思科邮件安全设备 AsyncOS 9.7 CLI 参考指南

2015 年 10 月 13 日

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices

思科邮件安全设备 AsyncOS 9.7 CLI 参考指南

目 录

前言

本书的说明面向具有网络和邮件管理知识的经验丰富的系统管理员。

读前须知

注 如果您已将设备用电缆连接到您的网络，请确保该设备的默认 IP 地址与您网络中的其他 IP 地址未发生冲突。出厂时分配给 Management 端口的 IP 地址是 `192.168.42.42`。有关为设备分配 IP 地址的详细信息，请参阅 《用户指南》中的 “设置和安装”一章以了解您所用的版本。

排版规则

字样或符号	含义	示例
AaBbCc123	命令、文件和目录名称；屏幕显示的计算机输出。	`Please choose an IP interface for this Listener.` `sethostname` 命令用于设置设备的名称。
AaBbCc123	您键入的内容，与屏幕显示的计算机输出形成鲜明对比。	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**
AaBbCc123	书名、新词语或术语，要强调的词语。命令行变量；使用实名或值替换。	阅读 《*快速入门指南*》。 设备*必须*能够唯一地选择接口，以发送一个传出数据包。 `Before you begin, please reset your password to a new value.` `Old password:` **`ironport`** `New password:` *`your_new_password`* `Retype new password:` *`your_new_password`*

其他资源

文档

可从以下网址获得邮件安全设备的说明文档：

http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html

解决方案信息

要访问知识库以了解有关思科内容安全产品的信息，请访问：

http://www.cisco.com/web/ironport/knowledgebase.html

注 您需要 Cisco.com 用户 ID 才能访问网站。如果您没有 Cisco.com 用户 ID，请参阅注册思科帐户，第 3 页。

思科支持社区

思科支持社区是一个面向 Cisco 客户、合作伙伴和员工的在线论坛。它提供了一个场所，供相关人员讨论常规内容安全问题以及有关具体思科产品的技术信息。您可以在论坛中发布主题，以咨询问题并与其他用户分享信息。

请通过以下地址访问邮件安全设备的思科支持社区：

https://supportforums.cisco.com/community/netpro/security/email

客户支持

可通过以下方法获得支持：

美国：致电 1 (408) 526-7209 或免付费电话 1 (800) 553-2447

全球：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

支持网站：http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

如果您是通过经销商或另一个供应商购买了支持，请直接联系该供应商咨询您的产品支持问题：

注册思科帐户

Cisco.com 上的许多资源需要思科帐户才可访问。

如果您没有 Cisco.com 用户 ID，可以登录以下网址注册一个：
https://tools.cisco.com/RPF/register/register.do

思科欢迎您提出意见

技术出版物团队致力于提高产品文档的质量。我们时刻欢迎您的意见和建议。您可以将意见发送至以下电邮地址：

contentsecuritydocs@cisco.com

请在邮件的主题行中加入本书的书名和书名页中的出版日期。

CLI 快速参考指南

使用表可以找到相应的 CLI 命令、简要说明及其在 C、 X 和 M 系列平台上的可用性。

CLI 命令 （不需要提交）

CLI 命令	说明	平台可用性
antispamstatus	显示反垃圾邮件状态	C 系列和 X 系列
antispamupdate	手动更新垃圾邮件定义	C 系列和 X 系列
antivirusstatus	显示防病毒状态	C 系列和 X 系列
antivirusupdate	手动更新病毒定义	C 系列和 X 系列
archivemessage	存档您的队列中的旧邮件	C 系列和 X 系列
bouncerecipients	从队列中退回邮件	C 系列、 X 系列和 M 系列
clearchanges 或 clear	清除更改	C 系列、 X 系列和 M 系列
commit	提交更改	C 系列、 X 系列和 M 系列
commitdetail	显示有关上次提交的详细信息	C 系列和 X 系列
contentscannerstatus	显示内容扫描工具版本信息	C 系列和 X 系列
contentscannerudpate	请求手动更新内容扫描引擎	C 系列和 X 系列
日期	显示当前日期和时间	C 系列、 X 系列和 M 系列
deleterecipients	从队列中删除邮件	C 系列、 X 系列和 M 系列
delivernow	重新安排立即传送的邮件	C 系列、 X 系列和 M 系列
诊断	检查 RAID 磁盘、网络缓存和 SMTP 连接。清除网络缓存	C 系列、 X 系列和 M 系列
dig	在 DNS 服务器上查找记录	C 系列和 X 系列
displayalerts	显示设备最近发送的 n 条警告	C 系列、 X 系列和 M 系列
dlprollback	回滚 RSA DLP 引擎	C 系列和 X 系列
dlpstatus	RSA DLP 引擎的版本信息	C 系列和 X 系列
dlpupdate	更新 RSA DLP 引擎	C 系列和 X 系列
dnsflush	清除 DNS 缓存中的所有条目	C 系列、 X 系列和 M 系列
dnslisttest	测试对基于 DNS 的列表服务的 DNS 查找	C 系列和 X 系列
dnsstatus	显示 DNS 统计信息	C 系列、 X 系列和 M 系列
ecstatus	检查用于获取证书的注册客户端的版本	C 系列
ecupdate	更新用于获取证书的注册客户端	C 系列
emdiagnostic	ESA 上的 RSA EM 诊断工具	C 系列、 X 系列和 M 系列
encryptionstatus	显示 PXE 引擎和域映射文件的版本	C 系列和 X 系列
encryptionupdate	请求更新 PXE 引擎	C 系列和 X 系列
featurekey	管理系统功能密钥	C 系列、 X 系列和 M 系列
findevent	在邮件日志文件中查找事件	C 系列、 X 系列和 M 系列
graymailstatus	显示现有灰色邮件规则的详细信息	C 系列和 X 系列
graymailupdate	手动更新灰色邮件规则	C 系列和 X 系列
grep	在日志文件中搜索文本	C 系列、 X 系列和 M 系列
healthcheck	检查您的邮件安全设备的运行状况	C 系列和 X 系列
help 或 h 或 ?	帮助	C 系列、 X 系列和 M 系列

hostrate	监控特定主机的活动	C 系列、X 系列和 M 系列
hoststatus	获取给定主机名的状态	C 系列、X 系列和 M 系列
last	显示最近登录到系统中的人员	C 系列、X 系列和 M 系列
ldapflush	刷新任何缓存的 LDAP 结果	C 系列和 X 系列
ldaptest	执行单个 LDAP 查询测试	C 系列和 X 系列
loadlicense	加载虚拟设备许可证	所有虚拟设备
mailconfig	通过邮件将当前配置发送到邮件地址	C 系列、X 系列和 M 系列
nslookup	查询名称服务器	C 系列、X 系列和 M 系列
netstat	显示网络连接、路由表和网络接口统计信息	C 系列、X 系列和 M 系列
outbreakflush	清除缓存的病毒爆发规则	C 系列和 X 系列
outbreakstatus	显示当前病毒爆发规则	C 系列和 X 系列
outbreakupdate	更新病毒爆发过滤器规则	C 系列和 X 系列
oldmessage	在队列中显示旧邮件列表	C 系列和 X 系列
packetcapture	拦截并显示通过网络传输或接收的数据包	C 系列、X 系列和 M 系列
password or passwd	更改您的密码	C 系列、X 系列和 M 系列
ping	对网络主机执行 ping 操作	C 系列、X 系列和 M 系列
ping6	对采用 IPv6 的网络主机执行 ping 操作	C 系列、X 系列和 M 系列
quit 或 q 或 exit	退出	C 系列、X 系列和 M 系列
rate	监控邮件吞吐量	C 系列、X 系列和 M 系列
reboot	重新启动系统	C 系列、X 系列和 M 系列
redirectrecipients	将所有邮件重定向到另一个转发主机	C 系列和 X 系列
removemessage	从队列中删除旧的未传输的邮件	C 系列和 X 系列
repengstatus	请求信誉引擎的版本信息	C 系列、X 系列和 M 系列
resetconfig	恢复出厂默认配置	C 系列、X 系列和 M 系列
resetcounters	重置系统中的所有计数器	C 系列、X 系列和 M 系列
恢复	恢复接收和传送	C 系列、X 系列和 M 系列
resumedel	恢复传送	C 系列、X 系列和 M 系列
resumelistener	恢复接收	C 系列、X 系列和 M 系列
revert	恢复到以前版本	C 系列、X 系列和 M 系列
rollovernow	滚动更新日志文件	C 系列、X 系列和 M 系列
saveconfig	将配置保存到磁盘	C 系列、X 系列和 M 系列
sbstatus	显示 SenderBase 查询的状态	C 系列和 X 系列
settime	手动设置系统时钟	C 系列、X 系列和 M 系列
showmessage	显示队列中旧的未传输的邮件	C 系列和 X 系列
showconfig	显示所有配置值	C 系列、X 系列和 M 系列
showlicense	显示虚拟设备许可证信息	所有虚拟设备
showrecipients	按收件人主机、邮件发件人地址显示队列中的邮件，或者显示所有邮件	C 系列和 X 系列
shutdown	关闭要关闭电源的系统	C 系列、X 系列和 M 系列

slblconfig	配置安全列表/阻止列表设置	C 系列和 X 系列
状态	系统状态	C 系列、 X 系列和 M 系列
supportrequest	将邮件发送到思科 TAC	C 系列、 X 系列和 M 系列
supportrequeststatus	显示支持请求关键字版本信息	C 系列、 X 系列和 M 系列
supportrequestupdate	请求手动更新支持请求关键字	C 系列、 X 系列和 M 系列
suspend	暂停接收和传送	C 系列、 X 系列和 M 系列
suspenddel	暂停传送	C 系列、 X 系列和 M 系列
suspendlistener	暂停接收	C 系列、 X 系列和 M 系列
systemsetup	首次系统设置	C 系列和 X 系列
tail	连续显示日志文件的结尾	C 系列、 X 系列和 M 系列
techsupport	允许思科 TAC 访问您的系统	C 系列、 X 系列和 M 系列
telnet	连接到远程主机	C 系列、 X 系列和 M 系列
tlsverify	建立到远程主机的出站 TLS 连接并调试任何 TLS 连接问题	C 系列和 X 系列
tophosts	按队列大小显示排名前列的主机	C 系列、 X 系列和 M 系列
topin	按传入连接数显示排名前列的主机	C 系列、 X 系列和 M 系列
跟踪	通过系统跟踪邮件流	C 系列、 X 系列和 M 系列
traceroute	显示到远程主机的网络路由	C 系列、 X 系列和 M 系列
traceroute6	显示到采用 IPV6 的远程主机的网络路由	C 系列、 X 系列和 M 系列
tzupdate	更新时区规则	C 系列、 X 系列和 M 系列
updatenow	更新所有组件	C 系列、 X 系列和 M 系列
upgrade	安装升级	C 系列、 X 系列和 M 系列
version	查看系统版本信息	C 系列、 X 系列和 M 系列
wipedata	擦除磁盘上的核心文件并检查最近一次核心转储操作的状态	C 系列、 X 系列和 M 系列
webcacheflush	通过 URL 过滤功能刷新已用的缓存	C 系列、 X 系列和 M 系列
websecuritydiagnostics	查看 URL 过滤的诊断统计信息	C 系列、 X 系列和 M 系列
who	列出已登录的人员	C 系列、 X 系列和 M 系列
whoami	显示当前用户 ID	C 系列、 X 系列和 M 系列
workqueue	显示和/或修改工作队列暂停状态	C 系列和 X 系列

CLI 命令 （需要提交）

CLI 命令	说明	平台可用性
addressconfig	配置系统生成的邮件的发件人地址	C 系列、 X 系列和 M 系列
addresslistconfig	配置地址列表	C 系列和 X 系列
adminaccessconfig	配置网络访问列表和横幅登录	C 系列和 X 系列
aggregatorconfig	配置思科汇聚器服务器的地址	C 系列和 X 系列
alertconfig	配置邮件警报	C 系列、 X 系列和 M 系列
aliasconfig	配置邮件别名	C 系列和 X 系列
altsrchost	配置虚拟网关™ 映射	C 系列和 X 系列
ampconfig	配置高级恶意软件保护 （文件信誉和分析）	C 系列、 X 系列和 M 系列
antispamconfig	配置反垃圾邮件策略	C 系列和 X 系列
antivirusconfig	配置防病毒策略	C 系列和 X 系列
bounceconfig	配置退回行为	C 系列、 X 系列和 M 系列
bvconfig	配置外发邮件的主要设置，并配置如何处理无效退回	C 系列和 X 系列
callaheadconfig	添加、编辑和删除 SMTP Call-Ahead 配置文件	C 系列、 X 系列和 M 系列
certconfig	配置安全证书和密钥	C 系列、 X 系列和 M 系列
clusterconfig	配置与集群相关的设置	C 系列和 X 系列
deliveryconfig	配置邮件传送	C 系列和 X 系列
destconfig	配置目标控制表的选项	C 系列和 X 系列
dictionaryconfig	配置内容词典	C 系列、 X 系列和 M 系列
diskquotaconfig	配置磁盘空间	C 系列、 X 系列和 M 系列
dmarcconfig	配置 DMARC 设置	C 系列和 X 系列
dnsconfig	配置 DNS 设置	C 系列和 X 系列
dnshostprefs	配置 IPv4/IPv6 DNS 首选项	C 系列、 X 系列和 M 系列
dnslistconfig	配置 DNS 列表服务支持	C 系列和 X 系列
domainkeysconfig	配置 DomainKeys 支持	C 系列和 X 系列
ecconfig	配置用于获取证书的注册客户端	C 系列、 X 系列和 M 系列
emconfig	配置 RSA Enterprise Manager 互操作性设置	C 系列和 X 系列
encryptionconfig	配置邮件加密	C 系列和 X 系列
etherconfig	配置以太网设置	C 系列、 X 系列和 M 系列
exceptionconfig	配置域异常表	C 系列和 X 系列
featurekeyconfig	自动检查和更新功能密钥	C 系列、 X 系列和 M 系列
filters	配置邮件处理选项	C 系列和 X 系列
generalconfig	配置浏览器设置和其他常规设置	C 系列、 X 系列和 M 系列
graymailconfig	配置灰色邮件检测和安全取消订阅全局设置	C 系列和 X 系列
healthconfig	配置设备的各个运行状况参数的阈值	C 系列、 X 系列和 M 系列
imageanalysisconfig	配置 IronPort 图像分析设置	C 系列、 X 系列和 M 系列

incomingrelayconfig	配置传入转发	C 系列和 X 系列
interfaceconfig	配置以太网 IP 地址	C 系列、 X 系列和 M 系列
ldapconfig	配置 LDAP 服务器	C 系列和 X 系列
listenerconfig	配置邮件侦听器	C 系列和 X 系列
loadconfig	加载配置文件	C 系列、 X 系列和 M 系列
localeconfig	配置多语言设置	C 系列和 X 系列
logconfig	配置对日志文件的访问	C 系列、 X 系列和 M 系列
ntpconfig	配置 NTP 时间服务器	C 系列、 X 系列和 M 系列
outbreakconfig	配置病毒爆发过滤器	C 系列和 X 系列
policyconfig	配置基于收件人或发件人的策略	C 系列和 X 系列
quarantineconfig	配置系统隔离区	C 系列和 X 系列
reportingconfig	配置报告设置	C 系列、 X 系列和 M 系列
rollbackconfig	回滚到以前提交的配置之一	C 系列、 X 系列和 M 系列
routeconfig	配置 IP 路由表	C 系列、 X 系列和 M 系列
scanconfig	配置附件扫描策略	C 系列和 X 系列
senderbaseconfig	配置 SenderBase 连接设置	C 系列和 X 系列
setgateway	设置默认网关 （路由器）	C 系列、 X 系列和 M 系列
sethostname	设置机器的名称	C 系列、 X 系列和 M 系列
settz	设置本地时区	C 系列、 X 系列和 M 系列
sievechar	按照 RFC 3598 的说明配置 Sieve 邮件过滤的特征	C 系列和 X 系列
smimeconfig	配置 S/MIME 功能	C 系列、 X 系列和 M 系列
smtpauthconfig	配置 SMTP 自动配置文件	C 系列和 X 系列
smtproutes	设置永久域重定向	C 系列、 X 系列和 M 系列
snmpconfig	配置 SNMP	C 系列、 X 系列和 M 系列
sshconfig	配置 SSH 密钥	C 系列、 X 系列和 M 系列
sslconfig	配置 SSL 设置	C 系列、 X 系列和 M 系列
sslv3config	启用/禁用 SSLv3	C 系列、 X 系列和 M 系列
stripheaders	设置要删除的邮件报头	C 系列和 X 系列
tcpservices	显示有关流程打开的文件的信息	C 系列、 X 系列和 M 系列
textconfig	配置文本资源	C 系列和 X 系列
trackingconfig	配置跟踪系统	C 系列、 X 系列和 M 系列
unsubscribe	更新全局取消订阅列表	C 系列、 X 系列和 M 系列
updateconfig	配置系统更新参数	C 系列和 X 系列
LDAP	配置系统升级参数 （弃用的命令）	
urllistconfig	配置安全 URL 白名单	C 系列、 X 系列和 M 系列
userconfig	管理用户帐户以及至外部身份验证源的连接	C 系列、 X 系列和 M 系列
websecurityadvancedconfig	配置 URL 过滤的高级设置	C 系列、 X 系列和 M 系列
websecurityconfig	配置 URL 过滤的全局设置	C 系列、 X 系列和 M 系列

命令行界面：基础知识

本章包含以下各部分：

访问命令行界面 (CLI)

命令行界面可通过 IP 接口上的 SSH 或 Telnet 访问，这两个协议已在启用这些服务的情况下进行了配置，或者通过串行端口上的终端仿真软件进行了配置。按出厂默认设置， SSH 和 Telnet 均在管理 (Management) 端口上进行配置。使用 `interfaceconfig` 命令可以禁用这些服务。

访问 CLI 的方式因设置设备时选择的管理连接方式而异。下文列出了出厂默认用户名和密码。最初，只有管理员用户帐户具有访问 CLI 的权限。在您通过管理员帐户第一次访问命令行界面后，您可以添加其他具有不同级别权限的用户。系统设置向导会要求您更改管理员帐户的密码。还可以随时使用 `password` 命令直接重置管理员帐户的密码。

通过以太网连接：使用出厂默认 IP 地址 192.168.42.42 启动 SSH 或 Telnet 会话。SSH 配置为使用端口 22。 Telnet 配置为使用端口 23。输入下面的用户名和密码。

通过串行连接进行连接的步骤：在串行电缆所连接的个人计算机上启动与通信端口的终端会话。请参阅 “设置和安装”一章了解详细信息。输入下面的用户名和密码。

通过输入下面的用户名和密码登录设备。

出厂默认用户名和密码

- 用户名：**admin**
- 密码：**ironport**

例如：

```
login: admin

password: ironport
```

命令行界面约定

本部分介绍 AsyncOS CLI 的规则和约定。

命令提示符

顶层命令提示符包括完全限定的主机名，后面依次跟着大于号 (>) 和空格。例如：

```
mail3.example.com>
```

如果设备配置为具有集中管理功能的集群的成员，则 CLI 中的提示符会更改，以指示当前模式。例如：

```
(Cluster Americas) >
```

或

```
(Machine los_angeles.example.com) >
```

有关详细信息，请参阅 《用户指南》中的 “集中管理”。

运行命令时， CLI 要求您输入信息。当 CLI 要求您输入信息时，命令提示符将显示默认输入，用方括号 ([]) 括起来，后面紧跟大于号 (>)。当没有默认输入时，命令提示符括号内为空。

例如：

```
Please create a fully-qualified hostname for this Gateway
(Ex: "mail3.example.com"):
[]> mail3.example.com
```

当有默认设置时，该设置会显示在命令提示符的方括号内。例如：

```
Ethernet interface:
1.Data 1
2.Data 2
3.Management
[1]> 1
```

显示默认设置时，键入 “Return”等同于键入默认设置：

```
Ethernet interface:
1.Data 1
2.Data 2
3.Management
[1]> (type Return)
```

命令语法

在交互模式下运行时， CLI 命令语法由单个命令组成，无空格，无参数。例如：

```
mail3.example.com> systemsetup
```

选择列表

当系统显示多种输入选择时，有些命令使用带编号的列表。在提示符中输入选择的编号。

例如：

```
Log level:
1.Error
2.Warning
3.Information
4.Debug
5.Trace
[3]> 3
```

是/否查询

当系统给出 yes 或 no 选项时，会提出一个问题，默认设置用括号括起来。您可以回答 **Y**、**N**、**Yes** 或 **No**。大小写不重要。

例如：

```
Do you want to enable FTP on this interface?[Y]> n
```

子命令

有些命令会为您提供使用子命令的机会。子命令包括指令，例如 NEW、EDIT 和 DELETE。对于 EDIT 和 DELETE 函数，这些命令提供先前在系统中配置的记录的列表。

例如：

```
mail3.example.com> interfaceconfig


Currently configured interfaces:
1.Management (192.168.42.42/24: mail3.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>
```

在子命令中，在空白提示符中键入 Enter 或 Return，会让您返回主命令。

退出

在子命令中，您随时可以使用 Control-C 键盘快捷键立即退出，返回到 CLI 的顶层。

历史记录

CLI 保留您在会话期间键入的所有命令的历史记录。使用键盘上的 Up 和 Down 箭头键，或者 Control-P 和 Control-N 组合键，滚动浏览近期使用的命令的列表。

```
mail3.example.com> (type the Up arrow key)


mail3.example.com> interfaceconfig (type the Up arrow key)


mail3.example.com> topin (type the Down arrow key)
```

命令补全

命令行界面支持命令补全。您可以键入某些命令的头几个字母，然后按 Tab 键， CLI 将补全唯一命令的字符串。如果您输入的字母在命令中不是唯一的， CLI 将 “缩小”此字母集。例如：

```
mail3.example.com> set (type the Tab key)
setgateway, sethostname, settime, settz
mail3.example.com> seth (typing the Tab again completes the entry with
sethostname)
```

对于 CLI 的历史记录和文件补全功能，您必须键入 Enter 或 Return 以调用命令。

配置更改

您可以在邮件操作正常进行的同时，对配置进行更改。

在您完成以下步骤前，配置更改不会生效：

步骤 1　在命令提示符中发出 `commit` 命令。

步骤 2　为 `commit` 命令提供所需的输入。

步骤 3　在 CLI 收到 `commit` 程序确认。

系统将记录尚未提交的配置更改，但这些更改在运行 `commit` 命令后才生效。

注　并非所有的命令均需要运行 `commit` 命令。请参阅第 1 章 “CLI 快速参考指南”，了解必须运行 commit 命令才能使更改生效的命令的汇总信息。

退出 CLI 会话、系统关机、重新启动、故障或发出 `clear` 命令都会清除尚未提交的更改。

通用 CLI 命令

本部分介绍用于提交或清除更改、获取帮助和退出命令行界面的命令。

提交配置更改

commit 命令对于将配置更改保存到设备至关重要。许多配置更改在您输入 commit 命令后才生效。（有些命令不要求您使用 commit 命令，即可让更改生效。commit 命令会应用自上次发出 commit 命令或上次发出 clear 命令后所做的配置更改。评论最多包含 255 个字符。直到您收到确认和时间戳后，更改才验证为已提交。

您可以选择在 commit 命令后输入评论。

```
mail3.example.com> commit


Please enter some comments describing your changes:

[]> Changed "psinet" IP Interface to a different IP address

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

注　为成功提交更改，您必须位于顶层命令提示符中。在空白提示符中键入 Return，在命令行层次结构中向上移动一层。

清除配置更改

clear 命令会清除自上次发出 commit 或 clear 命令后所做的所有配置更改。

```
mail3.example.com> clear

Are you sure you want to clear all changes since the last commit?[Y]> y

Changes cleared: Mon Jan 01 12:00:01 2003
mail3.example.com>
```

退出命令行界面会话

quit 命令可以让您从 CLI 应用注销。系统会清除尚未提交的配置更改。quit 命令不会影响邮件操作。系统将注销记录在日志文件中。（键入 exit 等同于键入 quit。）

```
mail3.example.com> quit

Configuration changes entered but not committed.Exiting will lose
changes.
Type 'commit' at the command prompt to commit changes.
Are you sure you wish to exit?[N]> Y
```

寻求有关命令行界面的帮助

help 命令会列出所有可用的 CLI 命令，并为每个命令提供简短说明。要调用 help 命令，可以在命令提示符中键入 help 或一个问号 (?)。

```
mail3.example.com> help
```

批处理命令

AsyncOS 提供了对批处理命令格式的支持，允许您使用一个新的单行 CLI 格式执行某些 CLI 命令。此格式可以减少完成任务所需的输入量，并提供一个允许您轻松地自动执行常见配置任务的机制。批处理命令还允许您使用 SSH 客户端远程发出命令。这使您可以轻松地编写 CLI 命令脚本，并同时在多个设备上执行这些命令。

并非所有命令都能进行批处理，但是所有批处理命令均可以作为非批处理命令执行。

批处理命令语法取决于所使用的具体命令。请参阅第 3 章 “命令：参考示例”中相应的 CLI 示例，了解关于特定于该命令的语法的详细信息。

批处理命令示例

在下面的示例中，会创建发件人组 REDLIST。然后将其与 THROTTLED 策略进行关联，最后将发件人 ‘possible_spammer.com’添加到发件人组。

使用 CLI 执行此操作：

```
example.com> listenerconfig



Currently configured listeners:

1.IncomingMail (on Management, 192.168.42.42/24) SMTP TCP Port 25 Public

2.OutgoingMail (on Data 2, 192.168.40.42/24) SMTP TCP Port 25 Private



Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.

[]> IncomingMail
```

```
Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected
on this listener.



- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]> HOSTACCESS

There are currently 4 policies defined.

There are currently 5 sender groups.



Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- MOVE - Move an entry.

- DEFAULT - Set the defaults.

- PRINT - Display the table.

- IMPORT - Import a table from a file.

- EXPORT - Export the table to a file.

- CLEAR - Remove all entries.

[]> NEW



1.New Sender Group
```

```
2.New Policy

[1]> 1



Enter a name for this sender group.(optional)

[]> REDLIST

Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed.

IP address ranges such as 10.1.1.10-20 are allowed.IP subnets such as
10.2.3. are allowed.

Hostnames such as crm.example.com are allowed.

Partial hostnames such as .example.com are allowed.

Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are
allowed.

SenderBase Network Owner IDs such as SBO:12345 are allowed.

Remote blacklist queries such as dnslist[query.blacklist.example] are
allowed.

Separate multiple hosts with commas

[]> possible_spammer.com

Select a behavior for this entry.

1.Accept

2.Relay

3.Reject

4.TCP Refuse

5.Continue

6.Policy: ACCEPTED

7.Policy: BLOCKED

8.Policy: THROTTLED

9.Policy: TRUSTED

[1]> 8



Enter a comment for this sender group.
```

```
[]>


There are currently 4 policies defined.

There are currently 6 sender groups.
```

使用 CLI 批处理命令执行相同操作：

```
example.com> listenerconfig edit IncomingMail hostaccess new sendergroup
REDLIST possible_spammer.com Policy:  “THROTTLED”
```

命令：参考示例

本章包含以下部分：

如何阅读列表

对于每个命令，均提供一个说明和至少一个命令使用示例。“用法”部分指定以下命令属性：

步骤 1　该命令是否需要在设备上执行 `commit` 命令？

步骤 2　该命令是否限定为在特定模式（集群、分组或计算机）下使用？

步骤 3　该命令是否允许批处理格式？

有关集中管理的更多信息，请参阅《*思科邮件安全设备 AsyncOS 用户指南*》。

有关批处理格式的更多信息，请参阅“命令行界面：基础知识”（第 1 页）。

高级恶意软件保护

ampconfig

配置文件信誉过滤和文件分析。未经思科 TAC 指导，请勿修改高级选项。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令支持批处理格式。有关详细信息，请键入命令 `help ampconfig` 来查阅联机帮助。

示例

启用文件信誉和文件分析

```
mail.example.com> ampconfig

File Reputation: Disabled

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
[]> setup
```

```
File Reputation: Disabled
Would you like to use File Reputation?[Y]>

Would you like to use File Analysis?[Y]>

File types supported for File Analysis:

1.Microsoft Executables

Do you want to modify the file types selected for File Analysis?[N]>

Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy.

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:

1.Microsoft Executables

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

配置邮件安全设备以使用公共云文件分析服务器

```
mail.example.com> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>
```

```
Enter cloud domain?
[cloud-domain.com]>

Enter reputation cloud server pool?
[cloud-server-pool.com]>

Do you want use the recommended reputation threshold from cloud service?[Y]>

Choose a file analysis server:
1.AMERICAS (https://americas-fa.com)
2.Private Cloud
[1]>
...
```

（仅公共云文件分析服务）配置设备组

对于发自组织内任意设备的待分析文件，为了允许组织内的所有内容安全设备可以在云中查看这些文件的文件分析结果详细信息，您需要将所有设备加入到同一设备组。

有关详细信息，请参阅《用户指南》中的“文件信誉过滤和文件分析”一章。

```
mail.example.com> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> setgroup

Does your organization have multiple Cisco Email, Web, and/or Content Security Management
appliances?[N]> Y

Do you want this appliance to display detailed analysis reports for files uploaded to the
cloud from other appliances in your organization, and vice-versa?[Y]>

Enter an Analysis Group name.This name is case-sensitive and must be configured
identically on each appliance in the Analysis Group.
[]> FA_Reporting

Registration is successful with the group name.This does not require commit
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: FA_Reporting


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- VIEWGROUP - view the group members details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

注　在配置设备组后，无法使用 setgroup 子命令。如果出于任何原因需要修改该组，则必须向思科 TAC 提交支持请求。
可以使用 viewgroup 子命令查看设备组的详细信息。

配置邮件安全设备以使用内部部署文件分析服务器

```
mail.example.com> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]>

Do you want use the recommended reputation threshold from cloud service?[Y]>

Choose a file analysis server:
1.AMERICAS (https://panacea.threatgrid.com)
2.Private Cloud
[1]> 2

Enter file analysis server url?
[]> https://mycloud.example.com

Certificate Authority:
1.Use Cisco Trusted Root Certificate List
2.Paste certificate to CLI
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation?[N]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

清除本地文件信誉缓存

```
mail.example.com> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> clearcache

Do you want to clear File Reputation Cache?[N]> y

Cache cleared successfully.
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

反垃圾邮件

本部分包含以下命令：

antispamconfig

说明

配置反垃圾邮件策略。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

以下示例演示反垃圾邮件功能的配置过程。

```
mail3.example.com> antispamconfig

Choose the operation you want to perform:
- IRONPORT - Configure IronPort Anti-Spam.
- CLOUDMARK - Configure Cloudmark Service Provider Edition.
- MULTISCAN - Configure IronPort Intelligent Multi-Scan.
[]> ironport

IronPort Anti-Spam scanning: Disabled

Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[]> setup

IronPort Anti-Spam scanning: Disabled
Would you like to use IronPort Anti-Spam scanning?[Y]> y

The IronPort Anti-Spam License Agreement is displayed (if you have not already accepted
it).

Do you accept the above IronPort Anti-Spam license agreement?[]> Y

Increasing the following size settings may result in decreased performance.Please consult
documentation for size recommendations based on your environment.

Never scan message larger than: (Add a trailing K for kilobytes, M for megabytes, or no
letters for bytes.)
[1M]>

Always scan message smaller than: (Add a trailing K for kilobytes, M for megabytes, or no
letters for bytes.)
[512K]>

Please specify the IronPort Anti-Spam scanning timeout (in seconds)
[60]>

Would you like to enable regional scanning?[N]>

IronPort Anti-Spam scanning is now enabled on the system.Please note: you must issue the
'policyconfig' command (CLI) or Mail Policies (GUI) to configure
Cisco IronPort scanning behavior for default and custom Incoming and Outgoing Mail
Policies.This is recommended for your DEFAULT policy.

IronPort Anti-Spam scanning: Enabled


Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[]>
```

antispamstatus

说明

显示反垃圾邮件状态。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> antispamstatus


Choose the operation you want to perform:
- IRONPORT - Display IronPort Anti-Spam version and rule information.
- CLOUDMARK - Display Cloudmark Service Provider Edition version and rule information.
- MULTISCAN - Display Intelligent Multi-Scan version and rule information.
[]> ironport

  Component             Last Update                 Version
 CASE Core Files        Never updated               3.4.0-013
 CASE Utilities         Never updated               3.4.0-013
 Structural Rules       Never updated 3.3.1-009-20141210_214201
 Web Reputation DB      Never updated               20141211_111021
 Web Reputation Rules   Never updated 20141211_111021-20141211_170330
 Content Rules          Never updated               unavailable
 Content Rules Update   Never updated               unavailable


Last download attempt made on: Never
```

antispamupdate

说明

手动请求即时更新反垃圾邮件规则和相关案例组件。这也包括反垃圾邮件规则和智能多重扫描 (IMS) 使用的案例组件，但不适用于 IMS 使用的第三方反垃圾邮件引擎。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> antispamupdate

Choose the operation you want to perform:
- MULTISCAN - Request updates for Intelligent Multi-Scan
- IRONPORT - Request updates for IronPort Anti-Spam
- CLOUDMARK - Request updates for Cloudmark Anti-Spam
```

```
[]> ironport

Requesting check for new CASE definitions
```

incomingrelayconfig

说明

使用 incomingrelayconfig 命令可以启用并配置传入中继功能。在下面的示例中，会首先启用传入中继功能，然后添加两个中继，对其中一个进行修改，将另一个删除。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例：启用传入中继并配置传入中继

```
mail3.example.com> incomingrelayconfig

Incoming relays: Disabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- RELAYLIST - Configure incoming relays.
[]> setup

This command helps your Cisco IronPort appliance determine the sender's
originating IP address.

You should ONLY enable this command if your Cisco IronPort appliance is NOT
directly connected to the Internet as the "first hop" in your email
infrastructure.

You should configure this feature if other MTAs or servers are configured at
your network's perimeter to relay mail to your Cisco IronPort appliance.

Do you want to enable and define incoming relays?[N]> y

Incoming relays: Enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- RELAYLIST - Configure incoming relays.
[]> relaylist

There are no relays defined.

Choose the operation you want to perform:
- NEW - Create a new entry
[]> new

Enter a name for this incoming relay (Ex: "first-hop")
[]> first-hop
```

```
Enter the IP address of the incoming relay.IPv4 and IPv6 addresses are supported.

For IPv4, CIDR format subnets such as 10.1.1.0/24, IP address ranges such as 10.1.1.10-20,
and subnets such as 10.2.3. are allowed.

For IPv6, CIDR format subnets such as 2001:db8::/32 and IP address ranges such as
2001:db8::1-2001:db8::11 are allowed.

Hostnames such as crm.example.com and partial hostnames such as .example.com are allowed.
[]> 192.168.1.1

Do you want to use the "Received:" header or a custom header to determine the originating
IP address?
1.Use "Received:" header
2.Use a custom header
[1]> 1

Within the "Received:" header, enter the special character or string after which to begin
parsing for the originating IP address:
[from]> [

Within the headers, enter the position of the "Received:" header that contains the
originating IP address:
[1]> 1

There is 1 relay defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]> print

Incoming                                    Header          Match
relay name:    IP address:                  to parse:       after:      Hops:
-----------    -----------                  ---------       ------      -----
first-hop      192.168.1.1                  Received        [           1

There is 1 relay defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]> new

Enter a name for this incoming relay (Ex: "first-hop")
[]> second-hop

Enter the IP address of the incoming relay.IPv4 and IPv6 addresses are supported.

For IPv4, CIDR format subnets such as 10.1.1.0/24, IP address ranges such as 10.1.1.10-20,
and subnets such as 10.2.3. are allowed.

For IPv6, CIDR format subnets such as 2001:db8::/32 and IP address ranges such as
2001:db8::1-2001:db8::11 are allowed.

Hostnames such as crm.example.com and partial hostnames such as .example.com are allowed.
[]> 192.168.1.2

Do you want to use the "Received:" header or a custom header to determine the originating
IP address?
```

```
1.Use "Received:" header
2.Use a custom header
[1]> 2

Enter the custom header name that contains the originating IP address:
[]> x-Connecting-IP

There are 2 relays defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]> print

Incoming                                    Header          Match
relay name:    IP address:                  to parse:       after:      Hops:
-----------    -----------                  ---------       ------      -----
first-hop      192.168.1.1                  Received        [           1
second-hop     192.168.1.2                  x-Connecting-IP n/a         n/a

There are 2 relays defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]> delete

1. first-hop:      192.168.1.1
2. second-hop:     192.168.1.2
Enter the number of the entry you wish to delete:
[1]> 1

Incoming relay "first-hop" deleted.

There is 1 relay defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]>
```

slblconfig

说明

配置最终用户安全列表/阻止列表。

注　必须通过 GUI 在设备上启用安全列表/阻止列表，才能运行此命令。

Usage

提交：此命令不需要 “提交”。

批处理命令：此命令支持批处理格式。

批处理格式 - 导入

批处理格式

使用指定文件中的条目替换最终用户安全列表/阻止列表中的所有条目。

```
slblconfig import <filename> <ignore invalid entries>
```

- `filename` - 必须导入的文件的名称。该文件必须位于设备上的 `/configuration` 目录中。
- `ignore invalid entries` - 是否忽略无效的条目。选择 “是 (Yes)”或 “否 (No)”。

批处理格式 - 导出

将最终用户安全列表/阻止列表中的所有条目导出到设备上的文件。

```
slblconfig export
```

设备使用以下命名约定将 .CSV 文件保存到 `/configuration` 目录：

slbl<timestamp><serial number>.csv.

示例 - 导入安全列表/阻止列表条目

```
mail.example.com> slblconfig

End-User Safelist/Blocklist: Enabled

Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[]> import

Currently available End-User Safelist/Blocklist files:
1. slbl.csv
Choose the file to import from.
[1]> 1

Do you want to ignore invalid entries? [Y]> Y

End-User Safelist/Blocklist import has been initiated...
Please wait while this operation executes.

End-User Safelist/Blocklist successfully imported.

Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[]>
```

灰色邮件检测和安全取消订阅

任务	命令
配置灰色邮件检测和安全取消订阅全局设置	graymailconfig
配置灰色邮件检测和安全取消订阅的传入邮件策略	policyconfig
显示现有灰色邮件规则的详细信息	graymailstatus
手动请求更新灰色邮件规则	graymailupdate

graymailconfig

说明

配置灰色邮件检测和安全取消订阅全局设置。

注　要启用灰色邮件检测和安全取消订阅，必须全局启用反垃圾邮件扫描。这可以是 IronPort 反垃圾邮件或智能多重扫描功能。

要为灰色邮件检测和安全取消订阅配置策略设置，请使用 `policyconfig` 命令。有关详细信息，请参阅创建传入策略以丢弃标识为大宗邮件或社交网络邮件的邮件，（第 3-211 页）。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。有关详细信息，请键入命令 `help graymailconfig` 参阅联机帮助。

示例

```
Graymail Detection: Disabled

Choose the operation you want to perform:
- SETUP - Configure Graymail.
[]> setup

Would you like to use Graymail Detection?[Y]>

Increasing the following size settings may result in decreased performance.
Please consult documentation for size recommendations based on your
environment.

Maximum Message Size to Scan (Add a trailing K for kilobytes, M for megabytes,
or no letters for bytes.):
[1M]>

Timeout for Scanning Single Message(in seconds):
[60]>
```

```
Graymail Safe Unsubscribe: Disabled
Would you like to use Graymail Safe Unsubscribe?[Y]>

Graymail Detection and Safe Unsubscribe is now enabled.Please note: The global
settings are recommended only for your DEFAULT mail policy.To configure policy
settings, use the incoming or outgoing policy page on web interface or the
'policyconfig' command in CLI.
```

graymailstatus

说明

显示现有灰色邮件规则的详细信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> graymailstatus

Component            Version         Last Updated
Graymail Library     01.378.53#15    Never updated
Graymail Tools       1.0             Never updated
```

graymailupdate

说明

手动请求更新灰色邮件规则。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> graymailupdate

Requesting check for new Graymail updates.
```

防病毒

本部分包含以下 CLI 命令：

- antivirusconfig
- antivirusstatus
- antivirusupdate

antivirusconfig

说明

配置防病毒策略。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，antivirusconfig 命令用于在系统上启用 Sophos 病毒扫描，并将超时值设为 60 秒。要配置更新服务器、更新间隔和可选的代理服务器，请参阅 “updateconfig”（第 108 页）。

注　如果您在执行 systemsetup 命令期间未接受许可，则在首次调用 antivirusconfig 命令时，系统会向您显示许可协议，如果您未接受许可协议，在该设备上将不会启用 Sophos 病毒扫描引擎。

```
mail3.example.com> antivirusconfig

Choose the operation you want to perform:
- SOPHOS - Configure Sophos Anti-Virus.
- MCAFEE - Configure McAfee Anti-Virus.
[]> sophos

Sophos Anti-Virus: Disabled

Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
[]> setup

Sophos Anti-Virus scanning: Disabled
Would you like to use Sophos Anti-Virus scanning?[Y]> y

(First time users see the license agreement displayed here.)

