**网站预警系统**

**用户手册**

**北京华清泰和科技有限公司**

**2015年3月**

目录

[一、产品概述 3](#_Toc414005949)

[二、系统介绍 4](#_Toc414005950)

[1、 首页 4](#_Toc414005951)

[2、 安全监控 7](#_Toc414005952)

[（1）变更统计 7](#_Toc414005953)

[（2）文字监测 7](#_Toc414005954)

[（3）链接监测 8](#_Toc414005955)

[（4）脚本变化 8](#_Toc414005956)

[（5）图片监测 8](#_Toc414005957)

[（6）暗链扫描 9](#_Toc414005958)

[（7）敏感词监测 10](#_Toc414005959)

[（8）挂马监测 10](#_Toc414005960)

[（9）漏洞监测 10](#_Toc414005961)

[3、 性能监控 11](#_Toc414005962)

[（1）首页连通拓扑 11](#_Toc414005963)

[（2）首页连通状态 11](#_Toc414005964)

[4、网站运维 12](#_Toc414005965)

[（1）域名解析监测 12](#_Toc414005966)

[（2）站点可用性 14](#_Toc414005967)

[5、站点诊断 15](#_Toc414005968)

[（1）错误页面 15](#_Toc414005969)

[（2）内外部链接错误 15](#_Toc414005970)

[6、报表管理 16](#_Toc414005971)

[7、系统管理 16](#_Toc414005972)

[（1）系统配置 16](#_Toc414005973)

[(2)系统日志 18](#_Toc414005974)

[(3)用户管理 19](#_Toc414005975)

[(4)网站管理 19](#_Toc414005976)

[（5）敏感词配置 23](#_Toc414005977)

[（6）发送配置 23](#_Toc414005978)

[（7）发送记录 24](#_Toc414005979)

[（8）报表配置 25](#_Toc414005980)

# 一、产品概述

Early Warning 预警机（又称网站预警系统）产品针对WEB系统，提供WEB内容预警解决方案，避免重大节假日期间基于内容发布人员和网站系统管理人员工作职责分离造成的信息审计不及时而导致的网站首页图片被恶意替换、网站首页和特定页面出现敏感信息、网站内容被恶意修改等政治敏感性事件的发生。

网站预警系统是集网站上的内容变更监测预警、暗链监测预警、DNS解析时间监测预警、错误页和连接错误监测预警等为一体的综合网站预警系统。网站预警系统用高效的网站诊断监测技术对目标网站进行监测，能够针对网站进行采集—分析—预警—统计，通过强大的对比分析技术，及时的反应网站变化情况、及时监测网站危害性信息以及敏感信息。并以立体感图片墙的形式展现出来。如果网页发生异常变化，则平台会发送手机短信、邮件等告警信息。

无论是针对一个主网站还是针对网站群，网站预警系统都是一个不可或缺的网站预警系统，它可以帮您做以下事情

1：通过DNS的监控预警，避免网站客户或者领导发现网站打不开，或者链接到了其他一个违法的网站上时，而管理人员却依然不知此情。

2：通过暗链的监测预警，避免网站上长久挂载暗链。尤其是政府、教育发布信息具有权威性的部门，如果挂载非法暗链、挂载含有木马的暗链，影响会非常的大，通过暗链的预警，可避免发生政治敏感性问题

3：通过敏感词的监测预警，可以避免网站上出现敏感性信息，尤其是在重要、敏感时期，网站上出现敏感词汇可以随时发送邮件、短信报警。或者管理人员可以随时查找任一关心的敏感词，及时预警、发现有助于管理人员及时解决问题，降低影响力。

4：通过挂马检测，可以及时发现网站被黑客攻击后设置的木马，使网站管理员可以及时采取措施，清除木马，避免木马危害更多的网站访问者，确保网站的信誉。

5：通过定期漏洞扫描，可以发现网站的漏洞，使网站管理员对网站的安全进行重新评估，采取相应措施进行安全加固，确保网站的安全性。

6：通过图片墙功能，无需监控人员或读网人不停的点击链接，打开页面再观察网页信息情况。

图片墙可以把每个站点以立体感图片墙形式展现出来，无论是领导还是对网站的监控人员，都可以很方便、直观的观察网站的信息。节省了大量的时间、人力，同时提高效率。

7：通过文字的监测，避免了网站出现敏感文字内容时管理人员与领导还不知情，并且采用了文字对比的机制，与被修改前的内容可以实现改动内容的对比，更是方便了管理人员对监控页面实时全面的一个了解，可避免发生政治性敏感问题。

