

---

爱思华宝统一通信

# 反病毒向导

版本 10.4

**IceWarp**<sup>®</sup>





# 目录

<b>反病毒</b>	<b>1</b>
反病毒.....	2
最新的 Avast! 引擎.....	2
支持卡巴斯基反病毒.....	2
支持 LB 环境.....	2
想到.....	3
常规.....	3
Avast 镜像站 URL 设置.....	4
定义一个 Web 站点.....	4
测试 Web 站点.....	5
设置镜像.....	5
测试镜像站点.....	5
安排镜像更新.....	5
动作.....	7
扩展名过滤器.....	9
外部病毒过滤.....	10
高级.....	13
EICAR 测试.....	16
访问模式 -- 策略.....	17



## 第 1 章

# 反病毒



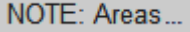
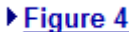
爱思华宝反病毒引擎将对 SMTP 传输中的进站和出站邮件进行病毒扫描。

版本 10.1.2 及以前版本使用履获殊荣的 Avast 引擎。

对于更高版本，将可在 Avast 或 Kaspersky 反病毒引擎中选择使用 - 取决于所购买的 License 类型。

当发现邮件中的病毒时将执行处理动作。

### Legend

图标	描述
	警告 - 非常重要!
	便笺或提示 - 好的建议。
	表内注意。
	图表链接 - 点击连接显示图例，再次点击将其关闭。(只工作在 CHM 格式。)

### 本章内容

反病毒 .....	2
向导 .....	3
EICAR 测试.....	16
Access Mode – Policies .....	17

## 反病毒

### 最新的 Avast! 引擎

内部反病毒升级到最新版本。

### 支持卡巴斯基反病毒

VAVCOM 支持替代 DKAV 库(外部卡巴斯基反病毒)。

### 支持 LB 环境

支持负载均衡环境增加，新的 API 变量能得到每次的更新触发，发行时自动更新并自动加载。

# 想到

## 常规



注意：该服务的访问模式可以从域和用户级别进行设置，请查看相应位置 ([域] -- 策略, [用户] --策略)。

**更新**

日
  一
  二
  三
  四
  五
  六

仅一次在:

每隔 (小时):

禁止更新

**立即更新**

字段	描述
日 - 六	选中这些复选框，以指定系统在哪天检查防病毒更新。
仅一次在:	选中此选项，并指定在选定工作日执行一次更新检查的时间。
每次 (小时)	选中此选项，并输入执行更新检查的时间间隔。



注意 - 必须运行 **Control** 服务才能正常使用防病毒更新。

**信息**

最后更新日期:

最后更新大小:

最后更新版本:

**信息** 部分显示反病毒定义的状态信息。

- 最后更新文件的日期。
- 最后更新文件的大小。
- 当前文件的版本。
- 当前使用的引荐类型

在请求技术支持时，这些信息非常有用。

## 本章内容

Avast 镜像站 URL 设置 .....4

## Avast 镜像站 URL 设置

### 定义一个 Web 站点

- 为镜像站点创建一个主目录，例如 D:\mywebdirs\avastmirror
- 在爱思华宝服务器的 Web 服务节点设置一个新的 Web 站点，指向之前定义的主目录，并指定一个适当的虚拟主机名，例如 "avastmirror.com"。

**Web 站点**

HTTP 信头 | 重寄 | 目录别名

Web 站点 | 选项 | 访问 | 应用映射 | MIME | 文档 | 错误

Web 站点

激活

主机: avastmirror.com

描述:

主目录: html\

IP地址: <所有可用 >

使用默认设置

使用定制设置

W3C 日志

启用 W3C 日志

日志文件路径:

删除过期的日志文件 (天): 0

确定 取消



记得为你的新主机设置一个 DNS 记录。



## 测试 Web 站点

- 在 "D:\mywebdirs\avastmirror" 创建一个文件 test.txt 。
- 使用任意浏览器从 <http://avastmirror.com:32000/test.txt> (必需替换为你的主机名和端口)下载该文件。

