



# 天融信基线管理系统

## 用户手册

天融信  
2019 年



## 版权声明

本手册的所有内容，其版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，天融信及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不承担另行通知之义务。

版权所有不得翻印© 1995-2019 天融信公司

## 免责条款

本档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

北京天融信科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但北京天融信科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

## 信息反馈

如果您有任何宝贵意见，请反馈：

地址：北京市海淀区上地东路1号华控大厦 100085

电话：+8610-82776666

传真：+8610-82776677

服务热线：+8610-8008105119

您也可以访问北京天融信网站：<http://www.topsec.com.cn> 获得最新技术和产品信息

# 目录

<b>1</b>	<b>前言</b> .....	<b>1</b>
1.1	文档目的.....	1
1.2	读者对象.....	1
1.3	文档基本内容.....	1
1.4	约定.....	2
1.5	技术服务体系.....	2
<b>2</b>	<b>系统简介</b> .....	<b>3</b>
<b>3</b>	<b>首页</b> .....	<b>4</b>
3.1	登录系统.....	4
3.2	首页.....	5
3.2.1	全网安全级别.....	5
3.2.2	不合规检查范围热点.....	7
3.2.3	设备分类不合规情况占比.....	7
<b>4</b>	<b>设备中心</b> .....	<b>8</b>
4.1	设备中心主页.....	8
4.1.1	设备域.....	9
4.1.2	设备.....	10
4.2	设备发现.....	15
<b>5</b>	<b>检查任务</b> .....	<b>18</b>
5.1	创建检查任务.....	19
5.1.1	创建在线任务.....	19
5.1.2	创建离线任务.....	21
5.1.3	合并检查任务.....	25
5.2	执行检查任务.....	25

5.3	查看检查结果.....	26
<b>6</b>	<b>分析报表.....</b>	<b>30</b>
6.1	报表模板.....	30
6.2	报表配置.....	31
6.3	报表查看.....	32
<b>7</b>	<b>检查标准.....</b>	<b>35</b>
7.1	标准库.....	35
7.2	设备分类标准.....	38
<b>8</b>	<b>系统管理.....</b>	<b>40</b>
8.1	部门管理.....	40
8.2	角色管理.....	42
8.3	邮件配置.....	44
8.4	LICENSE 管理.....	44
8.5	审计日志.....	45

# 1 前言

本用户手册主要介绍了天融信基线管理系统 V3 的系统架构、使用和管理。通过阅读本文档，用户可以了解系统的基本组成，并使用系统。

本章内容主要包括：

- 文档目的
- 读者对象
- 文档基本内容
- 约定
- 相关文档
- 技术服务体系

## 1.1 文档目的

通过阅读本文档，使用户能够正确地配置使用系统，实现对日志、事件的综合分析，同时能实时监控日志并生成报表，方便对网络中的设备资产做安全监管。

## 1.2 读者对象

本用户手册适用于具有基本网络知识的系统管理员和网络管理员阅读。

## 1.3 文档基本内容

本用户手册包含以下章节：

- 第一章“前言”，介绍了本手册目的、读者对象、各章节的基本内容、文档约定和技术支持信息。
- 第二章“系统简介”，介绍了系统的功能点、组成等。
- 第三章“使用系统”，主要介绍系统登录和系统中各功能点。

## 1.4 约定

本文档遵循以下约定：

图形界面操作的描述采用以下约定：

“ ” 表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择）高级管理>特殊对象>用户；

点击（选择）步骤一 ->步骤二；

文档中出现的提示、警告、说明、示例等，是关于用户在使用本手册过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

## 1.5 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

<http://www.topsec.com.cn/>

天融信全国安全服务热线

800-810-5119

400-610-5119

## 2 系统简介

天融信基线管理系统 V3 制定了一套设备配置的检查基准，为安全管理提供参考与分析依据。系统通过各种技术手段进行自动化安全配置检查，检验对配置基准的合规度，发现潜在的安全问题；并将检查结果生成文档报告，为安全评估与加固工作提供技术支撑。

## 3 首页

### 3.1 登录系统

管理员可以通过 WEB 浏览器访问管理系统，访问 URL 地址 `http://IP`，其中的 IP 指搭建该系统的服务器对应的 IP，例如：<http://192.168.73.241>。



输入正确的用户名和密码后进入首页。

登录系统后，首页默认显示“首页”页面，如下图所示。



北京天融信公司

北京（总部）：010-82776666 咨询热线：400-610-5119 网址：[www.topsec.com.cn](http://www.topsec.com.cn)



## 3.2 首页

首页主要提供从主页快速执行检查的操作入口，显示全网合规情况统计、不合规检查范围热点、设备分类不合规情况占比，如下图所示。



### 3.2.1 全网安全级别

在“全网安全级别”统计图中包括两部分：全网安全级别、各安全级别占比。

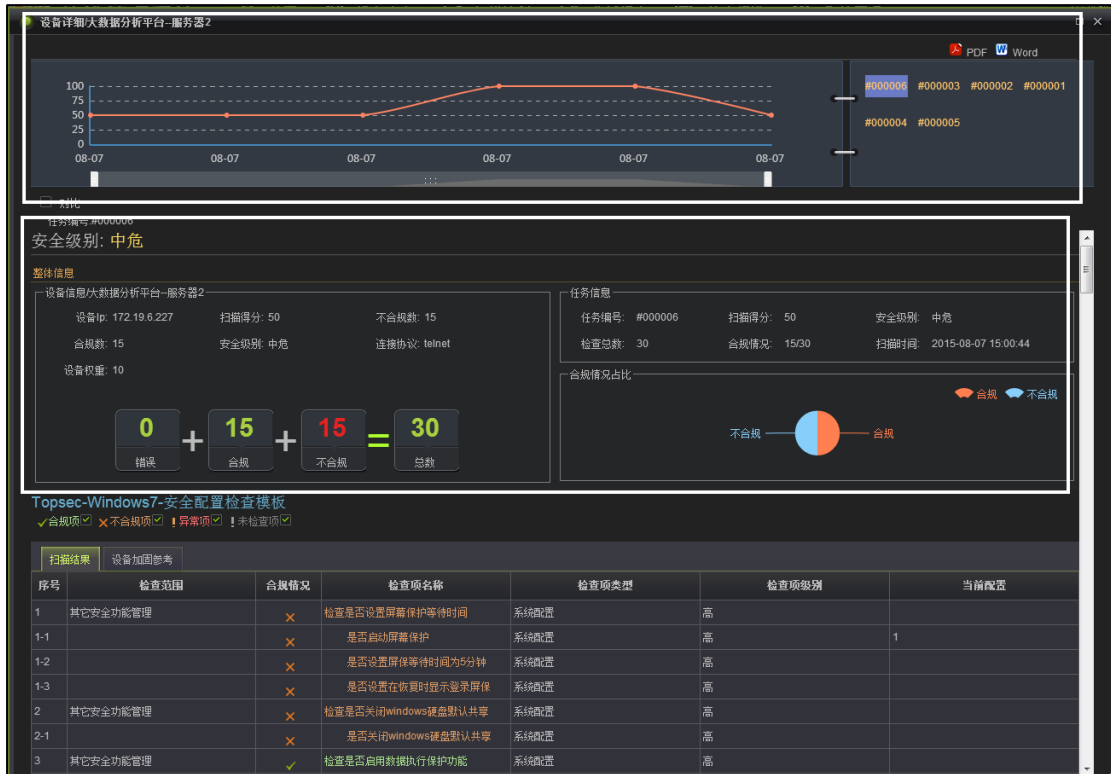
- 1) 全网安全级别分为：高危（0-39）、中危（40-79）、低危（80-99）、安全（100）。
- 2) 图形中色块：长度代表所在安全级别得分总和的占比，长度越长占比越大。
- 3) 图例中：百分比代表各等级检查得分总和占全得分的比值，与图形一一对应。

点击某个安全级别进入如下图所示的页面。

The screenshot shows the '中危的扫描设备' (Medium Risk Scanned Devices) page. It displays a table with 11 devices. The table columns are: 设备名称 (Device Name), 设备IP (Device IP), 上次检查得分 (Last Check Score), 扫描状态 (Scan Status), 设备类型 (Device Type), 所属任务 (Task), 所属模板 (Template), and 扫描时间 (Scan Time).

设备名称	设备IP	上次检查得分	扫描状态	设备类型	所属任务	所属模板	扫描时间
suse	192.168.72.240	72	完成	OpenSUSE-12.1	任务已删除	Topsec-OpenSUSE-12.1-安全配置检查模板	2015-07-31 09:39:32
redhat	192.168.234.129	44	完成	Redhat6.4	任务已删除	Topsec-Redhat6.4-安全配置检查模板	2015-07-31 09:39:32
大数据分析平台-服务器2	172.19.6.227	50	完成	Windows7	AASDF	Topsec-Windows7-安全配置检查模板	2015-07-31 11:12:55
大数据分析平台-服务器1	172.19.6.226	40	完成	WindowsXP	AASDF	Topsec-WindowsXP-安全配置检查模板	2015-07-31 11:12:57
安全管理平台-服务器5	172.19.6.224	61	完成	Solaris11	AASDF	Topsec-Solaris11-安全配置检查模板	2015-07-31 11:12:57
安全管理平台-服务器4	172.19.6.229	47	完成	Windows8	AASDF	Topsec-Windows8-安全配置检查模板	2015-07-31 11:12:57
centos	192.168.72.29	61	完成	CentOS6.5	sadfa	Topsec-CentOS6.5-安全配置检查模板	2015-08-04 16:51:30
solaris	192.168.72.41	72	完成	Solaris11	sadfa	Topsec-Solaris11-安全配置检查模板	2015-08-04 16:51:29
centos2	192.168.72.119	61	完成	CentOS6.5	sadfa	Topsec-CentOS6.5-安全配置检查模板	2015-08-04 16:51:30
suse	192.168.72.240	72	完成	OpenSUSE-12.1	sadfa	Topsec-OpenSUSE-12.1-安全配置检查模板	2015-08-04 16:51:29
redhat	192.168.234.129	44	完成	Redhat6.4	sadfa	Topsec-Redhat6.4-安全配置检查模板	2015-08-04 16:51:29

列表显示同类安全级别的设备检查详情，包括此设备名称、IP 地址、上次检查得分、扫描状态、设备类型、所属任务和模板、扫描时间。点击设备名称可进入对应设备检查分析详情页面，如下图所示。



页面分为三部分：

- 1) 上半部分以曲线图显示此设备所属任务的检查统计分析图。曲线图右侧显示的编号为任务编号。有关检查任务的详细内容请参见[错误!未找到引用源。检查任务](#)。
- 2) 中间部分显示任务中的设备经检查完成后的统计信息，包括设备基本信息、合规数与不合规数、安全级别、设备权重。右侧显示对应检查任务的详情信息并以饼图显示合规情况占比。如果勾选“对比”，页面变为对比效果。用户可以通过点选上半部分中的任务编号，选择需要对比的两个任务，如下图所示。



3) 下半部分以列表形式显示。显示设备所属任务使用的模板名称、检查结果，同时根据检查结果列出了设备加固参考说明。对于检查结果，用户可以通过复选框勾选在列表中显示哪个项目。

此检查分析详情，可以导出为 Word、PDF、Html、XML 格式导出。

### 3.2.2 不合规检查范围热点

全网最后一次检查中检查范围不合规的分布图，字体越大说明此检查范围数量的不合规占有情况越多。

### 3.2.3 设备分类不合规情况占比

全网最后一次检查中得分设备分类的分布图。

内圆表示全网安全设备数量占比情况，占比所对应的面积越大。较安全( $\geq 90$ )、不安全( $< 90$ )。

外圆为表示安全汇总（左半边外圆空白区域），较安全的设备数量占比；其他色块为不安全设备中各类型的数量占比，占比越大所对应的面积越大。

## 4 设备中心

设备中心主要用于统一管理设备，以域的视角对设备进行分级管理。用户可以手动添加设备，也可以由系统检查自动发现或导入设备文件；对设备进行安全性检查，分析危险漏洞并给出加固建议。

### 4.1 设备中心主页

点击“设备中心”进入默认页面即设备中心页面，如下图所示。



页面左侧目录树是设备域，由用户定义并将设备加入。

页面右侧三个图例依次为“

- 设备安全级别占比统计：最后一次检查设备安全级别占比图。全网安全级别分为：高危（0-39）、中危（40-79）、低危（80-99）、安全（100）
- 设备类型合规统计排名：最后一次检查设备按类型合规统计排名。全网安全级别分为：高危（0-39）、中危（40-79）、低危（80-99）、安全（100）
- 设备域安全级别统计：最后一次检查设备按域安全级别统计。全网安全级别分为：高危（0-39）、中危（40-79）、低危（80-99）、安全（100）。

检查得分最低 20 分设备列表，列出了设备 IP 地址、设备类型、设备安全级别等信息。点击设备名称链接进入页面，页面详细描述请参见 [3.2.1 全网安全级别](#)。

## 4.1.1 设备域

添加设备域的操作步骤：

- 1) 点击左侧目录树下方的“添加”进入添加分组页面，如下图所示。



- 2) 输入分组名称（必填项），可以输入描述性文字。

- 3) 完成后点击“提交”即可。

注意：当没选中设备域时，新建的设备域建立在根分组下；当选中某个设备域时，新建的设备域建立在已选中域的下一级分组。

编辑设备域的操作步骤：

- 1) 点击左侧目录树下方的“查看”进入修改和删除的页面，如下图所示。



2) 在“查看”页面中，点击“修改”可以编辑设备域信息，点击“删除”可以删除设备域信息。

## 4.1.2 设备

对设备进行安全配置检查，需要先把设备信息添加到系统中，然后定制检查计划，才可以对设备进行检查。

目前添加设备有三种方式：人工添加设备、外部 Excel 导入、设备发现。

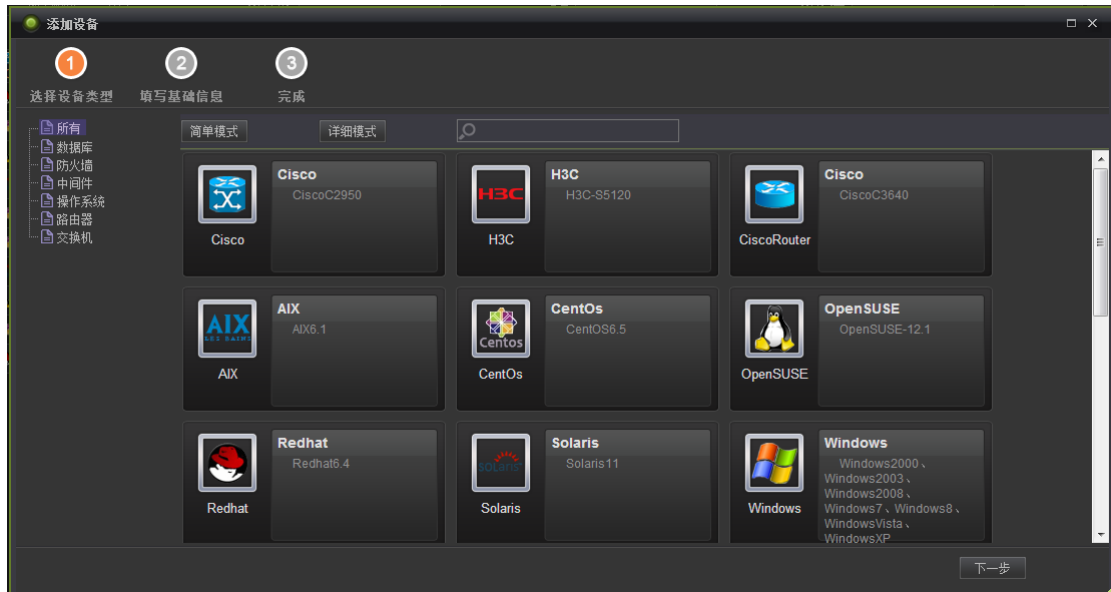
人工添加设备需要用户手动输入设备信息。

设备发现是根据输入的设备会自动发现网络中的设备信息，如设备 IP 地址、设备 MAC、设备类型、设备厂商等；设备发现的规则支持：IP 段，IP 掩码段、IP 通配符。

