

# 风险行为智能报表的使用

风险行为智能报表的作用是根据用户的上网关键字、上网行为、上网流量等特征，统计内网用户指定的上网信息，并根据这些信息和数据特征做出相应的风险分析，以报表的形式呈现给管理员。

## 1. 风险行为智能报表模板的设置

**步骤一：设置“报表名称”、“时间”、“周期”。**

设置界面如下图所示：



**以设置离职风险报表为例，**

【报表名称】用于设置生成的报表名称。

【时间】用于设置生成报表时统计的每天日志的时间范围。

【周期】用于设置此报表生成的周期时间，可以设置“每天”、“每周”、“每月”。系统自动生成时是生成前一天、前一周和前一月的报表。

**步骤二：设置报表的统计条件。依照您生成的报表类型设置相关的行为特征，可以设置的条件包括“关键字”、“行为特征”、“流量特征”、“时间特征”。**

设置界面如下图所示：

**“关键字”：**用于统计通过搜索引擎、WebBBS、Webmail 和 IM 聊天记录的关键字，本例中：在关键字列表中设置与“离职”相关的关键字，并定义阈值（阈值：当含有该关键字的记录总数超过该阈值时就会被认为有风险迹象）。当用户日

志中包含设置的关键字并且次数超过阈值时则认为存在风险，并记录其关键字次数。（阈值最小值为 1，最大值为 65535，也就是说关键字只出现一次是不会有告警的）



**“行为特征”**：用于设置与此类风险相关的应用行为特征，并设置阈值（安全阈值的作用是：仅当风险行为次数超过该值时才会被认为有风险迹象）、风险权重（风险权重指的是风险特征等级，权重越高，说明该特征越重要，在最后风险指数中所占的比重也越大）等。

比如本例中需要统计的是离职风险，则“访问求职招聘网站”可作为行为特征加以统计，设置界面如下：设置访问“求职招聘”类网站超过 15 次时，则认为有风险迹象（阈值越大说明该特征越不重要，或者说这种行为越能够被容忍）。



**“流量特征”**：用于设置与此类风险相关的应用流量特征，并设置阈值（阈值的作用是：仅当风险行为流量超过该值时才会被认为有风险迹象）、风险权重（风险权重指的是风险特征等级，权重越高，说明该特征越重要，在最后风险指

数中所占的比重也越大) 等。

比如本例中需要统计的是离职风险，则“访问求职招聘网站”的流量可作为流量特征加以统计，设置界面如下：访问“求职招聘”类网站流量超过 5MB，则认为有风险迹象。



※ 如果需要设置“总流量阈值”，则设置的总流量阈值不得小于各特征值之和，勾选检测“总流量阈值”后，只有页面上列出的所有特征之和大于总阈值时才认为有风险。

**“时间特征”**：用于设置与此类风险相关的应用时间特征，并设置阈值（阈值的作用是：仅当风险行为时间超过该值时才会被认为有风险迹象）、风险权重（风险权重指的是风险特征等级，权重越高，说明该特征越重要，在最后风险指数中所占的比重也越大）等。

比如本例中需要统计的是离职风险，则“访问求职招聘网站”的时间可作为时间特征加以统计，设置界面如下：访问“求职招聘”类网站流量超过 0.5 小时，则认为有风险迹象。



**步骤三：设置需要进行此类风险行为分析的用户组、排除用户名、订阅等**

信息，界面如下图所示：



【组名】：用于设置需要进行此类行为分析的用户组。

【排除用户名】：用于设置以上设置的组中不需要进行统计分析的用户（排除用户”是完全不参与统计的，最终统计文件里的总用户数也不会包含他们）。

【风险报告生成】：用于设置报表中列出前多少名有此类风险的用户，范围是 1-100。

【订阅】：用于设置此报表生成后自动发送的邮箱地址，可填写多个邮箱地址，用分号隔开。勾选<生成的报表无内容时也发送到订阅邮箱>则报表生成后如果没有内容也会发送到订阅的邮箱地址。

