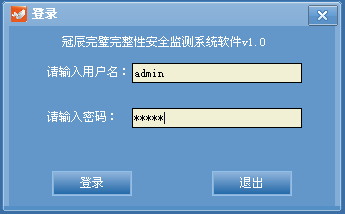
**登录页面 对应数据库 –表Users**



11.进入服务器端控制台主界面，安装完毕

### 对应数据库—表Client（界面的IP地址，需要简单的判断，合符[**IP规则**](http://www.baidu.com/link?url=m_I0L-H2TBn-f_sYWJcpwI6llktluUoBYwYo92O2JcPoxbgVw4i8AuUqP3FNVw7NWpYUuFwB7nDueXeP-JyRv4Bj5s47PXXhrl_WumDUEDe)



## 

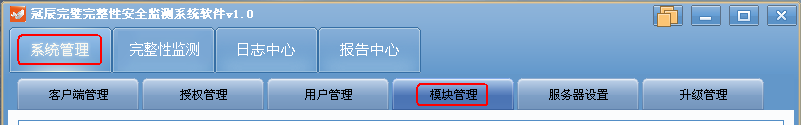
# 三、系统管理

## 3.1 模块管理

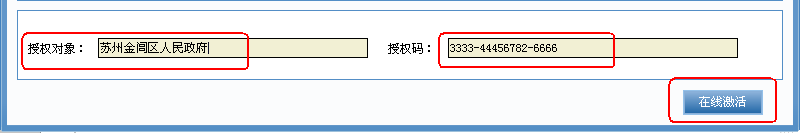
本产品使用前需先进行模块授权，用户购买相应的授权模块并在线激活开通后，相应的产品功能方可使用。具体操作如下：

1. 在主界面中点击系统管理-----模块管理

### 对应数据库-- 表 Module



2.在“授权对象”中输入客户单位名称，“授权码”中输入正确的序列号后，点击在线激活，程序会自动联网访问授权服务器以获取模块授权。



3.授权成功后，在“模块管理”的主界面中显示授权的“模块名称”、“授权码”、“授权点数”、“模块状态”、“授权期限”、“激活时间”等信息。



## 3.2 授权管理

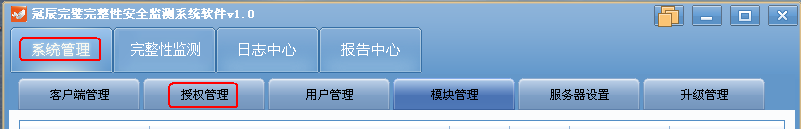
### 3.2.1 新建授权

“授权管理”主要用于对已经安装完璧客户端的主机、网络设备、安全设备进行连接授权以纳入服务器的统一控管。具体操作如下：

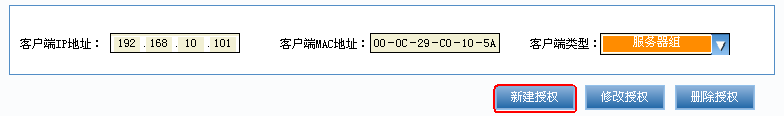
1. 在主界面中点击系统管理-----授权管理

### 对应数据库—表Client（界面的IP地址，需要简单的判断，合符[**IP规则**](http://www.baidu.com/link?url=m_I0L-H2TBn-f_sYWJcpwI6llktluUoBYwYo92O2JcPoxbgVw4i8AuUqP3FNVw7NWpYUuFwB7nDueXeP-JyRv4Bj5s47PXXhrl_WumDUEDe)

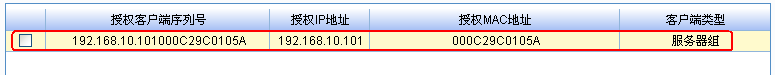
### 界面的MAC地址，合符[**MAC**地址**规则**](http://www.baidu.com/link?url=m_I0L-H2TBn-f_sYWJcpwI6llktluUoBYwYo92O2JcPoxbgVw4i8AuUqP3FNVw7NWpYUuFwB7nDueXeP-JyRv4Bj5s47PXXhrl_WumDUEDe)）



2.输入客户端IP地址、客户端MAC地址、客户端类型，再点击“新建授权”即可添加授权



3.添加授权成功后，会在授权管理主界面显示授权主机的“客户端序列号”、“授权IP地址”、“授权MAC地址”、“客户端类型”等基本信息。

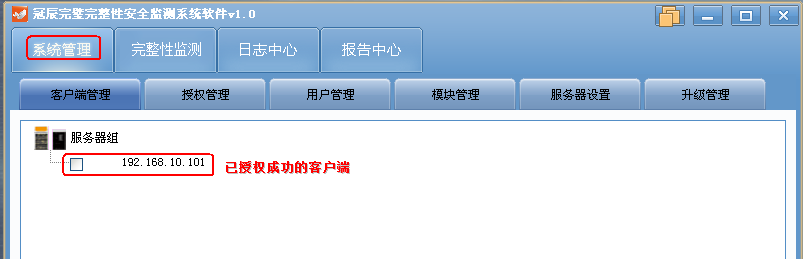


### 

## 3.3 客户端管理

客户端授权成功后，能够在“客户端管理”界面查看到基本信息，操作如下：

1.在主界面中点击系统管理-----客户端管理



2.通过勾选，可以显示该客户端的基本信息



客户端名称：在“客户端管理”中的显示名称，可修改，默认为IP地址

备注名称：对客户端进行备注标示，可修改，默认为空

客户端类型：客户端进行授权时所选择的类型，可修改

客户端状态：客户端的当前状态（启用或禁止），可修改，默认为启用

客户端IP地址：客户端进行授权时所输入的IP地址，不可修改

客户端MAC地址：客户端进行授权时所输入的MAC地址，不可修改

## 3.4 用户管理

用户管理界面主要负责管理与设置服务器端的账户，默认情况只有拥有完全控制权限的admin账户，该账户只允许修改密码，不允许删除。添加或删除账户的操作如下：

### 3.4.1 修改密码

1.在主界面中点击系统管理-----用户管理

用户管理对应数据库 – 表 users

//用户权限

enum

{

UserPermission\_IntegrityGuard = 0x01, //完整性监测

UserPermission\_SafeReinforce = 0x02, //安全加固（此功能界面暂没有）

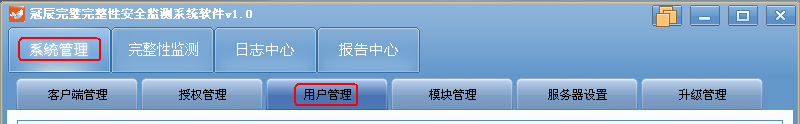
UserPermission\_LogCenter = 0x04, //日志中心

UserPermission\_ReportCenter = 0x08, //报告中心

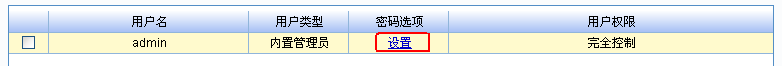
UserPermission\_Safetools = 0x10, //安全工具（此功能界面暂没有）

};

**界面的CHECK选项 值，按或取值 对应数据字段permission**



2.选择需要修改的用户名，点击密码选项中的设置按钮

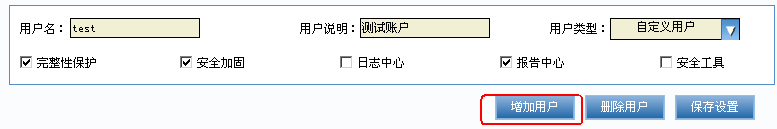


3.输入新的密码，点击确定按钮



### 3.4.2 增加用户

1.在“用户管理”界面下方输入新增用户基本信息，点击增加用户按钮



用户名：新建的用户名称

用户说明：描述性的标记语句

用户类型：可以选择“自定义用户”还是“管理员用户”

完整性监测：是否赋予新用户“完整性监测”的操作权限

日志中心：是否赋予新用户“日志中心”的操作权限

报告中心：是否赋予新用户“报告中心”的操作权限

2.添加成功后，可在“用户管理”界面查看到新增用户



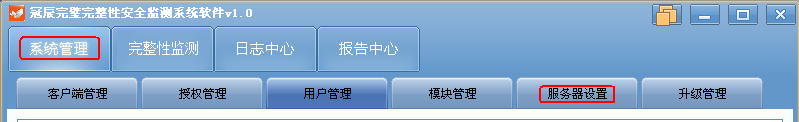
### 

## 3.5 服务器设置

服务器设置界面主要用于让用户修改服务器通讯端口、数据端口数值和退出客户端时的终止密码，具体操作如下：

### 3.5.1 修改通讯端口

1.在主界面中点击系统管理-----服务器设置



1. 输入新的服务器通讯端口（范围为0~65535），点击“应用配置”按钮

应用设置 和后台服务消息交互 消息号OPERATION\_SET\_SERVER\_CONFIG

消息结构体：typedef

struct \_ServerSetConfigInfo

{

DWORD dwDataPort;

DWORD dwCommandPort;

WCHAR szClientPassword[21];

}ServerSetConfigInfo, \*PServerSetConfigInfo;

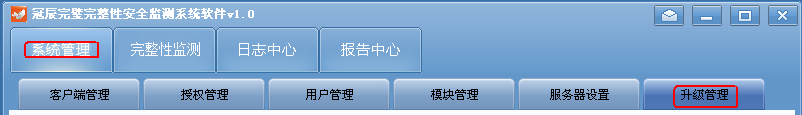


## 3.6 升级管理

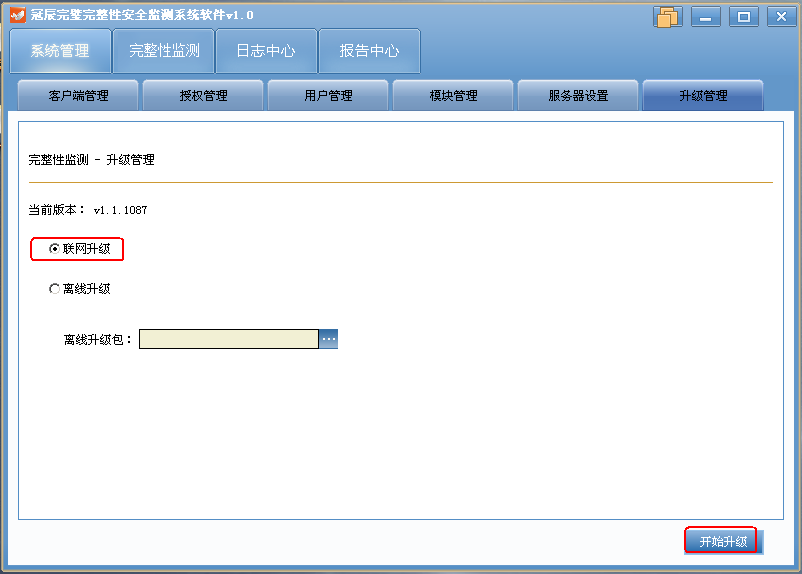
升级管理界面主要用于系统程序版本更新，升级方式有联网升级和离线升级两类，具体操作方式如下：

