ME 系列行为管理路由器审计功能

用户手册

（适用于 ME802、ME802W、ME808、ME808W、ME908、ME1008 系列产品）

大连网月科技开发有限公司

版权声明

版权所有 2009-2012，大连网月科技开发有限公司，保留所有权利。使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。如有变更，恕不另行通知。

遵守所生效的版权法是用户的责任。在未经大连网月科技开发有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

大连网月科技开发有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经大连网月科技开发有限公司明确书面许可的情况下，使用本文档 资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

第一章 审计功能开启方法

1.1 挂载 U 盘

路由器升级到 2.0 软件版本（2.0 软件版本以后支持审计功能），安装上 U 盘（安装在路由器的前面板上），启用审计功能，然后在审计功能的磁盘管理里面就可以看到 U 盘，点击初始化，然后就可以使用。

1.2 启用审计功能

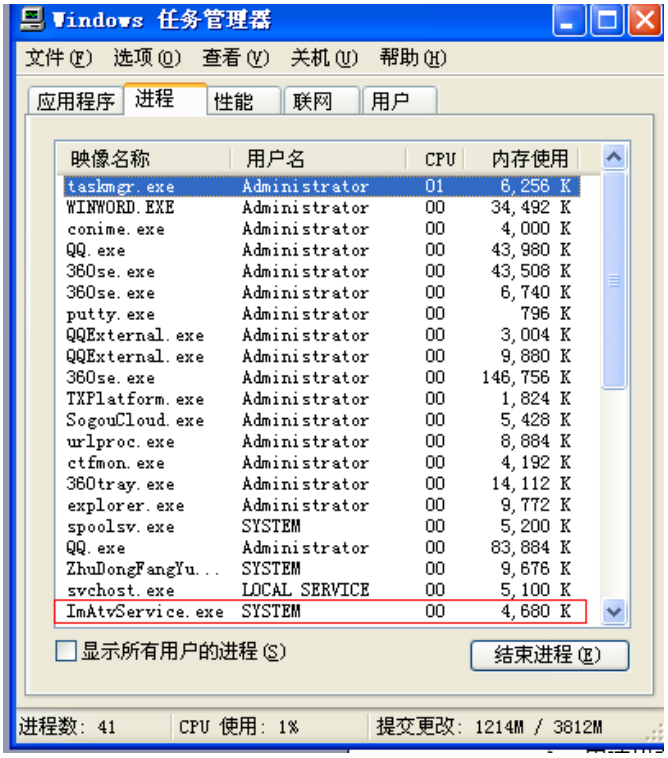
在行为审计—审计管理中启用审计功能，然后在审计授权功能那里点申请试用。（默认可以免费试用 1 个月，到期后不续费，无法使用此功能），如下图：

1.3 绑定用户

在行为管理—用户管理中将动态用户修改成静态用户，编辑页面修改带星的任何一项，然后点确定，用户状态变为静态用户，如下图：

1.4 安装客户端

在行为管理—客户端管理中，启用强制安装，然后选择安装对象。（启用后打开任何一网页都会提示客户端下载界面，然后安装就可以，安装后在安装列表里面会显示已安装）。安装成功后进程列表里会有 ImAtvService.exe 这个进程，如下图：



