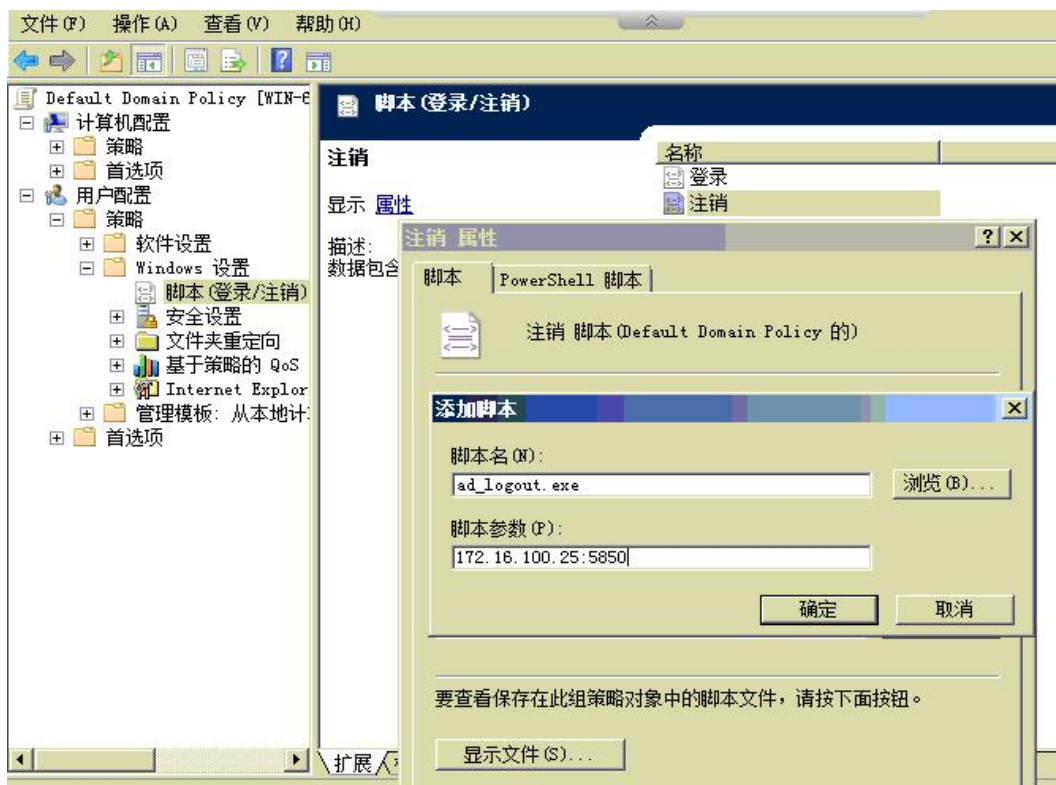
## 2.2 配置注销脚本程序

1. 步骤如上述第 5 步





2. 在弹出的注销脚本编辑窗口中单击“添加”按钮，在添加脚本窗口中，点击浏览，选择步骤 4 操作的注销脚本文件 (ad\_logout.exe)，并在脚本参数中输入范例 IP:5850，其中 IP 为行为管理设备接口 IP，端口固定为 5850，参数之间以英文字符的冒号分隔，点击应用，再点击确定，一次关闭注销属性页面配置。



3. 配置完脚本后,依次点击 PC 桌面左下角“开始-运行”,在弹出的运行窗口中输入:“gpupdate /force”更新策略,并点击确定,配置策略生效

4. 登录脚本程序设定 OK,当域用户登录时,该脚本程序通过域下发到 PC 的启动目录,并在该 PC 执行

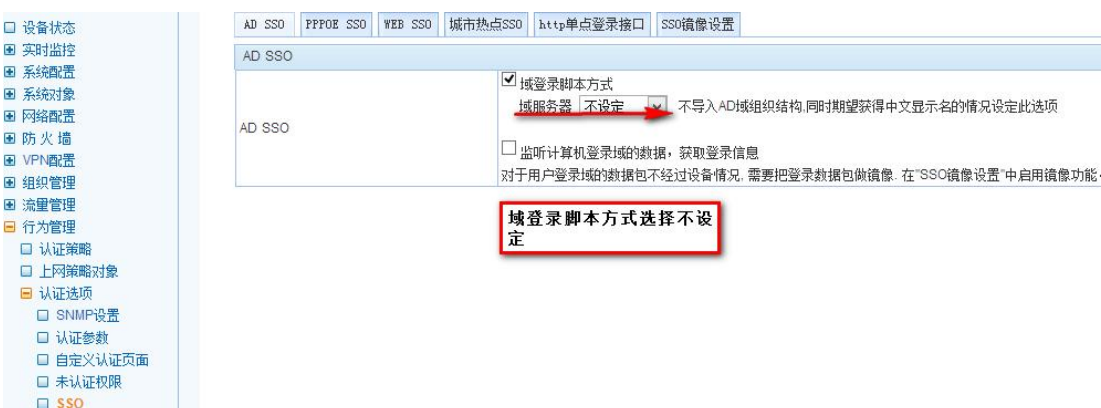
## 三、行为管理网关设置简述

### 1. AD 域用户导入



修改LDAP/AD导入规则	
名称	AD2008
服务器类型	Active Directory
服务器地址	172.16.122.226
服务器端口	389
导入入口(BaseDN)	dc=hytf2013,dc=com
用户查找	<input checked="" type="radio"/> 本地用户查询 <input type="radio"/> 匿名查询
用户名	cn=administrator,cn=users,dc=hytf2013,dc=com
密码	*****
用户名属性字段	sAMAccountName <span style="border: 1px solid red; padding: 2px;">参数默认</span>
显示名属性字段	displayName <span style="border: 1px solid red; padding: 2px;">参数默认</span>
绑定属性字段	绑定格式同组织结构中的绑定格式,多条用","号分开
描述属性字段	
导入目的组	Root/AD2008 <span style="float: right;">选择</span>
自动更新	<input type="checkbox"/> 启用
覆盖原有组织结构	否

### 2. 启用 AD SSO 开关



AD SSO	
域登录脚本方式	<input checked="" type="checkbox"/> 域登录脚本方式 域服务器: 不设定 <span style="border: 1px solid red; padding: 2px;">域登录脚本方式选择不设定</span> 不导入AD域组织结构,同时期望获得中文显示名的情况设定此选项
监听计算机登录域的数据,获取登录信息	<input type="checkbox"/> 监听计算机登录域的数据,获取登录信息 对于用户登录域的数据包不经过设备情况,需要把登录数据包做镜像.在"SSO镜像设置"中启用镜像功能。

行为管理设定完毕, PC 登入登出测试