Please specify the Anti-Virus scanning timeout (in seconds)
[60]> 60

Sophos Anti-Virus scanning is now enabled on the system.
```

```
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure Sophos Anti-Virus scanning behavior for default and custom
Incoming and Outgoing Mail Policies.
This is recommended for your DEFAULT policy.

Sophos Anti-Virus: Enabled

Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
[]>
```

查看防病毒 IDE 详细信息

AsyncOS 会提供设备已经下载的特定防病毒签名文件 （IDE 文件）的详细状态。您可以使用 `antivirusconfig -> detail` 子命令访问这些详细信息。例如：

```
mail3.example.com> antivirusconfig

Choose the operation you want to perform:
- SOPHOS - Configure Sophos Anti-Virus.
- MCAFEE - Configure McAfee Anti-Virus.
[]> sophos

Sophos Anti-Virus: Enabled

Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
- STATUS - View Sophos Anti-Virus status.
- DETAIL - View Sophos Anti-Virus detail.
[]> detail

Sophos Anti-Virus:

Product - 3.87
Engine - 2.25.0
Product Date - 01 Nov 2004


Sophos IDEs currently on the system:

   'Mkar-E.Ide'           Virus Sig.- 23 Dec 2004 01:24:02
   'Rbot-Sd.Ide'          Virus Sig.- 22 Dec 2004 19:10:06
   'Santy-A.Ide'          Virus Sig.- 22 Dec 2004 06:16:32
   'Bacbanan.Ide'         Virus Sig.- 21 Dec 2004 18:33:58
   'Rbot-Sb.Ide'          Virus Sig.- 21 Dec 2004 14:50:46
   'Rbotry.Ide'           Virus Sig.- 21 Dec 2004 06:13:40
   'Sdbot-Si.Ide'         Virus Sig.- 20 Dec 2004 20:52:04
   'Oddbob-A.Ide'         Virus Sig.- 19 Dec 2004 23:34:06
   'Rbot-Rw.Ide'          Virus Sig.- 19 Dec 2004 00:50:34
   'Wortd.Ide'            Virus Sig.- 18 Dec 2004 07:02:44
   'Delf-Jb.Ide'          Virus Sig.- 17 Dec 2004 22:32:08
[...command continues...]
```

antivirusstatus

说明

显示防病毒状态。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> antivirusstatus

Choose the operation you want to perform:
- MCAFEE - Display McAfee Anti-Virus version information
- SOPHOS - Display Sophos Anti-Virus version information
[]> sophos

    SAV Engine Version        3.85
    IDE Serial                2004101801
 Engine Update        Mon Sep 27 14:21:25 2004
    Last IDE Update           Mon Oct 18 02:56:48 2004
    Last Update Attempt       Mon Oct 18 11:11:44 2004
    Last Update Success       Mon Oct 18 02:56:47 2004
```

antivirusupdate

说明

手动更新病毒定义。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> antivirusupdate

Choose the operation you want to perform:
- MCAFEE - Request updates for McAfee Anti-Virus
- SOPHOS - Request updates for Sophos Anti-Virus
[]> sophos
```

```
Requesting update of virus definitions
mail3.example.com>
```

命令行管理

本部分包含以下 CLI 命令：

- commit
- commitdetail
- clearchanges 或 clear
- help 或 h 或 ?
- rollbackconfig
- quit 或 q 或 exit

commit

说明

提交更改。您可以选择在 commit 命令后输入评论。

Usage

提交：N/A

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> commit

Please enter some comments describing your changes:

[]> Changed "psinet" IP Interface to a different IP ad dress

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

commitdetail

说明

显示最近一次提交的详细信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> commitdetail

Commit at Mon Apr 18 13:46:28 2005 PDT with comments: "Enabled loopback".
mail3.example.com>
```

clearchanges 或 clear

说明

clear 命令会清除自上次发出 commit 或 clear 命令后所做的所有配置更改。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> clear

Are you sure you want to clear all changes since the last commit?[Y]> y

Changes cleared: Mon Jan 01 12:00:01 2003
mail3.example.com>
```

help 或 h 或 ?

说明

help 命令会列出所有可用的 CLI 命令，并为每个命令提供简短说明。要调用 help 命令，可以在命令提示符中键入 help 或一个问号 (?)。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> help
Displays the list of all available commands.
```

rollbackconfig

rollbackconfig 命令允许您回滚到之前提交的 10 个配置之一。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> rollbackconfig

Previous Commits:
    Committed On                  User                Description
--------------------------------------------------------------------------------
1.Fri May 23 06:53:43 2014      admin               new user
2.Fri May 23 06:50:57 2014      admin               rollback
3.Fri May 23 05:47:26 2014      admin
4.Fri May 23 05:45:51 2014      admin               edit user

Enter the number of the config to revert to.
[]> 2

Are you sure you want to roll back the configuration?[N]> y

Reverted to Fri May 23 06:50:57 2014      admin               rollback
Do you want to commit this configuration now?[N]> y

Committed the changes successfully
```

quit 或 q 或 exit

说明

quit 命令可以让您从 CLI 应用注销。系统会清除尚未提交的配置更改。quit 命令不会影响邮件操作。系统将注销记录在日志文件中。（键入 exit 等同于键入 quit。）

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> quit

Configuration changes entered but not committed.Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.
Are you sure you wish to exit?[N]> Y
```

配置文件管理

本部分包含以下 CLI 命令：

- loadconfig
- mailconfig
- resetconfig
- saveconfig
- showconfig

loadconfig

说明

加载配置文件。

注　仅使用 GUI 才支持在加入集群的计算机上加载配置。有关说明，请参阅 《*思科邮件安全设备 AsyncOS 用户指南*》。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在本示例中，新的配置文件从本地位置导入。

```
mail3.example.com> loadconfig

1.Paste via CLI
2.Load from file
[1]> 2

Enter the name of the file to import:
[]> changed.config.xml

Values have been loaded.
Be sure to run "commit" to make these settings active.
```

```
mail3.example.com> commit
Please enter some comments describing your changes:
[]> loaded new configuration file

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

在此示例中，直接在命令行粘贴新配置文件。（请记得在空白行输入 Control-D 以结束粘贴命令。）然后，使用 “系统设置向导” (System Setup wizard) 更改默认主机名、 IP 地址以及默认网关信息。最后，提交更改。

```
mail3.example.com> loadconfig

1.Paste via CLI
2.Load from file
[1]> 1

Paste the configuration file now.
Press CTRL-D on a blank line when done.

[The configuration file is pasted until the end tag </config>. Control-D is entered on a
separate line.]

Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> systemsetup

[The system setup wizard is run.]

mail3.example.com> commit

Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings via
systemsetup

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

mailconfig

说明

要测试配置，您可以立即使用 `mailconfig` 命令发送包含系统配置数据（刚刚用 `systemsetup` 命令创建）的测试邮件。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> mailconfig

Please enter the email address to which you want to send the configuration file.
Separate multiple addresses with commas.
[]> user@example.com

Choose the password option:
1.Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2.Encrypt passwords
3.Plain passwords
[1]> 2

The configuration file has been sent to user@example.com.
```

将配置发送到您具有访问权限的邮箱以确认系统是否能够在您的网络中发送邮件。

resetconfig

说明

当对设备进行物理传输时，您可能希望从出厂默认值开始。 resetconfig 命令会将*所有*配置值重置为出厂默认设置。此命令极具破坏性，只有当您传输设备或解决配置问题万不得已时方可使用。我们建议，在运行 resetconfig 命令后，请在重新连接到 CLI 后运行 systemsetup 命令。

注　resetconfig 命令只在设备处于离线状态时起作用。当 resetconfig 命令完成时，设备会自动返回到联机状态，即使之后您再次运行 systemsetup 命令也如此。如果在发出 resetconfig 命令之前邮件传输已暂停，则当 resetconfig 命令完成时，将尝试再次传输邮件。

警告　**resetconfig 命令会将所有网络设置恢复为出厂默认设置，这可能会断开您与 CLI 的连接，禁用连接设备所用的服务 （FTP、 Telnet、 SSH、 HTTP、 HTTPS），甚至删除您使用 userconfig 命令创建的其他用户帐户。如果您无法通过默认 “管理员” (Admin) 用户帐户使用串行接口或管理端口上的默认设置重新连接到 CLI，请勿使用此命令。**

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> suspend

Delay (seconds, minimum 30):
[30]> 45

Waiting for listeners to exit...
```

```
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> resetconfig

Are you sure you want to reset all configuration values?[N]> Y

All settings have been restored to the factory default.
```

saveconfig

说明

saveconfig 命令会将具有唯一文件名的配置文件保存到 configuration 目录。

注　如果您是位于集群环境中，则此命令会保存完整的集群配置。要在集群计算机上运行此命令，请将您的配置模式更改为集群。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，配置文件中的密码将会被加密并保存在 configuration 目录中。

```
mail.example.com> saveconfig

Choose the password option:
1.Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2.Encrypt passwords
3.Plain passwords
[1]> 2

File written on machine "mail.example.com" to the location
"/configuration/C100V-4232116C4E14C70C4C7F-7898DA3BD955-20140319T050635.xml".
Configuration saved.
```

showconfig

说明

showconfig 命令会将当前配置打印到屏幕。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，该配置显示在 CLI 上，并且配置中的密码会加密。

```
mail.example.com> showconfig

Choose the password display option:
1.Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2.Encrypt passwords
3.Plain passwords
[1]> 2

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">

<!--
  Product: Cisco C100V Email Security Virtual Appliance
  Model Number: C100V
  Version: 9.0.0-038
  Serial Number: 4232116C4E14C70C4C7F-7898DA3BD955
  Number of CPUs: 2
  Memory (MB): 6144
  Current Time: Wed Mar 19 05:30:05 2014
-->
<config>
<!--
********************************************************************************
*                            Network Configuration                             *
********************************************************************************
-->
[The remainder of the configuration file is printed to the screen.]
```

集群管理

本部分包含以下 CLI 命令：

- clusterconfig

clusterconfig

说明

clusterconfig 命令用于配置集群相关的设置。如果此计算机不是集群的一部分，运行 clusterconfig 将使您可以选择，是加入集群还是创建新集群。

clusterconfig 命令提供附加的子命令：

非集群命令

当您不在集群时，以下命令可用。

- clusterconfig new <name> - 这将使用给定的名称创建新的集群。此计算机将是此集群的成员和名为 “Main Group”的默认集群组的成员。

  <name> - 新集群的名称。

- clusterconfig join [--port=xx] <ip_of_remote_cluster> [<admin_password>]<groupname> - 这会将此计算机添加到集群。

  <ip_of_remote_cluster> - 集群中另一台计算机的 IP 地址。

  <admin_password > - 集群的 admin 密码。如果
  通过 CCS 加入，则不应指定此密码。

  <groupname> - 要加入的组的名称。

  <port> - 要连接的远程计算机的端口 （默认为 22）。

- clusterconfig prepjoin print

  这将显示准备通过 CCS 端口将此计算机加入集群所需的信息。

集群命令

当您在集群中时，以下命令可用。

- clusterconfig addgroup <groupname> - 创建新的集群组。此组最初没有成员。
- clusterconfig renamegroup <old_groupname> <new_groupname> - 更改集群组的名称。
- clusterconfig deletegroup <groupname> [new_groupname] - 删除集群组。

  <groupname> - 要删除的集群组的名称。

  <new_groupname> - 要将旧集群组中的计算机放入其中的集群组。

- clusterconfig setgroup <machinename> <groupname> - 设置（更改）某个计算机所属的组。

  <machinename> - 要设置的计算机的名称。

  <groupname> - 要计算机设置到其中的组。

- clusterconfig removemachine <machinename> - 从集群中删除计算机。
- clusterconfig setname <name> - 将集群的名称更改为指定名称。
- clusterconfig list - 显示集群中当前所有的计算机。
- clusterconfig connstatus - 显示集群中当前所有的计算机，并为断开连接的计算机添加路由详细信息。
- clusterconfig disconnect <machinename> - 此命令会临时将计算机从集群中断开。

  <machinename> - 要断开连接的计算机的名称。

- clusterconfig reconnect <machinename> - 这将会恢复被 “disconnect”命令断开连接的计算机的连接。
- clusterconfig prepjoin new <serial_number> <hostname> <user_key> - 这将会添加一个新主机，该新主机将通过 CCSport 加入集群。

`<serial_number>` - 要添加的计算机的序列号。

`<hostname>` - 要添加的计算机的主机名。

`<user_key>` - 来自加入计算机的 “prepjoin print” 命令的 SSH 用户密钥 。

- `clusterconfig prepjoin delete <serial_number|hostname>` - 这行命令会删除以前通过 “prepjoin new” 命令指定为要添加的主机。如果您稍后决定不添加该主机，则只需要使用这一行命令。当主机成功添加到集群时，会自动删除它的 prepjoin 信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在集群模式下使用。

批处理命令：此命令不支持批处理格式。

示例

有关 `clusterconfig` 命令及其使用的说明，请参阅 《*思科邮件安全设备 AsyncOS 用户指南*》。

数据丢失保护

本部分包含以下 CLI 命令：

- dlprollback
- dlpstatus
- dlpupdate
- emconfig
- emdiagnostic

dlprollback

说明

回滚 DLP 引擎和 config 到上一版本。

注　必须通过 GUI 中的 “DLP 全局设置” (Global Settings) 页配置 DLP 后，才能使用 `dlprollback` 命令。

警告　**此命令会将您的设备复原为以前的 DLP 策略。必须在出站邮件策略中重新启用 DLP 策略，才能恢复 DLP 扫描。**

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可以用于集群、分组或计算机模式中。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> dlprollback

This will revert to older DLP policies.
IMPORTANT: After rollback, you must re-enable DLP policies in Outbound Mail Policies so
that DLP scanning can be resumed successfully.
Do you wish to rollback? [N]> Y

Requesting rollback for DLP engine.
Re-enable DLP policies in Outbound Mail Policies when rollback is completed (Please check
rollback status in mail logs)
```

dlpstatus

请求 DLP 引擎的版本信息。

注　必须通过 GUI 中的 DLP 全局设置 (Global Settings) 页配置 DLP 后，才能使用 `dlpstatus` 命令。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可以用于集群、分组或计算机模式中。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> dlpstatus

Component                Version    Last Updated
RSA DLP Engine           3.0.2.31   Never updated
```

dlpupdate

说明

更新 RSA DLP 引擎。

注　必须通过 GUI 中的 DLP 全局设置 (Global Settings) 页配置 DLP 后，才能使用 `dlpupdate` 命令。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可以用于集群、分组或计算机模式中。

批处理命令：此命令支持批处理格式。

批处理格式

即便没有检测到更改，`dlpupdate` 命令的批处理格式也会强制更新 DLP 引擎。

```
dlpupdate [force]
```

示例

```
mail.example.com> dlpupdate
Checking for available updates.This may take a few seconds..
Could not check for available updates.Please check your Network and Service Updates
settings and retry.

Choose the operation you want to perform:
- SETUP - Enable or disable automatic updates for DLP Engine.
[]> setup

Automatic updates for DLP are disabled
Do you wish to enable automatic updates for DLP Engine?[N]> y


Choose the operation you want to perform:
- SETUP - Enable or disable automatic updates for DLP Engine.
[]>
```

emconfig

说明

配置 RSA 企业管理器的互操作性设置。

注　必须通过 GUI 中的 DLP 全局设置 (Global Settings) 页配置 RSA 企业管理器后，才能使用 `emconfig` 命令。您不能使用 CLI 启用此功能，仅可编辑现有设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可以用于集群、分组或计算机模式中。

批处理命令：此命令不支持批处理格式。

批处理格式

要设置邮件安全设备和 RSA 企业管理器之间的连接：

```
emconfig setup [options]
```

表 3-1　emconfig 设置选项

选项	说明
--remote_host	RSA 企业管理器的主机名或 IP 地址。
--remote_port	连接到 RSA 企业管理器的端口。
--local_port	ESA 上用于连接到企业管理器的端口。
--enable_ssl	启用到 RSA 企业管理器的 SSL 通信 Manager。 使用 `1` 启用，使用 `0` 禁用。

连接到 RSA 企业管理器的示例

```
vm10esa0031.qa> emconfig

RSA Enterprise Manager connection status is: "UNKNOWN"

Choose the operation you want to perform:
- SETUP - Edit RSA Enterprise Manager interop config.
[]> setup

RSA Enterprise Manager: test.example.com:20000
Local port for EM to connect to: 20002
SSL Communication to RSA EM: disabled
Enter hostname of RSA Enterprise Manager:
[test.example.com]> em.example.com
```

```
Enter port number of RSA Enterprise Manager:
[20000]>

Enter local port for EM to connect:
[20002]>

Enable SSL communication to EM [N]>

Advanced Settings:
  RSA Enterprise Manager GUID: emlocalsite
  Device Vendor name: Cisco Systems
  Device Status Interval: 5 seconds
  Polling Cycle Interval: 30 seconds
  Connection Throttle Interval: 0 milliseconds
  Max event archive size: 31457280 bytes
  Max files in event archive: 50
  Max file size in event archive: 10485760 MB
  Max size of event.xml file: 1048576 MB
  Interoperability subsystem heartbeat interval: 500 milliseconds
  Heartbeat service attempts before failing: 3
  Connection timeout duration: 30 seconds
  Command status timeout duration: 30 seconds
  Max chunk size: 1000
  Msg exchange cycle: 1
Do you want to change advanced settings?[N]>


Choose the operation you want to perform:
- SETUP - Edit RSA Enterprise Manager interop config.
[]>
```

emdiagnostic

说明

ESA 上的 RSA EM 诊断工具。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

S/MIME 安全服务

smimeconfig

说明

配置 S/MIME 设置，例如发送配置文件、管理公共密钥等。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

- 创建一个发送配置文件以便进行签名和加密，（第 3-32 页）
- 添加公共密钥以便进行加密，（第 3-33 页）

创建一个发送配置文件以便进行签名和加密

以下示例显示如何使用 S/MIME 创建发送配置文件，以便进行签名和加密邮件。

```
mail.example.com> smimeconfig

Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.
[]> gateway

Choose the operation you want to perform:
- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[]> sending

Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[]> new

Enter a name for this profile:
> hr_sign_and_encrypt

1.Encrypt
2.Sign
3.Sign/Encrypt
4.Triple
Enter S/MIME mode:
[2]> 3

1. smime_signing

Select S/MIME certificate to sign:
[1]>

1.Detached
2.Opaque
Enter S/MIME sign mode:
[1]>

1.Bounce
2.Drop
3.Split
```

```
Enter S/MIME action:
[1]> 3

Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[]> print

S/MIME Sending Profiles
Name       Certificate      S/MIME Mode   Sign Mode  Action
---------  ---------------  ------------  ---------  --------
hr_sign_a  smime_signing   Sign/Encrypt     Detached      Split

Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[]>
```

添加公共密钥以便进行加密

以下示例显示如何将收件人的 S/MIME 证书的公共密钥添加到设备以加密邮件。

```
mail.example.com> smimeconfig

Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.
[]> gateway

Choose the operation you want to perform:
- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[]> verification

Choose the operation you want to perform:
- NEW - Create a new S/MIME Public Key.
- IMPORT - Import the list of S/MIME Public Keys from a file.
[]> new

Enter a name for this profile:
> hr_signing

1.Import
2.Paste
Choose one of the options for the certificate introducing:
[2]>

Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDdDCCAlygAwIBAgIBDTANBgkqhkiG9w0BAQUFADCBljELMAkGA1UEBhMCSU4x
CzAJBgNVBAg...
-----END CERTIFICATE-----
.
C=IN,ST=KA,L=BN,O=Cisco,OU=stg,CN=cert_for_enc,emailAddress=admin@example.com
```

```
Choose the operation you want to perform:
- NEW - Create a new S/MIME Public Key.
- EDIT - Edit a S/MIME Public Key.
- RENAME - Rename a S/MIME Public Key.
- DELETE - Delete a S/MIME Public Key.
- IMPORT - Import the list of S/MIME Public Keys from a file.
- EXPORT - Export the list of S/MIME Public Keys to a file.
- PRINT - Display S/MIME Public Keys.
[]> print

S/MIME Public Keys
Name       Emails                     Domains                    Remaining
---------  -------------------------  -------------------------  ---------
hr_signin  admin@vm30bsd0008.ibqa     dns.vm30bsd0008.ibqa       145 days
```

域密钥

本部分包含以下 CLI 命令：

- domainkeysconfig

domainkeysconfig

说明

配置 DomainKeys/DKIM 支持。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式 - 签名配置文件

`domainkeysconfig` 命令的批处理格式可以用于创建、编辑或者删除签名配置文件。

- 添加 DomainKeys/DKIM 签名配置文件：

```
domainkeysconfig profiles signing new <name> <type> <domain>
<selector> <user-list> [options]
```

表 3-2　domainkeysconfig 新的签名配置文件参数

参数	说明
< 姓名 >	域配置文件的名称。
<type>	域的类型。可以是 `dk` 或 `dkim`。
<domain>	域配置文件的域字段。这形成了域密钥签名的 `d` 标记。

表 3-2　domainkeysconfig 新的签名配置文件参数

参数	说明
<selector>	域配置文件的选择器字段。这形成了域密钥签名的 s 标记。
<user-list>	逗号分隔的域配置文件用户列表。用户用于与邮件地址匹配，以确定特定域配置文件是否应该用于签名邮件。使用特殊关键字 all 匹配所有域用户。
[options]	
--key_name	用于签名的私钥的名称。
--canon	当由 DK 签名时要使用的规范化算法。目前支持的算法有 simple 和 nofws。默认为 nofws。
--body_canon	当由 DKIM 签名时要使用的正文规范化算法。目前支持的算法有 simple 和 relaxed。默认为 simple。
--header_canon	当由 DKIM 签名时要使用的信头规范化算法。目前支持的算法有 simple 和 relaxed。默认为 simple。
--body_length	用于计算签名的规范化正文的字节数。仅用于 DKIM 配置文件中。如果使用，则此值成为签名的 l 标记。默认情况下，不使用此值。
--headers_select	确定如何选择要签名的信头。仅用于 DKIM 配置文件中。可以是 all、 standard、 standard_ 和 _custom 之一。 all 意味着签名所有非重复的信头。“standard”意味着签名预定义组的常见信头，例如，主题、发件人、收件人、发送人以及 MIME 信头等。 standard_and_custom 意味着签名常见信头和用户定义组信头。默认为 standard。
--custom_headers	要签名的用户定义组信头。如果 headers_select 为 standard_and_custom，则仅用于 DKIM 配置文件中。默认为空组。
--i_tag	确定是否将 i 标记包括到签名中。可能的值为 yes 或 no。默认值为 yes。
--agent_identity	签名此邮件的代表用户或代理的身份。该语法是标准邮件地址，其中可以省略本地部分。此地址的域部分应为 <domain> 的子域或等同部分。此选项仅在 --i_tag 值设置为 yes 时才适用。默认值为空的本地部分，后跟 @ 和 <domain>。
--q_tag	确定是否将 q 标记包括到签名中。可能的值为 yes 或 no。默认值为 yes。
--t_tag	确定是否将 t 标记包括到签名中。可能的值为 yes 或 no。默认值为 yes。
--x_tag	确定是否将 x 标记包括到签名中。可能的值为 yes 或 no。默认值为 yes。
-expiration_time	签名到期之前的秒数。仅用于 DKIM 配置文件中。此值成为签名的 x 和 t 标记之间的差异。仅在 --x_tag 值设置为 yes 时此选项才适用。默认值为 31536000 秒 （一年）。
--z_tag	确定是否将 z 标记包括到签名中。可能的值为 yes 或 no。默认值为 no。

- 编辑签名配置文件：

```
domainkeysconfig profiles signing edit <name>
[signing-profile-options]
```

  签名配置文件选项：

  - rename <name>
  - domain <domain>
  - selector <selector>
  - canonicalization <canon>
  - canonicalization <header_canon> <body_canon>
  - key <key_name>
  - bodylength <body_length>
  - headerselect <header_select>
  - customheaders <custom_headers>
  - itag <i_tag> [<agent_identity>]
  - qtag <q_tag>
  - ttag <t_tag>
  - xtag <x_tag> [<expiration_time>]
  - ztag <z_tag>
  - new <user-list>
  - delete <user-list>
  - print
  - clear

- 删除签名配置文件：

```
domainkeysconfig profiles signing delete <name>
```

- 显示配置文件列表：

```
domainkeysconfig profiles signing list
```

- 打印签名配置文件的详细信息：

```
domainkeysconfig profiles signing print <name>
```

- 测试签名配置文件：

```
domainkeysconfig profiles signing test <name>
```

- 导入签名配置文件的本地副本：

```
domainkeysconfig profiles signing import <filename>
```

- 从设备导出签名配置文件的副本：

```
domainkeysconfig profiles signing export <filename>
```

- 从设备删除所有签名配置文件：

```
domainkeysconfig profiles signing clear
```

批处理格式 - 验证配置文件

- 创建新的 DKIM 验证配置文件。

```
domainkeysconfig profiles verification new <name>
<verification-profile-options>
```

表 3-3　domainkeysconfig 验证配置文件选项

参数	说明
--name	DKIM 验证配置文件的名称。
--min_key_size	可接受的最小密钥。可能的密钥长度值 （以位为单位）为 512、768、1024、1536 和 2048。默认值为 512。
--max_key_size	可接受的最大密钥。可能的密钥长度值 （以位为单位）为 512、768、1024、1536 和 2048。默认值为 2048。
--max_signatures_num	邮件中要验证的最大签名数量。可能的值为任何正数。默认值为 5。
--key_query_timeout	密钥查询超时前的秒数。可能的值为任何正数。默认值为 10。
--max_systemtime_divergence	容许发件人与验证人的挂钟异步相差的秒数。可能的值为任何正数。默认值为 60。
--use_body_length	是否使用正文长度参数。可能的值为 yes 或 no。默认值为 yes。
--tempfail_action	在出现临时故障的情况下应采取的 SMTP 操作。可能的值为 accept 或 reject。默认值为 accept。
--tempfail_response_code	在出现临时故障的情况下，被拒绝邮件的 SMTP 响应代码。可能的值为 4XX 格式的数字。默认值为 451。
--tempfail_response_text	在出现临时故障的情况下，被拒绝邮件的 SMTP 响应文本。默认值为 #4.7.5 Unable to verify signature - key server unavailable。
--permfail_action	在出现永久故障的情况下应采取的 SMTP 操作。可能的值为 accept 或 reject。默认值为 accept。
--permfail_response_code	在出现永久故障的情况下，被拒绝邮件的 SMTP 响应代码。可能的值为 5XX 格式的数字。默认值为 550。
--permfail_response_text	在出现永久故障的情况下，被拒绝邮件的 SMTP 响应文本。默认值为 #5.7.5， DKIM unauthenticated mail is prohibited。

- 编辑验证配置文件：

```
domainkeysconfig profiles verification edit <name>
<verification-profile-options>
```

- 删除验证配置文件：

```
domainkeysconfig profiles verification delete <name>
```

- 打印现有验证配置文件的详细信息：

```
domainkeysconfig profiles verification print <name>
```

- 显示现有验证配置文件的列表：

```
domainkeysconfig profiles verification list
```

- 从本地计算机导入验证配置文件：

```
domainkeysconfig profiles verification import <filename>
```

- 从设备导出验证配置文件：

```
domainkeysconfig profiles verification export <filename>
```

- 从设备删除所有现有验证配置文件：

```
domainkeysconfig profiles verification clear
```

批处理格式 - 签名密钥

- 创建新的签名密钥：

```
domainkeysconfig keys new <key_name> <key-options>
```

表 3-4　domainkeysconfig 签名密钥选项

参数	说明
--generate_key	生成私钥。可能的密钥长度值 （以位为单位）为 512、 768、 1024、 1536 和 2048。
--use_key	使用提供的私钥。
--public_key	标记以便推导指定私钥的匹配公共密钥并打印输出到屏幕。如果首先指定 --generate_key，则将先生成新私钥，后面显示匹配的公共密钥。

- 编辑签名密钥：

```
domainkeysconfig keys edit <key_name> key <key-options>
```

- 重命名现有签名密钥：

```
domainkeysconfig keys edit <key_name> rename <key_name>
```

- 指定公钥：

```
domainkeysconfig keys publickey <key_name>
```

- 删除密钥：

```
domainkeysconfig keys delete <key_name>
```

- 显示所有签名密钥的列表：

```
domainkeysconfig keys list
```

- 显示有关指定签名密钥的所有信息：

```
domainkeysconfig keys print <key_name>
```

- 从本地计算机导入签名密钥：

```
domainkeysconfig keys import <filename>
```

- 从设备导出签名密钥：

```
domainkeysconfig keys export <filename>
```

- 删除设备上的所有签名密钥：

```
domainkeysconfig keys clear
```

批处理格式 - 搜索密钥或配置文件

- 搜索配置文件签名密钥：

```
domainkeysconfig search <search_text>
```

批处理格式 - 全局设置

- 为设备上的域密钥/DKIM 修改全局设置。

```
domainkeysconfig setup <setup_options>
```

可用的选项如下：

  - `--sign_generated_msgs` - 指定是否对系统生成的邮件签名。可能的值为 `yes` 或 `no`。

示例：通过 CLI 配置域密钥

使用 CLI 中的 domainkeysconfig 命令配置设备上的域密钥。

domainkeysconfig 命令具有邮件策略 (Mail Policies) -> 域密钥 (Domain Keys) 页面上的所有功能。它还提供生成示例域密钥 DNS TXT 记录的功能。有关生成示例域密钥 DNS TXT 记录的详细信息，请参阅创建示例域密钥 DNS TXT 记录，（第 3-43 页）。

在本示例中，会生成密钥，并且创建域配置文件：

```
mail3.example.com> domainkeysconfig

Number of DK/DKIM Signing Profiles: 0
Number of Signing Keys: 0
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> keys


No signing keys are defined.

Choose the operation you want to perform:
- NEW - Create a new signing key.
- IMPORT - Import signing keys from a file.
[]> new

Enter a name for this signing key:
[]> testkey

1.Generate a private key
2.Enter an existing key
[1]>

Enter the size (in bits) of this signing key:
1.512
2.768
3.1024
4.1536
5.2048
[3]>

New key "testkey" created.

There are currently 1 signing keys defined.

Choose the operation you want to perform:
- NEW - Create a new signing key.
- EDIT - Modify a signing key.
- PUBLICKEY - Create a publickey from a signing key.
- DELETE - Delete a signing key.
- PRINT - Display signing keys.
- LIST - List signing keys.
- IMPORT - Import signing keys from a file.
- EXPORT - Export signing keys to a file.
- CLEAR - Clear all signing keys.
[]>

Number of DK/DKIM Signing Profiles: 0
```

```
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> profiles


Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]> signing


No domain profiles are defined.

Choose the operation you want to perform:
- NEW - Create a new domain profile.
- IMPORT - Import domain profiles from a file.
[]> new

Enter a name for this domain profile:
[]> Example

Enter type of domain profile:
1. dk
2. dkim
[2]>


The domain field forms the basis of the public-key query.The value in
this field MUST match the domain of the sending email address or MUST
be one of the parent domains of the sending email address.This value
becomes the "d" tag of the Domain-Keys signature.
Enter the domain name of the signing domain:
[]> example.com


Selectors are arbitrary names below the "_domainkey." namespace.A
selector value and length MUST be legal in the DNS namespace and in
email headers with the  additional provision that they cannot contain a
semicolon.This value becomes the "s" tag of the DomainKeys
Signature.
Enter selector:
[]> test


The private key which is to be used to sign messages must be entered.
A corresponding public key must be published in the DNS following the
form described in the DomainKeys documentation.If a key is not
immediately available, a key can be entered at a later time.
Select the key-association method:
1.Create new key
2.Paste in key
3.Enter key at later time
4.Select existing key
[1]> 4

Enter the name or number of a signing key.
1. testkey
```

```
[1]>


The canonicalization algorithm is the method by which the headers and
content are  prepared for presentation to the signing algorithm.
Possible choices are "simple" and "relaxed".

Select canonicalization algorithm for body:
1. simple
2. relaxed
[1]> 1

How would you like to sign headers:
1.Sign all existing, non-repeatable headers (except Return-Path header).
2.Sign "well-known" headers (Date, Subject, From, To, Cc, Reply-To, Message-ID, Sender,
MIME headers).
3.Sign "well-known" headers plus a custom list of headers.
[2]>

Body length is a number of bytes of the message body to sign.
This value becomes the "l" tag of the signature.
Which body length option would you like to use?
1.Whole body implied.No further message modification is possible.
2.Whole body auto-determined.Appending content is possible.
3.Specify a body length.
[1]>

Would you like to fine-tune which tags should be used in the
DKIM Signature?(yes/no) [N]>

Finish by entering profile users.The following types of entries are
allowed:
- Email address entries such as "joe@example.com".
- Domain entries such as "example.com".
- Partial domain entries such as ".example.com".For example, a partial
  domain of ".example.com" will match "sales.example.com".这
  sort of entry will not match the root domain ("example.com").
- Leave blank to match all domain users.
Enter user for this signing profile:
[]> sales.example.com

Do you want to add another user?[N]>


There are currently 1 domain profiles defined.

Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]>


Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
```

```
[]>

Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]>
```

创建示例域密钥 DNS TXT 记录

```
mail3.example.com> domainkeysconfig

Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> profiles


Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]> signing


There are currently 1 domain profiles defined.

Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]> dnstxt

Enter the name or number of a domain profile.
1.Example

[1]>

The answers to the following questions will be used to construct DKIM text
record for DNS.It can be used to publish information about this profile.


Do you wish to constrain the local part of the signing identities
```

```
("i=" tag of "DKIM-Signature" header field) associated with this
domain profile?[N]>

Do you wish to include notes that may be of interest to a human (no
interpretation is made by any program)?[N]>

The "testing mode" can be set to specify that this domain is testing DKIM and
that unverified email must not be treated differently from verified email.

Do you want to indicate the "testing mode"?[N]>

Do you wish to disable signing by subdomains of this domain?[N]>


The DKIM DNS TXT record is:

test._domainkey.example.com.IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDX5dOG9J8rXreA/uPtYr5lrCTCqR+qlS5Gm1f0OplAzSuB2BvO
nxZ5Nr+se0T+k7mYDP0FSUHyWaOvO+kCcum7fFRjS3EOF9gLpbIdH5vzOCKp/w7hdjPy3q6PSgJVtqvQ6v9E8k5Ui7
C+DF6KvJUiMJSY5sbu2zmm9rKAH5m7FwIDAQAB;"


There are currently 1 domain profiles defined.

Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]>


Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]>

Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]>
```

DMARC 验证

本部分包含以下 CLI 命令：

- dmarcconfig

dmarcconfig

说明

配置 WAAS 设置

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式 - DMARC 验证配置文件

`dmarcconfig` 的批处理格式可以用于创建、编辑或者删除验证配置文件并修改全局设置。

添加 DMARC 验证配置文件

```
dmarcconfig profiles new <name> [options]
```

参数	说明
< 姓名 >	DMARC 配置文件的名称。
[options]	
--rejectpolicy_action	当 DMARC 记录中的策略为 reject 时，AsyncOS 必须采取的邮件操作。可能的值为 “reject”、“quarantine” 或 “none”。
--rejectpolicy_response_code	被拒绝邮件的 SMTP 响应代码。默认值为 550。
--rejectpolicy_response_text	被拒绝邮件的 SMTP 响应文本。默认值为 “#5.7.1 DMARC unauthenticated mail is prohibited”。
--rejectpolicy_quarantine	未通过 DMARC 验证的邮件的隔离区。
--quarantinepolicy_action	当 DMARC 记录中的策略为 quarantine 时， AsyncOS 必须采取的邮件操作。可能的值为 “quarantine” 或 “none”。
--quarantinepolicy_quarantine	未通过 DMARC 验证的邮件的隔离区。
--tempfail_action	对于在 DMARC 验证期间导致临时故障的邮件， AsyncOS 必须采取的邮件操作。可能的值为 “accept” 或 “reject”。
--tempfail_response_code	在出现临时故障的情况下，被拒绝邮件的 SMTP 响应代码。默认值为 451。
--tempfail_response_text	在出现临时故障的情况下，被拒绝邮件的 SMTP 响应文本。默认值为 “#4.7.1 Unable to perform DMARC verification”。

参数	说明
--permfail_action	对于在 DMARC 验证期间导致永久故障的邮件， AsyncOS 必须采取的邮件操作。可能的值为 “accept”或 “reject”。
--permfail_response_code	在出现永久故障的情况下，被拒绝邮件的 SMTP 响应代码。默认值为 550。
--permfail_response_text	在出现永久故障的情况下，被拒绝邮件的 SMTP 响应文本。默认值为 “#5.7.1 DMARC verification failed”。

编辑 DMARC 验证配置文件

```
dmarcconfig profiles edit <name> [options]
```

删除 DMARC 验证配置文件

```
dmarcconfig profiles delete <name>
```

删除所有 DMARC 验证配置文件

```
dmarcconfig profiles clear
```

查看 DMARC 验证配置文件的详细信息

```
dmarcconfig profiles print <name>
```

导出 DMARC 验证配置文件

```
dmarcconfig profiles export <filename>
```

导入 DMARC 验证配置文件

```
dmarcconfig profiles import <filename>
```

更改全局设置

```
dmarcconfig setup [options]
```

选项	说明
--report_schedule	您希望 AsyncOS 生成 DMARC 汇聚报告的时间。
--error_reports	如果 DMARC 汇总报告大小超过 10 MB 或超过 DMARC 记录的 RUA 标记中指定的大小，则将向域所有者发送传输错误报告。
--org_name	生成 DMARC 汇聚报告的实体。必须是域名。
--contact_info	如果收到 DMARC 汇总报告的域所有者希望与生成报告的实体联系，可能需要的其他联系信息，例如，您的组织的客户支持详细信息。
--copy_reports	将所有 DMARC 汇总报告的副本发送到特定用户，例如，对综合报告执行分析的内部用户。输入一个邮件地址或多个地址 （由逗号分隔）。
--bypass_addresslist	跳过来自特定发件人 （地址列表）的邮件的 DMARC 验证。 **注**　可以仅选择使用完整邮件地址创建的地址列表。
--bypass_headers	为包含特定信头字段名称的邮件跳过 DMARC 验证。例如，使用此选项跳过邮件列表和受信任转发器的邮件的 DMARC 验证。输入一个报头或多个报头 （由逗号分隔）。

示例

以下示例展示了如何设置 DMARC 验证配置文件并编辑 DMARC 验证配置文件的全局设置。

```
mail.example.com> dmarcconfig

Number of DMARC Verification Profiles: 1
Daily report generation time is: 00:00
Error reports enabled: No
Reports sent on behalf of:
Contact details for reports:
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: None Specified

Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]> profiles

There are currently 1 DMARC verification profiles defined.

Choose the operation you want to perform:
- NEW - Create a new DMARC verification profile.
- EDIT - Modify a DMARC verification profile.
- DELETE - Delete a DMARC verification profile.
- PRINT - Display DMARC verification profiles.
- IMPORT - Import DMARC verification profiles from a file.
- EXPORT - Export DMARC verification profiles to a file.
- CLEAR - Clear all DMARC verification profiles.
[]> new

Enter the name of the new DMARC verification profile:
[]> dmarc_ver_profile_1

Select the message action when the policy in DMARC record is reject:
1.No Action
2.Quarantine the message
3.Reject the message
[3]> 1

Select the message action when the policy in DMARC record is quarantine:
1.No Action
2.Quarantine the message
[2]> 2

Select the quarantine for messages that fail DMARC verification (when the DMARC policy is
quarantine).
1.Policy
[1]> 1

What SMTP action should be taken in case of temporary failure?
1.Accept
2.Reject
[1]> 2

Enter the SMTP response code for rejected messages in case of temporary failure.
[451]>

Enter the SMTP response text for rejected messages in case of temporary failure.Type
DEFAULT to use the default response text '#4.7.1 Unable to perform
DMARC verification.'
[#4.7.1 Unable to perform DMARC verification.]>
```

```
What SMTP action should be taken in case of permanent failure?
1.Accept
2.Reject
[1]> 2

Enter the SMTP response code for rejected messages in case of permanent failure.
[550]>

Enter the SMTP response text for rejected messages in case of permanent failure.Type
DEFAULT to use the default response text '#4.7.1 Unable to perform
DMARC verification.'
[#5.7.1 DMARC verification failed.]>

There are currently 2 DMARC verification profiles defined.

Choose the operation you want to perform:
- NEW - Create a new DMARC verification profile.
- EDIT - Modify a DMARC verification profile.
- DELETE - Delete a DMARC verification profile.
- PRINT - Display DMARC verification profiles.
- IMPORT - Import DMARC verification profiles from a file.
- EXPORT - Export DMARC verification profiles to a file.
- CLEAR - Clear all DMARC verification profiles.
[]>

Number of DMARC Verification Profiles: 2
Daily report generation time is: 00:00
Error reports enabled: No
Reports sent on behalf of:
Contact details for reports:
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: None Specified

Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]> setup

Would you like to modify DMARC report settings?(Yes/No) [N]> y

Enter the time of day to generate aggregate feedback reports.Use 24-hour format (HH:MM).
[00:00]>

Would you like to send DMARC error reports?(Yes/No) [N]> y

Enter the entity name responsible for report generation.This is added to the DMARC
aggregate reports.
[]> example.com

Enter additional contact information to be added to DMARC aggregate reports.This could be
an email address, URL of a website with additional help, a phone
number etc.
[]> http://dmarc.example.com

Would you like to send a copy of all aggregate reports?(Yes/No) [N]>

Would you like to bypass DMARC verification for an addresslist?(Yes/No) [N]>

Would you like to bypass DMARC verification for specific header fields?(Yes/No) [N]> y


Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
```

```
[]> add

Enter the header field name
[]> List-Unsubscribe

DMARC verification is configured to bypass DMARC verification for messages containing the
following header fields.
1.List-Unsubscribe

Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
- REMOVE - Remove a header field from the list.
[]> add

Enter the header field name
[]> List-ID

DMARC verification is configured to bypass DMARC verification for messages containing the
following header fields.
1.List-Unsubscribe
2.List-ID

Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
- REMOVE - Remove a header field from the list.
[]>

Number of DMARC Verification Profiles: 2
Daily report generation time is: 00:00
Error reports enabled: Yes
Reports sent on behalf of: example.com
Contact details for reports: http://dmarc.example.com
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: List-Unsubscribe, List-ID

Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]>
```