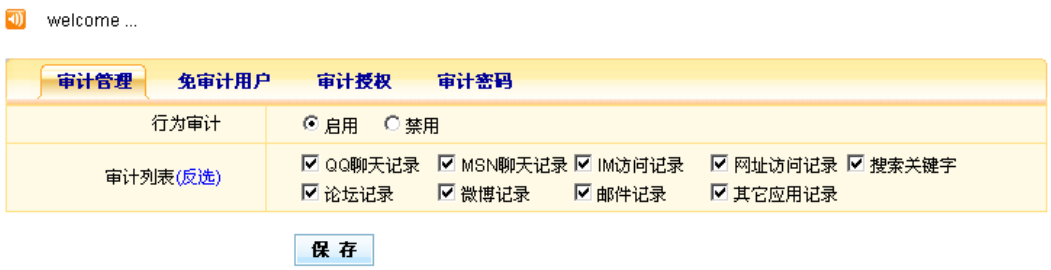
完成上述功能后，审计功能就可以正常使用了，（默认审计密码是 admin）。

第二章 审计功能详细配置指南

2.1 审计管理

2.1.1 审计管理

您可以在本功能中对行为审计功能进行启用或禁用的操作，并且可以对不同的审计内容进行选取及过滤操作，还可以进行对审计用户进行选择，审计功能的授权操作等，如下图：



(1) 行为审计：您可以选择启用或者禁用行为审计功能。

(2) 审计列表：您可以选择对哪些审计内容进行记录（打钩表示对此功能启用审计，不打钩表示对此功能不启用审计）。

2.1.2 免审计用户

在本页面中，您可以通过对不想启用审计的用户进行例外的操作，如下图：

(1) 免审计用户:不启用审计功能的用户会在此列表中显示。

(2) 可选用户：所有在行为管理-用户管理中绑定了的用户都会在此列表中显示。

(3) 保存：写入路由器的静态配置，使参数生效。

※ 提示：

(1) 本页面中，可通过“ >> ”将免审计用户移动到可选用户中。

(2) 本页面中，可通过“ << ”将可选择用户移动到免审计用户中。

2.1.3 审计授权

在本页面中您可以对审计功能进行授权管理的操作，如下图：

(1) 授权状态：此处初始状态为未授权状态，您可以点击申请授权功能免费试用一段时间的审计功能。

(2) 最后充值时间：显示用户最近一次针对审计功能的充值时间。

(3) 最后更新时间：显示用户最近一次更新审计状态的时间。

(4) 授权到期时间：显示用户审计功能到期时间。

(5) 更新：对审计功能的授权状态进行更新操作。

(6) 充值：输入授权卡密码后，点击充值按钮，可对授权时间进行充值操作。

※ 提示：

(1) 审计功能按时间收费，目前初次使用，您用一个月的免费试用时间。

(2) 点击申请授权之后，请再点击更新按钮，对授权状态进行更新。

2.1.4 审计密码