8：通过图片监测，可以避免网站上被挂有一些带有敏感信息的图片，当网站更新新的图片的时候，不管是合法的还是非法的都会被图片监测下载下来，由我们的监控人员分析是正常的还是非法的，大大的提高了监控人员的工作效率，并且能够及时发现，避免了政治性敏感问题。

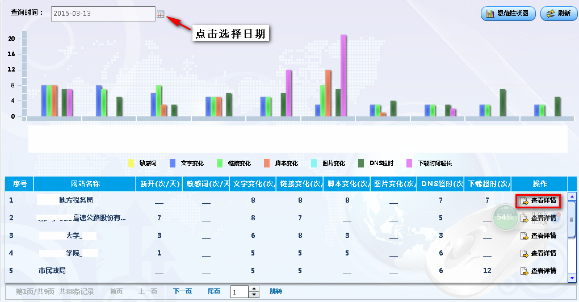
9：监控人员通过链接监测可以对网站被修改的链接通过预警系统做出一个修改前的与修改后的对比，及时发现问题，避免出现敏感的网站链接。

10：通过对网站首页、性能监控、网站运维、站点诊断这4大功能可以对网站整体的通断情况做出一个全方面的统计，包括域名解析、首页实时连通状态、站点可用性、错误页面、内外部错误链接等。可以帮助监控人员知道错误的页面，错误的原因，错误的时间，错误累计的时间等，做到真正对网站实时的监测，及时的发现，并通知监控人员，避免发生网站断开等情况。

# 二、系统介绍

## 1、 首页

1. **报警汇总**



默认展示了当天的报警信息汇总，可以选择日期。通过点击下一页，找到想查看的网站，再点击查看详情，就可以了解某个网站当天报警的所有信息。如果想了解某个报警的具体信息，可以在选中报警后，点击详情。如下所示：



1. **首页监控**

首页监控显示区分为上下格局，上为显示网站主页和各链接以及子类网站和各链接页面，以图片的形式展现出来，下为系统模块信息展示区域。

★点击主页右下角处的3D墙，可以立体感的图片墙的形式展现页面。此外还有2D墙展示。

★预警机3D图片墙滚动速度为原速、快速与超速，可以根据实际情况设定。

**★如果网站打开时间超过3秒，就无法截取网页图片，该网站链接会在‘问题’模块显示。**

如下图所示



在系统首页的模块信息展示区分为三大部分，主要为‘断开网站’、‘平均DNS超出阈值’、‘平均下载超出阈值’

1. **断开网站**

断开网站模块分为五部分：“链接名称”“首页中断开始时间”、“首页中断累计时间”、“首页中断结束时间”、“实时通断情况”。目前系统首页只显示当天网站断开的情况信息，如果需要看更早的历史网站断开情况，可以到站点可用性模块查看。

1：链接名称：显示所监控网站的名称。

2：首页中断开始时间：记录首页中断时，最初的开始时间。

3：首页中断累计时间：记录首页中断从起初到目前的累计时间。

4：首页中断结束时间：记录首页中断结束的时间。

5：实时通断情况：记录网站首页实时的通断情况。

6：操作：点击‘验证网站连通状态’可以打开网站链接。

1. **平均DNS超出阈值**

系统默认阈值为3000毫秒，该阈值的设置位置在系统管理—监控配置—阈值设定。

1. **平均下载超出阈值**

系统默认阈值为3000毫秒，该阈值的设置位置在系统管理—监控配置—阈值设定。

## 2、 安全监控

## （1）变更统计

变更统计汇总一天网站的文字、图片、链接、脚本的变化，可以设置查询的日期、时段，通过高级查询可以进一步设置过滤的内容。



## （2）文字监测

文字监测避免了网站首页出现敏感文字内容时管理人员与领导还不知情，并且采用了文字对比的机制，与被修改前的内容可以实现改动内容的对比，更是方便了管理人员对监控页面实时的更新状况有一个了解，避免发生政治性敏感问题。