### 3.6.1 联网升级

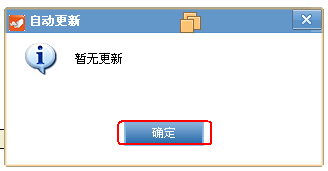
1.在主界面中点击系统管理-----升级管理（需当面交流）



2.选择“联网升级”，点击“开始升级”



3.更新完成后，系统会弹出确认对话框，单击“确定”按钮



### 3.6.2 离线升级

1.选择“离线升级”，点击“离线升级包”选择按钮，



2. 浏览本地磁盘定位升级文件，确定后点击“开始升级”按钮



# 四、完整性监测

## 4.1 策略对象

Regstrategytable 注册表

Appstrategytable app

Equipstrategytable 设备

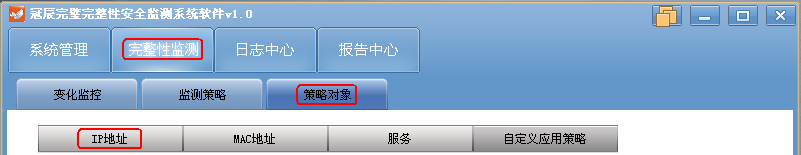
策略对象的元素涉及IP地址、MAC地址、服务等，通过让用户灵活的进行自定义，再弹性的应用到各类自定义策略中，使得策略更加符合用户定制化需求。

### 4.1.1 IP地址

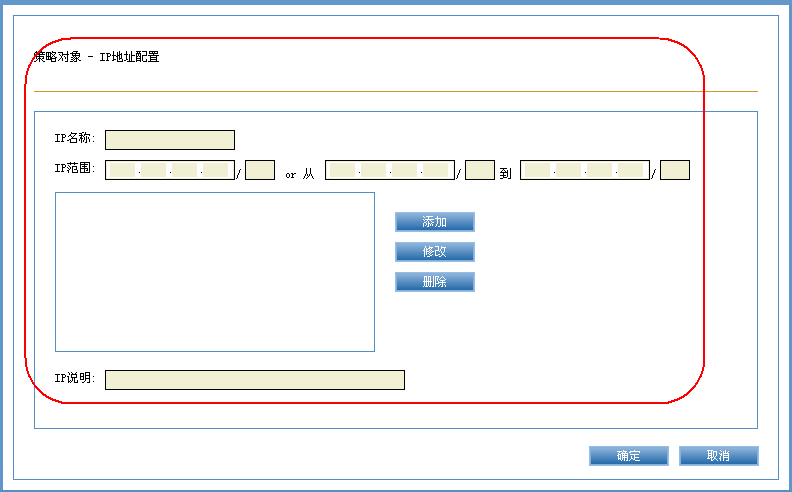
#### 4.1.1.1 添加IP地址

1.在主界面中点击完整性监测-----策略对象-----IP地址

对应数据库—表IPAddressTable

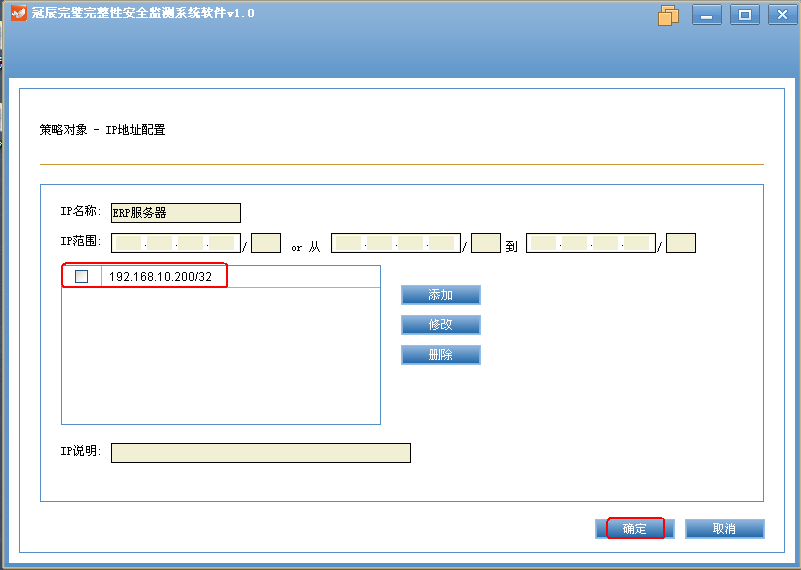
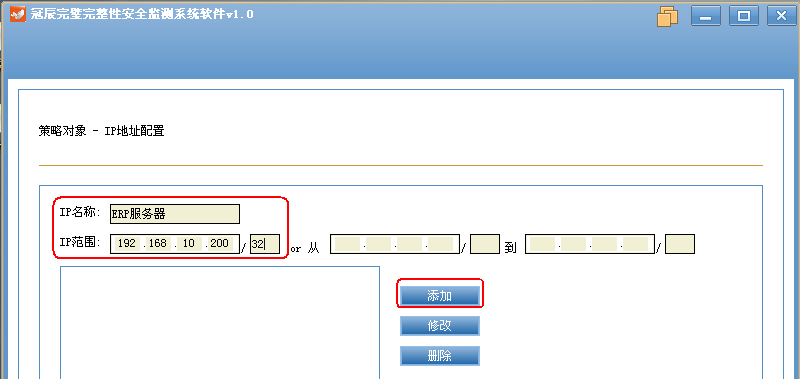


2.点击“添加”按钮以新增一个IP地址对象



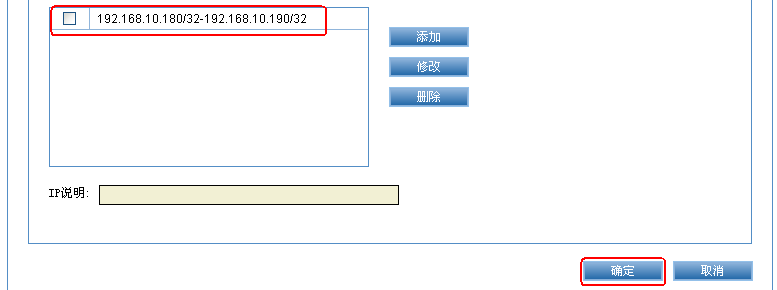
##### 4.1.1.1.1 添加单个地址

添加单个IP地址如下图所示：



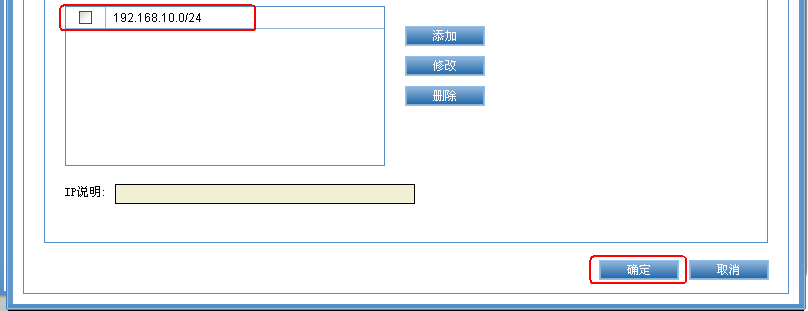
##### 4.1.1.1.2 添加地址范围

添加地址范围如下图所示：



##### 4.1.1.1.3 添加地址网段

添加地址段如下图所示：

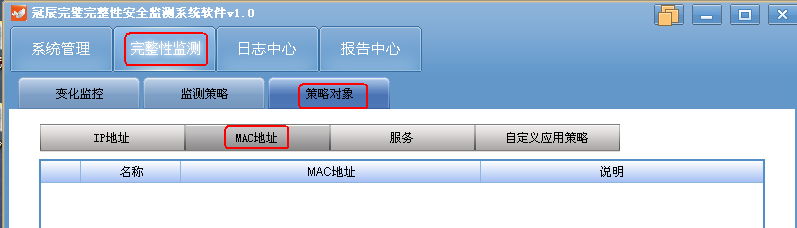


### 4.1.2 MAC地址

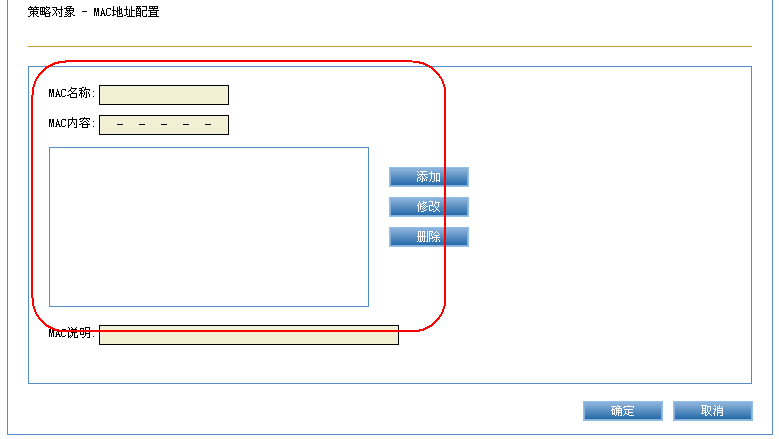
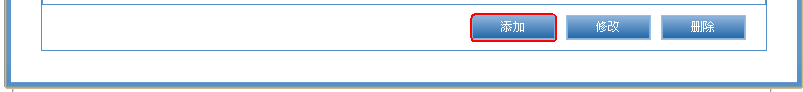
#### 4.1.2.1 添加MAC地址