DNS

本部分包含以下 CLI 命令：

- dig
- dnsconfig
- dnsflush
- dnshostprefs
- dnslistconfig
- dnslisttest
- dnsstatus

dig

说明

在 DNS 服务器上查找记录。

Usage

提交：此命令不需要 “提交”。
集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。
批处理命令：此命令支持批处理格式。

批处理格式

`dig` 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 在 DNS 服务器上查找记录

```
dig [options] [@<dns_ip>] [qtype] <hostname>
```

- 在 DNS 服务器上为特定 IP 地址执行反向查找

```
dig -x <reverse_ip> [options] [@<dns_ip>]
```

下面是 `dig` 命令的批处理格式可用的选项

```
-s <source_ip>  Specify the source IP address.

-t              Make query over TCP.

-u              Make query over UDP (default).


dns_ip - Query the DNS server at this IP address.

qtype - Query type: A, PTR, CNAME, MX, SOA, NS, TXT.

hostname - Record that user want to look up.

reverse_ip - Reverse lookup IP address.

dns_ip - Query the DNS server at this IP address.
```

示例

以下示例明确指定要进行查找的 DNS 服务器。

```
mail.com> dig @111.111.111.111 example.com MX
```

```
; <<>> DiG 9.4.3-P2 <<>> @111.111.111.111 example.com MX
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18540
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; QUESTION SECTION:
;example.com.IN      MX

;; ANSWER SECTION:
mexample.com.10800   IN      MX      10 mexample.com.

;; AUTHORITY SECTION:
example.com.10800   IN      NS      test.example.com.

;; ADDITIONAL SECTION:
example.com.10800 IN      A       111.111.111.111
example.com.10800 IN      AAAA    2620:101:2004:4201::bd
example.com.300     IN      A       111.111.111.111

;; Query time: 6 msec
;; SERVER: 10.92.144.4#53(10.92.144.4)
;; WHEN: Fri Dec  9 23:37:42 2011
;; MSG SIZE  rcvd: 143
```

注　如果在使用此命令时未明确指定 DNS 服务器，则 `dig` 命令会过滤掉 Authority 和 Additional 部分的信息。

dnsconfig

说明

配置 DNS 设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式

`dnsconfig` 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 配置 DNS 以使用本地名称服务器缓存：

```
dnsconfig parent new <ns_ip> <priority>
```

命令参数：

- `<ns_ip>` - 名称服务器的 IP 地址。以逗号分隔多个 IP 地址。
- `<priority>` - 此条目的优先级。

- 删除本地名称服务器缓存：

```
dnsconfig parent delete <ns_ip>
```

- 配置备用 DNS 缓存用于特定域：

```
dnsconfig alt new <domains> <ns_ip>
```

注 当使用互联网根名称服务器时，无法使用。

命令参数：

  - <ns_ip> - 名称服务器的 IP 地址。以逗号分隔多个 IP 地址。
  - <domains> - 逗号分隔的域列表。

- 删除特定域的备用 DNS 缓存：

```
dnsconfig alt delete <domain>
```

- 配置 DNS 以使用互联网根名称服务器：

```
dnsconfig roots new <ns_domain> <ns_name> <ns_ip>
```

名称服务器参数：

  - <ns_domain> - 要覆盖的域。
  - <ns_name> - 名称服务器的名称。
  - <ns_ip> - 名称服务器的 IP 地址。

注 可以通过指定该域的备用名称服务器覆盖某些特定域。

- 删除名称服务器：

```
dnsconfig roots delete <ns_domain> [ns_name]
```

注 当删除时，如果未指定 ns_name，则将删除该域的所有名称服务器。

- 清除所有 DNS 设置并将系统自动配置为使用互联网根服务器：

```
dnsconfig roots
```

显示当前的 DNS 设置。

```
dnsconfig print
```

示例

每个用户指定的 DNS 服务器需要以下信息：

- 主机名
- IP 地址
- （仅备用服务器）的域权威

在 dnsconfig 命令内可用的四个子命令：

表 3-5　　dnsconfig 命令的子命令

语法	说明
new	添加新的备用 DNS 服务器，用于特定域或本地 DNS 服务器。
delete	删除备用服务器或本地 DNS 服务器。
edit	修改备用服务器或本地 DNS 服务器。
setup	在互联网根 DNS 服务器或本地 DNS 服务器之间切换。

```
mail3.example.com> dnsconfig


Currently using the Internet root DNS servers.

Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]> setup

Do you want the Gateway to use the Internet's root DNS servers or would you like
it to use your own DNS servers?
1.Use Internet root DNS servers
2.Use own DNS cache servers
[1]> 1

Choose the IP interface for DNS traffic.
1.Auto
2.Management (10.92.149.70/24: mail3.example.com)
[1]>

Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>

Enter the minimum TTL in seconds for DNS cache.
[1800]>


Currently using the Internet root DNS servers.

Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
```

```
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

添加特定域的备用 DNS 服务器

您可以配置设备以便为所有 DNS 查询使用互联网根服务器 （特定本地域除外）。

```
mail3.example.com> dnsconfig

Currently using the Internet root DNS servers.

No alternate authoritative servers configured.

Choose the operation you want to perform:
- NEW - Add a new server.
- SETUP - Configure general settings.
[]> new

Please enter the domain this server is authoritative for.(Ex: "com").
[]> example.com

Please enter the fully qualified hostname of the DNS server for the domain "example.com".
(Ex: "dns.example.com").
[]> dns.example.com

Please enter the IP address of dns.example.com.
[]> 10.1.10.9


Currently using the Internet root DNS servers.

Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

使用您自己的 DNS 缓存服务器

您可以配置设备使用您自己的 DNS 缓存服务器。

```
mail3.example.com> dnsconfig


Currently using the Internet root DNS servers.

Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]> setup

Do you want the Gateway to use the Internet's root DNS servers or would you like
it to use your own DNS servers?
1.Use Internet root DNS servers
```

```
2.Use own DNS cache servers
[1]> 2

Please enter the IP address of your DNS server.
Separate multiple IPs with commas.
[]> 10.10.200.03

Please enter the priority for 10.10.200.3.
A value of 0 has the highest priority.
The IP will be chosen at random if they have the same priority.
[0]> 1

Choose the IP interface for DNS traffic.
1.Auto
2.Management (192.168.42.42/24)
3.PrivateNet (192.168.1.1/24: mail3.example.com)
4.PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1

Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>

Enter the minimum TTL in seconds for DNS cache.
[1800]>


Currently using the local DNS cache servers:
1.Priority: 1  10.10.200.3

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

dnsflush

说明

清除 DNS 缓存的所有条目。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> dnsflush
确认清空所有DNS缓存?[N]> Y
```

dnshostprefs

说明

配置 IPv4/IPv6 DNS 首选项。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> dnshostprefs


Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]> new

Enter the domain you wish to configure.
[]> example.com

How should the appliance sort IP addresses for this domain?
1.Prefer IPv4
2.Prefer IPv6
3.Require IPv4
4.Require IPv6
[2]> 3



Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]> setdefault

How should the appliance sort IP addresses?
1.Prefer IPv4
2.Prefer IPv6
3.Require IPv4
4.Require IPv6
[2]> 1



Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]>
```

dnslistconfig

说明

配置 DNS 列表服务支持。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> dnslistconfig

Current DNS List Settings:
Negative Response TTL:  1800 seconds
DNS List Query Timeout:  3 seconds

Choose the operation you want to perform:
- SETUP - Configure general settings.
[]> setup

Enter the cache TTL for negative responses in seconds:
[1800]> 1200

Enter the query timeout in seconds:
[3]>

Settings updated.

Current DNS List Settings:
Negative Response TTL:  1200 seconds
DNS List Query Timeout:  3 seconds

Choose the operation you want to perform:
- SETUP - Configure general settings.
[]>
```

dnslisttest

说明

对基于 DNS 的列表服务进行 DNS 查找测试。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> dnslisttest

Enter the query server name:
[]> mail4.example.com

Enter the test IP address to query for:
[127.0.0.2]> 10.10.1.11

Querying:  10.10.1.11.mail4.example.com
Result:  MATCHED
```

dnsstatus

说明

显示 DNS 统计信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> dnsstatus

Status as of: Mon Apr 18 10:58:07 2005 PDT

Counters:                    Reset          Uptime        Lifetime
  DNS Requests               1,115           1,115           1,115
  Network Requests             186             186             186
  Cache Hits                 1,300           1,300           1,300
  Cache Misses                   1               1               1
  Cache Exceptions               0               0               0
  Cache Expired                185             185             185
```

一般管理/管理/故障排除

本部分包含以下 CLI 命令：

- addressconfig
- adminaccessconfig
- certconfig
- 日期
- 诊断
- diskquotaconfig

- ecconfig
- ecstatus
- ecupdate
- encryptionconfig
- encryptionstatus
- encryptionupdate
- featurekey
- featurekeyconfig
- generalconfig
- healthcheck
- healthconfig
- ntpconfig
- reboot
- repengstatus
- repengstatus
- 恢复
- resumedel
- resumelistener
- revert
- settime
- settz
- shutdown
- sshconfig
- 状态
- supportrequest
- supportrequeststatus
- supportrequestupdate
- suspend
- suspenddel
- suspendlistener
- tcpservices
- techsupport
- tlsverify
- 跟踪
- trackingconfig
- updateconfig
- updatenow
- upgrade

- version
- wipedata

另请参阅虚拟设备管理，（第 3-285 页）。

addressconfig

说明

addressconfig命令用于配置 “发件人：” 地址信头。您可以指定 “发件人：” 地址的显示、用户和域名称。您也可以选择将虚拟网关域用于域名。为 AsyncOS 生成的邮件使用 addressconfig 命令，用于以下环境：

- 防病毒通知
- 退回
- DMARC 反馈报告
- 通知 （notify() 和 notify-copy() 过滤操作）
- 隔离区邮件 （和隔离区管理中的 “发送副本”）
- 报告
- 所有其他邮件

在下面的示例中，通知的 “发件人：” 地址从 Mail Delivery System [MAILER-DAEMON@domain]（默认）更改为 Notifications [Notification@example.com]

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> addressconfig

Current anti-virus from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current bounce from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current notify from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current quarantine from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current DMARC reports from: "DMARC Feedback" <MAILER-DAEMON@domain>
Current all other messages from: "Mail Delivery System" <MAILER-DAEMON@domain>

Choose the operation you want to perform:
- AVFROM - Edit the anti-virus from address.
- BOUNCEFROM - Edit the bounce from address.
- NOTIFYFROM - Edit the notify from address.
- QUARANTINEFROM - Edit the quarantine bcc from address.
- DMARCFROM - Edit the DMARC reports from address.
- OTHERFROM - Edit the all other messages from address.
[]> notifyfrom

Please enter the display name portion of the "notify from" address
```

```
["Mail Delivery System"]> Notifications

Please enter the user name portion of the "notify from" address
[MAILER-DAEMON]> Notification

Do you want the virtual gateway domain used for the domain?[Y]> n

Please enter the domain name portion of the "notify from" address
[]> example.com

Current anti-virus from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current bounce from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current notify from: Notifications <Notification@example.com>
Current quarantine from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current DMARC reports from: "DMARC Feedback" <MAILER-DAEMON@domain>
Current all other messages from: "Mail Delivery System" <MAILER-DAEMON@domain>

Choose the operation you want to perform:
- AVFROM - Edit the anti-virus from address.
- BOUNCEFROM - Edit the bounce from address.
- NOTIFYFROM - Edit the notify from address.
- QUARANTINEFROM - Edit the quarantine bcc from address.
- DMARCFROM - Edit the DMARC reports from address.
- OTHERFROM - Edit the all other messages from address.
[]>
```

adminaccessconfig

说明

使用 adminaccessconfig 命令可以配置：

- 管理员的登录消息 （欢迎信息）。
- 对设备管理界面的基于 IP 的访问。
- Web 界面跨站点请求伪造保护。
- 在 HTTP 请求中使用主机信头的选项。
- Web 界面和 CLI 会话不活动超时。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式

adminaccessconfig 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 选择是否允许访问所有 IP 地址或限制对特定 IP 地址/子网/范围的访问。

```
adminaccessconfig ipaccess <all/restrict/proxyonly/proxy>
```

- 添加新的 IP 地址/子网/范围

```
adminaccessconfig ipaccess new <address>
```

- 编辑现有 IP 地址/子网/范围

```
adminaccessconfig ipaccess edit <oldaddress> <newaddress>
```

- 删除现有 IP 地址/子网/范围

```
adminaccessconfig ipaccess delete <address>
```

- 打印 IP 地址/子网/范围的列表

```
adminaccessconfig ipaccess print
```

- 删除所有现有 IP 地址/子网/范围

```
adminaccessconfig ipaccess clear
```

- 打印登录标语

```
adminaccessconfig banner print
```

- 从设备上的文件导入登录标语

```
adminaccessconfig banner import <filename>
```

- 删除现有登录标语

```
adminaccessconfig banner clear
```

- 打印欢迎信息

```
adminaccessconfig welcome print
```

- 从设备上的文件导入欢迎标语

```
adminaccessconfig welcome import <filename>
```

- 删除现有欢迎标语

```
adminaccessconfig welcome clear
```

- 导出欢迎标语

```
adminaccessconfig welcome export <filename>
```

- 添加允许的代理 IP 地址

```
adminaccessconfig ipaccess proxylist new <address>
```

- 编辑允许的代理 IP 地址

```
adminaccessconfig ipaccess proxylist edit <oldaddress> <newaddress>
```

- 删除允许的代理 IP 地址

```
adminaccessconfig ipaccess proxylist delete <address>
```

- 删除所有现有允许的代理 IP 地址

```
adminaccessconfig ipaccess proxylist clear
```

- 配置包含源 IP 地址的信头名称

```
adminaccessconfig ipaccess proxy-header <header name>
```

- 启用或禁用 Web 界面跨站点请求伪造保护

```
adminaccessconfig csrf <enable|disable>
```

- 检查 Web 界面跨站点请求伪造保护是否已启用

```
adminaccessconfig csrf print
```

- 配置 Web 界面会话超时

```
adminaccessconfig timeout gui <value>
```

- 配置 CLI 会话超时

```
adminaccessconfig timeout gui <value>
```

示例 - 配置网络访问列表

您可以控制用户从哪些 IP 地址访问邮件安全设备。用户可以从任意具有您定义的访问列表中 IP 地址的计算机访问设备。当创建网络访问列表时，您可以指定 IP 地址、子网或 CIDR 地址。

如果在网络访问列表中未包括您当前计算机的 IP 地址，则 AsyncOS 会显示一个警告。如果当前计算机的 IP 地址不在列表中，则在您提交更改后将无法访问设备。

在下面的示例中，对设备的网络访问限定为两组 IP 地址：

```
mail.example.com> adminaccessconfig

Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]> ipaccess

Current mode: Allow All.
Please select the mode:
- ALL - All IP addresses will be allowed to access the administrative interface.
- RESTRICT - Specify IP addresses/Subnets/Ranges to be allowed access.
- PROXYONLY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy.
- PROXY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy or
directly.
[]> restrict


List of allowed IP addresses/Subnets/Ranges:


Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
[]> new

Please enter IP address, subnet or range.
[]> 192.168.1.2-100


List of allowed IP addresses/Subnets/Ranges:

1.192.168.1.2-100

Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
- EDIT - Modify an existing entry.
- DELETE - Remove an existing entry.
- CLEAR - Remove all the entries.
[]> new

Please enter IP address, subnet or range.
[]> 192.168.255.12


List of allowed IP addresses/Subnets/Ranges:

1.192.168.1.2-100
2.192.168.255.12

Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
- EDIT - Modify an existing entry.
- DELETE - Remove an existing entry.
- CLEAR - Remove all the entries.
[]>
```

```
Warning: The host you are currently using [72.163.202.175] is not included in the User
Access list.Excluding it will prevent your
host from connecting to the administrative interface.Are you sure you want to
continue?[N]> Y

Current mode: Restrict.
Please select the mode:
- ALL - All IP addresses will be allowed to access the administrative interface.
- RESTRICT - Specify IP addresses/Subnets/Ranges to be allowed access.
- PROXYONLY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy.
- PROXY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy or
directly.
[]>
```

示例 - 配置登录标语

当用户尝试通过 SSH、Telnet、FTP 或 Web UI 登录到设备时，您可以配置邮件安全设备以显示名为“登录标语”的消息。登录标语是可自定义文本，显示在 CLI 中的登录提示上方，以及 GUI 登录提示右侧。您可以使用登录横幅显示设备的内部安全信息或最佳实践说明。例如，您可以创建简单的通知，说明禁止未经授权使用设备或者关于贵组织审查用户对设备所做更改的权利的详细警告。

登录横幅的最大长度为 2000 个字符，以适合 80x25 控制台。可以从设备上的 `/data/pub/configuration` 目录中的文件来导入登录标语。创建横幅后，提交更改。

在下面的示例中，登录标语 “Use of this system in an unauthorized manner is prohibited”会添加到设备：

```
mail.example.com> adminaccessconfig

Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]> banner

A banner has not been defined.

Choose the operation you want to perform:
- NEW - Create a banner to display at login.
- IMPORT - Import banner text from a file.
[]> new

Enter or paste the banner text here.Enter CTRL-D on a blank line to end.
Use of this system in an unauthorized manner is prohibited.
^D

Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]> banner

Banner: Use of this system in an unauthorized manner is prohibited.
```

```
Choose the operation you want to perform:
- NEW - Create a banner to display at login.
- IMPORT - Import banner text from a file.
- DELETE - Remove the banner.
[]>
```

示例 - 配置 Web 界面和 CLI 会话超时

以下示例会将 Web 界面和 CLI 会话的超时时间设置为 32 分钟。

注 CLI 会话超时仅适用于采用安全外壳 (SSH)、 SCP 的连接以及直接串行连接。在 CLI 会话超时时未确认的配置更改都会丢失。确保在进行配置更改后立即进行确认。

```
mail.example.com> adminaccessconfig

Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]> timeout

Enter WebUI inactivity timeout(in minutes):
[30]> 32

Enter CLI inactivity timeout(in minutes):
[30]> 32


Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]>

mail.example.com> commit

Please enter some comments describing your changes:
[]> Changed WebUI and CLI session timeout values

Do you want to save the current configuration for rollback?[Y]>

Changes committed: Wed Mar 12 08:03:21 2014 GMT
```

注 在提交更改之后，仅在后续登录期间新的 CLI 会话超时才会生效。

certconfig

说明

配置安全证书和密钥。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例 - 在证书中粘贴

在下面的示例中，通过在证书和私钥中粘贴可以安装证书。

```
mail3.example.com> certconfig

Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists

[]> certificate

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3467 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- PRINT - View certificates assigned to services
[]> paste

Enter a name for this certificate profile:
> partner.com

Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgaAxCzAJBgNVBAYTAlBUMRMwEQYD
VQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5ldXJv
bmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZpMB4X
DTk2MDkwNTAzNDI0M1oXDTk2MTAwNTAzNDI0M1owgaAxCzAJBgNVBAYTAlBUMRMw
EQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5l
dXJvbmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMT
EmJydXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNw
L4lYKbpzzlmC5beaQXeQ2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAATAN
BgkqhkiG9w0BAQQFAANBAFqPEKFjk6T6CKTHvaQeEAsX0/8YHPHqH/9AnhSjrwuX
9EBc0n6bVGhN7XaXd6sJ7dym9sbsWxb+pJdurnkxjx4=
-----END CERTIFICATE-----
.
C=PT,ST=Queensland,L=Lisboa,O=Neuronio,
Lda.,OU=Desenvolvimento,CN=brutus.partner.com,emailAddress=admin@example.com
```

```
Paste private key in PEM format (end with '.'):
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNwL4lYKbpzzlmC5beaQXeQ
2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAAQJBALjkK+jc2+iihI98riEF
oudmkNziSRTYjnwjx8mCoAjPWviB3c742eO3FG4/soi1jD9A5alihEOXfUzloenr
8IECIQD3B5+0l+68BA/6d76iUNqAAV8djGTzvxnCxycnxPQydQIhAMXt4trUI3nc
a+U8YL2HPFA3gmhBsSICbq2OptOCnM7hAiEA6Xi3JIQECOb8YwkRj29DU3/4WYD7
WLPgsQpwo1GuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IZmxdcLpRcpslpeWBBAiEA
6/5B8J0GHdJq89FHwEG/H2eVVUYu5y/aD6sgcm+0Avg=
-----END RSA PRIVATE KEY-----
.

Do you want to add an intermediate certificate?[N]> n


List of Certificates
Name       Common Name           Issued By             Status         Remaining
--------  -------------------  --------------------  -------------  ---------
partner.c brutus.partner.com   brutus.partner       Active        30 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3467 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>


Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists

[]>

mail3.example.com> commit
Please enter some comments describing your changes:
[]> Installed certificate and key for receiving, delivery, and https

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

示例 - 创建自签名证书

在下面的示例中，会创建自签名证书。

```
mail3.example.com> certconfig


Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists

[]> certificate

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
partner.c  brutus.neuronio.pt    brutus.neuronio.pt    Expired        -4930
```

```
days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3467 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]> new

1.Create a self-signed certificate and CSR
2.Create a self-signed SMIME certificate and CSR
[1]> 1

Enter a name for this certificate profile:
> example.com

Enter Common Name:
> example.com

Enter Organization:
> Example

Enter Organizational Unit:
> Org

Enter Locality or City:
> San Francisoc

Enter State or Province:
> CA

Enter Country (2 letter code):
> US

Duration before expiration (in days):
[3650]>

1.1024
2.2048
Enter size of private key:
[2]>

Do you want to view the CSR?[Y]> y

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDELMAkGA1UEBhMCVVMxFDASBgNVBAMTC2V4YW1wbGUuY29t
MRYwFAYDVQQHEw1TYW4gRnJhbmNpc29jMRAwDgYDVQQKEwdleGFtcGxlMQswCQYD
VQQIEwJDQTEMMAoGA1UECxMDb3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA+NwamZyX7VgTZka/x1I5HHrN9V2MPKXoLq7FjzUtiIDwznElrKIuJovw
Svonle6GvFlUHfjv8B3WobOzk5Ny6btKjwPrBfaY+qr7rzM4lAQKHM+P6l+lZnPU
P05N9RCkLP4XsUuyY6Ca1WLTiPIgaq2fR8Y0JX/kesZcGOqlde66pN+xJIHHYadD
oopOgqi6SLNfAzJu/HEu/fnSujG4nhF0ZGlOpVUx4fg33NwZ4wVl0XBk3GrOjbbA
ih9ozAwfNzxb57amtxEJk+pW+co3uEHLJIOPdih9SHzn/UVU4hiu8rSQR19sDApp
kfdWcfaDLF9tnQJPWSYoCh0USgCc8QIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEB
AGiVhyMAZuHSv9yA08kJCmrgO89yRlnDUXDDo6IrODVKx4hHTiOanOPu1nsThSvH
7xV4xR35T/QV0U3yPrL6bJbbwMySOLIRTjsUcwZNjOE1xMM5EkBM2BOI5rs4l59g
FhHVejhG1LyyUDL0U82wsSLMqLFH1IT63tzwVmRiIXmAu/lHYci3+vctb+sopnN1
lY1OIuj+EgqWNrRBNnKXLTdXkzhELOd8vZEqSAfBWyjZ2mECzC7SG3evqkw/OGLk
AilNXHayiGjeY+UfWzF/HBSekSJtQu6hIv6JpBSY/MnYU4tllExqD+GX3lru4xc4
zDas2rS/Pbpn73Lf503nmsw=
```

```
-----END CERTIFICATE REQUEST-----

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  ------------------- --------------------  -------------  ---------
example.c  example.com           example.com           Valid          3649 days
partner.c  brutus.partner.com   brutus.partner.com  Valid         30 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3467 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>
```

示例 - 创建自签名 S/MIME 签名证书

以下示例展示如何创建自签名 S/MIME 证书以便为邮件签名。

```
vm10esa0031.qa> certconfig


Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3329 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- PRINT - View certificates assigned to services
[]> new

1.Create a self-signed certificate and CSR
2.Create a self-signed SMIME certificate and CSR
[1]> 2

Enter a name for this certificate profile:
> smime_signing

Enter Common Name:
> CN

Enter Organization:
> ORG

Enter Organizational Unit:
> OU

Enter Locality or City:
> BN
```

```
Enter State or Province:
> KA

Enter Country (2 letter code):
> IN

Duration before expiration (in days):
[3650]>

1.1024
2.2048
Enter size of private key:
[2]>

Enter email address for 'subjectAltName' extension:
[]> admin@example.com

Add another member?[Y]> n

Begin entering domain entries for 'subjectAltName'.

Enter the DNS you want to add.
[]> domain.com

Add another member?[Y]> n

Do you want to view the CSR?[Y]> n

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
smime_sig  CN                    CN                    Valid          3649 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3329 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>
```

日期

说明

显示当前日期和时间。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> date

Tue Mar 10 11:30:21 2015 GMT
```

诊断

说明

使用 diagnostic 命令可以：

- 使用各种实用程序排除硬件和网络问题
- 检查 RAID 状态
- 显示 ARP 缓存
- 清除 LDAP、 DNS 和 ARP 缓存
- 发送 SMTP 测试邮件

使用 diagnostic 命令

以下命令在 diagnostic 子菜单内可用：

表 3-6　　diagnostic 子命令

选项	子命令	可用性
RAID	1.Run disk verify	仅在 C30 和 C60 上可用。
	2.Monitor tasks in progress	
	3.Display disk verify verdict	
DISK_USAGE（已弃用）	无子命令	此命令已被弃用。而是要使用 diskquotaconfig 命令。
网络	FLUSH	C 系列、 X 系列和 M 系列
	ARPSHOW	
	SMTPPING	
	TCPDUMP	
REPORTING	DELETEDB	C 系列、 X 系列和 M 系列
	DISABLE	
TRACKING	DELETEDB	C 系列、 X 系列和 M 系列
	DEBUG	
RELOAD	无子命令	C 系列、 X 系列和 M 系列

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令支持批处理格式。

批处理格式

诊断命令的批处理量格式可用于检查 RAID 状态、清除缓存和显示 ARP 缓存中的内容。要作为批处理命令调用，请使用以下格式：

使用批处理格式执行以下操作：

- 检查 RAID 状态

```
diagnostic raid
```

- 显示 ARP 缓存的内容

```
diagnostic network arpshow
```

- 显示 NDP 缓存的内容

```
diagnostic network ndpshow
```

- 清除 LDAP、 DNS、 ARP 和 NDP 缓存

```
diagnostic network flush
```

- 重置并删除报告数据库

```
diagnostic reporting deletedb
```

- 启用报告后台守护程序

```
diagnostic reporting enable
```

- 禁用报告后台守护程序

```
diagnostic reporting disable
```

- 重置并删除该跟踪数据库

```
diagnostic tracking deletedb
```

- 重置对初始制造商值的配置

```
diagnostic reload
```

示例：显示和清除缓存

以下示例显示有关用于显示 ARP 缓存的内容以及刷新所有网络相关缓存的诊断命令。

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[]> network


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> arpshow

System ARP cache contents:

(10.76.69.3) at 00:1e:bd:28:97:00 on em0 expires in 1193 seconds [ethernet]
(10.76.69.2) at 00:1e:79:af:f4:00 on em0 expires in 1192 seconds [ethernet]
(10.76.69.1) at 00:00:0c:9f:f0:01 on em0 expires in 687 seconds [ethernet]
(10.76.69.149) at 00:50:56:b2:0e:2b on em0 permanent [ethernet]


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> flush

Flushing LDAP cache.
Flushing DNS cache.
Flushing system ARP cache.
10.76.69.3 (10.76.69.3) deleted
10.76.69.2 (10.76.69.2) deleted
10.76.69.1 (10.76.69.1) deleted
10.76.69.149 (10.76.69.149) deleted
Flushing system NDP cache.
fe80::250:56ff:feb2:e2d%em2 (fe80::250:56ff:feb2:e2d%em2) deleted
fe80::250:56ff:feb2:e2c%em1 (fe80::250:56ff:feb2:e2c%em1) deleted
fe80::250:56ff:feb2:e2b%em0 (fe80::250:56ff:feb2:e2b%em0) deleted

Network reset complete.
```

示例：验证到另一台邮件服务器的连接性

以下示例显示用于检查到另一台邮件服务器的连接性的诊断命令。您可以通过发送邮件或 ping 服务器的方式测试邮件服务器。

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
```

```
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[]> network


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> smtpping

Enter the hostname or IP address of the SMTP server:
[mail.example.com]> mail.com

The domain you entered has MX records.
Would you like to select an MX host to test instead?[Y]> y

Select an MX host to test.
1. mx00.gmx.com
2. mx01.gmx.com
[1]>

Select a network interface to use for the test.
1.Management
2. auto
[2]> 1

Do you want to type in a test message to send?If not, the connection will be tested but no
email will be sent.[N]>

Starting SMTP test of host mx00.gmx.com.
Resolved 'mx00.gmx.com' to 74.208.5.4.
Unable to connect to 74.208.5.4.
```

示例：将设备配置重置为初始制造商值

以下示例显示如何将您的设备配置重置为初始制造商值。

```
mail.example.com> diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.

[]> reload

This command will remove all user settings and reset the entire device.

If this is a Virtual Appliance, all feature keys will be removed,
and the license must be reapplied.
Are you sure you want to continue?[N]> Y
Are you *really* sure you want to continue?[N]> Y
Do you want to wipe also?[N]> Y
```

diskquotaconfig

查看或配置报告和跟踪、隔离区、日志文件、数据包捕获和配置文件的磁盘空间分配。

请参阅 《*思科邮件安全设备 AsyncOS 用户指南*》了解有关此功能的完整信息。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

```
diskquotaconfig <feature> <quota> [<feature> <quota> [<feature> <quota>[<feature>
<quota>]]]
```

Valid values for `<feature>` are `euq`, `pvo`, `tracking`, `reporting`

Valid values for `<quota>` are integers.

示例

```
mail.example.com> diskquotaconfig

     Service                                       Disk Usage(GB)     Quota(GB)
     ------------------------------------------------------------------------------
     Spam Quarantine (EUQ)                         1                  1
     Policy, Virus & Outbreak Quarantines          1                  3
     Reporting                                     5                  10
     Tracking                                      1                  10
     Miscellaneous Files                           5                  30
           System Files Usage : 5 GB
           User Files Usage : 0 GB
     Total                                         13                 54 of 143

Choose the operation you want to perform:
- EDIT - Edit disk quotas
[]> edit

Enter the number of the service for which you would like to edit disk quota:
1.Spam Quarantine (EUQ)
2.Policy, Virus & Outbreak Quarantines
3.Reporting
4.Tracking
5.Miscellaneous Files
[1]> 1

Enter the new disk quota -
[1]> 1

Disk quota for Spam Quarantine (EUQ) changed to 1

     Service                                       Disk Usage(GB)     Quota(GB)
     ------------------------------------------------------------------------------
     Spam Quarantine (EUQ)                         1                  1
     Policy, Virus & Outbreak Quarantines          1                  3
     Reporting                                     5                  10
     Tracking                                      1                  10
```

```
     Miscellaneous Files                              5                 30
           System Files Usage : 5 GB
           User Files Usage : 0 GB
     Total                                            13                54 of 143

Choose the operation you want to perform:
- EDIT - Edit disk quotas
[]>
```

ecconfig

设置或清除用于获取 URL 过滤功能证书的注册客户端。

没有思科支持人员的指导，请不要使用此命令。

条目必须为 <hostname:port> 或 <IPv4 address:port> 格式。端口是可选的。

要指定默认服务器，请输入 ecconfig server default。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可以用于集群中的所有级别。

批处理命令：此命令支持批处理格式。

批处理格式

- 指定非默认注册客户端服务器：

  > ecconfig server *<server_name:port>*

使用默认注册客户端服务器：

> ecconfig server default

示例

```
mail.example.com> ecconfig

Enrollment Server: Not Configured (Use Default)

Choose the operation you want to perform:
- SETUP - Configure the Enrollment Server
[]> setup

Do you want to use non-default Enrollment server?
WARNING: Do not configure this option without the assistance of Cisco Support.
Incorrect configuration can impact the services using certificates from the Enrollment
server.[N]> y


[]> 192.0.2.1


Choose the operation you want to perform:
- SETUP - Configure the Enrollment Server
[]>
```

ecstatus

显示用于获取 URL 过滤功能证书的注册客户端的当前版本。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> ecstatus
Component                Version    Last Updated
Enrollment Client        1.0.2-046  Never updated
```

ecupdate

手动更新用于自动获取 URL 过滤功能证书的注册客户端。通常，这些更新会自动发生。没有思科支持人员的指导，请不要使用此命令。

如果您使用 `force` 参数 (`ecupdate [force]`)，则客户端会更新，即便没有检测到更改。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

```
> ecupdate [force]
```

示例

```
mail.example.com> ecupdate
Requesting update of Enrollment Client.
```

encryptionconfig

配置邮件加密。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

以下示例显示对加密配置文件的修改：

```
mail.example.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> setup

PXE Email Encryption: Enabled
Would you like to use PXE Email Encryption?[Y]>


WARNING: Increasing the default maximum message size(10MB) may result in
decreased performance.Please consult documentation for size recommendations
based on your environment.

Maximum message size for encryption: (Add a trailing K for kilobytes, M for
megabytes, or no letters for bytes.)
[10M]>


Enter the email address of the encryption account administrator
[administrator@example.com]>


IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIPAA                Hosted Service         No          Not Provisioned


Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]> edit

1.HIPAA
Select the profile you wish to edit:
[1]> 1

Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
```

```
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLET - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]> security

1.High Security (Recipient must enter a password to open the encrypted
message, even if credentials are cached ("Remember Me" selected).)
2.Medium Security (No password entry required if recipient credentials are
cached ("Remember Me" selected).)
3.No Password Required (The recipient does not need a password to open the
encrypted message.)
Please enter the envelope security level:
[1]> 1

Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
```

```
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLET - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]> forward

Would you like to enable "Secure Forward"?[N]> y

Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: Yes
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLET - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]>

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIPAA                Hosted Service         No          Not Provisioned


Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
```

```
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]>

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]>
```

encryptionstatus

说明

encryptionstatus 命令显示邮件安全设备上 PXE 引擎和域映射文件的版本，以及上次更新组件的日期和时间。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> encryptionstatus

Component                 Version    Last Updated
PXE Engine                6.7.1      17 Nov 2009 00:09 (GMT)
Domain Mappings File      1.0.0      Never updated
```

encryptionupdate

说明

encryptionupdate 命令请求对邮件安全设备上的 PXE 引擎的更新。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> encryptionupdate

Requesting update of PXE Engine.
```

featurekey

说明

featurekey 命令列出了系统上由密钥启用的所有功能以及与密钥相关的信息。它还允许您使用密钥激活功能或者检查新的功能密钥。

有关虚拟设备，另请参阅 loadlicense 和 showlicense。

Usage

提交：此命令需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

在本示例中，featurekey 命令用于检查新的功能密钥。

```
mail3.example.com> featurekey
Module                          Quantity   Status     Remaining   Expiration Date
Outbreak Filters                1          Active     28 days     Tue Feb 25 06:40:53
2014
IronPort Anti-Spam              1          Dormant    30 days     Wed Feb 26 07:56:57
2014
Sophos Anti-Virus               1          Active     26 days     Sun Feb 23 02:27:48
2014
Bounce Verification             1          Dormant    30 days     Wed Feb 26 07:56:57
2014
Incoming Mail Handling          1          Active     20 days     Sun Feb 16 08:55:58
2014
IronPort Email Encryption       1          Dormant    30 days     Wed Feb 26 07:56:57
2014
RSA Email Data Loss Prevention  1          Active     25 days     Fri Feb 21 10:07:10
2014
McAfee                          1          Dormant    30 days     Wed Feb 26 07:56:57
2014
Choose the operation you want to perform:
- ACTIVATE - Activate a (pending) key.
- CHECKNOW - Check now for new feature keys.
[]> checknow
没有可用的新特性密钥。
```

featurekeyconfig

说明

featurekeyconfig 命令允许您配置计算机，以便自动下载可用密钥和更新计算机上的密钥。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机。

批处理命令：此命令不支持批处理格式。

示例

在本示例中， featurekeyconfig 命令用于启用自动激活和自动检查功能。

```
mail3.example.com> featurekeyconfig

Automatic activation of downloaded keys: Disabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- SETUP - Edit feature key configuration.
[]> setup

Automatic activation of downloaded keys: Disabled
Automatic periodic checking for new feature keys: Disabled

Choose the operation you want to perform:
- AUTOACTIVATE - Toggle automatic activation of downloaded keys.
- AUTOCHECK - Toggle automatic checking for new feature keys.
[]> autoactivate

Do you want to automatically apply downloaded feature keys?[N]> y

Automatic activation of downloaded keys: Enabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- AUTOACTIVATE - Toggle automatic activation of downloaded keys.
- AUTOCHECK - Toggle automatic checking for new feature keys.

[]> autocheck
Do you want to periodically query for new feature keys?[N]> y

Automatic activation of downloaded keys: Enabled
Automatic periodic checking for new feature keys: Enabled
```

generalconfig

说明

generalconfig 命令允许您配置浏览器设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。有关详细信息，请键入命令 `help generalconfig` 查阅联机帮助。

示例 - 配置 Internet Explorer 兼容模式覆盖

以下示例显示如何覆盖 IE 兼容模式：

```
mail.example.com> generalconfig

Choose the operation you want to perform:
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]> ieoverride

    For better web interface rendering, we recommend that you enable Internet
    Explorer Compatibility Mode Override.However, if enabling this feature
    is against your organizational policy, you may disable this feature.

    Internet Explorer Compatibility Mode Override is currently disabled.

Would you like to enable Internet Explorer Compatibility Mode Override?[N]y

Choose the operation you want to perform:
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]>
```

healthcheck

说明

检查您的邮件安全设备的运行状况。运行状况检查分析当前状态日志中的历史数据 （最多三个月），以确定设备的运行状况。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> healthcheck

Analyzing the system to determine current health of the system.
The analysis may take a while, depending on the size of the historical data.

System analysis is complete.
The analysis indicates that the system has experienced the following issue(s)recently:
Entered Resource conservation mode
Delay in mail processing
```

```
High CPU usage
High memory usage

Based on this analysis,
we recommend you to contact Cisco Customer Support before upgrading.
```

healthconfig

说明

配置设备的各个运行状况参数的阈值，例如 CPU 使用情况、工作队列中的最大邮件数等

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> healthconfig


Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> workqueue

Number of messages in the workqueue : 0
Current threshold on the workqueue size : 500
Alert when exceeds threshold : Disabled
Do you want to edit the settings?[N]> y

Please enter the threshold value for number of messages in work queue.
[500]> 550

Do you want to receive alerts if the number of messages in work queue exceeds
threshold value?[N]> n


Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> cpu

Overall CPU usage : 0 %
Current threshold on the overall CPU usage: 85 %
Alert when exceeds threshold : Disabled
Do you want to edit the settings?[N]> y

Please enter the threshold value for overall CPU usage (in percent)
[85]> 90
```

```
Do you want to receive alerts if the overall CPU usage exceeds threshold value?[N]> n


Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> swap

Number of pages swapped from memory in a minute : 0
Current threshold on the number of pages swapped from memory per minute : 5000
Alert when exceeds threshold : Disabled
Do you want to edit the settings?[N]> y

Please enter the threshold value for number of pages swapped from memory in a
minute.
[5000]> 5500

Do you want to receive alerts if number of pages swapped from memory in a
minute exceeds the threshold?[N]> n


Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]>
```

ntpconfig

说明

ntpconfig 命令用于将 AsyncOS 配置为使用网络时间协议 (NTP)，以便将系统时钟与其他计算机同步。可以使用 settime 命令关闭 NTP。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> ntpconfig

Currently configured NTP servers:
1. time.ironport.com

Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should originate.