在本页面中您可以更改审计功能的初始密码，默认初始密码为 admin，如下图：

(1) 原始密码：修改密码前的原始密码，若您未曾修改过，默认密码为 admin。

(2) 新密码：输入您想要修改的新密码。

(3) 密码确认：再次输入您想要修改的新密码。

(4) 保存：写入路由器的静态配置，使参数生效。

※ 提示：

凡带有 “*” 标识的项是必须填写的

2.2 磁盘管理

2.2.1 磁盘管理

在本配置页面中，您可以对存储审计信息的存储设备进行管理，如下图：

※ 提示：

(1) 首次使用请先点击初始化按钮，点击之后如下图：

(2) 如果在未卸载情况下拔出磁盘，数据可能会丢失。

(3) 如果自动挂载失败，请点击挂载按钮。

(4) 格式化会清空磁盘上的所有审计日志。

2.2.2 磁盘日志

在本配置页面中，您查看到磁盘的挂载以及卸载等日志信息，如下图：

2.3 IM 聊天记录

在本配置页面中，您可以查看局域网内主机的 IM 聊天记录信息。

2.3.1 QQ 聊天记录

在本页面中，您可以查看在内网电脑中所登陆的 QQ 的聊天信息，如下图：

(1) 本地 QQ：在客户机登陆的 QQ 号码。

(2) 用户：在行为管理-用户管理中编辑的用户名称。

(3) 收/发消息数：此 QQ 接收以及发送的消息数目，接收在前，收发在后。

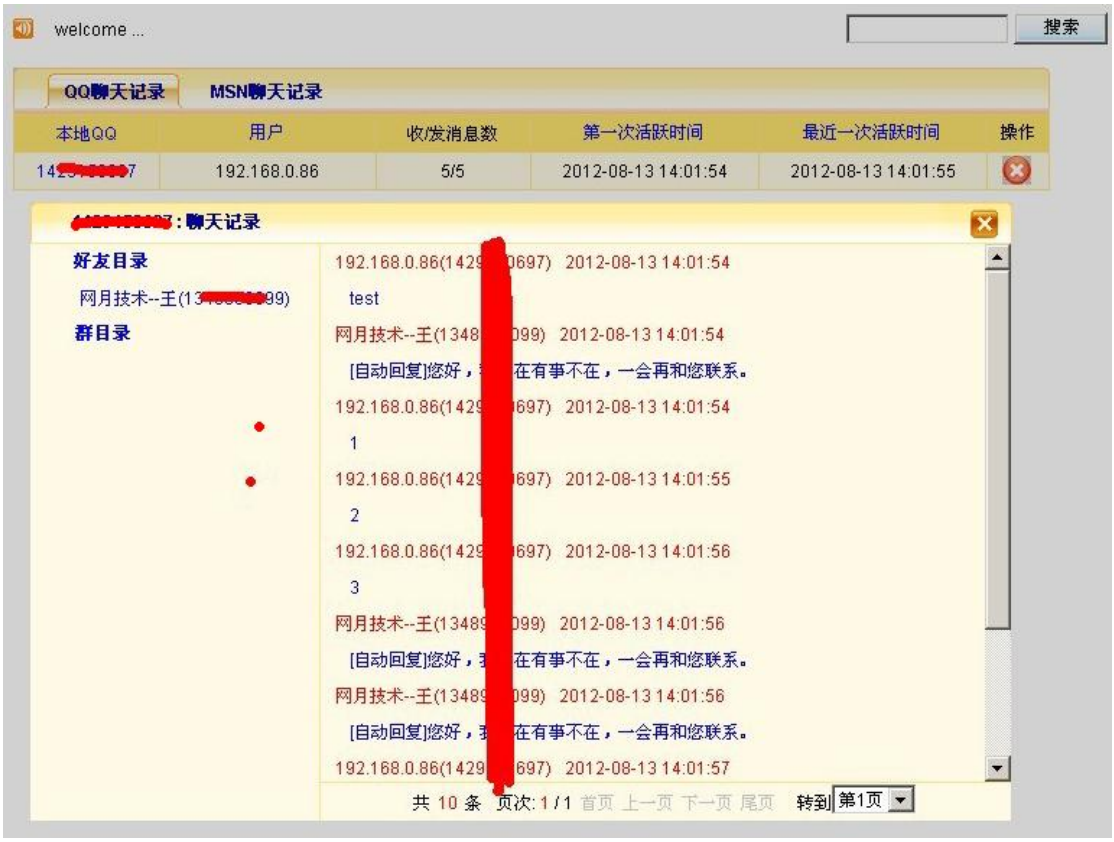
(4) 第一次活跃时间：此 QQ 第一次发送信息或接收到信息的时间。

(5) 最近一次活跃时间：此 QQ 最后一次发送或接收到信息的时间。

(6) 操作：可删除对应 QQ 的聊天记录。

点击相应的 QQ 号码，即可查看聊天信息的具体内容，查看时需要输入审计密码，如下图：

输入密码后，便可查看聊天信息的具体内容，如下图：



※ 提示：

通过右上角的搜索栏，可对想要查看的用户进行搜索。

2.3.2 MSN 聊天记录