如下图所示：

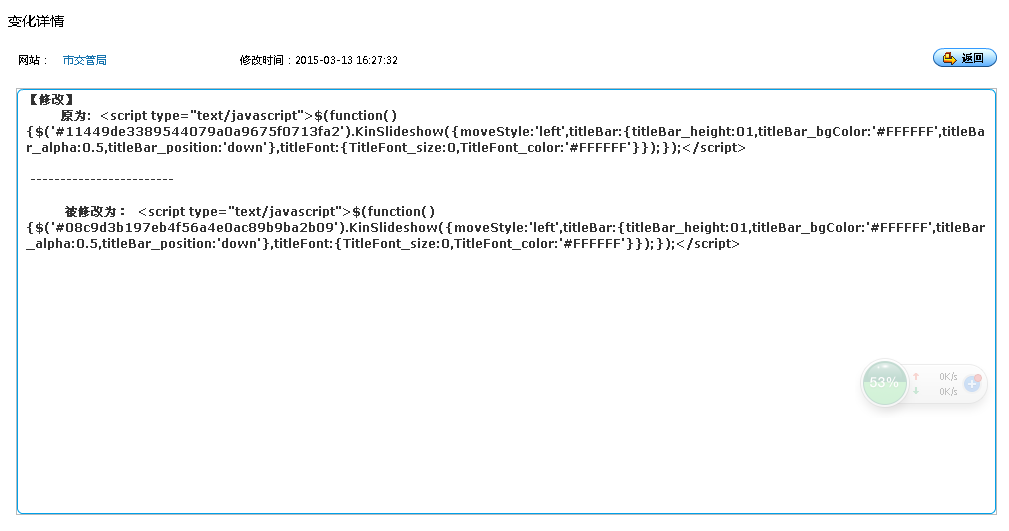


## （3）链接监测

链接监测显示对首页链接更新状况，原连接与更改后的新连接进行对比的结果。

## （4）脚本变化

实时监测脚本的变更数据。



## （5）图片监测

通过首页图片监测，可以避免网站上被挂有一些带有敏感信息的图片，当网站有更新的图片时，网站上的所有图片都被展示出来，由我们的监控人员分析是正常的还是非法的，大大的提高了监控人员的工作效率，并且能够及时发现，避免了政治性敏感问题。

### （6）暗链扫描

“暗链”也称为黑链。如果再通俗的说一点“暗链”就是看不见的网站链接，放暗链的人希望借助政府、教育等网站来提升自己网站的权重。来达到推广自己网站的目的。

EW预警系统可以监测出暗链的链接，并指出暗链所在网站的链接。根据监测出暗链的连接，可以打开查看此暗链网页的内容是否属于用户网站需要的信息；根据监测出暗链所在的网页，可以及时锁定暗链所在位置，更方便管理人员及时做修改。

* 精确定位：

1：建议客户使用此模块对网站进行暗链扫描，精确率高，定位详细，可扫描网站首页、二级页面、三级页面的暗链。

2：报表可生成EXCEL格式的报表：首页为综合概况，后续为出现暗链网站的详情

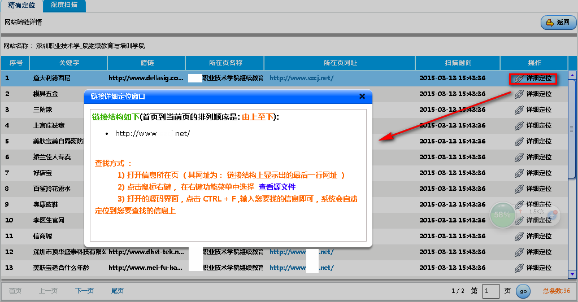
3：定向搜索：输入监测的网站全名、网站名称的部分字，在扫描结果中，查询该名称下是否存在暗链。

如下图所示：



用户可以针对每个网站点击‘查看详情’按钮进行查询，显示此网站暗链存在的详细信息， 包括(关键字、暗链、所在页面名称、所在页网址、扫描时间的详细定位)