[]> new
```

```
Please enter the fully qualified hostname or IP address of your NTP server.
[]> ntp.example.com

Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi

Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should
originate.
[]> sourceint

When initiating a connection to an NTP server, the outbound IP address
used is chosen automatically.
If you want to choose a specific outbound IP address,please select
its interface name now.
1.Auto
2.Management (172.19.0.11/24: elroy.run)
3.PrivateNet (172.19.1.11/24: elroy.run)
4.PublicNet (172.19.2.11/24: elroy.run)
[1]> 1
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi

Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should originate.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added new NTP server

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

reboot

说明

重新启动设备。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> reboot

Enter the number of seconds to wait before abruptly closing connections.
[30]>

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

repengstatus

说明

请求信誉引擎的版本信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> repengstatus

  Component                  Last Update                      Version
  Reputation Engine          28 Jan 2014 23:47 (GMT +00:00)   1
  Reputation Engine Tools    28 Jan 2014 23:47 (GMT +00:00)   1
```

恢复

说明

恢复接收和传送。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> resume

Receiving resumed for Listener 1.
Mail delivery resumed.
Mail delivery for individually suspended domains must be resumed individually.
```

resumedel

说明

恢复传输。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> resumedel

Currently suspended domains:
1. domain1.com
2. domain2.com
3. domain3.com

Enter one or more domains [comma-separated] to which you want to resume delivery.
[ALL]> domain1.com, domain2.com

Mail delivery resumed.
```

resumelistener

说明

恢复接收监听程序。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> resumelistener

Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1.All
2.InboundMail
3.OutboundMail
[1]> 1

Receiving resumed.
mail3.example.com>
```

revert

说明

恢复为先前的版本。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all IronPort Spam Quarantine message and end-user safelist/blocklist data



Only the network settings will be preserved.


Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords unmasked)
- exported the IronPort Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots
again to the desired version.
```

```
    Available versions
    ==================
 1.9.1.0-019
Please select an AsyncOS version [1]:
Do you want to continue?[N]>
```

settime

说明

如果您未使用 NTP 服务器，则 settime 命令允许您手动设置时间。该命令会询问您是否要停止 NTP 和手动设置系统时钟。按如下格式输入时间：**MM/DD/YYYY HH:MM:SS**。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> settime

WARNING: Changes to system time will take place immediately
and do not require the user to run the commit command.
Current time 09/23/2001 21:03:53.
This machine is currently running NTP.
In order to manually set the time, NTP must be disabled.
Do you want to stop NTP and manually set the time?[N]> Y

Please enter the time in MM/DD/YYYY HH:MM:SS format.
[]> 09/23/2001 21:03:53

Time set to 09/23/2001 21:03:53.
```

settz

说明

设置本地时区。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> settz

Current time zone: Etc/GMT
Current time zone version: 2010.02.0

Choose the operation you want to perform:
- SETUP - Set the local time zone.
[]> setup

Please choose your continent:
1.Africa
2.America
[ ...]
11.GMT Offset
[2]> 2

Please choose your country:
1.Anguilla
[ ...]
45.United States
46.Uruguay
47.Venezuela
48.Virgin Islands (British)
49.Virgin Islands (U.S.)
[45]> 45

Please choose your timezone:
1.Alaska Time (Anchorage)
2.Alaska Time - Alaska panhandle (Juneau)
[ ...]
21.Pacific Time (Los_Angeles)
[21]> 21

Current time zone: America/Los_Angeles

Choose the operation you want to perform:
- SETUP - Set the local time zone.
[]>
```

shutdown

说明

关闭要关闭电源的系统。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> shutdown

Enter the number of seconds to wait before forcibly closing connections.
[30]>

System shutting down.Please wait while the queue is being closed...

Closing CLI connection.
The system will power off automatically.
Connection to mail.example.com closed.
```

sshconfig

说明

配置 SSH 服务器和用户密钥设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在集群模式下使用。

批处理命令：此命令不支持批处理格式。

重新启动。需要重新启动，更改才会生效。

示例

在以下示例中，为管理员帐户安装了新的公钥：

```
mail.example.com> sshconfig

Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> userkey

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]

Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

以下示例显示了如何编辑 SSH 服务器配置。

```
mail.example.com> sshconfig

Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd

ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1

Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>

Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,c
ast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]>

Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha
1-96,hmac-md5-96]>

Enter the Minimum Server Key Size do you want to use
[1024]>

Enter the KEX Algorithms do you want to use
```

```
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-gr
oup14-sha1,diffie-hellman-group1-sha1]>

ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1

Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>


Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

状态

说明

显示系统状态。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> status

Status as of:               Thu Oct 21 14:33:27 2004 PDT
Up since:                   Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:         Never
System status:              Online
Oldest Message:             4 weeks 46 mins 53 secs

Feature - McAfee:              161 days
[....]
Feature - Outbreak Filters:    161 days

Counters:                               Reset          Uptime        Lifetime
  Receiving
    Messages Received              62,049,822         290,920      62,049,822
    Recipients Received            62,049,823         290,920      62,049,823
  Rejection
    Rejected Recipients             3,949,663          11,921       3,949,663
    Dropped Messages               11,606,037             219      11,606,037
  Queue
    Soft Bounced Events             2,334,552          13,598       2,334,552
  Completion
    Completed Recipients           50,441,741         332,625      50,441,741
  Current IDs
    Message ID (MID)                                                99524480
    Injection Conn. ID (ICID)                                       51180368
    Delivery Conn. ID (DCID)                                        17550674

Gauges:                                 Current
  Connections
    Current Inbound Conn.                     0
    Current Outbound Conn.                   14
Queue
    Active Recipients                         1
    Messages In Work Queue                    0
    Kilobytes Used                           92
    Kilobytes Free                    8,388,516
  Quarantine
    Messages In Quarantine
      Policy, Virus and Outbreak              0
    Kilobytes In Quarantine
      Policy, Virus and Outbreak              0
```

supportrequest

说明

向思科客户支持发送邮件。此命令要求设备可以向互联网发送邮件。故障通知单会自动创建，或者您可以将支持请求与现有故障通知单关联。

要直接从设备访问思科技术支持，您的 Cisco.com 用户 ID 必须与此设备的服务协议合同相关联。要查看当前与您的 Cisco.com 简档相关的服务合同列表，请访问位于 https://sso.cisco.com/autho/forms/CDClogin.html 的 Cisco.com 简档管理器。如果您没有 Cisco.com 用户 ID，则请注册一个。请参阅适用于您的版本的联机帮助或用户指南以了解注册帐户的信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

以下示例显示与现有支持申请单不相关的支持请求。

```
mail.example.com> supportrequest

Please Note:
If you have an urgent issue, please call one of our worldwide Support Centers
(www.cisco.com/support).Use this command to open a technical support request
for issues that are not urgent, such as:
- Request for information.
- Problem for which you have a work-around, but would like an alternative
solution.

Do you want to send the support request to supportrequest@mail.qa?
[Y]>

Do you want to send the support request to additional recipient(s)?
[N]>

Is this support request associated with an existing support ticket?
[N]>

Please select a technology related to this support request:
1.Security - Email and Web
2.Security - Management
[1]> 1

Please select a subtechnology related to this support request:
1.Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - Misclassified
Messages
2.Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - SBRS
3.Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - Other
4.Email Security Appliance - Virtual
[1]> 3

Please select the problem category:
1.Upgrade
2.Operate
3.Configure
4.Install
[1]> 3

Please select a problem sub-category:
1.Error Messages, Logs, Debugs
2.Software Failure
3.Interoperability
4.Configuration Assistance
5.Install, Uninstall or Upgrade
6.Hardware Failure
7.Licensing
8.Data Corruption
9.Software Selection/Download Assistance
10.Password Recovery
```

```
[1]> 5

Please enter a subject line for this support request:
[]> <Subject line for support request>

Please enter a description of your issue, providing as much detail as possible
to aid in diagnosis:
[]> <Description of issue>

It is important to associate all your service contracts with your Cisco.com profile (CCO
ID) in order for you to receive complete access to support and
services from Cisco.Please follow the URLs below to associate your contract coverage on
your Cisco.com profile.If you do not have a CCO ID, please follow
the URL below to create a CCO ID.

How to create a CCO ID:
https://tools.cisco.com/RPF/register/register.do
How to associate your CCO ID with contract:
https://tools.cisco.com/RPFA/profile/profile_management.do
Frequently Asked Question:
http://www.cisco.com/web/ordering/cs_info/faqs/index.html

Select the CCOID
1.New CCOID
[1]>

Please enter the CCOID of the contact person :
[]> your name

The CCO ID may contain alphabets, numbers and '@', '.', '-' and '_' symbols.

Please enter the CCOID of the contact person :
[]> me@example.com

Please enter the name of the contact person :
[]> yourname

Please enter your email address:
[]> me@example.com

Please enter the contract ID:
[]> 1234

Please enter any additional contact information (e.g. phone number):
[]>

Please wait while configuration information is generated...

Do you want to print the support request to the screen?
[N]>
```

supportrequeststatus

说明

显示从思科 TAC 请求支持的支持请求关键字版本信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> supportrequeststatus

Component                 Version    Last Updated
Support Request           1.0        Never updated
```

supportrequestupdate

说明

请求手动更新支持请求关键字，以便从思科 TAC 请求支持。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> supportrequestupdate

Requesting update of Support Request Keywords.
```

suspend

说明

暂停接收和传送。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> suspend

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended for Listener 1.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com>
```

suspenddel

说明

暂停传送。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> suspenddel

Enter the number of seconds to wait before abruptly closing connections.
[30]>

Enter one or more domains [comma-separated] to which you want to suspend delivery.
[ALL]> domain1.com, domain2.com, domain3.com

Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

suspendlistener

说明

暂停接收。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> suspendlistener

Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1.All
2.InboundMail
3.OutboundMail
[1]> 1

Enter the number of seconds to wait before abruptly closing connections.
[30]>

Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

tcpservices

说明

显示流程打开的文件的相关信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.cisco.com> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  euq_webui    - GUI for ISQ
  gui          - GUI process
  hermes       - MGA mail server
  postgres     - Process for storing and querying quarantine data
  splunkd      - Processes for storing and querying Email Tracking data

COMMAND      USER         TYPE NODE   NAME
interface    root         IPv4 TCP    127.0.0.1:53
postgres     pgsql        IPv4 TCP    127.0.0.1:5432
qabackdoo    root         IPv4 TCP    *:8123
```

```
ftpd.main     root         IPv4 TCP    10.1.1.0:21
euq_webui     root         IPv4 TCP    10.1.1.0:83
euq_webui     root         IPv6 TCP    [2001:db8::]:83
gui           root         IPv4 TCP    172.29.181.70:80
gui           root         IPv4 TCP    10.1.1.0:80
gui           root         IPv6 TCP    [2001:db8::]:80
gui           root         IPv4 TCP    172.29.181.70:443
gui           root         IPv4 TCP    10.1.1.0:443
gui           root         IPv6 TCP    [2001:db8::]:443
ginetd        root         IPv4 TCP    172.29.181.70:22
ginetd        root         IPv4 TCP    10.1.1.0:22
ginetd        root         IPv6 TCP    [2001:db8::]:22
ginetd        root         IPv4 TCP    10.1.1.0:2222
ginetd        root         IPv6 TCP    [2001:db8::]:2222
hermes        root         IPv4 TCP    172.29.181.70:25
splunkd       root         IPv4 TCP    127.0.0.1:8089
splunkd       root         IPv4 TCP    127.0.0.1:9997
api_serve     root         IPv4 TCP    10.1.1.0:6080
api_serve     root         IPv6 TCP    [2001:db8::]:6080
api_serve     root         IPv4 TCP    10.1.1.0:6443
api_serve     root         IPv6 TCP    [2001:db8::]:6443
java          root         IPv6 TCP    [::127.0.0.1]:9999
```

techsupport

说明

允许思科 TAC 访问您的系统。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> techsupport

Service Access currently disabled.
Serial Number: XXXXXXXXXXXX-XXXXXXX

Choose the operation you want to perform:
- SSHACCESS - Allow a Cisco IronPort Customer Support representative to remotely access
your system, without establishing a tunnel.
- TUNNEL - Allow a Cisco IronPort Customer Support representative to remotely access your
system, and establish a secure tunnel for communication.
- STATUS - Display the current techsupport status.
[]> sshaccess

A random seed string is required for this operation

1.Generate a random string to initialize secure communication (recommended)
2.Enter a random string
[1]> 1
```

```
Are you sure you want to enable service access?[N]> y

Service access has been ENABLED.Please provide the string:

QT22-JQZF-YAQL-TL8L-8@2L-95

to your Cisco IronPort Customer Support representative.

Service Access currently ENABLED (0 current service logins).
Tunnel option is not active.

Serial Number: XXXXXXXXXXXX-XXXXXXX

Choose the operation you want to perform:
- DISABLE - Prevent customer service representatives from remotely accessing your system.
- STATUS - Display the current techsupport status.
[]>
```

tlsverify

说明

按需建立出站 TLS 连接，并且调试与目的域相关的 TLS 连接问题。要创建连接，请指定要验证的域和目标主机。 AsyncOS 会根据所需的 （验证）TLS 设置检查 TLS 连接

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

`tlsverify` 命令的批处理格式可以用于执行传统 CLI 命令的所有功能，可以检查与指定主机名的 TLS 连接。

```
tlsverify <domain> <hostname>[:<port>]
```

示例

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:
[]> example.com

Enter the destination host to connect to.Append the port (example.com:26) if you are not
connecting on port 25:
[example.com]> mxe.example.com:25

Connecting to 1.1.1.1 on port 25.
Connected to 1.1.1.1 from interface 10.10.10.10.
Checking TLS connection.
```

```
TLS connection established: protocol TLSv1, cipher RC4-SHA.
Verifying peer certificate.
Verifying certificate common name mxe.example.com.
TLS certificate match mxe.example.com
TLS certificate verified.
TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.
TLS verification completed.
```

跟踪

说明

通过系统跟踪邮件流。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> trace

Enter the source IP
[]> 192.168.1.1

Enter the fully qualified domain name of the source IP
[]> example.com

Select the listener to trace behavior on:
1.InboundMail
2.OutboundMail
[1]> 1

Fetching default SenderBase values...
Enter the SenderBase Org ID of the source IP.The actual ID is N/A.
[N/A]>

Enter the SenderBase Reputation Score of the source IP.The actual score is N/A.
[N/A]>

Enter the Envelope Sender address:
[]> pretend.sender@example.net

Enter the Envelope Recipient addresses.Separate multiple addresses by commas.
[]> admin@example.com

Load message from disk?[Y]> n

Enter or paste the message body here.Enter '.' on a blank line to end.
Subject: Hello
This is a test message.
.
```

```
HAT matched on unnamed sender group, host ALL
 - Applying $ACCEPTED policy (ACCEPT behavior).
 - Maximum Message Size:  100M (Default)
 - Maximum Number Of Connections From A Single IP:  1000 (Default)
 - Maximum Number Of Messages Per Connection:  1,000 (Default)
 - Maximum Number Of Recipients Per Message:  1,000 (Default)
 - Maximum Recipients Per Hour:  100 (Default)
 - Use SenderBase For Flow Control:  Yes (Default)
 - Spam Detection Enabled:  Yes (Default)
 - Virus Detection Enabled:  Yes (Default)
 - Allow TLS Connections:  No (Default)

Processing MAIL FROM:
 - Default Domain Processing:  No Change

Processing Recipient List:
Processing admin@ironport.com
 - Default Domain Processing:  No Change
 - Domain Map:  No Change
 - RAT matched on admin@ironport.com, behavior = ACCEPT
 - Alias expansion:  No Change

Message Processing:
 - No Virtual Gateway(tm) Assigned
 - No Bounce Profile Assigned

Domain Masquerading/LDAP Processing:
 - No Changes.

Processing filter 'always_deliver':
Evaluating Rule:   rcpt-to == "@mail.qa"
    Result = False
Evaluating Rule:   rcpt-to == "ironport.com"
    Result = True
Evaluating Rule:   OR
    Result = True
Executing Action:  deliver()

Footer Stamping:
 - Not Performed

Inbound Recipient Policy Processing: (matched on Management Upgrade policy)
Message going to:  admin@ironport.com

AntiSpam Evaluation:
 - Not Spam

AntiVirus Evaluation:
 - Message Clean.
 - Elapsed Time = '0.000 sec'

Outbreak Filter Evaluation:
 - No threat detected

Message Enqueued for Delivery

Would you like to see the resulting message?[Y]> y


Final text for messages matched on policy Management Upgrade
Final Envelope Sender:  pretend.sender@example.doma
Final Recipients:
 - admin@ironport.com
```

```
Final Message Content:

Received: from remotehost.example.com (HELO TEST) (1.2.3.4)
  by stacy.qa with TEST; 19 Oct 2004 00:54:48 -0700
Message-Id: <3i93q9$@Management>
X-IronPort-AV: i="3.86,81,1096873200";
   d="scan'208"; a="0:sNHT0"
Subject: hello

This is a test message.

Run through another debug session?[N]>
```

注　When using `trace`, you must include both the header and the body of the message pasted into the CLI.

trackingconfig

说明

配置跟踪系统。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> trackingconfig

Message Tracking service status: Message Tracking is enabled.

Choose the operation you want to perform:
- SETUP - Enable Message Tracking for this appliance.
[]> setup

Would you like to use the Message Tracking Service?[Y]>

Do you want to use Centralized Message Tracking for this appliance?[N]>

Would you like to track rejected connections?[N]>

Message Tracking service status: Local Message Tracking is enabled.
Rejected connections are currently not being tracked.

Choose the operation you want to perform:
- SETUP - Enable Message Tracking for this appliance.
[]>
```

tzupdate

说明

更新时区规则。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令支持批处理格式。

批处理格式

即便没有检测到更改，`tzupdate` 命令的批处理格式也会强制更新所有时区规则。

```
tzupdate [force]
```

示例

```
mail.example.com> tzupdate

Requesting update of Timezone Rules
```

updateconfig

说明

配置系统更新参数。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

- 配置设备以便从更新服务器下载更新，（第 3-109 页）
- 配置设备以验证更新程序服务器器证书的有效性，（第 3-111 页）
- 配置设备以信任代理服务器通信，（第 3-112 页）

配置设备以便从更新服务器下载更新

在下面的示例中， updateconfig 命令用于配置设备以便从思科服务器下载更新图像，并从本地服务器下载可用 AsyncOS 升级的列表。

```
mail.example.com> updateconfig

Service (images):                                   Update URL:

-------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> setup

For the following services, please select where the system will download updates from:
Service (images):                                    Update URL:

-------------------------------------------------------------------------------------
Feature Key updates
http://downloads.ironport.com/asyncos

1.Use Cisco IronPort update servers (http://downloads.ironport.com)
2.Use own server
[1]>

For the following services, please select where the system will download updates from
(images):
Service (images):                                   Update URL:

-------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers

1.Use Cisco IronPort update servers
2.Use own server
[1]>
```

```
For the following services, please select where the system will download updates from
(images):
Service (images):                                   Update URL:

-------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

1.Use Cisco IronPort update servers
2.Use own server
[1]>

For the following services, please select where the system will download the list of
available
updates from:
Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers

1.Use Cisco IronPort update servers
2.Use own update list
[1]>

For the following services, please select where the system will download the list of
available
updates from:
Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

1.Use Cisco IronPort update servers
2.Use own update list
[1]>

Enter the time interval between checks for new:
    - Timezone rules
    - Enrollment Client Updates (used to fetch certificates for URL Filtering)
    - Support Request updates
Use a trailing 's' for seconds, 'm' for minutes or 'h' for hours.The minimum
valid update time is 30s or enter '0' to disable automatic updates (manual
updates will still be available for individual services).
[5m]>

When initiating a connection to the update server the originating IP interface
is chosen automatically.If you want to choose a specific interface, please
specify it now.
1.Auto
2.Management (10.76.69.149/24: vm30esa0086.ibqa)
[1]>

Do you want to set up a proxy server for HTTP updates for ALL of the following
services:

    - Feature Key updates
    - Timezone rules
    - Enrollment Client Updates (used to fetch certificates for URL Filtering)
    - Support Request updates
    - Cisco IronPort AsyncOS upgrades
[N]>
```

```
Do you want to set up an HTTPS proxy server for HTTPS updates for ALL of the following
services:

    - Feature Key updates
    - Timezone rules
    - Enrollment Client Updates (used to fetch certificates for URL Filtering)
    - Support Request updates
    - Cisco IronPort AsyncOS upgrades
    - SenderBase Network Participation sharing
[N]>

Service (images):                                   Update URL:

-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates  Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

配置设备以验证更新程序服务器器证书的有效性

如果您配置此选项，则每次设备与思科更新程序服务器通信时，更新程序服务器证书的有效性得到验证。如果验证失败，更新未下载，详细信息会记录到更新程序日志中。下面的示例显示如何配置此选项：

```
mail.example.com> updateconfig

Service (images):                                   Update URL:

-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Service (list):                                     Update URL:
```

```
-------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> validate_certificates

Should server certificates from Cisco update servers be validated?
[Yes]>

Service (images):                                   Update URL:
-------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates     Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers

Service (list):                                     Update URL:

-------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

配置设备以信任代理服务器通信

如果您使用的是非透明代理服务器，则可以添加用于将代理证书签署到设备中的 CA 证书。这样，设备就会信任代理服务器通信。下面的示例显示如何配置此选项：

```
...
```

```
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
[]> add

Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
Paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAgTA0tBUjENM.....................................
-----END CERTIFICATE-----
.

Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

updatenow

说明

请求对所有系统服务组件进行更新。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令支持批处理格式。

批处理格式

即便没有检测到更改，updatenow 命令的批处理格式可以用于更新设备上的所有组件。

```
updatenow [force]
```

示例

```
mail3.example.com> updatenow

Success - All component updates requested
```

version

说明

查看系统版本信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> version

Current Version
===============
Product: Cisco C100V Email Security Virtual Appliance
Model: C100V
Version: 9.1.0-019
Build Date: 2015-02-17
Install Date: 2015-02-19 05:17:56
Serial #: 421C73B18CFB05784A83-B03A99E71ED8
BIOS: 6.00
CPUs: 2 expected, 2 allocated
Memory: 6144 MB expected, 6144 MB allocated
RAID: NA
RAID Status: Unknown
RAID Type: NA
BMC: NA
```

wipedata

说明

使用 wipedata 命令可以清除磁盘上的核心文件，并检查最近一次核心转储操作的状态。

注　根据数据的规模，擦除操作可能需要一段时间，因此可能会影响系统性能，直到操作完成。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> wipedata

Wiping data may take a while and can affect system performance till it completes.

Choose the operation you want to perform:
- STATUS - Display status of last command run
- COREDUMP - Wipe core files on disk
[]> coredump

wipedata: In progress
mail.example.com> wipedata

Wiping data may take a while and can affect system performance till it completes.

Choose the operation you want to perform:
- STATUS - Display status of last command run
- COREDUMP - Wipe core files on disk
[]> status

Last wipedata status: Successful
```

upgrade

说明

升级 CLI 命令显示可用升级的列表，并且将 AsyncOS 系统升级到用户指定的版本。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> upgrade

Upgrades available:
1.AsyncOS (***DON'T TOUCH!***)4.0.8 upgrade, 2005-05-09 Build 900
2.AsyncOS 4.0.8 upgrade, 2005-08-12 Build 030
.......
45.SenderBase Network Participation Patch
[45]>

Performing an upgrade will require a reboot of the system after the upgrade is applied.
 Do you wish to proceed with the upgrade?[Y]> Y
```

内容过滤器 (Content Filters)

contentscannerstatus

显示内容扫描引擎版本信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> contentscannerstatus

Component              Version               Last Updated
Content Scanner Tools  11.2.1884.970097      Never updated
```

contentscannerudpate

请求手动更新内容扫描引擎。如果使用 “强制”参数，即使未检测到更改，也会执行更新。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> contentscannerupdate force

Requesting forced update for Content Scanner.
```

LDAP

本部分包含以下 CLI 命令：

ldapconfig

说明

配置 LDAP 服务器。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例 - 创建新的 LDAP 服务器配置文件

在下面的示例中，`ldapconfig` 命令用于定义设备要绑定到的 LDAP 服务器，会配置以下查询：收件人接受情况 （`ldapaccept` 子命令）、路由 （`ldaprouting` 子命令）、伪装 （`masquerade` 子命令）、垃圾邮件隔离区的最终用户身份验证 （`isqauth` 子命令）、垃圾邮件通知的别名合并 （`isqalias` 子命令）。

首先，将会为 `mldapserver.example.com` LDAP 服务器指定 “PublicLDAP” 别名。将查询定向到端口 3268 （默认）。会定义 `example.com` 的搜索库 (`dc=example,dc=com`)，同时还定义收件人接受情况、邮件重新路由和伪装。本示例中的查询与 OpenLDAP 目录配置类似，会使用已到期的 Internet Draft *draft-lachman-laser-ldap-mail-routing-xx.txt* 中定义的 inetLocalMailRecipient 附属对象类，有时也称为 “Laser 规格”。（此草稿的 A 版本包含在 OpenLDAP 源分发中。）请注意，在本示例中，在邮件重新路由查询中用于已查询收件人的备用邮件主机为 `mailForwardingAddress`。确保查询名称区分大小写，必须完全一致才能返回正确的结果。

```
mail3.example.com> ldapconfig

No LDAP server configurations.

Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]> new

Please create a name for this server configuration (Ex: "PublicLDAP"):
[]> PublicLDAP

Please enter the hostname:
[]> myldapserver.example.com

Use SSL to connect to the LDAP server?[N]> n

Select the authentication method to use for this server configuration:
1.Anonymous
2.Password based
[1]> 2

Please enter the bind username:
[cn=Anonymous]>
```

```
Please enter the bind password:
[]>

Connect to LDAP server to validate setting?[Y]

Connecting to the LDAP server, please wait...
Select the server type to use for this server configuration:
1.Active Directory
2.OpenLDAP
3.Unknown or Other
[3]> 1

Please enter the port number:
[3268]> 3268

Please enter the base:
[dc=example,dc=com]> dc=example,dc=com

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
Base: dc=example,dc=com

Choose the operation you want to perform:
- SERVER - Change the server for the query.
- TEST - Test the server configuration.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- CERTAUTH - Configure certificate authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> ldapaccept

Please create a name for this query:
[PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept

Enter the LDAP query string:
[(proxyAddresses=smtp:{a})]> (proxyAddresses=smtp:{a})

Do you want to test this query?[Y]> n

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
```

```
[]> ldaprouting

Please create a name for this query:
[PublicLDAP.routing]> PublicLDAP.routing

Enter the LDAP query string:
[(mailLocalAddress={a})]> (mailLocalAddress={a})

The query requires one of the attributes below.Please make a selection.
  [1] Configure MAILROUTINGADDRESS only - Rewrite the Envelope Recipient (and
leave MAILHOST unconfigured)?
  [2] Configure MAILHOST only - Send the messages to an alternate mail host
(and leave MAILROUTINGADDRESS unconfigured)?
  [3] Configure both attributes
[]> 1

Enter the attribute which contains the full rfc822 email address for the
recipients.
[mailRoutingAddress]> mailRoutingAddress

Do you want to test this query?[Y]> n

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing

Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> masquerade

Please create a name for this query:
[PublicLDAP.masquerade]> PublicLDAP.masquerade

Enter the LDAP query string:
[(mailRoutingAddress={a})]> (mailRoutingAddress={a})

Enter the attribute which contains the externally visible full rfc822 email address.
[]> mailLocalAddress

Do you want the results of the returned attribute to replace the entire friendly portion
of the original recipient?[N]> n

Do you want to test this query?[Y]> n

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
```

```
MASQUERADE: PublicLDAP.masquerade

Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> isqauth

Please create a name for this query:
[PublicLDAP.isqauth]> PublicLDAP.isqauth

Enter the LDAP query string:
[(sAMAccountName={u})]> (sAMAccountName={u})

Enter the list of email attributes.
[]> mail,proxyAddresses

Do you want to activate this query?[Y]> y

Do you want to test this query?[Y]> y

User identity to use in query:
[]> admin@example.com

Password to use in query:
[]> password

LDAP query test results:
LDAP Server: myldapserver.example.com
Query: PublicLDAP.isqauth
User: admin@example.com
Action: match positive

LDAP query test finished.

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
MASQUERADE: PublicLDAP.masquerade
ISQAUTH: PublicLDAP.isqauth [active]

Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]>
```

```
Current LDAP server configurations:
1.PublicLDAP: (myldapserver.example.com:3268)

Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
- EDIT - Modify a server configuration.
- DELETE - Remove a server configuration.
[]>
```

示例 - 配置全局设置

在下面的示例中，会配置 LDAP 全局设置，包括 TLS 连接的证书。

```
mail3.example.com> ldapconfig

No LDAP server configurations.


Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]> setup

Choose the IP interface for LDAP traffic.
1.Auto
2.Management (10.92.145.175/24: esx16-esa01.qa)
[1]> 1

LDAP will determine the interface automatically.

Should group queries that fail to complete be silently treated as having
negative results?[Y]>

The "Demo" certificate is currently configured.You may use "Demo", but this will not be
secure.


1. partner.com
2.Demo
Please choose the certificate to apply:
[1]> 1

No LDAP server configurations.


Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]>
```

ldapflush

说明

清理所有缓存的 LDAP 结果。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> ldapflush

Are you sure you want to flush any cached LDAP results?[N]> y

Flushing cache
mail3.example.com>
```

ldaptest

说明

执行单个 LDAP 查询测试。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

在本示例中，该 `ldaptest` 命令用于为配置的 LDAP 服务器配置测试唯一的收件人接受查询。收件人地址 “admin@example.com” 会通过测试，而收件人地址 “bogus@example.com” 则未通过测试。

```
mail3.example.com> ldaptest

Select which LDAP query to test:
1.PublicLDAP.ldapaccep
[1]> 1
Address to use in query:
[]> admin@example.com

LDAP query test results:

               Query: PublicLDAP.ldapaccept
            Argument: admin@example.com
              Action: pass

LDAP query test finished.
mail3.example.com> ldaptest

Select which LDAP query to test:
1.PublicLDAP.ldapaccep
[1]> 1
```

```
Address to use in query:
[]> bogus@example.com

LDAP query test results:

 Query: PublicLDAP.ldapaccept
 Argument: bogus@example.com
 Action: drop or bounce (depending on listener settings)
 Reason: no matching LDAP record was found
LDAP query test finished.
mail3.example.com>
```

sievechar

说明

设置或禁用用于 Sieve 邮件过滤的字符，如 RFC 3598 中所述。请注意， Sieve 字符仅在 LDAP 接受和 LDAP 重新路由查询中会被识别。系统的其他部分将在完整的邮件地址中操作。

允许的字符为：-_=+/^#

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在本示例中， sievechar 命令用于将 + 定义为在接受和 LDAP 重新路由查询中可被识别的 Sieve 字符。

```
mail3.example.com> sievechar

Sieve Email Filtering is currently disabled.

Choose the operation you want to perform:
- SETUP - Set the separator character.
[]> setup

Enter the Sieve Filter Character, or a space to disable Sieve Filtering.
[]> +

Sieve Email Filter is enabled, using the '+' character as separator.
This applies only to LDAP Accept and LDAP Reroute Queries.

Choose the operation you want to perform:
- SETUP - Set the separator character.
[]>
```

邮件传输配置/监控

本部分包含以下 CLI 命令：

addresslistconfig

说明

配置地址列表。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式

addresslistconfig 命令的批处理格式可以用于创建新的地址列表、编辑现有地址列表、打印地址列表的列表、删除地址列表或者查找地址列表中的冲突地址。

- 添加新的地址列表：

```
addresslistconfig new <name> --descr=<description>
--addresses=<address1,address2,...>
```

- 编辑现有地址列表：

```
addresslistconfig edit <name> --name=<new-name> --descr=<description>
--addresses=<address1,address2,...>
```

- 删除地址列表：

```
addresslistconfig delete <name>
```

- 打印地址列表的列表：

```
addresslistconfig print <name>
```

- 查找地址列表中的冲突地址：

```
addresslistconfig conflicts <name>
```

示例

```
mail.example.com> addresslistconfig

No address lists configured.

Choose the operation you want to perform:
- NEW - Create a new address list.
[]> new

Enter a name for the address list:
> add-list1

Enter a description for the address list:
> This is a sample address list.

Do you want to enter only full Email Addresses?[N]> Y

Enter a comma separated list of addresses:
(e.g.: user@example.com)
> user1@example.com, user2@example.com
```

```
Address list "add-list1" added.

Choose the operation you want to perform:
- NEW - Create a new address list.
- EDIT - Modify an address list.
- DELETE - Remove an address list.
- PRINT - Display the contents of an address list.
- CONFLICTS - Find conflicting entries within an address list.
[]>
```

aliasconfig

说明

配置邮件别名。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式

aliasconfig 命令的批处理格式可以用于添加新的别名表、编辑现有表、打印邮件别名的列表以及导入/导出别名表。要调用为批处理命令，请将以下格式的 `aliasconfig` 命令与下面列出的变量结合使用：

- 添加新的邮件别名：

```
aliasconfig new <domain> <alias> [email_address1] [email_address2] ...
```

注　使用带非现存域的 ‘`aliasconfig new`’命令会导致创建域。

- 编辑现有邮件别名

```
aliasconfig edit <domain> <alias> <email_address1] [email_address2] ...
```

- 显示邮件别名：

```
aliasconfig print
```

- 导入本地别名列表：

```
aliasconfig import <filename>
```

- 导出设备上的别名列表：

```
aliasconfig export <filename>
```

示例

```
mail3.example.com> aliasconfig
Enter address(es) for "customercare".
Separate multiple addresses with commas.
[]> bob@example.com, frank@example.com, sally@example.com

Adding alias customercare: bob@example.com,frank@example.com,sally@example.com
Do you want to add another alias?[N]> n


There are currently 1 mappings defined.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> new

How do you want your aliases to apply?

1.Globally
2.Add a new domain context
3. example.com
[1]> 1

Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
    - "user@domain" - This email address.
    - "user" - This user for any domain
    - "@domain" - All users in this domain.
    - "@.partialdomain" - All users in this domain, or any of its sub domains.
[]> admin

Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com

Adding alias admin: administrator@example.com
Do you want to add another alias?[N]> n


There are currently 2 mappings defined.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
```

```
[]> print

admin: administrator@example.com

[ example.com ]
customercare: bob@example.com, frank@example.com, sally@example.com

There are currently 2 mappings defined.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]>
```

表 3-7　用于配置别名的参数

参数	说明
<domain>	**应用别名的域环境。“全局”指定全球域环境。**
<alias>	要配置的别名名称 全局域环境允许的别名： ‘user@domain’ - 此邮件地址。 ‘user’ - 任何域的此用户。 ‘@domain - 此域中的所有用户。 ‘@.partialdomain’ - 此域或其任意子域中的所有用户。 为特定域环境允许的别名： ‘user’ - 此域环境中的用户 ‘user@domain’ - 此邮件地址
<email_address>	别名映射到的邮件地址。单一别名可以映射到多个邮件地址。
<filename>	导入 / 导出别名表要使用的文件名。

archivemessage

说明

在您的队列中存档旧邮件。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，会存档一封较早的邮件：

```
mail3.example.com> archivemessage

Enter the MID to archive.

[0]> 47

MID 47 has been saved in file oldmessage_47.mbox in the configuration
```

altsrchost

说明

配置虚拟网关 (tm) 映射。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，将 `altsrchost` 表打印出来以显示目前没有任何现有映射。然后，创建两个条目：

- 从名为 `@exchange.example.com` 的组件服务器主机发送的邮件会映射到 PublicNet 接口。
- 来自发件人 IP 地址 192.168.35.35 的邮件会映射到 AnotherPublicNet 接口。

最后，将 `altsrchost` 映射打印出来，以确认并提交更改。

```
mail3.example.com> altsrchost

There are currently no mappings configured.

Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
[]> new

Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping.Partial addresses such as "@example.com" or "user@" are allowed.
[]> @exchange.example.com

Which interface do you want to send messages for @exchange.example.com from?
1.AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2.Management (192.168.42.42/24: mail3.example.com)
3.PrivateNet (192.168.1.1/24: mail3.example.com)
4.PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 4

Mapping for @exchange.example.com on interface PublicNet created.

Choose the operation you want to perform:
- NEW - Create a new mapping.
```

```
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> new

Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping.Partial addresses such as "@example.com" or "user@" are allowed.
[]> 192.168.35.35

Which interface do you want to send messages for 192.168.35.35 from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 1

Mapping for 192.168.35.35 on interface AnotherPublicNet created.

Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> print

1. 192.168.35.35 -> AnotherPublicNet
2. @exchange.example.com -> PublicNet

Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]>
mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added 2 altsrchost mappings

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

bounceconfig

说明

配置退回行为。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，会使用 bounceconfig 命令创建名为 bounceprofile 的退回配置文件。在此配置文件，所有硬退回邮件均发送到备用地址 bounce-mailbox@example.com。启用延迟警告邮件。将向每个收件人发送一封警告邮件，并且接受了警告邮件之间 4 小时 （14400 秒）的默认值。

```
mail3.example.com> bounceconfig

Current bounce profiles:
1.Default

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
[]> new

Please create a name for the profile:
[]> bounceprofile

Please enter the maximum number of retries.
[100]> 100

Please enter the maximum number of seconds a message may stay in the queue before being
hard bounced.