在本配置页面中，您可以查看在内网电脑中所登陆的 MSN 的聊天信息，如下图：

(1) 本地 MSN：在客户机上登录的 MSN 的号码。

(2) 用户：在行为管理-用户管理中编辑的用户名称。

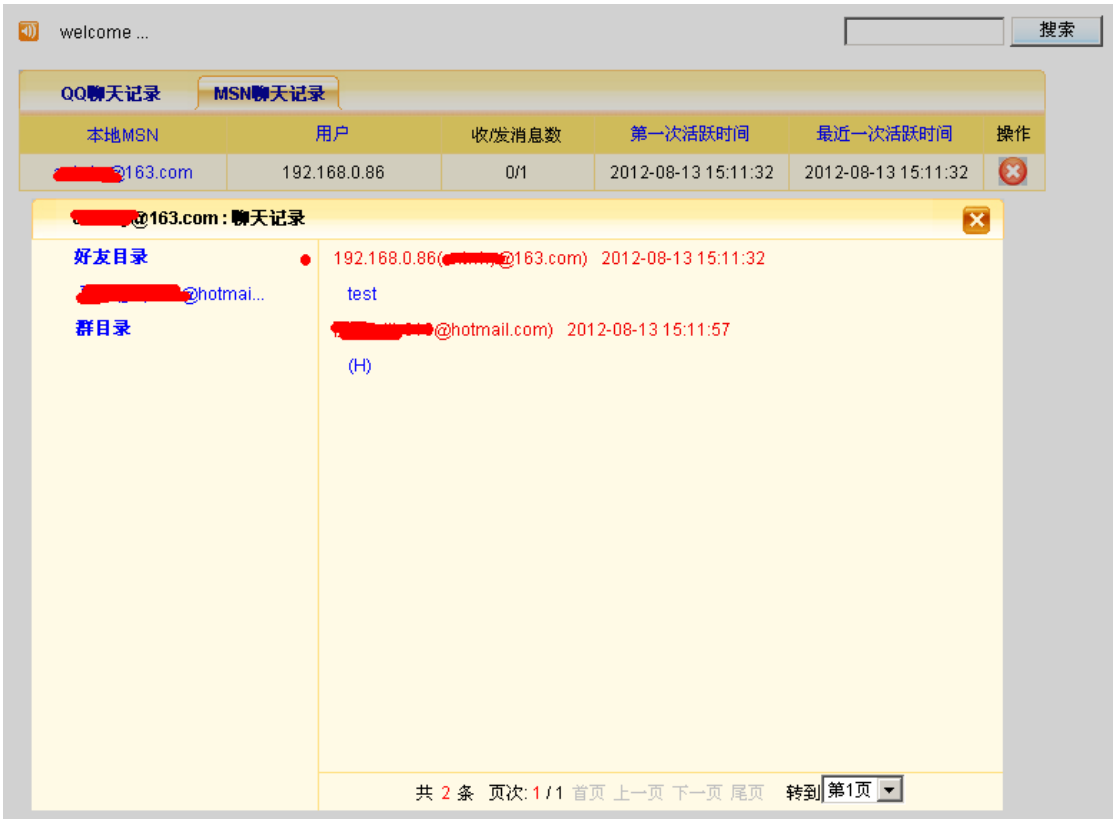
(3) 收/发消息数：此 MSN 接收以及发送的消息数目，接收在前，收发在后。

(4) 第一次活跃时间：此 MSN 第一次发送信息或接收到信息的时间。

(5) 最近一次活跃时间：此 MSN 最后一次发送或接收到信息的时间。

(6) 操作：可删除对应 QQ 的聊天记录工作线路：要访问这个域名的外网路线。

点击相应的 MSN 号码，即可查看聊天信息的具体内容，查看时需要输入审计密码，输入密码后，便可查看聊天信息的具体内容，如下图：



※ 提示：

通过右上角的搜索栏，可对想要查看的用户进行搜索。

2.4 IM 访问记录

通过本功能，您可以查看内网用户都登录了哪些 IM 软件，如下图：

(1) 用户名：在行为管理-用户管理中编辑的用户名称。

(2) IP：登录 IM 聊天软件的客户机的 IP 地址。

(3) IM 类型：对应客户机所登录的 IM 软件的类型，以图标形式显示。

(4) 账号：对应客户机所登录的 IM 软件的账号信息。

(5) 状态：登录的 IM 软件的登录状态

(6) 时间：IM 聊天软件的登录时间。

(7) 详细：可以查看登录的 IM 软件的详细情况。

※ 提示：

通过右上角的搜索栏，可对想要查看的用户进行搜索。

2.5 网址访问记录

在本配置页面中，您可以查看内网客户机所访问的网址信息，如下图：

(1) 用户名：在行为管理-用户管理中编辑的用户名称。

(2) URL：对应用户访问的网址 URL，鼠标点击之后可连接到此 URL。

(3) 标题：对应用户访问的网址 URL 的标题。

(4) 状态：用户访问的 URL 的状态信息。

(5) 时间：用户访问此 URL 的时间。