如下图所示：



* 深度扫描：

深度扫描扫描结果包含暗链、外链，可以详细定位。

扫描外链的目的是从外链中获取非暗链的非法链接，比如明链等，更全面地扫描出网站上的非法链接。如果客户只需要查看暗链，建议使用‘精确定位’模块。

首页扫描：为网站首页的暗链、外链扫描的数据。

全网扫描：为网站首页及二级、三级页面的暗链、外链扫描的数据。

### （7）敏感词监测

根据与数据库敏感词库匹配，监测用户所重视的敏感词信息，每天更新统计的数据，且分别以柱状图、文字和数字两种方式表示。统计内容包括敏感词所在的网站、总数、监测时间、以及敏感词所在网页的连接等。点击查看详情，可以显示出敏感词所在的网页的地址，以及敏感词名称。

### （8）挂马监测

挂马检测显示扫描出来的网页木马，分为首页监测数据和全网监测数据，可以设置日期显示某天的扫描结果。

### （9）漏洞监测

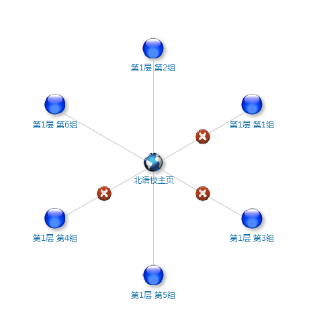
此界面显示最近一次漏洞扫描结果，反应当前的网站漏洞情况。

## 3、 性能监控

### （1）首页连通拓扑

拓扑图是通过网络爬虫技术完整而详细的分析出目标网站页面的分布结构，获得网站目录和内容结构，并自动形成可视化的网站拓扑图。这样显示出来的网站拓扑图结构符合用户的监控需求，如果有页面无法访问会显示红色标志，比较简练直观。通过拓扑，对网站群进行监控。监测网站的通断性能。当监控的页面WEB服务停掉时，可以通过短信、声音、邮件通知网络管理人员。

如下图所示：



1：通过此网站拓扑，可以清晰的看到出现故障的网站，为了方便管理人员追踪管理，拓扑中每个链接都可以双击打开，直接链接到web浏览器进行浏览网页。

2：如果网站打开速度超过20秒，或者打不开的情况，系统都会显示为断开。

### （2）首页连通状态

1：详细的显示所监控的网站**当前连通状态**，包括网站当前的通断性、时间点等。如果某个网站现在的链接中断，通过时间点来给管理人员提供一个参考的故障发生时间。

2：如果网站打开速度超过20秒，或者打不开的情况，系统都会显示为断开。

如下图所示：



## 4、网站运维

### （1）域名解析监测

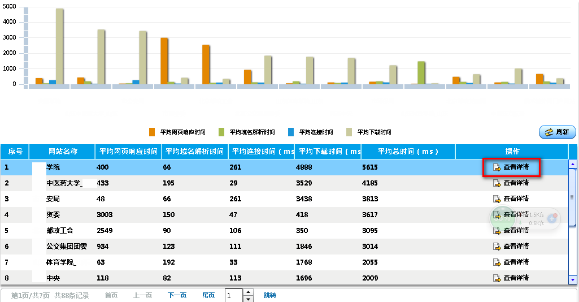
该功能对站点根域名以及根下的所有域名进行分析与监测；

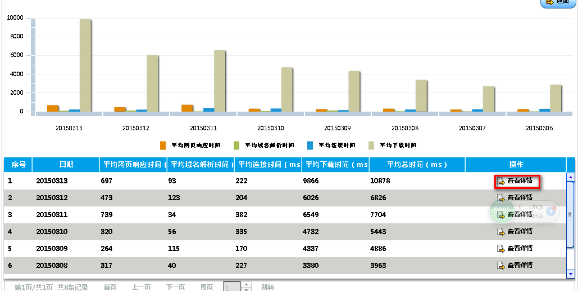
监测项目有：域名解析时间、站点响应时间、连接时间、页面响应时间、下载时间、及总时间。