如果它工作,则表示已正常工作。

## 设置镜像

- 为 Avast 镜像程序创建一个目录,例如"D:\mirrorbase",并解压镜像内容。  
Mirror.zip 下载站点为 <http://files.avast.com/files/eng/mirror.zip>
- 修改 "D:\mirrorbase\config\"下文件 mirror.ini :
- 改变[server 0\_0]下的两行。  
改变 "url"到网站主机名。本案例为"url= <http://avastmirror.com/>"  
改变 "upload\_dest\_directory"为 Web 站点的主目录,比如"upload\_dest\_directory=d:\mywebdirs\avastmirror"
- 运行第一个镜像更新: "D:\mirrorbase\avastmirror\mirror.exe /oem "IceWarp""  
程序将运行并输出类似以下信息 -

```
C:\Documents and Settings\Merak>"D:\mirrorbase\avastmirror\mirror.exe /oem "IceWarp""
mirror begin...
Mirroring...
Using server: http://www2.avast.com/beta
Downloading file: servers.def.stamp ===== 100%
Using server: http://www2.avast.com/beta
Downloading file: jollyroger.vpu.stamp ===== 100%
Downloading file: mirror.def.stamp ===== 100%
Setting product 'av_oem' files (110 of 1114 set)
Resetting existing files (reset 110 files, leaving 0 files).
Using server: http://www2.avast.com/beta
mirroring 'av_oem' - nothing to do.
Mirroring done.
Building distributions...
```

将弹出你的站点主目录和当前的 Avast 文件。

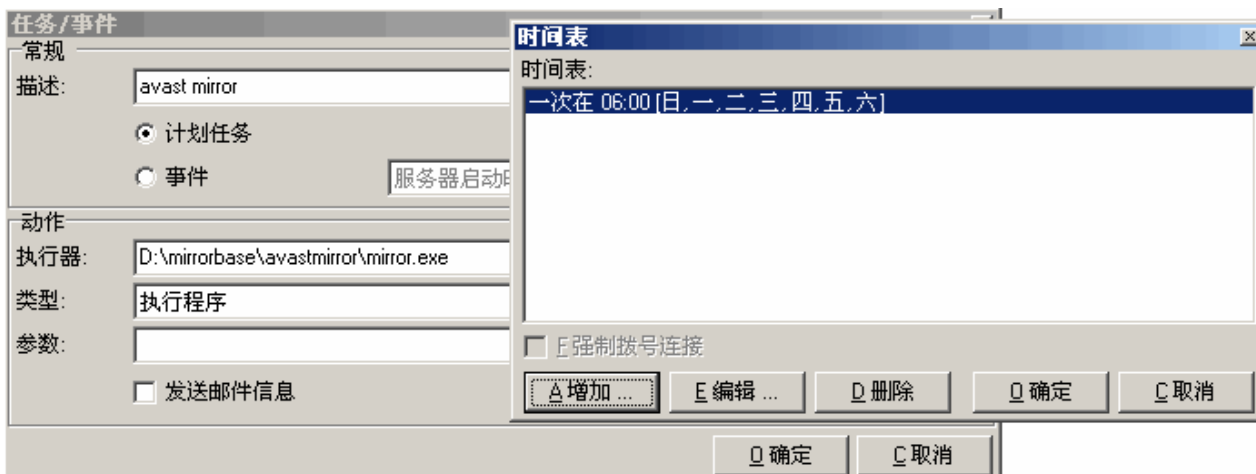
## 测试镜像站点

- 使用任何浏览器从"[http://avastmirror.com:32000/servers\\_mirror.def](http://avastmirror.com:32000/servers_mirror.def)"下载定义文件

如果下载成功,则表示镜像工作正常。

## 安排镜像更新

- 添加一个新任务到爱思华宝服务器控制台/系统/工具/任务和事件,使用如下设置(你可能想改变安排时期)。



- 点击"爱思华宝服务器控制台/系统/工具/任务和事件"下 "立即运行"
- 稍等片刻后检查 `D:\mirrorbase\avastmirror\logs\mirrors.log` 日志文件

如果一切正常，它将显示更新被执行。

## 动作

在 **动作** 选项卡中，您可以指定在发现邮件中包含病毒时，系统采取的操作。

The screenshot shows a configuration window titled '邮件' (Mail). It contains several settings:

- 激活 (Activate)
- 扫描模式: (Scan mode) dropdown menu showing '邮件所有部份和 MIME 信息' (Scan all parts and MIME information)
- 拒绝病毒邮件 (Reject virus mail)
- 删除病毒邮件 (Delete virus mail)
- 移除病毒附件 (Remove virus attachments)
- 应用扩展名过滤器 (Apply extension filters)
- 应用外部过滤器 (Apply external filters)
- 应用反病毒到出站邮件 (Apply anti-virus to outgoing mail)

字段	描述
激活	勾选此项，如果您想启用该功能。
模式	从以下选项中选择中一个： <b>检查邮件所有已提取的附件</b> 只有邮件附件被扫描。 <b>邮件所有部份和 MIME 信息</b> 完整邮件，包含附件等都被扫描。 <b>MIME 信息</b> 只有邮件内容被扫描（不包含附件）。
拒绝病毒邮件	被感染邮件将立即被服务器拒绝。
删除病毒邮件	被感染邮件将被接收但同时被服务器删除。 该选项通常用于当邮件包含病毒时，您仍想进一步对其处理。例如：您可以使用内容过滤器将病毒邮件转发给反病毒团队。.
移除病毒附件	所有含有病毒的附件将从邮件中被移除。 如果一个感染附件不能被除作，邮件将被拒绝。 如果 "描邮件所有部份..." 选项被选择，该功能将不能正常工作。
应用扩展名过滤器	勾选此项,如果您想使用在 <b>扩展名过滤器</b> 选项处定义的扩展名选项卡。
应用外部过滤器	勾选此项，如果您想使用在 <b>外部过滤器</b> 选项卡处定义的外部过滤器。
应用反病毒到出站邮件	勾选此项，如果您也想对出站邮件进行反病毒检查。

FTP

激活

应用扩展名过滤器

应用外部过滤器

字段	描述
激活	勾选此项，如果您希望反病毒引擎检查您的上传文件。
应用扩展名过滤器	勾选此项,如果您想使用在 <b>扩展名过滤器</b> 选项处定义的扩展名选项卡。
应用外部过滤器	勾选此项，如果您想使用在 <b>外部过滤器</b> 选项卡处定义的外部过滤器。

SOCKS /代理

激活

勾选此项，如果您想启用 SOCKS/代理的反病毒检查。

协同工作

激活

应用扩展名过滤器

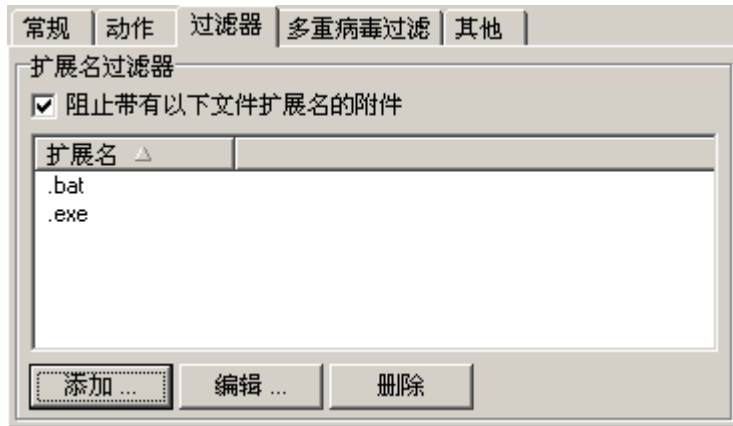
应用外部过滤器

字段	描述
启用	勾选此项，如果您希望协同工作项目被反病毒引擎检查。
应用扩展名过滤器	勾选此项,如果您想使用在 <b>扩展名过滤器</b> 选项处定义的扩展名选项卡。
应用外部过滤器	勾选此项，如果您想使用在 <b>外部过滤器</b> 选项卡处定义的外部过滤器。

## 扩展名过滤器

**过滤器** 选项卡允许您定义将被视为病毒的文件扩展名的列表。

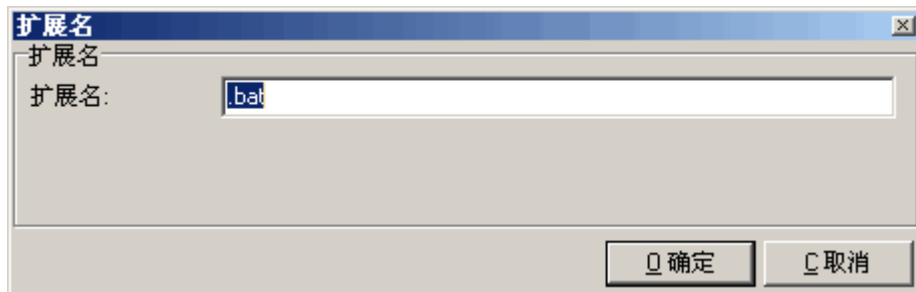
如果爱思华宝服务器发现随附的文件带有列出的扩展名，则信息将被视为包含病毒，并进行相关处理。