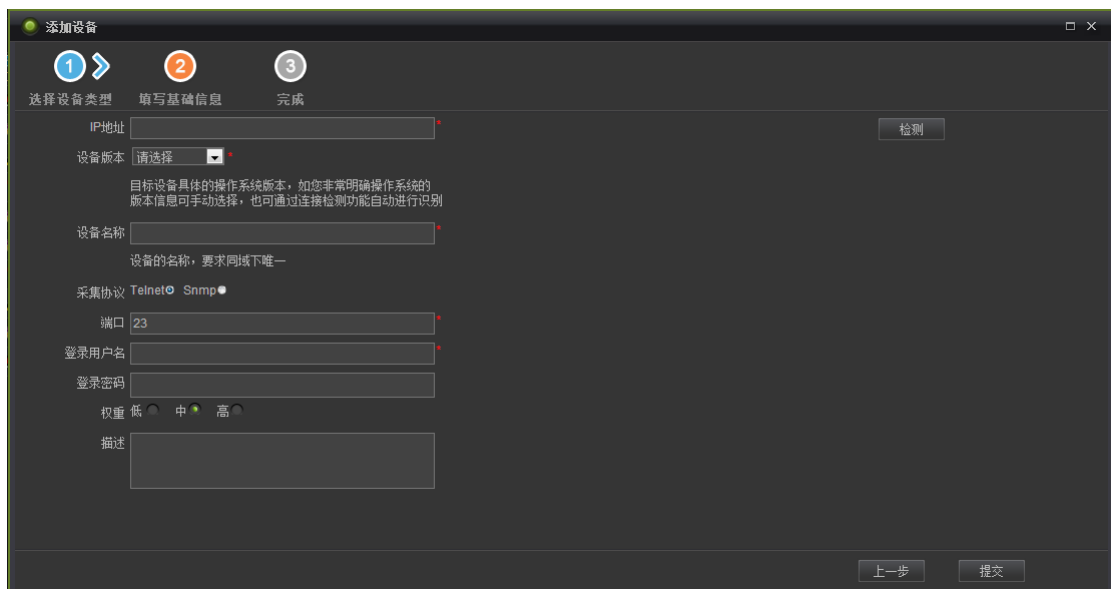
以下将进行详细描述。

### 4.1.2.1 人工添加设备

在左侧目录树中选中一个设备域，点击“ 添加”进入添加设备页面，如下图所示。



首先选择一个设备类型。简单模式和详细模式的区别在于详细模式标明有版本号。点击“下一步”进入填写基础信息页面，如下图所示。



填写设备 IP 地址、设备名称、端口号、登录信息，其中设备版本如不明确，可以通过“检测”功能由系统自动识别完成。完成后点击“提交”。页面自动刷新后在列表列出新添加的设备，如下图所示。

设备名称	IP地址	设备类型	创建时间	最后修改时间	描述	操作
172.16.56.120(Cisc oC2950)	172.16.56.120	思科C2950交换机	2015-08-10 13:34:26	2015-08-10 13:34:26		删除
redhat	192.168.234.129	RedHat6.4	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
centos	192.168.72.29	CentOS6.5	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
suse	192.168.72.240	OpenSUSE-12.1	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
solaris	192.168.72.41	Solaris11	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
centos2	192.168.72.119	CentOS6.5	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
centos	192.168.72.29	CentOS6.5	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
solaris	192.168.72.41	Solaris11	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
suse	192.168.72.240	OpenSUSE-12.1	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
centos2	192.168.72.119	CentOS6.5	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
redhat	192.168.234.129	RedHat6.4	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除

## 2、编辑

点击设备名称链接进入设备详细信息查看页面，如下图所示。



详细信息查看 / 172.16.56.120(CiscoC2950)

编辑 删除

**设备信息**

- 基础信息
- telnet / 连接参数信息
- 采集参数信息

**基础信息**

设备类型: CiscoC2950

设备名称: 172.16.56.120(CiscoC2950)

设备IP地址: 172.16.56.120

创建时间: 2015-08-10 13:34:26

最后修改时间: 2015-08-10 13:34:26

描述:

**telnet / 连接参数信息**

协议: telnet

enable密码: \*\*

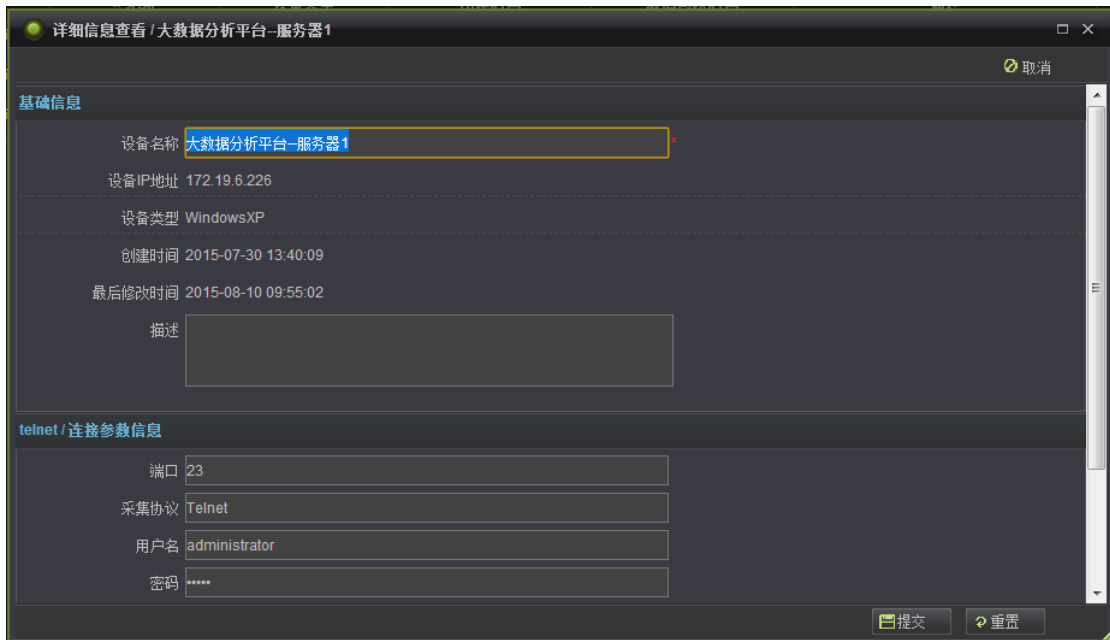
端口: 23

用户名: df

密码: \*\*

在此详细信息页面中，点击“编辑”进入编辑页面进行设备信息修改，完成后点击“提交”即可，如下图所示。

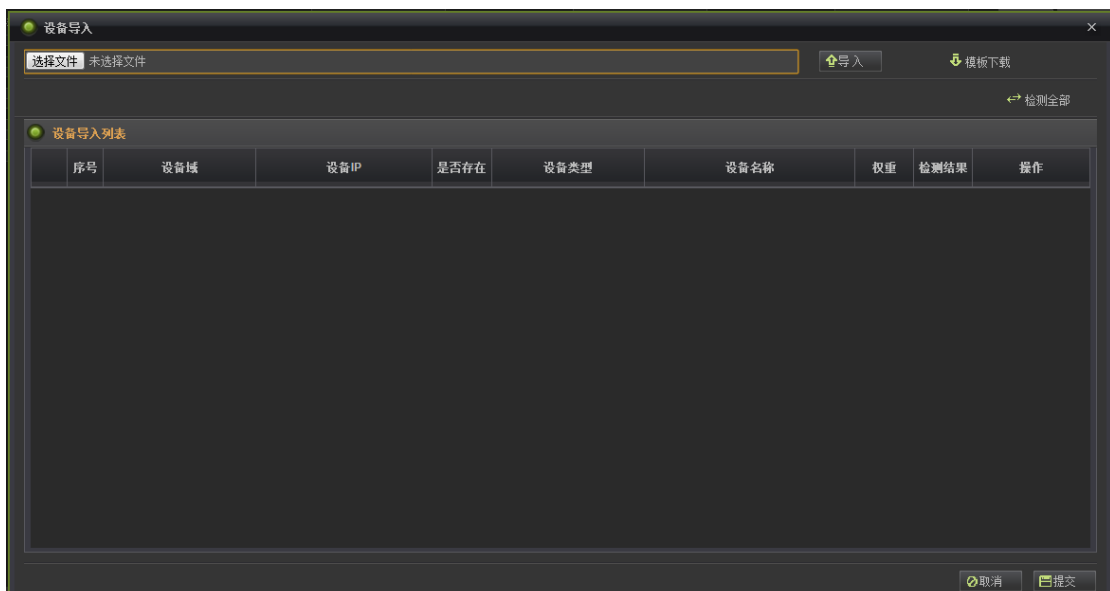




在此详细信息页面中，点击“删除”可以将此设备信息删除。

#### 4.1.2.2 设备导入

在设备中心首页面或点击选中某个设备域进入的页面中点击“导入”进入设备导入页面，如下图所示。

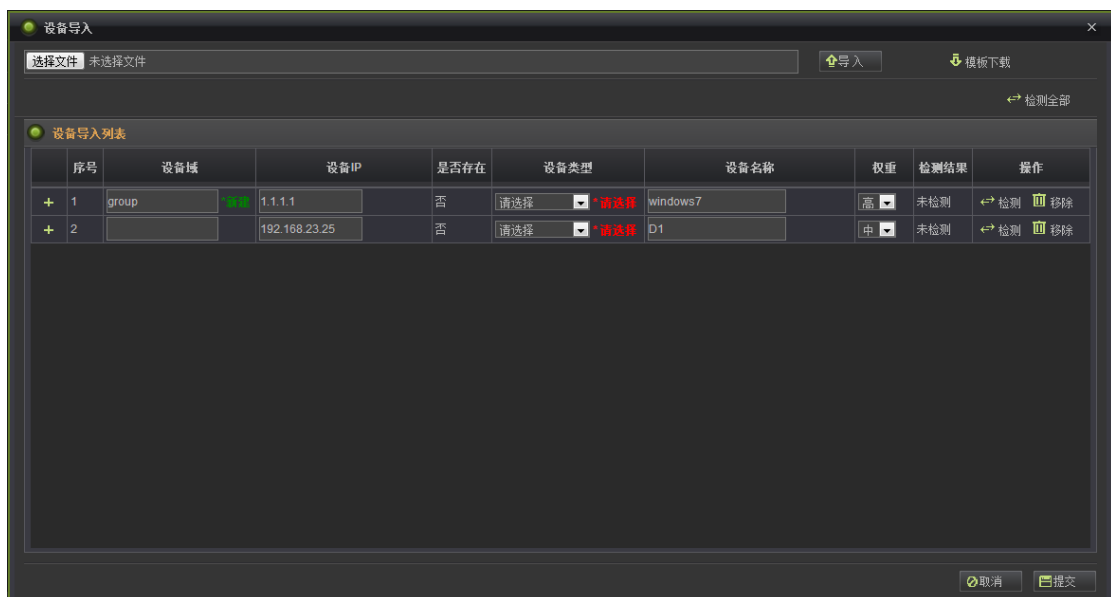


1) 点击“模版下载”按钮下载导入的模版。打开模板后，在模版中正确填写完设备的基础信息，如下图所示。

序号	设备域	IP地址	设备类型	设备名称	协议类型	端口	登录用户名	登录密码	Root密码	权重	采集参数
1	group	1.1.1.1	Windows	windows7	Telnet	23	admin	admin		高	
2		192.168.23.25	CentOs	D1	Ssh	23	admin	admin		中	
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											
28											
29											
30											
31											
32											
33											
34											

填写完后将文件名存为“设备列表”，在导入指南有文件命名和填写的详细说明。

2) 点击“导入”按钮，在下方的设备导入列表中会显示第一步在模版中填写的设备信息。完善列表中没有填写的信息，然后需要检测一下设备的网络可达状态，点击操作列表中“检测”，当提示“检测成功”表示网路可达，如下图所示。



设备导入

选择文件 未选择文件  模板下载

序号	设备域	设备IP	是否存在	设备类型	设备名称	权重	检测结果	操作
+	1	group	否	请选择	windows7	高	未检测	<input type="button" value="检测"/> <input type="button" value="移除"/>
+	2		否	请选择	D1	中	未检测	<input type="button" value="检测"/> <input type="button" value="移除"/>

说明：如果在模板中设备域为空时导入在根分组下，不为空且存在此设备域时会导入在此分组下，不为空但不存在时会先创建分组然后导入在其下，设备域只支持一级。

在模板示例中，一个设备域为空，一个是不存在的分组，导入完成后如下图所示。

设备名称	IP地址	设备类型	创建时间	最后更新时间	描述	操作
172.16.56.120(CiscoC2950)	172.16.56.120	思科C2950交换机	2015-08-10 13:34:26	2015-08-10 13:34:26		删除
redhat	192.168.234.129	RedHat6.4	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
centos	192.168.72.29	CentOS6.5	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
suse	192.168.72.240	OpenSUSE-12.1	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
solaris	192.168.72.41	Solaris11	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
centos2	192.168.72.119	CentOS6.5	2015-07-30 17:42:29	2015-07-30 17:42:29	设备来自系统数据自动添加	删除
centos	192.168.72.29	CentOS6.5	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
solaris	192.168.72.41	Solaris11	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
suse	192.168.72.240	OpenSUSE-12.1	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
centos2	192.168.72.119	CentOS6.5	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
redhat	192.168.234.129	RedHat6.4	2015-07-30 17:42:11	2015-07-30 17:42:11	设备来自系统数据自动添加	删除
D1	192.168.23.25	CentOS6.5	2014-08-10 16:35:50	2014-08-10 16:35:50		删除