对目标网站主要进行周期性监控探测，记录每次HTTP请求发出和对应WebServer的HTTP响应时间，记录网页第一个字节到达浏览器时间和传输完毕时最后一个字节到达的时间，从而描绘出目标网站长时间的性能变化趋势。站点每一次监控探测时间，速度探针将向告警中心发送一个报告代码。

根据域名解析时间，判断网页浏览是否流畅，如果解析时间过长，说明此网页出现故障或者需要做优化；同时如果网页打开速度慢，域名解析时间正常，而下载时间很长，说明并非是域名解析问题。

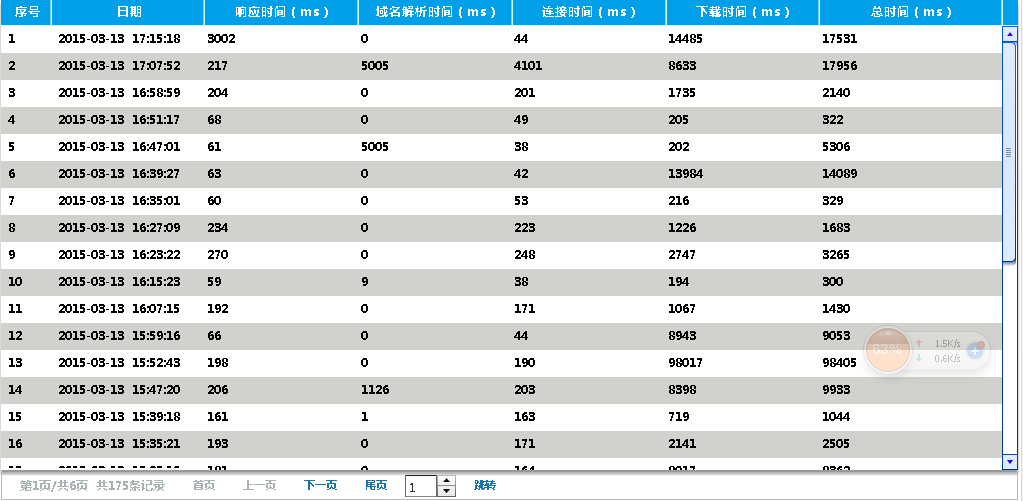
1. 页面响应时间：从访问页面请求发出，经过域名解析，确定地址和端口正确，直到webserver确认HTTP请求通过，并向客户机做出响应，这整个过程的总时间。
2. 域名解析时间：从客户机发出域名解析请求，到当地DNS查找缓存并返回A记录，整个过程的总时间。
3. 连接时间：从访问页面请求发出，通过域名解析，到webserver确认地址和端口都可以通过，并返回响应的总时间。
4. 下载时间：从访问页面请求发出，直到网页被完全下载并保存的总时间。
5. 总时间：从访问页面请求发出，直到网页完全保存并显示的总时间。





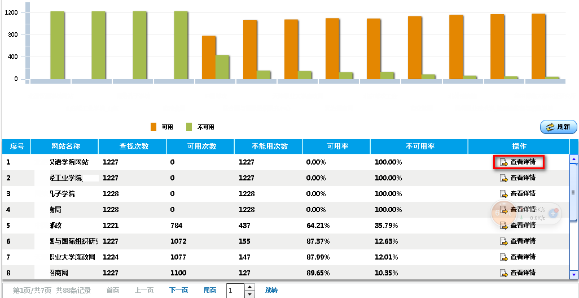
注：该图显示的时间，是从系统中记录的最初日期到目前所有检测记录的总时间，如需查看精确到日的时间里，网页下载打开情况，则双击所选行进行查看，如下图所示

如需查看精确到分钟时间里网页打开情况，点击上图中的查看详情进行查看，如下图所示：



### （2）：站点可用性

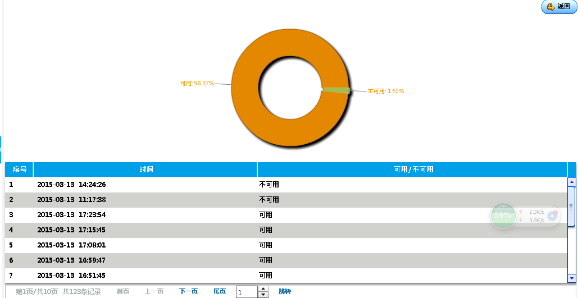
站点可用性监控功能用于监控网站、子网站、栏目和重点页面是否在线、系统记录对该站点监测次数、可用次数、不可用次数及不可用的百分比。