对应数据库 –表MacAddressTable

1.在主界面中点击完整性监测-----策略对象-----MAC地址

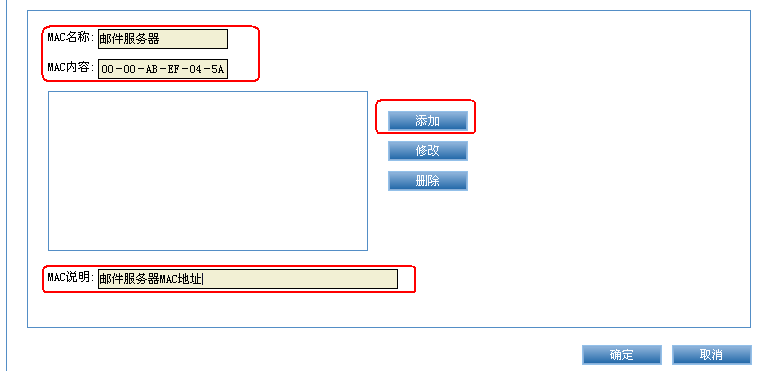


2.点击添加按钮以新增加一个MAC地址对象

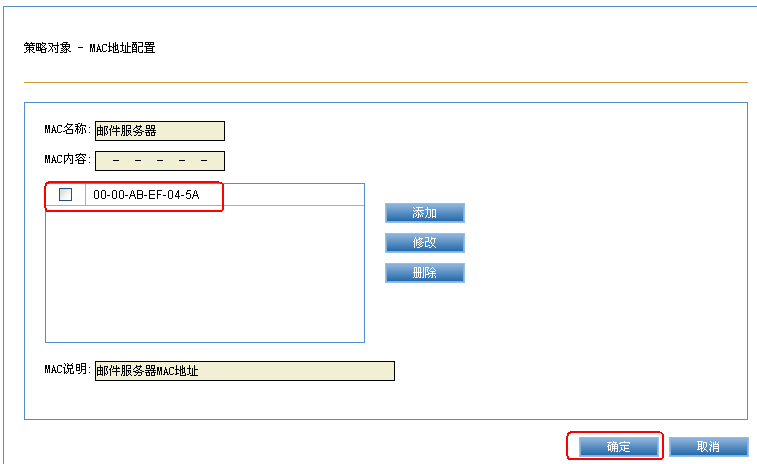


##### 4.1.2.1.1 增加单个MAC地址

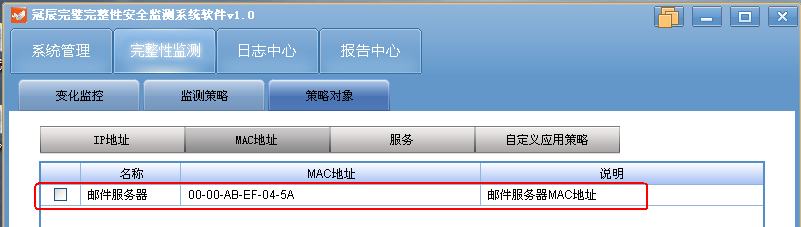
1.输入MAC地址名称、说明和内容后，单击“添加”按钮



2.添加完成后，点击确定按钮



3.在添加MAC地址主界面，新增MAC已在列表中

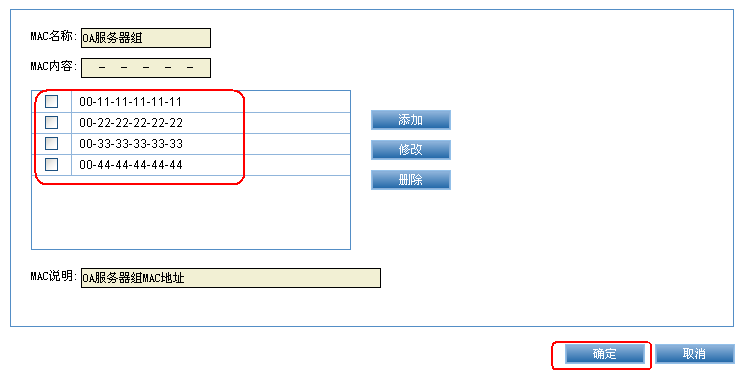


##### 4.1.2.1.2 添加多个MAC地址

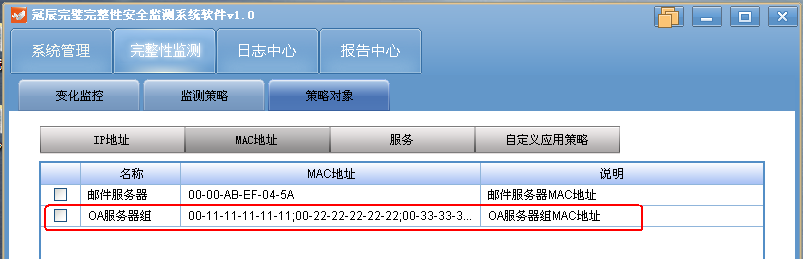
1.依次输入多个MAC地址，单击“添加”按钮



2.输入完毕后，单击“确定”按钮



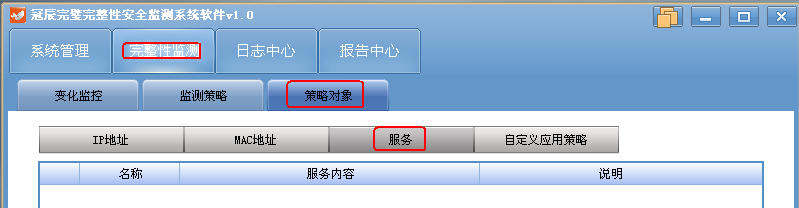
3.在添加MAC地址主界面，新增MAC组已在列表中



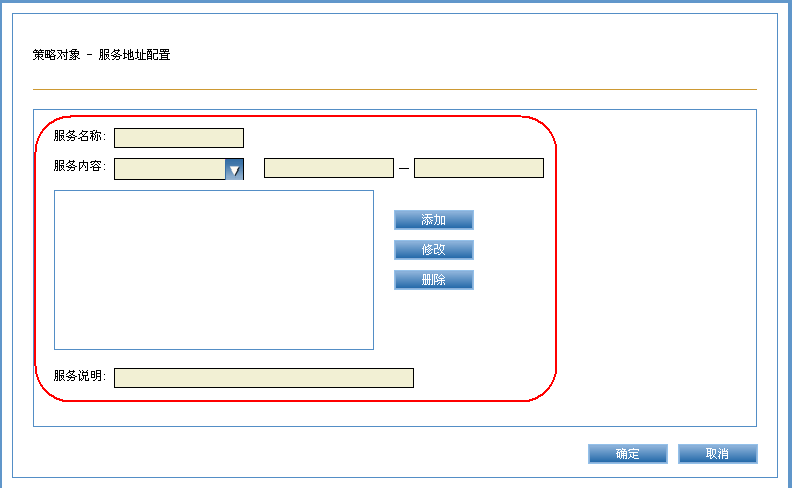
#### 4.1.3.1 添加服务

1.在主界面中点击完整性监测-----策略对象-----服务

对应数据库—表SeverStrategyTable

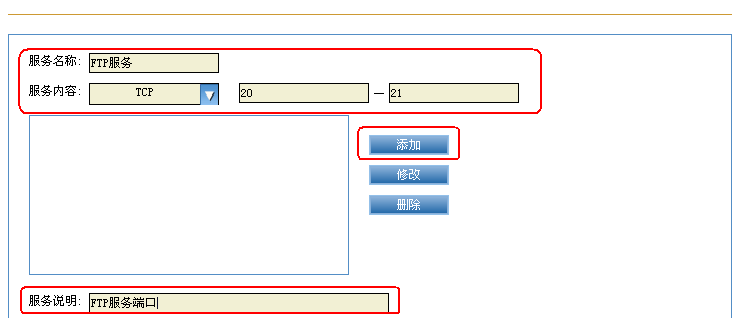


2.点击添加按钮以新增加一个服务对象

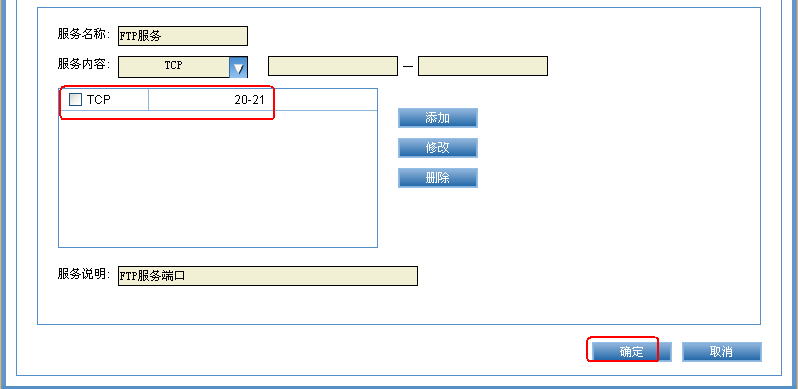


##### 4.1.3.1.1 添加单个服务

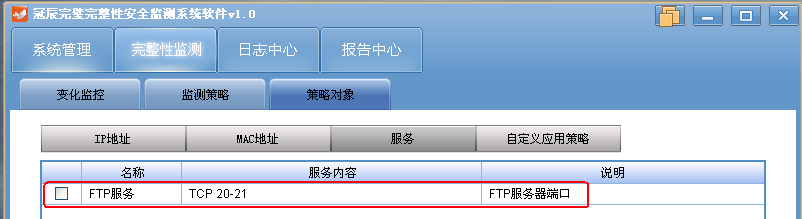
1.输入服务名称、说明和内容后，单击“添加”按钮



2.添加完成后，点击确定按钮

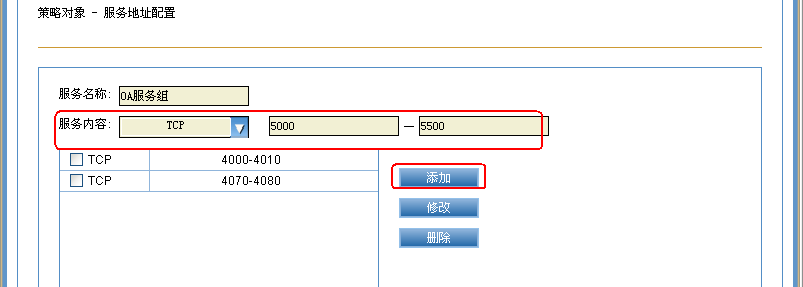


3.在添加服务主界面，新增服务已在列表中

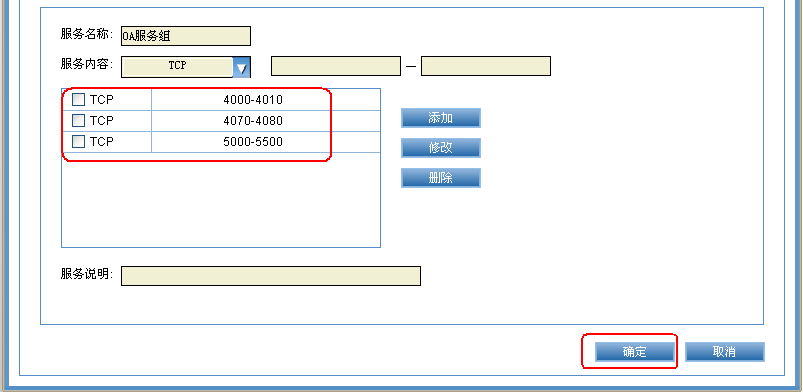


##### 4.1.3.1.2 添加多个服务

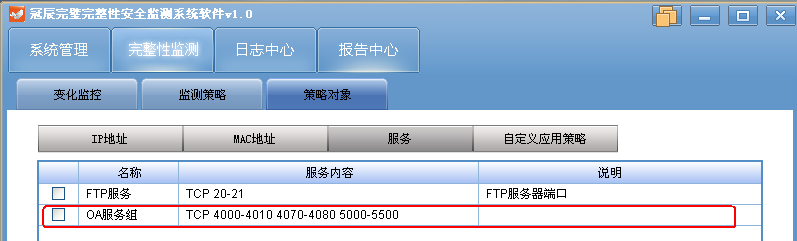
1.依次输入多个服务端口，单击“添加”按钮



2.输入完毕后，单击“确定”按钮



3.在添加服务主界面，新增服务组已在列表中

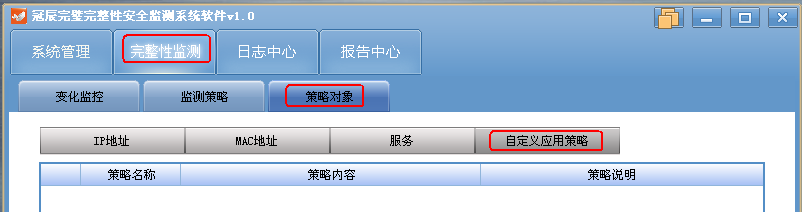


### 4.1.4 自定义应用策略

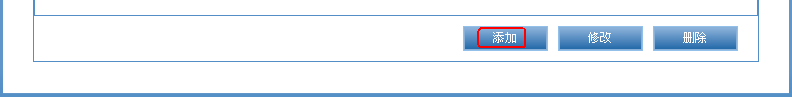
##### 4.1.4.1 添加自定义应用策略

1.在主界面中点击完整性监测-----策略对象-----自定义应用策略

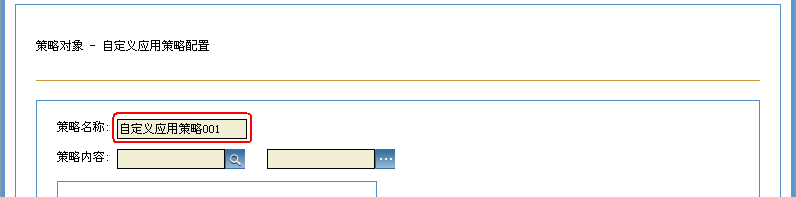
对应数据库—表AppStrategyTable