## 4.2 设备发现

设备发现是根据输入的设备发现规则自动发现网络中的设备信息,如设备 IP 地址、设备 MAC、设备类型、设备厂商等。

设备发现的规则支持:

IP 段, 示例: 192.168.72.1-200

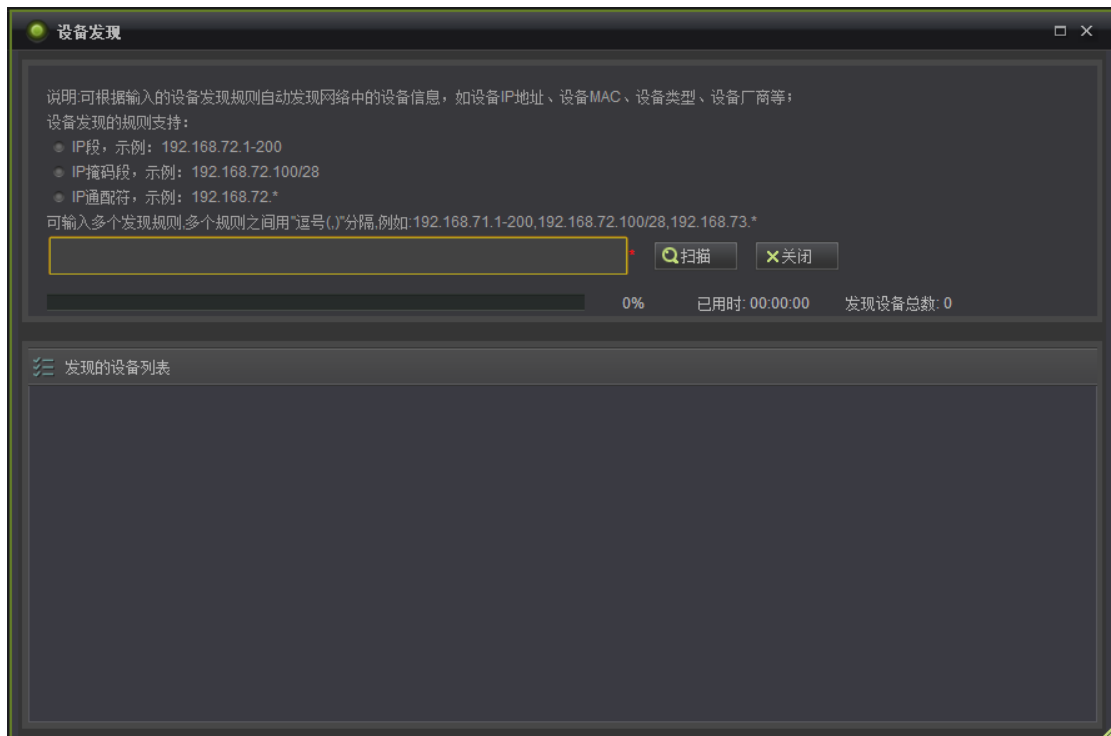
IP 掩码段, 示例: 192.168.72.100/28

IP 通配符, 示例: 192.168.72.\*

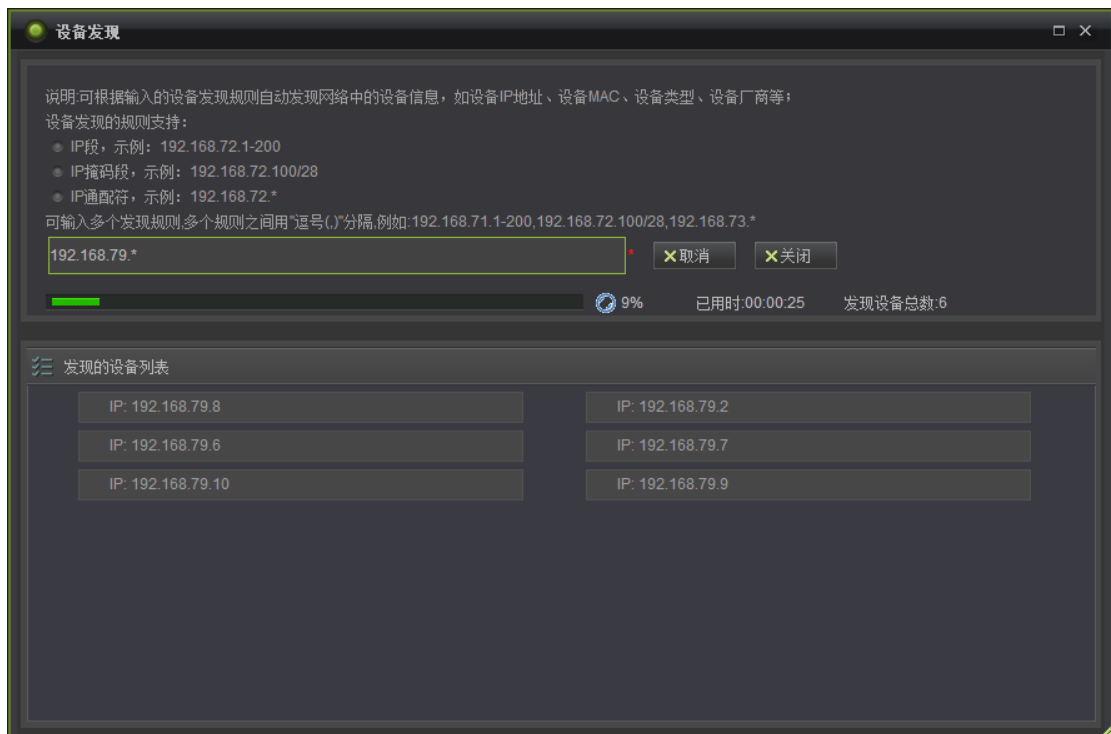
可输入多个 IP 段, 多个 IP 段之间用“逗号 ( , )”分隔, 示例


192.168.71.1-200,192.168.72.100/28,192.168.73.\*

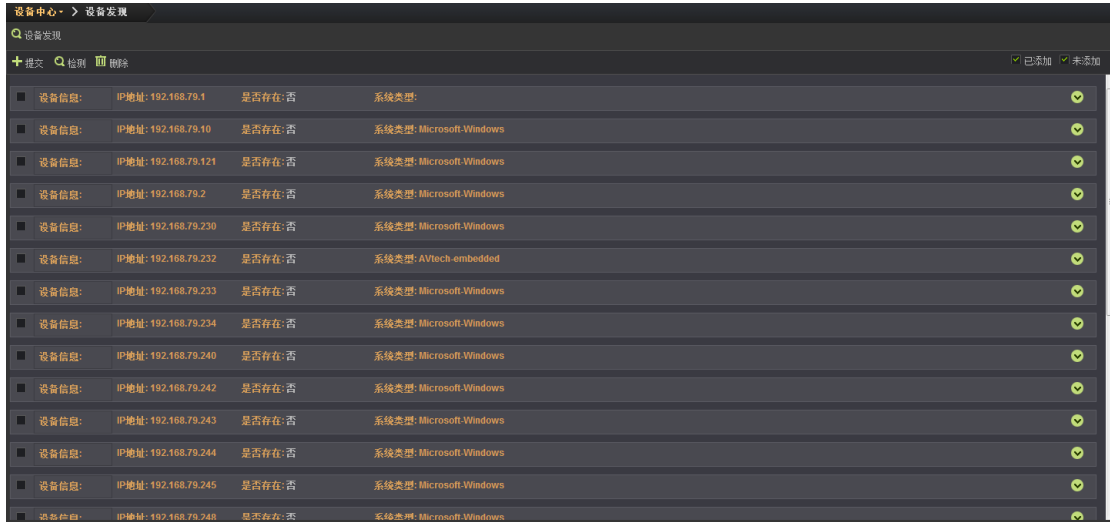
点击设备中心首页面的“设备自动发现”按钮或点击**设备中心>设备发现**, 打开设备发现对话框, 如下图所示。



在设备发现对话框中输入需要检查的 IP 段。当检查结束后符合检查条件的设备列于下方，如下图所示。



当检查完成后点击“关闭”按钮，则在页面中显示发现的所有设备信息列表，点击“”展开可以查看设备的详细信息，如下图所示。



选中需要添加的设备左侧复选框，点击“提交”，当设备信息右侧提示“添加成功”则该设备添加成功，详细信息如下图所示。



至此设备自动发现添加设备完成。

## 5 检查任务

创建计划检查任务，首先添加要检测的设备，对设备进行统一的检测。目前可以添加的任务类型包括即时任务、定时任务、周期任务、离线任务。

任务添加包含内容：任务基础信息、任务类型（即时、定时、周期）、检查设备列表、检查模板、结果展示、是否告警、是否生成报表、结果是否发送邮件。

当检查计划任务执行完成后可以查看任务基础信息、历史分数趋势图、合规数据趋势图、检查设备基础信息；支持查看最新检查结果；支持查看检查历史列表；支持修改任务信息、支持删除任务。

通过任务进度查看检查任务的详细信息，任务检查用时、设备数量、检查项合规、不合规与异常数；支持通过 IP 地址查询检查结果；支持查看日志。

点击“检查任务”进入页面，显示任务列表，如下图所示。

任务名称	完成时间	得分 (合规/不合规)	状态	操作
#g	4小时以前	49 (13 / 17)	#000001	扫描 暂停 取消 续扫
cgh-描述	1天以前	49 (14 / 15)	#000003	扫描 暂停 取消 续扫
周期任务		100 (0 / 0)	#000009	扫描 暂停 取消 续扫
定时任务	4天以前	38 (11 / 18)	#000001	扫描 暂停 取消 续扫
xl_离线任务	4天以前	49 (14 / 15)	#000003	扫描
xl_hebing	5天以前	51 (29 / 30)	#000002	扫描 暂停 取消 续扫
xl_230	5天以前	64 (18 / 12)	#000004	扫描 暂停 取消 续扫
xitest1_low	5天以前	51 (29 / 30)	#000004	扫描 暂停 取消 续扫
zctest1	5天以前	93 (237 / 232)	#000001	扫描 暂停 取消 续扫
xitest1	5天以前	51 (29 / 30)	#000004	扫描 暂停 取消 续扫
ere茶	5天以前	100 (29 / 0)	#000002	扫描 暂停 取消 续扫
13432435	5天以前	100 (0 / 0)	#000001	扫描 暂停 取消 续扫
444444444	6天以前	100 (0 / 0)	#000001	扫描 暂停 取消 续扫
XJ_249	5天以前	38 (11 / 19)	#000030	扫描 暂停 取消 续扫
cgh-负责人	6天以前	100 (0 / 0)	#000001	扫描 暂停 取消 续扫
错误-cgh	6天以前	100 (0 / 0)	#000001	扫描 暂停 取消 续扫
周期-cgh	3小时以前	49 (14 / 15)	#000007	扫描 暂停 取消 续扫
定时-cgh	6天以前	49 (14 / 15)	#000001	扫描 暂停 取消 续扫
scanner_报目录_wf	6天以前	100 (0 / 0)	#000001	扫描 暂停 取消 续扫

