

U-Mail[®]Gateway 使用手册

深圳市福洽科技有限公司

中国·深圳市福田区彩田路 3069 号星河世纪大厦 A 座 24 层 U-Mail 客服中心

电话: 800-999-6561 400-8181-568 传真: 86-755-82793235

网站: [Http://www.ComingChina.com](http://www.ComingChina.com) 邮箱: Services@comingchina.com

U-Mail®Gateway 使用手册.....	- 1 -
第一部分：U-Mail Gateway安装手册	- 4 -
1.产品说明.....	- 4 -
1.1 产品简介.....	- 5 -
1.2 产品特性.....	- 5 -
2. U-Mail安装.....	- 7 -
2.1 安装环境与设置.....	- 7 -
2.2 安装U-Mail.....	- 8 -
2.3 安装常见问题.....	- 16 -
2.4 序列号验证.....	- 20 -
第二部分：Gateway使用手册	- 20 -
1 登录	- 21 -
2 菜单结构.....	- 21 -
2.1 主菜单.....	- 22 -
2.2 设置.....	- 42 -
2.3 安全.....	- 56 -
2.4 日志/设置文件.....	- 70 -
2.5 注销.....	- 74 -
3 系统后台常用功能说明.....	- 122 -
第三部分：技术白皮书.....	- 123 -
1. U-Mail技术资料.....	- 124 -
2. 邮件域名DNS相关知识.....	- 125 -
2.1 什么是IP地址?	- 126 -
2.2 什么是固定IP地址?	- 126 -
2.3 什么是动态IP地址?	- 126 -
2.4 什么是域名? 域名由什么构成?	- 127 -
2.5 什么是DNS?.....	- 127 -
2.6 什么是A记录?.....	- 127 -

2.7 什么是NS记录?.....	- 128 -
2.8 什么是别名记录(CNAME)?	- 128 -
2.9 什么是泛域名解析?.....	- 128 -
2.10 什么是MX记录?	- 128 -
2.11 什么是IP反向解析?	- 129 -
2.12 什么是SPF记录	- 129 -
2.13 RBL是什么?	- 130 -
2.14 全国各地电信、联通、网通DNS服务器地址	- 130 -
3. U-Mail退信分析	- 137 -

第一部分：U-Mail Gateway安装手册



1.产品说明

1.1 产品简介

U-Mail GateWay 以广大企事业单位的邮箱应用需求为目标做了深入的开发，将邮件安全网关的功能发挥至极致，最大拓展了邮件网关的功能、性能和稳定性，在已有数千家企业单位应用需求的基础上做了大量改进，使之更加适合政府、教育、企事业单位、络服务商、集成商使用。

U-MailGateWay 高安全、高效率、高性能的企业邮局系统。支持 SMTP, SSL SMTP, POP3, SSL POP3, IMAP4, SSL IMAP4, WebMail, CA Server, TLS/SSL, S/MIME, Daytime 全功能服务的邮件安全网关。

1.2 产品特性

U-Mail 提供一流的 web 界面，强大的后台管理，完善的系统安全，反垃圾过滤，反病毒过滤，邮件监控管理等。

1.2.1 功能简介

提供优秀的 Web 支持，让您可以直接通过 IE 浏览器收、发电子邮件，更支持强大的 Web 远程管理服务，让您无需登录服务器，仅靠浏览器就可以实现对邮件网关全面管理。

多域名支持。

强大的后台管理功能， 具备操作日志、、邮件监控管理等。

软件安全性高。(除强劲的反垃圾，病毒邮件外，系统前后台管理都支持 128 位 SSL 安全连接)。

系统高度自动化管理，自动升级病毒代码库，垃圾邮件过滤规则。

1.2.2 完善的系统安全

支持数字证书服务并提供强大的管理功能，可直接在 WebMail 中撰写或阅读经过数字签名或数字加密的安全邮件(S/MIME)。提供军事级别的高安全强度(4096 位 DH/DSS 加密或 2048 位 RSA 加密)；

使用 TLS/SSL 标准安全套接字层通讯协议(1024 位 RSA 加密)，支持包括 SSL SMTP，SSL POP3，SSL IMAP4 安全通讯服务，防止网络侦听，使得通信更安全。

内嵌邮件 ip 监控，自动判断恶意的连接并拒绝掉。

1.2.3 强大的邮件监控管理

全面监视公司所有员工的邮件通信，包括 Outlook 和 Webmail 收发的邮件，即使员工将邮件已经删除仍然有备份。

总经理可以监控各个职能机构经理的邮件；各机构经理监控下面员工的邮件；系统管理员可以备份所有的邮件，当有员工误操作删除重要邮件的时候可以快速恢复。

1.2.4 垃圾邮件过滤

本系统使用第四代基于行为识别的过滤引擎，具有强大、设置灵活的垃圾邮件过滤设置，确保将垃圾邮件拒之门外。

1.2.5 反病毒过滤

反病毒模块同时扫描邮件的正文和附件，一旦发现问题，邮件服务器就会拒绝接收该邮件。有时候，系统会在收取这类邮件后将其隔离，尝试清除其中的病毒或者直接将其删除。

2. U-Mail安装

2.1 安装环境与设置

安装前检查域名解析是否正确，IIS 是否安装，防火墙与杀毒软件设置等。

2.1.1 服务器硬件设置

推荐服务器硬件配置：单 XEON + 2048M 内存。

2.1.2 支持的操作系统

U-Mail GateWay for win 版本 需要安装在 windows 2000/2003/2008 32 或 64 位的服务器操作系统上。

2.2 安装U-Mail

如果您还没有 U-Mail GateWay安装包，可以到 <http://www.comingchina.com> 去下载最新的安装程序

在安装系统之前，还必须选定操作系统平台，U-Mail for Windows 可以安装在 Windows 2000、Windows 2003 、Windows2008 操作系统上（建议打全所有的操作系统补丁）

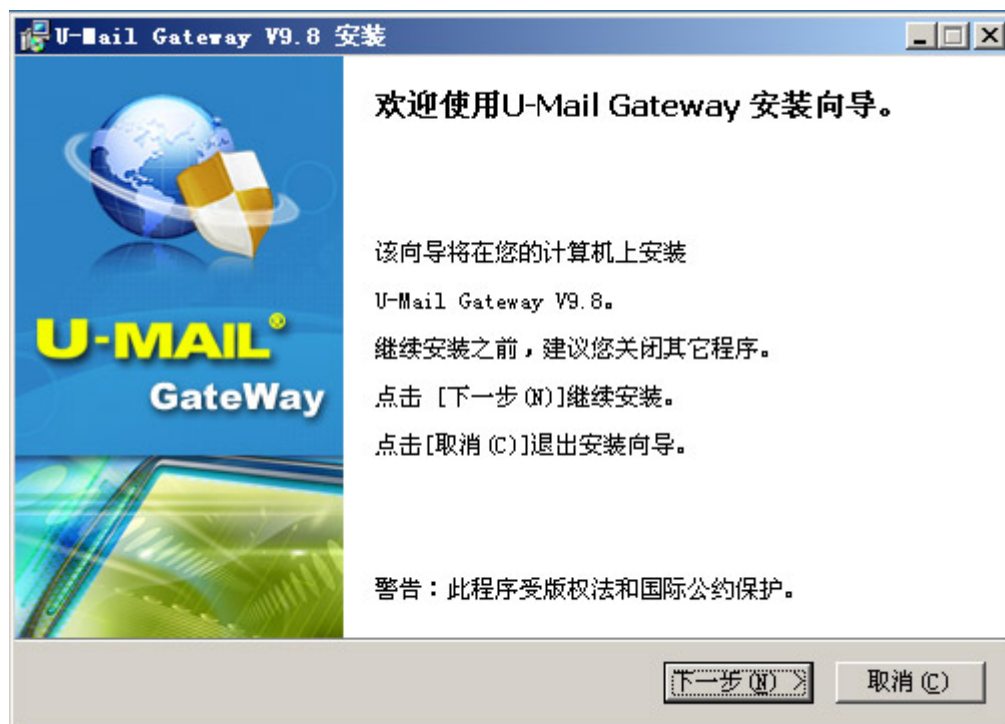
系统安装

在安装过程中和一般的软件类似，下面只给一些要注意的步骤，如安装组件、安装目录、以及设置管理员的登陆密码等。

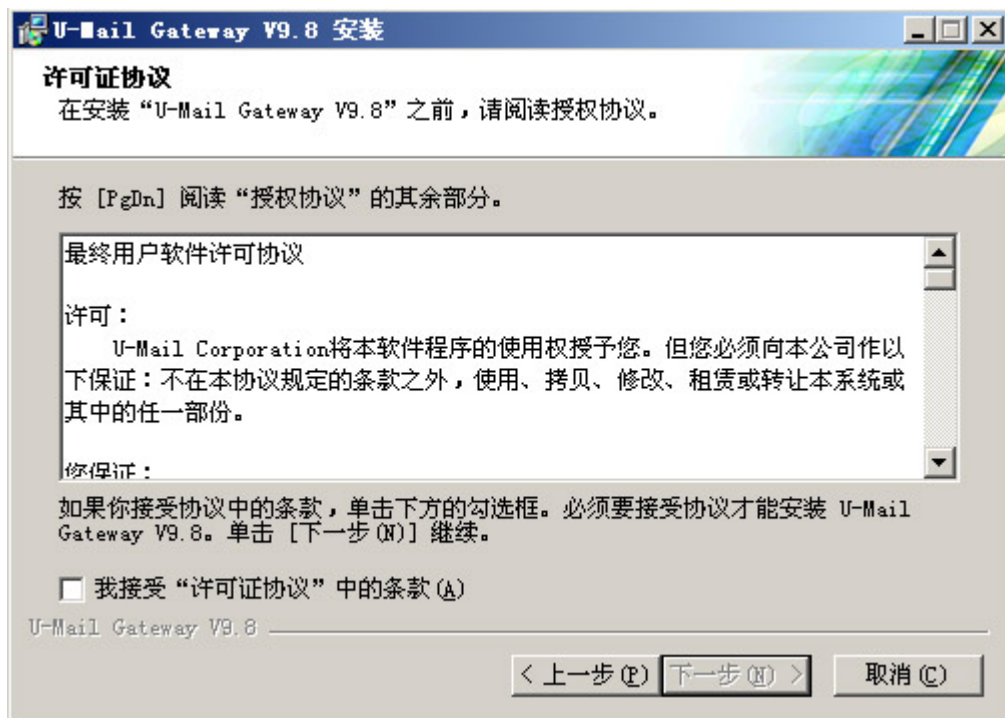
1) 开始安装，检测安装环境，这里我们用简体中文演示



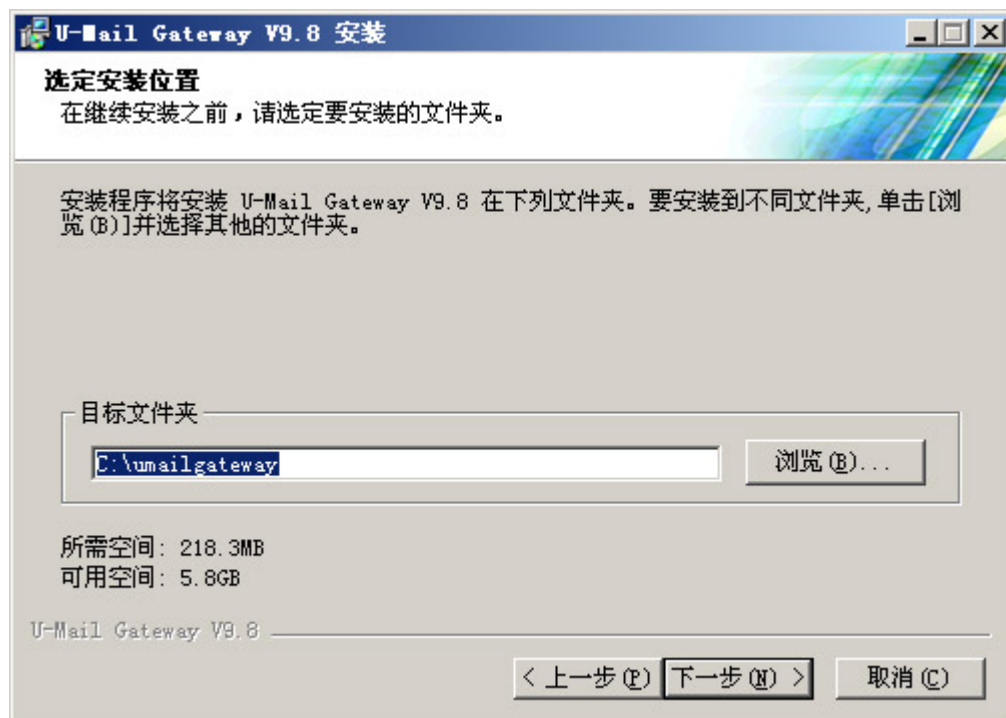
2) 安装向导



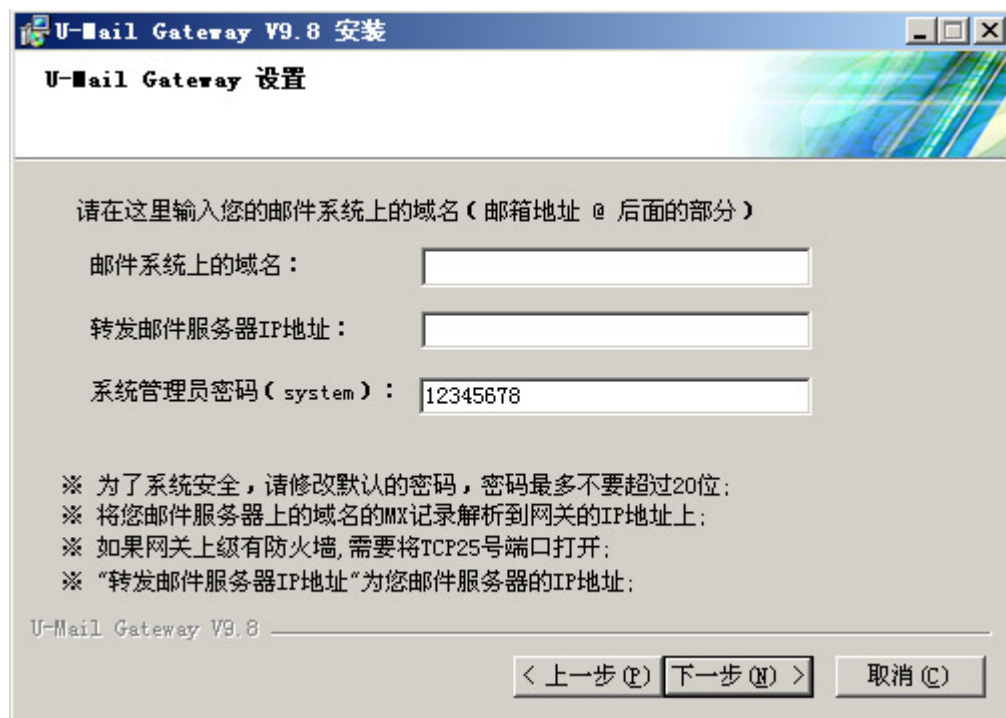
3) 授权条款



4) 选定安装位置



5) 设置



6) 开始安装



7) 安装



8) 安装完成



安装完成后点击完成即可。

2.3 安装常见问题

1、如果安装 U-Mail 出现如下图：



需要安装 windows instsller3.0 版本才可以进行安装 U-Mail。

下载地址: <http://www.comingchina.com/tmp/WindowsInstaller3140002435.rar>

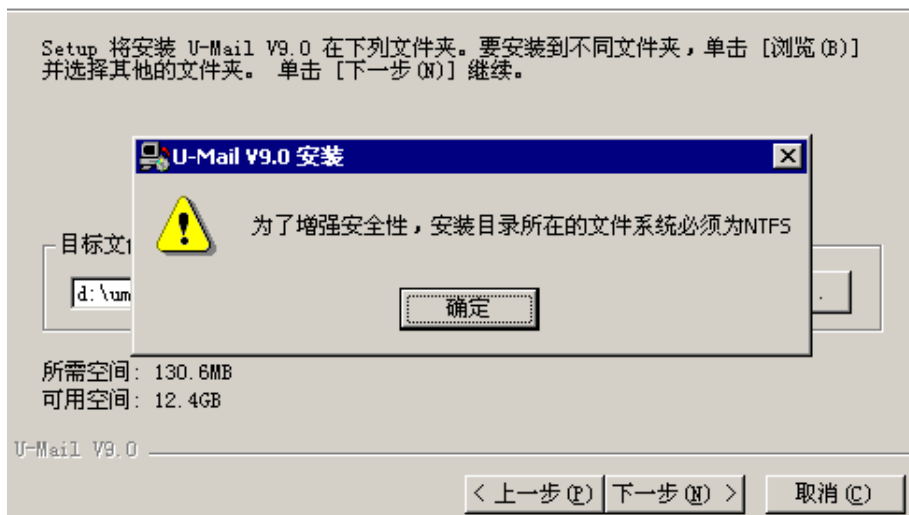
2、安装的盘符需要转换为 ntfs 格式吗?

Umail 做了一些安全设置, 必须把安装的盘符转换为 ntfs 格式才可以进行安装。如 d 盘格式为 fat32, 要转换为 ntfs, 则执行命令 `convert d: /fs:ntfs`

没有转换 ntfs, 安装会出现提示, 如图:

选定安装位置

在继续安装之前, 请选定要安装的文件夹。



3、服务器上有 PHP/MYSQL 的环境, 可以直接安装 U-MAIL 吗?

可以直接安装。

U-MAIL 有自己独立的 MYSQL 环境, U-Mail 的 MYSQL 使用 6603 服务端口, 服务名称为 UMAILMYSQL。不会覆盖当前操作系统的 mysql 设置, 不会和现有任何 PHP/MYSQL 环境冲突。

4、服务器上需要装杀毒软件吗? 装什么杀毒软件比较好?