1. 网站名称：网站的url在该系统里设置时，所对应显示的名称，并对该网站进行了可用性检测。
2. 查找次数：针对于该网站检测可用性的总次数。
3. 可用次数：经过总的查找次数，其中可以打开连接的次数。
4. 不可用次数：经过总的查找次数，其中不可以打开连接的次数。
5. 可用率：可用次数占总查找次数的百分率。
6. 不可用率：不可用次数占总查找次数的百分率。

注：该图显示的时间，是从系统中记录的最初日期到目前所有检测记录的总次数，如需查看精确到日的时间里，网页性能情况，则点击查看详情进行查看，如下图所示

如需查看精确到分钟的时间里，网页性能情况，则点击具体日期的查看详情进行查看，如下图所示



## 5、站点诊断

### （1）错误页面

系统根据监测探针判断网站各站点是否含有无法打开或者打开网站时给出错误的返回值的链接，统计出错误页的数量，列出所有错误页的链接以及错误页返回的错误状态值。且以柱状图和文字、数字结合两种展示形式。

### （2）内外部链接错误

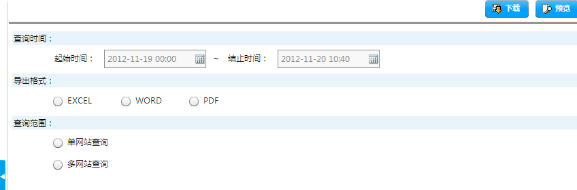
内外部链接错误指网站内部连接错误和本网站上挂载的其他网站的url出现链接错误的。系统会记录内外部连接数各有多少，以及内外部错误链接数各有多少。

错误链接探针对网站URL链接进行缺失扫描。记录所有错误链接，以及错误追溯路径，可以让用户通过“错误定位”直接找到发生错误的页面。

## 6、报表管理

报表管理针对各类信息提供多种查询与统计分析的方式，支持单网站导出报表、全部网站导出报表，还可以对网站进行报表分组，针对各组进行报表导出，可以支持任意设定输出项进行报表的输出。可以导出为PDF、EXCEL、WORD格式。

如下图所示：

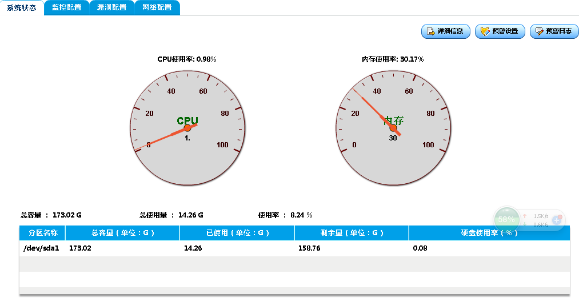


## 系统管理

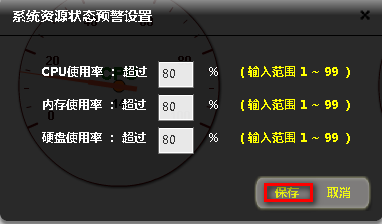
### （1）系统配置

（1）系统状态

系统状态显示当前系统的操作系统信息，cpu、内存、硬盘、网络的使用状况。



如果想设置硬件信息报警，点击预警设置。



设置完成后，需要保存才能生效。当出现报警信息时，报警内容反映在预警日志里。

(2)监控设置



即时监控：对即时监控（文字、图片、通断性）的参数进行设置，设置之前点击停止，设置完成后点击启动生效。

深度监控：在全网范围内进行扫描，把涉及到全网的敏感词、连接错误、暗链等进行扫描，上图是设置定时每天扫描的时间，设置前点击停止，然后点击启动按钮即可生效。

（3）漏洞配置



此处设置漏洞扫描的网站和进行扫描的当日时点，注意设置的时点必须在设置时点以后，否则不进行扫描。设置完成后点击启动，此时停止按钮变亮，可点击停止。扫描完成后停止按钮变灰失效，启动按钮变亮可用。如需再扫描，需进行配置后再点击启动。