任务状态图标含义：

- “” 即时计划；
- “” 离线计划；
- “” 表示检查任务完成；
- “” 表示未开始检查；
- “” 表示检查取消或结束；
- “” 表示检查进行中；

“⏸”表示检查暂停。

## 5.1 创建检查任务

### 5.1.1 创建在线任务

创建一个在线任务步骤如下：

1、点击“在线任务”进入添加基础信息，填写任务名称、负责人、任务类型，设置完成后点击“下一步”，如下图所示。



其中任务类型分为：

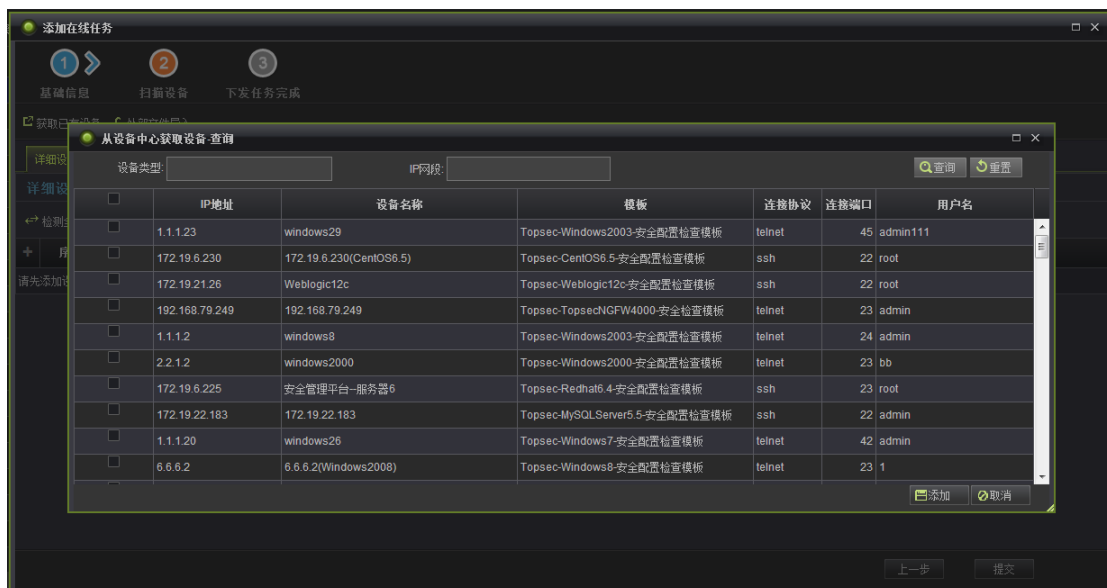
**即时任务：**即时任务需要人工触发进行检查，每次检查结束后任务即结束；

**定时任务：**定时任务是用户设置开始时间，然后由系统自动触发，检查完成后当前检查计划结束；

**周期任务：**周期任务为系统自动触发，触发条件为时间到达所设置的检查时间点（由用户设置周期为每天、每周、每月中的具体时间），周期任务如不取消系统将周期性执行此任务。

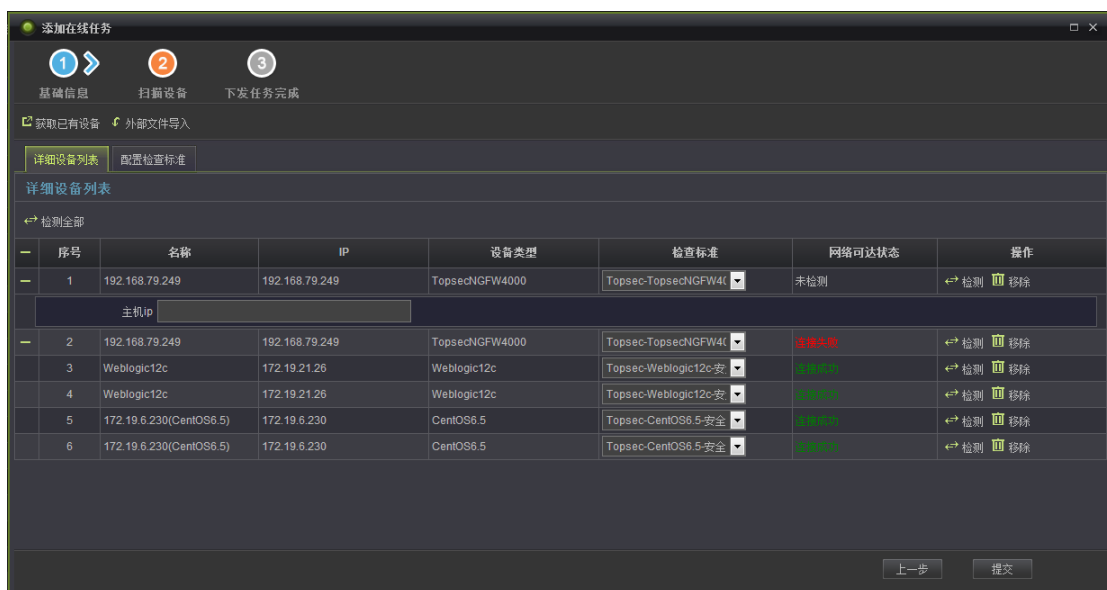
2、添加设备

可从系统中获取已有设备，也可以从外部导入（请参见 4.1.2.2 设备导入），如下图所示。



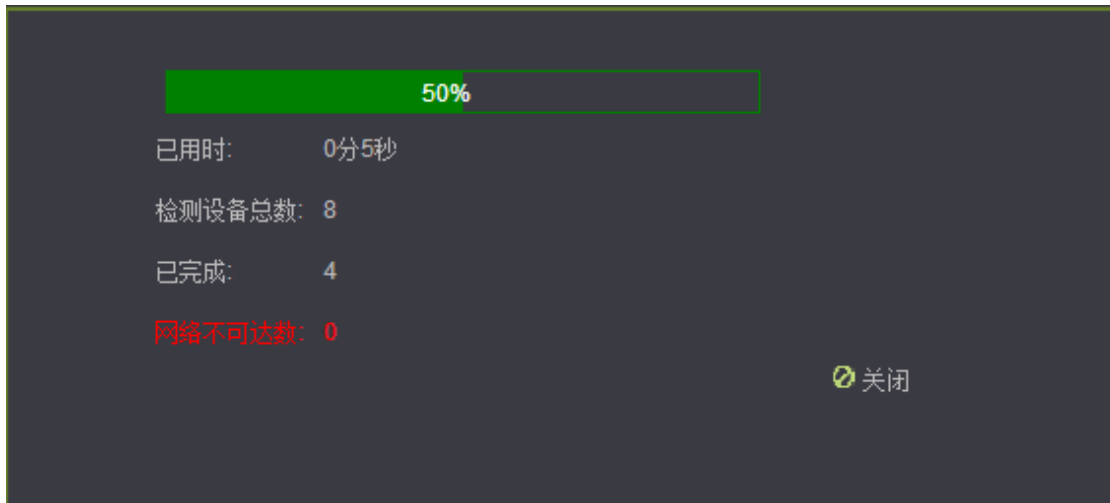
在详细设备列表页签中，可以检测设备连接状态；检查标准是在“检查标准”模块中已预置完成的，不同的设备类型对应的检查模板不同，具体请参见 7 检查标准。

在配置检查标准页签中，可以查看设备类型与检查标准的关联配置信息，如下图所示。



完成后点击“提交”，提示用户“是否进行设备网络可达性检测”，如下图所示。





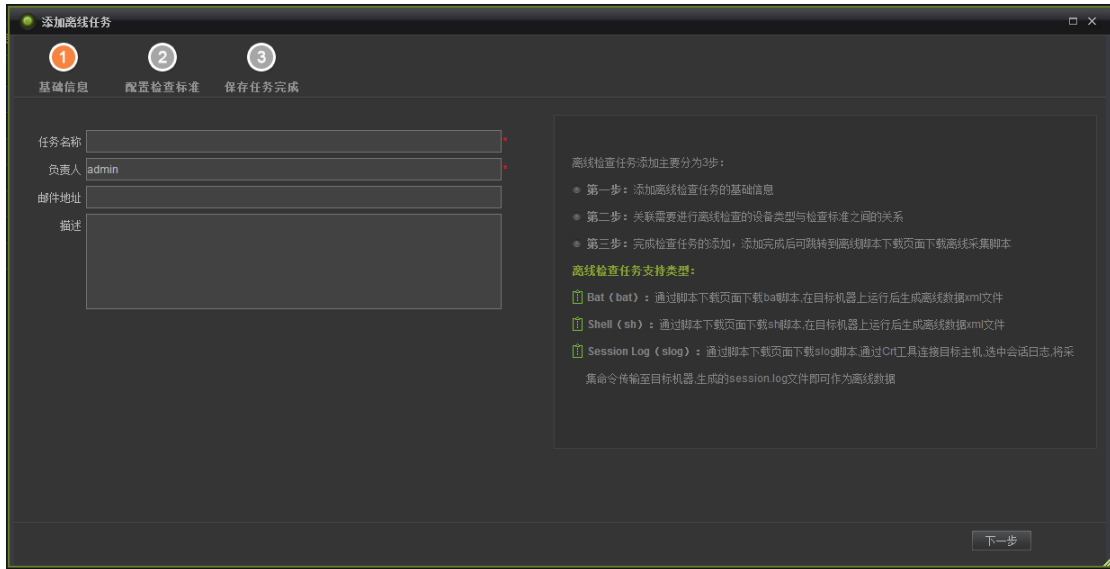
检测完成后提交即可，在线任务创建完成。点击“查看检查”可跳转到检查计划实时检查页面，如下图所示。



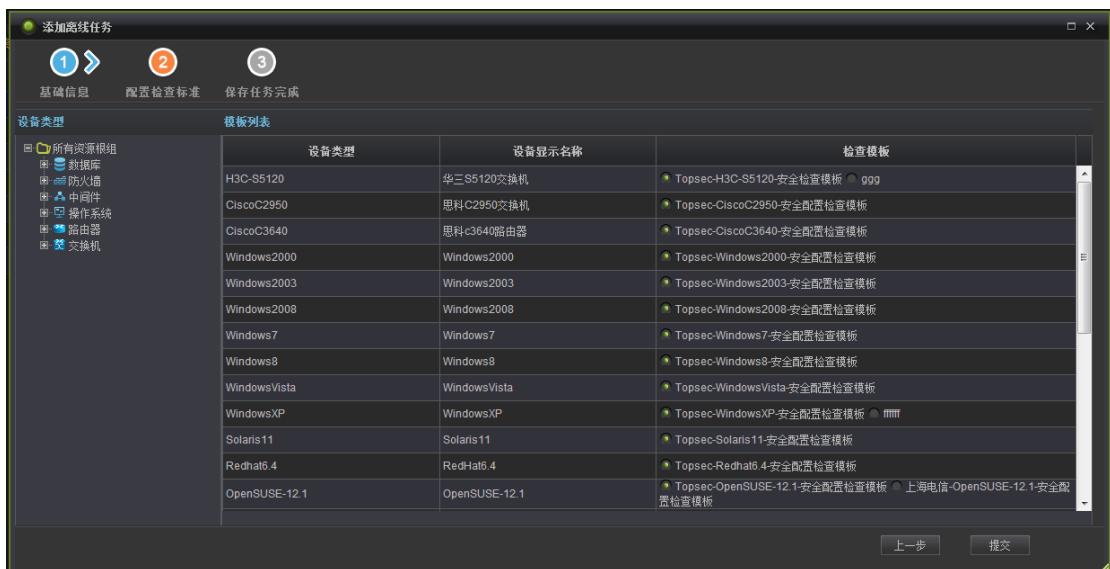
## 5.1.2 创建离线任务

创建一个离线任务步骤如下：

- 1、点击“离线任务”进入添加基础信息，填写任务名称、负责人、邮件地址，设置完成后点击“下一步”，如下图所示。



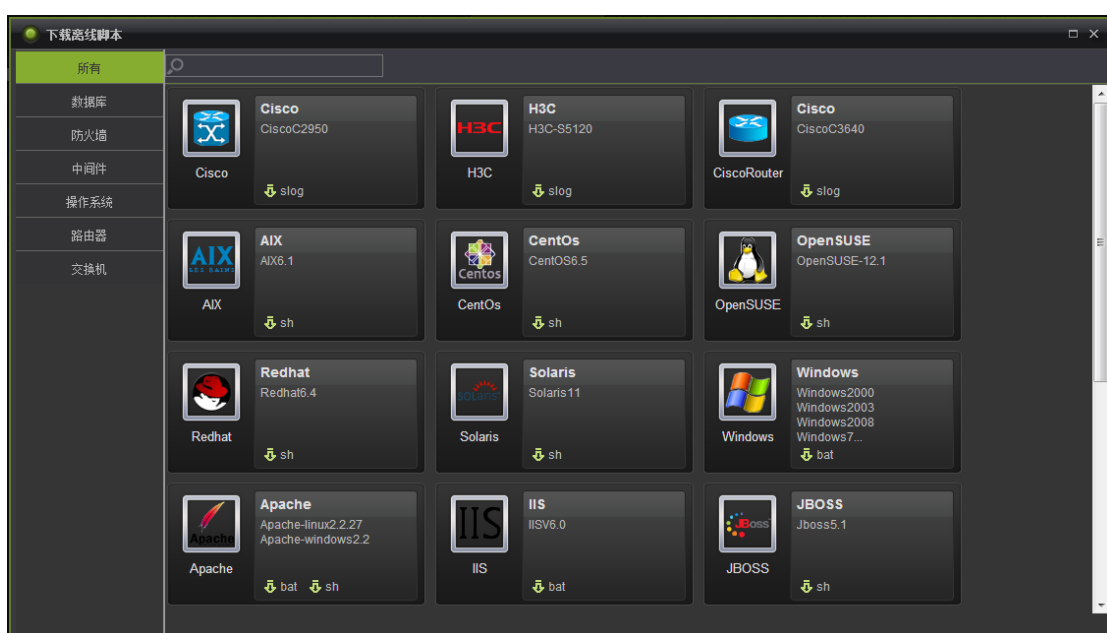
2、在配置检查标准页面，左侧可以选择“设备类型”选中对应设备类型，点击“提交”离线任务创建完毕，如下图所示。



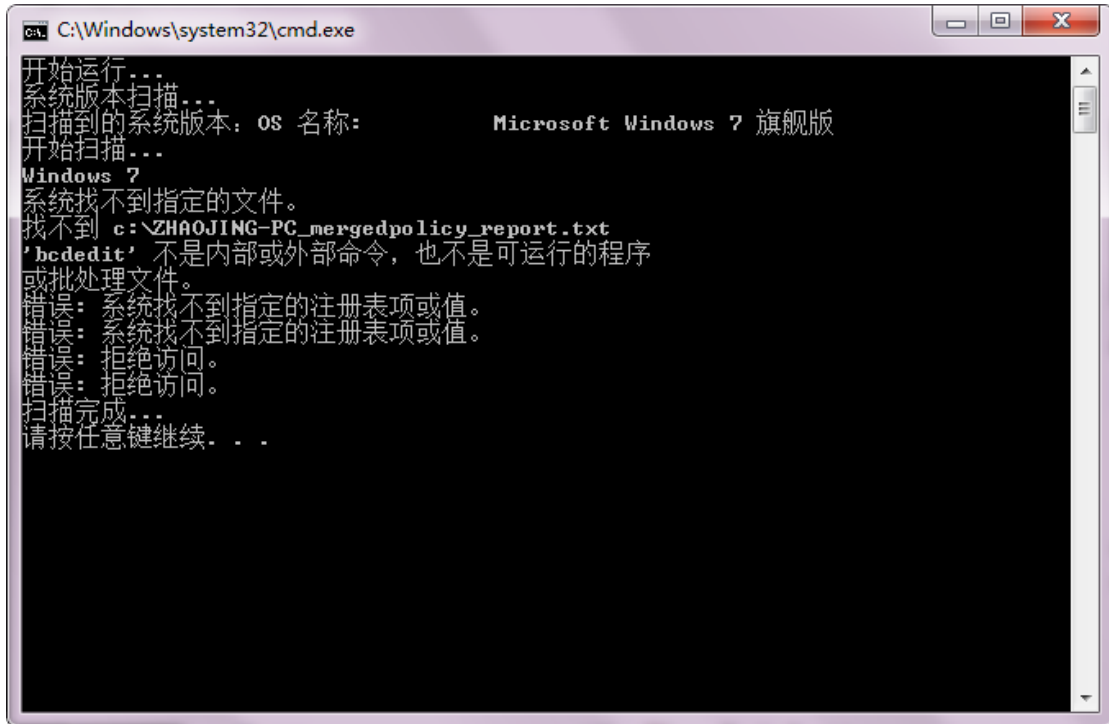
3、添加离线检查任务完成后，在出现的添加成功页面中点击“下载脚本”或从“检查任务”页面中点击“ 脚本下载”按钮，如下图所示。