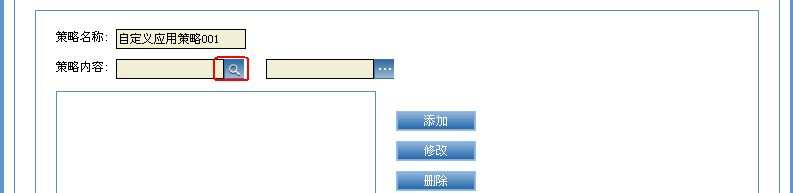
2.点击添加按钮以新增加一个自定义应用策略



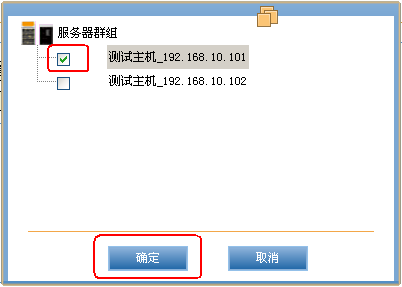
3.填写自定义策略名称



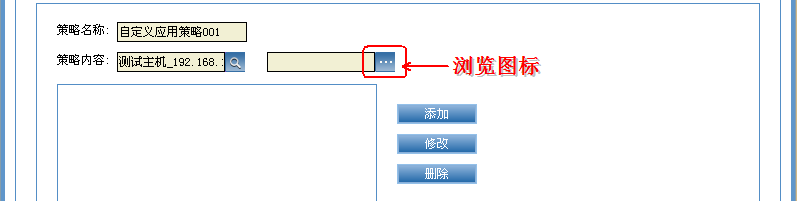
4.点击搜索图标，系统将会跳出对话框让用户选择策略对象（*策略对象的创建见3.2.1小节新建授权*）



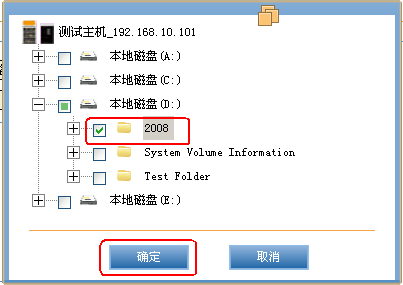
5.勾选需要执行自定义策略的主机，单击确定按钮



6.点击浏览图标以选择策略对象中的具体内容



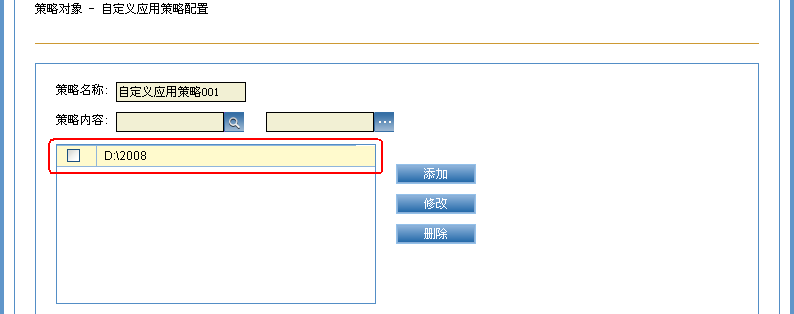
7.浏览策略对象主机中需要进行保护的目录，完成后单击“确定”按钮



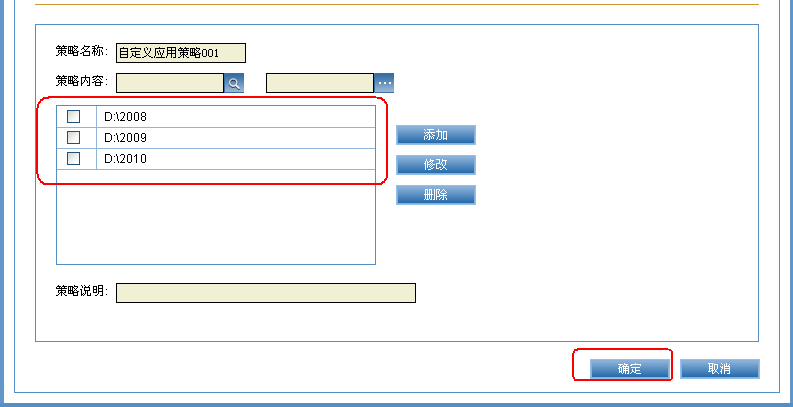
8.选择完策略对象主机和所对应的保护目录后单击“添加”按钮



9.添加成功后，我们可以在列表框中看见刚才所添加的策略。



10.重复步骤4-8以添加不同的策略对象主机和策略内容到同一个自定义的应用策略中，添加完毕后单击确定按钮。

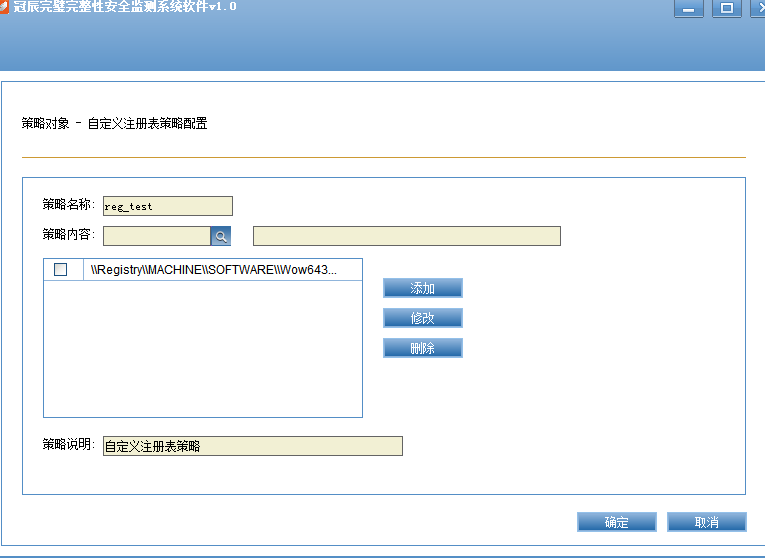
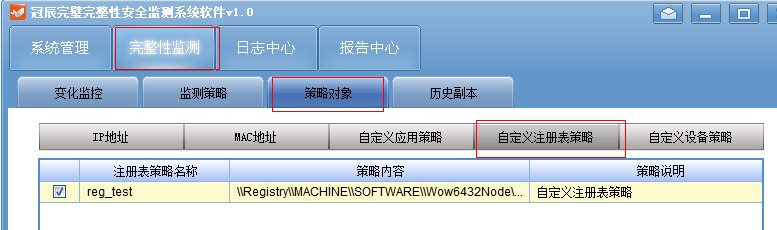


11.在“自定义应用策略”主界面，可以看到刚才添加的策略（*重复步骤1-10以添加不同的自定义应用策略*）



1.在主界面中点击完整性监测-----策略对象-----自定义注册表

对应数据库—表RegStrategyTable



1.在主界面中点击完整性监测-----策略对象-----自定义设备策略

对应数据库—表EquipStrategyTable



## 4.2 监测策略

### 4.2.1 系统默认策略

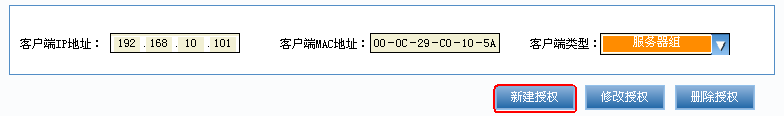
#### 4.2.1.1 添加系统默认策略

通过3.2.1小节新建授权后，本程序会自动添加一个针对授权对象的系统默认策略（*默认策略内容为操作系统完整性监测策略*），操作如下：

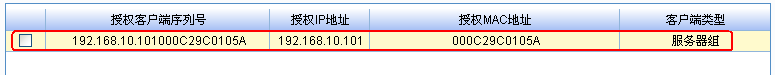
1.在主界面中点击系统管理-----授权管理



2.输入客户端IP地址、客户端MAC地址、客户端类型，再点击“新建授权”即可添加授权



3.添加授权成功后，会在授权管理主界面显示授权主机的“客户端序列号”、“授权IP地址”、“授权MAC地址”、“客户端类型”等基本信息。



4.在完整性监测--监测策略主界面，能看到系统针对该授权对象添加的系统默认策略



#### 4.2.1.2 修改系统默认策略

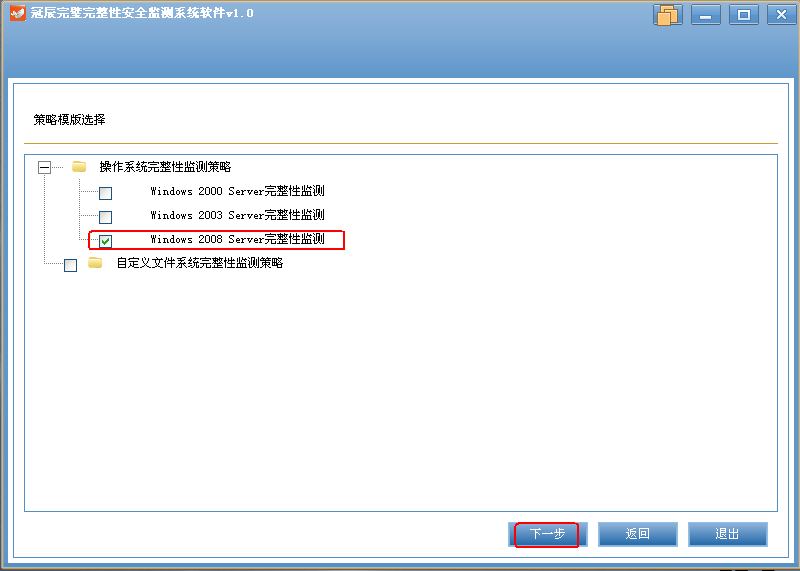
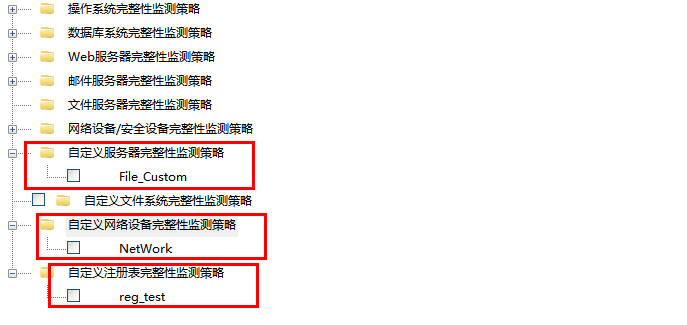
**对应数据库 -- 表StrategyTable**