（4）网络配置：在网络配置里可以添加设置的IP地址。

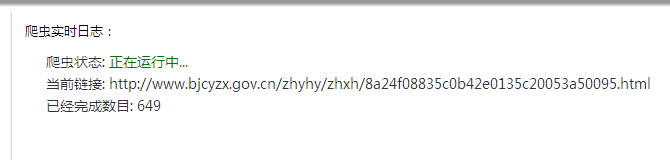
如下图所示：



### (2)系统日志

显示爬虫状态信息。

如下图所示：

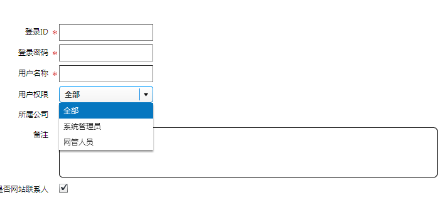


### (3)用户管理

用于添加和删除系统的用户，以及给用户拥有的权限。

如下图所示





### (4)网站管理

（1）网站配置：

用于配置系统监控的网站信息。网站管理里配置的所有网站信息，系统都会进行监测，并且显示出来。也可以说网站配置是系统显示信息的基础。

点击添加，即可添加网站信息，如下图所示：



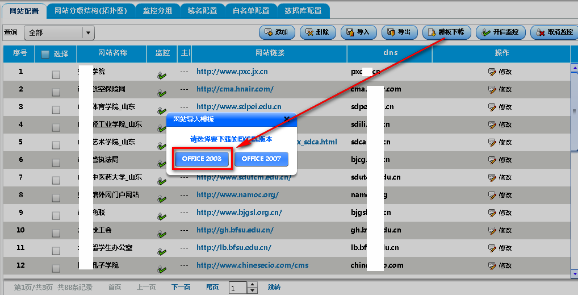
网站名称：网站的实际名称，或者是用户自定义的名称均可

网站链接：可以有效打开网站的url链接（如果是跳转页面，需添加跳转以后的链接。）

IP：可以有效打开网站的IP地址（注：网站链接和IP可以二选一的方式添加）。

是否监控：选择表示系统会对该网站进行监测，不选择表示此网站填写的所有信息还会保存，但系统不会对该网站做任何监测。

批量导入网站，先下载模板。



模板填写格式：



然后点击导入选择模板文件即可批量导入网站。



此外可以选中网站点击开启监控/取消监控设置是否监控网站。

（2）网站分级结构（拓扑图）：对网站进行拓扑展示分组的设定。先选中左边需要添加网站的分组，然后选中右边的网站，点击分配成员即可。可以修改组名，删除分组。点击初始化按钮将恢复到未分组状态。

如下图所示：



（3）监控分组：使用与网络分级结构类似。方便在网站配置里对网站批量管理。

（4）域名配置：该模块无需设置，添加完网站链接以后，系统自动识别域名地址。可进行修改。

如下图所示：



（5）白名单配置：加入白名单的网站，当系统爬取得数据中含有这些链接，系统默认为正常数据，不会认为是暗链。如下图所示：



（6）数据库配置：清空系统中的数据。（需要确认3次才可成功）。

### （5）敏感词配置

（1）敏感词配置：用于配置系统监控站点的敏感词，词库。用户可自行添加敏感词。

如下图所示：



### （6）发送配置

（1）邮件服务器配置：

配置发送邮件报警的发信邮箱的信息，需要配置邮箱服务器地址、端口、给系统一个邮箱地址即发信人邮箱地址、发信人邮箱密码。（发信人地址和收信人地址可以相同）保存生效。

2）邮件收件人配置

配置收取报警邮件的收件人邮箱信息，可选择收取报警的内容、时间、网站。

****

（2）短信发送（需要接短信猫）

短信发送的报警内容为汇总信息，没有详情。点击页面右侧添加，即可添加联系人的信息，其中‘手机号码’为必填项目。如下图所示



### （7）发送记录

记录邮件发送情况。

### （8）报表配置

在此可以进行导出报表的分组，方便在报表管理中导出某些特定网站的报表。最多可自定义10组。如下图所示：