查找到需要添加离线设备的设备类型，点击“下载 bat”按钮下载采集脚本，如下图所示。




下载后直接运行脚本采集信息，运行完成后生成为.xml 文件，如下图所示。

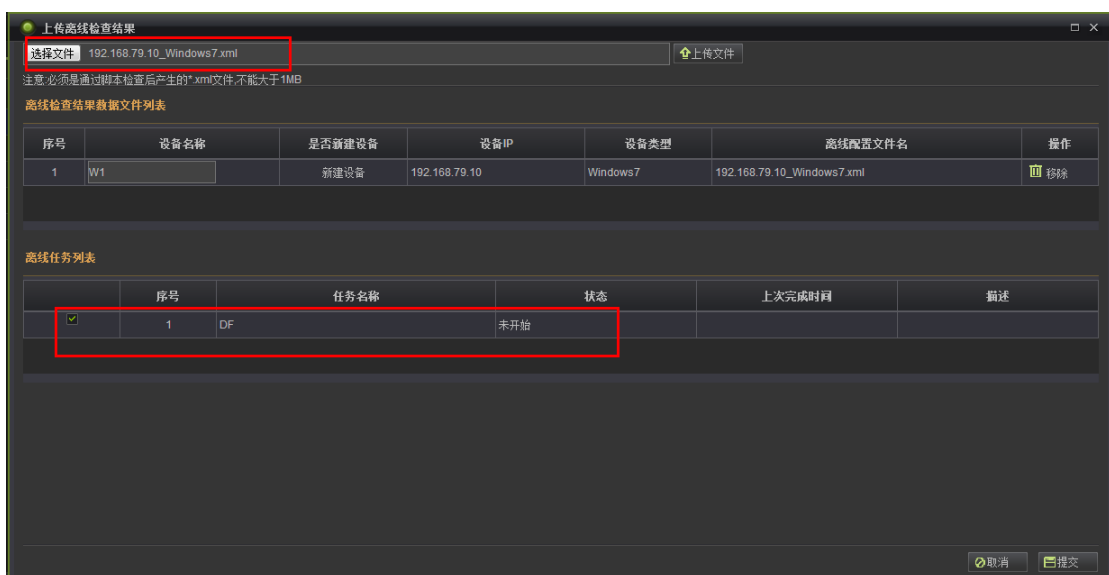


名称	修改日期	类型	大小
192.168.79.10_Windows7.xml	2015/8/13 15:09	UltraEdit Document (.xml)	55 KB
Windows.bat	2015/8/13 15:08	Windows 批处理文件	97 KB
设备列表.xls	2015/8/10 16:48	Microsoft Excel 97-2003 ...	27 KB

采集脚本运行完毕, 会生成一个后缀为 XML 的文档, 就是采集信息。

#### 4、上传离线采集结果关联离线任务

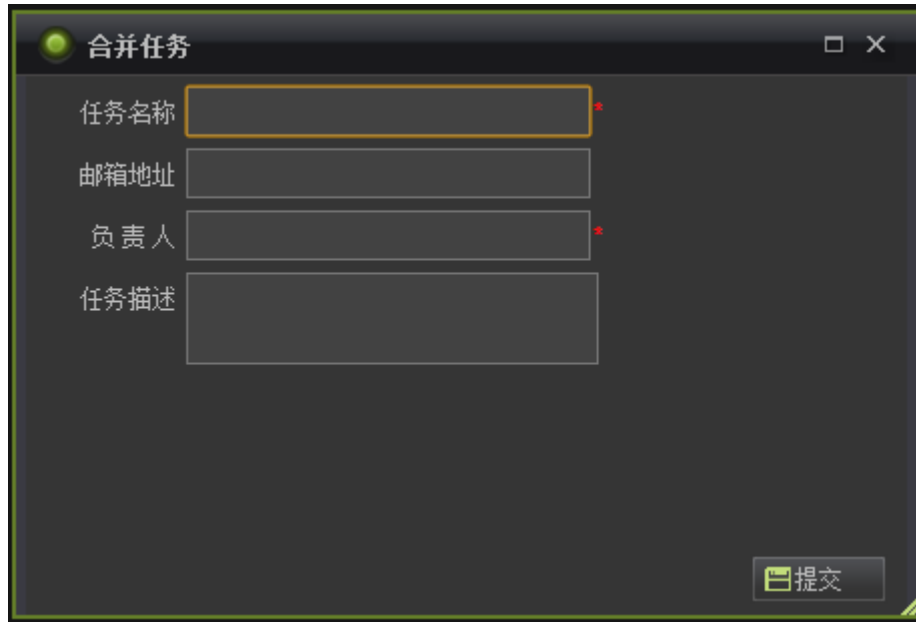
在“检查任务”首页面中点击“”，将上一步骤生成的 XML 文件上传。在页面下方的离线检查结果数据文件列表中列出采集的设备信息, 完成后点击“提交”，如下图所示。



至此离线任务创建完成。

### 5.1.3 合并检查任务

检查任务合并是将多个检查完成的任务合并成新的任务，合并后的新任务设备信息与原任务相同。选中需要合并的任务，然后点击“合并”进入对话框，如下图所示。



合并任务对话框包含以下输入项：

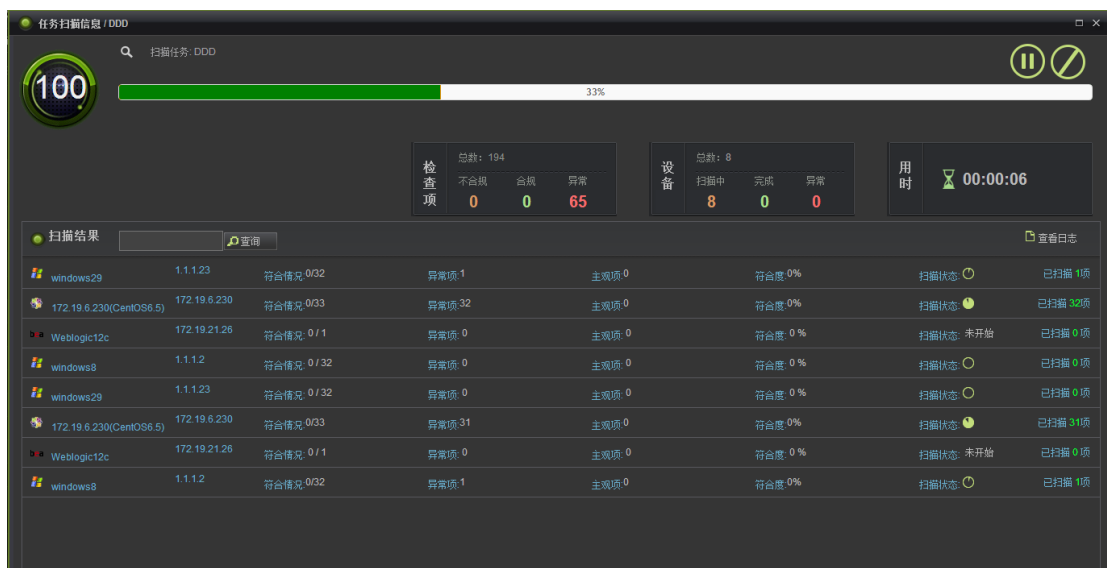
- 任务名称
- 邮箱地址
- 负责人
- 任务描述

对话框右下角有一个提交按钮，按钮上标有“提交”字样。

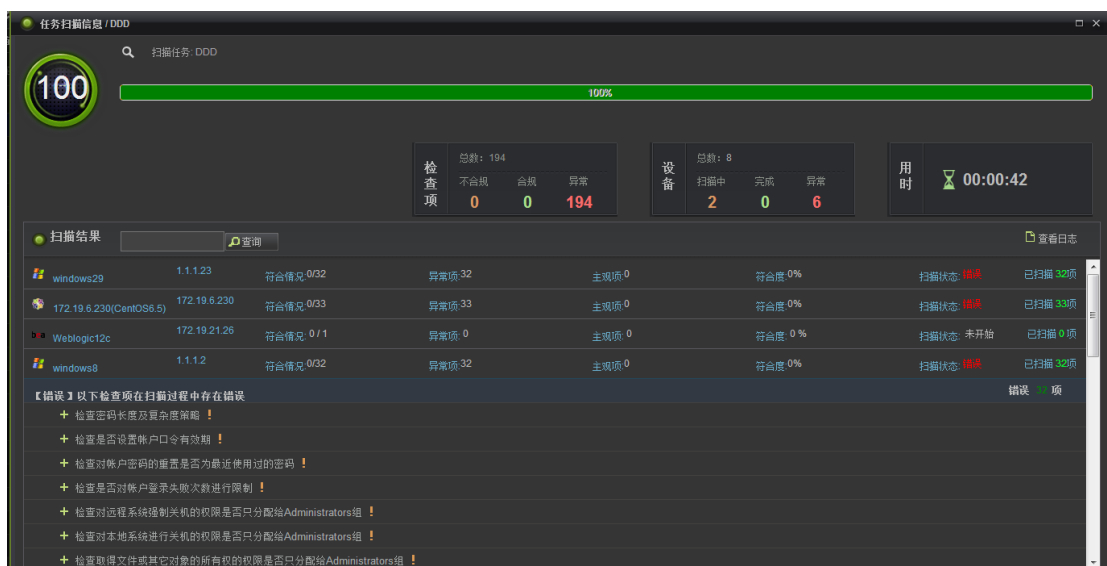
在任务合并对话框中，输入任务名称、邮箱地址、负责人、任务描述信息，点击“提交”完成。

## 5.2 执行检查任务

点击进入检查任务页面，选择需要执行检查任务，点击“检查”按钮，即可开始检测系统。当检查结束，可以看到实时的详细检查结果，包括检测用时，检查项合规与不合规的个数，详细的检查结果会列出每一项的检查情况等信息，如下图所示。



点击某一项，展开此项检查完成后存在的错误信息，如下图所示。



## 5.3 查看检查结果

查看检查计划任务包含了：任务信息、最新检查结果、检查历史结果。

### 1、任务信息

检查计划列表中的任务名称，进入默认“任务信息”页面，如下图所示。



页面显示任务基础信息、历史分数趋势图、检查项趋势图以及检查设备列表

在“基础信息”中，可以点击“编辑”、“删除”进行相应的操作。“另存为”可创建一个新的检查计划，新的检查计划中的设备信息、检查模版与此检查计划的相同。

点击“检查设备”列表中的检查模板链接，可以查看模板的检查项详细信息。点击“网络检测”用于检测网络可达状态。

## 2、最新检查结果

显示最近一次检测的时间、得分、设备数目，并以饼图显示分析设备检查情况、检查范围合规占比以及符合度占比，如下图所示。



显示设备列表详细信息以及检测得分、模板检查项详情（每一个检查项合规数、不合规主机 IP 地址）、检查日志等，如下图所示。

检查范围	检查项名称	权重	不合规总数	错误主机	不合规主机	合规主机
用户帐号配置	检查是否修改Administrator帐户名称并且禁用guest(来宾)帐号	80	1/5		172.19.6.229	
用户帐号配置	检查密码长度及复杂度策略	80	1/5		172.19.6.229	
用户帐号配置	检查是否设置帐户口令有效期	80	0/5			172.19.6.229
用户帐号配置	检查对帐户密码的重置是否为最近使用过的密码	80	1/5		172.19.6.229	
用户帐号配置	检查是否对帐户登录失败次数进行限制	80	1/5		172.19.6.229	
用户帐号配置	检查对远程系统控制主机的权限是否只分配给Administrators组	80	0/5			172.19.6.229
用户帐号配置	检查对本地系统进行关机的权限是否只分配给Administrators组	80	1/5		172.19.6.229	
用户帐号配置	检查取得文件或其它对象的所有权的权限是否只分配给Administrators组	80	0/5			172.19.6.229
用户帐号配置	检查允许访问本地计算机的用户列表	80	1/5		172.19.6.229	
用户帐号配置	检查允许访问远程计算机的用户列表	80	0/5			172.19.6.229
日志审计配置	检查是否配置用户帐户登录、注销日志	80	1/5		172.19.6.229	
日志审计配置	检查是否配置用户帐户的权限分配、审核、信任策略更改的日志功能	80	1/5		172.19.6.229	
日志审计配置	检查用户帐户查询事件	80	1/5		172.19.6.229	
日志审计配置	检查是否启用用户对目录服务访问日志	80	1/5		172.19.6.229	

点击每个设备可以进入设备详细检查信息页面，显示设备信息、任务信息、合规情况占比、详细的检查结果、和设备加固参考。

### 3、检查历史列表

历史列表列出检测任务检测的次数（用编号加以识别）、检查开始与结束时间、合规率、得分等，如下图所示。

检查编号	任务类型	任务名称	检查状态	得分	合规率	负责人	检查开始时间	检查结束用时	操作
#000007	即时任务		已完成	45	54.63	admin	2015-08-07 16:20:30	2015-08-07 16:20:46	↓ 下载
#000006	即时任务		已完成	45	54.63	admin	2015-08-07 15:00:44	2015-08-07 15:01:00	↓ 下载
#000005	即时任务		暂停	86	07.15	admin	2015-08-07 14:59:34	2015-08-07 14:59:37	↓ 下载
#000004	即时任务		取消	-	00.00	admin	2015-08-07 14:59:27	2015-08-07 14:59:29	↓ 下载
#000003	即时任务		已完成	43	53.84	admin	2015-08-07 14:54:51	2015-08-07 14:55:03	↓ 下载
#000002	即时任务		已完成	53	45.56	admin	2015-08-07 14:53:49	2015-08-07 14:54:02	↓ 下载
#000001	即时任务		已完成	45	54.63	admin	2015-08-07 14:53:11	2015-08-07 14:53:39	↓ 下载

点击检查编号链接进入任务查看页面，如下图所示。





1) 上半部分以曲线图显示此设备所属任务的检查统计分析图。曲线图右侧显示的编号为任务编号。

2) 中间部分显示任务中的设备经检查完成后的统计信息，包括设备基本信息、合规数与不合规数、安全级别、设备权重。对应检查任务的详情信息并以饼图显示设备检查情况、检查范围合规占比以及符合度占比。

如果勾选“对比”，页面变为对比效果。用户可以通过点选上半部分中的任务编号，选择需要对比的两个任务，如下图所示。



3) 下半部分以列表形式显示设备列表详细信息以及检测得分、模板检查项详情（每一个检查项合规数、不合规主机 IP 地址）、检查日志等。

此检查分析详情，可以导出为 Word、PDF 格式。

## 6 分析报表

分析报表主要提供了报表模版管理、报表配置、报表查询、报表下载等功能。

报表通过图表的方式展示，可以让管理人员能够清晰了解到全网设备检查范围合规情况、全网设备域安全情况等统计。使管理人员方便、效率的管理全网设备的安全情况。

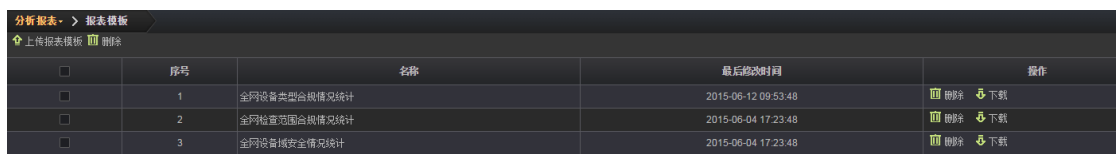
### 6.1 报表模版

报表模板采用 office 办公软件 word 预先定义出生成报表的样式，其中需要填充数据的地方采用参数替代，将其另存为 xml 格式的文件，此文件即为模板。

目前系统提供了：全网设备类型合规情况统计、全网合规情况分析报表、全网检查范围合规情况统计、全网设备域安全情况统计这四个报表模版。

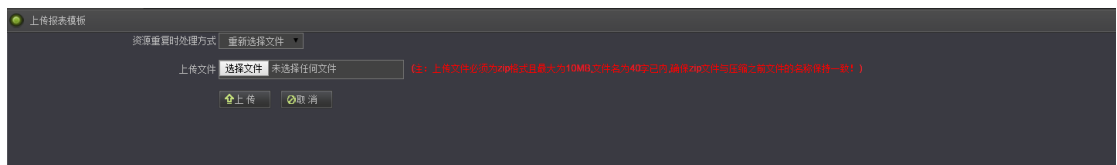
以下是对报表模版功能的简单操作：

- 1) 选择**分析报表>报表模版**，这里列出了系统中的所有报表模版，如下图所示。




<input type="checkbox"/>	序号	名称	最后修改时间	操作
<input type="checkbox"/>	1	全网设备类型合规情况统计	2015-06-12 09:53:48	删除  下载
<input type="checkbox"/>	2	全网检查范围合规情况统计	2015-06-04 17:23:48	删除  下载
<input type="checkbox"/>	3	全网设备域安全情况统计	2015-06-04 17:23:48	删除  下载