需要。虽然 U-Mail 已经内置了卡巴斯基的杀毒引擎, 但这是邮件网关专用的, 只对邮件网关收发的邮件进行病毒过滤。Windows 平台的杀毒软件推荐用户安装 NOD32, 这也许是 WINDOWS 平台上最好的操作系统杀毒软件。

5、安装杀毒软件要注意哪些？

(1)关闭杀毒软件的邮件检测。

(2)杀毒软件排除下列目录：**umail** 目录下 **Queues** 和 **Users**（队列目录和用户邮件数据目录）

注意：某些杀毒软件 如 **McAfee**，默认会禁止 25 端口，导致邮件系统无法正常收发邮件。去掉这个对勾。

6、安装防火墙需要注意哪些？

如果开启 windows 自带防火墙或者安装其他防火墙软件，需要设置如下：

(1) 允许外面连接服务器 25、10000 端口，允许服务器访问外网的 25 端口。

25 端口为 **SMTP** 服务，服务器到服务器收发需要使用 25 端口。

10000 端口是 web 的系统管理后台，如果只在本机进行管理，可不开放。

(2) 如安装 **U-Mail** 过程中防火墙提示，选择允许安装 **U-MAIL** 期间所有应用程序的访问。

(3) 如果邮件服务器是放置在内网，请将外网 IP 地址的 25 端口映射到内网服务器。

7、为什么装好 U-Mail 之后，打开 webmail 之后弹出操作系统的密码框？

U-MAIL 邮件系统在安装的时候会在操作系统内新建两个 **U-MAIL** 专用帐号，分别是 **umail** 和 **mysql**，如果修改过操作系统的账户策略等操作，则这两个帐号的建立有可能失败，从而导致 **webmail** 不正常。

解决办法：手工建立帐号，打开控制面板—管理工具--计算机管理 然后手工建立两个帐号 **umail** 和 **mysql**，密码的设定用\umail\readme.txt 里面的密码，帐号属性为：永不过期、用户不能修改密码。

2.4 序列号验证

本地验证

安装好 U-Mail 重启后, 会出现注册 U-Mail 的提示, 点击“注册”, 在出现的页面中输入序列号即可。(可以退出桌面右下角的 u-mail 图标, 在开始——程序——U-Mail Gateway, 点击运行 U-Mail 程序, 可看到注册页面。)注意: 序列号与提供的主域名进行绑定, 此序列号终身使用, 不可更改。

如果 wscip.shell 对象禁用, 注册序列号的页面将会提示错误。

执行命令“regsvr32 WSHom.ocx”即可进行注册。

第二部分: Gateway使用手册



系统管理员后台 system 帐号主要针对系统方面的设置。可以设置域、用户、邮件列表、网关、邮件头翻译、IP 缓存、邮箱别名、附件、内容过滤器、邮件监控、DNS 黑名单、垃圾邮件过滤器、中转信任、IP 主机屏蔽、SMTP 验证、日志设置与查看等操作。默认设置已经是优化设置，一般不建议用户修改。如果对某些设置不清楚，请不要乱修改，以免影响邮件系统正常工作。

1 登录

在 IE 地址栏输入 `http://IP:10000`，即可看到以下登录页面，输入帐号密码即可。帐号为 `system`，默认密码是 `12345678`。还可以选择登录的语言，点击“登录”即可。

The image shows a login form with a green background. It contains three input fields: '帐号:' (Account) with 'system' entered, '密码:' (Password) which is empty, and '语言:' (Language) with a dropdown menu showing 'Chinese'. Below these fields is a green button labeled '登录' (Login). A mouse cursor is pointing at the button.

2 菜单结构

系统共有五个大的菜单按钮，包括主菜单、设置、安全、日志/设置文件、注销。

2.1 主菜单

默认进去 webadmin 后台, 显示的是“主菜单”中的“状态”。主菜单包括状态、我的帐号、我的邮件列表、域、用户、邮件列表、网关、选项等设置。



The screenshot shows the U-Mail webadmin interface. On the left is a sidebar menu with the following items: 状态 (Status), 我的帐号 (My Account), 我的邮件列表 (My Mail List), 域 (Domain), 用户 (Users), 邮件列表 (Mail List), 网关 (Gateway), 选项 (Options), 主菜单 (Main Menu), 设置 (Settings), 安全 (Security), 日志/配置文件 (Logs/Config Files), and 注销 (Logout). The '主菜单' item is highlighted. The main content area has a '刷新' (Refresh) button at the top left. It contains three sections: '服务器状态' (Server Status) with a table showing 'U-Mail Server' is 'Running'; 'U-Mail 统计' (U-Mail Statistics) with a table showing 9 users, 6 domains, 8 lists, and 0 gateways; and '统计信息: system@domain.com' (Statistics: system@domain.com) with a table showing 2 emails, N/A allowed emails, 0.00 MB used space, and 307200.01 MB allowed space.

程序	状态
U-Mail Server	Running

用户	9
域	6
列表	8
网关	0

统计信息: system@domain.com	
邮件	2
被允许的邮件	N/A
已使用的磁盘空间	0.00 MB
允许的磁盘空间	307200.01 MB

2.1.1 状态

点击菜单左边的“状态”按钮，可看到如下。“服务器状态”中显示 U-Mail Server 是否运行。“U-Mail 统计”中显示邮件系统中的用户、域、列表、网关数量。“统计信息：system@domain.com”显示 system 帐号的信息，如已使用的磁盘空间，允许使用的磁盘空间。



状态

我的账号

我的邮件列表

域

用户

邮件列表

网关

选项

主菜单

设置

安全

日志/配置文件

注销

刷新

服务器状态

程序	状态
U-Mail Server	Running

U-Mail 统计

用户	9
域	6
列表	8
网关	0

统计信息: system@domain.com

邮件	2
被允许的邮件	N/A
已使用的磁盘空间	0.00 MB
允许的磁盘空间	307200.01 MB

2.1.2 我的帐号

点击左边菜单中的“我的帐号”，此页面中显示的是 system 帐号的设置。可看到有帐号、转发、列表、引用、限制、管理员、Web、自动回复、IMAP 规则、MultPOP、选项等设置选项。

帐号

在“个人信息”下的全名，可以修改 system 帐号的显示名称。

在“帐号信息”下可以修改 system 邮箱的账户名和密码；默认新建的所有帐号“Enable POP access”和“Enable IMAP access”两个对勾都是打上的，可以用 outlook 客户端使用 POP3 或 IMAP 方式进行收发邮件。

在“邮件存储信息”下的邮件目录，可以修改 system 帐号的邮件保存路径。默认设置为 umail\users\domain.com\system 目录。修改完后，点击上面的“保存”按钮即可。



状态
我的账号
我的邮件列表
域
用户
邮件列表
网关
选项

主菜单
设置
安全
日志/配置文件
注销

自动回复 IMAP 规则 MultiPOP 选项
账号 转发 列表 引用 限制 管理员 Web

保存 取消

个人信息
全名: system
此账号创建于: <unknown>
此账号最近访问于: Fri Jul 06 11:33:00 2007

账号信息
邮箱: system @ domain.com
密码:
☐ 对此账号禁用所有访问
☒ Enable POP access
☒ Enable IMAP access

邮件存储信息
此帐号的所有到达的邮件将会被做为文本文件保存在此目录中。
邮件目录: d:\umail\Users\domain.com\system\
选择决定此帐号的 Email 存储格式的 MBF 文件。MBF 文件是允许你自定义格式的邮件会存储的脚本。
存储格式: RFC822 编辑 MBF
☐ 启用自动解压 MIME 编码的附件

此账号的注意/备注

转发

若要将收到的邮件转发到某个信箱，将“此帐号是当前转发邮件”对勾打上，在转发地址中填写要转发到哪个信箱，如有多个地址用逗号分割。

自动回复IMAP 规则MultiPOP选项

账号转发列表引用限制管理员Web

保存取消

邮件转发选项

☐ 此账号是当前转发邮件

转发地址(使用逗号分隔)。输入 Email 地址收到的邮件的副本会被发送。

☒ 保留转发邮件的本地副本

高级传送选项

转发此邮件到此主机:

在 SMTP 信封使用这个地址

使用此 SMTP 端口:

25

SMTP 默认是 25

列表

可设置将 `system@domain.com` 加入以下列表中，新建立的邮箱默认 `Everynoe@domain.com` 和 `MasterEveryone@domain.com` 两个对勾会打上。其中，`Everyone` 包含本域的所有信箱地址，`MasterEveryone` 为全局即所有域的所有信箱地址。



此页允许你管理你的邮件列表订阅。
只有允许订阅的邮件列表可以显示。

- ☐ aa@domain.com
- ☐ Everyone@aaa.com
- ☐ Everyone@bbbb.com
- ☒ Everyone@domain.com
- ☐ Everyone@fff.cn
- ☐ Everyone@test.com
- ☐ Everyone@wee33.net
- ☒ MasterEveryone@domain.com

引用

“队列选项”下可设置：帐号可以存储的邮件最大数量，允许最大磁盘空间。

“帐号和旧邮件清理”下可以设置：如果空间超过多少天自动删除帐号；如果邮件旧于多少天自动删除邮件；如果邮件旧于多少天删除已删除的 IMAP 邮件。默认设置都为无限制，一般不进行设置。

自动回复

IMAP 规则

MultiPOP

选项

账号

转发

列表

引用

限制

管理员

Web

保存

取消

队列选项

☒ 此帐号必须遵守这些限额设置

当一个帐号超过它的限额设置, 后来所递送的邮件都将被拒绝并把一个警告邮件发到此帐号的邮箱中。

一次可存储的邮件最大数量

允许的最大磁盘空间

KB

帐号和旧邮件清理

☒ 这个域名的使用默认设置。

自动删除帐号, 如果空闲超过

天(0 = 永不)

自动删除邮件, 如果旧于

天(0 = 永不)

删除已删除的 IMAP 邮件, 旧于

天(0 = 永不)

☐ 直接从 IMAP 文件夹中删除旧邮件

限制

此项可以限制用户对外部收发邮件。

“内接邮件限制”下对勾打上，则此帐号不能接收外部的邮件。还可以设置排除接收的外部地址。

“外送邮件限制”下对勾打上，则此帐号不能发送邮件给外部。还可以设置排除发送的外部地址。

自动回复IMAP 规则MultiPOP选项

账号转发列表引用限制管理员Web

保存取消

内接邮件限制

☐ 此账号不能从外部世界接收邮件

... 除非来自下列地址

添加

移除

从未认证源的邮件被:

Refused

外送邮件限制

☐ 此账号不能发送邮件给外部世界

... 除非到下列地址中的一个

添加

移除

从未认证源的邮件被:

Refused

管理员

system 帐号是全局管理员对勾是打上的。可以对邮件系统进行全局设置。普通用户此项是没有打勾的, 如果打勾也可登录系统管理后台。

The screenshot shows the 'Administrator Access' (管理员访问) configuration page in the U-Mail WebAdmin interface. At the top, there are tabs for '账号' (Account), '转发' (Forwarding), '列表' (List), '引用' (Quote), '限制' (Limit), '管理员' (Administrator), and 'Web'. The '管理员' tab is selected. Below the tabs, there are buttons for '保存' (Save) and '取消' (Cancel). The main content area is titled '管理员访问' (Administrator Access) and contains two sections:

- ☒ 此账号是全局管理员 (This account is a global administrator).
全局管理员至少有下列权限:
 - 通过 WebAdmin 完全访问服务器配置
 - 访问所有用户的日历
 - 象即时信息一样访问所有用户
 - 可以发送给列表, 即使标记为“只读”的能力
 - 可以发送给列表, 即使不是成员的能力
- ☐ 此账号是域管理员 (This account is a domain administrator).
域管理员至少有下列权利:
 - 通过 WebAdmin 访问域配置

Web

“Web 邮件访问”下的对勾表示是否可以通过 web 方式访问邮箱, 所有普通用户默认都可以访问。“web 远程设置权限”下 system 帐号可设置全部选项, 普通用户建议不用修改。

system@domain.com

自动回复

IMAP 规则

MultiPOP

选项

账号

转发

列表

引用

限制

管理员

Web

保存

取消

Web 邮件访问

☒ 账号可以通过 WorldClient 访问 Email

单击[这里](#)并且此帐号可以通过 Web 访问邮件。

Web 远程配置权限

☒ 账号可以用过 WebAdmin 访问它自己的设置

账号可以编辑下来设置:

☒ 编辑全名

☒ 编辑“所有人”列表设置

☒ 编辑密码

☒ 编辑邮件限制

☒ 编辑邮件目录位置

☒ 编辑队列设置

☒ 编辑转发地址

☒ 编辑 MultiPOP 设置

☒ 编辑高级转发

☒ 编辑自动回复设置

☒ 编辑加密邮件设置

☒ 编辑允许通过 Email 更改

☒ 编辑 IMAP 规则(仅 PRO 版本)

自动回复

选择 “对此帐号启用自动回复” 的对勾, 即可自动回复, 还可设置自动回复时间表。“自动回复文本” 下可以写入自动回复的内容。在最下面 “如果他是这些地址之一则不发送自动回复” 输入框内还可以填写排除地址, 排除的地址不使用自动回复。

system@domain.com

自动回复

IMAP 规则

MultiPOP

选项

账号

转发

列表

引用

限制

管理员

Web

保存 取消

Auto response event

☐ 对此账号启用自动回复

☒ 自动回复时间表

启动日期:

启动时间:

12:00 上午

结束日期:

结束时间:

12:00 上午

自动回复文本:

如果他是这些地址之一则不发送自动回复:

添加

新的排除地址 - 可用通配符

MultPOP

此项可以设置使用 pop 方式接收其他邮箱的邮件。新建 MultPOP 邮箱收集, 填写服务如 pop3.163.com, 登录

帐号如 aaa@163.com, 填写密码。可选择是否在 pop 服务器上保留邮件副本。



2.1.3 域


点击左边菜单中的“域”，可设置每个域的域名、IP 地址、是否启用反垃圾或反病毒、帐号和邮件清理，用户列表等。用鼠标双击要设置的域名，即可进入此域名的设置页面。

2.1.4 邮件列表

邮件列表在 admin 后台已经有介绍, 这里一般不用修改即可。所有新建、添加成员、删除邮件列表都在 admin 后台进行操作。这里可进行一些特殊的设置。

2.1.5 选项

点击左边菜单的“邮件列表”，可设置所有域的邮件列表。双击需要编辑的邮件列表，打开默认看到的是“选项”。“列表属性”下的第一个对勾默认是打上的，表示此列表是私人的，只允许列表里的用户可以发送。如果要是所有人都可以发送，则去掉对勾即可。第四个对勾默认也是打上的，表示发送给此列表的邮件，会在主题中显示列表名如 `aa@domain.com`。

 新建
  编辑
  删除
  过滤器

名称 /
 aa@domain.com
 Everyone@aaa.com
 Everyone@bbbb.com
 Everyone@domain.com
 Everyone@fff.cn
 Everyone@test.com
 Everyone@wee33.net
 MasterEveryone@domain.com

U-Mail WebAdmin -- 网页对话框

选项

成员

路由

订阅

通告

安全

摘要

文件夹

保存

取消

列表地址

名称: @

列表的"Reply-To:"地址:

保持"回复人"区域空白, 回复会直接给发送者

列表属性

☒ 此列表是私人的(非成员不能张贴)

☐ 此列表在全局地址簿中是隐藏的

☐ 此列表回复给(&R)"EXPN"和"LIST"请求

☒ 邮件在主题中有列表名(例如:主题:[列表名]文本)

☐ 邮件在主题中有线程号(例如...主题文本 [5])

递交此列表传送的优先等级 (0 - 99)

 使用此作为指引: 10 = 紧急, 50 = 普通, 80 = 大批

替换"收信人:"区域使用: ☐ N/A ☐ 列表的名字 ☒ 成员的全名

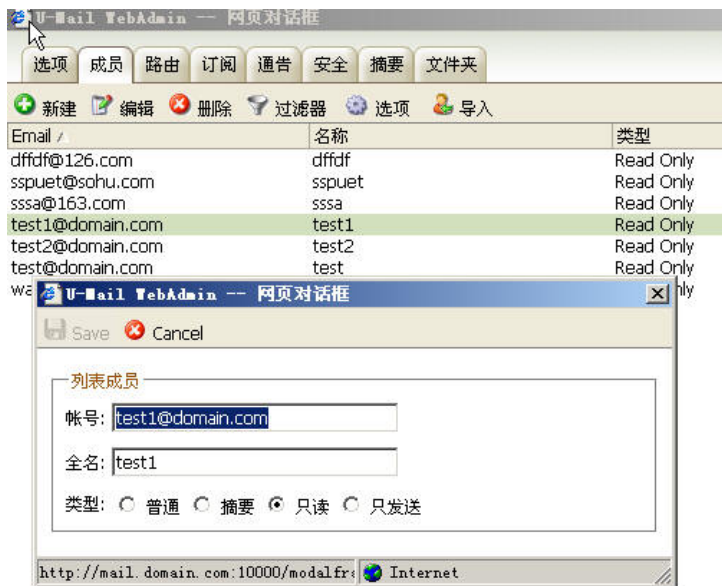
☒ 包括 "ListMember" 在"收件人:"区域

不发送邮件, 如果大小超过 KB(0=不管)

成员

点击上面的“成员”选项, 可看到该邮件列表里的所有成员。双击需要设置的成员如 test1@domian.com, 默认权限为只读, 要让此成员可以发送该列表, 则将“只读”修改为“普通”。这里虽然可以设置权限, 但建

议在 admin 域管理后台设置权限。



Everyone列表

邮件系统默认创建两个邮件列表，在 admin 后台是不显示的，分别为 Everyone 和 MasterEveryone。每添加一个域，系统都会为此域名创建 Everyone 列表。Everyone 邮件列表为本域所有信箱地址，MasterEveryone 邮件列表为系统所有域的所有信箱地址。本域下所有用户都可以发送 everyone 邮件列表。

(1) 编辑 everyone 列表

打开 everyone 列表的编辑页面。在“列表地址”下列表的“Reply-To:”地址, 在 admin 后台新建立的其他列表默认都是空的, 表示回复的地址是发件人。Everyone 列表默认是回复 everyone 地址, 如下图是自动回复 everyone@aaa.com, 如果要让回复的时候是发件人地址, 则去掉该行内容即可。

列表地址

名称: Everyone @ aaa.com

列表的“Reply-To:”地址: Everyone@aaa.com

保持“回复人”区域空白, 回复会直接给发送者

列表属性

☒ 此列表是私人的(非成员不能张贴)

☐ 此列表在全局地址簿中是隐藏的

☐ 此列表回复给(&R)“EXPN”和“LIST”请求

☒ 邮件在主题中有列表名(例如:主题:[列表名]文本)

☒ 邮件在主题中有线程号(例如...主题文本 [5])

递交此列表传送的优先等级 80 (0 - 99)

使用此作为指引: 10 = 紧急, 50 = 普通, 80 = 大批

替换“收信人:”区域使用: ☒ N/A ☐ 列表的名字 ☐ 成员的全名

☐ 包括“ListMember”在“收件人:”区域

不发送邮件, 如果大小超过 0 KB(0=不管)

(2) 删除 everyone 列表

如不想使用 everyone 列表, 点击左边菜单中“邮件列表”, 选择 everyone@aaa.com, 点击删除。注意, 这里删除后, 邮件系统重启的时候还是会自动创建。点击左边菜单中的“设置”——“其他选项”——“其他”。在下面去掉“创建“Everyone”列表”的对勾即可。MasterEveryone 列表为全局地址, 在下面也可以去掉。

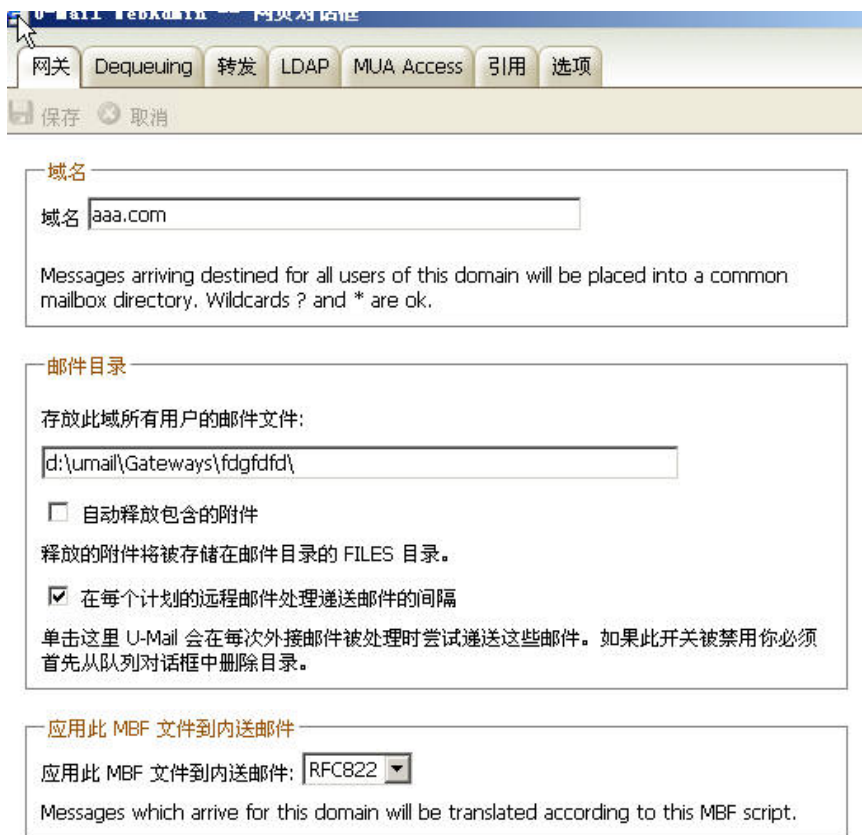


2.1.6 网关

点击左边菜单的“网关”，可以添加网关。如果企业有其他邮件服务器，垃圾邮件比较多，可以将那个域名的 mx 记录指定到本地服务器进行代收，先过滤垃圾病毒邮件，再转发到那台服务器上。如果那台服务器和本地服务器在一局域网内，使用同一个外网 IP 地址，则只需用本地服务器代收邮件，转发那台服务器内网 IP 地址。