1.在完整性监测--监测策略界面，勾选需要修改的系统默认策略，单击修改策略按钮

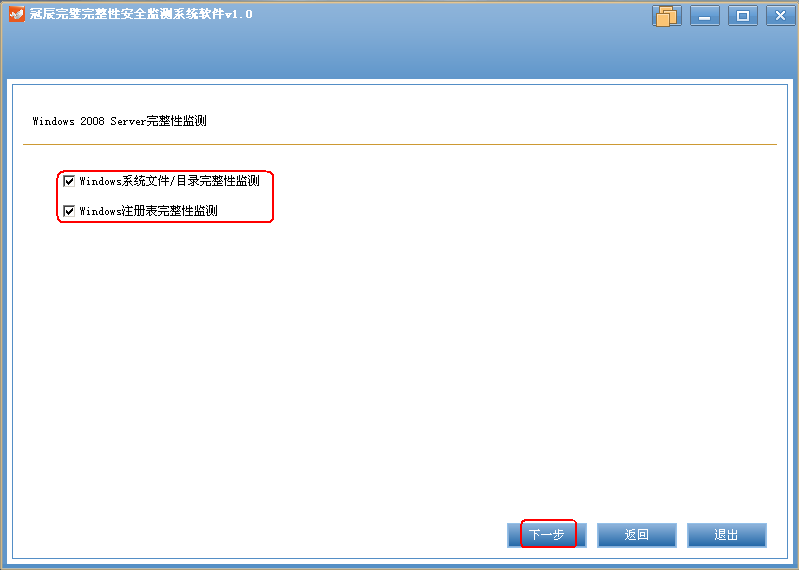


1. 选择需要保护的操作系统环境，单击下一步按钮

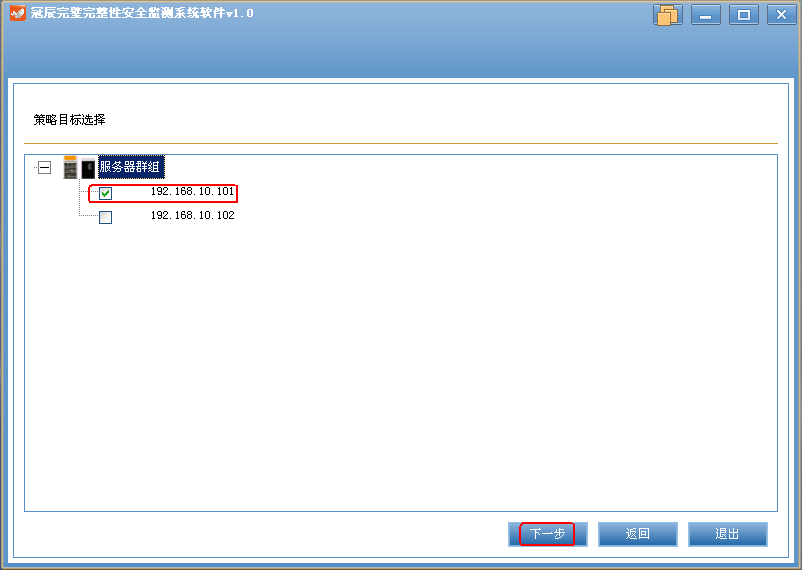
此界面对应多个策略对象记录 如：树型目录树子目录包括 表AppStrategyTable，EquipStrategyTable，RegStrategyTable