- 2) 点击“ 上传报表模版”按钮，选择压缩好的报表模版文件即可上传模版。如下图所示。



注：上传文件必须为 zip 格式且最大为 10MB,文件名为 40 字以内,确保 zip 文件与压缩之前文件的名称保持一致！

- 3) 点击“ 下载”按钮，会以 zip 压缩包的格式下载对应的报表模版，压缩包里包含了报表的样式、数据处理等文件，如下图所示。

名称	大小	压缩后大小	类型	安全
..(上层目录)				
dataSource.properties	1 KB	1 KB	PROPERTIES 文件	
sql.xml	2.34 KB	1 KB	XML 文档	
全网合规情况分析报表_doc.xml	29.33 KB	5.65 KB	XML 文档	
全网合规情况分析报表_html.xml	2.58 KB	1 KB	XML 文档	

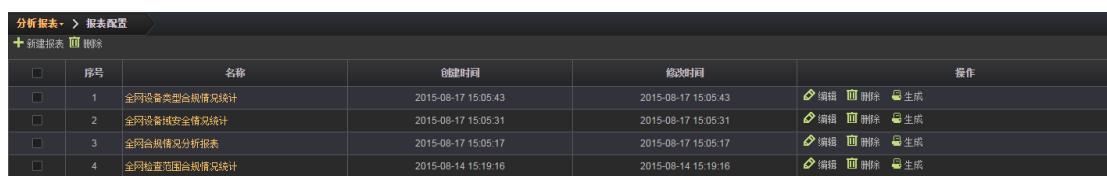
4) 点击“ 删除”按钮，可删除对应的报表模版。













## 6.2 报表配置


报表配置提供新建报表、根据报表模板，手动定期生成相关报表的功能。

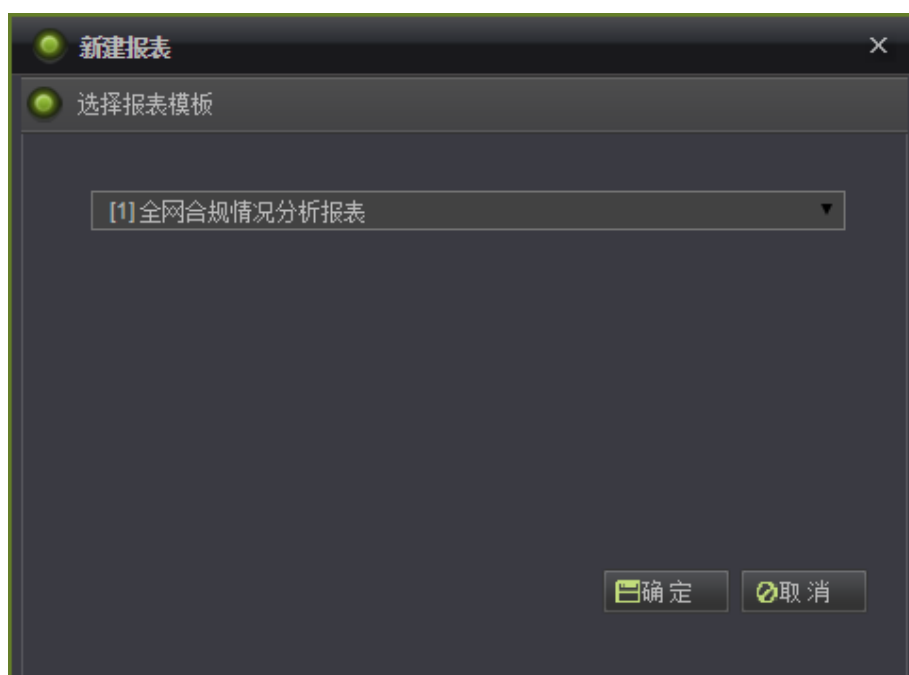
以下是对报表配置功能的简单操作：

1) 选择分析报表>报表配置，进入如下图的页面。



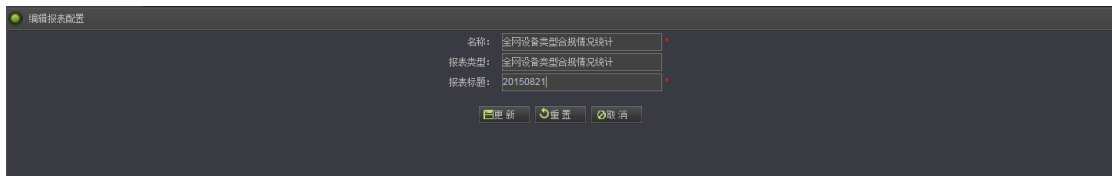
序号	名称	创建时间	修改时间	操作
1	全网设备类型合规情况统计	2015-08-17 15:05:43	2015-08-17 15:05:43	  
2	全网设备安全情况统计	2015-08-17 15:05:31	2015-08-17 15:05:31	  
3	全网合规情况分析报表	2015-08-17 15:05:17	2015-08-17 15:05:17	  
4	全网检查范围合规情况统计	2015-08-14 15:19:16	2015-08-14 15:19:16	  

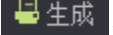
2) 点击“ 新建报表”按钮，先选择报表模版，然后填写报表名称等信息，点击新建按钮即可完成新建报表的操作，如下图所示。



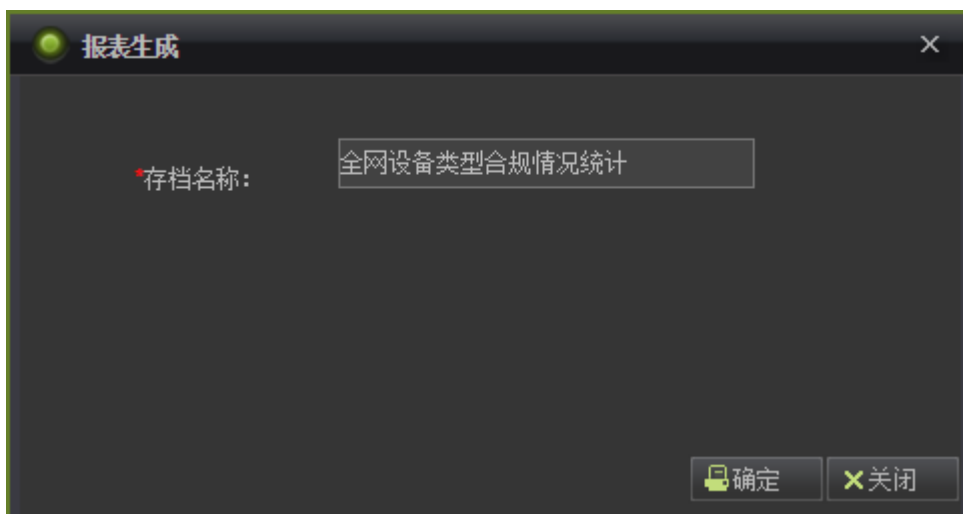



3) 点击“编辑”按钮，可以修改报表的基本信息，如下图所示。



4) 点击“生成”按钮，填写报表的存档名称点击确定按钮可生成相关报表，如下图所示。

生成的报表可在**分析报表>报表查看**页面列表中查看。



5) 点击“删除”按钮，可删除对应的报表。

## 6.3 报表查看

报表查看支持查询报表、实现报表导出、删除、编辑等功能。

以下是对报表查看功能的简单操作：

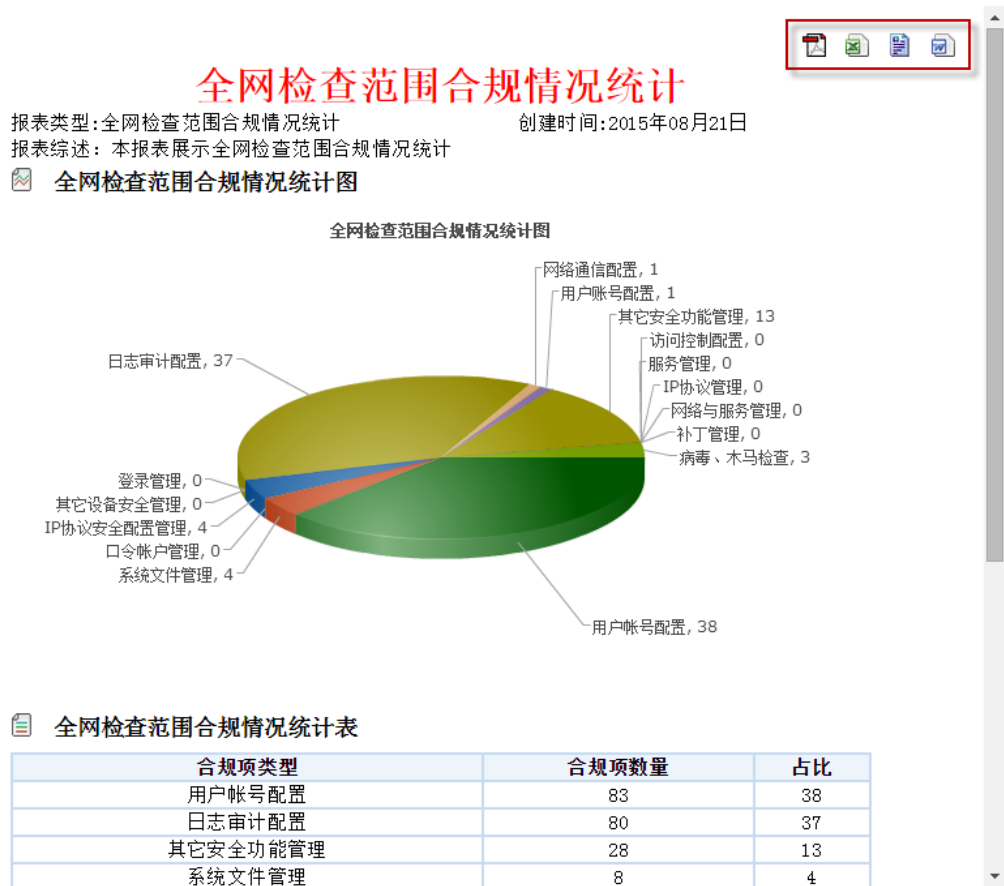
1) 选择**分析报表>报表查看**，进入如下图的页面。该页面列出了生成的所有报表。

分析报表 > 报表查看					
删除					
<input type="checkbox"/>	序号	名称	创建时间	修改时间	操作
<input type="checkbox"/>	1	全网设备网络安全情况统计	2015-08-21 09:48:29	2015-08-21 09:48:29	 编辑  删除  查看  下载
<input type="checkbox"/>	2	全网设备范围合规情况统计	2015-08-21 09:48:09	2015-08-21 09:48:09	 编辑  删除  查看  下载
<input type="checkbox"/>	3	全网合规情况分析报告	2015-08-19 14:59:44	2015-08-19 14:59:44	 编辑  删除  查看  下载

2) 点击“编辑”按钮，可以修改报表的存档名称，如下图所示。



3) 点击“查看”按钮，可查看到生成报表具体的图表信息，在页面中同时支持导出报表操作（点击左上角对应格式的图标即可导出报表），如下图所示。



4) 点击“下载”按钮，弹出下载格式选项目前支持 Word、PDF、Excel 这三种文件格式，如下图所示。



## 全网合规情况分析报表

报表类型: 全网合规情况分析报表 创建时间: 2015年08月19日


报表综述: 本报表展示全网合规统计情况

### 全网合规评估表

全网平均得分	评估结果
43.5000	危

### 重点关注设备 Top10

设备名	设备 IP	设备类型	得分	安全级别	扫描时间
172.19.6.37 (Windows2008)	172.19.6.37	Windows2008	5	高危	2015-08-18 16:27:24.0
172.19.6.37 (Windows2008)	172.19.6.37	Windows2008	19	高危	2015-08-18 16:27:24.0
Redhat6.4	172.19.6.225	Redhat6.4	50	中危	2015-08-18 14:14:48.0
192.168.72.52 (Windows7)	192.168.72.52	Windows7	100	安全	2015-08-18 16:27:24.0

5) 点击“ 删除”按钮，可删除对应的报表。

## 7 检查标准

基线管理系统根据系统的检查标准库，对网络中的安全设备进行检查。因此，在设置检查任务之前，需预先设置检查模板。

基线管理系统支持通过两种视角对标准库进行查看和管理，分别是以单位为基准的“标准库”视角，和以设备类型为基准的“设备分类标准”视角。

### 7.1 标准库

系统的标准库是在部署和初始化系统时导入系统的，后续通过系统管理页面，无法导入标准库。但是，可以导入的标准库进行增删改等维护操作。

此处的标准库按照单位名称进行分类管理，管理标准库的具体操作为：

1) 选择**检查标准>标准库**，进入如下图的页面。



模板名称	检查设备类型	是否为系统模板	是否为默认模板	所属用户	描述	操作
Topsec-Windows7-安全配置检查模板	Windows7	是	是	admin		模板参数(0) 检查参数(7) 另存为
Topsec-Windows2008-安全配置检查模板	Windows2008	是	是	admin		模板参数(0) 检查参数(5) 另存为
Topsec-WindowsXP-安全配置检查模板	WindowsXP	是	是	admin		模板参数(0) 检查参数(7) 另存为
Topsec-Windows8-安全配置检查模板	Windows8	是	是	admin		模板参数(0) 检查参数(7) 另存为
Topsec-Windows2003-安全配置检查模板	Windows2003	是	是	admin		模板参数(0) 检查参数(7) 另存为
Topsec-Windows2000-安全配置检查模板	Windows2000	是	是	admin		模板参数(0) 检查参数(7) 另存为
Topsec-Oracle10g-安全配置检查模板	Oracle10g	是	是	admin		模板参数(5) 检查参数(4) 另存为
Topsec-IISV6.0-安全配置检查模板	IISV6.0	是	是	admin		模板参数(0) 检查参数(4) 另存为
Topsec-Redhat6.4-安全配置检查模板	Redhat6.4	是	是	admin		模板参数(0) 检查参数(3) 另存为
Topsec-Comware5-安全配置检查模板	Comware5	是	是	admin		模板参数(0) 检查参数(0) 另存为