例如企业有一台邮件服务器，域名为 aaa.com，ip 地址为 111.222.111.222。使用本服务器做为垃圾邮件过滤网关，则操作步骤为：

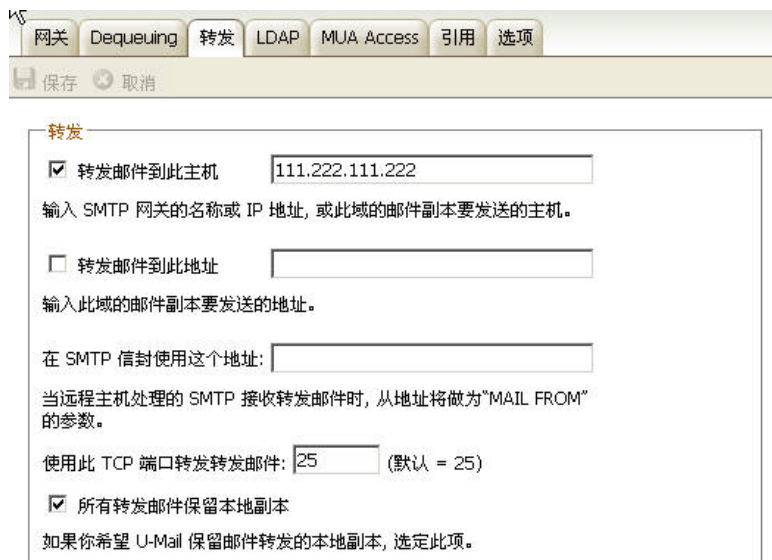
1. 首先将那台服务器的 mx 记录指定到本地服务器的地址。
2. 在下面的“网关”项中建立一个域名为 aaa.com 的网关，并选择下面的对勾“在每个计划的远程邮件处理递送邮件的间隔”。



The screenshot shows the U-Mail configuration window. At the top, there are tabs: 网关 (Gateway), Dequeueing, 转发 (Forwarding), LDAP, MUA Access, 引用 (Citation), and 选项 (Options). Below the tabs are buttons for 保存 (Save) and 取消 (Cancel). The main content area is divided into three sections:

- 域名 (Domain):** A text box contains 'aaa.com'. Below it, a message states: 'Messages arriving destined for all users of this domain will be placed into a common mailbox directory. Wildcards ? and * are ok.'
- 邮件目录 (Mail Directory):** A text box contains 'd:\umail\Gateways\fdgfd\'. Below it, there is a checkbox for '自动释放包含的附件' (Automatically release attached files). A note says: '释放的附件将被存储在邮件目录的 FILES 目录。' (Released attachments will be stored in the FILES directory of the mail directory). There is a checked checkbox for '在每个计划的远程邮件处理递送邮件的间隔' (At the interval of remote mail processing and delivery). A note below says: '单击这里 U-Mail 会在每次外接邮件被处理时尝试递送这些邮件。如果此开关被禁用你必须首先从队列对话框中删除目录。' (Click here, U-Mail will attempt to deliver these emails when external emails are processed. If this switch is disabled, you must first delete the directory from the queue dialog box).
- 应用此 MBF 文件到内送邮件 (Apply this MBF file to incoming mail):** A dropdown menu shows 'RFC822'. Below it, a message states: 'Messages which arrive for this domain will be translated according to this MBF script.'

3. 点击上面的“转发”项，在“转发邮件到此主机”输入框内输入 IP 地址为 111.222.111.222,默认选择对勾“所有转发邮件保留本地副本”，表示转发到那台服务器后，保留本地邮件副本不删除。如下：



The screenshot shows the 'Forwarding' (转发) tab in the U-Mail configuration window. The window has a title bar with a mouse cursor icon. Below the title bar is a tabbed interface with tabs: '网关' (Gateway), 'Dequeueing', '转发' (Forwarding), 'LDAP', 'MUA Access', '引用' (Citation), and '选项' (Options). The '转发' tab is selected. Below the tabs is a bar with '保存' (Save) and '取消' (Cancel) buttons. The main content area of the '转发' tab contains the following settings:

- ☒ 转发邮件到此主机: 111.222.111.222
输入 SMTP 网关的名称或 IP 地址, 或此域的邮件副本要发送的主机。
- ☐ 转发邮件到此地址:
输入此域的邮件副本要发送的地址。
- 在 SMTP 信封使用这个地址:
当远程主机处理的 SMTP 接收转发邮件时, 从地址将做为“MAIL FROM”的参数。
- 使用此 TCP 端口转发邮件: 25 (默认 = 25)
- ☒ 所有转发邮件保留本地副本
如果你希望 U-Mail 保留邮件转发的本地副本, 选定此项。

4. 点击上面的“选项”选项, 选择对勾“启用 AntiVirus 扫描此网关”、“启用 AntiSpam 扫描此网关”和“已验证的要求有效, 而不管连接的 IP”。



The screenshot shows the 'Options' (选项) tab in the U-Mail configuration window. The window has a title bar with a mouse cursor icon. Below the title bar is a tabbed interface with tabs: '网关' (Gateway), 'Dequeueing', '转发' (Forwarding), 'LDAP', 'MUA Access', '引用' (Citation), and '选项' (Options). The '选项' tab is selected. Below the tabs is a bar with '保存' (Save) and '取消' (Cancel) buttons. The main content area of the '选项' tab contains the following settings:

- ☒ 启用 AntiVirus 扫描此网关
- ☒ 启用 AntiSpam 扫描此网关
- ☐ 出列邮件需要验证
- ☒ 已验证的要求有效, 而不管连接的 IP
- ☐ 当作为此网关的用户发送邮件时需要认证

5. 点击菜单中“设置”下的“事件安排”，默认设置要过 15 分钟才转发邮件，需要设置一下。去掉上面第一个对勾“使用此间隔，递送/收集远程邮件 15 分钟”，选择“计划选项”下对勾“总是发送邮件如果有”输入 1，表示有一个或更多邮件在队列等待时，就处理邮件。

事件安排

发送 & 接收邮件 AntiSpam 更新

保存 取消

远程邮件处理间隔

☐ 使用此间隔, 递送/收集远程邮件 分钟 (1-60)

☒ 收取后即时递送远程邮件

☒ ... 包含为网关存储的邮件

简易计划

☐ 等待 分钟, 在上个邮件连接后, 下一个正在初始化启动前。

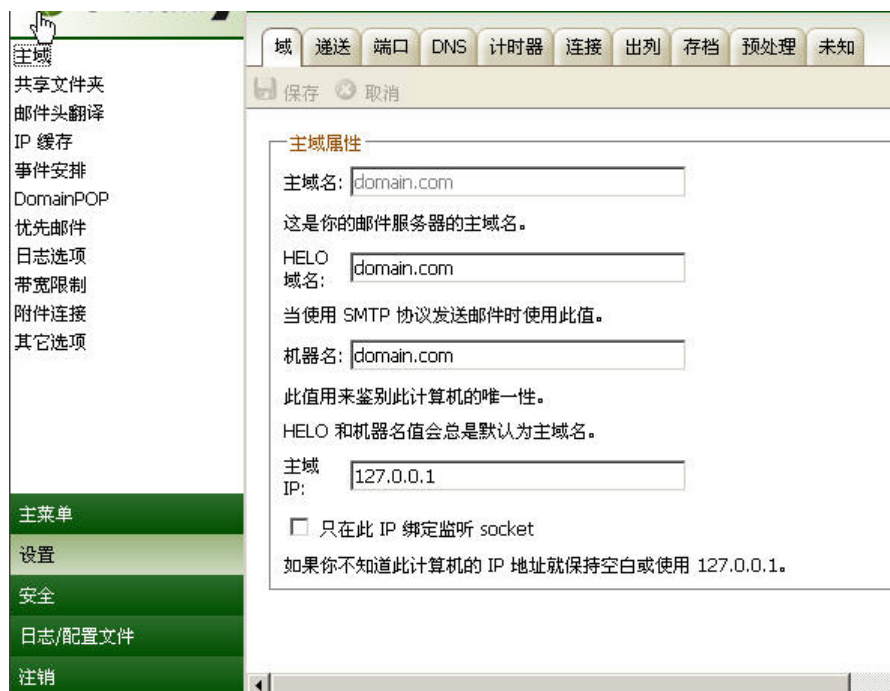
计划选项

☒ 总是发送邮件如果有 个或更多邮件在外接队列中等待。

☐ 如果等待邮件 分钟。

2.2 设置

点击左边菜单中的“设置”，包括主域、共享文件夹、邮件头翻译、IP 缓存、事件安排、DomainPOP、优先邮件、日志选项、带宽限制、附件连接、其他选项等设置。



2.2.1 主域

“主域”菜单下包括域、递送、端口、DNS、计时器、连接、存档、预处理、未知等设置选项。

域

点击菜单左边的“主域”，默认显示的是“域”选项。此项可以设置主域名的 IP 地址，默认为 127.0.0.1，可修改为服务器的 ip 地址。一般不用修改。

主域

域 递送 端口 DNS 计时器 连接 出列 存档 预处理 未知

保存 取消

主域属性

主域名:

这是你的邮件服务器的主域名。

HELO 域名:

当使用 SMTP 协议发送邮件时使用此值。

机器名:

此值用来鉴别此计算机的唯一性。

HELO 和机器名值会总是默认为主域名。

主域 IP:

☐ 只在此 IP 绑定监听 socket

如果你不知道此计算机的 IP 地址就保持空白或使用 127.0.0.1。

主域
共享文件夹
邮件头翻译
IP 缓存
事件安排
DomainPOP
优先邮件
日志选项
带宽限制
附件连接
其它选项
主菜单
设置
安全
日志/配置文件
注销

递送

点击上面的“递送”选项，邮件系统默认选择对勾“总是把所有外送的邮件直接发送给接收者的邮件服务器”，表示邮件直接发送给接收者的服务器，如果地址发送失败会退信。重试频率默认设置为：至少将邮件保留在主要队列 60 分钟，重试发送无法递送的邮件时间 240 分钟；选择对勾 1 和 3，第 1 个对勾当邮件放在重试队列时，通知发件人，第 3 个对勾当通知发件人时包含原始信息。

可设置“尝试直接发送但是有问题的邮件发送到下列指定的服务器”，在“邮件服务器”输入框填写递送到 IP 地址，则邮件发送失败后会递送到这个地址再进行发送尝试。

主域

域

递送

端口

DNS

计时器

连接

出列

存档

预处理

未知

保存

取消

邮件递送选项

☐

总是把外送的邮件发送到下列指定的服务器

☐

尝试直接发送但是有问题的邮件发送到下列指定的服务器

邮件服务器:

☐

访问上述邮件服务器要求登录。

☐

发送正在等待的邮件之前, 先进行 POP 检查

☒

总是把所有外送的邮件直接发送给接受者的邮件服务器

选择此选项, U-Mail 会作为一个自给自足的邮件服务器。Messages 将总是直接发送给容易接收的邮件服务器, 并且无法投递的邮件会稍后重新进入队列或退回。

重试频率:

至少将邮件保留在主要队列 分钟

重试发送无法递送的邮件时间 分钟

☒

当邮件放在重试队列时, 通知发信人

☐

当随后递送失败时, 通知原发信人

☒

当通知发件人时包含原始信息

端口

点击上面的“端口”选项，此项可设置 SMTP、SMTP SSL、POP、POP SSL、IMAP、IMAP SSL 等服务的端口。SMTP 服务端口为 25，修改后会收不到邮件。其他端口也不建议用户修改，SMTP SSL 服务端口为 465，POP 服务端口为 110，POP SSL 服务端口为 995，IMAP 服务端口为 143，IMAP SSL 服务端口为 993。

此外，还可以看到 DNS、LDAP 服务的端口，若修改后可能影响邮件正常工作。DNS 服务端口为 53，LDAP 端口为 389。

主域

域

递送

端口

DNS

计时器

连接

出列

存档

预处理

未知

保存 取消

SMTP/ODMR 服务端口

SSL/TLS available in U-Mail PRO only

在这些 TCP 端口监听接收 SMTP/MSA 事件

25

587

在此 TCP 端口创建创建外送 SMTP 事件

25

在此 TCP 端口监听内送 ODMR 事件

366

SMTP 的专用 SSL 端口

465

POP/IMAP 服务端口 - IMAP 服务在 PRO 版本中可用

在此 TCP 端口监听内送 POP 事件

110

在此 TCP 端口创建外送 POP 事件

110

POP 的专用 SSL 端口

995

在此 TCP 端口监听内送 IMAP 事件

143

IMAP 的专用 SSL 端口

993

DNS/LDAP/WebAdmin 服务端口

使用此 UDP 端口查询 DNS 服务

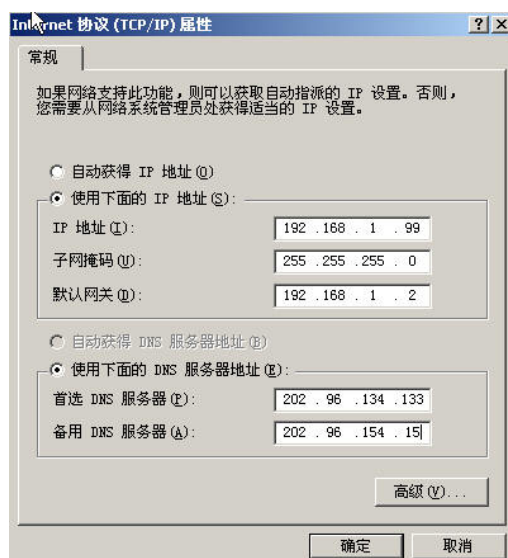
53

LDAP port for database & address book posting

389

DNS

点击上面的“DNS”选项，此项主要设置 DNS 相关的设置，建议也不用修改。在“DNS 服务器设置”下默认选择对勾“试图使用在 Windows 的 TCP/IP 当中的 DNS 服务器”，表示使用网卡 TCP/IP 属性中设置的 dns 服务器地址进行解析。如果不想使用网卡 TCP/IP 属性中的 dns 服务器地址进行解析，可在“主要 DNS 服务器 IP”和“后备 DNS 服务器 IP 地址”输入框中填写 dns 服务器的 ip 地址，一般使用当地电信或网通提供的 dns 服务器地址。在“重试失败的查询次数”中默认重试是 3 次，一般不用修改。



在“A 和 MX record 处理”下默认选择 2、3、4 对勾，为确保邮件系统正常，不建议用户修改。第 2 个对勾是“递送邮件时查询 DNS 服务器的 MX 记录”，第 3 个对勾是“使用在‘MX’记录包里找到的‘A’记录 IP 地址”，第 4 个对勾是“当 SMTP 发生错误时发送邮件到下一个 MX 主机”。

主域

域 递送 端口 DNS 计时器 连接 出列 存档 预处理 未知

保存 取消

DNS 服务器设置

☒ 试图使用在 Windows 的 TCP/IP 当中设置的 DNS 服务器

主要 DNS 服务器 IP: 202.96.134.133

后备 DNS 服务器 IP 地址: 202.96.154.15

重试失败的查询次数: 3

如果指定后备 DNS IP, 在每次重试时会一起尝试。

A 和 MX record 处理

☐ 当 DNS 反馈 A 记录域不存在时立即退回邮件

☒ 递送邮件时查询 DNS 服务器的 MX 记录

☒ 使用在 'MX' 记录包里找到的 'A' 记录 IP 地址

注意: 当从 'MX' 记录包获取时 'A' 记录的 IP 不会被缓存。

☒ 当 SMTP 发生错误时发送邮件到下一个 MX 主机

☐ 如果 MX 在 RCPT 命令后返回 5XX, 中止递送

☐ 当 DNS 反馈 MX record 域不存在时立即退回邮件

本地查询表

主机文件: C:\WINDOWS\system32\drivers\etc\hosts

计时器

点击上面的“计时器”选项，一般也不用修改。在“事件计时器”下可看到默认等待 30 秒 socket 连接、等待 60 秒协议对话框启动、等待 10 秒 MX DNS 服务器回应、等待 10 秒 A-Record DNS 服务器回应。SMTP 和 POP 连接超时于 10 分钟不活动，表示 10 分钟不活动，SMTP 和 POP 连接会超时。IMAP 连接超时于 30 分钟不活动，表示 30 分钟不活动，IMAP 连接会超时。

在“循环检测和控制”下，最大的邮件 hop 计数为默认为 20。表示邮件回复的跳数，即邮件发给对方服务器，对方使用回复发送，这里再回复发送，对方再回复发送，依次使用回复的次数。此项可防止双方都使用自动回复，造成无限制的回复发送。

在“延迟”下设置在 POP/IMAP/SMTP 命令间的毫秒延迟，默认设置为 5 毫秒。此项数值越小，会话延迟时间越短。

主域

域

递送

端口

DNS

计时器

连接

出列

存档

预处理

未知

保存

取消

事件计时器 - IMAP 选项只在 PRO 版中可用

等待

30

秒 socket 连接, 否则放弃

等待

60

秒协议对话框启动, 否则放弃

等待

10

秒 MX DNS 服务器回应

等待

10

秒 A-Record DNS 服务器回应

SMTP 和 POP 连接超时于

10

 不活动的分钟

IMAP 连接超时于

30

 不活动的分钟

☐
IMAP NOOP 和 IDLE 命令触发 1 分钟超时

循环检测和控制

最大的邮件 hop 计数(1-100)

20

这个设置规定了在邮件被移除并放到坏的邮件队列之前, 由 SMTP 邮件服务处理的最高的次数限制。

延迟

在 POP/IMAP/SMTP 命令间毫秒延迟 - 5 毫秒

无延迟

250

连接

点击上面的“连接”选项, 可设置 SMTP、POP、IMAP 等服务的连接数。在“SMTP”下可看到“最大同时连接 SMTP 外连接数”为 12, 表示服务器对外发送邮件的线程数为 12 个, 一般建议设置 10 到 20 之间。“每个线程的最大 SMTP 外送邮件假脱机数”为 0, 此项一般不建议修改。“最大同时发生的 SMTP 内接连接

数”为 30，表示服务器接收内部和外来邮件的最大线程数为 30；如果线程超过 30，客户端将会出现“服务器忙”的消息；一般建议设置 20 到 50 之间。

在“POP/IMAP”下可看到“最大同时发生的 POP 外接连接数”为 5，表示使用 pop 收集‘其他邮件服务器的邮件’最大连接数为 5，一般不建议修改。“最大同时发生的 POP 内接连接数”为 20，表示客户端使用 pop 方式和服务器连接的最大线程数为 20，一般建议设置 10 到 30 之间。“最大同时发生的 IMAP 线程数”为 20，表示客户端使用 imap 方式和服务器连接的最大线程数为 20，一般建议设置 10 到 30 之间。