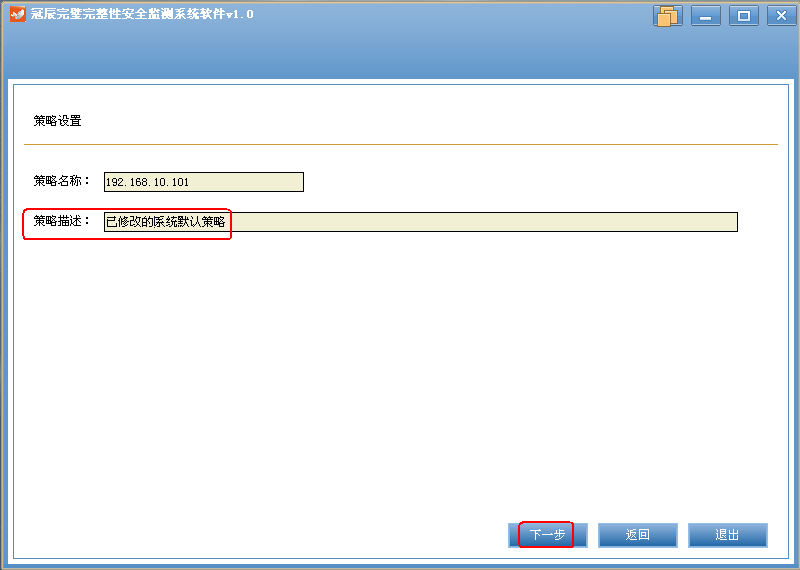
3.选择操作系统完整性监测策略需要保护的内容，单击下一步按钮



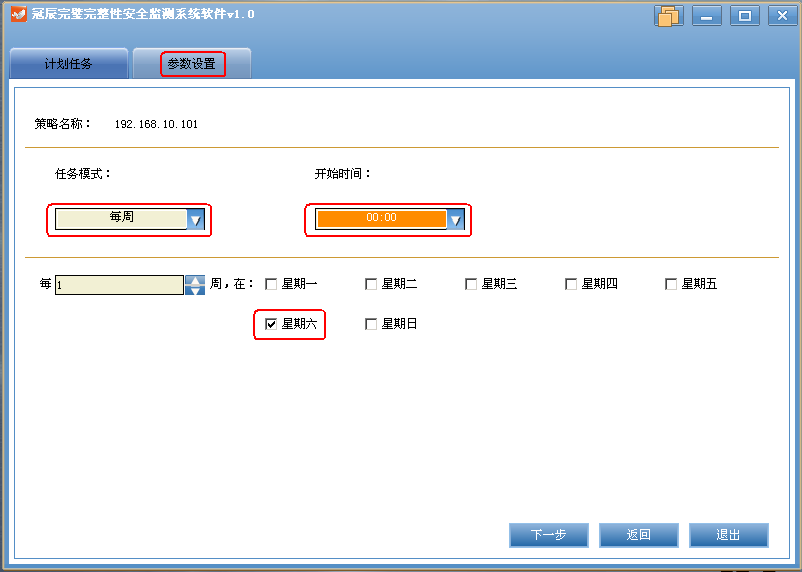
4.对策略保护的目标对象进行选择，单击下一步按钮：



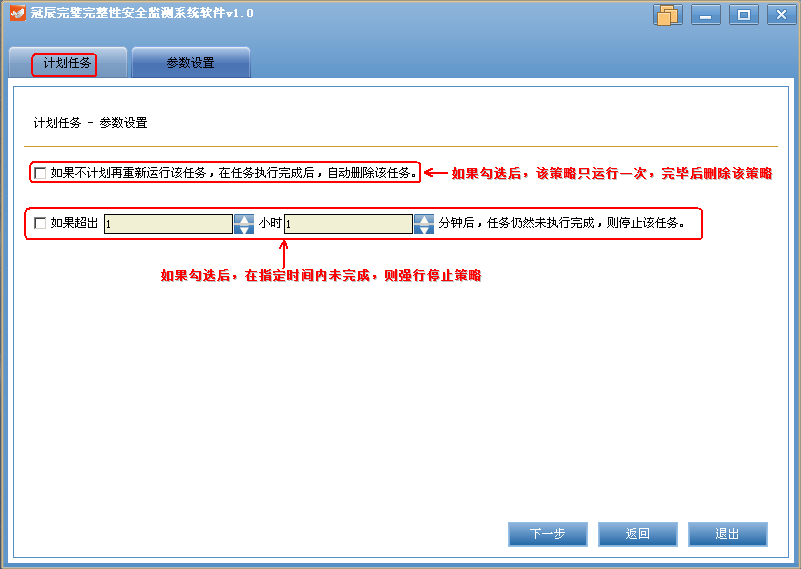
5.对策略进行名称和内容描述，单击下一步按钮



6.选择策略的执行周期，单击参数选择按钮，进行扩展参数配置



7.根据自身需要进行扩展参数配置，配置完后单击下一步按钮



### 4.2.4 自定义文件系统完整性监测策略

#### 4.2.4.1 新建自定义文件系统完整性监测策略

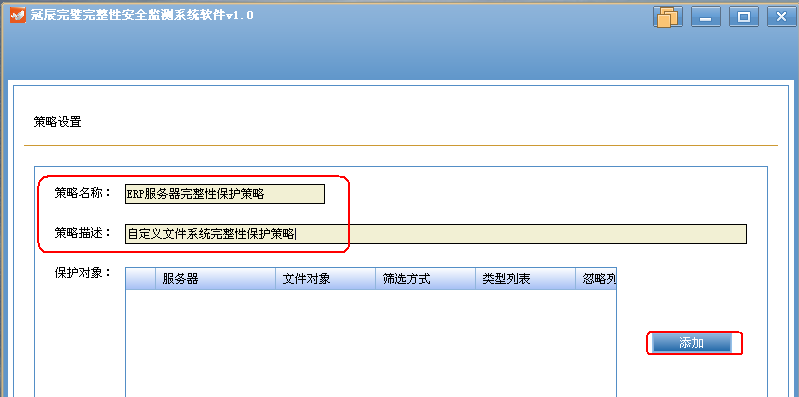
1.在完整性监测--监测策略主界面，点击新建策略按钮



2.勾选自定义文件系统完整性监测策略，单击下一步按钮



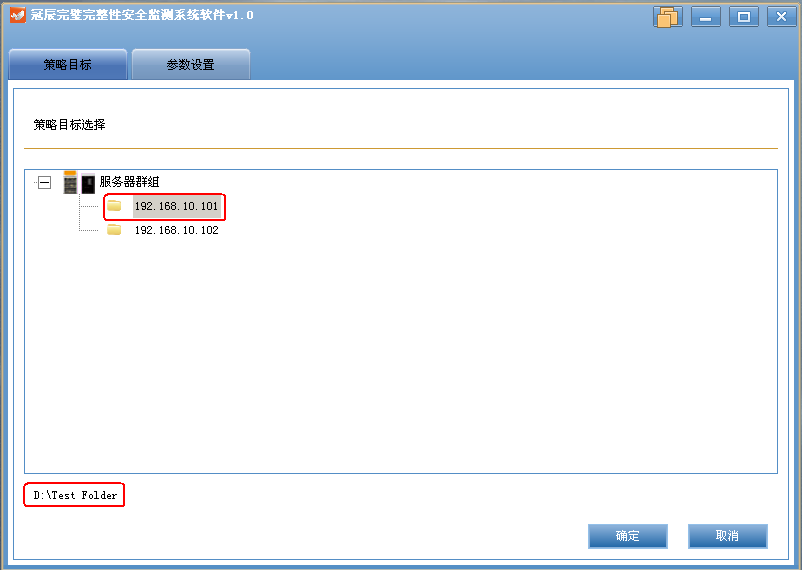
3. 输入策略名称和相应的描述信息，单击添加按钮



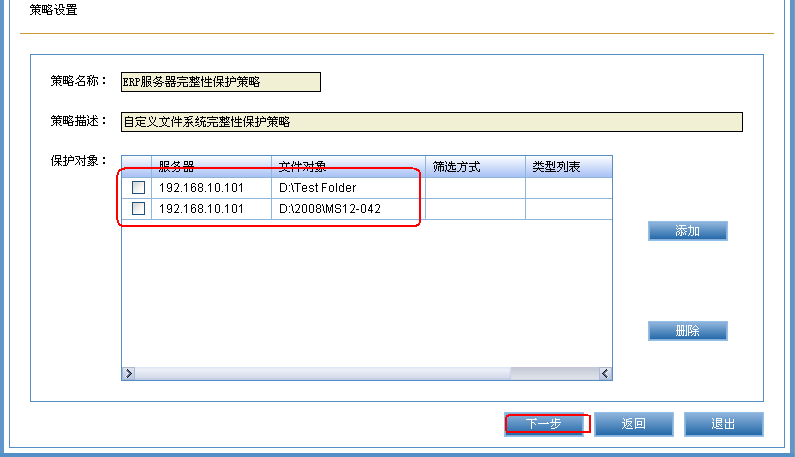
1. 选择需要进行文件完整性监测的目标主机和目标文件夹后单击确定按钮



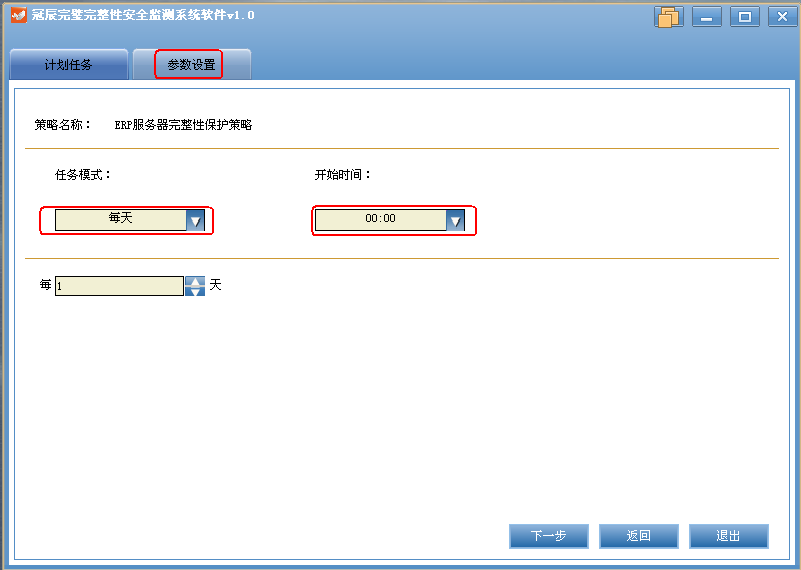
5.对选择的目标和保护目录进行再次确认，后单击确定按钮



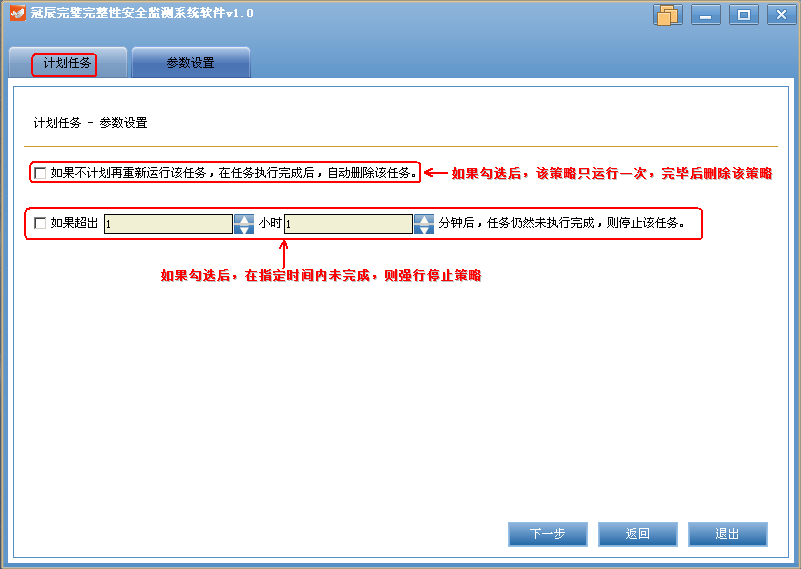
6.根据实际情况重复动作3-4，添加多个保护目录后，单击下一步按钮



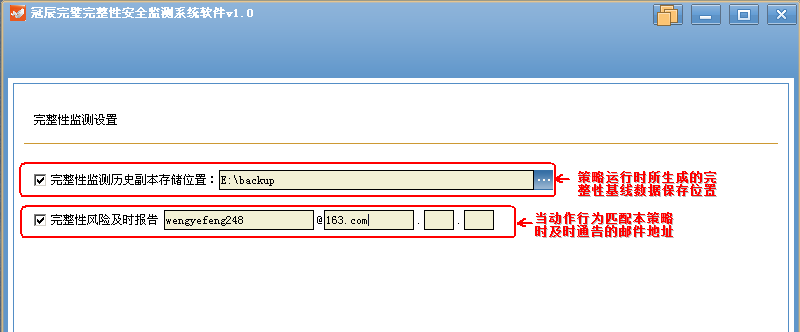
7.选择策略的执行周期后，单击参数选择按钮，进行扩展参数配置



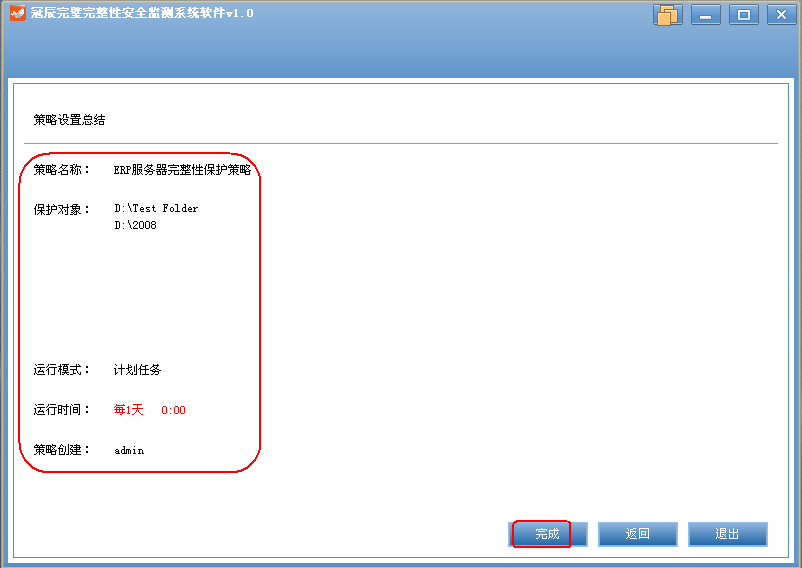
8. 根据自身需要进行扩展参数配置，配置完后单击下一步按钮



9.针对该策略进行完整性监测设置，配置完毕后点击完成按钮



10.对策略汇总信息进行确认，无误后点击完成按钮



11.完整性监测-监测策略主界面可以看到新建的自定义文件系统完整性监测策略

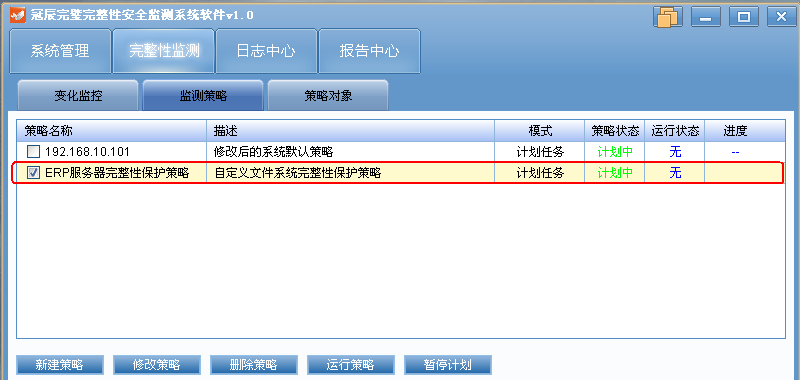
**新建完策略，发送SERVER\_STRATEGYGUARD\_ADD 消息 至服务端，具体消息格式参照备注**

**（修改，删除策略均需发消息至服务端 ）**

**SERVER\_STRATEGYGUARD\_ADD, //新增策略 （新加）**

**SERVER\_STRATEGYGUARD\_DELETE, //删除策略**

**SERVER\_STRATEGYGUARD\_MODIFY, //修改策略**



### 4.2.6 策略相关操作

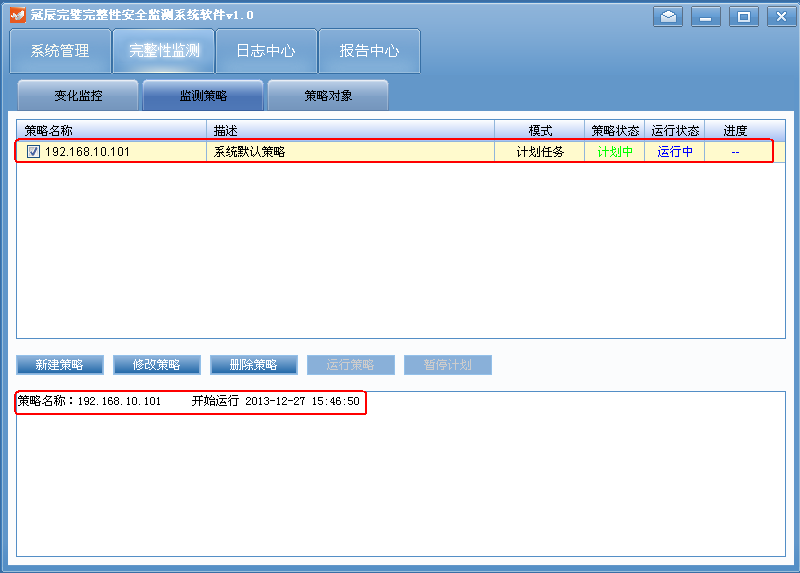
#### 4.2.6.3 运行策略

1.在完整性监测--监测策略主界面，勾选需要运行的策略，单击运行策略按钮

**策略运行 消息SERVER\_STRATEGYGUARD\_START**



2.策略处于运行状态



1. 策略运行完毕后

这个UI需要处理消息SERVER\_STRATEGYOBJECT\_STATUSNOTIFY //策略运行状态

提醒

typedef struct \_STRATEGY\_RUNSTATUS

{

DWORD Status;1:开始运行，2：运行成功，3：失败

WCHAR StrategyName[64];