点击<保存配置>，则将此报表的设置保存为模板，此模板将按照设定的统计周期和统计条件，计算每个用户风险指数，最后根据指数大小排列，生成风险行为智能报表。

※ 其他类型的报表模板设置不再赘述，可参考以上的设置。

## 2. 查看风险行为智能报表的模板

点击<智能报表模板>，用于查看已经保存的报表模板，界面如下图所示：



【报表名称】用于显示定义的报表名称；

【报表类型】用于显示报表的周期、类型等信息；

【最新生成时间】用于显示此类报表最后生成时间，并且显示最后一次生成的报表中是否有风险行为；

【用户】用于显示设置此报表模板的数据中心用户，admin 可以查看所有用户设置的报表模板，但其他用户只能查看自己定义的模板及对应生成的报表。

【操作】包含<编辑>、<删除>、<生成>、<查看>等操作。

<编辑>用于重新编辑对应的模板设置；

<删除>用于删除对应的模板；

<生成>用于手动点击生成风险报表，手动在页面上点生成是生成以系统当前时间为基准的当天、当周和当月的报表。

<查看>用于点击链接到历史报表，显示对应的报表模板生成的历史报表。

【操作信息】用于显示可生成的报表日期，以及生成报表的进度等信息。

【智能报表新增向导】用于链接到生成报表模板的向导，用于新增模板。

【导入配置\导出配置】用于将已设置的报表模板进行导入和导出。

【全部生成】用于手动生成所有的报表。

【删除所有】用于一次删除所有的报表模板。

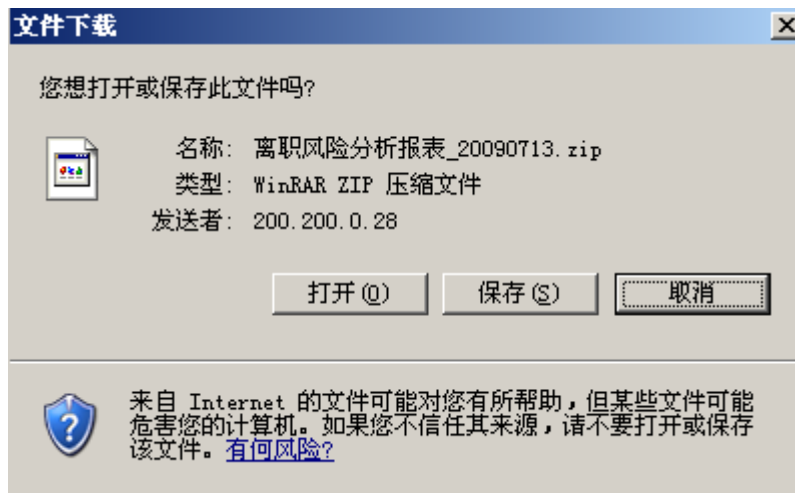
### 3. 查看已生成的风险报表

已生成的历史风险报表，可以在“历史报表“中进行下载查看。如下图所示：

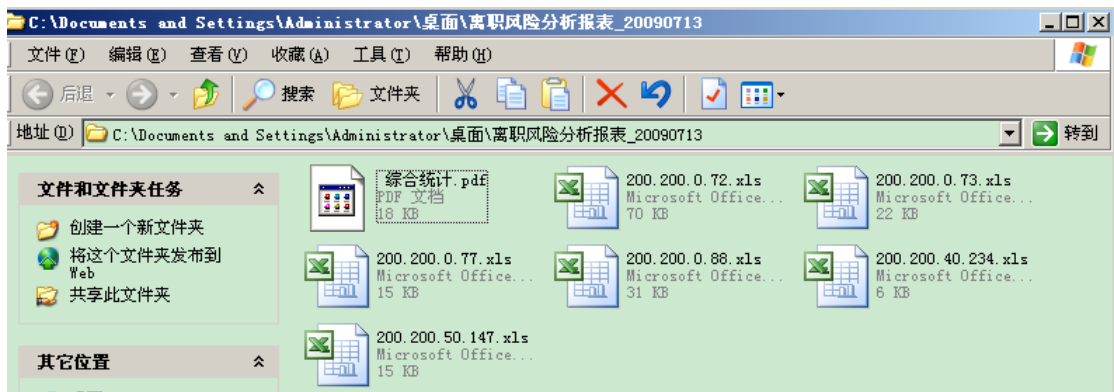


【报表名称】由报表模板名称和报表生成时间组成。

【操作】点击<下载>，将报表下载到本地进行查看，如下图所示：



将此压缩包保存到本地，进行解压，解压后，可以看到此压缩文件中包含如下图所示的文件：



“综合统计.pdf”是用户风险排名的统计表，里面包含各用户风险行为值等信息。

其他的 excel 文件，保存的是对应用户的详细风险行为，包括风险行为的详

细记录等信息。

打开“综合统计.pdf”，如下图所示：



【汇总评估图】中用柱状图列出前十名有风险的客户，以及对应的风险指数（风险指数：由风险行为的次数、流量、时间以及各种行为特征对应的风险权重计算得出，量化用户的行为风险程度）