[259200]> 259200

Please enter the initial number of seconds to wait before retrying a message.
[60]> 60

Please enter the maximum number of seconds to wait before retrying a message.
[3600]> 3600

Do you want a message sent for each hard bounce?(Yes/No/Default) [Y]> y

Do you want bounce messages to use the DSN message format?(Yes/No/Default) [Y]> y

If a message is undeliverable after some interval, do you want to send a delay warning
message?(Yes/No/Default) [N]> y

Please enter the minimum interval in seconds between delay warning messages.
[14400]> 14400

Please enter the maximum number of delay warning messages to send per
recipient.
[1]> 1

Do you want hard bounce and delay warning messages sent to an alternate address, instead
of the sender?[N]> y

Please enter the email address to send hard bounce and delay warning.
[]> bounce-mailbox@example.com

Current bounce profiles:
```

```
1. Default
2. bounceprofile

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
[]>
mail3.example.com>
```

编辑默认退回配置文件

您还可以编辑默认的退回配置文件。在本示例中，将默认配置文件编辑为将 `maximum number of seconds to wait before retrying unreachable hosts` 从 3600 秒（1 小时）增加到 10800 秒（3 小时）：

```
mail3.example.com> bounceconfig

Current bounce profiles:
1. Default
2. bounceprofile

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
[]> edit

Please enter the number of the profile to edit:
[]> 2

Please enter the maximum number of retries.
[100]>

Please enter the maximum number of seconds a message may stay in the queue before being
hard bounced.
[259200]>

Please enter the initial number of seconds to wait before retrying a message.
[60]>

Please enter the maximum number of seconds to wait before retrying a message.
[3600]> 10800

Do you want a message sent for each hard bounce?(Yes/No/Default)[Y]>

Do you want bounce messages to use the DSN message format?(Yes/No/Default) [N]>

If a message is undeliverable after some interval, do you want to send a delay warning
message?(Yes/No/Default)[N]>

Do you want hard bounce messages sent to an alternate address, instead of the sender?[Y]>

Please enter the email address to send hard bounce.
[bounce-mailbox@example.com]>

Current bounce profiles:
1. Default
2. bounceprofile
```

```
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
```

将退回配置文件应用到监听程序

在配置完退回配置文件后，您可以使用 `listenerconfig -> bounceconfig` 命令并提交更改来为每个监听程序应用配置文件。

注　可以基于接收邮件所在的监听程序来应用退回配置文件。但是，此监听程序与该邮件的最终传输方式没有关系。

在本示例中，会编辑 OutboundMail 专用监听程序，并且名为 **bouncepr1** 的退回配置文件会应用于该监听程序。

```
mail3.example.com> listenerconfig

Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit

Enter the name or number of the listener you wish to edit.
[]> 2

Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> bounceconfig

Please choose a bounce profile to apply:
1. Default
2. bouncepr1
3. New Profile
```

```
[1]> 2

Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: bouncepr1
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>

Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Enabled the bouncepr1 profile to the Outbound mail listener

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

bouncerecipients

说明

从队列退回邮件。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式

示例

目标收件人主机或邮件信封的信封发件人行所示的特定地址识别的邮件发件人可对要退回的收件人进行识别。另外，可以一次性退回传送队列中的所有邮件。

按收件人主机退回

```
mail3.example.com> bouncerecipients

Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to bounce.
[]> example.com

Are you sure you want to bounce all messages being delivered to "example.com"?[N]> Y

Bouncing messages, please wait.
100 messages bounced.
```

按信封收件人地址退回

```
mail3.example.com> bouncerecipients

Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2

Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com

Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"?[N]> Y

Bouncing messages, please wait.
100 messages bounced.
```

全部退回

```
mail3.example.com> bouncerecipients

Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>

Are you sure you want to bounce all messages in the queue?[N]> Y

Bouncing messages, please wait.
1000 messages bounced.
```

bvconfig

说明

配置退回验证的设置。使用此命令可以配置密钥和无效的退回邮件。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

下面的示例显示为无效退回邮件配置的关键配置和设置。

```
mail3.example.com> bvconfig

Behavior on invalid bounces: reject

Key for tagging outgoing mail: key

Previously-used keys for verifying incoming mail:

        1. key (current outgoing key)
        2. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)

Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]> key

Enter the key to tag outgoing mail with (when tagging is enabled in the Good
Neighbor Table)
[]> basic_key

Behavior on invalid bounces: reject

Key for tagging outgoing mail: basic_key

Previously-used keys for verifying incoming mail:

        1. basic_key (current outgoing key)
        2. key (last in use Wed May 31 23:22:49 2006 GMT)
        3. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)

Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]> setup

How do you want bounce messages which are not addressed to a valid tagged
recipient to be handled?
```

```
1. Reject.
2. Add a custom header and deliver.
[1]> 1

Behavior on invalid bounces: reject

Key for tagging outgoing mail: basic_key

Previously-used keys for verifying incoming mail:

        1. basic_key (current outgoing key)
        2. key (last in use Wed May 31 23:22:49 2006 GMT)
        3. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)

Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Configuring a new key and setting reject for invalid email bounces

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

deleterecipients

说明

从队列中删除邮件。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

设备为您提供了根据需要删除收件人的选项。以下示例显示了按收件人主机删除收件人、按信封发件人地址删除收件人以及删除队列中的全部收件人。

按收件人域删除

```
mail3.example.com> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
```

```
Please enter the hostname for the messages you wish to delete.
[]> example.com

Are you sure you want to delete all messages being delivered to "example.com"?[N]> Y

Deleting messages, please wait.
100 messages deleted.
```

按信封发件人地址删除

```
mail3.example.com> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com

Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"?[N]> Y

Deleting messages, please wait.
100 messages deleted.
```

删除全部

```
mail3.example.com> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
Are you sure you want to delete all messages in the queue?[N]> Y

Deleting messages, please wait.
1000 messages deleted.
```

deliveryconfig

说明

配置邮件传送。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在以下示例中，deliveryconfig 命令用于将默认接口设置为“自动”(Auto) 并启用“可能传送”(Possible Delivery)。整个系统的最大出站邮件传送并发连接数设为 9000 个连接。

```
mail3.example.com> deliveryconfig

Choose the operation you want to perform:
- SETUP - Configure mail delivery.
[]> setup

Choose the default interface to deliver mail.
1. Auto
2. AnotherPublicNet (192.168.3.1/24: mail4.example.com)
3. Management (192.168.42.42/24: mail3.example.com)
4. PrivateNet (192.168.1.1/24: mail3.example.com)
5. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1

Enable "Possible Delivery" (recommended)?[Y]> y

Please enter the default system wide maximum outbound message delivery
concurrency
[10000]> 9000

mail3.example.com>
```

delivernow

说明

重新安排邮件以立即进行传输。用户可以选择单个收件人主机或是当前计划要传输的所有邮件。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> delivernow

Please choose an option for scheduling immediate delivery.
1. By recipient domain
2. All messages
[1]> 1

Please enter the recipient domain to schedule for delivery.
[]>foo.com

Scheduling all messages to foo.com for delivery.
```

destconfig

以前为 setgoodtable 命令。该表格现在称为目标控制表。使用此表格可以为指定的域配置传输限制。

使用 destconfig 命令

以下命令在 destconfig 子菜单内可用：

表 3-8　destconfig 子命令

语法	说明
SETUP	更改全局设置。
NEW	添加域的新限制。
EDIT	修改域的限制。
DELETE	删除域的限制。
DEFAULT	更改非指定域的默认限制。
LIST	显示域及其限制的列表。
DETAIL	显示一个目标或所有条目的详细信息。
CLEAR	从表格中删除所有条目。
IMPORT	从 .INI 配置文件中导入目标控制条目的表格。
EXPORT	向 .INI 配置文件导出目标控制条目的表格。

destconfig 命令要求为目标控制表中的每行提供以下信息。

- 域 （收件人主机）
- 与域的最大同时连接数
- 每个连接允许的邮件数限制
- 收件人限制
- 全系统或虚拟网关交换机
- 按 MX 或域实施限制
- 收件人时段限制 （分钟）
- 退回验证
- 用于域的退回配置文件

目标控制表示例

下表在目标控制表中显示条目。

表 3-9　目标控制条目示例

域	连接限制	收件人 Limit	最小时段	实施 MX/DOM
（默认）	500	无	1	域
未列出的域获取他们自己的 500 个连接集，每小时的收件人数没有限制				
（默认）	500	无	1	MXIP

表 3-9　　目标控制条目示例

域	连接限制	收件人 Limit	最小时段	实施 MX/DOM
未列出域处的邮件网关可以获取最多 500 个连接，每小时的收件人数没有限制				
partner.com	10	500	60	域
partner.com 处的所有网关将共享 10 个连接，每分钟最大收件人数为 500				
101.202.101.2	500	无	0	MXIP
指定 IP 地址				

批处理格式

`destconfig` 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 创建新的目标控制表

```
destconfig new <profile> [options]
```

- 编辑现有的目标控制表

```
destconfig edit <default|profile> [options]
```

- 删除现有的目标控制表

```
destconfig delete <profile>
```

- 显示所有目标控制条目的摘要

```
destconfig list
```

- 显示一个目标或所有条目的详细信息

```
destconfig detail <default|profile|all>
```

- 删除所有现有的目标控制表条目

```
destconfig clear
```

- 从文件导入表格

```
destconfig import <filename>
```

- 将表格导出到文件

```
destconfig export <filename>
```

对于 edit 和 new 批处理命令，可以通过利用变量名称和等号来标识值的方式，提供以下任意或全部选项。不会修改未指定的选项 （如果使用 edit），或将被设置为默认值 （如果使用 new）。

```
concurrency_limit=<int> - The maximum concurrency for a specific host.

concurrency_limit_type=<host|MXIP> - Maximum concurrency is per host or
per MX IP.

concurrency_limit_apply=<system|VG> - Apply maximum concurrency is system
wide or by Virtual Gateway(tm).

max_messages_per_connection=<int> - The maximum number of messages that
will be sent per connection.

recipient_limit_minutes=<int> - The time frame to check for recipient
limits in minutes.

recipient_limit=<int> - The number of recipients to limit per unit of
time.

use_tls=<off|on|require|on_verify|require_verify> - Whether TLS should be
on, off, or required for a given host.

bounce_profile=<default|profile> - The bounce profile name to use.

bounce_verification=<off|on> - Bounce Verification option.
```

示例：创建新的 destconfig 条目

在下面的示例中，当前 destconfig 条目会打印到屏幕。然后，会创建域 partner.com 的新条目。将会为该域设置 60 分钟时段内 100 个同时连接的并发限制以及 50 个收件人的收件人限制。因此，系统在指定小时内不会向域 partner.com 打开超过 100 个连接或向多于 50 个的收件人进行传输。不会为此特定域分配退回配置文件，不会配置特定 TLS 设置。最后，会打印更改以进行确认，并提交更改。

```
mail3.example.com> destconfig

There are currently 2 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> list

1
           Rate                Bounce        Bounce
Domain     Limiting  TLS       Verification  Profile
=========  ========  =======   ============  =========
(Default)  On        Off       Off           (Default)
```

```
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.

[]> partner.com

Do you wish to configure a concurrency limit for partner.com?[Y]> y

Enter the max concurrency limit for "partner.com".
[500]> 100

Do you wish to apply a messages-per-connection limit to this domain?[N]> n

Do you wish to apply a recipient limit to this domain?[N]> y

Enter the number of minutes used to measure the recipient limit.
[60]> 60

Enter the max number of recipients per 60 minutes for "partner.com".
[]> 50

Select how you want to apply the limits for partner.com:
1. One limit applies to the entire domain for partner.com
2. Separate limit for each mail exchanger IP address
[1]> 1

Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1

Do you wish to apply a specific TLS setting for this domain?[N]> n

Do you wish to apply a specific bounce verification address tagging setting for
this domain?[N]> n

Do you wish to apply a specific bounce profile to this domain?[N]> n


There are currently 3 entries configured.

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Throttled delivery to partner.com in the destconfig table

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

示例：退回配置文件和 TLS 设置

在本示例中，将会为域 newpartner.com 配置新的 destconfig 条目。需要 TLS 连接。此示例还显示名为 bouncepr1（请参阅“编辑默认退回配置文件”（第 132 页））的退回配置文件，该配置文件配置为用于将所有邮件传输到域 newpartner.com。

```
mail3.example.com> destconfig

There is currently 1 entry configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
[]> newpartner.com

Do you wish to configure a concurrency limit for newpartner.com?[Y]> n

Do you wish to apply a messages-per-connection limit to this domain?[N]> n

Do you wish to apply a recipient limit to this domain?[N]> n

Do you wish to apply a specific TLS setting for this domain?[N]> y

Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred(Verify)
5. Required(Verify)
[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there is
a valid certificate configured.

Do you wish to apply a specific bounce verification address tagging setting for this
domain?[N]> y

Perform bounce verification address tagging?[N]> y

Do you wish to apply a specific bounce profile to this domain?[N]> y

Please choose a bounce profile to apply:
1. Default
2. New Profile
[1]> 1

There are currently 2 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
```

```
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> detail

                Rate                Bounce        Bounce
Domain          Limiting  TLS       Verification  Profile
==============  ========  =======   ============  =========
newpartner.com  Default   Req       On            Default
(Default)       On        Off       Off           (Default)

Enter the domain name to view, or enter DEFAULT to view details for the
default, or enter ALL to view details for all:
[]> all

newpartner.com
 Maximum messages per connection: Default
 Rate Limiting: Default
 TLS: Required
 Bounce Verification Tagging: On
 Bounce Profile: Default

Default
 Rate Limiting:
 500 concurrent connections
 No recipient limit
 Limits applied to entire domain, across all virtual gateways
 TLS: Off
 Bounce Verification Tagging: Off

There are currently 2 entries configured.

[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> enabled TLS for delivery to newpartner.com using demo certificate

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

示例：入站 “缓冲区”

在本示例中，会创建另一 destconfig 条目，以限制邮件传输到内部组件服务器 exchange.example.com。内部服务器的此 “入站缓冲区” 条目会限制邮件入站传输到您的内部组件服务器，特别是高峰流量时段。在本示例中，设备在任意指定的*分钟*内绝不会同时打开超过十个连接，或绝不会将邮件传输到内部组件服务器 exchange.example.com 内的超过 1000 个收件人。未配置退回配置文件或 TLS 设置。

```
mail3.example.com> destconfig

There are currently 2 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
```

```
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[]> new

Enter the domain you wish to configure.
[]> exchange.example.com

Do you wish to configure a concurrency limit for exchange.example.com?[Y]> y

Enter the max concurrency limit for "exchange.example.com".
[500]> 10

Do you wish to apply a recipient limit to this domain?[N]> y

Enter the number of minutes used to measure the recipient limit.
[60]> 1

Enter the max number of recipients per 1 minutes for "exchange.example.com".
[]> 1000

Select how you want to apply the limits for exchange.example.com:
1. One limit applies to the entire domain for exchange.example.com
2. Separate limit for each mail exchanger IP address
[1]> 1

Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1

Do you wish to apply a specific TLS setting for this domain?[N]> n
Do you wish to apply a specific bounce verification address tagging setting for this
domain?[N]> n

Do you wish to apply a specific bounce profile to this domain?[N]> n

There are currently 3 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> set up shock absorber for inbound mail

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

示例：全局设置

在本示例中，会配置 TLS 连接的 TLS 警告和证书。

```
mail3.example.com> destconfig
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> setup

The "Demo" certificate is currently configured.You may use "Demo", but this will not be
secure.

1. partner.com
2. Demo
Please choose the certificate to apply:
[1]> 1

Do you want to send an alert when a required TLS connection fails?[N]> n
```

hostrate

说明

监控特定主机的活动。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> hostrate

Recipient host:
[]> aol.com

Enter the number of seconds between displays.
[10]> 1

    Time      Host  CrtCncOut   ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt
              Status                      Delta   Delta     Delta     Delta
23:38:23        up          1         0       0       4         0         0
23:38:24        up          1         0       0       4         0         0
23:38:25        up          1         0       0      12         0         0
^C
```

使用 Control-C 可停止 hostrate 命令。

hoststatus

说明

获取指定主机名的状态。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com

Host mail status for: 'aol.com'
Status as of:         Fri Aug  8 11:12:00 2003
Host up/down:         up

Counters:
  Queue
    Soft Bounced Events                     0
  Completion
    Completed Recipients                    1
      Hard Bounced Recipients               1
        DNS Hard Bounces                    0
        5XX Hard Bounces                    1
        Filter Hard Bounces                 0
        Expired Hard Bounces                0
        Other Hard Bounces                  0
      Delivered Recipients                  0
      Deleted Recipients                    0

Gauges:
  Queue
    Active Recipients                       0
      Unattempted Recipients                0
      Attempted Recipients                  0
    Connections
      Current Outbound Connections          0
      Pending Outbound Connections          0

Oldest Message        No Messages
Last Activity         Fri Aug  8 11:04:24 2003
Ordered IP addresses: (expiring at Fri Aug  8 11:34:24 2003)
    Preference   IPs
    15           64.12.137.121    64.12.138.89     64.12.138.120
    15           64.12.137.89     64.12.138.152    152.163.224.122
    15           64.12.137.184    64.12.137.89     64.12.136.57
    15           64.12.138.57     64.12.136.153    205.188.156.122
```

```
    15          64.12.138.57     64.12.137.152    64.12.136.89
    15          64.12.138.89     205.188.156.154  64.12.138.152
    15          64.12.136.121    152.163.224.26   64.12.137.184
    15          64.12.138.120    64.12.137.152    64.12.137.121
MX Records:
    Preference   TTL        Hostname
    15           52m24s     mailin-01.mx.aol.com
    15           52m24s     mailin-02.mx.aol.com
    15           52m24s     mailin-03.mx.aol.com
    15           52m24s     mailin-04.mx.aol.com

    Last 5XX Error:
    ----------
    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
    (at Fri Aug  8 11:04:25 2003)
    ----------

Virtual gateway information:
============================================================
example.com (PublicNet_017):
    Host up/down:up
    Last ActivityWed Nov 13 13:47:02 2003
    Recipients0
============================================================
example.com (PublicNet_023):
    Host up/down:up
    Last ActivityWed Nov 13 13:45:01 2003
    Recipients
```

imageanalysisconfig

说明

配置 IronPort 图像分析设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com>imageanalysisconfig

IronPort Image Analysis: Enabled
Image Analysis Sensitivity: 65
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
Skip small images with size less than 100 pixels (width or height)

(First time users see the license agreement displayed here.)

Choose the operation you want to perform:
- SETUP - Configure IronPort Image Analysis.
[]> setup
```

```
IronPort Image Analysis: Enabled
Would you like to use IronPort Image Analysis?[Y]>

Define the image analysis sensitivity.Enter a value between 0 (least sensitive) and 100
(most sensitive).As sensitivity increases, so does the false
positive rate.The default setting of 65 is recommended.
[65]>

Define the range for a CLEAN verdict.Enter the upper bound of the CLEAN range by entering
a value between 0 and 98.The default setting of 49 is
recommended.
[49]>

Define the range for a SUSPECT verdict.Enter the upper bound of the SUSPECT range by
entering a value between 50 and 99.The default setting of 74 is
recommended.
[74]>

Would you like to skip scanning of images smaller than a specific size?[Y]>

Please enter minimum image size to scan in pixels, representing either height or width of
a given image.
[100]>

IronPort Image Analysis: Enabled
Image Analysis Sensitivity: 65
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
Skip small images with size less than 100 pixels (width or height)

Choose the operation you want to perform:
- SETUP - Configure IronPort Image Analysis.
[]>
```

oldmessage

说明

显示系统上最早的非隔离区邮件的中间部分和信头。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，会显示最早的邮件：

```
mail3.example.com> oldmessage

MID 9: 1 hour 5 mins 35 secs old
Received: from test02.com ([172.19.0.109])
by test02.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@test02.com
To: 4031@example.com
```

```
Subject: Testing
Message-Id: <20070215061136.68297.16346@test02.com
```

rate

说明

监控邮件吞吐量。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1

Hit Ctrl-C to return to the main prompt.

Time     Connections Recipients          Recipients              Queue
            In   Out   Received    Delta  Completed    Delta     K-Used
23:37:13    10     2   41708833        0   40842686        0         64
23:37:14     8     2   41708841        8   40842692        6        105
23:37:15     9     2   41708848        7   40842700        8         76
23:37:16     7     3   41708852        4   40842705        5         64
23:37:17     5     3   41708858        6   40842711        6         64
23:37:18     9     3   41708871       13   40842722       11         67
23:37:19     7     3   41708881       10   40842734       12         64
23:37:21    11     3   41708893       12   40842744       10         79
^C
```

redirectrecipients

说明

将所有邮件重定向到另一个中继主机。

警告 **将邮件重定向至目标为 /dev/null 的接收域会导致邮件丢失。如果您将邮件重定向至这种域，那么 CLI 就不会显示警告。请在重定向邮件之前检查接收域的 SMTP 路由。**

警告 **如果将收件人重定向到尚未准备好从此主机接受大量 SMTP 邮件的主机或 IP 地址，将会导致邮件退回，并可能导致邮件丢失。**

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

redirectrecipients 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 将所有邮件重定向到另一主机名称或 IP 地址

```
redirectrecipients host <hostname>
```

示例

以下示例将所有邮件重定向至 example2.com 主机。

```
mail3.example.com> redirectrecipients

Please enter the hostname or IP address of the machine you want to send all mail to.
[]> example2.com

WARNING: redirecting recipients to a host or IP address that is not prepared to accept
large volumes of SMTP mail from this host will cause messages to bounce and possibly
result in the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"?[N]> y

Redirecting messages, please wait.
246 recipients redirected.
```

resetcounters

说明

重置系统中的所有计数器。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> resetcounters

Counters reset: Mon Jan 01 12:00:01 2003
```

removemessage

说明

尝试安全删除特定邮件 ID 的邮件。

removemessage 命令只能删除位于工作队列、重试队列或目标队列中的邮件。请注意，有效邮件和活动邮件可能不在上述任意队列中，这取决于系统状态。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
example.com> removemessage

Enter the MID to remove.
[]> 1

MID 1: 19 secs old

Received: from example2.com ([172.16.0.102])
  by test02.com with SMTP; 01 Mar 2007 19:50:41 -0800
From: user123@test02.com
To: 9526@example.com
Subject: Testing
Message-Id: <20070302035041.67424.53212@test02.com>

Remove this message?[N]> y
```

showmessage

说明

显示指定邮件 ID 的邮件和邮件正文。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
example.com> showmessage

MID 9: 1 hour 5 mins 35 secs old
```

```
Received: from example2.com([172.19.0.109])
  by test02.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@test02.com
To: 4031@example.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@test02.com>

This is the message body.
```

showrecipients

说明

按收件人主机、信封收件人地址显示队列中的邮件，或显示所有邮件。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

showrecipients 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 按收件人主机名称查找邮件

```
showrecipients host <hostname>
```

- 按信封收件人地址查找邮件

```
showrecipients [sender_options] <sender_email>
```

  下面的 sender_option 可用：

  --match-case 地址的用户名部分大小写匹配。

- 查找所有邮件

```
showrecipients all
```

示例

以下示例显示所有收件人主机队列中的邮件。

```
mail3.example.com> showrecipients

Please select how you would like to show messages:
1.By recipient host.
2.By Envelope From address.
3.All.
[1]> 3
```

```
Showing messages, please wait.

MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
1527     1230      user123456@ironport.com Testing
[0]      [0]       9554@example.com

1522     1230      user123456@ironport.com Testing
[0]      [0]       3059@example.com

1529     1230      user123456@ironport.com Testing
[0]      [0]       7284@example.com

1530     1230      user123456@ironport.com Testing
[0]      [0]       8243@example.com

1532     1230      user123456@ironport.com Testing
[0]      [0]       1820@example.com

1531     1230      user123456@ironport.com Testing
[0]      [0]       9595@example.com

1518     1230      user123456@ironport.com Testing
[0]      [0]       8778@example.com

1535     1230      user123456@ironport.com Testing
[0]      [0]       1703@example.com

1533     1230      user123456@ironport.com Testing
[0]      [0]       3052@example.com

1536     1230      user123456@ironport.com Testing
[0]      [0]       511@example.com
```

状态

status 命令用于显示设备的系统状态。使用 “详细”选项 （状态详细信息）显示附加信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> status detail

Status as of:                  Mon Sep 08 00:01:44 2014 GMT
Up since:                      Tue Aug 26 17:24:16 2014 GMT

(12d 6h 37m 28s)
Last counter reset:            Never
System status:                 Online
Oldest Message:                No Messages
Feature - IronPort Anti-Spam:  1459 days
Feature - Incoming Mail Handling: Perpetual
```

```
Feature - Outbreak Filters:    1459 days

Counters:                                  Reset          Uptime        Lifetime
  Receiving
    Messages Received                          2               2               2
    Recipients Received                        2               2               2
  Rejection
    Rejected Recipients                        0               0               0
    Dropped Messages                           0               0               0
  Queue
    Soft Bounced Events                        0               0               0
  Completion
    Completed Recipients                       0               0               0
  Current IDs
    Message ID (MID)                                                           2
    Injection Conn. ID (ICID)                                                  0
    Delivery Conn. ID (DCID)                                                  13

Gauges:                                    Current
  Connections
    Current Inbound Conn.                        0
    Current Outbound Conn.                       0
  Queue
    Active Recipients                            2
    Messages In Work Queue                       0
    Kilobytes Used                             184
    Kilobytes Free                       8,388,424
  Quarantine
    Messages In Quarantine
      Policy, Virus and Outbreak                 0
    Kilobytes In Quarantine
      Policy, Virus and Outbreak                 0
```

tophosts

说明

要获得有关邮件队列的实时信息并确定特定收件人主机存在传送问题 - 例如队列组合 - 请使用 tophosts 命令。tophosts 命令会返回队列中的前 20 个收件人主机的列表。列表可按照不同统计信息进行排序，包括正在处理的收件人数、出站连接数、传送的收件人数、软退回事件数和硬退回的收件人数。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> tophosts

Sort results by:

1.Active Recipients
2.Connections Out
3.Delivered Recipients
```

```
4.Hard Bounced Recipients
5.Soft Bounced Events
[1]> 1

Status as of:                   Fri Mar 13 06:09:18 2015 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.     Deliv.Soft       Hard
#   Recipient Host              Recip.Out     Recip.Bounced    Bounced

1*  example.com                      2      0          0          0          0
2   the.encryption.queue             0      0          0          0          0
3   the.euq.queue                    0      0          0          0          0
4   the.euq.release.queue            0      0          0          0          0
```

topin

说明

按传入连接数显示排名前列的主机。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003

#   Remote hostname            Remote IP addr.listener        Conn. In
1   mail.remotedomain01.com    172.16.0.2        Incoming01           10
2   mail.remotedomain01.com    172.16.0.2        Incoming02           10
3   mail.remotedomain03.com    172.16.0.4        Incoming01            5
4   mail.remotedomain04.com    172.16.0.5        Incoming02            4
5   mail.remotedomain05.com    172.16.0.6        Incoming01            3

6   mail.remotedomain06.com    172.16.0.7        Incoming02            3
7   mail.remotedomain07.com    172.16.0.8        Incoming01            3
8   mail.remotedomain08.com    172.16.0.9        Incoming01            3
9   mail.remotedomain09.com    172.16.0.10       Incoming01            3
10  mail.remotedomain10.com    172.16.0.11       Incoming01            2

11  mail.remotedomain11.com    172.16.0.12       Incoming01            2
12  mail.remotedomain12.com    172.16.0.13       Incoming02            2
13  mail.remotedomain13.com    172.16.0.14       Incoming01            2
14  mail.remotedomain14.com    172.16.0.15       Incoming01            2
15  mail.remotedomain15.com    172.16.0.16       Incoming01            2

16  mail.remotedomain16.com    172.16.0.17       Incoming01            2
17  mail.remotedomain17.com    172.16.0.18       Incoming01            1
18  mail.remotedomain18.com    172.16.0.19       Incoming02            1
19  mail.remotedomain19.com    172.16.0.20       Incoming01            1
20  mail.remotedomain20.com    172.16.0.21       Incoming01            1
```

unsubscribe

说明

更新全局取消订阅列表。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在本示例中，将地址 user@example.net 添加到全局取消订阅列表中，并且将此功能配置为硬退回邮件。发送到此地址的邮件将被退回；设备在传送邮件之前会将其退回。

```
mail3.example.com> unsubscribe

Global Unsubscribe is enabled.Action: drop.

Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import entries from a file.
- SETUP - Configure general settings.
[]> new

Enter the unsubscribe key to add.  Partial addresses such as "@example.com"
or "user@" are allowed, as are IP addresses.Partial hostnames such as "@.example.com" are
allowed.
[]> user@example.net

Email Address 'user@example.net' added.
Global Unsubscribe is enabled.Action: drop.

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup

Do you want to enable the Global Unsubscribe feature?[Y]> y

Would you like matching messages to be dropped or bounced?
1.Drop
2.Bounce
[1]> 2

Global Unsubscribe is enabled.Action: bounce.

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
```

```
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added username “user@example.net” to global unsubscribe

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

workqueue

说明

显示和/或修改工作队列暂停状态。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> workqueue

Status:   Operational
Messages: 1243

Manually pause work queue?This will only affect unprocessed messages.[N]> y

Reason for pausing work queue:
[]> checking LDAP server

Status:   Paused by admin: checking LDAP server
Messages: 1243
```

注　输入原因是可选的。如果您未输入原因，则系统会将原因记录为“operator paused”。

在此示例中，工作队列继续：

```
mail3.example.com> workqueue

Status:   Paused by admin: checking LDAP server
Messages: 1243

Resume the work queue?[Y]> y

Status:   Operational
Messages: 1243
```

网络配置/网络工具

本部分包含以下 CLI 命令：

etherconfig

说明

配置以太网设置，包括媒体设置、 NIC 配对、 VLAN 配置和 DSR 配置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> vlan
```

```
VLAN interfaces:

Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new

VLAN tag ID for the interface (Ex: "34"):
[]> 12

Enter the name or number of the ethernet interface you wish bind to:
1.Data 1
2.Data 2
3.Management
[1]> 1

VLAN interfaces:
1.VLAN   12 (Data 1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>


Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> loopback

Currently configured loopback interface:

Choose the operation you want to perform:
- ENABLE - Enable Loopback Interface.
[]>


Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> mtu

Ethernet interfaces:
1.Data 1 default mtu 1500
2.Data 2 default mtu 1500
3.Management default mtu 1500
4.VLAN   12 default mtu 1500

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]> edit

Enter the name or number of the ethernet interface you wish to edit.
[]> pair1

That value is not valid.

Enter the name or number of the ethernet interface you wish to edit.
```

```
[]> 12

That value is not valid.

Enter the name or number of the ethernet interface you wish to edit.
[]> 2

Please enter a non-default (1500) MTU value for the Data 2 interface.
[]> 1200

Ethernet interfaces:
1.Data 1 default mtu 1500
2.Data 2 mtu 1200
3.Management default mtu 1500
4.VLAN   12 default mtu 1500

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

interfaceconfig

说明

配置接口。您可以创建、编辑或删除接口。您可以启用 FTP，更改 IP 地址和配置以太网 IP 地址。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

`interfaceconfig` 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 创建新接口

```
interfaceconfig new <name>

                    <ethernet interface>

                    <hostname>

                    --ip=IPv4 Address/Netmask

                    --ip6=IPv6 Address/Prefix Lenght

                    [--ftp[=<port>]]

                    [--telnet[=<port>]]

                    [--ssh[=<port>]]
```

```
                    [--http][=<port>]

                    [--https[=<port>]]

                    [--euq_http[=<port>]]

                    [--euq_https][=<port>]

                    [--ccs[=<port>]].

FTP is available only on IPv4.
```

- 删除接口

```
interfaceconfig delete <name>
```

示例：配置接口

```
mail.example.com> interfaceconfig

Currently configured interfaces:
1.Management (10.76.69.149/24 on Management: mail.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Management]>

Would you like to configure an IPv4 address for this interface (y/n)?[Y]>

IPv4 Address (Ex: 192.168.1.2 ):
[1.1.1.1]>

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[0xffffffff]>

Would you like to configure an IPv6 address for this interface (y/n)?[N]> n

Ethernet interface:
1.Data 1
2.Data 2
3.Management
[3]>

Hostname:
[mail.example.com]>

Do you want to enable SSH on this interface?[Y]>

Which port do you want to use for SSH?
```

```
[22]>

Do you want to enable FTP on this interface?[N]>

Do you want to enable Cluster Communication Service on this interface?[N]>

Do you want to enable HTTP on this interface?[Y]>

Which port do you want to use for HTTP?
[80]>

Do you want to enable HTTPS on this interface?[Y]>

Which port do you want to use for HTTPS?
[443]>

Do you want to enable Spam Quarantine HTTP on this interface?[N]>

Do you want to enable Spam Quarantine HTTPS on this interface?[N]>

Do you want to enable AsyncOS API (Monitoring) HTTP on this interface?[N]> y

Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6080]>

Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface?[N]> y

Which port do you want to use for AsyncOS API (Monitoring) HTTPS?
[6443]>

The "Demo" certificate is currently configured.You may use "Demo", but this will not be
secure.To assure privacy, run "certconfig" first.

Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the
secure service?[Y]>

You have edited the interface you are currently logged into.Are you sure you want to
change it?[Y]>


Currently configured interfaces:
1.Management (10.76.69.149/24 on Management: mail.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>
```

nslookup

说明

使用 nslookup 命令检查 DNS 功能。

使用 nslookup 命令可以确认设备是否能够从工作中的 DNS （域名服务）服务器到达并解析主机名和 IP 地址。

表 3-10　nslookup 命令查询类型

查询类型	说明
A	主机的 Internet 地址
CNAME 记录	别名的规范名称
MX	邮件交换器
NS 记录	用于指定区域的名称服务器
PTR	如果查询互联网地址，则是主机名，否则指向其他信息
SOA	域名的 “start-of-authority”信息
TXT	文本信息

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> nslookup

Please enter the host or IP address to resolve.
[]> vm30esa0086.ibqa

Choose the query type:
1.A       the host's IP address
2.AAAA    the host's IPv6 address
3.CNAME   the canonical name for an alias
4.MX      the mail exchanger
5.NS      the name server for the named zone
6.PTR     the hostname if the query is an Internet address,

otherwise the pointer to other information
7.SOA     the domain's "start-of-authority" information
8.TXT     the text information
[1]> 2

AAAA=2001:420:54ff:ff06::95 TTL=30m
```

netstat

说明

使用 netstat 命令可以显示网络连接 （传入和传出）、路由表和一些网络接口统计信息。请注意此版本并非支持所有参数。具体而言，您不能使用 -a、-A、-g、-m、-M、-N、-s。该命令旨在以交互模式运行，因此您可以输入 netstat，然后从五个选项中选择以进行报告。您还可以指定要监听的接口以及显示的间隔。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
example.com> netstat
Choose the information you want to display:
1.List of active sockets.
2.State of network interfaces.
3.Contents of routing tables.
4.Size of the listen queues.
5.Packet traffic information.
[1]> 2
Select the ethernet interface whose state you wish to display:
1.Data 1
2.Data 2
3.Management
4.ALL
[]> 1
Show the number of bytes in and out?[N]>
Show the number of dropped packets?[N]> y
Name    Mtu Network       Address              Ipkts Ierrs    Opkts
Oerrs  Coll Drop
Data 1 1500 197.19.1/24   example.com       30536     -        5     -
-    -
example.com>
```

packetcapture

说明

使用 netstat 命令可以显示网络连接 （传入和传出）、路由表和一些网络接口统计信息。请注意此版本并非支持所有参数。具体而言，您不能使用 -a、-A、-g、-m、-M、-N、-s。该命令旨在以交互模式运行，因此您可以输入 netstat，然后从五个选项中选择以进行报告。您还可以指定要监听的接口以及显示的间隔。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> packetcapture

Capture Information:
  Status:             No capture running

Current Settings:
```

```
  Maximum File Size:  200 MB
  Limit:              None (Run Indefinitely)
  Interface(s):       ALL
  Filter:             (tcp port 25)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> start

Success - Packet Capture has started

Capture Information:
  File Name:          C100V-421C73B18CFB05784A83-B03A99E71ED8-20150312-105256.cap
  File Size:          0 of 200M
  Duration:           0s
  Limit:              None (Run Indefinitely)
  Interface(s):       ALL
  Filter:             (tcp port 25)

Choose the operation you want to perform:
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[]> stop

Success - Packet Capture has stopped

Capture Information:
  File Name:          C100V-421C73B18CFB05784A83-B03A99E71ED8-20150312-105256.cap
  File Size:          24 of 200M
  Duration:           10s
  Limit:              None (Run Indefinitely)
  Interface(s):       ALL
  Filter:             (tcp port 25)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> setup

Enter maximum allowable size for the capture file (in MB)
[200]>

Do you want to stop the capture when the file size is reached?(If not, a new file will be
started and the older capture data will be discarded.)
[N]>

The following interfaces are configured:
1.Management
2.ALL
Enter the name or number of one or more interfaces to capture packets from, separated by
commas (enter ALL to use all interfaces):
[2]>

Select an operation.Press enter to continue with the existing filter.
- PREDEFINED - PREDEFINED filter.
- CUSTOM - CUSTOM filter.
- CLEAR - CLEAR filter.
[]>

Capture settings successfully saved.
```

```
Current Settings:
  Maximum File Size:  200 MB
  Limit:              None (Run Indefinitely)
  Interface(s):       ALL
  Filter:             (tcp port 25)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]>
```

ping

说明

使用 ping 命令可以测试网络主机与设备的连接。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> ping

Which interface do you want to send the pings from?
1.Auto
2.Management (192.168.42.42/24: mail3.example.com)
3.PrivateNet (192.168.1.1/24: mail3.example.com)
4.PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1

Please enter the host you wish to ping.
[]> anotherhost.example.com


Press Ctrl-C to stop.
PING anotherhost.example.com (x.x.x.x): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=0 ttl=64 time=1.421 ms
64 bytes from 10.19.0.31: icmp_seq=1 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=2 ttl=64 time=0.118 ms
64 bytes from 10.19.0.31: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 10.19.0.31: icmp_seq=4 ttl=64 time=0.139 ms
64 bytes from 10.19.0.31: icmp_seq=5 ttl=64 time=0.125 ms
64 bytes from 10.19.0.31: icmp_seq=6 ttl=64 time=0.124 ms
64 bytes from 10.19.0.31: icmp_seq=7 ttl=64 time=0.122 ms
64 bytes from 10.19.0.31: icmp_seq=8 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
```

```
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
^C
```

注　您必须使用 Control-C 才能结束 ping 命令。

ping6

说明

对采用 IPv6 的网络主机执行 ping 操作。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> ping6

Which interface do you want to send the pings from?
1.Auto
2.Management (192.168.42.42/24: mail3.example.com)
[1]> 1

Please enter the host you wish to ping.
[]> anotherhost.example.com


Press Ctrl-C to stop.
```

注　必须使用 Control-C 来结束 ping6 命令。

routeconfig

说明

routeconfig 命令允许您创建、编辑以及删除 TCP/IP 流量的静态路由。默认情况下， setgateway 命令用于通过默认网关集路由流量。但是， AsyncOS 允许基于目标的特定路由。

路由包括别名 （供将来参考）、目标和网关。网关 （下一跳）是 IP 地址，如 10.1.1.2。目标可以是以下两项之一：

- IP 地址，例如 192.168.14.32。
- 使用 CIDR 标记的子网。例如，192.168.5.0/24 是指从 192.168.5.0 到 192.168.5.255 的整个 C 类网络。

对于 IPv6 地址，您可以使用以下格式：

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

该命令会为呈现所有当前配置的 TCP/IP 路由的列表，以供您使用 edit 和 delete 子命令进行选择。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

smtproutes 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。您可以选择是使用 IPv4 还是 IPv6 地址进行路由。

- 创建静态路由：

```
routeconfig new 4|6 <name> <destination_address> <gateway_ip>
```

表 3-11　routeconfig 参数

参数	说明
4|6	要应用此命令的 IP 版本 （IPv4 或 IPv6）。对于 clear 和 print，可以忽略此选项，该命令同时适用于这两个版本。
name	路由的名称。
destination_address	针对传出 IP 流量而匹配的 IP 或 CIDR 地址。
gateway_ip	将此流量发送到的目标 IP 地址。

- 编辑静态路由：

```
routeconfig edit 4|6 <name> <new_name> <destination_address>
<gateway_ip>
```

- 删除静态路由：

```
routeconfig delete 4|6 <name>
```

- 删除所有静态路由：

```
routeconfig clear [4|6]
```

- 打印静态路由列表：

```
routeconfig print [4|6]
```

示例

```
mail3.example.com> routeconfig

Configure routes for:

1.IPv4
2.IPv6
[1]>


Currently configured routes:


Choose the operation you want to perform:
- NEW - Create a new route.
[]> new

Please create a name for the route:
[]> EuropeNet

Please enter the destination IPv4 address to match on.
CIDR addresses such as 192.168.42.0/24 are also allowed.
[]> 192.168.12.0/24

Please enter the gateway IP address for traffic to 192.168.12.0/24:
[]> 192.168.14.4


Currently configured routes:
1.EuropeNet Destination: 192.168.12.0/24 Gateway: 192.168.14.4


Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[]>

mail3.example.com> routeconfig

Configure routes for:

1.IPv4
2.IPv6
[1]> 2


Currently configured routes:


Choose the operation you want to perform:
- NEW - Create a new route.
[]> new

Please create a name for the route:
```

```
[]> EuropeIPv6Net

Please enter the destination IPv6 address to match on.
CIDR addresses such as 2001:db8::/32 are also allowed.
[]>  2620:101:2004:4202::/6

Please enter the gateway IP address for traffic to 2620:101:2004:4202::/6:
[]> 2620:101:2004:4202::23


Currently configured routes:
1.EuropeIPv6Net Destination: 2620:101:2004:4202::/6 Gateway:
2620:101:2004:4202::23


Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[]>
```

setgateway

说明

setgateway 命令通过应路由的数据包配置默认下一跳中介。使用 routeconfig 命令配置备用 （非默认）网关。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection to be
interrupted when the changes are committed.
Enter new default gateway:
[10.1.1.1]> 192.168.20.1

mail3.example.com> commit

Please enter some comments describing your changes:
[]> changed default gateway to 192.168.20.1

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

sethostname

说明

主机名用于在收到 CLI 提示时识别系统。您必须输入完全限定的主机名。 sethostname 命令设置邮件安全设备的名称。新主机名只有在您发出 commit 命令后才会生效。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
oldname.example.com> sethostname

[oldname.example.com]> mail3.example.com

oldname.example.com>
```

对于要生效的主机名更改，您必须输入 commit 命令。成功提交主机名更改后，系统会在 CLI 提示中显示新名称：

```
oldname.example.com> commit

Please enter some comments describing your changes:
[]> Changed System Hostname

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

新的主机名会按如下所示显示在提示符中：

```
mail3.example.com>
```

smtproutes

说明

设置永久域重定向。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式

smtproutes 命令的批处理格式可以用于执行传统 CLI 命令的所有功能。

- 创建新的 SMTP 路由

```
smtproutes new <source> <destination> [destination] [destination] [...]
```

- 删除现有 SMTP 路由

```
smtproutes delete <source>
```

- 清除 SMTP 路由列表

```
smtproutes clear
```

- 打印 SMTP 路由列表

```
smtproutes print
```

- 导入 SMTP 路由列表

```
smtproutes import <filenames>
```

- 导出 SMTP 路由列表

```
smtproutes export <filenames>
```

示例

在下面的示例中， smptroutes 命令用于为域 example.com 构建路由 （映射）至 relay1.example.com、 relay2.example.com 和 backup-relay.example.com。使用 /pri=# 可以指定目标优先级。 THE # 应介于 0-65535，数字越大，表示优先级越低。如果未指定该值，则优先级默认为 0。

（请注意，您可能在配置 InboundMail 公共监听程序时已在 systemsetup 命令期间构建了相同的映射。）

```
mail3.example.com> smtproutes

There are no routes configured.

Choose the operation you want to perform:
- NEW - Create a new route.
- IMPORT - Import new routes from a file.
[]> new

Enter the domain for which you want to set up a permanent route.
Partial hostnames such as ".example.com" are allowed.
Use "ALL" for the default route.
[]> example.com

Enter the destination hosts, separated by commas, which you want mail
```

```
for example.com to be delivered.
Enter USEDNS by itself to use normal DNS resolution for this route.
Enter /dev/null by itself if you wish to discard the mail.
Enclose in square brackets to force resolution via address (A)
records, ignoring any MX records.
[]> relay1.example.com/pri=10, relay2.example.com, backup-relay.example.com

Mapping for example.com to relay1.example.com, relay2.example.com,
backup-relay.example.com/pri=10 created.

There are currently 1 routes configured.

Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.
[]>
```

sslconfig

说明

配置设备的 SSL 设置。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers:
        RC4-SHA
        RC4-MD5
        ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers:
        RC4-SHA
        RC4-MD5
        ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers:
        RC4-SHA
        RC4-MD5
        ALL
```

```
Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> gui

Enter the GUI HTTPS ssl method you want to use.
1.SSL v2.
2.SSL v3
3.TLS v1
4.SSL v2 and v3
5.SSL v3 and TLS v1
6.SSL v2, v3 and TLS v1
[5]> 6

Enter the GUI HTTPS ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
  GUI HTTPS method:  sslv2sslv3tlsv1
  GUI HTTPS ciphers:
        RC4-SHA
        RC4-MD5
        ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers:
        RC4-SHA
        RC4-MD5
        ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers:
        RC4-SHA
        RC4-MD5
        ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1.SSL v2.
2.SSL v3
3.TLS v1
4.SSL v2 and v3
5.SSL v3 and TLS v1
6.SSL v2, v3 and TLS v1
[5]> 6

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
  GUI HTTPS method:  sslv2sslv3tlsv1
  GUI HTTPS ciphers:
        RC4-SHA
        RC4-MD5
        ALL
  Inbound SMTP method:  sslv2sslv3tlsv1
  Inbound SMTP ciphers:
        RC4-SHA
```

```
        RC4-MD5
        ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers:
        RC4-SHA
        RC4-MD5
        ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>
```

sslv3config

说明

为设备启用或禁用 SSLv3 设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机。

批处理命令：此命令不支持批处理格式。

示例

以下示例显示如何禁用最终用户隔离区的 SSLv3。

```
mail.example.com> sslv3config

     Current SSLv3 Settings:
     ------------------------------------------------
                 UPDATER     :     Enabled
              WEBSECURITY    :     Enabled
                     EUQ     :     Enabled
                    LDAP     :     Enabled
     ------------------------------------------------

Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]> setup

Choose the service to toggle SSLv3 settings:
1.EUQ Service
2.LDAP Service
3.Updater Service
4.Web Security Service
[1]>

Do you want to enable SSLv3 for EUQ Service ?[Y]>n
```

```
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]>
```

telnet

说明

连接到远程主机。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> telnet

Please select which interface you want to telnet from.
1.Auto
2.Management (192.168.42.42/24: mail3.example.com)
3.PrivateNet (192.168.1.1/24: mail3.example.com)
4.PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 3

Enter the remote hostname or IP.
[]> 193.168.1.1

Enter the remote port.
[25]> 25

Trying 193.168.1.1...
Connected to 193.168.1.1.
Escape character is '^]'.
```

traceroute

说明

使用 `traceroute` 命令可以使用来自设备的 IPV4 测试到网络主机的连接性，并使用网络步跳调试路由问题。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> traceroute

Which interface do you want to trace from?
1.Auto
2.Management (192.168.42.42/24: mail3.example.com)
3.PrivateNet (192.168.1.1/24: mail3.example.com)
4.PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1

Please enter the host to which you want to trace the route.
[]> 10.1.1.1

Press Ctrl-C to stop.
traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets
 1  gateway (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms
 2  hostname (10.1.1.1)  0.298 ms  0.302 ms  0.291 ms
mail3.example.com>
```

traceroute6

说明

使用 `traceroute6` 命令可以使用来自设备的 IPV6 测试到网络主机的连接性，并使用网络步跳调试路由问题。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> traceroute6

Which interface do you want to trace from?
1.Auto
2.D1 (2001:db8::/32: example.com)
[1]> 1

Please enter the host to which you want to trace the route.
[]> example.com

Press Ctrl-C to stop.
connect: No route to host
vm10esa0031.qa> traceroute6

Which interface do you want to trace from?
1.Auto
```

```
2.D1 (2001:db8::/32: example.com)
[1]> 2

Please enter the host to which you want to trace the route.
[]> example.com

Press Ctrl-C to stop.
traceroute6 to example.com (2606:2800:220:1:248:1893:25c8:1946) from 2001:db8::, 64 hops
max, 12 byte packets
sendto: No route to host
 1 traceroute6: wrote example.com 12 chars, ret=-1
 *sendto: No route to host
traceroute6: wrote example.com 12 chars, ret=-1
 *sendto: No route to host
traceroute6: wrote example.com 12 chars, ret=-1
```

病毒爆发过滤器

本部分包含以下 CLI 命令：

- outbreakconfig
- outbreakflush
- outbreakstatus
- outbreakupdate

outbreakconfig

说明

使用 `outbreakconfig` 命令可以配置病毒爆发过滤器功能。使用此命令可以执行以下操作：

- 全局启用病毒爆发过滤器
- 启用自适应规则扫描
- 设置要扫描的最大文件大小 （注意，输入以*字节*为单位的大小）
- 为病毒爆发过滤器启用警报
- 启用 URL 记录

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> outbreakconfig

Outbreak Filters: Enabled
```

```
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]> setup

Outbreak Filters: Enabled
Would you like to use Outbreak Filters?[Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below), meaning that new messages of
certain types could be quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts?[N]>

What is the largest size message Outbreak Filters should scan?
[524288]>

Do you want to use adaptive rules to compute the threat level of messages?[Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's?[N]> Y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system.You must use the
'policyconfig' command in the CLI or the Email
Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and
Outgoing Mail Policies.