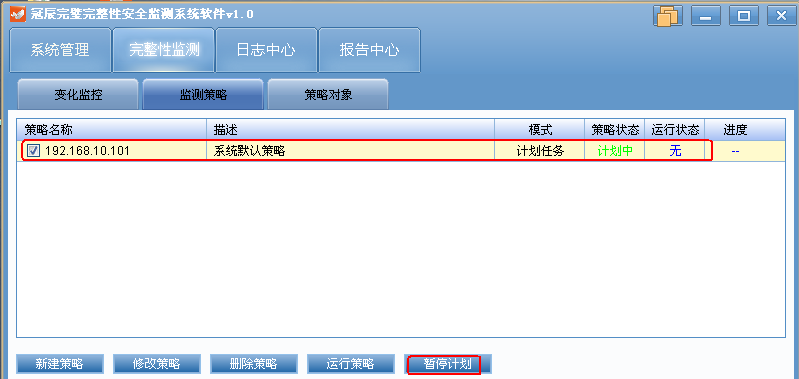
WCHAR FailReason[MAX\_PATH];

}STRATEGY\_RUNSTATUS,\*LPSTRATEGY\_RUNSTATUS;



#### 4.2.6.4 暂停计划

1.在完整性监测--监测策略界面，勾选需要暂停计划的策略，点击暂停计划按钮



2.程序显示计划暂停，可以根据实际需要点击恢复计划按钮以运行计划



## 4.3 变化监控

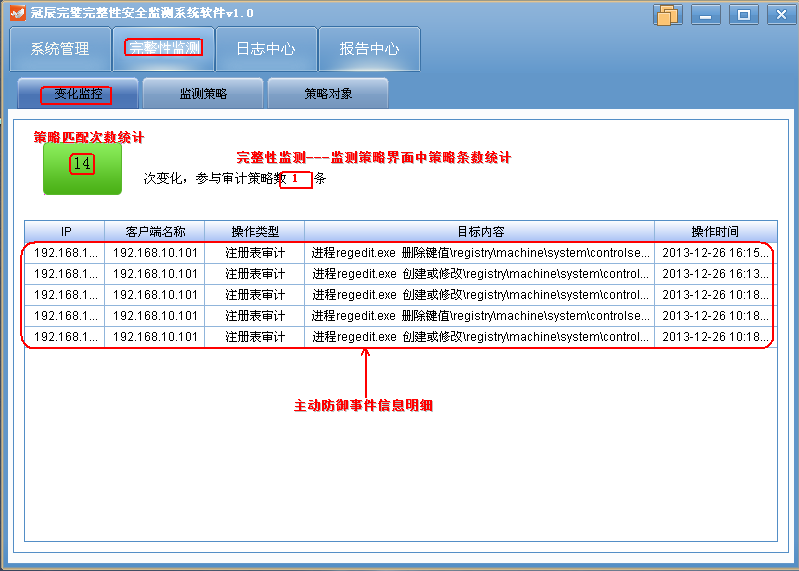
### 4.3.1 变化监控工作原理

变化监控主要监控以下内容：

1.在完整性监测--监测策略界面中审计策略条数统计

### 4.3.2 变化监控实例讲解

**对应 数据库—表HIPSLog**

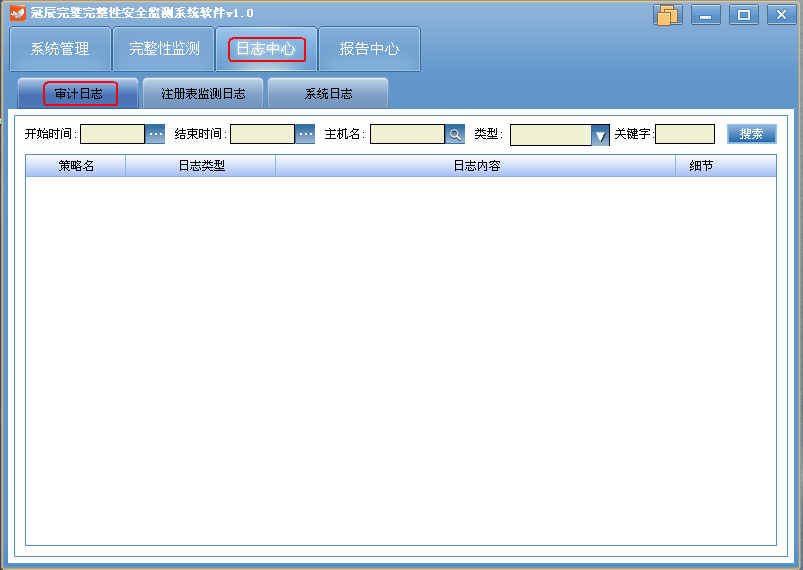


# 五、日志中心

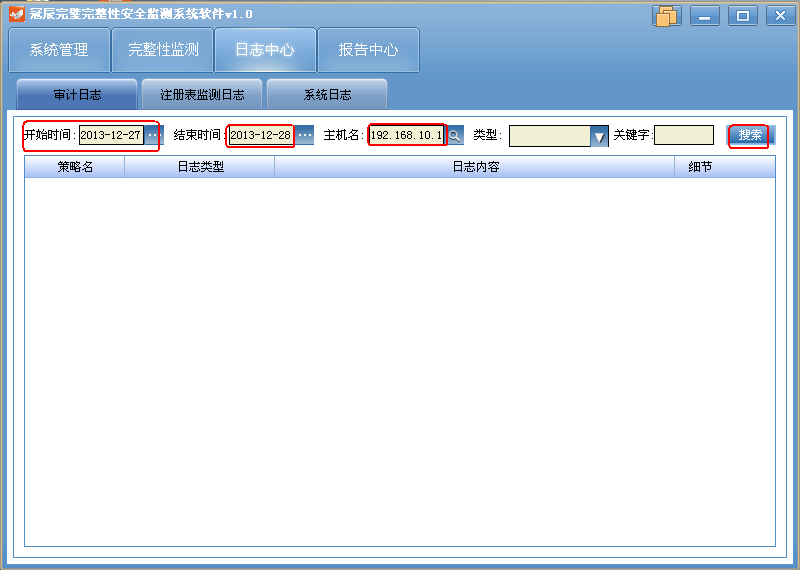
## 5.1 审计日志

1.在日志中心--审计日志页面，可以对特定主机的历史审计信息进行查询

审记日志对应数据库 -- AuditLog



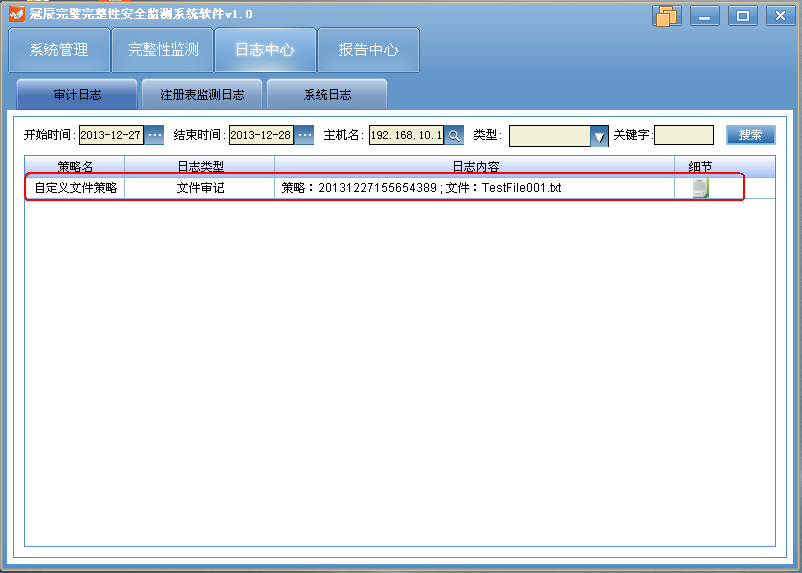
2.输入开始时间、结束时间、主机对象、日志类型等信息，点击搜索按钮



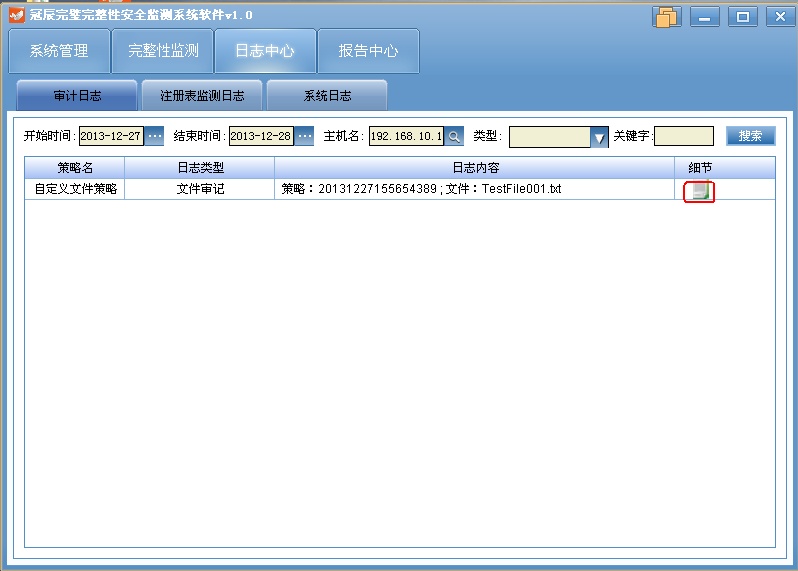
3.出现提示框，单击确定按钮，继续执行搜索



4.系统会从数据库中按照搜索要求检索数据，并进行显示



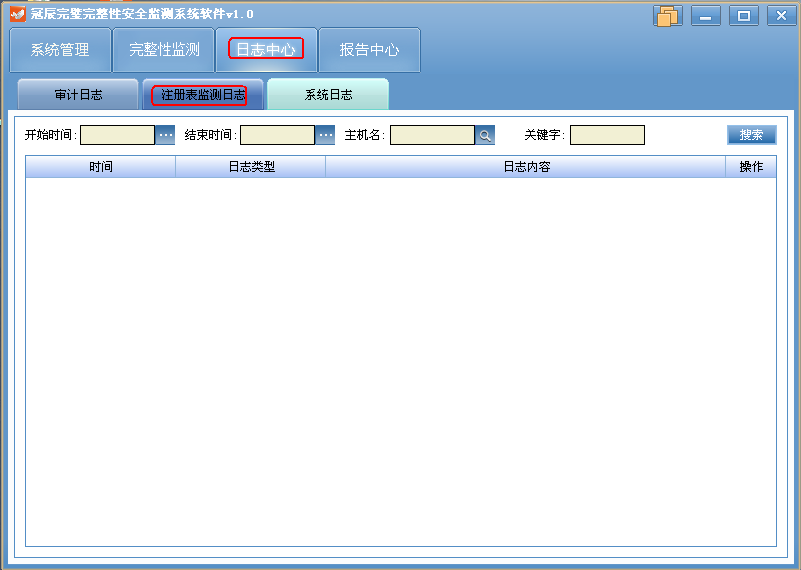
5.针对某条记录，单击细节按钮以显示更多信息



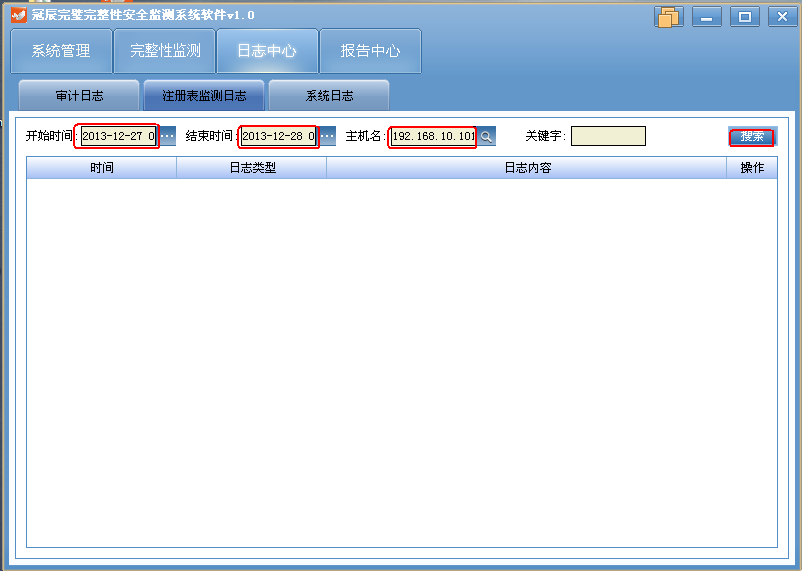
## 5.2 注册表监测日志

1.在日志中心--注册表监测日志页面，可以对特定主机的注册表监测信息进行查询