选中阻止带有以下扩展名的附件复选框，让爱思华宝服务器根据扩展名列表处理附件。

使用删除按钮删除选定的扩展名。

使用增加或编辑按钮将新的扩展名添加到列表或编辑选定的扩展名。随即打开扩展名对话框：



输入要将其视为病毒的扩展名，然后按下确定将该扩展名保存到列表。



注意：必须在扩展名前加上一个圆点 (.)。

此外，请注意不应当阻止 .TMP 扩展名，因为这会导致爱思华宝服务器将所有信息均视为包含病毒。

## 外部病毒过滤

外部病毒过滤 选项可以配置爱思华宝服务器使用支持命令行扫描方式的第三方反病毒软件。



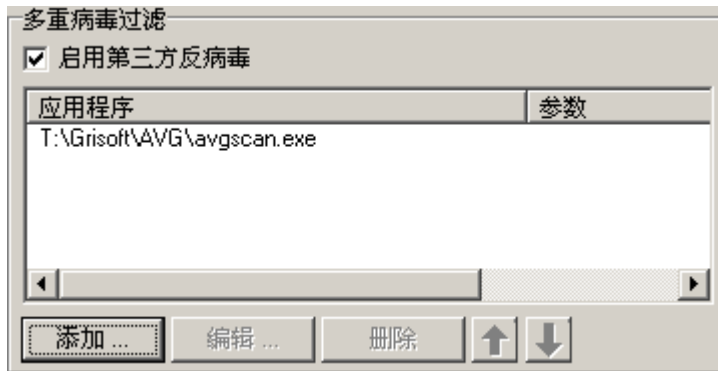
注意 - 此功能是为了向后兼容，我们强烈建议您使用爱思华宝服务器提供的防病毒引擎。本节展示了一个使用命令行扫描的 **AVGscan** 程序的例子。

爱思华宝服务器允许两种典型的外部防病毒方法 -

- 可执行应用程序
- 库，有关使用库的更多信息，请参阅标准安装的爱思华宝服务器随附的示例文件 */examples/libraryexternalav.txt.html*。



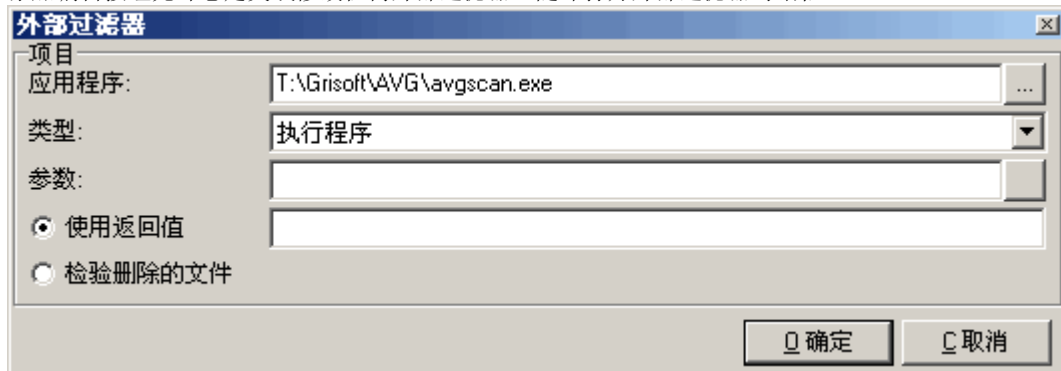
请注意，如果选择使用任何外部实时病毒扫描程序，您应当排除扫描 `<icewarpdirectory>\Temp` 文件夹，因为扫描该文件夹可能导致服务器速度大大降低和爱思华宝服务器本身出现问题。