主域

域 递送 端口 DNS 计时器 连接 出列 存档 预处理 未知

保存 取消

SMTP

最大同时连接 SMTP 外接连接数: 12

这是 U-Mail 连接到一个远程系统并递送邮件时, 它将能同时进行的线程数。

每个线程的最大 SMTP 外送邮件假脱机数: 0

在这个控件输入 0, 每个线程将会继续, 直到外接队列没有邮件剩余。

最大同时发生的 SMTP 内接连接数: 30

“服务器忙”的消息发送给客户端前的临界值。

POP/IMAP - IMAP 选项只适用于 PRO 版本

最大同时发生的 POP 外接连接数: 5

这是同一时间多 POP 连接线程的最大数。U-Mail 将会用来进行邮件收集。

最大同时发生的 POP/IMAP 内接连接数: 20

最大同时发生的 IMAP 线程数: 20

“服务器忙”的消息发送给客户端前的临界值。

存档

点击上面的“存档”，可以对邮件系统所有收发的邮件进行备份。如果要备份所有收发邮件，将上面的对勾“存档所有外送/内送邮件副本”打上，然后在下面的地址框输入指定的备份邮箱如 backup@domain.com，可以通过逗号分开每个地址来指定备份到多个邮箱地址。注意，需要先建立 backup@domain.com 邮箱，还可以在“用户”菜单下把这个邮箱目录指定其他路径。

对勾打上后，默认还会打上第 1 个和第 3 个对勾。第 1 个对勾为“在存档中也包含 U-Mail 邮件列表中的邮件”，表示还会备份发送邮件列表的邮件。第 3 个对勾为“在邮件主题中使用‘(存档副本)’标记备份邮件”，表示在备份的邮件主题中包含“(存档副本)”的文字。

未知

点击上面的“未知”选项，此项是如何处理未知用户的邮件。默认选择第 3 个对勾“把邮件防到坏邮件目录”，表示将未知的邮件放到坏邮件目录。一般未知邮件可能是恶意邮件等，不建议进行设置。



2.2.2 共享文件夹

公共文件夹可以让用户在 web 上面拥有共享的文件夹，共享文件夹目录保存在 umail\Public Folders。点击左边菜单的“公共文件夹”，这里可利用此项进行垃圾邮件学习。

共享文件夹

默认看到的是“共享文件夹”选项，在“公共文件夹”下将“启用公用文件夹”的对勾打上，则普通用户在 web 登录可看到“公共文件夹”项里的内容。

共享文件夹

共享文件夹

公共文件夹

保存 取消

IMAP 文件夹选项

IMAP 层次分隔字符:

这是分隔 IMAP 子文件夹的字符。默认是'/'。

公共文件夹

☐ 启用公用文件夹

如果你希望允许 IMAP 用户访问公用 IMAP 文件夹, 单击[这里](#)。公用 IMAP 文件夹只为系统所有, 并不绑定于特定帐号。

☐ 允许有“写入”访问的用户, 也设置“删除”标记。

当在个别用户的基础上存储邮件标记时, 你可能希望同意有“写入”权限的用户, 亦设置“删除”标记。

公用文件夹前缀字符串(如: '#' 或 'Pub-'):

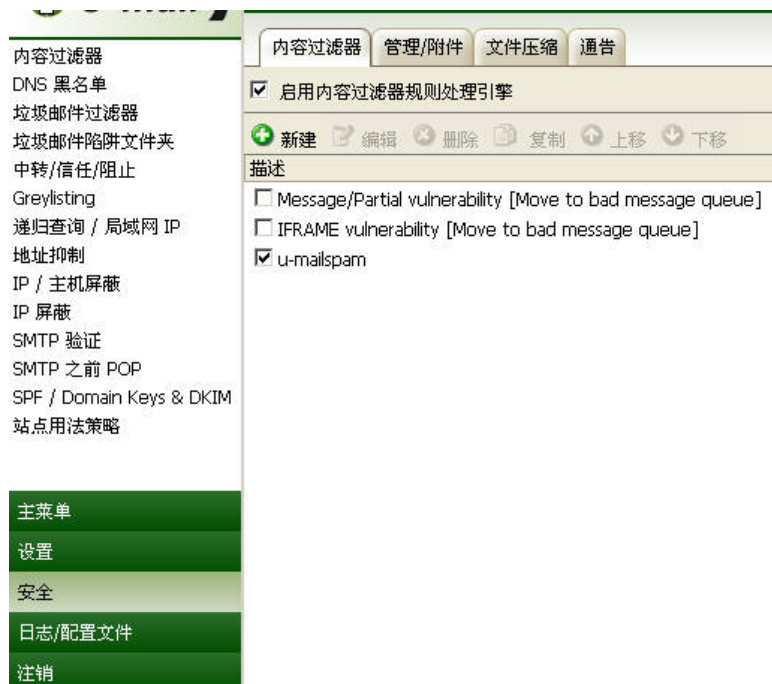
公共文件夹

点击上面的“公共文件夹”选项，此项里默认含有 Bayesian Learning 目录，此目录下包含 Non-Spam 和 Spam 两个目录。其中 Bayesian Learning/Non-Spam 文件夹表示不是垃圾邮件的意思，Bayesian Learning/Spam 文件夹表示是垃圾邮件的意思。



2.3 安全

点击左边菜单中的“安全”，包括内容过滤器、DNS 黑名单、垃圾邮件过滤器、垃圾邮件陷阱文件夹、中转信任阻止、Greylisting、递归查询、局域网 IP、地址抑制、IP 屏蔽、主机屏蔽、SMTP 验证、SMTP 之前 POP、SPF/Domain Keys & DKIM、站点用法策略等设置。



2.3.1 内容过滤器

点击左边菜单中的“安全”，默认显示的是“内容过滤器”菜单。里面有“内容过滤器”、“管理/附件”、“文件压缩”、“通告”等选项。可以进行各种规则设置和管理附件等操作。

内容过滤器

“内容过滤器”菜单打开默认显示的是“内容过滤器”选项。此项可以设置邮件标题内容过滤，邮箱备份监控等多种规则。默认最上面的对勾“启用内容过滤器规则处理引擎”是打上的，表示可以对内容过滤器进行任何操作；如果对勾去掉，则下面的所有规则都不生效，也不可以进行操作。下面每条规则前都有可选对勾，对勾去掉则该条规则不生效。选中其中一个规则，可以进行编辑、删除、复制、上移、下移等操作，在最上面的规则会优先处理。



(1) 规则内容介绍

点击“新建”，可以看到如下图。在上面“规则描述”输入框填写此条规则的名称，可根据自己情况任意填写。



The screenshot shows a dialog box for creating a new rule. At the top, there are two buttons: "保存" (Save) and "取消" (Cancel). Below this, the dialog is divided into several sections:

- 规则描述** (Rule Description): A section with a label "描述:" followed by a text input field.
- 选择一个以上的会触发规则活动的条件** (Choose one or more conditions that trigger rule activity): A section containing four checkboxes:
 - ☐ 如果 FROM 头包含 (If FROM header contains)
 - ☐ 如果 TO 头包含 (If TO header contains)
 - ☐ 如果主题头包含 (If subject header contains)
 - ☐ 如果 CC 头包含 (If CC header contains)
- 选择此规则要执行的一个或多个动作** (Choose one or more actions to perform for this rule): A section containing four checkboxes:
 - ☐ 删除此邮件 (Delete this email)
 - ☐ 从此邮件中移除所有附件 (Remove all attachments from this email)
 - ☐ 移动文件到坏邮件目录 (Move files to bad email directory)
 - ☐ 跳过后 'n' 个规则 (Skip the next 'n' rules)
- 规则描述** (Rule Description): A section with the text "应用此规则到邮件在 LOCAL & REMOTE 队列" (Apply this rule to emails in LOCAL & REMOTE queue).

在“选择一个以上的会触发规则活动的条件”下选择一个或多个条件，表示如果执行下面“选择此规则要执行的一个或多个动作”的执行规则，需要满足的条件。包括：

如果 FROM 头包含，

如果 TO 头包含，

如果主题头包含，

如果 CC 头包含，

如果 REPLY-TO 头包含，

如果用户自定义 1 头包含，

如果用户自定义 2 头包含,
如果用户自定义 3 头包含,
如果用户自定义 4 头包含,
如果用户自定义 5 头包含,
如果邮件正文包含,
如果用户头包含文本文件中的词,
如果用户头不包含文本文件中的词,
如果邮件正文包含文本文件中的词,
如果邮件正文不包含文本文件中的词,
如果邮件有附件,
如果邮件大小大于,
如果邮件有文件调用,
如果邮件有附件带有 **CONTENT-TYPE** 的,
如果邮件被感染,
如果从上一个“运行程序”规则的退出代码等于,
如果垃圾邮件过滤器分数等于,
如果邮件被数字签名,
如果邮件包含一个密码保护的 **ZIP** 文件, 如果所有邮件。

在“选择此规则要执行的一个或多个动作”下选择一个或多个动作, 表示如果满足“选择一个以上的会触发规则活动的条件”上面的条件则执行的动作。包括:

删除此邮件,
从此邮件中移除所有附件,
移动文件到坏邮件目录,
跳过以后 ‘n’ 个规则,
停止处理规则,
复制邮件给制动用户,
追加一个公司标志,

添加扩展头项目 1 到邮件，
添加扩展头项目 2 到邮件，
添加扩展头项目 3 到邮件，
删除一个邮件头项目 1 到邮件，
删除一个邮件项目 2 到邮件，
删除一个邮件头项目 3 到邮件，
发送一个通告 1 给，
发送一个通告 2 给，
发送一个通告 3 给，
移除任何数字签名，
运行一个程序，
发送邮件给我的 SMS 网关，
复制邮件到文件夹，
在文本文件中添加一行，
复制邮件到公共文件夹，
移动文件到公共文件夹，
在邮件头内搜索和替换文本，
在邮件正文内搜索和替换文本，
跳到一个规则，
发送一个快递邮件，
添加到 Windows 事件日志中，
释放附件到文件夹，
改变邮件处理优先级，
用 DomainKeys 选择器标记。

在最下面“规则描述”下，默认此规则运行在 **LOCAL** 和 **REMOTE** 队列。可以选择规则只运行于某个队列。**Local** 队列表示本地队列，是内部收发和外部发进来的邮件队列。**Remote** 队列表示远程队列，是发送到外部的邮件队列。

(2) 设置邮件过滤规则

1. U-Mail 系统默认创建一个名称为 u-mailspam 的过滤规则。在“选择一个以上的会触发规则活动的条件”下，选择“如果主题头包含”，表示如果邮件主题包含的字符串；选择“如果邮件正文包含”，表示如果邮件正文包含的字符串。在“选择此规则要执行的一个或多个动作”下，选择“删除此邮件”。

The screenshot shows the 'U-Mail WebAdmin' web interface. At the top, there's a title bar and a navigation bar with '保存' (Save) and '取消' (Cancel) buttons. The main content area is divided into several sections:

- 规则描述 (Rule Description):** A text box labeled '描述:' (Description:) containing the text 'u-mailspam'.
- 选择一个以上的会触发规则活动的条件 (Choose one or more conditions that trigger rule activity):** A list of checkboxes with a vertical scrollbar on the right:
 - ☐ 如果 FROM 头包含 (If FROM header contains)
 - ☐ 如果 TO 头包含 (If TO header contains)
 - ☒ 如果主题头包含 (If subject header contains)
 - ☐ 如果 CC 头包含 (If CC header contains)
- 选择此规则要执行的一个或多个动作 (Choose one or more actions to perform for this rule):** A list of checkboxes with a vertical scrollbar on the right:
 - ☒ 删除此邮件 (Delete this email)
 - ☐ 从此邮件中移除所有附件 (Remove all attachments from this email)
 - ☐ 移动文件到坏邮件目录 (Move files to bad email directory)
 - ☐ 跳过以后 'n' 个规则 (Skip the next 'n' rules)
- 规则描述 (Rule Description):** A section with a title '应用此规则到邮件在 本地 队列' (Apply this rule to emails in the local queue). Below it, a text area contains the following text: '如果此 SUBJECT 邮件头 包含 '邮件监管' 或 '3721' 或 '化妆' 或 '★' 或 '免费推广' 或 '家长如何' 或 '亿' 或 如果此 邮件正文 包含 '代开' 或 '代.开' 或 '建达实业' 或 '易邮' 或 'YMailserver' 或 '发票经营' 或 '发... 接着 删除邮件' (If this SUBJECT email header contains '邮件监管' or '3721' or '化妆' or '★' or '免费推广' or '家长如何' or '亿' or if this email body contains '代开' or '代.开' or '建达实业' or '易邮' or 'YMailserver' or '发票经营' or '发... then delete the email).

2. 在下面的“规则描述”里，点击“本地”。可以选择“本地队列”和“远程队列”对勾，默认是两个对勾都打的，这里只选择“本地队列”，表示只过滤接收的邮件。如下图



3. 点击位于“SUBJECT 邮件头”和“邮件正文”中间的“或”。默认是选择第一个“所有条件匹配 AND”，表示要同时满足“邮件主题头”和“邮件正文内容”的活动条件，才执行“删除邮此件”的动作。这里选择第二个“任何条件匹配 OR”，表示只需满足“邮件主题头”和“邮件正文内容”的其中一个活动条件，都执行“删除此邮件”的动作。



4. 点击“SUBJECT 邮件头”后面的“包含”，可在“检查此字符串”下的输入框内添加需要过滤的邮件主题关键词，点击“添加”即可。默认“如果此 SUBJECT 邮件头”的包含条件选择“下列字符串的全部”，表示需要满足下列字符串的值，才执行“删除此邮件”的动作。这里选择“任何或”，表示只要满足下列任何一个字符串的值，都执行“删除此邮件”的动作。



5. 点击“邮件正文”后面的包含字符串，和以上设置类似。

(3) 设置监控一个或多个邮箱

如果要监控一个或多个邮箱收发的邮件，也可以说是备份一个或多个邮箱收发的邮件。就是将一个或多个邮箱收发的邮件，同时复制到指定的邮箱中。例如将 aaa@domain.com 和 bbb@domain.com 邮箱收发的邮件，复制到 bak@domain.com 邮箱。

1. 可新建一条规则，在上面“规则描述”输入框中输入名称。
2. 在“选择一个以上的会触发规则活动的条件”下，选择对勾“如果 FROM 头”，表示发件人的地址包含，利用此项监控发送出去的邮件；选择对勾“如果 TO 头”，表示收件人的地址包含，利用此项监控接收到的邮件。
3. 在“选择此规则要执行的一个或多个动作”下，选择对勾“复制邮件给制动用户”，表示复制邮件到某一个邮箱用户。

The screenshot shows the U-Mail WebAdmin interface with a rule configuration form. The form has a title bar with 'U-Mail WebAdmin' and '网际对信'. Below the title bar are '保存' (Save) and '取消' (Cancel) buttons. The form is divided into several sections:

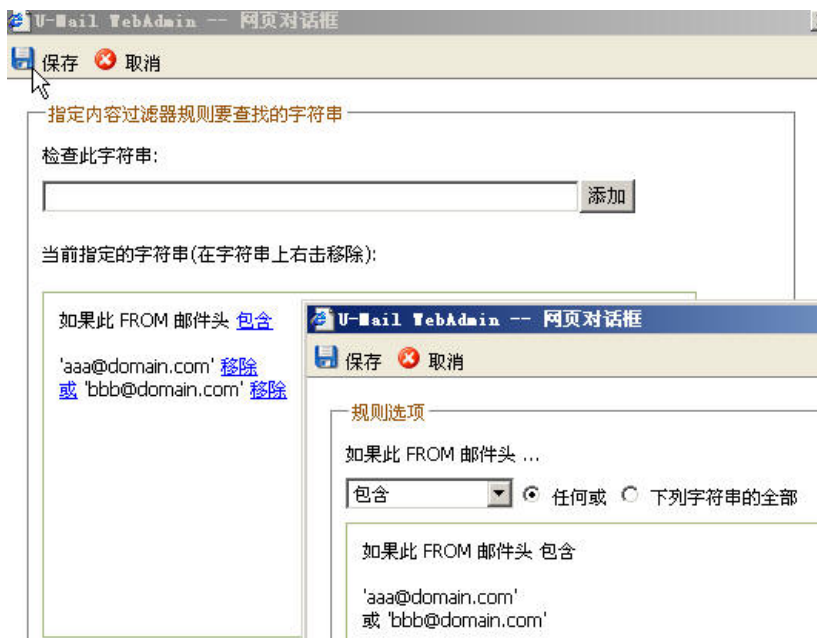
- 规则描述** (Rule Description): A text input field with the value 'test'.
- 选择一个以上的会触发规则活动的条件** (Choose one or more conditions that trigger rule activity): A list of checkboxes with the following options:
 - ☒ 如果 FROM 头包含 (If FROM header contains)
 - ☒ 如果 TO 头包含 (If TO header contains)
 - ☐ 如果主题头包含 (If subject header contains)
 - ☐ 如果 CC 头包含 (If CC header contains)
- 选择此规则要执行的一个或多个动作** (Choose one or more actions to execute for this rule): A list of checkboxes with the following options:
 - ☐ 跳过后 'n' 个规则 (Skip the next 'n' rules)
 - ☐ 停止处理规则 (Stop processing rules)
 - ☒ 复制邮件给制动用户 (Copy mail to the user who triggered the rule)
 - ☐ 追加一个公司标志 (Append a company logo)
- 规则描述** (Rule Description): A section for the rule's description, containing the text: '应用此规则到邮件在 [LOCAL & REMOTE](#) 队列' (Apply this rule to mail in the LOCAL & REMOTE queue). Below this, it says: '如果此 FROM 邮件头 包含 ['aaa@domain.com'](#) 或 ['bbb@domain.com'](#) 或 如果此 TO 邮件头 包含 ['aaa@domain.com'](#) 或 ['bbb@domain.com'](#) ... 接着 复制此邮件到 ["bak@domain.com"](#)' (If this FROM mail header contains 'aaa@domain.com' or 'bbb@domain.com' or if this TO mail header contains 'aaa@domain.com' or 'bbb@domain.com' ... then copy this mail to 'bak@domain.com').