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]>
```

outbreakflush

说明

清除缓存的病毒爆发规则。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> outbreakflush

Warning - This command removes the current set of Outbreak Filter Rules, leaving your
network exposed until the next rule download.Run "outbreakupdate force" command to
immediately download Outbreak Filter Rules.
```

```
Are you sure that you want to clear the current rules?[N]> y

Cleared the current rules.

mail3.example.com>
```

outbreakstatus

说明

outbreakstatus 命令显示当前病毒爆发过滤器功能设置，包括病毒爆发过滤器功能是否已启用、任意病毒爆发规则以及当前阈值。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> outbreakstatus

Outbreak Filters: Enabled

Component              Last Update                       Version
CASE Core Files        26 Jan 2014 06:45 (GMT +00:00)    3.3.1-005
CASE Utilities         26 Jan 2014 06:45 (GMT +00:00)    3.3.1-005
Outbreak Rules         26 Jan 2014 07:00 (GMT +00:00)    20140126_063240

   Threat Outbreak         Outbreak
   Level  Rule Name        Rule Description
   ------------------------------------------------------------------------
   5   OUTBREAK_0002187_03  A reported a MyDoom.BB outbreak.
   5   OUTBREAK_0005678_00  This configuration file was generated by...
   3   OUTBREAK_0000578_00  This virus is distributed in pictures of...

Outbreak Filter Rules with higher threat levels pose greater risks.
(5 = highest threat, 1 = lowest threat)

Last update: Mon Jan 27 04:36:27 2014

mail3.example.com>
```

outbreakupdate

说明

请求立即更新 CASE 规则和引擎核心。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令不支持批处理格式。

示例

```
elroy.run> outbreakupdate

Requesting updates for Outbreak Filter Rules.
```

策略实施

本部分包含以下 CLI 命令：

- dictionaryconfig
- exceptionconfig
- filters
- policyconfig
- quarantineconfig
- scanconfig
- stripheaders
- textconfig

dictionaryconfig

说明

配置内容词典。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

使用 `dictionaryconfig -> new` 可以创建词典，使用 `dictionaryconfig -> delete` 可以删除词典。

创建词典

```
example.com> dictionaryconfig

No content dictionaries have been defined.

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new

Enter a name for this content dictionary.
[]> HRWords

Do you wish to specify a file for import?[N]>

Enter new words or regular expressions, enter a blank line to finish.
<list of words typed here>

Currently configured content dictionaries:
1.HRWords

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> delete

Enter the number of the dictionary you want to delete:
1.HRWords
[]> 1

Content dictionary "HRWords" deleted.
No content dictionaries have been defined.

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]>
```

创建词典 2

在本示例中，会创建一个名为“secret_words”的新词典，以包含术语“codename”。词典一经输入，则 `edit -> settings` 子命令用于为词典中的词定义大小写以及字词边界检测。

```
mail3.example.com> dictionaryconfig

No content dictionaries have been defined.

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new

Enter a name for this content dictionary.
[]> secret_words

Do you wish to specify a file for import?[N]>

Enter new words or regular expressions, enter a blank line to finish.
codename

Currently configured content dictionaries:
1. secret_words
```

```
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1

Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> settings

Do you want to ignore case when matching using this dictionary?[Y]>

Do you want strings in this dictionary to only match complete words?[Y]>

Enter the default encoding to be used for exporting this dictionary:
1.US-ASCII
2.Unicode (UTF-8)
3.Unicode (UTF-16)
4.西欧语言/拉丁语-1 (ISO 8859-1)
5.西欧语言/拉丁语-1 (Windows CP1252)
6.繁体中文 (Big 5)
7.简体中文 (GB 2312)
8.简体中文 (HZ GB 2312)
9.韩语 (ISO 2022-KR)
10.韩语 (KS-C-5601/EUC-KR)
11.日语 (Shift-JIS (X0123))
12.日语 (ISO-2022-JP)
13.日语 (EUC)
[2]>

Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]>

Currently configured content dictionaries:
1. secret_words

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added new dictionary: secret_words

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

导入词典

在下面的示例中，使用 dictionaryconfig 命令， profanity.txt 文本文件中的 84 个术语会以 Unicode (UTF-8) 形式导入名为 profanity 的词典。

```
mail3.example.com> dictionaryconfig

No content dictionaries have been defined.

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new

Enter a name for this content dictionary.
[]> profanity

Do you wish to specify a file for import?[N]> y

Enter the name of the file to import:
[]> profanity.txt

Enter the encoding to use for the imported file:
1.US-ASCII
2.Unicode (UTF-8)
3.Unicode (UTF-16)
4.西欧语言/拉丁语-1 (ISO 8859-1)
5.西欧语言/拉丁语-1 (Windows CP1252)
6.繁体中文 (Big 5)
7.简体中文 (GB 2312)
8.简体中文 (HZ GB 2312)
9.韩语 (ISO 2022-KR)
10.韩语 (KS-C-5601/EUC-KR)
11.日语 (Shift-JIS (X0123))
12.日语 (ISO-2022-JP)
13.日语 (EUC)
[2]>

84 entries imported successfully.
Currently configured content dictionaries:
1. profanity

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
```

导出词典

在下面的示例中，使用 dictionaryconfig 命令， secret_words 词典会导出到名为 secret_words_export.txt 的文本文件。

```
mail3.example.com> dictionaryconfig

Currently configured content dictionaries:
1. secret_words

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
```

```
[]> edit

Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1

Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> export

Enter a name for the exported file:
[]> secret_words_export.txt

mail3.example.com> dictionaryconfig

Currently configured content dictionaries:
1. secret_words

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit

Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1

Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> export

Enter a name for the exported file:
[]> secret_words_export.txt
```

exceptionconfig

说明

使用 CLI 中的 exceptionconfig 命令可以创建域例外表。在本示例中，邮件地址“admin@zzzaaazzz.com”会添加到域例外表，策略为“Allow”。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> exceptionconfig

Choose the operation you want to perform:
- NEW - Create a new domain exception table entry
[]> new

Enter a domain, sub-domain, user, or email address for which you wish to
provide an exception:
[]> mail.partner.com

Any of the following passes:
- @[IP address]
  Matches any email address with this IP address.
- @domain
  Matches any email address with this domain.
- @.partial.domain
  Matches any email address domain ending in this domain.
- user@
  Matches any email address beginning with user@.
- user@domain
  Matches entire email address.

Enter a domain, sub-domain, user, or email address for which you wish to
provide an exception:
[]> admin@zzzaaazzz.com

Choose a policy for this domain exception:
1.Allow
2.Reject
[1]> 1

Choose the operation you want to perform:
- NEW - Create a new domain exception table entry
- EDIT - Edit a domain exception table entry
- DELETE - Delete a domain exception table entry
- PRINT - Print all domain exception table entries
- SEARCH - Search domain exception table
- CLEAR - Clear all domain exception entries
[]>
```

filters

说明

配置消息处理选项。

Usage

提交：此命令需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

在本示例中， `filter` 命令用于创建三个新的过滤器。

- 第一个过滤器命名为 **`big_messages`**。它使用 `ody-size` 规则丢弃大于 10 MB 的邮件。
- 第二个过滤器命名为 **`no_mp3s`**。它使用 `attachment-filename` 规则丢弃包含文件扩展名为 `.mp3` 的附件的邮件。
- 第三个过滤器命名为 **`mailfrompm`**。它使用 `mail-from` 规则检查来自 `postmaster@example.com` 的所有邮件并密件抄送到 `administrator@example.com`。

使用 `filter -> list` 子命令，系统会列出过滤器以确认其处于活动状态并有效，然后使用 `move` 子命令切换第一个和最后一个过滤器的位置。最后，确定更改，以便过滤器生效。

```
mail3.example.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new

Enter filter script.Enter '.' on its own line to end.
big_messages:
    if (body-size >= 10M) {
       drop();
    }
.
1 filters added.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script.Enter '.' on its own line to end.
no_mp3s:
    if (attachment-filename == '\\.mp3$') {
        drop();
     }
.
1 filters added.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
```

```
Enter filter script.Enter '.' on its own line to end.
mailfrompm:
    if (mail-from == "^postmaster$")
     { bcc ("administrator@example.com");}
.
1 filters added.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list
```

policyconfig

说明

配置按收件人或基于发件人的策略。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

- 创建传入邮件策略以丢弃垃圾邮件和存档疑似垃圾邮件，（第 3-191 页）
- 为销售团队创建策略，（第 3-193 页）
- 为工程团队创建策略，（第 3-195 页）
- 创建 scan_for_confidential 内容过滤器，（第 3-197 页）
- 创建 no_mp3s 和 ex_employee 内容过滤器，（第 3-201 页）
- 为特定策略启用内容过滤器，（第 3-206 页）
- 默认传出策略的 DLP 策略，（第 3-209 页）
- 创建传入策略以丢弃标识为大宗邮件或社交网络邮件的邮件，（第 3-211 页）

创建传入邮件策略以丢弃垃圾邮件和存档疑似垃圾邮件

在本示例中，policyconfig -> edit -> antispam 子命令用于为默认传入邮件策略编辑反垃圾邮件设置。（请注意，在 GUI 中的邮件安全管理器功能中有相同的配置可用。）

- 首先，被*明确*标识为垃圾邮件的邮件会被选为不进行存档，它们将被丢弃。
- *疑似*垃圾邮件的邮件会被选为进行存档。它们也会被发送到名为 quarantine.example.com 的服务器上安装的垃圾邮件隔离区。文本 [quarantined: possible spam] 会被添加到主题行前，X-quarantined: true 的特殊信头会被配置为添加到这些可疑邮件。在此情形下，管理员和最终用户可以检查隔离区是否存在误报的垃圾邮件，而且管理员可以在必要时调整疑似垃圾邮件阈值。

最后，提交更改。

```
mail3.example.com> policyconfig

Would you like to configure Incoming or Outgoing Mail Policies?
1.Incoming
2.Outgoing
[1]> 1


Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit

    Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
    -----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                           Protection:               ----------   -----------
                                           ----------

1.  DEFAULT      Ironport     Mcafee       N/A          N/A          Off          Enabled


Enter the name or number of the entry you wish to edit:
[]> 1

Policy Summaries:

Anti-Spam: IronPort - Deliver, Prepend "[SPAM] " to Subject
Suspect-Spam: IronPort - Deliver, Prepend "[SUSPECTED SPAM] " to Subject
Anti-Virus: Off
Content Filters: Off (No content filters have been created)

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy
[]> antispam
```

```
Choose the operation you want to perform:
- EDIT - Edit Anti-Spam policy
- DISABLE - Disable Anti-Spam policy (Disables all policy-related actions)
[]> edit

Begin Anti-Spam configuration

Some messages will be positively identified as spam.Some messages will be
identified as suspected spam.You can set the IronPort Anti-Spam Suspected Spam Threshold
below.
The following configuration options apply to messages POSITIVELY identified as spam:
What score would you like to set for the IronPort Anti-Spam spam threshold?
[90]> 90

1.DELIVER
2.DROP
3.BOUNCE
4.IRONPORT QUARANTINE
What do you want to do with messages identified as spam?
[1]> 2

Do you want to archive messages identified as spam?[N]>

Do you want to enable special treatment of suspected spam?[Y]> y

What score would you like to set for the IronPort Anti-Spam suspect spam threshold?
[50]> 50

The following configuration options apply to messages identified as SUSPECTED spam:
1.DELIVER
2.DROP
3.BOUNCE
4.IRONPORT QUARANTINE
What do you want to do with messages identified as SUSPECTED spam?
[1]> 4

Do you want to archive messages identified as SUSPECTED spam?[N]> y

1.PREPEND
2.APPEND
3.NONE
Do you want to add text to the subject of messages identified as SUSPECTED spam?
[1]> 1

What text do you want to prepend to the subject?
[[SUSPECTED SPAM] ]> [quarantined: possible spam]

Do you want to add a custom header to messages identified as SUSPECTED spam?[N]> y

Enter the name of the header:
[]> X-quarantined

Enter the text for the content of the header:
[]> true


Anti-Spam configuration complete

Policy Summaries:

Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Content Filters: Off (No content filters have been created)
```

```
Outbreak Filters: Enabled.No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy
[]>

Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

DEFAULT      Ironport     Mcafee       N/A          N/A          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> configured anti-spam for Incoming Default Policy

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

为销售团队创建策略

```
Incoming Mail Policy Configuration

Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

DEFAULT      Ironport     Mcafee       N/A          N/A          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> new

Enter the name for this policy:
[]> sales_team

Begin entering policy members.The following types of entries are allowed:
Username entries such as joe@, domain entries such as @example.com, sub-domain
entries such as @.example.com, LDAP group memberships such as ldap(Engineers)

Enter a member for this policy:
[]> ldap(sales)
```

```
Please select an LDAP group query:
1.PublicLDAP.ldapgroup
[1]> 1

Is this entry a recipient or a sender?
1.Recipient
2.Sender
[1]> 1

Add another member?[Y]> n

Would you like to enable Anti-Spam support?[Y]> y

Use the policy table default?[Y]> n

Begin Anti-Spam configuration

Some messages will be positively identified as spam.Some messages will be
identified as suspected spam.You can set the IronPort Anti-Spam Suspected Spam Threshold
below.
The following configuration options apply to messages POSITIVELY identified as spam:
What score would you like to set for the IronPort Anti-Spam spam threshold?
[90]> 90

1.DELIVER
2.DROP
3.BOUNCE
4.IRONPORT QUARANTINE
What do you want to do with messages identified as spam?
[1]> 2

Do you want to archive messages identified as spam?[N]> n

Do you want to enable special treatment of suspected spam?[Y]> y

What score would you like to set for the IronPort Anti-Spam suspect spam
threshold?
[50]> 50

The following configuration options apply to messages identified as SUSPECTED
spam:
1.DELIVER
2.DROP
3.BOUNCE
4.IRONPORT QUARANTINE
What do you want to do with messages identified as SUSPECTED spam?
[1]> 4

Do you want to archive messages identified as SUSPECTED spam?[N]> n

1.PREPEND
2.APPEND
3.NONE
Do you want to add text to the subject of messages identified as SUSPECTED
spam?
[1]> 3

Do you want to add a custom header to messages identified as SUSPECTED spam?[N]> n

Anti-Spam configuration complete

Would you like to enable Anti-Virus support?[Y]> y
```

```
Use the policy table default?[Y]> y

Would you like to enable Outbreak Filters for this policy?[Y]> y

Use the policy table default?[Y]> y

Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

然后，为工程团队（三个单独的邮件收件人）创建策略，指定 .dwg 文件已经从病毒爆发过滤器扫描中排除。

为工程团队创建策略

```
Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> new

Enter the name for this policy:
[]> engineering

Begin entering policy members.The following types of entries are allowed:
Username entries such as joe@, domain entries such as @example.com, sub-domain entries
such as @.example.com, LDAP group memberships such as ldap(Engineers)

Enter a member for this policy:
[]> bob@example.com
```

```
Is this entry a recipient or a sender?
1.Recipient
2.Sender
[1]> 1

Add another member?[Y]> y

Enter a member for this policy:
[]> fred@example.com

Is this entry a recipient or a sender?
1.Recipient
2.Sender
[1]> 1

Add another member?[Y]> y

Enter a member for this policy:
[]> joe@example.com

Is this entry a recipient or a sender?
1.Recipient
2.Sender
[1]> 1

Add another member?[Y]> n

Would you like to enable Anti-Spam support?[Y]> y

Use the policy table default?[Y]> y

Would you like to enable Anti-Virus support?[Y]> y

Use the policy table default?[Y]> y

Would you like to enable Outbreak Filters for this policy?[Y]> y

Use the policy table default?[Y]> n

Would you like to modify the list of file extensions that bypass
Outbreak Filters?[N]> y


Choose the operation you want to perform:
- NEW - Add a file extension
[]> new

Enter a file extension:
[]> dwg


Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]> print

The following file extensions will bypass Outbreak Filter processing:
dwg


Choose the operation you want to perform:
- NEW - Add a file extension
```

```
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]>

Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

engineering  Default      Default      Default      Default      Default      Enabled

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

下一步，创建传入邮件概述策略表中要使用的三个新内容过滤器。

在 CLI 中，`policyconfig` 命令的 `filters` 子命令等同于传入内容过滤器 GUI 页。当您在 CLI 中创建内容过滤器，您必须使用 `save` 子命令来保存过滤器并返回到 `policyconfig` 命令。

首先，请创建 `scan_for_confidential` 内容过滤器：

创建 `scan_for_confidential` 内容过滤器

```
Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

engineering  Default      Default      Default      Default      Default      Enabled

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> filters

No filters defined.
```

```
Choose the operation you want to perform:
- NEW - Create a new filter
[]> new

Enter a name for this filter:
[]> scan_for_confidential

Enter a description or comment for this filter (optional):
[]> scan all incoming mail for the string 'confidential'

Filter Name:  scan_for_confidential

Conditions:
Always Run

Actions:
No actions defined yet.

Description:
scan all incoming mail for the string 'confidential'

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add

1.Condition
2.Action
[1]> 1

1.Message Body Contains
2.Only Body Contains (Attachments are not scanned)
3.Message Body Size
4.Subject Header
5.Other Header
6.Attachment Contains
7.Attachment File Type
8.Attachment Name
9.Attachment MIME Type
10.Attachment Protected
11.Attachment Unprotected
12.Attachment Corrupt
13.Envelope Recipient Address
14.Envelope Recipient in LDAP Group
15.Envelope Sender Address
16.Envelope Sender in LDAP Group
17.Reputation Score
18.Remote IP
19.DKIM authentication result
20.SPF verification result
[1]> 1

Enter regular expression or smart identifier to search message contents for:
[]> confidential

Threshold required for match:
[1]> 1

Filter Name:  scan_for_confidential

Conditions:
body-contains("confidential", 1)
```

```
Actions:
No actions defined yet.

Description:
scan all incoming mail for the string 'confidential'

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[]> add

1.Condition
2.Action
[1]> 2

1.Bcc
2.Notify
3.Redirect To Alternate Email Address
4.Redirect To Alternate Host
5.Insert A Custom Header
6.Insert A Message Tag
7.Strip A Header
8.Send From Specific IP Interface
9.Drop Attachments By Content
10.Drop Attachments By Name
11.Drop Attachments By MIME Type
12.Drop Attachments By File Type
13.Drop Attachments By Size
14.Send To System Quarantine
15.Duplicate And Send To System Quarantine
16.Add Log Entry
17.Drop (Final Action)
18.Bounce (Final Action)
19.Skip Remaining Content Filters (Final Action)
20.Encrypt (Final Action)
21.Encrypt on Delivery
22.Skip Outbreak Filters check
[1]> 1

Enter the email address(es) to send the Bcc message to:
[]> hr@example.com

Do you want to edit the subject line used on the Bcc message?[N]> y

Enter the subject to use:
[$Subject]> [message matched confidential filter]

Do you want to edit the return path of the Bcc message?[N]> n

Filter Name:  scan_for_confidential

Conditions:
body-contains("confidential", 1)

Actions:
bcc ("hr@example.com", "[message matched confidential filter]")

Description:
scan all incoming mail for the string 'confidential'

Choose the operation you want to perform:
- RENAME - Rename this filter
```

```
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> add

1.Condition
2.Action
[1]> 2

1.Bcc
2.Notify
3.Redirect To Alternate Email Address
4.Redirect To Alternate Host
5.Insert A Custom Header
6.Insert A Message Tag
7.Strip A Header
8.Send From Specific IP Interface
9.Drop Attachments By Content
10.Drop Attachments By Name
11.Drop Attachments By MIME Type
12.Drop Attachments By File Type
13.Drop Attachments By Size
14.Send To System Quarantine
15.Duplicate And Send To System Quarantine
16.Add Log Entry
17.Drop (Final Action)
18.Bounce (Final Action)
19.Skip Remaining Content Filters (Final Action)
20.Encrypt (Final Action)
21.Encrypt on Delivery
22.Skip Outbreak Filters check
[1]> 14

1.Policy
[1]> 1

Filter Name:  scan_for_confidential

Conditions:
body-contains("confidential", 1)

Actions:
bcc ("hr@example.com", "[message matched confidential filter]")
quarantine ("Policy")

Description:
scan all incoming mail for the string 'confidential'

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- MOVE - Reorder the conditions or actions
- SAVE - Save filter
[]> save

Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
```

```
- DELETE - Delete a filter
- PRINT - Print all filters
- RENAME - Rename a filter
[]>
```

创建 no_mp3s 和 ex_employee 内容过滤器

```
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- RENAME - Rename a filter
[]> new

Enter a name for this filter:
[]> no_mp3s

Enter a description or comment for this filter (optional):
[]> strip all MP3 attachments

Filter Name:  no_mp3s

Conditions:
Always Run

Actions:
No actions defined yet.

Description:
strip all MP3 attachments

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add

1.Condition
2.Action
[1]> 2

1.Bcc
2.Notify
3.Redirect To Alternate Email Address
4.Redirect To Alternate Host
5.Insert A Custom Header
6.Insert A Message Tag
7.Strip A Header
8.Send From Specific IP Interface
9.Drop Attachments By Content
10.Drop Attachments By Name
11.Drop Attachments By MIME Type
12.Drop Attachments By File Type
13.Drop Attachments By Size
14.Send To System Quarantine
15.Duplicate And Send To System Quarantine
16.Add Log Entry
17.Drop (Final Action)
18.Bounce (Final Action)
19.Skip Remaining Content Filters (Final Action)
20.Encrypt (Final Action)
21.Encrypt on Delivery
```

```
22.Skip Outbreak Filters check
[1]> 12

Enter the file type to strip:
[]> mp3

Do you want to enter specific text to use in place of any stripped attachments?[N]> n

Filter Name:  no_mp3s

Conditions:
Always Run

Actions:
drop-attachments-by-filetype("mp3")

Description:
strip all MP3 attachments

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- SAVE - Save filter
[]> save

Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter
[]> new

Enter a name for this filter:
[]> ex_employee

Enter a description or comment for this filter (optional):
[]> bounce messages intended for Doug

Filter Name:  ex_employee

Conditions:
Always Run

Actions:
No actions defined yet.

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add

1.Condition
2.Action
```

```
[1]> 1

1.Message Body Contains
2.Only Body Contains (Attachments are not scanned)
3.Message Body Size
4.Subject Header
5.Other Header
6.Attachment Contains
7.Attachment File Type
8.Attachment Name
9.Attachment MIME Type
10.Attachment Protected
11.Attachment Unprotected
12.Attachment Corrupt
13.Envelope Recipient Address
14.Envelope Recipient in LDAP Group
15.Envelope Sender Address
16.Envelope Sender in LDAP Group
17.Reputation Score
18.Remote IP
19.DKIM authentication result
20.SPF verification result
[1]> 13

Enter regular expression to search Recipient address for:
[]> doug

Filter Name:  ex_employee

Conditions:
rcpt-to == "doug"

Actions:
No actions defined yet.

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[]> add

1.Condition
2.Action
[1]> 2

1.Bcc
2.Notify
3.Redirect To Alternate Email Address
4.Redirect To Alternate Host
5.Insert A Custom Header
6.Insert A Message Tag
7.Strip A Header
8.Send From Specific IP Interface
9.Drop Attachments By Content
10.Drop Attachments By Name
11.Drop Attachments By MIME Type
12.Drop Attachments By File Type
13.Drop Attachments By Size
14.Send To System Quarantine
15.Duplicate And Send To System Quarantine
```

```
16.Add Log Entry
17.Drop (Final Action)
18.Bounce (Final Action)
19.Skip Remaining Content Filters (Final Action)
20.Encrypt (Final Action)
21.Encrypt on Delivery
22.Skip Outbreak Filters check
[1]> 2

Enter the email address(es) to send the notification to:
[]> joe@example.com

Do you want to edit the subject line used on the notification?[N]> y

Enter the subject to use:
[]> message bounced for ex-employee of example.com

Do you want to edit the return path of the notification?[N]> n

Do you want to include a copy of the original message as an attachment to the
notification?[N]> y

Filter Name:  ex_employee

Conditions:
rcpt-to == "doug"

Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of
example.com")

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> add

1.Condition
2.Action
[1]> 2

1.Bcc
2.Notify
3.Redirect To Alternate Email Address
4.Redirect To Alternate Host
5.Insert A Custom Header
6.Insert A Message Tag
7.Strip A Header
8.Send From Specific IP Interface
9.Drop Attachments By Content
10.Drop Attachments By Name
11.Drop Attachments By MIME Type
12.Drop Attachments By File Type
13.Drop Attachments By Size
14.Send To System Quarantine
15.Duplicate And Send To System Quarantine
16.Add Log Entry
17.Drop (Final Action)
18.Bounce (Final Action)
```

```
19.Skip Remaining Content Filters (Final Action)
20.Encrypt (Final Action)
21.Encrypt on Delivery
22.Skip Outbreak Filters check
[1]> 18

Filter Name:  ex_employee

Conditions:
rcpt-to == "doug"

Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of
example.com")
bounce()

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> save

Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments
3. ex_employee: bounce messages intended for Doug

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter
[]>

Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

engineering  Default      Default      Default      Default      Default      Enabled

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

为特定策略启用内容过滤器

代码示例说明如何再次启用策略，以便为某些策略启用内容过滤器，而不为另一些策略启用内容过滤器。

```
Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

engineering  Default      Default      Default      Default      Default      Enabled

DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> edit

    Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
    -----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                           Protection:               ----------   -----------
                                           ----------

1.  sales_team   IronPort     Default      Default      Default      Default      Default

2.  engineering  Default      Default      Default      Default      Default      Enabled

3.  DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Enter the name or number of the entry you wish to edit:
[]> 3

Policy Summaries:

Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Graymail Detection:  Unsubscribe - Disabled
Content Filters: Off
Outbreak Filters: Enabled.No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]> filters


Choose the operation you want to perform:
- ENABLE - Enable Content Filters policy
```

```
[]> enable

1.scan_for_confidential
2.no_mp3s
3.ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1

1.Active scan_for_confidential
2.no_mp3s
3.ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 2

1.Active scan_for_confidential
2.Active no_mp3s
3.ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3

1.Active scan_for_confidential
2.Active no_mp3s
3.Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>

Policy Summaries:

Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Graymail Detection:  Unsubscribe - Disabled
Content Filters: Enabled.Filters: scan_for_confidential, no_mp3s, ex_employee
Outbreak Filters: Enabled.No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]>

Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

engineering  Default      Default      Default      Default      Default      Enabled

DEFAULT      Ironport     Mcafee       N/A          Off          Enabled      Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
```

```
- CLEAR - Clear all policies
[]> edit

    Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
    -----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                           Protection:               ----------   -----------
                                           ----------

1.  sales_team   IronPort     Default      Default      Default      Default      Default

2.  engineering  Default      Default      Default      Default      Default      Enabled

3.  DEFAULT      Ironport     Mcafee       N/A          Off          Off          Enabled


Enter the name or number of the entry you wish to edit:
[]> 2

Policy Summaries:

Anti-Spam: Default
Anti-Virus: Default
Graymail Detection:  Unsubscribe - Default
Content Filters: Default
Outbreak Filters: Enabled.Bypass extensions: dwg

Choose the operation you want to perform:
- NAME - Change name of policy
- NEW - Add a new member
- DELETE - Remove a member
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]> filters


Choose the operation you want to perform:
- DISABLE - Disable Content Filters policy (Disables all policy-related
actions)
- ENABLE - Enable Content Filters policy
[]> enable

1.scan_for_confidential
2.no_mp3s
3.ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1

1.Active scan_for_confidential
2.no_mp3s
3.ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3

1.Active scan_for_confidential
2.no_mp3s
3.Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>
```

```
Policy Summaries:

Anti-Spam: Default
Anti-Virus: Default
Graymail Detection:  Unsubscribe - Default
Content Filters: Enabled.Filters: scan_for_confidential, ex_employee
Outbreak Filters: Enabled.Bypass extensions: dwg

Choose the operation you want to perform:
- NAME - Change name of policy
- NEW - Add a new member
- DELETE - Remove a member
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]>

Incoming Mail Policy Configuration
Name:        Anti-Spam:   Anti-Virus:  Advanced     Graymail:    Content      Outbreak
-----        ----------   ----------   Malware      ----------   Filter:      Filters:
                                       Protection:               ----------   -----------
                                       ----------

sales_team   IronPort     Default      Default      Default      Default      Default

engineering  Default      Default      Default      Default      Enabled      Enabled

DEFAULT      Ironport     Mcafee       N/A          Off          Enabled      Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

注　CLI 不包含在单个策略内添加新的内容过滤器的说明。而是 `filters` 子命令会强制您在 `policyconfig` 命令内的一个子小节管理所有内容过滤器。为此，此示例省略了添加 `drop_large_attachments` 的部分。

默认传出策略的 DLP 策略

下面的示例说明如何在默认传出策略上启用 DLP 策略。

```
mail3.example.com> policyconfig

Would you like to configure Incoming or Outgoing Mail Policies?
1.Incoming
2.Outgoing
[1]> 2
```

```
Outgoing Mail Policy Configuration
Name:    Anti-Spam:  Anti-Virus:  Advanced     Graymail:   Content     Outbreak     DLP:
-----    ----------  ----------   Malware      ----------  Filter:     Filters:     ----
                                  Protection:              ----------  -----------
                                  ----------

DEFAULT  N/A         N/A          N/A          Off         Off         Off          Off


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit

    Name:    Anti-Spam:  Anti-Virus:  Advanced     Graymail:   Content     Outbreak     DLP:
    -----    ----------  ----------   Malware      ----------  Filter:     Filters:     ----
                                      Protection:              ----------  -----------
                                      ----------

1.  DEFAULT  N/A         N/A          N/A          Off         Off         Off          Off


Enter the name or number of the entry you wish to edit:
[]> 1

Policy Summaries:

Anti-Spam: Off
Anti-Virus: Off
Graymail Detection:  Unsubscribe - Disabled
Content Filters: Off (No content filters have been created)
Outbreak Filters: Off
DLP: Off

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- DLP - Modify DLP policy
[]> dlp

Choose the operation you want to perform:
- ENABLE - Enable DLP policy
[]> enable

1.California AB-1298
2.Suspicious Transmission - Zip Files
3.Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[]> 1

1.Active California AB-1298
2.Suspicious Transmission - Zip Files
3.Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[]> 2

1.Active California AB-1298
2.Active Suspicious Transmission - Zip Files
3.Restricted Files
```

```
Enter the policy to toggle on/off, or press enter to finish:
[]> 3

1.Active California AB-1298
2.Active Suspicious Transmission - Zip Files
3.Active Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[]>

Policy Summaries:

Anti-Spam: Off
Anti-Virus: Off
Graymail Detection:  Unsubscribe - Disabled
Content Filters: Off (No content filters have been created)
Outbreak Filters: Off
DLP: Enabled.Policies: California AB-1298, Suspicious Transmission - Zip
Files, Restricted Files

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- DLP - Modify DLP policy
[]>
```

创建传入策略以丢弃标识为大宗邮件或社交网络邮件的邮件

```
mail.example.com> policyconfig

Would you like to configure Incoming or Outgoing Mail Policies?
1.Incoming
2.Outgoing
[1]> 1


Incoming Mail Policy Configuration
Name:     Anti-Spam:   Anti-Virus:   Advanced       Graymail:    Content     Outbreak
-----     ----------   ----------    Malware        ----------   Filter:     Filters:
                                     Protection:                 ----------  -----------
                                     ----------

DEFAULT   Off          N/A           N/A            Off          Off         N/A


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit

    Name:     Anti-Spam:   Anti-Virus:   Advanced      Graymail:    Content     Outbreak
    -----     ----------   ----------    Malware       ----------   Filter:     Filters:
                                         Protection:                ----------  -----------
                                         ----------

1.  DEFAULT   Off          N/A           N/A           Off          Off         N/A
```

```
Enter the name or number of the entry you wish to edit:
[]> 1

Policy Summaries:

Anti-Spam: Off
Graymail Detection: Off
Content Filters: Off (No content filters have been created)

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- GRAYMAIL - Modify Graymail policy
- FILTERS - Modify filters
[]> graymail


Choose the operation you want to perform:
- ENABLE - Enable Graymail policy
[]> enable

Begin Graymail configuration

Do you want to enable Safe Unsubscribe?[N]> y

Do you want to perform Safe Unsubscribe action only for unsigned messages
(recommended)?[Y]>

Do you want to enable actions on messages identified as Marketing Email?[N]>

Do you want to enable actions on messages identified as Social Networking Email?[N]> y

1.DELIVER
2.DROP
3.BOUNCE
What do you want to do with messages identified as Social Networking Email?
[1]> 2

Do you want to archive messages identified as Social Networking Email?[N]>

Do you want to enable actions on messages identified as Bulk Email?[N]> y

1.DELIVER
2.DROP
3.BOUNCE
What do you want to do with messages identified as Bulk Email?
[1]> 2

Do you want to archive messages identified as Bulk Email?[N]>

Graymail configuration complete.

Policy Summaries:

Anti-Spam: Off
Graymail Detection:  Unsubscribe - Enabled
    Social Networking mails : Drop
    Bulk mails : Drop
Content Filters: Off (No content filters have been created)

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- GRAYMAIL - Modify Graymail policy
- FILTERS - Modify filters
[]>
```

quarantineconfig

说明

配置系统隔离区。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> quarantineconfig

Currently configured quarantines:

 #  Quarantine Name    Size (MB)  % full  Messages  Retention  Policy
 1  Outbreak           3,072      0.0          1        12h    Release
 2  Policy             1,024      0.1        497        10d    Delete
 3  Virus              2,048      empty        0        30d    Delete

2,048 MB available for quarantine allocation.

Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- OUTBREAKMANAGE - Manage the Outbreak Filters quarantine.
[]> new

Please enter the name for this quarantine:
[]> HRQuarantine

Retention period for this quarantine.(Use 'd' for days or 'h' for hours or 'm' for
'minutes'.):
[]> 15d
1.Delete
2.发布人
Enter default action for quarantine:
[1]> 2
Do you want to modify the subject of messages that are released because
"HRQuarantine" overflows?[N]>

Do you want add a custom header to messages that are released because
"HRQuarantine" overflows?[N]>

Do you want to strip all attachments from messages that are released
because "HRQuarantine" overflows?[N]>

Do you want default action to apply automatically when quarantine space fills up?[Y]>


Currently configured quarantines:

 #  Quarantine Name     Size (MB) % full  Messages  Retention  Policy
```

```
 1  HRQuarantine        1,024      N/A        N/A        15d   Release
 2  Outbreak            3,072      0.0          1        12h   Release
 3  Policy              1,024      0.1        497        10d   Delete
 4  Virus               2,048      empty        0        30d   Delete
(N/A: Quarantine contents is not available at this time.)

1,024 MB available for quarantine allocation.

Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- OUTBREAKMANAGE - Manage the Outbreak Filters quarantine.
```

用户和隔离区

一旦对添加用户的相关问题回答了 “y” 或 “yes”，您即开始用户管理，在这里您可以管理用户列表。这将允许您将多个添加到隔离区或从隔离区删除用户，而无需全部回答其他隔离区配置问题。在空提示符 ([]>) 处按 Return (Enter) 可以退出用户管理部分，并继续配置隔离区。

注　仅在已经在系统上创建了访客或操作员用户的情况下，才会提示您为隔离区指定用户访问权限。

隔离区的用户列表仅包含属于操作员组或访客组的用户。管理员组的用户始终拥有对隔离区的访问权限。当管理用户列表时，如果所有操作员/访客用户已经位于隔离区用户列表上，则会抑制 NEW 命令。同样，如果没有要删除的用户，则会抑制 DELETE。

scanconfig

说明

配置附件扫描策略。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

示例

在本示例中， `scanconfig` 命令用于设置这些参数。

- 会跳过 video/*、 audio/*、 image/* 的 MIME 类型 （不会为内容扫描这些类型）。
- 最多扫描 10 个级别的嵌套 （递归）存档附件。（默认值为 5 个级别。）
- 要扫描的附件的最大大小为 25 MB；将跳过超过此大小的任何内容。（默认值为 5 MB。）
- 会扫描文档元数据。
- 附件扫描超时设置为 180 秒。

- 未扫描的附件假设为与搜索模式不匹配。（这是默认行为。）
- 会配置 ASCII 编码，以便当未为普通正文或其 MIME 类型为 plain/text 或 plain/html 的任意内容指定任何内容时使用。

注 在将 `assume the attachment matches the search pattern` 设置为 Y 时，无法扫描的邮件将导致邮件过滤器规则评估为 true。这可能导致意外行为，例如隔离与词典不匹配的邮件，但是因其内容无法正确扫描而被隔离。此设置不适用于 RSA 邮件 DLP 扫描。

```
mail3.example.com> scanconfig
There are currently 5 attachment type mappings configured to be SKIPPED.
Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[]> setup
1.Scan only attachments with MIME types or fingerprints in the list.
2.Skip attachments with MIME types or fingerprints in the list.
Choose one:
[2]> 2

Enter the maximum depth of attachment recursion to scan:
[5]> 10

Enter the maximum size of attachment to scan:
[5242880]> 10m

Do you want to scan attachment metadata?[Y]> y

Enter the attachment scanning timeout (in seconds):
[30]> 180

If a message has attachments that were not scanned for any reason (e.g.
because of size, depth limits, or scanning timeout), assume the attachment matches the
search pattern?[N]> n

If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:

1.Deliver
2.Bounce
3.Drop
[1]>

Configure encoding to use when none is specified for plain body text or
anything with MIME type plain/text or plain/html.
1.US-ASCII
2.Unicode (UTF-8)
3.Unicode (UTF-16)
4.西欧语言/拉丁语-1 (ISO 8859-1)
5.西欧语言/拉丁语-1 (Windows CP1252)
6.繁体中文 (Big 5)
7.简体中文 (GB 2312)
8.简体中文 (HZ GB 2312)
9.韩语 (ISO 2022-KR)
10.韩语 (KS-C-5601/EUC-KR)
```

```
11.日语 (Shift-JIS (X0123))
12.日语 (ISO-2022-JP)
13.日语 (EUC)
[1]> 1

Scan behavior changed.

There are currently 5 attachment type mappings configured to be SKIPPED.

Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

[]> print
1.Fingerprint   Image
2.Fingerprint   Media
3.MIME Type     audio/*
4.MIME Type     image/*
5.MIME Type     video/*
```

stripheaders

说明

定义要删除的邮件信头的列表。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> stripheaders

Not currently stripping any headers.

Choose the operation you want to perform:
- SETUP - Set message headers to remove.
[]> setup

Enter the list of headers you wish to strip from the messages before they are
delivered.Separate multiple headers with commas.
[]> Delivered-To

Currently stripping headers: Delivered-To
```

```
Choose the operation you want to perform:
- SETUP - Set message headers to remove.
[]>

mail3.example.com>
```

textconfig

说明

配置文本资源，例如防病毒警告模板、邮件免责声明和通知模板，包括 DLP、退回和加密通知。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

Use `textconfig -> NEW` to create text resources, and `textconfig > delete` to remove them.

```
mail3.example.com> textconfig

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[]> new


What kind of text resource would you like to create?
1.防病毒容器模板
2.防病毒通知模板
3.DLP 通知模板
4.Bounce and Encryption Failure Notification Template
5.Message Disclaimer
6.加密通知模板 (HTML)
7.加密通知模板 (文本)
8.通知模板
[1]> 5

Please create a name for the message disclaimer:
[]> disclaimer 1

Enter the encoding for the message disclaimer:
1.US-ASCII
2.Unicode (UTF-8)
3.Unicode (UTF-16)
4.西欧语言/拉丁语-1 (ISO 8859-1)
5.西欧语言/拉丁语-1 (Windows CP1252)
6.繁体中文 (Big 5)
7.简体中文 (GB 2312)
8.简体中文 (HZ GB 2312)
9.韩语 (ISO 2022-KR)
10.韩语 (KS-C-5601/EUC-KR)
```

```
11.日语 (Shift-JIS (X0123))
12.日语 (ISO-2022-JP)
13.日语 (EUC)
[1]>

Enter or paste the message disclaimer here.Enter '.' on a blank line to end.
This message was sent from an IronPort(tm) Email Security appliance.
.

Message disclaimer "disclaimer 1" created.


Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> delete

Please enter the name or number of the resource to delete:
[]> 1


Message disclaimer "disclaimer 1" has been deleted.


Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[]>
```

使用 `textconfig -> EDIT` 可以修改现有文本资源。您可以更改编码或更换选定文本资源的文本。

导入文本资源

使用 `textconfig -> IMPORT` 可以将文本文件作为文本资源导入。文本文件必须出现在设备上的配置目录中。

```
mail3.example.com> textconfig

Current Text Resources:
1. footer.2.message (Message Footer)

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> import

What kind of text resource would you like to create?
1.防病毒容器模板
2.防病毒通知模板
3.DLP 通知模板
4.Bounce and Encryption Failure Notification Template
5.Message Disclaimer
```

```
6.加密通知模板 (HTML)
7.加密通知模板 (文本)
8.通知模板
[1]> 8

Please create a name for the notification template:
[]> strip.mp3files

Enter the name of the file to import:
[]> strip.mp3.txt

Enter the encoding to use for the imported file:
1.US-ASCII
[ list of encodings ]
[1]>

Notification template "strip.mp3files" created.

Current Text Resources:
1. disclaimer.2.message (Message Disclaimer)
2. strip.mp3files (Notification Template)

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>
```

导出文本资源

使用 `textconfig -> EXPORT` 可以将文本资源导出为文本文件。将会在设备上的配置目录中创建该文本文件。

```
mail3.example.com> textconfig

Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> export

Please enter the name or number of the resource to export:
[]> 2

Enter the name of the file to export:
[strip.mp3]> strip.mp3.txt

Enter the encoding to use for the exported file:
1.US-ASCII
[ list of encoding types ]
[1]>
```

```
File written on machine "mail3.example.com" using us-ascii encoding.

Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>
```

日志记录和提示

本部分包含以下 CLI 命令：

- alertconfig
- displayalerts
- findevent
- grep
- logconfig
- rollovernow
- snmpconfig
- tail

alertconfig

说明

配置邮件警告。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例：创建新的提示

在本示例中，将会创建新的提示收件人 (alertadmin@example.com)，并对其进行设置以接收关键系统、硬件和目录搜集攻击提示。

```
vm30esa0086.ibqa> alertconfig

Not sending alerts (no configured addresses)
```

```
Alerts will be sent using the system-default From Address.

Cisco IronPort AutoSupport: Disabled

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> new

Please enter a new email address to send alerts.
(Ex: "administrator@example.com")
[]> alertadmin@example.com

Choose the Alert Classes.Separate multiple choices with commas.
1.All
2.System
3.Hardware
4.Updater
5.Outbreak Filters
6.Anti-Virus
7.Anti-Spam
8.Directory Harvest Attack Prevention
9.Release and Support Notifications
[1]> 2,3,8

Select a Severity Level.Separate multiple choices with commas.
1.All
2.Critical
3.Warning
4.Information
[1]> 2

Sending alerts to:
  alertadmin@example.com
      Class: Hardware - Severities: Critical
      Class: Directory Harvest Attack Prevention - Severities: Critical
      Class: System - Severities: Critical

Initial number of seconds to wait before sending a duplicate alert: 300
Maximum number of seconds to wait before sending a duplicate alert: 3600
Maximum number of alerts stored in the system are: 50

Alerts will be sent using the system-default From Address.

Cisco IronPort AutoSupport: Disabled

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify alert subscription for an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]>
```

displayalerts

说明

显示设备最近发送的 n 条警告。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
> displayalerts

Date and Time Stamp           Description

--------------------------------------------------------------------------------

10 Mar 2015 11:33:36 +0000    The updater could not validate the server certificate.Server
certificate not validated - unable to get local issuer
certificate

Last message occurred 28 times between Tue Mar 10 10:34:57 2015 and Tue Mar 10 11:32:24
2015.


10 Mar 2015 11:23:39 +0000    The updater has been unable to communicate with the update
server for at least 1h.

Last message occurred 8 times between Tue Mar 10 10:29:57 2015 and Tue Mar 10 11:18:24
2015.


10 Mar 2015 10:33:36 +0000    The updater could not validate the server certificate.Server
certificate not validated - unable to get local issuer
certificate

Last message occurred 26 times between Tue Mar 10 09:33:55 2015 and Tue Mar 10 10:29:57
2015.


10 Mar 2015 10:23:39 +0000    The updater has been unable to communicate with the update
server for at least 1h.

Last message occurred 9 times between Tue Mar 10 09:26:54 2015 and Tue Mar 10 10:22:56
2015.
```

findevent

说明

在邮件日志文件中查找事件。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例：按信封发件人搜索

```
mail.example.com> findevent

Please choose which type of search you want to perform:
1.Search by envelope FROM
2.Search by Message ID
3.Search by Subject
4.Search by envelope TO
[1]> 1

Enter the regular expression to search for.
[]> "

Currently configured logs:
    Log Name            Log Type                      Retrieval           Interval
 ------------------------------------------------------------------------------------
 1. mail_logs           IronPort Text Mail Logs       Manual Download     None
Enter the number of the log you wish to use for message tracking.
[1]> 1

Please choose which set of logs to search:
1.All available log files
2.Select log files by date list
3.Current log file
[3]> 3

No matching message IDs were found
```

示例：按消息 ID 搜索

```
mail.example.com> findevent

Please choose which type of search you want to perform:
1.Search by envelope FROM
2.Search by Message ID
3.Search by Subject
4.Search by envelope TO
[1]> 2

Enter the Message ID (MID) to search for.
[]> 1

Currently configured logs:
    Log Name            Log Type                      Retrieval           Interval
 ------------------------------------------------------------------------------------
 1. mail_logs           IronPort Text Mail Logs       Manual Download     None
Enter the number of the log you wish to use for message tracking.
[1]> 1

Please choose which set of logs to search:
1.All available log files
2.Select log files by date list
```

```
3.Current log file
[3]> 1
```

示例：按主题搜索

```
mail.example.com> findevent

Please choose which type of search you want to perform:
1.Search by envelope FROM
2.Search by Message ID
3.Search by Subject
4.Search by envelope TO
[1]> 3

Enter the regular expression to search for.
[]> "

Currently configured logs:
    Log Name            Log Type                      Retrieval           Interval
 -------------------------------------------------------------------------------
 1. mail_logs           IronPort Text Mail Logs       Manual Download     None
Enter the number of the log you wish to use for message tracking.
[1]> 1

Please choose which set of logs to search:
1.All available log files
2.Select log files by date list
3.Current log file
[3]> 2

Available mail log files, listed by log file start time.Specify multiple log files by
separating with commas or specify a range with a dash:
1.Thu Feb 19 05:18:02 2015
[1]>

No matching message IDs were found
```

示例：按信封收件人搜索

```
mail.example.com> findevent

Please choose which type of search you want to perform:
1.Search by envelope FROM
2.Search by Message ID
3.Search by Subject
4.Search by envelope TO
[1]> 4

Enter the regular expression to search for.
[]> '

Currently configured logs:
    Log Name            Log Type                      Retrieval           Interval
 -------------------------------------------------------------------------------
 1. mail_logs           IronPort Text Mail Logs       Manual Download     None
Enter the number of the log you wish to use for message tracking.
[1]> 1

Please choose which set of logs to search:
```

```
1.All available log files
2.Select log files by date list
3.Current log file
[3]> 3

No matching message IDs were found
```

grep

说明

搜索日志文件中的文本。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

grep 命令可用于搜索日志中的文本字符串。当运行 grep 命令时，请使用以下语法：

```
grep [-C count] [-e regex] [-i] [-p] [-t] [regex] log_name
```

注　必须输入 -e regex 或 regex 才能返回结果。

当运行 grep 命令时，请使用以下选项：

表 3-12　grep 命令选项

选项	说明
-C	提供找到的 grep 模式旁的情景行数。输入一个值以指定要包括的行数。
-e	输入正则表达式。
-i	忽略大小写。
-p	为输出标记页数。
-t	在日志文件尾部运行 grep 命令。
regex	输入正则表达式。

grep 的示例

以下示例显示在防病毒日志内搜索文本字符串 “clean”或“viral”。grep 命令包括一个 regex 表达式：

```
mail3.example.com> grep "CLEAN\\|VIRAL" antivirus

Fri Jun  9 21:50:25 2006 Info: sophos antivirus - MID 1 - Result 'CLEAN' ()
Fri Jun  9 21:53:15 2006 Info: sophos antivirus - MID 2 - Result 'CLEAN' ()
```

```
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 3 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 4 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 5 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 6 - Result 'CLEAN' ()
Fri Jun  9 22:47:42 2006 Info: sophos antivirus - MID 12 - Result 'CLEAN' ()
Fri Jun  9 22:53:04 2006 Info: sophos antivirus - MID 18 - Result 'VIRAL' ()
Fri Jun  9 22:53:05 2006 Info: sophos antivirus - MID 16 - Result 'VIRAL' ()
Fri Jun  9 22:53:06 2006 Info: sophos antivirus - MID 19 - Result 'VIRAL' ()
Fri Jun  9 22:53:07 2006 Info: sophos antivirus - MID 21 - Result 'VIRAL' ()
Fri Jun  9 22:53:08 2006 Info: sophos antivirus - MID 20 - Result 'VIRAL' ()
Fri Jun  9 22:53:08 2006 Info: sophos antivirus - MID 22 - Result 'VIRAL' ()
mail3.example.com>
```

logconfig

说明

配置对日志文件的访问。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

FTP 推送日志订阅的示例

在下面的示例中，`logconfig` 命令用于配置名为 `myDeliveryLogs` 的新传输日志。然后，会配置该日志，以便将其通过 FTP 推送到远程主机。

```
mail3.example.com> logconfig


Currently configured logs:
1."antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2."antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3."asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4."authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5."avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6."bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7."cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8."encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9."error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10."euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11."euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12."ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13."gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14."mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15."reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16."reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17."scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18."slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19."sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20."status" Type: "Status Logs" Retrieval: FTP Poll
21."system_logs" Type: "System Logs" Retrieval: FTP Poll
22."trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
```

```
23."updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> new

Choose the log file type for this subscription:
1.IronPort Text Mail Logs
2.qmail Format Mail Logs
3.Delivery Logs
4.Bounce Logs
5.Status Logs
6.Domain Debug Logs
7.Injection Debug Logs
8.SMTP Conversation Logs
9.System Logs
10.CLI Audit Logs
11.FTP Server Logs
12.HTTP Logs
13.NTP logs
14.LDAP Debug Logs
15.Anti-Spam Logs
16.Anti-Spam Archive
17.Anti-Virus Logs
18.Anti-Virus Archive
19.Scanning Logs
20.IronPort Spam Quarantine Logs
21.IronPort Spam Quarantine GUI Logs
22.Reporting Logs
23.Reporting Query Logs
24.Updater Logs
25.Tracking Logs
26.Safe/Block Lists Logs
27.Authentication Logs
[1]> 8

Please enter the name for the log:
[]> myDeliveryLogs

Choose the method to retrieve the logs.
1.FTP Poll
2.FTP Push
3.SCP Push
4.Syslog Push
[1]> 2


Hostname to deliver the logs:
[]> yourhost.example.com

Username on the remote host:
[]> yourusername

Password for youruser:
[]> thepassword

Directory on remote host to place logs:
[]> /logs
```

```
Filename to use for log files:
[conversation.text]>

Maximum time to wait before transferring:
[3600]>

Maximum filesize before transferring:
[10485760]>

Currently configured logs:
1."antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2."antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3."asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4."authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5."avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6."bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7."cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8."encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9."error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10."euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11."euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12."ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13."gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14."mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15."myDeliveryLogs" Type: "SMTP Conversation Logs" Retrieval: FTP Push - Host
yourhost.example.com
16."reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
17."reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
18."scanning" Type: "Scanning Logs" Retrieval: FTP Poll
19."slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
20."sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
21."status" Type: "Status Logs" Retrieval: FTP Poll
22."system_logs" Type: "System Logs" Retrieval: FTP Poll
23."trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
24."updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
```

SCP 推送日志订阅的示例

在下面的示例中，`logconfig` 命令用于配置名为 `LogPush` 的新传输日志。该日志配置为通过 SCP 推送到 IP 地址为 10.1.1.1 的远程主机 （作为用户 `logger`），并存储在目录 `/tmp` 中。请注意，当日志取回方法为 SCP 推送时，会从 `logconfig` 命令内自动调用 `sshconfig` 命令。（有关主机密钥的信息，请参阅 《*思科邮件安全设备 AsyncOS 用户指南*》中的 “配置主机密钥”，有关用户密钥的更多信息信息，请参阅 “管理安全外壳 (SSH) 密钥”。）另请注意，可以在主机名提示符处使用 IP 地址。

```
mail3.example.com> logconfig

Currently configured logs:
1."antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2."antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3."asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4."authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5."avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6."bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7."cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8."encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9."error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10."euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11."euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12."ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13."gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
```

```
14."mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15."reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16."reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17."scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18."slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19."sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20."status" Type: "Status Logs" Retrieval: FTP Poll
21."system_logs" Type: "System Logs" Retrieval: FTP Poll
22."trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23."updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.

[]> new
Choose the log file type for this subscription:
1.IronPort Text Mail Logs
2. qmail Format Mail Logs
3.Delivery Logs
4.Bounce Logs
5.Status Logs
6.Domain Debug Logs
7.Injection Debug Logs
8.SMTP Conversation Logs
9.System Logs
10.CLI Audit Logs
11.FTP Server Logs
12.HTTP Logs
13.NTP logs
14.LDAP Debug Logs
15.Anti-Spam Logs
16.Anti-Spam Archive
17.Anti-Virus Logs
18.Anti-Virus Archive
19.Scanning Logs
20.IronPort Spam Quarantine Logs
21.IronPort Spam Quarantine GUI Logs
22.Reporting Logs
23.Reporting Query Logs
24.Updater Logs
25.Tracking Logs
26.Safe/Block Lists Logs
27.Authentication Logs
[1]> 3

Please enter the name for the log:
[]> LogPush

Choose the method to retrieve the logs.
1.FTP Poll
2.FTP Push
3.SCP Push
[1]> 3


Hostname to deliver the logs:
[]> 10.1.1.1
```

```
Port to connect to on the remote host:
[22]>

Username on the remote host:
[]> logger

Directory on remote host to place logs:
[]> /tmp

Filename to use for log files:
[delivery.log]>

Maximum time to wait before transferring:
[3600]>

Maximum filesize before transferring:
[10485760]>

协议：
1.SSH1
2.SSH2
[2]> 2

Do you want to enable host key checking?[N]> y

Do you want to automatically scan the host for its SSH key, or enter it
manually?
1.Automatically scan.
2.Enter manually.
[1]> 1



SSH2:dsa
10.1.1.1 ssh-dss
AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwEsArt9LVE2ts5yE9JBTSdUwLvoq0G3FRqifrce92zgyHtc/ZWyXav
UTIM3Xd1bpiEcscMp2XKpSnPPx21y8bqkpJsSCQcM8zZMDjnOPm8ghiwHXYh7oNEUJCCPnPxAy44rlJ5Yz4x9eIoAL
p0dHU0GR+j1NAAAAFQDQi5GY/X9PlDM3fPMvEx7wc0edlwAAAIB9cgMTEFP1WTAGrlRtbowZP5zWZtVDTxLhdXzjlo
4+bB4hBR7DKuc80+naAFnThyH/J8R3WlJVF79M5geKJbXzuJGDK3Zwl3UYefPqBqXp2O1zLRQSJYx1WhwYz/rooopN
1BnF4sh12mtq3tde1176bQgtwaQA4wKO15k3zOWsPwAAAIAicRYat3y+Blv/V6wdE6BBk+oULv3eK38gafuip4WMBx
kG9GO6EQi8nss82oznwWBy/pITRQfh4MBmlxTF4VEY00sARrlZtuUJC1QGQvCgh7Nd3YNais2CSbEKBEaIOTF6+SX2
RNpcUF3Wg5ygw92xtqQPKMcZeLtK2ZJRkhC+Vw==

Add the preceding host key(s) for 10.1.1.1?[Y]> y

Currently installed host keys:
1.10.1.1.1 1024 35 122606420764474441178474079962066753 25...3520565607
2.10.1.1.1 ssh-dss AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwE...JRkhC+Vw==

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display this machine's host keys.
[]>
Maximum filesize before transferring:
[10485760]>

协议：
1.SSH1
2.SSH2
```

```
[2]> 2

Do you want to enable host key checking?[N]> y

Currently installed host keys:

Choose the operation you want to perform:
- NEW - Add a new key.
- SCAN - Automatically download a host key.
- HOST - Display this machine's host keys.
[]> scan

Choose the ssh protocol type:
1.SSH1:rsa
2.SSH2:rsa
3.SSH2:dsa
4.All
[4]> 4


SSH1:rsa
10.1.1.1 1024 35
122606420764474441178474079962066753259278682648965870690129496065430424463013457294798980
627829828033793152226448694514316218272814453986931612508282328008815740072109975632356478
532128816187806830746328234327778100131128176672666244511191783747965898000855947022484692
079466697707373948871554575173520565607
```

系统日志推送日志订阅的示例

在下面的示例中，`logconfig` 命令用于配置名为 MailLog`SyslogPush` 的新传输日志。该日志配置为使用 UPDP 推送到 IP 地址为 10.1.1.2 的远程主机，并且 ‘mail’ facilityand 存储在目录中。

```
mail3.example.com> logconfig

Currently configured logs:
1."antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2."antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3."asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4."authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5."avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6."bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7."cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8."encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9."error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10."euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11."euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12."ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13."gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14."mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15."reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16."reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17."scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18."slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19."sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20."status" Type: "Status Logs" Retrieval: FTP Poll
21."system_logs" Type: "System Logs" Retrieval: FTP Poll
22."trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23."updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
```

```
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> new

Choose the log file type for this subscription:
1.IronPort Text Mail Logs
2. qmail Format Mail Logs
3.Delivery Logs
4.Bounce Logs
5.Status Logs
6.Domain Debug Logs
7.Injection Debug Logs
8.SMTP Conversation Logs
9.System Logs
10.CLI Audit Logs
11.FTP Server Logs
12.HTTP Logs
13.NTP logs
14.LDAP Debug Logs
15.Anti-Spam Logs
16.Anti-Spam Archive
17.Anti-Virus Logs
18.Anti-Virus Archive
19.Scanning Logs
20.IronPort Spam Quarantine Logs
21.IronPort Spam Quarantine GUI Logs
22.Reporting Logs
23.Reporting Query Logs
24.Updater Logs
25.Tracking Logs
26.Safe/Block Lists Logs
27.Authentication Logs
[1]> 1

Please enter the name for the log:
[]> MailLogSyslogPush

Log level:
1.Critical
2.Warning
3.Information
4.Debug
5.Trace
[3]> 2

Choose the method to retrieve the logs.
1.FTP Poll
2.FTP Push
3.SCP Push
4.Syslog Push
[1]> 4

Hostname to deliver the logs:
[]> 10.1.1.2

Which protocol do you want to use to transfer the log data?
1.UDP
2.TCP
[1]> 1

Which facility do you want the log data to be sent as?
1. auth
```

```
2. authpriv
3. console
4. daemon
5. ftp
6. local0
7. local1
8. local2
9. local3
10. local4
11. local5
12. local6
13. local7
14. mail
15. ntp
16. security
17. user
[14]> 14

Currently configured logs:
1."MailLogSyslogPush" Type: "IronPort Text Mail Logs" Retrieval: Syslog Push -
Host 10.1.1.2
```

rollovernow

说明

滚动更新日志文件。

Usage

提交：此命令不需要“提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> rollovernow


Currently configured logs:

1."antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2."antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3."asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4."authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5."avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6."bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7."cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8."encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9."error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10."euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11."euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12."ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13."gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14."mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
```

```
15."reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16."reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17."scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18."slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19."sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20."status" Type: "Status Logs" Retrieval: FTP Poll
21."system_logs" Type: "System Logs" Retrieval: FTP Poll
22."trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23."updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
24.All Logs
Which log would you like to roll over?
[]> 2

Log files successfully rolled over.
mail3.example.com>
```

snmpconfig

说明

配置 SNMP。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，`snmpconfig` 命令用于在端口 161 上的 “PublicNet” 接口上启用 SNMP。输入版本 3 的口令密码，再次输入以进行确认。系统会配置为服务版本 1 和版本 2 的请求，为来自版本 1 和版本 2 的 GET 请求输入 `public`。输入 `snmp-monitor.example.com` 的陷阱目标。最后，输入系统位置和联系信息。

```
mail3.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> setup

Do you want to enable SNMP?[N]> y

Please choose an IP interface for SNMP requests.
1.Data 1 (192.168.1.1/24: buttercup.run)
2.Data 2 (192.168.2.1/24: buttercup.run)
3.Management (192.168.44.44/24: buttercup.run)
[1]>

Enter the SNMPv3 passphrase.
>
Please enter the SNMPv3 passphrase again to confirm.
>
```

```
Which port shall the SNMP daemon listen on?
[161]>

Service SNMP V1/V2c requests?[N]> y

Enter the SNMP V1/V2c community string.
[]> public

From which network shall SNMP V1/V2c requests be allowed?
[192.168.2.0/24]>

Enter the Trap target (IP address).Enter "None" to disable traps.
[None]> snmp-monitor.example.com

Enterprise Trap Status
1.RAIDStatusChange             Enabled
2. fanFailure                   Enabled
3. highTemperature              Enabled
4. keyExpiration                Enabled
5. linkDown                     Enabled
6. linkUp                       Enabled
7. powerSupplyStatusChange      Enabled
8. resourceConservationMode     Enabled
9. updateFailure                Enabled
Do you want to change any of these settings?[N]> y

Do you want to disable any of these traps?[Y]>

Enter number or numbers of traps to disable.Separate multiple numbers with commas.
[]> 1,8

Enterprise Trap Status
1.RAIDStatusChange             Disabled
2. fanFailure                   Enabled
3. highTemperature              Enabled
4. keyExpiration                Enabled
5. linkDown                     Enabled
6. linkUp                       Enabled
7. powerSupplyStatusChange      Enabled
8. resourceConservationMode     Disabled
9. updateFailure                Enabled
Do you want to change any of these settings?[N]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #31, position 2

Enter the System Contact string.
[snmp@localhost]> Joe Administrator, x8888

Current SNMP settings:
Listening on interface "Data 1" 192.168.2.1/24 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.
SNMP v1/v2 Community String: public
Trap target: snmp-monitor.example.com
Location: Network Operations Center - west; rack #31, position 2
System Contact: Joe Administrator, x8888

mail3.example.com>
```

tail

说明

不断显示日志文件结尾。tail 命令还接受日志的名称或编号，作为参数 `tail 9` 或 `tail mail_logs` 进行查看。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> tail

Currently configured logs:
1."antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2."antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3."asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4."authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5."avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6."bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7."cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8."encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9."error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10."euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11."euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12."ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13."gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14."mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15."reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16."reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17."scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18."slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19."sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20."status" Type: "Status Logs" Retrieval: FTP Poll
21."system_logs" Type: "System Logs" Retrieval: FTP Poll
22."trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23."updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 19

Press Ctrl-C to stop.
Sat May 15 12:25:10 2008 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host
Sat May 15 23:18:10 2008 Info: PID 19626: User admin commit changes:
Sat May 15 23:18:10 2008 Info: PID 274: User system commit changes: Updated filter logs
config
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Receiving suspended.
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Suspended receiving.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving resumed.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving resumed.
Sat May 15 23:48:17 2008 Info: PID 25696: User admin commit changes:
```

```
Sun May 16 00:00:00 2008 Info: Generated report: name b, start time Sun May 16 00:00:00
2004, size 2154 bytes
^Cmail3.example.com>
```

报告

本部分包含以下 CLI 命令：

- reportingconfig

reportingconfig

使用 reportingconfig 命令

以下子命令在 reportingconfig 子菜单中可用：

表 3-13　　reportingconfig 子命令

语法	说明	可用性
filters	配置安全管理设备的过滤器。	仅 M 系列
alert_timeout	配置何时因未能获取报告数据而您发出提示。	仅 M 系列
domain	配置域报告设置。	仅 M 系列
mode	在安全管理设备上启用集中式报告。为邮件安全设备启用集中式或本地报告。	C 系列、 M 系列
mailsetup	配置邮件安全设备的报告。	仅 C 系列

Usage

提交：此命令需要 “提交”。

示例：启用报告过滤 （仅 M 系列）

```
mail3.example.com> reportingconfig


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> filters

Filters remove specific sets of centralized reporting data from the "last year"
reports.Data from the reporting groups selected below will not be recorded.

All filtering has been disabled.

1.No Filtering enabled
2.IP Connection Level Detail.
3.User Detail.
```

```
4.Mail Traffic Detail.
Choose which groups to filter, you can specify multiple filters by entering a comma
separated list:
[]> 2, 3


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get
reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

为域报告启用 HAT REJECT 信息 （仅 M 系列）

```
mail3.example.com> reportingconfig


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> domain

If you have configured HAT REJECT policy on all remote appliances providing reporting data
to this appliance to occur at the message recipient level then of domain reports.
Use message recipient HAT REJECT information for domain reports?[N]> y


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

启用超时提示 （仅 M 系列）

```
mail3.example.com> reportingconfig


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> alert_timeout

An alert will be sent if reporting data has not been fetched from an appliance after 360
minutes.
Would you like timeout alerts to be enabled?[Y]> y

After how many minutes should an alert be sent?
[360]> 240
```

```
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

为邮件安全设备启用集中式报告

```
mail3.example.com> reportingconfig


Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]> mode

Centralized reporting: Local reporting only.

Do you want to enable centralized reporting?[N]> y


Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]>
```

配置报告数据的存储限制 （仅 C 系列）

```
mail.example.com> reportingconfig


Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]> mailsetup

SenderBase timeout used by the web interface: 5 seconds
Sender Reputation Multiplier: 3
The current level of reporting data recording is: unlimited
No custom second level domains are defined.
Legacy mailflow report: Disabled


Choose the operation you want to perform:
- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.
- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series before
being overwritten.
- LEGACY - Configure legacy mailflow report.
[]> storage


While in centralized mode the C-series will store reporting data for the M-series to
collect.If the M-series does not collect that data then eventually the C-series will begin
to overwrite the oldest data with new data.
```

```
A maximum of 24 hours of reporting data will be stored.
How many hours of reporting data should be stored before data loss?
[24]> 48

SenderBase timeout used by the web interface: 5 seconds
Sender Reputation Multiplier: 3
The current level of reporting data recording is: unlimited
No custom second level domains are defined.
Legacy mailflow report: Disabled


Choose the operation you want to perform:
- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.
- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series
before being overwritten.
- LEGACY - Configure legacy mailflow report.
[]>
```

Senderbase

本部分包含以下 CLI 命令：

- sbstatus
- senderbaseconfig

sbstatus

说明

显示 SenderBase 查询的状态。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> sbstatus

SenderBase host status
Status as of:         Tue Oct 21 10:55:04 2003
Host up/down:         up
```

如果设备无法与 SenderBase 信誉服务联系，或者该服务从未被联系，则将显示以下内容：

```
mail3.example.com> sbstatus

SenderBase host status
Host up/down:         Unknown (never contacted)
```

senderbaseconfig

说明

配置 SenderBase 连接设置。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> senderbaseconfig

Share statistics with SenderBase Information Service: Enabled

Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
[]> setup

Do you want to share statistical data with the SenderBase Information Service
(recommended)?[Y]>

Share statistics with SenderBase Information Service: Enabled

Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
[]>
```

SMTP 服务配置

本部分包含以下 CLI 命令：

- callaheadconfig
- listenerconfig
- localeconfig
- smtpauthconfig

callaheadconfig

说明

添加、编辑和删除 SMTP Call-Ahead 配置文件。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，您可以为传输主机创建新的 SMTP Call-Ahead 配置文件。

```
> callaheadconfig

No SMTP Call-Ahead profiles are configured on the system.

Choose the operation you want to perform:
- NEW - Create a new profile.
[]> new

Select the type of profile you want to create:
1.Delivery Host
2.Static Call-Ahead Servers
[1]> 1

Please enter a name for the profile:
[]> delhost01

Advanced Settings:
  MAIL FROM Address: <>
  Interface: Auto
  Timeout Value: 30
  Validation Failure Action: ACCEPT
  Temporary Failure Action: REJECT with same code
  Maximum number of connections: 5
  Maximum number of validation queries: 1000
  Cache size: 10000
  Cache TTL: 900
Do you want to change advanced settings?[N]> n

Currently configured SMTP Call-Ahead profiles:
1. delhost01 (Delivery Host)

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]>
```

In the following example you can create a new SMTP call-ahead profile for call ahead server.

```
> callaheadconfig

Currently configured SMTP Call-Ahead profiles:
1. delhost01 (Delivery Host)

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]> new

Select the type of profile you want to create:
1.Delivery Host
2.Static Call-Ahead Servers
[1]> 2

Please enter a name for the profile:
[]> Static

Enter one or more Call-Ahead servers hostname separated by commas.
[]> 192.168.1.2

Advanced Settings:
  MAIL FROM Address: <>
  Interface: Auto
  Timeout Value: 30
  Validation Failure Action: ACCEPT
  Temporary Failure Action: REJECT with same code
  Maximum number of connections: 5
  Maximum number of validation queries: 1000
  Cache size: 10000
  Cache TTL: 900
Do you want to change advanced settings?[N]> n

Currently configured SMTP Call-Ahead profiles:
1.Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]> print

Select the profile you want to print:
1.Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)
[1]>
```

listenerconfig

说明

listenerconfig 命令允许您创建、编辑和删除监听程序。 AsyncOS 要求您指定条件，邮件必须满足该条件才能被接受并中继到收件人主机 - 可能是在您的网络内部，也可能是互联网上的外部收件人。

这些限定条件是在监听程序中定义的；他们共同定义和执行您的邮件流策略。监听程序还定义设备如何与注入邮件的系统通信。

表 3-14　　listenerconfig 子命令

Name	您提供给侦听器的唯一昵称以供将来参考。您对侦听器定义的名称区分大小写。 AsyncOS 不允许创建两个相同的监听程序名称。	
IP 接口	监听程序会分配到 IP 接口。在创建监听程序并将其分配到 IP 接口前，必须使用 `systemstartup` 命令或 `interfaceconfig` 命令配置所有 IP 接口。	
邮件协议	邮件协议用于邮件接收：ESMTP 或 QMQP	
IP 端口	用于连接到监听程序的特定 IP 端口。默认情况下 SMTP 使用端口 25， QMQP 使用端口 628。	
监听程序类型：	公共	公共和专用监听程序适用于大多数配置。按约定，专用监听程序适用于专用 （内部）网络，而公共监听程序包含用于从互联网接收邮件的默认特征。
	私有	
	Blackhole	“Blackhole”监听程序用于测试或者故障排除目的。当创建 blackhole 侦听器时，您可以选择是否在删除邮件前将其写入磁盘。（请参阅 《*思科邮件安全设备 AsyncOS 用户指南*》中的 “测试和故障排除”一章了解更多信息。）

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

批处理格式 - 通用 listenerconfig

`listenerconfig` 命令的批处理格式可以用于在特定接口上添加和删除监听程序。 listenerconfig 命令的批处理格式还允许您配置监听程序的 HAT 和 RAT。

- 添加新监听程序：

```
listenerconfig new <name> <public|private|blackhole|blackholequeueing>
<interface_name> <smtp|qmqp>
```

- 删除监听程序：

```
listenerconfig delete <name>
```

批处理格式 - HAT

以下示例说明如何使用 listenerconfig 的批处理格式执行各种 HAT 相关任务。有关参数的更多信息，请查阅表 3-15 “listenerconfig 参数值 - HAT”第 246 页。

- 向 HAT 添加新发件人组

```
listenerconfig edit <name> hostaccess new sendergroup <name>
<host_list> <behavior> [options [--comments]
```

- 向 HAT 添加新策略

```
listenerconfig edit <name> hostaccess new policy <name> <behavior>
[options]
```

- 向发件人组添加新的主机列表

```
listenerconfig edit sendergroup <name> hostaccess edit sendergroup
<name> new <host_list>
```

- 从发件人组删除主机

```
listenerconfig edit sendergroup <name> hostaccess edit sendergroup
<name> delete <host>
```

- 以发件人组列表顺序移动主机

```
listenerconfig edit sendergroup <name> hostaccess edit sendergroup
<name> move <host> <host-to-insert-before>
```

- 修改发件人组策略

```
listenerconfig edit sendergroup <name> hostaccess edit sendergroup
<name> policy <behavior> [options]
```

- 打印发件人组列表

```
listenerconfig edit <name> hostaccess edit sendergroup <name> print
```

- 重命名发件人组

```
listenerconfig edit sendergroup <name> hostaccess edit sendergroup
<name> rename <name>
```

- 编辑 HAT 策略

```
listenerconfig edit <name> hostaccess edit policy <name> <behavior>
[options]
```

- 从 HAT 删除发件人组

```
listenerconfig edit <name> hostaccess delete sendergroup <name>
```

- 删除策略

```
listenerconfig edit <name> hostaccess delete policy <name>
```

- 在 HAT 中移动发件人组的位置

```
listenerconfig edit <name> hostaccess move <group>
<group-to-insert-before>
```

- 更改 HAT 默认选项

```
listenerconfig edit <name> hostaccess default [options]
```

- 打印 hostaccess 表

```
listenerconfig edit <name> hostaccess print
```

- 导入 HAT 的本地副本

```
listenerconfig edit <name> hostaccess import <filename>
```

- 从设备导出 HAT 的副本

```
listenerconfig edit <name> hostaccess export <filename>
```

- 从 HAT 删除所有用户定义的发件人组和策略

```
listenerconfig edit <name> hostaccess clear
```

表 3-15　`listenerconfig` 参数值 - HAT

参数	说明
<behavior>	“接受” (Accept)、“中继” (Relay)、“拒绝” (Reject)、“TCP 拒绝” (TCP Refuse) 或 “继续” (Continue)。当选择一个行为用于发件人组时，表 “Policy: FOO”（“FOO”是策略的名称）的其他行为可用。

表 3-15　listenerconfig 参数值 - HAT

<filename>		导入和导出 hostaccess 表时要使用的文件名。
<group>		发件人组 <name>。
<host>		<host_list> 的单个实体。
<host_list>		输入要添加的主机。主机格式可以如下所示： CIDR 地址 (10.1.1.0/24) IP 地址范围 (10.1.1.10-20) IP 子网 (10.2.3) 主机名 (crm.example.com) 部分主机名 (.example.com) 发件人基本信誉分数范围 (7.5:10.0) 发件人基本网络所有者 IDS (SBO:12345) 远程黑名单查询 (dnslist[query.blacklist.example] **注**　用逗号分隔多个主机。
< 姓名 >		发件人组或策略的名称。 HAT 标签必须以一个字母或下划线开头，其后为任意数量的字母、数字、下划线或连字符。
[options]	--max_size	邮件最大大小为千字节添加后缀 K，为兆字节添加后缀 M，为字节则不添加任何字母。
	--max_conn	单一主机允许的最大连接数。
	--max_msgs	每次连接允许的邮件最大数。
	--max_rcpt	每个邮件的收件人的最大数。
	--override	覆盖 SMTP 标语中的主机名 “No” 或 SMTP 标语字符串。
	--cust_acc	指定自定义 SMTP 接受响应。“No” 或 SMTP 接受响应字符串。
	--acc_code	自定义 SMTP 接受响应代码。默认值为 220。
	--cust_rej	指定自定义 SMTP 拒绝响应。“No” 或 SMTP 拒绝响应字符串。
	--rej_code	自定义 SMTP 拒绝响应代码。默认值为 554。
	--rate_lim	启用每主机速率限制。“No”、“default” 或每个主机每小时的最大收件人数。
	--cust_lim	指定自定义 SMTP 超限响应。“No” 或 SMTP 拒绝响应字符串。默认值为 “No”。
	--lim_code	自定义 SMTP 超限响应代码。默认值为 452。
	--use_sb	默认情况下使用 SenderBase 进行流控制。“Yes”、“No” 或 “default”。
	--as_scan	启用反垃圾邮件扫描。“Yes”、“No”、“default”。
	--av_scan	启用防病毒扫描。“Yes”、“No”、“default”。