(6) 详细：可以查看本条网址访问记录的详细情况。

※ 提示：

通过右上角的搜索栏，可对想要查看的用户进行搜索。

2.6 搜索关键字

在本页面中您可以查看内网用户在搜索引擎中所输入的搜索关键字，如下图：

(1) 用户名：在行为管理-用户管理中编辑的用户名称。

(2) IP：此用户名所在客户机的 IP 地址。

(3) 搜索引擎：此用户所使用的搜索引擎，以图标形式显示。

(4) 关键字：用户在搜索引擎中输入的关键字内容。

(5) 时间：用户使用搜索引擎搜索关键字的时间。

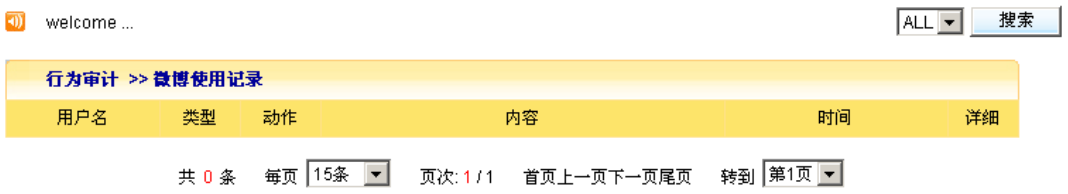
(6) 详细：可以查看本条搜索记录的详细信息。

※ 提示：

通过右上角的搜索栏，可对想要查看的用户进行搜索。

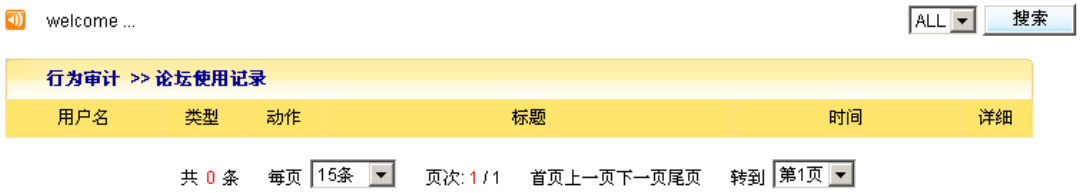
2.7 微博使用记录

在本配置页面中，您可以查看内网用户的微博使用记录，如下图：



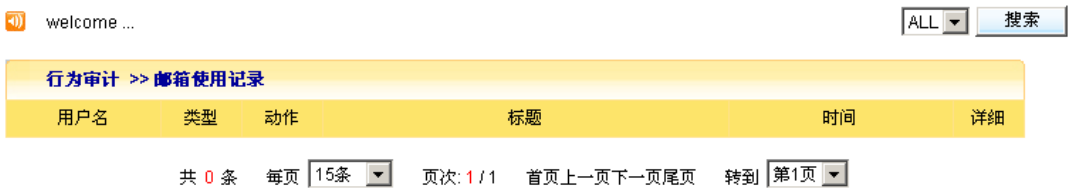
2.8 论坛使用记录

在本配置页面中，您可以查看内网用户的论坛使用记录，如下图：



2.9 邮箱使用记录

在本配置页面中，您可以查看内网用户的邮箱使用记录，如下图：



2.10 其他应用记录

在本页面中，您可以查看内网用户一些其他应用程序的使用记录，如下图：

(1) 用户名：在行为管理-用户管理中编辑的用户名称。

(2) 应用类别：用户所使用的应用程序的类别，以图标形式显示。

(3) 应用说明：对用户所使用的应用程序的说明，在内置数据库中搜集的程序之外的其他程序，以.EXE 的文件名显示。

(4) 状态：用户所使用的应用程序的状态信息。

(5) 时间：用户使用本条应用程序的时间。

(6) 详细：点击详细按钮，可查看本条应用程序的详细信息。

※ 提示：

通过右上角的搜索栏，可对想要查看的用户进行搜索。