4. 在下面的“规则描述”下，“FROM 邮件头”和“TO 邮件头”中间的条件匹配为“或”，选择第二个对勾

“任何条件匹配 OR”，表示只要发件人地址满足“FROM 邮件头”或收件人地址满足“TO 邮件头”中的字符串，都进行执行“复制邮件给制动用户”的动作。



5. 点击“FROM 邮件头”的“包含”，在出现页面中的规则选项选择“任何或”，在检查表示只要满足下列任何一个字符串的值，都执行“复制邮件给制动用户”的动作。在“检查此字符串”下分别输入 aaa@domain.com 和 bbb@domain.com，点击添加。见下图



6. 点击“TO 邮件头”的“包含”，类似上面设置。

7. 点击“接着就复制邮件到”后面的指定信息，在出现的页面中输入指定的邮箱，可指定多个邮箱地址。如下图



8. 其他设置

- 1) 如果只监控邮箱发送的邮件，在“选择一个以上的会触发规则活动的条件”下，只选择对勾“**如果 FROM 头**”。
- 2) 如果只监控邮箱接收的邮件，在“选择一个以上的会触发规则活动的条件”下，只选择对勾“**如果 TO 头**”。
- 3) 如果要监控某个域名如 `aaa.com` 下的邮件，点击“FROM 邮件头”或“TO 邮件头”的“包含”，在“检查此字符串”下输入 `*@aaa.com`。

2.3.2 管理/附件

点击上面的“管理/附件”选项，此项一般不进行设置。在“受限制的附件”下第二项“限制这样的文件”下，默认限制后缀名为 `vbs`、`exe`、`com` 等影响服务器安全的文件；在“排除”下第二项，可以添加某个域名排除“限制这样的文件”设置，如 `*@domain.com`。在“受限制附件”下第一项“仅允许这些附件”，默认为空。如果要设置只允许某几个附件格式，则输入如 `*.txt` 等允许的格式后点击“添加”即可。在“排除”下第一项，可以添加某个域名排除“受限制附件”设置，如 `*@domain.com`。

内容过滤器

内容过滤器

管理/附件

文件压缩

通告

保存

取消

删除

受限的附件

仅允许这些文件，如: *.txt

限制这样的文件, 如: ILOVE*.vbs

添加

删除

MINE.*

THE_FLY.*

*.PIF

*.SCR

*.VBS

*.EXE

*.CMD

*.COM

添加

删除

排除

Exclude messages BOUND for these addresses Ex: *@company.mail

Exclude messages FROM these addresses Ex: *@company.mail

添加

删除

添加

删除

2.4 日志/设置文件

点击左边菜单中的“日志/设置文件”，包括 U-Mail 日志文件、WebAdmin 日志文件、Webadmin 日志选项等。

查看			
	日志文件 /	大小	修改日期
U-Mail 日志文件	Friday-all.log	816 Bytes	2007-7-6 17:13
WebAdmin 日志文件	Friday-AntiSpam.log	831 Bytes	2007-7-6 17:13
WebAdmin 日志选项	Friday-AntiVirus.log	6.5 KB	2007-7-12 9:41
	Friday-Content-Filter.log	849 Bytes	2007-7-6 17:13
	Friday-DomainKeys.log	837 Bytes	2007-7-6 17:13
	Friday-DomainPOP.log	834 Bytes	2007-7-6 17:13
	Friday-IMAP.log	819 Bytes	2007-7-6 17:13
	Friday-MultiPOP.log	831 Bytes	2007-7-6 17:13
	Friday-Outlook-Connector.log	858 Bytes	2007-7-6 17:13
	Friday-Plug-ins.log	831 Bytes	2007-7-6 17:13
	Friday-POP.log	10.0 KB	2007-7-10 17:09
	Friday-RAW.log	816 Bytes	2007-7-6 17:13
	Friday-Routing.log	828 Bytes	2007-7-6 17:13
	Friday-SMTP-(in).log	19.5 KB	2007-7-11 19:13
	Friday-SMTP-(out).log	837 Bytes	2007-7-6 17:13
	Friday-Spam-Blocker.log	843 Bytes	2007-7-6 17:13
	Friday-SPF.log	816 Bytes	2007-7-6 17:13
	Friday-Statistics.log	0 Bytes	2007-7-6 11:17
	Friday-System.log	12.5 KB	2007-7-12 9:36
主菜单	Thursday-all.log	272 Bytes	2007-7-12 11:09
设置	Thursday-AntiSpam.log	277 Bytes	2007-7-12 11:09
安全	Thursday-AntiVirus.log	808 Bytes	2007-7-16 16:58
	Thursday-Content-Filter.log	283 Bytes	2007-7-12 11:09
	Thursday-DomainKeys.log	279 Bytes	2007-7-12 11:09
日志/配置文件	Thursday-DomainPOP.log	278 Bytes	2007-7-12 11:09
	Thursday-IMAP.log	273 Bytes	2007-7-12 11:09
注销	Thursday-MultiPOP.log	277 Bytes	2007-7-12 11:09

日志/设置文件

点击左边菜单的“日志/设置文件”，可看到“U-Mail 日志文件”、“WebAdmin 日志文件”和“WebAdmin 日志选项”。在“U-Mail 日志文件”下可以看到 U-Mail 系统收发邮件的日志；在“WebAdmin 日志文件”下可以看到邮件系统工作日志和 WebAdmin 后台登录日志；在“WebAdmin 日志选项”下是一些设置“WebAdmin 日志文件”的选项。

U-Mail 日志文件

点击左边的“U-Mail 日志文件”，可以看到当天的收发日志。其中 **SMTP-(out).log** 文件记录发送外网邮件的日志，**SMTP-(in).log** 文件记录内部发送和接收外网邮件的日志，**POP.log** 文件记录客户端使用 **pop** 方式收发邮件到服务器的日志，**IMAP.log** 文件记录客户端使用 **IMAP** 方式收发邮件到服务器的日志，**AntiVirus.log** 文件记录病毒过滤器的日志，**Spam-Blocker.log** 文件记录垃圾邮件过滤器的日志。

如果要查看更多日志，进服务器 **umail/logs** 目录进行查看。如有有发送出去对方反映没有收到，可以打开 **smtp-(out).log** 日志文件，查看此封邮件的发送日志；“**SMTP session successful**”表示发送成功，“**SMTP session terminated**”表示发送失败。如有对方发过来没有收到，可以打开 **smtp-(in).log** 日志文件，查看此封邮件的接收日志；“**SMTP session successful**”表示发送成功，



U-Mail 日志文件

WebAdmin 日志文件

WebAdmin 日志选项

主菜单

设置

安全

日志/配置文件

注销

日志文件

查看

日志文件 /	大小	修改日期
Friday-all.log	816 Bytes	2007-7-6 17:13
Friday-AntiSpam.log	831 Bytes	2007-7-6 17:13
Friday-AntiVirus.log	6.5 KB	2007-7-12 9:41
Friday-Content-Filter.log	849 Bytes	2007-7-6 17:13
Friday-DomainKeys.log	837 Bytes	2007-7-6 17:13
Friday-DomainPOP.log	834 Bytes	2007-7-6 17:13
Friday-IMAP.log	819 Bytes	2007-7-6 17:13
Friday-MultiPOP.log	831 Bytes	2007-7-6 17:13
Friday-Outlook-Connector.log	858 Bytes	2007-7-6 17:13
Friday-Plug-ins.log	831 Bytes	2007-7-6 17:13
Friday-POP.log	10.0 KB	2007-7-10 17:09
Friday-RAW.log	816 Bytes	2007-7-6 17:13
Friday-Routing.log	828 Bytes	2007-7-6 17:13
Friday-SMTP-(in).log	19.5 KB	2007-7-11 19:13
Friday-SMTP-(out).log	837 Bytes	2007-7-6 17:13
Friday-Spam-Blocker.log	843 Bytes	2007-7-6 17:13
Friday-SPF.log	816 Bytes	2007-7-6 17:13
Friday-Statistics.log	0 Bytes	2007-7-6 11:17
Friday-System.log	12.5 KB	2007-7-12 9:36
Monday-all.log	272 Bytes	2007-7-23 15:09
Monday-AntiSpam.log	277 Bytes	2007-7-23 15:09
Monday-AntiVirus.log	1.4 KB	2007-7-24 8:52
Monday-Content-Filter.log	283 Bytes	2007-7-23 15:09

WebAdmin 日志文件

点击左边菜单的“WebAdmin 日志文件”，这里一般不进行查看。其中 HTTP.log 和 WDaemon.log 文件记录邮件系统一些工作日志，Webadmin.log 文件记录 system 帐号后台的登录日志。

日志文件		
查看		
日志文件 /	大小	修改日期
HTTP.LOG	1.7 MB	2007-7-30 17:56
WDaemon.log	49.0 KB	2007-7-30 17:55
WebAdmin.log	20.5 KB	2007-7-30 17:55

WebAdmin 日志选项

点击左边菜单的“WebAdmin 日志选项”，此项可以设置一些“WebAdmin 日志文件”的选项。在“日志等级”下默认选择“通知”选项，在“日志模式”下默认选择“不循环日志文件”选项。在“日志维护”下，最大日志文件大小为 0，表示不限制。

WebAdmin 日志选项

保存

取消

日志等级

☐ 除错

☒ 通知

☐ 警告

☐ 错误

日志模式

☒ 不循环日志文件

☐ 每天创建一个新的日志文件

☐ 每星期创建一个新的日志文件

☐ 每月创建一个新的日志文件

日志维护

最大日志文件大小: KB(0=无大小限制)

当日志文件达到此大小, 它会改名为 .OLD 并启动一个新的日志文件。

2.5 注销

点击左边菜单中的“注销”，即可返回登录页面。

2.2.6 邮件头翻译

点击左边菜单的“邮件头翻译”此项可以让一个邮箱发出去的地址，在对方显示另外一个邮箱地址。例如有一邮箱 `abc@domain.com`，如果想让对方收到邮件后显示 `123@domain.com`。如果使用了邮件头转换，那么在发信的时候会把邮箱地址 `aaa@domain.com` 替换为 `123@domain.com`，收件人回复该邮件的时候，其实是回复到 `123@domain.com` 邮箱。

在“现有的邮件头文本”输入框中填写 `abc@domain.com`，“新的邮件头文本”输入框中填写 `123@domain.com`。点击“添加”即可。如果不想使用该邮件头，点击“删除”即可。

邮件头翻译

保存

取消

输入新建邮件头翻译

如果邮件是来自于本地的域, 并要递送到非本地的域, 这些外送邮件头部分所包含的特定文本。你可以指定以其它文本来替换它。这对于当你需要转换每封外送邮件头中的本地域名, 成为实际域名时相当有用。它将搜索匹配当前邮件头的文本, 并以新的邮件头来替换。

☒ 转发的邮件翻译邮件头

☒ 在网关邮件转发到主机或 IP 时翻译邮件头

现有的邮件头文本: abc@domain.com

新的邮件头文本: 123@domain.com

添加

移除

例外

2.2.7 IP缓存

利用 IP 缓存可以在发送邮件时不通过 dns 进行解析, 一般不建议设置。在“缓存选项”下选择对勾“自动缓存尚未缓存的域”, 则所有发出去的地址都进行缓存。默认存活时间是 60 分钟, 最大缓存的条目是 50 个, 在下面输入框可进行设置。注意如果选择该对勾后, 如果对方 ip 地址变动, 则可能造成发送不正常。

在“IP 缓存条目”下还可以手动添加 IP 缓存, 在“域”输入框中填写对方 mx 记录, 在“IP”输入框中填写对方服务器 IP 地址。可以设置默认存活的时间, 点击“添加”即可。如果不对该域进行缓存, 点击“移除”即可。点击“无缓存”还可以指定排除不进行缓存的域或 IP 地址。

- 75 -

IP 缓存

保存

取消

缓存选项

☐ 自动缓存尚未缓存的域

☐ 在每次处理间隔, 清除 IP 缓存

默认存活时间(分): (使用 9999 并登录将永不过期)

最大缓存的条目:

IP 缓存条目

域:

IP:

添加

移除

清除

无缓存

2.2.8 事件安排

点击左边菜单的“事件安排”，默认看到的是“发送&接收邮件”选项，此项一般不用做设置。默认选择第 1 个对勾和第 2 个对勾。第 1 个对勾为“使用此间隔，递送/收集远程邮件 15 分钟”，第 2 个对勾为“收取后即时递送远程邮件”。注意，如果使用此服务器做为垃圾邮件网关，可以看上面 3.3.6（网关）对此项进行的设置。

事件安排

发送 & 接收邮件

AntiSpam 更新

保存

取消

远程邮件处理间隔

- ☒ 使用此间隔, 递送/收集远程邮件 分钟 (1-60)
- ☒ 收取后立即递送远程邮件
- ☐ ... 包含为网关存储的邮件

点击上面的“AntiSpam 更新”选项, 可看到默认选择对勾“激活垃圾邮件过滤器更新”, 表示自动更新垃圾邮件过滤器。在“计划 AntiSpam 更新”下, 还可以设置哪一天几点几分进行更新。

事件安排

发送 & 接收邮件

AntiSpam 更新

保存

取消

激活垃圾邮件过滤器更新

- ☒ 激活垃圾邮件过滤器更新

U-Mail 能定期检查垃圾邮件过滤器的启发式引擎更新。此更新会保持你的垃圾邮件检测文件更节省时间。

此进程允许每天一次的更新。

计划 AntiSpam 更新

哪一天?

- ☐ 星期天 ☐ 星期四
- ☐ 星期一 ☐ 星期五
- ☐ 星期二 ☐ 星期六
- ☐ 星期三

几点?

几分?

Monday at 01:00

添加

移除

清除

2.2.9 日志选项

默认看到的“维护”选项，最大日志文件大小为 0KB，表示不限制。默认选择对勾“每天只运行不超过一次的自动备份”，表示每天自动备份一次。自动 ZIP 压缩存档日志文件，默认是旧于 1 天。一般不用进行设置。

日志选项

维护

选项

保存

取消

日志维护

最大日志文件大小: KB(0=无大小限制)

当日志文件达到此大小, 它会改名为 .OLD 并启动一个新的日志文件。

☒ 每天只运行不超过一次的自动备份

限制 *.OLD 文件日志回卷, 每天仅一次(活动日志可能比最大大小还大)。

☐ 当日志文件名在午夜改变时覆盖已存在的日志文件

选择此选项允许 U-Mail 在需要时覆盖已存在的日志文件。否则 U-Mail 会追加到已存在的日志文件后。

自动 ZIP 压缩存档日志文件, 当它旧于: 天(0 = 永不)

在午夜 U-Mail 会压缩并移动所有超过指定天数的 \Logs\OldLogs\ 目录中的日志文件。

当日志模式页的“创建一套标准日志文件”选项启用时, 存档不执行。

上面的在“选项”下，可看到记录日志的选项，默认选择对勾“记录 SMTP 活动”、“记录 POP 活动”、“记

录 IMAP 活动”、“记录 AntiVirus 活动”和“记录垃圾邮件过滤器活动”。表示记录 smtp, pop, imap, AntiVirus(病毒过滤)和垃圾邮件过滤器。

日志将会以文本方式记录在 umail/logs 目录下, 其中 SMTP-(out).log 文件记录发送外网邮件的日志, SMTP-(in).log 文件记录内部发送和接收外网邮件的日志, POP.log 文件记录客户端使用 pop 方式收发邮件到服务器的日志, IMAP.log 文件记录客户端使用 IMAP 方式收发邮件到服务器的日志, AntiVirus.log 文件记录病毒过滤器的日志, Spam-Blocker.log 文件记录垃圾邮件过滤器的日志。



2.2.10 带宽限制

在“带宽限制”项下, 默认是不限制速度的, 一般不进行设置。可以设置最大传输速度, 为每个域进行设置带宽限制, 还可以为每个服务进行带宽限制。

带宽限制

带宽限制

局域网域

局域网 IP

保存

取消

带宽限制

☐ 把限制应用到每个基本服务(默认是每个连接)

最大传输速度(KB/s): 未知

配置域的设置: domain.com

POP 带宽限制 - 无限

IMAP 带宽限制 - 无限

接入 SMTP 带宽限制 - 无限

接出 SMTP 带宽限制 - 无限

DomainPOP 带宽限制 - 无限

MultiPOP 带宽限制 - 无限

2.2.11 其他选项

服务

默认打开的是“服务”选项，一般不用进行设置。默认选择对勾“SMTP 系统在 ESMTP 可用时直接使用”和“允许连接到自己的 IP 地址”。POP/IMAP 服务始终接受来自此 IP 的连接，默认 ip 为 127.0.0.1。未处理的服务在每个间隔，转换的邮件数为 0，即全部。允许每封信可用 RCPT 命令数为 100，表示发送邮件时一次性可填写的邮件地址最多为 100 个。核心 socket 发送缓冲区大小默认为 0。

在最下面还可以设置“SMTP 最大可接收的邮件大小”输入框默认为 30720KB，即 30M；如果设置为 0 表示无限制接收。“如果数据发送超过多少断开连接”输入框默认为 30720KB，即 30M；如果设置为 0 表示不限制发送邮件的大小，发送大附件邮件是否可以到达还要看对方服务器设置的可接收大小。

其它选项

服务

邮件头

修正

系统

磁盘

MultiPOP

WAB

其它

保存

取消

服务相关选项

☒ SMTP 系统在 ESMTP 可用时直接使用

☐ 允许 ESMTP VRFY 命令

☐ 允许 ESMTP EXPN 命令

☐ 在重新开机时仍记忆 SMTP/POP/IMAP 服务状态

☐ 服务允许 APOP/CRAM-MD5 验证方法

☐ POP DELE 命令立即从邮箱移除邮件

☐ 隐藏 ESMTP SIZE 命令参数

☐ SMTP 超过限时, 送出错误 552 的回复(常规为 452)

☒ 允许连接到自己的 IP 地址

POP/IMAP 服务始终接受来自此 IP 的连接:

未处理的服务在每个间隔, 转换的邮件数(0=全部):

允许每封信可用 RCPT 命令数(RFC 标准为 100):

核心 socket 发送缓冲区大小(字节, 0=系统默认):

服务相关选项

SMTP 最大可接收的邮件大小 KB(0=无限制)

如果数据发送超过多少断开连接 KB(0=永不)

邮件头

点击上面的“邮件头”选项，一般不用进行设置。默认选择后面几个对勾“从列表邮件去除”Received:”

邮件头”、“从输入的邮件剥离”X-RBL-Warning:”头”、“从本地邮件去除”X-”开始的邮件头”、“处理邮件头时隐藏本地 IP”、“创建安全”接收”头”等 5 个选项。

其它选项

服务邮件头修正系统磁盘MultiPOPWAB其它

保存取消

邮件头处理

☐ 强制 "Date:" 邮件头添加所有邮件

☐ 强制 "Reply-To:" 邮件头添加所有邮件

☐ 强制 "Message-ID:" 邮件头添加所有邮件

☐ 允许 "Return-Receipt-To" 邮件头

☐ 添加 "Precedence: bulk" 邮件头到系统产生的邮件

☐ 添加 "X-Authenticated-Sender:" 邮件头到验证的邮件

☐ 添加 "Content-ID:" 邮件头到有附件的未处理的邮件

☐ 添加 "For" 节段到 "Received:" 邮件头

☒ 从列表邮件去除 "Received:" 邮件头

☒ 从输入的邮件剥离"X-RBL-Warning:"头

☒ 从本地邮件去除 "X- " 开始的邮件头

☒ 处理邮件头时隐藏本地 IP

☒ 创建安全"接收"头

☐ 使用 "From:" 邮件头验证列表投递人

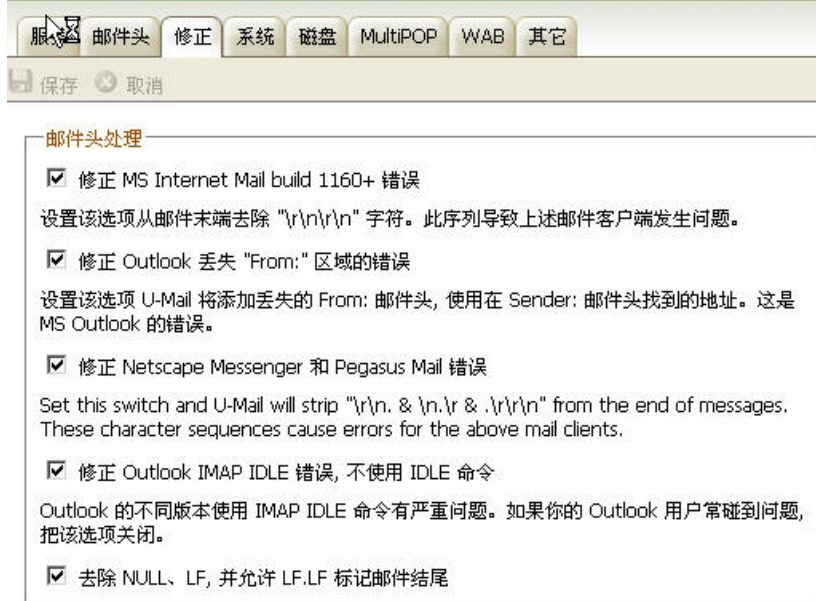
添加此邮件头和值到每一封列表邮件:

欢迎邮件主题:

修正

点击上面的“修正”选项，一般不用进行设置。默认选择所有对勾，表示修正所有错误。

其它选项



服务 邮件头 修正 系统 磁盘 MultiPOP WAB 其它

保存 取消

邮件头处理

- ☒ 修正 MS Internet Mail build 1160+ 错误
设置该选项从邮件末端去除 "\r\n\r\n" 字符。此序列导致上述邮件客户端发生问题。
- ☒ 修正 Outlook 丢失 "From:" 区域的错误
设置该选项 U-Mail 将添加丢失的 From: 邮件头, 使用在 Sender: 邮件头找到的地址。这是 MS Outlook 的错误。
- ☒ 修正 Netscape Messenger 和 Pegasus Mail 错误
Set this switch and U-Mail will strip "\r\n. & \n.\r & .\r\n\r\n" from the end of messages. These character sequences cause errors for the above mail clients.
- ☒ 修正 Outlook IMAP IDLE 错误, 不使用 IDLE 命令
Outlook 的不同版本使用 IMAP IDLE 命令有严重问题。如果你的 Outlook 用户常碰到问题, 把该选项关闭。
- ☒ 去除 NULL、LF, 并允许 LF.LF 标记邮件结尾

系统

点击上面的“系统”选项，一般不用进行设置。默认选择所有对勾，“U-Mail 系统帐号别名”输入框内容为空，“默认附件的扩展名”输入框内容为 .eml，“默认的登录分隔符”输入框内容为 \$，“默认垃圾邮件文件夹名”输入框内容为 **Junk E-mail**，“用在自动产生邮件的 Char-set 值”输入框内容为 **iso-8859-1**，“第二部主机 IP”输入框内容为空。“混乱邮件目录”对勾打上，当邮件用户目录多时，可提升性能。

其它选项

服务邮件头修正系统磁盘MultiPOPWAB其它

保存取消

邮件头处理

☒ 预处理邮件列表邮件
列表邮件的邮件本体第一行包含 'Subscribe' 或 'Unsubscribe' 等等，将拒绝处理。

☒ 当域名更改时，移动帐号邮件到新目录
U-Mail 系统账号别名:
系统产生的邮件，将使用此地址发送。

默认附件的扩展名:
系统使用的附件，将根据这个扩展名来创建。

默认的登录分隔符(字符串最长 10 字符):
除了 '@' 字符，它也用于邮件地址中，作为登录用途。

默认垃圾邮件文件夹名:

用在自动产生邮件的 Char-set 值:

第二部主机 IP，用于双重 socket 绑定:

☒ 混乱邮件目录
单击[这里](#) U-Mail 将在当前队列中创建并使用 65 个子目录。这在高容量的服务器中会表现为提升性能。

磁盘

点击上面的“磁盘监视属性”选项，一般不用设置此选项。默认“磁盘空间检查引擎”对勾是不打的，表示不监视 U-Mail 程序所在的磁盘空间。对勾打上后，会降低服务器性能。

其它选项

服务

邮件头

修正

系统

磁盘

MultiPOP

WAB

其它

保存

取消

磁盘监视属性

☐ 启用磁盘空间检查引擎

当该选项作用时, U-Mail 将监视 U-Mail.EXE 程序所在磁盘的剩余空间。

低磁盘空间警告

☒ 发送警告给 当剩余磁盘

当剩余空间低于 KB

自动关闭

☒ U-Mail 将自动禁用 TCP/IP 服务, 如果

当剩余空间低于 KB

其它

☒ 每天的午夜, 在坏的邮件队列删除所有文件

☐ 每天的午夜备份配置文件

要备份的文件:

使用 | 字符分开多个文件类型。通配符可用。

备份会被放到"Backups"文件夹里

MultiPOP

点击上面的“MultiPOP”选项，一般此项不用设置。默认选择第一个选项，每次远程邮件已处理，便收集 MultiPOP 邮件。第二个选项可以设置每多少次远程邮件被处理后，收集 MultiPOP 邮件。第三个选项表示动态收集 MultiPOP 邮件，可以设置每小时不超过多少次，还可以设置等待至少介于每次收集之间的分钟数。

最下面还可以选择对勾“MultiPOP 在收集完后总是从所有服务器中删除邮件”，表示收集完后从对方服务器删除邮件，此设置覆盖所有 MultiPOP 用户的“在 POP 服务器中保留副本”设置。

其它选项

服务 邮件头 修正 系统 磁盘 MultiPOP WAB 其它

保存 取消

MultiPOP 选项

☒ 每次远程邮件已处理, 便收集 MultiPOP 邮件

☐ 收集 MultiPOP 邮件, 每 次远程邮件被处理

☐ 动态收集 MultiPOP 邮件

但不超过 次/小时

等待至少 介于每次收集之间的分钟数

☐ MultiPOP 在收集完后总是从所有服务器中删除邮件

此设置覆盖所有 MultiPOP 用户的“在 POP 服务器中保留副本”设置。

WAB

点击上面的“WAB”选项，一般此项不用设置。如果使用此项可选择对勾，在“使用此指定的 WAB 文件”下面的输入框填写 address.wab 文件路径，如 d:\umail\worldclinet\html\address.wab。需要在开始——附件——通讯簿，导出一个 address.wab 格式的文件，保存在 umail\worldclinet\html 目录。然后这样如果用户需要

更新本地 outlook 地址簿时, 只用下载 <http://mail.domain.com/webmail/address.wab> 即可。

其他

点击上面的“其他”选项, 一般此项不用设置, 用户可以根据实际情况进行调整。默认选择对勾启用磁盘检查来计算等待邮件数、使用严格限额、创建“Everynoe”列表、创建“MasterEveryone”列表、系统产生的邮件使用 NULL 反向路径、POP,IMAP,WebMail 的密码区分大小写、当遇到发送错误时删除前一封邮件。

其它选项

服务

邮件头

修正

系统

磁盘

MultiPOP

WAB

其它

保存

取消

磁盘监视属性

☒ 启用磁盘检查来计算等待邮件数

☒ 使用严格限额(计算子目录和隐藏文件)

☐ 不给新成员发送欢迎邮件

☒ 创建“Everyone”列表

☒ 创建 'MasterEveryone' 列表

☐ 允许要求帐号信息

☒ 系统产生的邮件使用 NULL 反向路径

☒ Apply content & spam filters to list mail before cracking individual copies

☒ POP, IMAP, WebMail 的密码区分大小写

☒ 启用磁盘检查来计算等待邮件数

☐ 列表清理器, 保存导致列表成员移除的邮件

☒ Honor '<List>-subscribe' and '<List>-unsubscribe' addresses

☐ 超过限额的帐号可接受邮件, 但无法发送邮件

☐ 在 NDR 邮件中不包含连接抄录

☐ 需要强密码

☒ 当遇到发送错误时删除前一封邮件(不选择让这些邮件返回给原发件人)

DNS黑名单

点击菜单左边的“DNS 黑名单”，此项反垃圾邮件组织联盟的 DNS 实时黑名单技术，开启 DNS 黑名单

可以过滤很多垃圾邮件。开启 DNS 黑名单后, 如果发件人 ip 地址在某个反垃圾组织名单, 将会拒绝接收邮件。

DNS-BL选项

默认看到的是“DNS-BL 选项”, 一般不用设置。默认选择第一个对勾“启用 DNS-BL 引擎”, 表示开启 DNS 黑名单即反垃圾组织检测; 如果不想开启 DNS 黑名单检测, 去掉该对勾即可。另外默认还选择下面 3 个对勾“来自白名单列表站点的邮件, 跳过‘received’邮件头”、“认证连接从 DNS-BL 查询排除”和“从 DNS-BL 查询中总是排除信任的 IP”。

DNS-BL主机

点击上面的“DNS-BL 选项”，系统默认添加几个反垃圾组织的主机，可以添加其他反垃圾组织主机。在“新建主机”输入框中输入反垃圾组织名称，“邮件”输入框中输入该组织的站点。

DNS 黑名单(DNS-BL)

DNS-BL 选项DNS-BL 主机缓存白名单

保存 取消

DNS-BL 主机

DNS-BL 引擎工作原理是查询下面的每个主机并查看接收 SMTP 连接的 IP 地址是否被因为传播垃圾邮件被加入黑名单。关于此工作怎样检查的完整细节查看 <http://www.ordb.org> 或 <http://www.mail-abuse.com>

当匹配下列主机之一时, 适合的邮件将被跟踪进入日志, 并在 SMTP 连接内报告。

新建主机:

邮件: 添加

sbl-xbl.spamhaus.org, mail from \$IP\$ refused by SpamHaus, see <http://www.sbl.org>

opm.blitzed.org, mail from \$IP\$ refused (blitzed)

relays.ordb.org, mail from \$IP\$ refused, see <http://www.ordb.org/faq/>

bl.spamcop.net, mail from \$IP\$ refused, see <http://www.spamcop.net>

移除

☐ 在找到一个匹配后停止主机查找

☐ 对于匹配发送“邮件”而不是“用户未知”

缓存

点击上面的“缓存”选项，一般不进行设置。系统默认选择对勾“自动缓存 DNS-BL”结果，存活时间为 5 分钟。由于黑名单主机可能在几分钟内更改，不建议修改默认存活时间。也可以在“输入新建缓存项目”下手动添加缓存，一般不进行设置。

DNS 黑名单(DNS-BL)

DNS-BL 选项

DNS-BL 主机

缓存

白名单

保存

取消

缓存选项

☒ 自动缓存 DNS-BL 结果

警告: 缓存 MAPS/RBL 查询的结果, 并不被 mail-abuse.org 的工程师建议。自从黑名单主机能在几分钟内更改, 我们建议你使用“默认存活时间”为最小值。
查看 <http://www.mail-abuse.com> 获得缓存的含义的详细信息

输入新建缓存项目

IP 地址

IP 地址将放在缓存

默认存活时间(分)

5

 (9999 = 用不过期)

☐ 亦使用默认存活时间自动缓存项目

最大缓存的条目

50

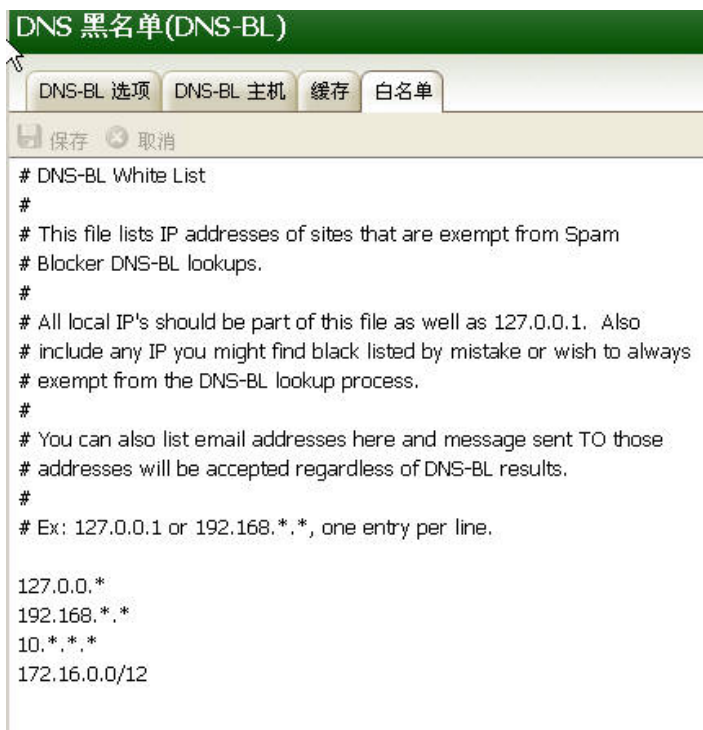
添加

移除

清除

白名单

点击上面的“白名单”选项，可以排除某个 ip 地址或某个网段，不进行 DNS 黑名单检测。一般是在对方发件人在 DNS 黑名单即反垃圾组织时，可以在此处暂时排除不进行 DNS 黑名单检测。



垃圾邮件过滤器

点击菜单左边的“垃圾邮件过滤器”，可以设置一些垃圾邮件过滤的参数，一般不建议进行调整。包含选项有“垃圾邮件过滤器”、“启发式”、“Bayesian”、“报告”、“排除”、“白名单（自动）”、“白名单（收件人）”、“白名单（发件人）”、“黑名单”等。比较常用的是在“白名单（收件人）”和“白名单（发件人）”项排除地址。

垃圾邮件过滤

默认显示的是“垃圾邮件过滤器”选项，此项一般不进行设置。“如果垃圾邮件过滤器判断邮件是垃圾邮件然后”下的选项是“完全删除邮件”。选择对勾“不过滤从本地源发送的邮件”和“不过滤从信任的或认证源的邮件”。默认不过滤大于 100k 的邮件，可根据自己情况设置。

垃圾邮件过滤器

白名单(收件人)

白名单(发件人)

黑名单

垃圾邮件过滤器

启发式

Bayesian

报告

HashCash

排除

白名单(自动)

保存

取消

垃圾邮件过滤器选项

U-Mail 的垃圾邮件过滤器使用多种技术检测和处理垃圾邮件。

如果垃圾邮件过滤器判断邮件是垃圾邮件然后...

☐ ... 把此邮件退回给发送者

☒ ... 完全删除邮件

☐ ... 把邮件放到垃圾邮件公共文件夹中

☐ ... 标记此邮件, 但让它继续沿路径传送

☒ 不过滤从本地源发送的邮件

☒ 不过滤从信任的或认证源的邮件

不过滤邮件大于 kb(0=升为2MB)

☐ 不发送标记为垃圾邮件的邮件

☐ 把垃圾邮件自动过滤到用户的 IMAP 垃圾邮件文件夹

DNS 可用? ☐ 是 ☐ 否 ☒ 测试

匹配白名单, 则从垃圾邮件分数减去

匹配黑名单, 则从垃圾邮件分数加上

匹配 DNS-BL 添加这么多点到垃圾邮件分数上

启发式

点击上面的“启发式”选项，此项一般不用修改。默认选择对勾“启用启发式邮件评分系统”和“在 SMTP 连接抄本中显示启发式结果”。如果关闭对勾“启用启发式邮件评分系统”，则表示不启用垃圾邮件过滤器。邮件是垃圾邮件，如果分数超过或等于 10.0，SMTP 邮件被拒，分数超过或等于 12.0，这里数值越大过滤越宽松，不建议修改默认参数。

垃圾邮件过滤器

白名单(收件人)

白名单(发件人)

黑名单

垃圾邮件过滤器

启发式

Bayesian

报告

HashCash

排除

白名单(自动)

保存

取消

启发式引擎选项

☒ 启用启发式邮件评分系统

启发式引擎用来辨别垃圾邮件。它使用规则来对每个邮件分析和分配一个“分数”。

邮件是垃圾邮件, 如果分数超过或等于 (0.0 - 550.0)

SMTP 邮件被拒, 分数超过或等于 (0 = 永不)

☒ 在 SMTP 连接抄本中显示启发式结果

由于性能的原因, SMTP 引擎不会检查超过 200kb 大小的邮件。

<= 2.0 - 非常不安全 - 潜在的高错误率

5.0 - 不安全, 但是错误率可以接受

10.0 - 公平的疏忽 - 某些垃圾邮件可能通过, 但是很低的错误率

500.0 - 如果不被看作垃圾邮件, 那它还是什么呢?

主题标签

保留空白并且主题文本将不可改变

例如: `[***SPAM*** Score/Req: _SCORE(0)/_REQD_]`

`_SCORE(0)_` 会被用接收的邮件的分数替换, `_REQD_` 会被请求的垃圾邮件限制替换。

Bayesian

点击上面的“Bayesian”选项，此项一般不用调整。默认选择对勾“把 Bayesian 知识应用到启发式邮件分数中”、“启用 Bayesian 预定学习”和“启用垃圾邮件地址和 ham 发送地址”等。在“对于已知垃圾邮件目录的路径”下输入框内容为 D:\umail\Public Folders\Bayesian Learning.IMAP\Spam.IMAP，在“对于已知非垃圾邮件目录的路径”下输入框内容为 D:\umail\Public Folders\Bayesian Learning.IMAP\Non-Spam.IMAP。

垃圾邮件过滤器

白名单(收件人)

白名单(发件人)

黑名单

垃圾邮件过滤器

启发式

Bayesian

报告

HashCash

排除

白名单(自动)

保存 取消

Bayesian 分类

Bayesian 分类是一个统计过程, 机器可以学习。通过分析成百上千的垃圾邮件和非垃圾邮件, 随着时间, 检测这两类邮件的类型越来越精确。

☒ 把 Bayesian 知识应用到启发式邮件分数中

单击这里, 分数处理会合并到目前为止的学习。

☒ 启用 Bayesian 预定学习

☒ 启用垃圾邮件和 ham 发送地址

对于已知垃圾邮件目录的路径(false negatives):

d:\umail\Public Folders\Bayesian Learning.IMAP\Spam.IMAP\

对于已知非垃圾邮件目录的路径(false positives):

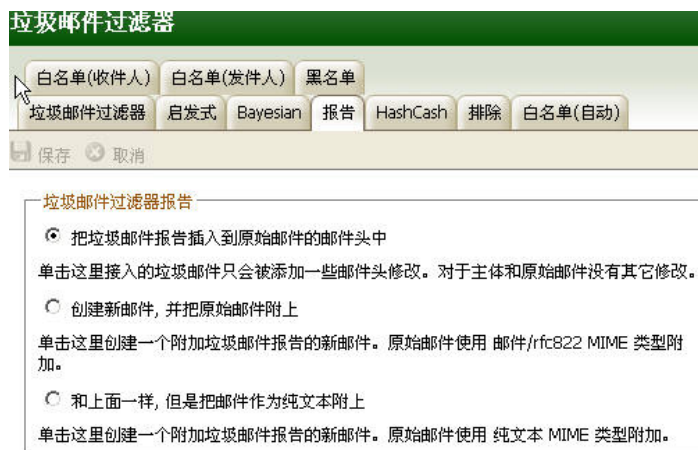
d:\umail\Public Folders\Bayesian Learning.IMAP\Non-Spam.IMAP\

在每晚午夜 U-Mail 会运行学习程序检查这两个目录的内容能改。

重要: 处理后邮件从这些文件夹中移除。

报告

点击上面的“报告”选项，此项一般不用更改。默认选择第一个对勾“把垃圾邮件报告插入到原始邮件的邮件头中”，表示接收的垃圾邮件只会添加一些邮件头，对于主体和原始邮件没有其他更改。



排除

点击上面的“排除”选项，可以排除发送到对方的地址，不进行垃圾邮件过滤。如发送到 comingchina.com 的邮件不通过反垃圾邮件过滤，则在下面输入*@comingchina.com。



白名单（自动）

点击上面的“白名单（自动）”项，一般不用进行设置。默认选择前3个对勾，第1个对勾为“启用地址簿白名单”，第2个对勾为“启用自动地址簿更新”，第3个对勾为“使用白名单邮件更新 Bayesian 引擎”。

垃圾邮件过滤器

白名单(收件人) 白名单(发件人) 黑名单

垃圾邮件过滤器 启发式 Bayesian 报告 HashCash 排除 白名单(自动)