页面左侧导航栏按照单位名称分别展示了已经导入系统的标准库分类。

2) 点击左侧标准库的资源类别，可以查看针对该类别资源的检查标准。例如，查看数据库类资源的检查标准，如下图。



模板名称	检查设备类型	是否为系统模板	是否为默认模板	所属用户	描述	操作
Topsec-Oracle10g-安全配置检查模板	Oracle10g	是	是	admin		模板参数(5) 检查参数(4) 另存为
Topsec-SqlServer2008-安全配置检查模板	SqlServer2008	是	是	admin		模板参数(2) 检查参数(1) 另存为
Topsec-Oracle11g-安全配置检查模板	Oracle11g	是	是	admin		模板参数(4) 检查参数(0) 另存为
Topsec-MySQLServer5.5-安全配置检查模板	MySQLServer5.5	是	是	admin		模板参数(5) 检查参数(0) 另存为

3) 点击模板名称，可以查看该检查标准引用的模板的详细信息，如下图。

序号	检查范围	检查项编号	检查项名称	类别	级别	类型	权重	启用	操作
1	日志审计配置	安全要求-设备-ORACLE-配置-16	检查是否配置用户登录日志功能	系统配置	高	默认	80	✓	—
2	日志审计配置	安全要求-设备-ORACLE-配置-19-可选	检查是否配置数据库审计策略	系统配置	高	默认	80	✓	—
3	补丁管理	安全要求-设备-ORACLE-配置-26	检查是否达到系统补丁基线	系统配置	高	默认	80	✓	—
4	用户帐号配置	安全要求-设备-ORACLE-配置-1-可选	检查是否设置了不同的帐户及帐户组	系统配置	高	默认	80	✓	—
5	用户帐号配置	安全要求-设备-ORACLE-配置-3	检查是否指定用户远程登录	系统配置	高	默认	80	✓	—
6	用户帐号配置	安全要求-设备-ORACLE-配置-9	检查是否指定角色来管理数据库对象	系统配置	高	默认	80	✓	—
7	用户帐号配置	安全要求-设备-ORACLE-配置-10-可选	检查是否设置用户属性控制	系统配置	高	默认	80	✓	—
8	用户帐号配置	安全要求-设备-ORACLE-配置-13	检查是否指定用户访问数据字典	系统配置	高	默认	80	✓	—
9	用户帐号配置	安全要求-设备-ORACLE-配置-4	检查密码长度及复杂度策略	系统配置	高	默认	80	✓	—

在此，管理员可以查看该检查模板中的所有检查项信息，并可决定是否启用检查项、或修改检查项的权重。

另外，点击检查项的编号，还可查看该检查项的详细信息，如下图。

检查项详细信息	
检查项名称	检查是否配置用户登录日志功能
检查项范围	日志审计配置
检查项编号	安全要求-设备-ORACLE-配置-16
检查项级别	高
是否启用	启用
权重	60
检查项描述	数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐户、登录时间。
	参考配置操作 创建ORACLE登录触发器，记录用户名及登录时间 1. 建表LOGON_TABLE，三列（id、username、time列） <pre>create table login_table(id number,username varchar2(20),time date,primary key(id))</pre> 2. 建立序列，自动生成唯一id <pre>create sequence autoid</pre>

4) 在检查模板列表中，点击“操作”栏对应的“模板参数”可以查看该模板中有哪些参数、及参数对应的名称，如下图。

Topsec-Oracle10g-安全配置检查模板-参数展示		
参数名称	参数键	所属模板
oracle的sid	SID	Topsec-Oracle10g-安全配置检查模板
用户名	oracle_db_username	Topsec-Oracle10g-安全配置检查模板
密码	oracle_db_password	Topsec-Oracle10g-安全配置检查模板
测试用户	username	Topsec-Oracle10g-安全配置检查模板
oracle安装根目录	oracle_home	Topsec-Oracle10g-安全配置检查模板



5) 在检查模板列表中, 点击“操作”栏对应的“检查参数”可以查看该检查标准需要检查哪些参数, 及参数的标准值。



参数名称	参数类型	参数值
密码长度	值区间	0 6
帐户口令生存天数	小于等于	90
密码历史次数	数值	5
登录次数	数值	7

在此, 管理员也可根据需求修改、重置参数值。

6) 在检查模板列表中, 点击“操作”栏对应的“另存为”可以复制当前的检查模板, 如下图。



复制模板/Topsec-Oracle10g-安全配置检查模板

模板名称

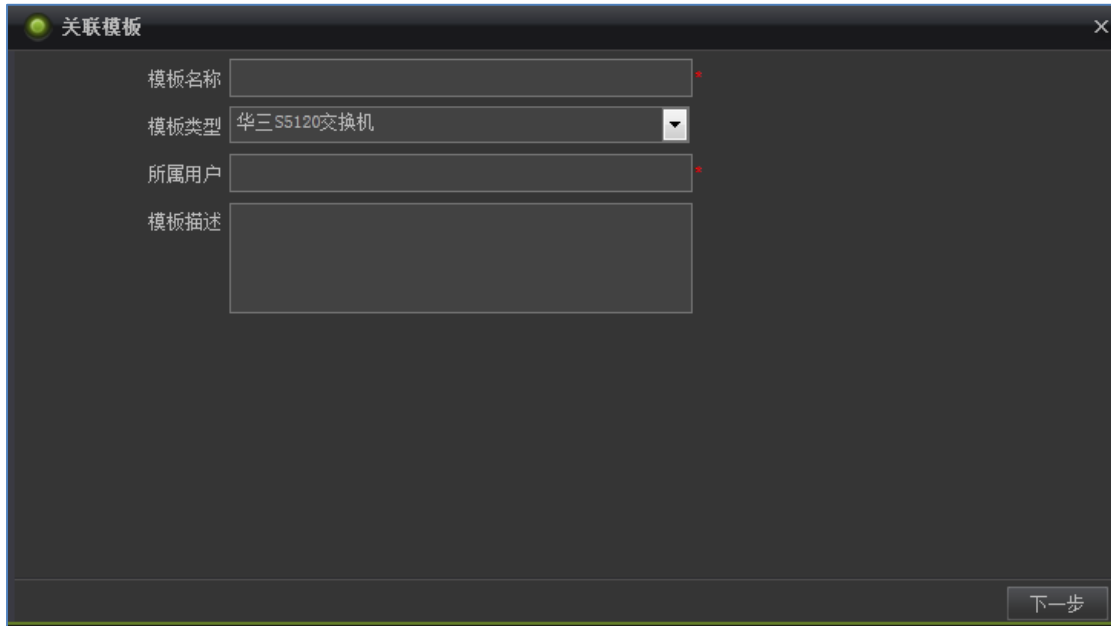
模板描述

模板类型 Oracle10g

检查项数 17 个

输入模板名称和描述信息后, 点击“提交”按钮便可完成模板的复制。

7) 点击检查模板列表上方的“添加”图标, 弹出添加检查模板窗口, 如下图。



关联模板配置界面，包含以下输入项：

- 模板名称：输入框
- 模板类型：下拉菜单，当前显示“华三 S5120交换机”
- 所属用户：输入框
- 模板描述：多行文本输入框

底部有“下一步”按钮。

输入模板名称、所属用户和模板描述信息，并选择关联的模板类型后，点击“下一步”按钮，为该模板选择检查项，如下图。



关联模板配置界面 - 检查项库

<input type="checkbox"/>	检查项编号	检查项名称	类别	检查范围	级别	类型	权重
<input type="checkbox"/>		检查是否配置交换机登录级别	系统配置	用户帐号配置	高	默认	80
<input type="checkbox"/>		检查密码口令是否配置不可逆加密算法	系统配置	用户帐号配置	高	默认	80
<input type="checkbox"/>		检查设备是否配置远程日志功能	系统配置	日志审计配置	高	默认	80
<input type="checkbox"/>		检查是否配置加密协议	系统配置	IP协议管理	高	默认	80
<input type="checkbox"/>		允许远程访问的地址列表	系统配置	IP协议管理	高	默认	80
<input type="checkbox"/>		检查系统是否配置Community默认通行字	系统配置	SNMP安全管理	高	默认	80
<input type="checkbox"/>		检查系统是否配置为SNMPV2或以上版本	系统配置	SNMP安全管理	高	默认	80
<input type="checkbox"/>		允许通过snmp访问网络的主机列表	系统配置	SNMP安全管理	高	默认	80
<input type="checkbox"/>		检查是否关闭未使用的	系统配置	SNMP安全管理	高	默认	80

底部有“上一步”和“提交”按钮。

勾选该模板需要包含的检查项，并为每个检查项设置编号。之后，点击“提交”按钮便可完成检查模板的添加。

对于管理员自行创建的检查模板，可对其进行删除、修改操作。

## 7.2 设备分类标准

设备分类标准是根据设备类型来分类查看系统中的检查模板。

根据设备类型查看检查模板的具体操作为：

1) 选择**检查标准>设备分类标准**，进入如下图的页面。



模板名称	设备类型	是否为系统模板	是否为默认模板	模板描述	操作
Topsec-Windows7-安全配置检查模板	Windows7	是	是		模板参数(0) 检查参数(7)
Topsec-Windows2008-安全配置检查模板	Windows2008	是	是		模板参数(0) 检查参数(5)
Topsec-WindowsXP-安全配置检查模板	WindowsXP	是	是		模板参数(0) 检查参数(7)
Topsec-Windows8-安全配置检查模板	Windows8	是	是		模板参数(0) 检查参数(7)
Topsec-Windows2003-安全配置检查模板	Windows2003	是	是		模板参数(0) 检查参数(7)
Topsec-Windows2000-安全配置检查模板	Windows2000	是	是		模板参数(0) 检查参数(7)
Topsec-Oracle10g-安全配置检查模板	Oracle10g	是	是		模板参数(5) 检查参数(4)
Topsec-IISV6.0-安全配置检查模板	IISV6.0	是	是		模板参数(0) 检查参数(4)
Topsec-Redhat6.4-安全配置检查模板	Redhat6.4	是	是		模板参数(0) 检查参数(3)

2) 在左侧导航栏中选择设备类型后，可以查看对应类型的检查模板。例如查看数据库类型的检查模板，如下图。



模板名称	设备类型	是否为系统模板	是否为默认模板	模板描述	操作
Topsec-Oracle10g-安全配置检查模板	Oracle10g	是	是		模板参数(5) 检查参数(4)
Topsec-SqlServer2008-安全配置检查模板	SqlServer2008	是	是		模板参数(2) 检查参数(1)
Topsec-Oracle11g-安全配置检查模板	Oracle11g	是	是		模板参数(4) 检查参数(0)
Topsec-MySQLServer5.5-安全配置检查模板	MySQLServer5.5	是	是		模板参数(5) 检查参数(0)

3) 同“标准库”类似的，管理员可以查看模板详情、检查项详情、模板参数、检查参数等信息。需要注意的是：管理员在“设备分类标准”中只能查看检查模板相关信息，不能对检查模板中的参数和参数值等数据进行修改。

## 8 系统管理

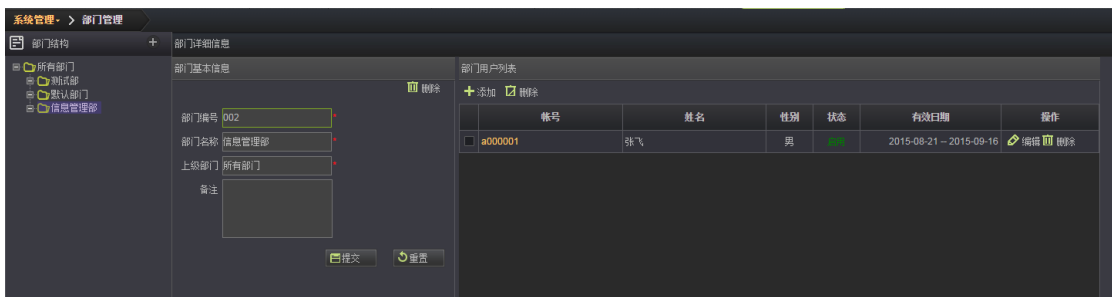
系统管理支持部门管理使用户按部门分类管理更方便；角色管理使不同的角色拥有不同对应的功能访问权限以及对角色关联用户；邮件系统管理；License 管理主要控制系统的有效期、支持设备最大数量、支持任务最大数量、单任务可检查设备最大数量；审计日志则提供了对操作员的详细操作记录的查询功能。