选中启用第三方防病毒软件勾选框以启用此功能。

删除按钮将删除任何选定过滤器。

添加编辑按钮允许您定义或修改任何外部过滤器。随即打开外部过滤器对话框：



字段	描述
应用程序	<p>指定外部过滤器的完全限定路径。</p> <p>使用...按钮打开标准文件浏览器对话框。</p>
类型	<p>选择要调用的模块类型：</p> <p><b>执行程序</b></p> <p>为标准可执行模块选择此项。</p> <p><b>StdCall Library, Cdecl Library</b></p> <p>选择此项以调用库中的过滤器。</p> <p>请参阅标准安装的爱思华宝服务器随附的示例文件 <i>/examples/libraryexternalav.txt.html</i>。</p>
参数	<p>你应当在此处指定外部过滤器所需的任何参数。</p> <p>有关详细信息，请参阅过滤器文档。</p>
使用返回值	<p>在此处输入外部过滤器发现病毒时返回的值。</p> <p>有关详细信息，请参阅过滤器文档。</p> <p>应当使用逗号来分隔多个值。</p> <p>例如，如果过滤器在发现病毒时返回的值为 1 至 5，则您应当在此处指定 1、2、3、4 和 5。</p> <p>例如, avgscan 将返回以下代码：</p> <p>0 - 一切 OK</p> <p>1 - 用户取消/中断测试</p> <p>2 - 测试期间的任何问题 - 不能打开文件等。</p> <p>3 - 更改识别</p> <p>4 - 通过启发式分析测试疑是</p> <p>5 - 启发式分析发现病毒</p> <p>6 - 指定病毒检测</p> <p>7 - 激活内存中病毒检测</p> <p>8 - AVG 损坏</p> <p>9 - Double extension</p> <p>10 - Archive contains password protected files</p> <p>Codes 4, 5, and 6 indicate a virus (7 is discounted as this virus would not be within a message!)</p> <p>So we would enter 4,5,6 in this field.</p>
检验删除的文件	<p>某些过滤器不需要返回值，而只是删除文件。</p> <p>如果过滤器采用此方式，则应当选中此选项。</p>

	<p>在过滤器运行后，爱思华宝服务器将检查文件是否已被删除，如果已删除，则系统将该信息视为包含病毒。</p>
--	--



## 高级

## 高级

 拒绝密码保护的文件

线程池:

8

反病毒处理的最大邮件容量:

5

MB

设定例外文件 (不扫描):

编辑 ...

字段	描述
拒绝密码保护的文件	<p>防病毒引擎必须解压缩附件，以检查是否包含病毒。</p> <p>如果附件具有密码保护，则爱思华宝服务器无法检查文件内容。</p> <p>默认情况下，信息将转发给接收者。</p> <p>此方案可能会被用来使您的系统感染病毒。</p> <p>选中此选项以将任何包含密码保护文件的信息视为包含病毒。</p> <p><b>注意：</b>本选项仅适用于类似于 ZIP 和 RAR 的压缩文件，不适用于被密码保护的 Word 或 Excel 文档。</p> <p><b>注意：</b>本功能同样能用于过滤器，从而给您更多的动作进行控制。</p>
线程池	<p>爱思华宝反病毒引擎是多线程，这在一些较慢的服务器上可能因为占用资源太多而导致一些问题，比如 CPU 100% 。</p> <p>输入一个非零值，这将对爱思华宝反病毒引擎同时运行的进程数进行限制。</p> <p>对发出的邮件应用病毒</p>
反病毒处理的最大邮件容量	<p>输入一个非零值，爱思华宝反病毒的处理将忽略超过这个大小的邮件。</p> <p><b>注意：</b>如果你没有邮件大小的通用限制，这可能导致一些包含病毒的较大邮件将被忽略处理。</p>
设定例外文件（不扫描）	<p>点击 编辑 按钮编辑一个爱思华宝服务器反病毒引擎的忽略文件。这是一个标准的爱思华宝忽略文件，示例文件您可以在编辑器中看到。</p> <p>在文件中指定的邮件发件人地址，域，以及 IP 范围都将不被反垃圾引擎处理。</p>

## 流设置 (SOCKS, 代理)

忽略的扩展名类型:

.gif;.jpg;.png;.exe

使用大文件模式时内存中保存的数据大小:

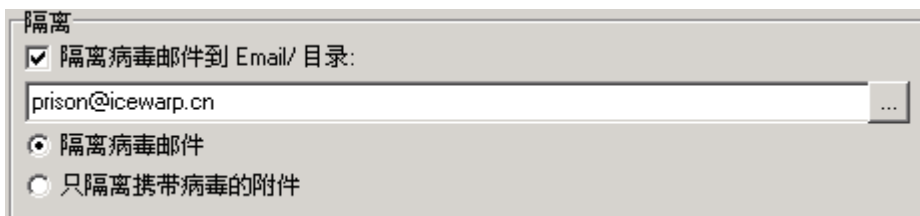
8

kB

大文件模式时发送数据大小的百分比(%):

50

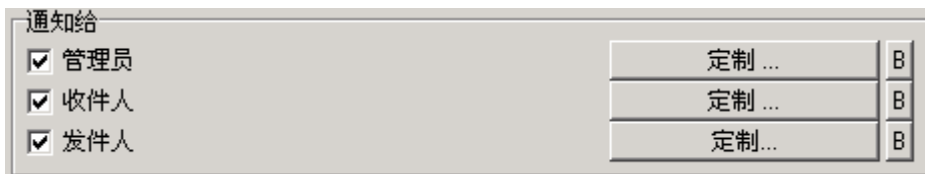
字段	描述
忽略的扩展名类型	此处您可以定义被反病毒引擎忽略的文件（扩展名）类型。 扩展名间请用分号隔开，定义扩展名时请加句号（如 .jpg）。
使用大文件模式时内存中保存的数据大小	检查文件的方式有两种： <ul style="list-style-type: none"> <li>被检查的文件放在内存中，这对于小文件将更快。</li> <li>被检查的文件保存在磁盘中，此处用于定义大文件的大小阈值，太大的文件将造成大量内存被占用。</li> </ul> 在此处定义一个大文件的限制。
大文件模式时发送数据大小的百分比 (%)	定义每次被检查的文件大小百分比。 例如：您定义了 50%，一个大文件的 50% 将首先被检查，然后剩余的 50% 也将被发送检查。



字段	描述
隔离感染邮件到 email/目录	勾选此项建立一个感染邮件的归档。 指定一个用于保存归档的完整目录名称，或在需转发时指定一个邮件地址。
隔离感染邮件	整个邮件将被隔离。
只隔离被感染的附件	只有被感染的附件才被隔离。



注意：这与反垃圾引擎中的隔离区完全不同！



字段	描述
管理员/收件人/发件人	您可以选择发送一封通知邮件到域管理员、其他收件人或发件人，请单击相应的选项。

---

定制	您可以在邮件内部使用爱思华宝服务器的系统变量自定义通知邮件的内容。按下收件人旁边的 定制 按钮打开邮件编辑对话框。
"B" 按钮	您同样也能为每个收件人定义一个忽略文件，按下收件人旁边的 <b>B</b> 按钮，您可以定制任何的忽略规则，您可以参考编辑框内的示例(文本 按钮)。

## EICAR 测试

你能测试你的反病毒设置，通过按发送 EICAR 病毒测试邮件按钮。

发送 EICAR 病毒测试邮件

EICAR (欧洲计算机反病毒研究协会)是一个由反病毒行业的独立专家组成的协会。

显然，你不会因为测试目的而发送一个真正的病毒，因此 EICAR 提供一个可以被安全发送的文件，它不是病毒但将触发你的防病毒软件，就像它是一个病毒。

如果你的反病毒设置是正确的，在你按下发送 EICAR 测试邮件按钮后，你将获得一个如下的警告信息。



如果警告没有出现，则表示你的设置还有些问题，你需要进行更多的检查。

注意：如果你要使用远程控制台，发送一封测试邮件可能会有不同的结果（比如警告），因为你现在连接到爱思华宝服务器的 IP 没有验证。



你可能得到如下几个错误：

- Access not allowed (due to the **Reject if sender local and not authenticated** option)
- Greylisting
- DNSBL.

---

## 访问模式 -- 策略

相应服务的访问模式可以在域和用户级设置：

- 通过域的 [域] - 策略 选项卡（域及帐户 -- 管理）。
- 通过用户的 [用户] - 策略 选项卡（域及帐户 -- 管理 - [域]）。