保存 取消

自动白名单

☒ 启用地址簿白名单

当此选项启用, U-Mail 为本地用户检查地址簿并跳过垃圾邮件过滤器处理, 如果邮件的发送者被在那里发现。

☒ 启用自动地址簿更新

当启用时, U-Mail 会更新用户发送到的所有邮件地址到用户地址簿文件。

这是主开关。单个用户必须通过账号属性启用这些选项。

☒ 使用白名单邮件更新 Bayesian 引擎

当启用时, U-Mail 会把白名单的邮件副本放到非垃圾邮件学习文件夹。在学习生效前 Bayesian 学习必须启用。

☐ 启用白名单转发地址

当地址簿白名单启用时, 用户可以发送邮件给 `whitelist@`, 并让这些邮件的发送人添加到他们的地址簿文件中。

白名单（收件人）

点击上面的“白名单（收件人）”选项，可以添加排除本地某个信箱，不进行垃圾邮件过滤。如排除 `aaa@domain.com` 信箱收到的邮件不进行过滤，则在下面添加“`whitelist_to aaa@domain.com`”即可。如排除服务器某个域名不进行过滤，如 `aaa.com` 域名不进行垃圾邮件过滤，则在下面添加“`*@aaa.com`”即可。



白名单（发件人）

点击上面的“白名单（发件人）”选项，可以排除外面发进来的地址不进行垃圾邮件过滤。如排除过滤 comingchina.com 域名发过来的邮件，则在下面输入“whitelist_from *comingchina.com”即可。如排除过滤 abc@comingchina.com 信箱发过来的邮件，则在下面输入“whitelist from abc@comingchina.com”即可。



黑名单

点击上面的“黑名单”选项，可以将某个地址发过来的邮件都列为垃圾邮件。如要让 qast.com 域名发过来的邮件列为垃圾邮件，则下面输入“*@qast.com”即可。如要让 abc@add.com 信箱发过来的邮件列为垃圾邮件，则下面输入“abc@add.com”即可。



中转/信任/阻止

点击左边菜单的“中转/信任/阻止”，可看到“中继设置”、信任主机”和阻止”等选项。主要是设置别的邮件服务器是否可以通过本地服务器进行中继发送，还可以设置阻止恶意连接的IP地址。

中继设置

默认看到的是“中继设置”的选项，不建议进行设置。默认选择前 3 个对勾，第 1 个对勾是“此服务器不能从外部域中继邮件”，表示不允许外部地址通过本地服务器进行中继；第 2 个对勾是“拒绝接收来自未知本地用户的邮件”，表示拒绝任何发送给不存在的本地用户的邮件；第 3 个对勾“如果发件人声明他来自本地域则他的地址必须有效”，表示发件人必须是本地域中有效的用户。

安全

中继设置

信任主机

阻止

Greylisting

反向查询

局域网 IP

保存

取消

邮件中继

☒ 此服务器不能从外部域中继邮件

启用此开关 U-Mail 不管邮件是发送还是接收给已知的用户, 都会拒绝递送。

☒ 拒绝接收来自未知本地用户的邮件

设置此开关 U-Mail 会拒绝任何发送给不存在的本地用户的邮件。

☒ 如果发件人声明他来自本地域则他的地址必须有效

通常的绕过防中继的方法是猜测一个可用的账号, 使用这个账号来发送邮件。单击[这里](#)则猜测将无效果。

☐ 到已知别名地址的邮件可以总是被中继

使用 U-Mail 可以创建指向其它非本地域的别名。如果可以中继邮件给这样的别名则单击[这里](#)。

☐ 通过认证 SMTP 连接发送的邮件总是可以被中继

如果可以认证的发送者使用 AUTH 协议将被允许中继。

☐ 邮件可以通过域网关总是被中继

中继通常被允许用于网关主机域。

信任主机

点击上面的“信任主机”选项, 一般不进行添加。在这里添加的域或 IP 地址可以通过本地服务器进行中继发送。注意: 如果要想让别人通过本地服务器进行中继发送, 请关闭 U-Mail 加强投递功能, 否则加强投递功能会停止。

在“信任域”下输入域名如 `aaa.com`，点击添加后，则 `aaa.com` 域名就可以通过本地服务器进行中继发送。在“信任的 IP 地址”下输入 IP 地址如 `111.111.111.111`，点击添加后，则这个 IP 地址就可以通过本地服务器进行中继发送。

安全

中继设置

信任主机

阻止

Greylisting

反向查询

局域网 IP

保存

取消

域和 IP 权限

这些域被信任, 并被排除在非中继规则外。

信任域

信任的 IP 地址 - 通配符(192.168.0.*)可用

添加

添加

删除

删除

阻止

点击上面的“阻止”选项，此项一般不进行设置。这里开启此项，可以阻止外面非法连接。

安全

中继设置 信任主机 阻止 Greylisting 反向查询 局域网 IP

保存 取消

阻止设置

阻止是预备的插入 SMTP 进程中的延迟, 阻止发送服务器持续尝试递送。

☒ 激活阻止 **白名单**

SMTP RCPT 阻止临界值:

SMTP RCPT 阻止延迟(单位秒): 比例系数:

自动 IP 屏蔽

☒ 激活自动 IP 屏蔽 **高级**

“未知接收者”错误临界值:

☒ 添加到 IP 屏蔽后关闭 SMTP 会话

U-Mail 会阻止以后从任何在一次连接中引起此数量的“未知接收者”递送错误的主机。

☐ 阻止站点, 如果连接超过 次/ 分钟

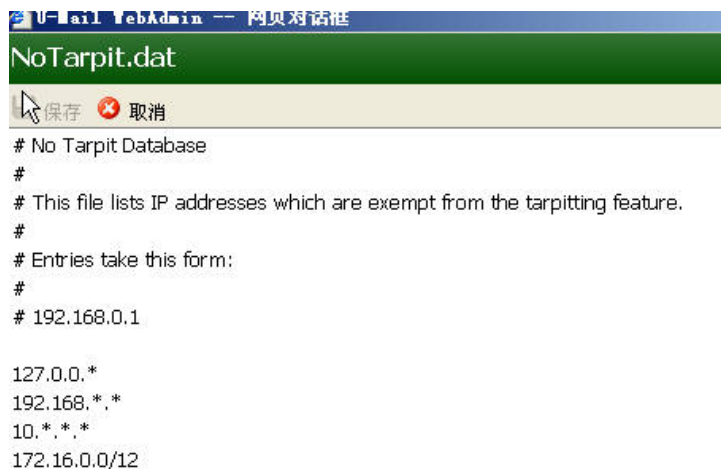
☒ 阻止站点, 如果认证尝试错误次数超过

阻止站点这么长时间(分钟)

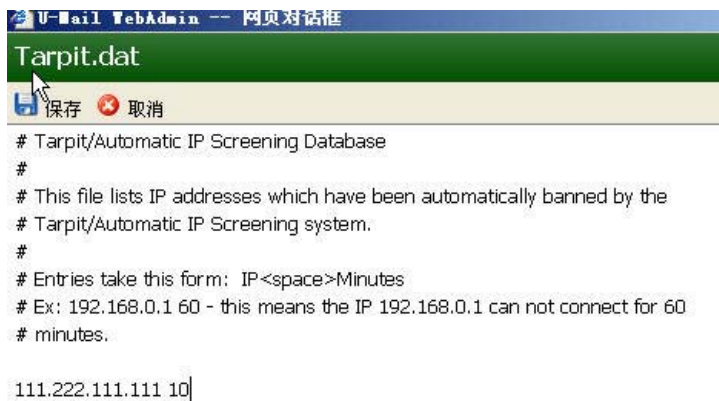
这是由自动 IP 屏蔽阻止的主机的时间长度。在此间隔后, 他们不再被阻止。

☒ 认证连接从阻止和 IP 屏蔽中排除

(1) 默认在“阻止设置”下选择对勾“激活阻止”。SMTP RCPT 阻止临界值为 5，SMTP RCPT 阻止延迟（单位秒）为 10，比例系数为 1。点击右边的“白名单”按钮，可以把某个 IP 地址加入白名单，排除阻止。



(2) 在“自动 IP 屏蔽”下，默认选择对勾“激活自动 IP 屏蔽”，“未知接收者”错误临界值为 3，选择对勾“阻止站点，如果认证尝试错误次数超过”为 3，阻止站点这么长时间（分钟）为 10，选择对勾“认证连接从阻止和 IP 屏蔽中排除”。可以选择第 3 个对勾“阻止站点，如果连接超过”，根据情况进行设置多少分钟内可以连接多少次。点击右边的“高级”按钮，可以看到被阻止的 ip 地址和剩余时间。如 111.222.111.111 10 表示 111.222.111.222 这个 IP 地址被阻止 10 分钟。



(3) 注意：如果个别局域网使用 outlook 客户端连接服务器频繁，ip 可能会被服务器阻止。点击右边“高级”按钮可以查看 IP 地址是否被阻止，可以点击右边的“白名单”按钮将 IP 地址加入白名单，不进行阻止。如果个别局域网使用 ADSL 等动态 ip 地址，则去掉在“自动 IP 屏蔽”下对勾“激活自动 IP 屏蔽”。

Greylisting

点击菜单左边的“Greylisting”，一般不使用此项。由于使用此项可能收不到正常邮件，这里不做介绍。

安全

中继设置

信任主机

阻止

Greylisting

反向查询

局域网 IP

保存

取消

Greylist 设置

Greylisting 通过通知发送邮件服务器发生临时错误, 必须在以后的时间再次尝试递送来工作。理论上是垃圾邮件工具不重试递送但是合法的邮件服务器会这么做。

☐ 启用 greylisting

白名单

☒ ... 仅用于网关域

延迟初始传递尝试 451 这么长时间:

15

在这些天后中止未使用的 greylisting 数据库记录:

10

Greylisting 维护一个有每个接入的连接的信息的数据文件。在此数据库中的记录如果这么多天没有活动则会被移除。

高级

☐ Don't include IP address when greylisting (use only MAIL & RCPT values)

☒ 不 greylist 通过 SPF 处理的并发连接

☒ 不 greylist 来自本地地址簿中的发件人的邮件

☒ 不 greylist 邮件到邮件列表

☒ 不 greylist 通过认证连接发送的邮件

Greylisting 是在和垃圾邮件做斗争中的有争议的武器。它对即使是可能的重要邮件也特意延迟。它也很消耗资源。详细的 greylisting 信息可以在 Internet 上很容易得找到。

递归查询/局域网 IP

点击菜单左边的“反向查询”，此项一般不进行设置。默认选择 3 个对勾，第 1 个对勾是“执行在 MAIL 命令中传递的值”，第 2 个对勾是“如果一个查询返回”域未找到”则拒绝接收邮件”，第 3 个对勾是“在可疑邮件插入”X-Lookup-Warning”邮件头”。

安全

中继设置

信任主机

阻止

Greylisting

反向查询

局域网 IP

保存

取消

反向查询

此开关允许 U-Mail 把反向查找输入主机的 IP 或身份验证的结果记录到日志文件中。

☐ 在输入 SMTP 连接执行反向 PTR 记录查找

☐ 如果 PTR 记录匹配则发送 501 并关闭连接

☐ 在 HELO/EHLO 域执行查找

☐ 忘记鉴定(警告)则发送 501 并关闭连接

☐ 如果一个查询返回“域未找到”则拒绝接收邮件

☐ ... 发送 501 错误代码(正常发送 451 错误代码)

☐ ... 并接着关闭连接

☒ 执行在 MAIL 命令中传递的值

☐ 忘记鉴定(警告)则发送 501 并关闭连接

☒ 如果一个查询返回“域未找到”则拒绝接收邮件

☐ ... 发送 501 错误代码(正常发送 451 错误代码)

☐ ... 并接着关闭连接

☒ 在可疑邮件插入“X-Lookup-Warning”邮件头

次文件头包含对过滤器有用的信息

白名单

地址抑制

点击菜单左边的“地址抑制”，利用此项可以拒绝接收外部某个恶意信箱的连接。在下面输入框内输入要拒绝接收的信箱地址，如 aaa@123.com。也可以拒绝接收某个域名的邮件，在输入框输入如*@123.com。

在上面的“选择域”下拉框还可以选择只让本地服务器某个域名拒绝接收。可以选择对勾“连接期间拒绝接收邮件”，表示此域名拒绝接收邮件。还可以选择对勾“当邮件被拒绝时通知发件人”。

The screenshot shows the '安全' (Security) configuration window with the '地址抑制' (Address Blocking) tab selected. The interface includes a title bar, tabs for '地址抑制', 'IP 屏蔽', and '主机屏蔽', and buttons for '保存' (Save) and '取消' (Cancel). The '地址抑制' section contains a description of address blocking, a '选择域' (Select Domain) dropdown menu set to 'All Domains', two checkboxes for '连接期间拒绝接收邮件' (Reject mail during connection) and '当邮件被拒绝时通知发件人' (Notify sender when mail is rejected), and a list of accounts with '添加' (Add) and '删除' (Delete) buttons.

安全

地址抑制 IP 屏蔽 主机屏蔽

保存 取消

地址抑制

地址抑制, 使用 E-mail 的地址、或内向 SMTP 连接通过的地址, 和在这里的配置的值互相比较。如果匹配邮件将被拒绝递送。在某些实例邮件将在前者就被拒绝。

选择域: All Domains

☒ 连接期间拒绝接收邮件

☐ 当邮件被拒绝时通知发件人

帐号: 可以使用如 "*@domain.com" 或 "*@????.com" 的通配符。

添加

删除

IP/主机屏蔽

点击左边菜单的“IP/主机屏蔽”，包含“IP 屏蔽”和“主机屏蔽”两项。

IP 屏蔽

点击菜单左边的“IP/主机屏蔽”，默认看到的是“IP 屏蔽”选项。这里可以屏蔽外面某个 IP 连接。一般在输入框内填写要屏蔽的 IP 地址如“111.222.111.222”，点击添加，然后“选择远程 IP 不能连接”。如果本地服务器有多个 IP 地址，还可以在上面“本地 IP”下拉框选择一个 IP，只对连接此 IP 地址进行屏蔽。下面“未定义的 IP 的默认”，默认是选择“未定义的 IP 可连接到此本地 IP”，这里不进行设置。

安全

地址抑制

IP 屏蔽

主机屏蔽

保存

取消

IP 屏蔽

IP 屏蔽通过比较连入的 IP 和在此对话框的指定 IP 来工作。如果内向连接匹配, 根据你在这里的配置来判断连入的连接是否匹配来决定是否被允许。

本地 IP:

All IPs

远程 IP: 192.168.0.* 或 192.168.*.1 通配符格式可用。

☒ 远程 IP 能够连接

☐ 远程 IP 不能连接

添加

删除

未定义的 IP 的默认:

☒ 未定义的 IP 可连接到此本地 IP

☐ 未定义的 IP 不能连接到此本地 IP

主机屏蔽

点击上面的“主机屏蔽”选项, 这里可以屏蔽外面某个主机连接。一般在输入框内填写要屏蔽的主机地址如“*@aaa.com”, 点击添加, 然后“选择远程主机不能连接”。如果本地服务器

有多个 IP 地址, 还可以在上面“本地 IP”下拉框选择一个 IP, 只对连接此 IP 地址进行屏蔽。下面“未定义的主机的默认”, 默认是选择“未定义的主机可连接到此本地 IP”, 这里不进行测试。

全

地址抑制 IP 屏蔽 主机屏蔽

保存 取消

主机屏蔽

主机屏蔽通过比较连入 SMTP 连接的 HELLO 或 HELO 和这里列出的值来工作。如果内向连接匹配, 根据你在这里的配置来判断连入的连接是否匹配来决定是否被允许。

本地 IP: All IPs

远程主机: Wildcards of the form *.altn.com or altn.* are acceptable.

☒ 远程主机能够连接
☐ 远程主机不能连接

添加

删除

未定义的主机默认:

☒ 未定义的主机可连接到此本地 IP
☐ 未定义的主机不能连接到此本地 IP

IP 防护

点击菜单左边的“IP 防护”，此项一般不用设置。默认选择两个对勾“发送给有效本地用户邮件，可免除域/IP 对比(&M)”和“IP 防护允许别名”。在下面填写域名和对应的 IP 地址，则这个域名发进来的邮件必须和这里的 IP 地址相对应。在域名输入框下的格式为“*.abc.com”；在 IP 地址输入框下填写对方邮件服务器 IP 地址，格式为“111.222.111.111”或“111.222.111.*”。

安全

IP 屏蔽

SMTP 验证

SMTP 之前 POP

站点策略

保存

取消

当前定义的 域/IP 对

☒ 发送给有效本地用户邮件, 可免除域/IP 比对(&M)

☒ IP 防护允许别名

当邮件声称来自下列域之一时(如 MAIL FROM: mailbox@domain.com), 它所递送的邮件也必须和指定的 IP 地址相同。

Wildcards like *.altn.com and 192.168.0.* are ok.

域名:

IP 地址:

添加

移除

SMTP 验证

点击菜单左边的“SMTP 验证”，此项一般不进行设置。默认选择对勾“已验证的发信人，他们使用的 IP 有效”、“已验证的用户，可免除在 SMTP 之前先 POP 的需求”和“来自”Postmaster”别名的邮件需要验证连接”。

安全

IP 屏蔽SMTP 验证SMTP 之前 POP 站点策略

保存取消

SMTP 验证

☒ 已验证的发信人, 他们使用的 IP 有效
选择该选项, 当邮件来自已验证的源时, U-Mail 将忽略由 IP 防护所设置的限制。

☒ 已验证的用户, 可免除在 SMTP 之前先 POP 的需求
选择该选项, U-Mail 将免除已验证的连接, 要 SMTP 发信之前先 POP 收信的限制。

☐ 当邮件来自本地帐号, 总是需要验证
☒ 你必须指定你的 DNS 服务器的 IP 地址。如果你对此信息不确认, 联系你的 ISP 或 Email 管理员。
当该选项已启用, 任何声称来自本地帐号的邮件, 在认可之前将需要验证。

☒ 来自“Postmaster”别名的邮件需要验证连接
垃圾邮件发送者和黑客知道 'Postmaster' 帐号存在。你可以使用该选项避免他们以此项事实剥削。

☐ 验证凭据必须匹配邮件发送者
该选项需要邮件发送者, 使用他自己拥有的验证凭据。

全局 AUTH 密码

在某些实例, 提供全局密码验证有用。

SMTP 之前 POP

点击菜单左边的“SMTP 之前 POP”, 此项一般不进行设置。默认选择对勾“本地发信人在时间内, 必须访问过邮箱 5 分钟”、“通过 ATRN 的邮件收集, 可免除此项需求”和“从下列地址发送的邮件不触发自动回复”。

安全

IP 屏蔽

SMTP 验证

SMTP 之前 POP

站点策略

保存

取消

SMTP 之前 POP

☒ 本地发信人在时间内, 必须访问过邮箱 分钟

单击[这里](#)强制本地用户, 必须先使用 POP、IMAP、或 WorldClient 检查邮件, U-Mail 才会接受他们的邮件。

☒ 通过 ATRN 的邮件收集, 可免除此项需求

☐ 发送到本地收信人的邮件, 可免除此项需求

☒ 从下列地址发送的邮件不触发自动回复。

SPF/Domain Keys & DKIM

点击菜单左边的“SPF,DK,和 DKIM”, 默认显示的是“发送者策略框架”选项, 此项一般不进行使用。SPF 记录表示接收邮件时, 会通过 DNS 查询对方的 SPF 记录是否真正地来源于 SPF 中所记录的服务器。由于很多邮件服务器都没有设置 SPF 记录, 开启此选项后, 可能造成某些正常邮件无法接收, 因此一般不使用此功能。



3 系统后台常用功能说明

1. 所有收发邮件存档

可以将系统所有收发的邮件备份到某个邮箱。详细设置见 3.4.1（主域）下第 7（存档）项。

2. 设置学习垃圾邮件

可以手动学习垃圾邮件，使垃圾邮件越来越少。详细设置见 3.4.2（共享文件夹）。

3. 邮件监控/内容过滤器

此项功能强大，可以做多种邮件监控（备份）设置和多种内容过滤选项等。详细设置见 3.5.1（内容过滤器）下第 1（内容过滤器）项。

4. 自动 IP 屏蔽

此项可以理解为邮件防火墙，可以自动屏蔽多个恶意连接。如果自己局域网连接频繁，被拒绝掉，可以打开此项查看自己 IP 是否被拌掉。详细设置见 3.5.4（中转/信任/阻止）下第 3 项（阻止）项。

第三部分：技术白皮书



1. U-Mail技术资料

1.8 忘记系统管理员 system 帐号密码怎么办？

请联系 U-MAIL 的技术支持。

1.11 我的邮件系统只能发，不能收，为什么？

不能收一般有如下几个原因：

- 1、MX 记录解析错误。您可以用这条命令测试一下你的域名解析是否正确：`nslookup -qt=mx yourdomain.com`
- 2、端口映射错误。有些邮件服务器是放在内网，然后通过路由器将外网 IP 的端口映射到内网的邮件服务器。你可以在外网执行命令测试端口映射是否做好：`telnet IP 地址 25` 是否有响应。
- 3、防火墙没有开放 25 端口。如果操作系统安装有防火墙软件或者网关有防火墙，一般至少要开放 25、80、110 端口。

1.12 我的邮件系统只能收，不能发，为什么？

- 安装有防火墙，服务器连接不到外面 25 端口。
- DNS 无效，不能解析对方域名。

解决办法：更换 DNS 服务器。例如：202.96.134.133 202.96.128.68 最好是本地电信的 DNS

- 邮件服务器的 IP 地址存在对端的垃圾邮件数据库内，导致邮件拒收。

解决办法：和对端邮件服务器网管联系，建立绿色通道；

联系维护垃圾邮件数据库的管理人员，将 IP 地址从数据库中去除；

U-MAIL 企业版中已经内置了全球收发保证，即使邮件服务器 IP 在对方的黑名单中，邮件照发不误

- 邮件符合对端的某些过滤规则。

例如：域名 MX 记录和服务器 IP 记录不符；在域名服务商那里一定要检查 MX 记录是否正确。

- 对方邮箱空间已满。不再接收邮件。
- 对方邮件服务器或两端之间线路故障。

服务器设置：

- 检查是否禁止邮件外发
- 检查设置发送邮件的大小是否符合需要
- 检查邮箱空间是否已满，如果空间已满并且设置了备份发送邮件的时候，用 webmail 发送邮件将会失败

总之，出现问题了，首先查看退信，查看 log 文件分析问题所在。

2. 邮件域名DNS相关知识

2.1 什么是IP地址?