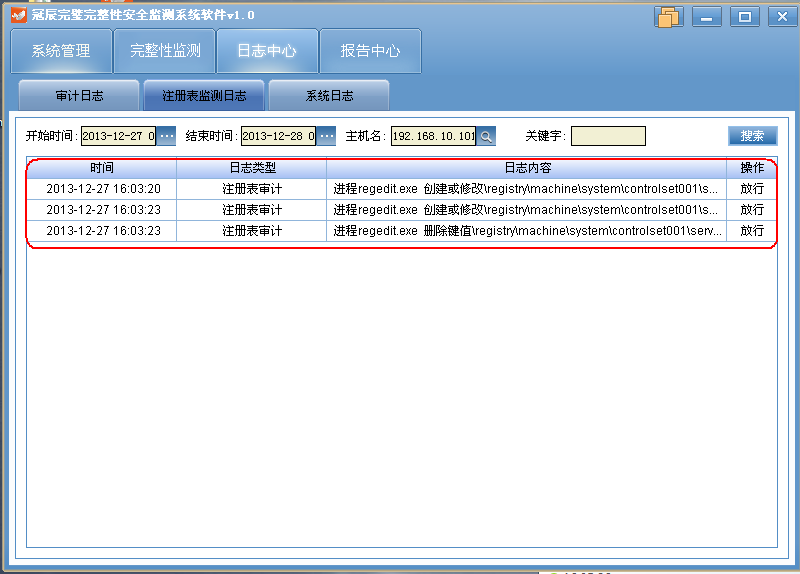
对应数据库HIPSLog



2.输入开始时间、结束时间、主机名、关键字等信息，点击搜索按钮



3.系统会从数据库中按照搜索要求检索数据，并进行显示



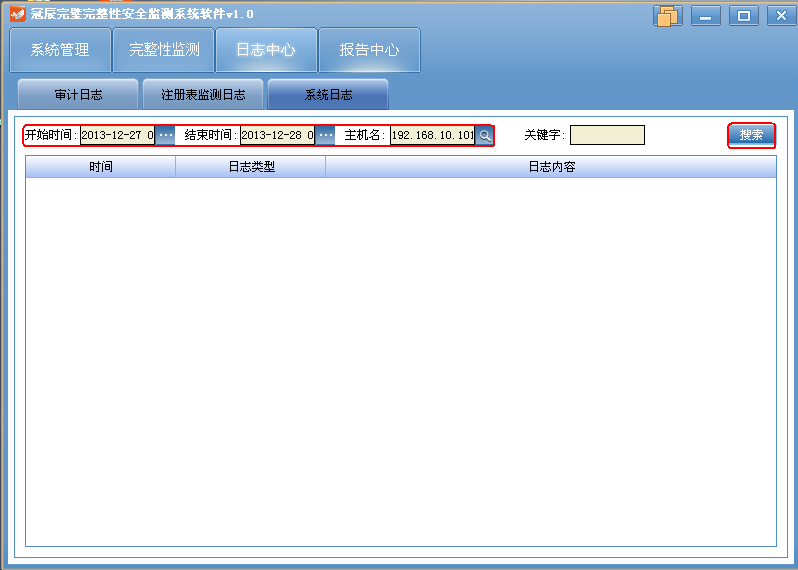
## 5.3 系统日志

1.在日志中心--系统日志页面，可以对特定主机的系统日志进行查询

**对应数据库SystemLog**



2.输入开始时间、结束时间、主机名、关键字等信息，点击搜索按钮



4.系统会从数据库中按照搜索要求检索数据，并进行显示



# 六、报告中心

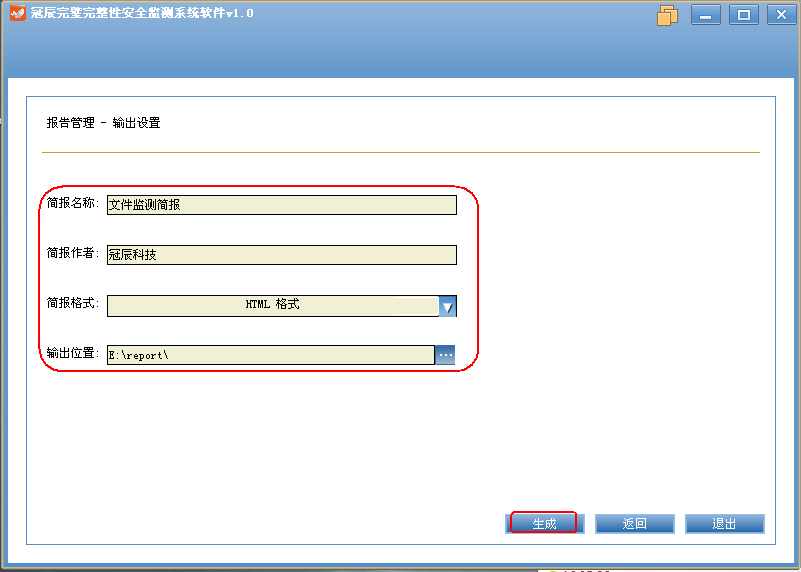
## 6.1 生成简报

本系统策略执行后，会自动保存策略执行情况信息，可以利用这些数据生成简报以便于查询

1. 在报告中心--报告管理页面，勾选要生成简报的策略执行信息记录，点击生成简报按钮
2. **对应数据库ReportCenterTable**



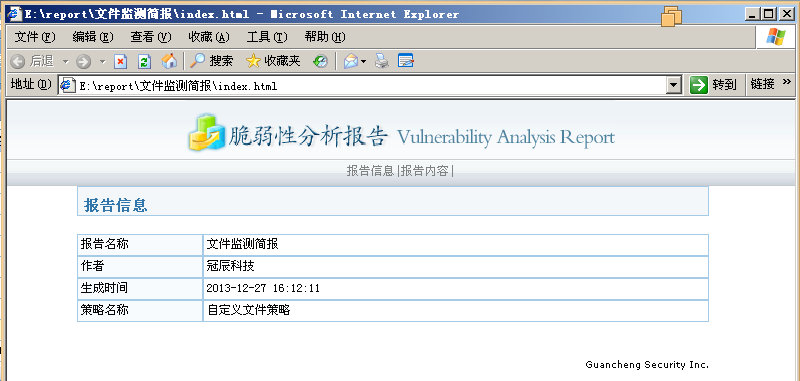
2.进行简报输出的相关设置，单击生成按钮



3. 系统生成报告，并进行存储



4. 存储完成后，程序自动打开报告页面

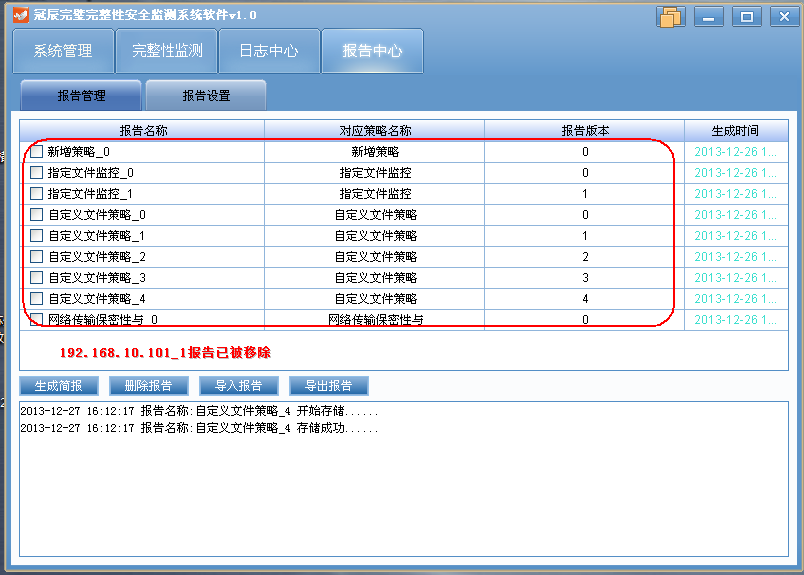


## 6.2 删除报告

1.在报告中心--报告管理页面，勾选需要删除的报告，单击删除报告按钮



2.删除成功后，该报告从报告中心--报告管理页面被移除



## 6.3 导出报告

1.报告中心--报告管理页面，勾选需要导出报告，单击导出报告按钮



2.选择报告的存储位置，单击保存，即可导出报表



## 6.4 导入报告

1.报告中心--报告管理页面，单击导入报告按钮



2.选择需要导入的报表，单击打开即可导入