【用户风险排行】用表格的形式列出有风险行为的用户，并进行排名，【风险明细】用于显示有风险的行为特征。

点击列表中的用户名，即会链接到对应用户的 excel 表，显示用户的详细行为记录，例如：点击用户名“200.200.0.72”，打开如下 excel 表格：

	A	B	C
1	<b>200.200.0.72总体评估</b>		
2	总体风险指数	3503.29	
3	时间范围	00:00:00 - 23:59:59	
4	统计日期	2009年07月13日 - 2009年07月13日	
5	周期	每天	
6			
7	<b>具体风险表</b>		
8	<b>序号</b>	<b>风险特征</b>	<b>实际指数</b>
9	1	上网行为	3503.29
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			

“Summary” 用于显示此用户的总体评估；

“Action Details” 用于显示此用户的行为明细，如下图所示：

	A	B	C	D	E	F
1	<b>200.200.0.72行为明细</b>					
2	风险指数: 3503.29					
3	风险特征包括下列应用(安全阈值): HTTP应用:WebMail,200次;邮件:发送邮件,200次;访问网站:求职招聘,15次					
4						
5	<b>访问网站:求职招聘 详细分析结果(总计293条记录 更多记录请到数据中心查询)</b>					
6	<b>序号</b>	<b>URL</b>	<b>网站类型</b>	<b>行为拦截明细</b>	<b>日期与时间</b>	
7	1	ehire.51job.com/rvs/a.aspx?c=325156&r=29775561	求职招聘	被记录	2009-07-13 16:27:17	
8	2	ehire.51job.com/rvs/a.aspx?c=325156&r=49627149	求职招聘	被记录	2009-07-13 16:15:42	
9	3	ehire.51job.com/rvs/a.aspx?c=325156&r=18408955	求职招聘	被记录	2009-07-13 16:14:50	
10	4	ehire.51job.com/rvs/a.aspx?c=325156&r=18408955	求职招聘	被记录	2009-07-13 16:14:46	
11	5	ehire.51job.com/rvs/a.aspx?c=325156&r=31082488	求职招聘	被记录	2009-07-13 16:14:37	
12	6	ehire.51job.com/rvs/a.aspx?c=325156&r=56349569	求职招聘	被记录	2009-07-13 16:14:30	
13	7	ehire.51job.com/rvs/a.aspx?c=325156&r=56349569	求职招聘	被记录	2009-07-13 16:14:29	
14	8	ehire.51job.com/rvs/a.aspx?c=325156&r=16038515	求职招聘	被记录	2009-07-13 16:14:25	
15	9	ehire.51job.com/rvs/a.aspx?c=325156&r=48906618	求职招聘	被记录	2009-07-13 16:14:23	
16	10	ehire.51job.com/rvs/a.aspx?c=325156&r=24775735	求职招聘	被记录	2009-07-13 16:14:13	
17	11	ehire.51job.com/rvs/a.aspx?c=325156&r=51388528	求职招聘	被记录	2009-07-13 16:14:11	
18	12	ehire.51job.com/rvs/a.aspx?c=325156&r=24775735	求职招聘	被记录	2009-07-13 16:14:07	
19	13	ehire.51job.com/rvs/a.aspx?c=325156&r=58637392	求职招聘	被记录	2009-07-13 16:14:04	
20	14	ehire.51job.com/rvs/a.aspx?c=325156&r=54312737	求职招聘	被记录	2009-07-13 16:13:52	
21	15	ehire.51job.com/rvs/a.aspx?c=325156&r=27680283	求职招聘	被记录	2009-07-13 16:13:46	
22						

※ 其他报表的查看不再赘述，可参考以上的介绍。