IP 地址是在网络上分配给每台计算机或网络设备的 32 位数字标识。在 Internet 上, 每台计算机或网络设备的 IP 地址是全世界唯一的。IP 地址的格式是 xxx.xxx.xxx.xxx, 其中 xxx 是 0 到 255 之间的任意整数。例如, 科迈网站主机的 IP 地址是 210.22.12.54。

2.2 什么是固定IP地址?

固定 IP 地址是长期分配给一台计算机或网络设备使用的 IP 地址。一般来说, 采用专线上网的计算机才拥有固定的 Internet IP 地址。建议邮件服务器使用固定 IP 地址更加稳定。

2.3 什么是动态IP地址?

通过 Modem、ISDN、ADSL、有线宽频、小区宽频等方式上网的计算机, 每次上网所分配到的 IP 地址都不相同, 这就是动态 IP 地址。因为 IP 地址资源很宝贵, 大部分用户都是通过动态 IP 地址上网的。如果服务器使用动态 IP 地址, 需要用花生壳类的动态域名解析软件进行域名解析。

2.4 什么是域名？域名由什么构成？

域名是 internet 上用来寻找网站所用的名字，是 internet 上的重要标识，相当于主机的门牌号码。每一台主机都对应一个 IP 地址，每一个 IP 地址由一连串的数字组成，如 101.25.11.34。人们为了方便记忆就用 域名来代替这些数字来寻找主机，如 mydomain.com。每一个域名与 IP 地址是一一对应的，人们输入域名，再由域名服务器（DNS）解析成 IP 地址，从而找到相应的网站。每一个网址和 EMAIL 都要用到域名。在英文国际域名中，域名可以英文字母和阿拉伯数字以及横杠“-”组成，最长可达 67 个字符（包括后缀），并且字母的大小写没有区别，每个层次最长不能超过 22 个字母。在国内域名中，三级域名长度不得超过 20 个字。

2.5 什么是DNS？

域名管理系统 DNS（Domain Name System）是域名解析服务器的意思.它在互联网的作用是：把域名转换成为网络可以识别的 ip 地址.比如：我们上网时输入的 www.163.com 会自动转换成为 202.108.42.72

2.6 什么是A记录？

A (Address) 记录是用来指定主机名（或域名）对应的 IP 地址记录。用户可以将该域名下的网站服务器指向到自己的 web server 上。同时也可以设置您域名的二级域名。

2.7 什么是NS记录?

NS (Name Server) 记录是域名服务器记录, 用来指定该域名由哪个 DNS 服务器来进行解析。

2.8 什么是别名记录(CNAME)?

也被称为规范名字。这种记录允许您将多个名字映射到同一台计算机。通常用于同时提供 WWW 和 MAIL 服务的计算机。例如, 有一台计算机名为“host.mydomain.com”(A 记录)。它同时提供 WWW 和 MAIL 服务, 为了便于用户访问服务。可以为该计算机设置两个别名 (CNAME): WWW 和 MAIL。这两个别名的全称就是“www.mydomain.com”和“mail.mydomain.com”。实际上他们都指向“host.mydomain.com”。

2.9 什么是泛域名解析?

泛域名解析定义为: 客户的域名 a.com, 之下所设的*.a.com 全部解析到同一个 IP 地址上去。比如客户设 b.a.com 就会自己自动解析到与 a.com 同一个 IP 地址上去。

2.10 什么是MX记录?

MX (Mail Exchanger) 记录是邮件交换记录, 它指向一个邮件服务器, 用于电子邮件系统发邮件时根据 收信人的地址后缀来定位邮件服务器。例如, 当 Internet 上的某用户要发一封信给 `user@mydomain.com` 时, 该用户的邮件系统通过 DNS 查找 `mydomain.com` 这个域名的 **MX** 记录, 如果 **MX** 记录存在, 用户计算机就将邮件发送到 **MX** 记录所指定的邮件服务器上。如果域名没有做 **MX** 记录, 将无法收到邮件。

2.11 什么是IP反向解析?

作过 DNS 服务器的朋友一定会知道 DNS 服务器里有两个区域, 即“正向查找区域”和“反向查找区域”, 反向查找区域即是这里所说的 **IP** 反向解析, 是将 **IP** 解析到域名。它的作用就是通过查询 **IP** 地址的 **PTR** 记录来得到该 **IP** 地址指向的域名, 当然, 要成功得到域名就必需要有该 **IP** 地址的 **PTR** 记录。

在垃圾邮件泛滥的今天, 垃圾邮件给我们的生活、工作、学习带来了极大的危害。由于 **SMTP** 服务器之间缺乏有效的发送认证机制, 即使采用了垃圾邮件识别阻拦技术效果仍旧一般, 再者垃圾邮件识别阻拦技术主要是在收到信件后根据一定条件进行识别的, 需要耗费大量服务器资源, 如果能在信件到达服务器之前就采取一定手段, 这样就能大大提高服务器效率了。因此, 目前许多邮件服务器如 `sina.com`, `hotmail.com`, `yahoo.com.cn` 等等都采用了垃圾邮件识别阻拦技术+**IP** 反向解析验证技术以更好的阻拦垃圾邮件。

2.12 什么是SPF记录

前一段时间, 微软公司已经开始进行了一项实验, 实验的内容是一种被叫做“来自寄件人许可” (**Sender Permitted From**, **SPF**) 的标准, 这个标准旨在阻止电子邮件被没有得到授权的人所发送, 并以此来减少垃圾邮件。

SPF 通过向某个邮件服务器的 DNS 入口中添加一个 TXT 的记录来进行工作;这个记录中提供了一些关于任何以该域的名义发送电子邮件的被授权的人的行为详细信息。

当 SPF 发觉邮件服务器收到了电子邮件的时候,它就会在发送者的地址中进行 DNS 的查找,以便确定是否存在有可供其使用的 SPF 记录。随后它会把电子邮件的标题与 SPF 记录进行比较,查看该电子邮件是否真正地来源于 SPF 中所记录的服务器。如果不是,那么接收方的服务器能够采取适合的行动(这种行动是能够增加该邮件的垃圾程度分数的一种,以便将其完全阻止)。

2.13 RBL是什么?

RBL 全称是 Real-time Blackhole Lists, 是国外的反垃圾邮件组织提供的检查垃圾邮件发送者地址的服务, RBL 功能对中国用户而言,几乎不可用。因为我们发现大部分中国的 IP 地址都在 RBL 数据库里。请不要启用 RBL 功能。常用的 RBL 服务器地址有:

relays.ordb.org;dnsbl.njabl.org;bl.spamcop.net;sbl.spamhaus.org;dun.dnsrbl.net;dnsbl.sorbs.net 查询和删除 RBL 中的 IP 地址请到 <http://openrbl.org/> 和 <http://ordb.org>

2.14 全国各地电信、联通、网通DNS服务器地址

1. 全国各地电信 DNS 服务器地址

北京: 202.96.199.133 202.96.0.133 202.106.0.20 202.106.148.1 202.97.16.195
上海: 202.96.199.132 202.96.199.133 202.96.209.5 202.96.209.133
天津: 202.99.96.68 10.10.64.68
广东: 202.96.128.143 202.96.128.68 202.96.128.110
深圳: 202.96.134.133 202.96.154.8 202.96.154.15
河南: 202.102.227.68 202.102.245.12 202.102.224.68
广西: 202.96.128.68 202.103.224.68 202.103.225.68
福建: 202.101.98.54 202.101.98.55
厦门: 202.101.103.55 202.101.103.54
湖南: 202.103.0.68 202.103.96.68 202.103.96.112
江苏: 202.102.15.162 202.102.29.3 202.102.13.141 202.102.24.35
陕西: 202.100.13.11 202.100.4.16
西安: 202.100.4.15 202.100.0.68
湖北: 202.103.0.68 202.103.0.117 202.103.24.68
山东: 202.102.154.3 202.102.152.3 202.102.128.68 202.102.134.68
浙江: 202.96.102.3 202.96.96.68 202.96.104.18
辽宁: 202.98.0.68 202.96.75.68 202.96.75.64 202.96.69.38 202.96.86.18 202.96.86.24
安徽: 202.102.192.68 202.102.199.68 10.89.64.5
重庆: 61.128.128.68 10.150.0.1
黑龙江: 202.97.229.133 202.97.224.68
河北: 202.99.160.68 10.17.128.90
保定: 202.99.160.68 202.99.166.4
吉林: 202.98.5.68 202.98.14.18 202.98.14.19
江西: 202.101.224.68 10.117.32.40 202.109.129.2 202.101.240.36
山西: 202.99.192.68 202.99.198.6
新疆: 61.128.97.74 61.128.97.73
贵州: 202.98.192.68 10.157.2.15
云南: 202.98.96.68 202.98.160.68

四川: 202.98.96.68 61.139.2.69
重庆: 61.128.128.68 61.128.192.4
成都: 202.98.96.68 202.98.96.69
内蒙古: 202.99.224.68 10.29.0.2
青海: 202.100.128.68 10.184.0.1
海南: 202.100.192.68 202.100.199.8
宁夏: 202.100.0.68 202.100.96.68
甘肃: 202.100.72.13 10.179.64.1
香港: 205.252.144.228 208.151.69.65
澳门: 202.175.3.8 202.175.3.3

2. 全国网通 DNS 服务器地址

北京: 202.106.196.152 202.106.196.115 202.96.199.133 202.97.16.195 202.106.0.20 202.106.148.1
移动北京: 211.136.17.107
天津: 202.99.96.68
上海: 202.96.199.132 202.96.199.133 202.96.209.5
移动上海: 211.136.18.171
重庆: 61.128.128.68 61.128.192.4
浙江: 202.96.102.3
广东: 202.96.128.143 202.96.128.68
深圳: 202.96.134.133 202.96.154.8 202.96.154.15
陕西: 202.100.13.11
西安: 202.100.4.15 202.100.0.68
辽宁: 202.96.75.68
江苏 pub.jsinfo.net 202.102.29.3
四川: 61.139.2.69
成都: 202.98.96.68

河北: 202.99.160.68
保定: 202.99.160.68 202.99.166.4
河南: 202.102.227.68 202.102.224.68
山西: 202.99.198.6
吉林: 202.98.0.68
山东;202.102.152.3 202.102.128.68
淄博: 211.97.168.129
福建: 202.101.98.55
湖南: 202.103.100.206
广西: 10.138.128.40
江西: 202.109.129.2
云南: 202.98.160.68
武汉: 202.103.24.68 202.103.0.117
新疆: 61.128.97.73 61.128.97.74
香港: 205.252.144.228
澳门: 202.175.3.8
辽宁: 202.96.75.68
江苏: 202.102.29.3
四川: 61.139.2.69
重庆: 61.128.128.68
河北: 202.99.160.68
山西: 202.99.198.6
吉林: 202.98.0.68
山东: 202.102.152.3
福建: 202.101.98.55
湖南: 202.103.100.206
广西: 10.138.128.40
江西: 202.109.129.2

云南: 202.98.160.68
移动广州: 211.136.20.203
南京: 202.102.24.35
深圳: 202.96.134.133
南宁: 202.103.224.68 202.103.225.68
西安交通大学: 202.117.0.20 202.117.0.21
重庆网通: 211.158.2.68
番禺: 202.96.128.68
大庆网通: 202.97.224.68
吉通北京: 203.93.18.2
吉通广西: 201.14.251.1
洛阳: 202.102.227.68
淄博: 202.102.137.68 202.102.128.68
上海市: 202.96.209.5 202.96.209.133
青岛: 202.102.134.68 202.102.128.68
河南洛阳: 202.102.224.68 202.102.227.68
大连: 202.96.64.68 202.96.69.38
济南: 210.52.207.2
云南: 202.96.209.5 202.106.0.20
福州还有一个备用的: 202.101.98.54
赤壁: 202.103.0.117 202.103.44.5
天津联通: 211.94.193.129
铁通徐州: 211.98.2.4 202.102.9.141
广西电信: 202.103.224.68 202.103.224.66
成都长宽: 211.162.130.8 211.162.130.9 61.139.2.69
杭州: 202.96.96.68 202.96.103.36
秦皇岛网通: 202.99.160.68
大庆电信: 202.97.224.68 202.97.230.4

山东临沂: 202.102.134.68 202.102.152.3 202.102.128.68

厦门: 202.101.103.55 202.101.103.54

江苏无锡: 202.102.2.141

淄博: 202.110.20.171 210.44.176.1

泉州: 202.101.107.55

福州: 202.101.98.55

四川攀枝花: 61.139.2.69

东莞: 202.96.128.143 202.96.128.68

温州: 202.96.104.16 202.96.96.68

赣州: 202.101.228.100

西安: 61.134.1.9 61.134.1.4

石家庄 211.162.226.80

湖南省 长沙 202.103.96.68 202.103.96.112

邵阳 202.103.103.3

岳阳 202.103.86.3 202.103.99.3

河南: 202.102.224.68 202.102.227.68

大连辽南地区: 202.96.69.38 202.96.64.68

内蒙赤峰: 202.99.224.8 202.99.224.68

河北石家庄: 202.99.160.68 202.99.168.8

河北邢台宁晋: 202.99.160.68 202.99.166.4

河北邢台邯郸: 202.99.160.68 202.99.166.4

内蒙古自治区包头市: 202.99.224.8 202.99.224.67 202.99.224.68

3. 全国各地铁通 DNS 服务器地址

香港: 205.252.144.228

澳門: 202.175.3.8

深圳: 202.96.134.133 202.96.154.8 202.96.154.15

北京: 202.96.0.133 202.96.199.133 202.97.16.195 202.106.0.20 202.106.148.1

廣東: 202.96.128.143 202.96.128.68

上海: 202.96.199.132 202.96.199.133 202.96.199.133

浙江: 202.96.102.3 202.96.96.68 202.96.104.18

陝西: 202.100.13.11

天津: 202.99.96.68

遼寧: 202.96.75.68 202.96.64.68 202.96.91.58

江蘇: 202.102.29.3

四川: 61.139.2.69

河北: 202.99.160.68

山西: 202.99.198.6

吉林: 202.98.0.68

山東: 202.102.152.3 202.102.128.68

福建: 202.101.98.55

湖南: 202.103.100.206

廣西: 10.138.128.40

江西: 202.109.129.2 202.101.224.68 202.101.240.36

雲南: 202.98.160.68

重慶: 61.128.128.68

河南: 202.102.227.68 202.102.224.68 202.102.245.12

新疆: 61.128.97.73 61.128.97.74

保定: 202.99.160.68 202.99.166.4

武漢: 202.103.24.68 202.103.0.117

西安: 202.100.4.15 202.100.0.68

成都: 202.98.96.68 202.98.96.69

重慶: 61.128.192.4

烏魯木齊: 61.128.97.73

廈門: 202.101.103.55

3. U-Mail退信分析

看退信最下面的日志，并按照相应的错误信息进行匹配。

511 sorry, no mailbox here by that name

unknown user account

... User unknown

Name server reports domain name unknown

mailbox unavailable

550 Invalid User:

invalid recipient

No such user here

All recipients are invalid

User unknown in virtual alias table

Mailbox not found

Recipient address rejected: User unknown in relay recipient table

以上信息均为收件人地址错误或者无效，检查收件人地址，检查邮件服务器的域名解析服务器

554 Connection refused(mx). MAIL FROM [test@test.com] mismatches client IP [74.86.11.12].

域名和 IP 地址不对应导致的拒收 [上面的域名和 IP 地址会变化，类似的情况]，修正您的域名解析，域名解析请参考：<http://www.comingchina.com/dnsconfig.htm>

553 5.7.1 SpamTrap=reject mode, dsn=5.7.1, Message blocked by BOX Solutions (www.box-sol.com)

SpamTrap Technology, please contact the MUSTEK site manager for help: (bkndr63272).

如果出现类似上述的信息是因为您发了不受对方欢迎的信件，导致对方拒收

551 User not local; please try

邮件被 GFW 过滤，GFW 是指 Great Firewall，中国国家防火墙。尝试将邮件内容打包压缩或者放入 OFFICE 文档内进行邮件传输

Winsock Error 10053 Connection abort.

网络通讯故障

Winsock Error 10060 The connection timed out.

连接超时，网络通讯故障造成

Winsock Error 10061 The connection timed out.

对方服务器拒绝连接，对方服务器主动断开链接，这通常是由国外不活跃的服务器造成的。

452 4.3.1 Out of memory

This message is 60 minutes old; it has 0 minutes left in this queue

Remote queue lifetime exceeded; message placed in retry queue

一般情况下，邮件会进入重试队列进行再次发送，这种情况下对方的邮件服务器一般是 Exchange，这是 Exchange 的内部错误造成的。

553 Requested action not taken: no smtp MX

收件人邮箱地址错误，域名无法被解析，检查收件人地址，或者对方域名解析设置错误。

501 syntax.helo hostname

501 Invalid domain name

502 unimplemented command

503 5.0.0 polite people say HELO first

533 relay restriction

544 <>:Recipient address rejected: Relay access denied

传输中的语法错误，原因不明。