### 8.1 部门管理

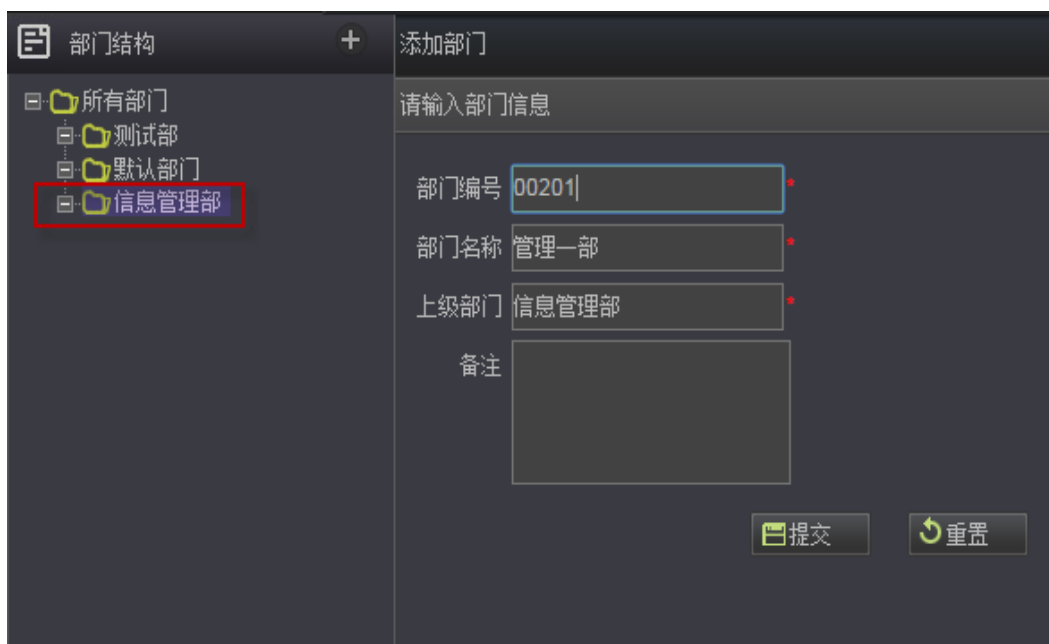
部门管理支持对部门进行新建、编辑、删除等操作，以及对部门下用户信息的管理。

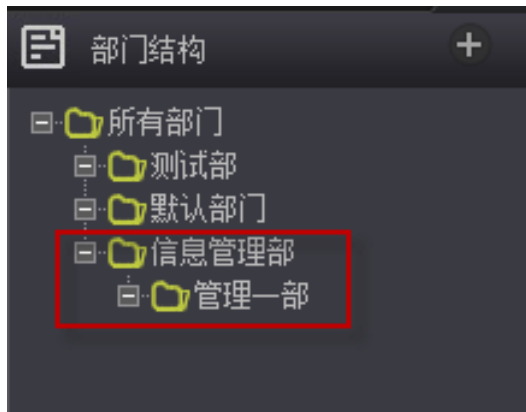
以下是对部门管理功能的简单操作：

- 1) 选择**系统管理>部门管理**，选中左侧对应部门，进入如下图的页面。



- 2) 先选中左侧部门，点击“”按钮，可以在选中部门下建立新的部门，如下图所示。







3) 选中左侧对应部门,可查看部门基本信息,如修改部分信息点击提交按钮可完成修改操作。

点击删除按钮可删除该部门,如下图所示。



4) 在部门用户列表处点击“添加”按钮,添加部门用户。如下图所示



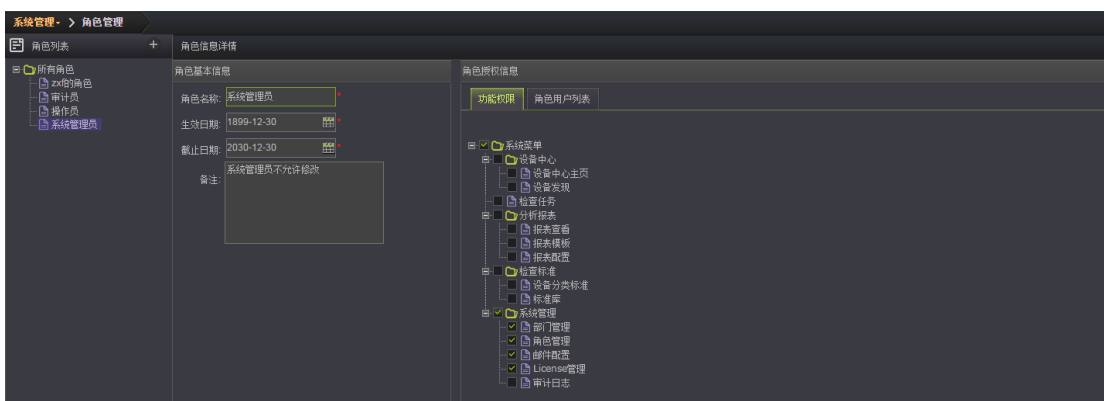
- 5) 在用户信息列表点击“编辑”按钮，可以修改用户信息以及用户状态。
- 6) 在用户信息列表点击“删除”按钮，可以删除该用户。

## 8.2 角色管理

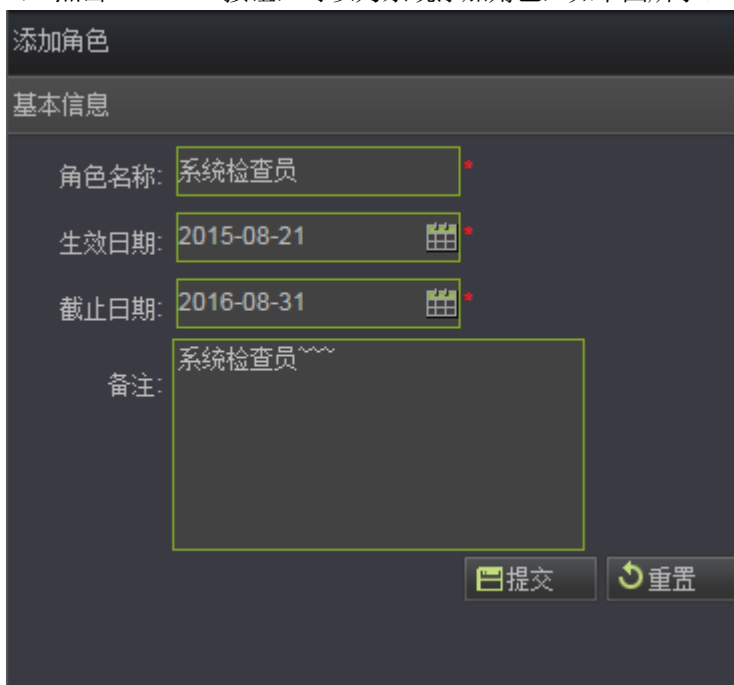
角色管理可以对不同角色授予对应的功能访问权限，以及管理角色和用户的关联关系。


以下是对角色管理功能的简单操作：

- 1) 选择**系统管理>角色管理**，选中左侧角色列表中角色，进入如下图的页面。



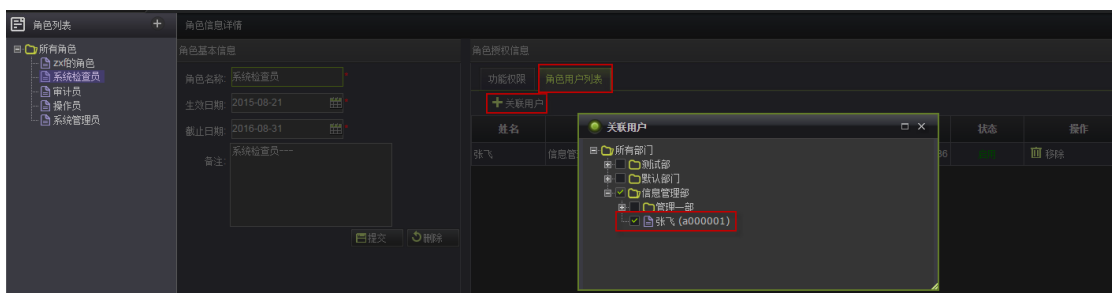
- 2) 点击“+”按钮，可以为系统添加角色，如下图所示。



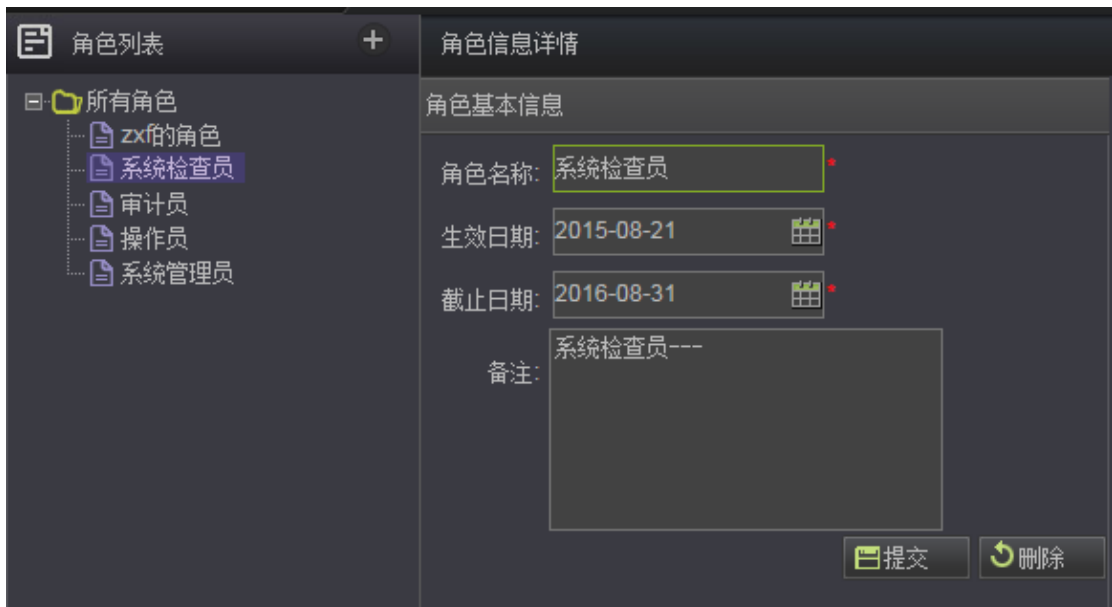
- 3) 选中对应角色，在右侧功能权限下选则该角色拥有的功能访问权限，然后点击“授权功能”按钮，即可为角色添加功能访问权限，如下图所示。



- 4) 选中对应角色，右侧切换到角色用户列表，点击“**+ 关联用户**”按钮，展开部门列表，选中用户就可以为该角色关联上用户。此用户就有了该角色的功能访问权限，如下图所示。



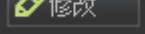
- 5) 在角色用户列表，点击“**移除**”按钮，可以将角色下移除该用户。
- 6) 在角色列表选中角色，修改角色基本信息点击提交按钮，可完成修改操作，点击删除按钮可以删除该角色。



## 8.3 邮件配置

1) 选择**系统管理**>**邮件配置**，进入如下图的页面。

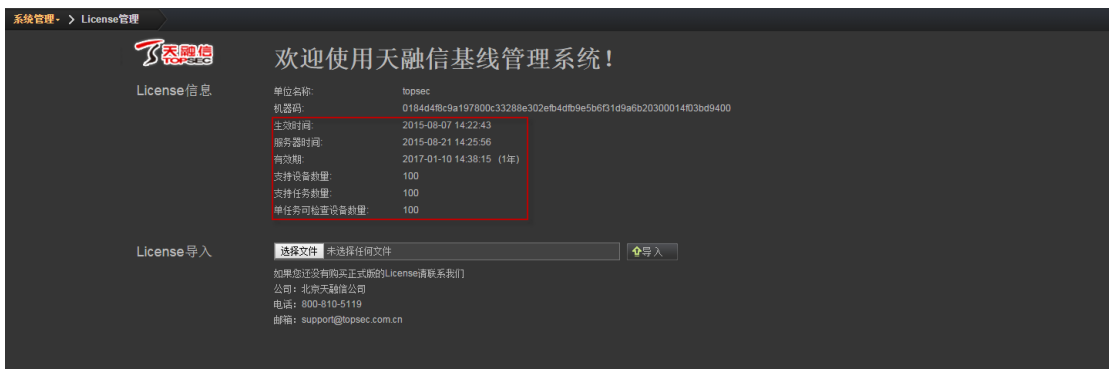


2) 点击 “” 按钮，可以修改邮件服务器的设置。

## 8.4 License 管理

License 主要控制系统的有效期、支持设备最大数量、支持任务最大数量、单任务可检查设备最大数量。如果有效期到期或者需要提供对设备的更大的支持，需要导入新的 License。

1) 选择**系统管理**>**License 管理**，进入如下图的页面。





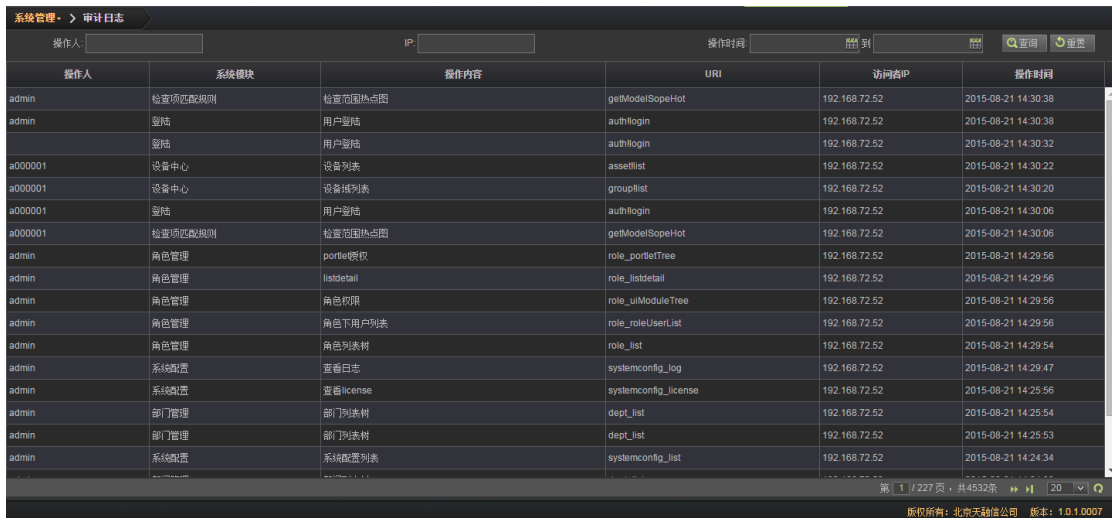
2) 选择新的 License 文件，点击“”按钮即可完成 License 导入。

## 8.5 审计日志

审计日志提供了对操作员的操作记录的查询功能。

审计日志详细记载了操作人、操作的系统模块、操作内容、访问者 IP、以及具体的操作时间。

1) 选择**系统管理>审计日志**，进入如下图的页面。



操作人	系统模块	操作内容	URI	访问者IP	操作时间
admin	检查项匹配规则	检查项匹配规则	getModelSopeHot	192.168.72.52	2015-08-21 14:30:38
admin	登陆	用户登陆	authlogin	192.168.72.52	2015-08-21 14:30:38
admin	登陆	用户登陆	authlogin	192.168.72.52	2015-08-21 14:30:32
admin	设备中心	设备列表	assetlist	192.168.72.52	2015-08-21 14:30:22
admin	设备中心	设备列表	groupList	192.168.72.52	2015-08-21 14:30:20
admin	登陆	用户登陆	authlogin	192.168.72.52	2015-08-21 14:30:06
admin	检查项匹配规则	检查项匹配规则	getModelSopeHot	192.168.72.52	2015-08-21 14:30:06
admin	角色管理	角色权限	role_portletTree	192.168.72.52	2015-08-21 14:29:56
admin	角色管理	角色列表	role_listdetail	192.168.72.52	2015-08-21 14:29:56
admin	角色管理	角色权限	role_allModuleTree	192.168.72.52	2015-08-21 14:29:56
admin	角色管理	角色下用户列表	role_roleUserList	192.168.72.52	2015-08-21 14:29:56
admin	角色管理	角色列表树	role_list	192.168.72.52	2015-08-21 14:29:54
admin	系统配置	查看日志	systemconfig_log	192.168.72.52	2015-08-21 14:29:47
admin	系统配置	查看license	systemconfig_license	192.168.72.52	2015-08-21 14:25:56
admin	部门管理	部门列表树	dept_list	192.168.72.52	2015-08-21 14:25:54
admin	部门管理	部门列表树	dept_list	192.168.72.52	2015-08-21 14:25:53
admin	系统配置	系统配置列表	systemconfig_list	192.168.72.52	2015-08-21 14:24:34

2) 点击“搜索”按钮，可根据操作人、IP、操作时间来具体查询。