表 3-15　listenerconfig 参数值 - HAT

	--dhap	目录搜集攻击预防。“No”、“default”或来自远程主机的每小时最大无效收件人数。
	--tls	不支持；使用菜单系统配置 TLS。
	--sig_bits	被视为重要的 IP 地址的位数。从 0 到 32、“No”或 “default”。
	--dkim_signing	启用 DKIM 签名。“Yes”、“No”、“Default”。
	--dkim_verification	启用 DKIM 验证。“Yes”、“No”、“Default”。
	--dkim_verification_profile <name>	DKIM 验证配置文件的名称。仅在 --dkim_verification 值设置为 “Yes”时此选项才适用。
	--spf	启用 SPF 验证。“Yes”、“No”、“Default”。
	--spf_conf_level	SPF 一致性级别。仅与 “--spf Yes”一起使用。“spf_only”、“sidf_compatible”、“sidf_strict”。
	--spf_downgrade_pra	降级 SPF PRA 验证结果。仅与 “--spf Yes”和“--spf_conf_level sidf_compatible”一起使用。“是”， “No ”
	--spf_helo_test	SPF HELO 测试。仅与 “--spf Yes”和“--spf_conf_level sidf_compatible”或“--spf_conf_level spf_only”一起使用。“Yes”、“No”。
	--dmarc_verification	启用 DMARC 验证。“Yes”、“No”、“Default”。
	--dmarc_verification_profile <name>	DMARC 验证配置文件的名称。仅在 --dmarc_verification 值设置为 “Yes”时此选项才适用。
	--dmarc_agg_reports	启用 DMARC 汇聚报告。“Yes”、“No”、“Default”。仅在 --dmarc_verification 值设置为 “Yes”时此选项才适用。

批处理格式 - RAT

以下示例说明如何使用 listenerconfig 的批处理格式执行各种 RAT 相关任务。有关参数的更多信息，请查阅表 3-16 “listenerconfig 参数值 - RAT”第 249 页。

- 向 RAT 添加新收件人

```
listenerconfig edit <name> rcptacess new <rat_addr> [options]
```

- 在 RAT中编辑收件人

```
listenerconfig edit <name> rcptacess edit <rat_addr> [options]
```

- 从 RAT 中删除收件人

```
listenerconfig edit <name> rcptacess delete <rat_addr>
```

- 打印 RAT 副本

```
listenerconfig edit <name> rcptacess print
```

- 将本地 RAT 导入您的设备

```
listenerconfig edit <name> rcptacess import <filename>
```

- 导出 RAT

```
listenerconfig edit <name> rcptacess export <filename>
```

- 清除默认访问

```
listenerconfig edit <name> rcptacess clear <default_access>
```

表 3-16　listenerconfig 参数值 - RAT

参数		说明
<rat_addr>		输入要添加的主机。主机格式可以如下所示： CIDR 地址 (10.1.1.0/24) 主机名 (crm.example.com) 部分主机名 (.example.com) 用户名 (postmaster@) 完整的邮件地址 （joe@example.com、 joe@[1.2.3.4]） **注**　用逗号分隔多个主机。
<options>	-- 操作	适用于地址的操作。“接受” (Accept) 或 “拒绝” (Reject)。默认值为 “接受” (Accept)。
	--cust_resp	指定自定义 SMTP 响应。“No” 或 SMTP 接受响应字符串。
	--resp_code	自定义 SMTP 响应代码。对于 “接受” (Accept) 操作，默认值为 250，对于 “拒绝” (Reject) 操作，默认值为 550。
	--bypass_rc	旁路接收控制。默认值为 “No”。
	--bypass_la	旁路 LDAP 接受查询。选择 “Yes” 或 “No”。

示例 - 添加监听程序

在下面的示例中，`listenerconfig` 命令用于创建名为 OutboundMail 的新专用监听程序，该监听程序可用于企业网络配置中所需的 B 监听程序。（请注意：您在 GUI 的系统设置向导 (System Setup Wizard) CLI `systemsetup` 命令期间可以选择添加此专用监听程序。）

选择一个专用监听程序类型，并命名为 OutboundMail。该监听程序会被指定为在 PrivateNet IP 接口上运行，使用端口 25 上的 SMTP 协议。然后会接受此监听程序的主机访问策略的默认值。

```
mail3.example.com> listenerconfig
Currently configured listeners:
```

```
1.InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> new

Please select the type of listener you want to create.
1.Private
2.Public
3.Blackhole
[2]> 1

Please create a name for this listener (Ex: "OutboundMail"):
[]> OutboundMail

Please choose an IP interface for this Listener.
1.Management (192.168.42.42/24: mail3.example.com)
2.PrivateNet (192.168.1.1/24: mail3.example.com)
3.PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 2

Choose a protocol.
1.SMTP
2.QMQP
[1]> 1

Please enter the TCP port for this listener.
[25]> 25


Please specify the systems allowed to relay email through the IronPort C60.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[]> .example.com
Do you want to enable rate limiting for this listener?(Rate limiting defines the maximum
number of recipients per hour you are willing to receive from a remote domain.)[N]> n

Default Policy Parameters
==========================
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 600
Maximum Number Of Messages Per Connection: 10,000
Maximum Number Of Recipients Per Message: 100,000
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control:  No
Spam Detection Enabled:  No
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Would you like to change the default host access policy?[N]> n

Listener OutboundMail created.
Defaults have been set for a Private listener.
Use the listenerconfig->EDIT command to customize the listener.

Currently configured listeners:
1.InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2.OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
```

```
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
```

示例 - 通过导入和导出为监听程序自定义主机访问表 (HAT)

`listenerconfig` 命令内的许多子命令允许您导入和导出数据，从而无需在 CLI 中输入数据块即可进行大的配置更改。

这些步骤使用 CLI 通过导出、修改和导入文件来修改监听程序的主机访问表 (HAT)。您还可以使用 HAT CLI 编辑器或 GUI 来为监听程序自定义 HAT。有关详细信息，请参阅 《*思科邮件安全设备 AsyncOS 用户指南*》中的 “配置网关以接收邮件”以及 “使用邮件流监控”章节。

为已经通过导出和导入定义的监听程序定义 HAT：

步骤 1　使用 `listenerconfig` 的 `hostaccess -> export` 子命令可以将默认 HAT 导出到文件。

在下面的示例中，会打印公共监听程序 InboundMail 的 HAT，然后导出到名为 `inbound.HAT.txt` 的文件。

```
mail3.example.com> listenerconfig


Currently configured listeners:
1.InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2.OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit

Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
```

```
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess

Default Policy Parameters
=================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces:  No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> print

$BLOCKED
    REJECT {}
$TRUSTED
    ACCEPT {
        tls = "off"
        dhap_limit = 0
        max_rcpts_per_hour = -1
        virus_check = "on"
        max_msgs_per_session = 5000
        spam_check = "off"
        use_sb = "off"
        max_message_size = 104857600
        max_rcpts_per_msg = 5000
        max_concurrency = 600
    }
$ACCEPTED
    ACCEPT {}
$THROTTLED
    ACCEPT {
        tls = "off"
        dhap_limit = 0
        max_rcpts_per_hour = 1
```

```
        virus_check = "on"
        max_msgs_per_session = 10
        spam_check = "on"
        use_sb = "on"
        max_message_size = 1048576
        max_rcpts_per_msg = 25
        max_concurrency = 10
    }
WHITELIST:
        $TRUSTED (My trusted senders have no anti-spam or rate limiting)

BLACKLIST:
        $BLOCKED (Spammers are rejected)

SUSPECTLIST:
        $THROTTLED (Suspicious senders are throttled)

UNKNOWNLIST:
        $ACCEPTED (Reviewed but undecided, continue normal acceptance)

ALL
    $ACCEPTED (Everyone else)

Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.

[]> export

Enter a name for the exported file:
[]> inbound.HAT.txt

File written on machine "mail3.example.com".
```

步骤 2　在命令行界面 (CLI) 之外，获取文件 `inbound.HAT.txt`。

步骤 3　利用文本编辑器，在该文件中创建新的 HAT 条目。

在本示例中，以下条目会添加到 ALL 条目上的 HAT：

```
spamdomain.com    REJECT
.spamdomain.com   REJECT
251.192.1.TCPREFUSE
169.254.10.10     RELAY
```

- 前两个条目会拒绝与域 spamdomain.com 和 spamdomain.com 的任意子域中远程主机的所有连接。
- 第三行会拒绝与 IP 地址为 251.192.1.*x* 的任意主机的连接。
- 第四行允许 IP 地址为 169.254.10.10 的远程主机将邮件安全设备用作 SMTP 中继，以便将其所有出站邮件中继到互联网。

注　规则在 HAT 中的显示顺序非常重要。对于尝试连接到侦听器的各主机，系统会从上到下读取 HAT。如果规则匹配连接主机，则会对该连接立即采取操作。您应将所有自定义条目放置到所有主机定义上的 HAT 中。您还可以使用 HAT CLI 编辑器或 GUI 来为监听程序自定义 HAT。有关详细信息，请参阅《*思科邮件安全设备 AsyncOS 用户指南*》中的“配置网关以接收邮件”以及“使用邮件流监控”章节。

步骤 4　保存文件并将其放置到接口的配置目录中，以便可以导入该文件。（有关详细信息，请参阅附录 B “访问设备”。）

步骤 5　使用 listenerconfig 的 hostaccess -> import 子命令可以导入编辑过的主机访问表文件。

在下面的示例中，会为 InboundMail 监听程序将名为 inbound.HAT.txt 的已编辑文件 导入到 HAT。使用 print 子命令打印新的条目。

```
mail3.example.com> listenerconfig


Currently configured listeners:
1.InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2.OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit

Enter the name or number of the listener you wish to edit.
[]> 1

Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off
```

```
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess

Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> import

Enter the name of the file to import:
[]> inbound.HAT.txt

9 entries imported successfully.

Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes

There are currently 4 policies defined.
There are currently 5 sender groups.
```

```
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> print

$ACCEPTED
    ACCEPT
$THROTTLED
    ACCEPT {
        spam_check = "on"
        max_msgs_per_session = 10
        max_concurrency = 10
        max_rcpts_per_msg = 25
        max_rcpts_per_hour = 1
        dhap_limit = 0
        virus_check = "on"
        max_message_size = 1048576
        use_sb = "on"
        tls = "off"
    }
$TRUSTED
    ACCEPT {
        spam_check = "off"
        max_msgs_per_session = 5000
        max_concurrency = 600
        max_rcpts_per_msg = 5000
        max_rcpts_per_hour = -1
        dhap_limit = 0
        virus_check = "on"
        max_message_size = 104857600
        use_sb = "off"
        tls = "off"
    }
$BLOCKED
    REJECT

WHITELIST:
        $TRUSTED (My trusted senders have no anti-spam scanning or rate limiting)

BLACKLIST:
        $BLOCKED (Spammers are rejected)

SUSPECTLIST:
        $THROTTLED (Suspicious senders are throttled)

UNKNOWNLIST:
        $ACCEPTED (Reviewed but undecided, continue normal acceptance)

spamdomain.com
    REJECT (reject the domain "spamdomain.com")

.spamdomain.com
    REJECT (reject all subdomains of ".spamdomain.com")

251.192.1.
    TCPREFUSE (TCPREFUSE the IP addresses in "251.192.1")
```

```
169.254.10.10
    RELAY (RELAY the address 169.254.10.10)

ALL
    $ACCEPTED (Everyone else)



Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]>
```

请记得在导入后发出 `commit` 命令，以使配置更改生效。

示例 - 启用公钥搜集和 S/MIME 解密和验证

下面的示例显示如何：

- 从传入的 S/MIME 签名邮件取回 （搜集）公钥
- 启用 S/MIME 解密和验证

```
mail.example.com> listenerconfig

Currently configured listeners:
1.MyListener (on Management, 172.29.181.70) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit

Enter the name or number of the listener you wish to edit.
[]> 1

Name: MyListener
```

```
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 50 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess

Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: No
S/MIME Decryption/Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces:  No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
```

```
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]> default

Enter the default maximum message size.Add a trailing k for kilobytes, M for megabytes, or
no letter for b
[10M]>

Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner?[N]>

Would you like to specify a custom SMTP acceptance response?[N]>

Would you like to specify a custom SMTP rejection response?[N]>

Do you want to enable rate limiting per host?[N]>

Do you want to enable rate limiting per envelope sender?[N]>

Do you want to enable Directory Harvest Attack Prevention per host?[Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1.Drop
2.Code
[1]>

Would you like to specify a custom SMTP DHAP response?[Y]>

Enter the SMTP code to use in the response.550 is the standard code.
[550]>

Enter your custom SMTP response.Press Enter on a blank line to finish.
custom_response

Would you like to use SenderBase for flow control by default?[Y]>

Would you like to enable anti-spam scanning?[Y]>

Would you like to enable anti-virus scanning?[Y]>

Do you want to allow encrypted TLS connections?
1.No
2.Preferred
3.Required
4.Preferred - Verify
5.Required - Verify
[1]>

Would you like to enable DKIM/DomainKeys signing?[N]>

Would you like to enable DKIM verification?[N]>
```

```
Would you like to enable S/MIME Public Key Harvesting?[N]> y

Would you like to harvest certificate on verification failure?[N]>

Would you like to harvest updated certificate?[Y]>

Would you like to enable S/MIME gateway decryption/verification?[N]> y

Select the appropriate operation for the S/MIME signature processing:
1.保持
2.删除
[1]>

Would you like to change SPF/SIDF settings?[N]>

Would you like to enable DMARC verification?[N]>

Would you like to enable envelope sender verification?[N]>

Would you like to enable use of the domain exception table?[N]>

Do you wish to accept untagged bounces?[N]>

Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: Yes
S/MIME Decryption/Verification Enabled: Yes
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces:  No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]>
```

示例 - 高级 HAT 参数

表 3-17 定义了高级 HAT 参数的语法。请注意，对于下面的数字值，您可以在数字后面添加一个 **k** 以指示千字节，或者可以在数字后面添加一个 **M** 以指示兆字节。无字母的值会被视作字节。带有星号的参数支持表 3-17 中显示的变量语法。

表 3-17　　高级 HAT 变量语法

参数	语法	值	示例值
每个连接的最大邮件数	max_msgs_per_session	编号	1000
每封邮件的最大收件人数	max_rcpts_per_msg	编号	10000 1k
最大邮件大小	max_message_size	编号	1048576 2000 万
对此侦听器允许的最大并发连接数	max_concurrency	编号	1000
SMTP 横幅代码	smtp_banner_code	编号	220
SMTP 横幅文本 (*)	smtp_banner_text	字符串	Accepted
SMTP 拒绝横幅代码	smtp_banner_code	编号	550
SMTP 拒绝横幅文本 (*)	smtp_banner_text	字符串	Rejected
覆盖 SMTP 横幅主机名	use_override_hostname	on | off | default	default
	override_hostname	字符串	newhostname
使用 TLS	tls	on | off | required	on
使用反垃圾邮件扫描	spam_check	on | off	off
使用 Sophos 病毒扫描	virus_check	on | off	off
每小时最大收件人数	max_rcpts_per_hour	编号	5k
每小时最大收件人数错误代码	max_rcpts_per_hour_code	编号	452
每小时最大收件人数文本 (*)	max_rcpts_per_hour_text	字符串	Too many recipients
使用 SenderBase	use_sb	on | off	on
定义 SenderBase 信誉分数	sbrs[*value1*:*value2*]	-10.0- 10.0	sbrs[-10:-7.5]
目录搜集攻击预防：每小时最大无效收件人数	dhap_limit	编号	150

示例 - 配置 SPF 和 SIDF

为侦听器的主机访问表配置默认设置时，您可以根据 SPF/SIDF 验证结果选择侦听器的 SPF/SIDF 一致性级别和设备执行的 SMTP 操作 （ACCEPT 或 REJECT）。您还可以定义设备拒绝邮件时发送的 SMTP 响应。

根据一致性级别，设备会对 HELO 身份、MAIL FROM 身份或 PRA 身份执行检查。对于各身份检查的以下 SPF/SIDF 验证结果，您可以指定设备继续会话 (ACCEPT) 或终止会话 (REJECT)：

- **无**。由于缺少信息无法执行任何验证。

- **不确定 (Neutral)**。域所有者无法判断客户端是否被授权使用给定身份。
- **SoftFail**。域所有者认为主机未被授权使用给定身份，但不愿作最终声明。
- **Fail**。客户端未被授权使用给定身份发送邮件。
- **TempError**。验证过程中发生暂时性错误。
- **PermError**。验证过程中发生永久错误。

如果邮件中存在 Resent-Sender: 或 Resent-From: 报头，除非您配置 SIDF 兼容一致性级别以将 PRA 身份的 “通过”结果降级为 “无”，否则设备会对 “通过”结果接受邮件。之后，设备会执行 PRA 检查返回 “无”时所指定的 SMTP 操作。

如果您选择不对身份检查定义 SMTP 操作，则设备会自动接受所有验证结果，包括 “失败”。

如果身份验证结果与任何已启用的身份检查的 REJECT 操作相匹配，则设备会终止会话。例如，管理员根据所有 HELO 身份检查结果 （包括 “失败”）将侦听器配置为接受邮件，但同时将侦听器配置为拒绝来自 MAIL FROM 身份检查的 “失败”结果的邮件。如果邮件未通过 HELO 身份检查，由于设备接受该结果，因此会话将继续。如果接下来邮件未通过 MAIL FROM 身份检查，则侦听器会终止会话并对 REJECT 操作返回 STMP 响应。

SMTP 响应是设备根据 SPF/SIDF 验证结果拒绝邮件时返回的代码数字和消息。与其他验证结果不同，“临时错误”结果会返回不同的 SMTP 响应。对于 TempError，默认响应代码为 451，默认消息文本为 `#4.4.3 Temporary error occurred during SPF verification`。对于所有其他验证结果，默认响应代码为 550，默认消息文本为 `#5.7.1 SPF unauthorized mail is prohibited`。您可以对 “临时错误”和其他验证结果指定您自己的响应代码和消息文本。

或者，如果对 “不确定”、“软失败”或 “失败”验证结果执行 REJECT 操作，则您可以将设备配置为返回来自 SPF 发布者域的第三方响应。默认情况下，设备会返回以下响应：

```
550-#5.7.1 SPF unauthorized mail is prohibited.
 550-The domain example.com explains:
 550 <Response text from SPF domain publisher>
```

要启用这些 SPF/SIDF 设置，请使用 `listenerconfig -> edit` 子命令并选择侦听器。然后使用 `hostaccess -> default` 子命令编辑主机访问表的默认设置。对以下提示回答 yes 以配置 SPF 控制：

```
Would you like to change SPF/SIDF settings?[N]> yes

Would you like to perform SPF/SIDF Verification?[Y]> yes
```

以下 SPF 控制设置可用于主机访问表：

表 3-18　SPF 控制设置

一致性级别	可用的 SPF 控制设置
仅限 SPF	• 是否执行 HELO 身份检查 • 根据以下身份检查结果执行 SMTP 操作： • HELO 身份 （如果启用） • MAIL FROM 身份 • 对 REJECT 操作返回的 SMTP 响应代码和文本 • 验证超时 （秒）
SIDF 兼容	• 是否执行 HELO 身份检查 • 如果邮件中存在 Resent-Sender: 或 Resent-From: 报头，是否将 PRA 身份的 “通过”结果降级为 “无” • 根据以下身份检查结果执行 SMTP 操作： • HELO 身份 （如果启用） • MAIL FROM 身份 • PRA 身份 • 对 REJECT 操作返回的 SMTP 响应代码和文本 • 验证超时 （秒）
SIDF 严格	• 根据以下身份检查结果执行 SMTP 操作： • MAIL FROM 身份 • PRA 身份 • SPF REJECT 操作的情况下返回的 SMTP 响应代码 • 验证超时 （秒）

以下示例显示了用户使用 “仅限 SPF”一致性级别配置 SPF/SIDF 验证。设备执行 HELO 身份检查并接受 “无”和 “不确定”验证结果并拒绝其他验证结果。 SMTP 操作的 CLI 提示与所有身份类型的 CLI 提示相同。用户不对 MAIL FROM 身份定义 SMTO 操作。设备自动接受所有该身份的验证结果。设备对所有 REJECT 结果使用默认拒绝代码和文本。

示例：SPF/SIDF 设置

```
Would you like to change SPF/SIDF settings?[N]> yes

Would you like to perform SPF/SIDF Verification?[N]> yes

What Conformance Level would you like to use?
1.SPF only
2.SIDF compatible
3.SIDF strict
[2]> 1

Would you like to have the HELO check performed?[Y]> y

Would you like to change SMTP actions taken as result of the SPF verification?[N]> y
```

```
Would you like to change SMTP actions taken for the HELO identity?[N]> y

What SMTP action should be taken if HELO check returns None?
1.Accept
2.Reject
[1]> 1

What SMTP action should be taken if HELO check returns Neutral?
1.Accept
2.Reject
[1]> 1

What SMTP action should be taken if HELO check returns SoftFail?
1.Accept
2.Reject
[1]> 2

What SMTP action should be taken if HELO check returns Fail?
1.Accept
2.Reject
[1]> 2

What SMTP action should be taken if HELO check returns TempError?
1.Accept
2.Reject
[1]> 2

What SMTP action should be taken if HELO check returns PermError?
1.Accept
2.Reject
[1]> 2

Would you like to change SMTP actions taken for the MAIL FROM identity?[N]> n

Would you like to change SMTP response settings for the REJECT action?[N]> n

Verification timeout (seconds)
[40]>
```

以下显示了 SPF/SIDF 设置针对侦听器的默认策略参数的显示方式。

示例：默认策略参数中的 SPF/SIDF

```
SPF/SIDF Verification Enabled: Yes
  Conformance Level: SPF only
  Do HELO test: Yes
  SMTP actions:
    For HELO Identity:
      None, Neutral: Accept
      SoftFail, Fail, TempError, PermError: Reject
    For MAIL FROM Identity: Accept
  SMTP Response Settings:
    Reject code: 550
    Reject text: #5.7.1 SPF unauthorized mail is prohibited.
    Get reject response text from publisher: Yes
    Defer code: 451
    Defer text: #4.4.3 Temporary error occurred during SPF verification.
  Verification timeout: 40
```

示例 - 启用 DMARC 验证

以下示例显示如何启用 DMARC 验证。

```
mail.example.com> listenerconfig


Currently configured listeners:
1.Listener 1 (on Management, 172.29.181.70) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit

Enter the name or number of the listener you wish to edit.
[]> 1

Name: Listener 1
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off


Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess

Default Policy Parameters
==========================
Maximum Message Size: 20M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
```

```
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces:  No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]> default

Enter the default maximum message size.Add a trailing k for kilobytes, M for megabytes, or
no letter for bytes.
[20M]>

Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner?[N]>

Would you like to specify a custom SMTP acceptance response?[N]>

Would you like to specify a custom SMTP rejection response?[N]>

Do you want to enable rate limiting per host?[N]>

Do you want to enable rate limiting per envelope sender?[N]>

Do you want to enable Directory Harvest Attack Prevention per host?[Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1.Drop
2.Code
[1]>

Would you like to specify a custom SMTP DHAP response?[Y]>

Enter the SMTP code to use in the response.550 is the standard code.
[550]>
```

```
Enter your custom SMTP response.Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default?[Y]>

Would you like to enable anti-spam scanning?[Y]>

Would you like to enable anti-virus scanning?[Y]>

Do you want to allow encrypted TLS connections?
1.No
2.Preferred
3.Required
4.Preferred - Verify
5.Required - Verify
[1]>

Would you like to enable DKIM/DomainKeys signing?[N]>

Would you like to enable DKIM verification?[N]>

Would you like to change SPF/SIDF settings?[N]>

Would you like to enable DMARC verification?[N]> Y

Select the DMARC verification profile to use:
1.DEFAULT

[1]> 1

Would you like to send aggregate reports?[N]> Y

Note: DMARC reports should be DMARC compliant.
      Secure delivery is recommended for delivery of DMARC reports.
      Please enable TLS support using the `destconfig` command.
Would you like to enable envelope sender verification?[N]> Y

Would you like to specify a custom SMTP response for malformed envelope senders?[Y]>

Enter the SMTP code to use in the response.553 is the standard code.
[553]>

Enter your custom SMTP response.Press Enter on a blank line to finish.

Would you like to specify a custom SMTP response for envelope sender domains which do not
resolve?[Y]>

Enter the SMTP code to use in the response.451 is the standard code.
[451]>

Enter your custom SMTP response.Press Enter on a blank line to finish.

Would you like to specify a custom SMTP response for envelope sender domains which do not
exist?[Y]>

Enter the SMTP code to use in the response.553 is the standard code.
[553]>

Enter your custom SMTP response.Press Enter on a blank line to finish.

Would you like to enable use of the domain exception table?[N]>

Do you wish to accept untagged bounces?[N]>

Default Policy Parameters
```

```
=========================
Maximum Message Size: 20M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: Yes
  DMARC Verification Profile: DEFAULT
  Aggregate reports: Yes
Envelope Sender DNS Verification Enabled: Yes
Domain Exception Table Enabled: No
Accept untagged bounces:  No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]>

Name: Listener 1
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off


Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
```

```
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>


Currently configured listeners:
1.Listener 1 (on Management, 172.29.181.70) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>

mail.example.com>
```

localeconfig

说明

配置多语言设置。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched encodings bodies and footers: Use encoding of message footer

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup
If a header is modified, encode the new header in the same encoding as the message
body?(Some MUAs incorrectly handle headers encoded in a different encoding than the
body.However, encoding a modified header in the same encoding as the message body may
cause certain characters in the modified header to be lost.)[Y]>

If a non-ASCII header is not properly tagged with a character set, impose the encoding of
the body on the header during processing and final representation of the message?(Many
MUAs create non-RFC-compliant headers that are then handled in an undefined way.Imposing
the encoding of the body on the header may encode the header more precisely.)[Y]>

When there is an encoding mismatch between the message body and a footer, the system
initially attempts to encode the entire message in the same encoding as the message
body.If the system cannot combine the message body and the footer in the same encoding, do
```

```
you want the system to failover and attempt to encode the entire message using the
encoding of the message footer?(When this feature is enabled, the system will attempt to
display the footer "in-line" rather than defaulting to adding it as an attachment.)[N]> y

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched encodings bodies and footers: Use encoding of message body

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.

[]>mail3.example.com>
```

smtpauthconfig

说明

配置 SMTP 身份验证传出和转发配置文件。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

在下面的示例中，`smtpauthconfig` 命令用于为服务器 “smtp2.example.com:” 创建一个新的基于转发的配置文件。

```
mail3.example.com> smtpauthconfig

Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
[]> new

Choose the type of profile you wish to create:
- FORWARD - Create an SMTP Auth forwarding server group profile
- OUTGOING - Create an outgoing SMTP Auth profile

[]> forward

Enter a name for this profile:
[]> forwarding-based

Please begin entering forwarding servers for this group profile.
Enter a hostname or an IP address for the forwarding server:
[]> smtp2.example.com

Enter a port:
[25]>

Choose the interface to use for forwarding requests:
1.Auto
2.Data 1 (192.168.1.1/24: mail3.example.com)
```

```
3.Data 2 (192.168.2.1/24: mail3.example.com)
4.Management (192.168.42.42/24: mail3.example.com)
[1]>
Require TLS?(issue STARTTLS) [Y]> y

Enter the maximum number of simultaneous connections allowed:
[10]>

Use SASL PLAIN mechanism when contacting forwarding server?[Y]>

Use SASL LOGIN mechanism when contacting forwarding server?[Y]>

Would you like to enter another forwarding server to this group?[N]>

Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
- EDIT - Edit an existing SMTP Auth profile
- PRINT - List all profiles
- DELETE - Delete a profile
- CLEAR - Delete all profiles
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> created SMTP auth profile

Do you want to save the current configuration for rollback?[Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

注　经身份验证的用户获得 RELAY HAT 策略。

注　您可以在配置文件中指定多个转发服务器。在邮件安全设备和转发服务器之间不支持 SASL 机制 CRAM-MD5 和DIGEST-MD5。

系统设置

systemsetup

说明

第一次系统设置以及重新安装系统。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> systemsetup


WARNING: The system setup wizard will completely delete any existing
'listeners' and all associated settings including the 'Host Access Table' -
mail operations may be interrupted.

Are you sure you wish to continue?[Y]> y


Before you begin, please reset the administrator password to a new value.
Old password:
New password:
Retype new password:

*****
You will now configure the network settings for the IronPort C100.
Please create a fully qualified hostname for the IronPort C100 appliance
(Ex: "ironport-C100.example.com"):
[]> ironport-C100.example.com


*****

You will now assign an IP address for the "Data 1" interface.
Please create a nickname for the "Data 1" interface (Ex: "Data 1"):
[]> Data 1

Enter the static IP address for "Data 1" on the "Data 1" interface?(Ex:
"192.168.1.1"):
[]> 192.168.1.1

What is the netmask for this IP address?(Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>

You have successfully configured IP Interface "Data 1".

*****

Would you like to assign a second IP address for the "Data 1" interface?[Y]> n

What is the IP address of the default router (gateway) on your network?:
[192.168.1.1]> 192.168.2.1


*****

Do you want to enable the web interface on the Data 1 interface?[Y]> y

Do you want to use secure HTTPS?[Y]> y

Note: The system will use a demo certificate for HTTPS.
Use the "certconfig" command to upload your own certificate.

*****

Do you want the IronPort C100 to use the Internet's root DNS servers or would
you like it to use your own DNS servers?
1.Use Internet root DNS servers
2.Use my own DNS servers
[1]> 2
```

```
Please enter the IP address of your DNS server.
[]> 192.168.0.3

Do you want to enter another DNS server?[N]>

You have successfully configured the DNS settings.

*****

You are now going to configure how the IronPort C100 accepts mail by creating a
"Listener".
Please create a name for this listener (Ex: "MailInterface"):
[]> InboundMail

Please choose an IP interface for this Listener.
1.Data 1 (192.168.1.1/24: ironport-C100.example.com)
[1]> 1

Enter the domain names or specific email addresses you want to accept mail for.

Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
Separate multiple addresses with commas.
[]> example.com, .example.com

Would you like to configure SMTP routes for example.com, .example.com?[Y]> n

Please specify the systems allowed to relay email through the IronPort C100.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[]> example.com, .example.com

Do you want to enable filtering based on SenderBase Reputation Service (SBRS)
Scores for this listener?(Your selection will be used to filter all incoming
mail based on its SBRS Score.)[Y]> y

Do you want to enable rate limiting for this listener?(Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a
remote domain.)[Y]> y

Enter the maximum number of recipients per hour to accept from a remote domain.
[]> 1000

Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: 1,000
Maximum Recipients Per Hour SMTP Response:
    452 Too many recipients received this hour
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
```

```
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces:  No
Would you like to change the default host access policy?[N]> n

Listener InboundMail created.
Defaults have been set for a Public listener.
Use the listenerconfig->EDIT command to customize the listener.

*****

Do you want to use Anti-Spam scanning in the default Incoming Mail policy?[Y]> y

Would you like to enable IronPort Spam Quarantine?[Y]> y

IronPort Anti-Spam configured globally for the IronPort C100 appliance.Use the
policyconfig command (CLI) or Mail Policies (GUI) to customize the IronPort
settings for each listener.

IronPort selected for DEFAULT policy

*****

Do you want to use Anti-Virus scanning in the default Incoming and Outgoing
Mail policies?[Y]> y

1.McAfee Anti-Virus
2.Sophos Anti-Virus
Enter the number of the Anti-Virus engine you would like to use on the default
Incoming and Outgoing Mail policies.
[]> 2

Sophos selected for DEFAULT policy

*****

Do you want to enable Outbreak Filters?[Y]> y

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below), meaning that new messages of certain types could be quarantined or will no
longer be quarantined, respectively.

Allow the sharing of limited data with SenderBase?[Y]> y

You have successfully configured Outbreak Filters and SenderBase.

*****

You will now configure system alerts.
Please enter the email address(es) to send alerts.
(Ex: "administrator@example.com")
Separate multiple addresses with commas.
[]> administrator@example.com

Would you like to enable IronPort AutoSupport, which automatically emails
system alerts and weekly status reports directly to IronPort Customer Support?
You will receive a complete copy of each message sent to IronPort.
(Recommended) [Y]> y
```

```
*****

You will now configure scheduled reporting.
Please enter the email address(es) to deliver scheduled reports to.
(Leave blank to only archive reports on-box.)
Separate multiple addresses with commas.
[]> administrator@example.com


*****

You will now configure system time settings.
Please choose your continent:
1.Africa
2.America
...
11.GMT Offset
[11]> 2


Please choose your country:
1.Anguilla
...
47.United States
48.Uruguay
49.Venezuela
50.Virgin Islands (British)
51.Virgin Islands (U.S.)
[]> 47

Please choose your timezone:
1.Alaska Time (Anchorage)
...
26.Pacific Time (Los_Angeles)
[]> 26

Do you wish to use NTP to set system time?[Y]> y

Please enter the fully qualified hostname or IP address of your NTP server, or
press Enter to use time.ironport.com:
[time.ironport.com]>


*****

Would you like to commit these changes at this time?[Y]> y


Congratulations!System setup is complete.

For advanced configuration, please refer to the User Guide.
```

URL 过滤

本部分包含以下 CLI 命令：

aggregatorconfig

说明

在邮件安全设备上为思科汇聚器服务器配置地址。此服务器向最终用户提供有关是谁点击了经过重写的 URL 以及与每个用户点击相关联操作 （允许、阻止或未知）的详细信息。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> aggregatorconfig


Choose the operation you want to perform:
- EDIT - Edit aggregator configuration
[]> edit

Edit aggregator address:
[aggregator.organization.com]> org-aggregator.com

Successfully changed aggregator address to : org-aggregator.com
```

urllistconfig

说明

配置或导入不会被 URL 过滤功能评估的 URL 白名单。这些白名单不会被病毒爆发过滤器功能所使用。

Usage

提交：此命令需要“提交”。

集群管理：此命令可用于所有三种计算机模式（集群、分组、计算机）。

批处理命令：此命令支持批处理格式。

示例

```
> urllistconfig
No URL lists configured.
Choose the operation you want to perform:
NEW - Create a new URL list-
[]> new
Do you want to import a URL list?
[N]>
Enter a name for the URL list
[]> sample
Enter the URL domains that need to be skipped from scanning for URL Filtering.
Enter one URL domain per line and '.' to finish.
cisco.com
ironport.com/*
*.example.com
10.2.4.5/24
[2001:DB8::1]
URL list sample added.
There are currently 4 URL lists configured.
Choose the operation you want to perform:
- NEW - Create a new URL whitelist.
- EDIT - Modify an existing URL whitelist.
- DELETE - Delete an existing URL whitelist.
[]>EDIT
Choose the operation to edit the URL whitelist:

-   IMPORT – Import a file into an existing URL whitelist
-   EXPORT – Export an existing URL whitelist into a file
-   RENAME – Rename an existing URL whitelist
[]>IMPORT

Assign new name to the imported list?(By default, name stored in the
file will be applied to the list)
[N] > Y

Enter name of the list > new_list

Enter filename to import from > URLfile
NOTE: These files will be stored in /pub/configuration

URL list  “new_list” added.
```

webcacheflush

说明

刷新 URL 过滤功能使用的缓存。如果您更改主了用于与思科网络安全服务进行通信的证书，请使用此命令。通常，您应仅在思科支持人员的指导下使用此命令。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
> webcacheflush
Web Security cache has been flushed.
```

websecurityadvancedconfig

说明

配置 URL 过滤的高级设置。

注　除非出于故障排除目的更改超时值，否则应仅在思科支持人员的指导下使用此命令。

超时值是一个以秒为单位的值，用于与云服务 （提供 URL 信誉和类别）进行通信。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令支持批处理格式。

批处理格式

有关批处理格式，请参阅 CLI 联机帮助。

示例

```
> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[15]>

Enter the URL cache size (no. of URLs):
[1215000]>

Do you want to disable DNS lookups?[N]>

Enter the maximum number of URLs that should be scanned:
[100]>

Enter the Web security service hostname:
[example.com]>
```

```
Enter the threshold value for outstanding requests:
[20]>

Do you want to verify server certificate?[Y]>

Enter the default time-to-live value (seconds):
[30]>

Do you want to include additional headers?[N]>

Enter the default debug log level for RPC server:
[Info]>

Enter the default debug log level for SDS cache:
[Info]>

Enter the default debug log level for HTTP client:
[Info]>
```

websecurityconfig

说明

配置 URL 过滤的基本设置 （URL 信誉和 URL 类别功能）。

通常，证书管理是自动的。除非经由思科 TAC 指导，否则您应在提示符处选择 No 来设置证书。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令支持批处理格式。请查阅联机 CLI 帮助了解更多详细信息。使用 help 命令可以访问此命令的联机帮助。

示例

```
mail.example.com> websecurityconfig

Enable URL Filtering?[N]> y

Do you wish to enable Web Interaction Tracking?[N]> y

Web Interaction Tracking is enabled.

Do you want to whitelist URLs using a URL list?[N]> y

1. urllist1
2. urllist2
3.No URL list
Enter the number of URL list
[1]> 1

URL list 'urllist1' added

mail.example.com> websecurityconfig
```

```
URL Filtering is enabled.
URL list 'urllist1' used.
System provided certificate used.
Web Interaction Tracking is enabled.
```

websecuritydiagnostics

说明

查看与 URL 过滤相关诊断统计信息。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> websecuritydiagnostics

Cache Size: 254

Cache Hits: 551

响应时间
     Minimum: None
     Average: 0.0
     Maximum: None

DNS Lookup Time
     Minimum: 9.4198775
     Average: 10.1786801765
     最大: 10.544356
```

用户管理

本部分包含以下 CLI 命令：

- userconfig
- password or passwd
- last
- who
- whoami

userconfig

说明

管理用户帐户以及至外部身份验证源的连接。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在集群模式下使用。

批处理命令：此命令支持批处理格式。请查阅联机 CLI 帮助了解更多详细信息。使用 `help` 命令可以访问此命令的联机帮助，例如，

```
mail.example.com> userconfig help
```

示例 - 创建新的用户帐户

以下示例显示如何使用服务中心用户角色创建新的用户帐户。

```
mail.example.com> userconfig

Users:
1. admin - "Administrator" (admin)

External authentication: Disabled

Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change password and account policy settings.
- PASSWORD - Change the password for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
[]> new

Enter the new username.
[]> helpdesk

Enter the full name for helpdesk.
[]> HELP DESK

Assign a role to "helpdesk":
1.Administrators - Administrators have full access to all settings of the system.
2.Operators - Operators are restricted from creating new user accounts.
3.Read-Only Operators - Read-Only operators may only view settings and status information.
4.Guests - Guest users may only view status information.
5.Technicians - Technician can only manage upgrades and feature keys.
6.Help Desk Users - Help Desk users have access only to ISQ and Message Tracking.
[1]> 6

Would you like to get a system generated password?[N]>

Enter the password for helpdesk
[]>
```

```
Please enter the new password again:

Users:
1. admin - "Administrator" (admin)
2. helpdesk - "HELP DESK" (helpdesk)

External authentication: Disabled

Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change password and account policy settings.
- PASSWORD - Change the password for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
[]>
```

示例 - 设置外部身份验证的 RADIUS 服务器

以下示例显示如何为外部身份验证设置 RADIUS 服务器。要设置 RADIUS 服务器，请输入主机名、端口、共享的密码以及是将 CHAP 还是 PAP 用于身份验证协议。

```
mail.example.com> userconfig

Users:
1. admin - "Administrator" (admin)
2. hdesk_user - "Helpdesk User" (helpdesk)

External authentication: Disabled

Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change password and account policy settings.
- PASSWORD - Change the password for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
[]> external

Choose the operation you want to perform:
- SETUP - Set up global settings.
[]> setup

Do you want to enable external authentication?[N]> Y

Please enter the timeout in seconds for how long the external authentication credentials
will be cached.(Enter '0' to disable expiration of
authentication credentials altogether when using one time passwords.)
[0]> 30

Choose a mechanism to use:
LDAP is unavailable because no LDAP queries of type EXTERNALAUTH are configured
1.RADIUS
[1]> 1

Configured RADIUS servers:
- No RADIUS servers configured
```

```
Choose the operation you want to perform:
- NEW - Add a RADIUS server configuration.
[]> new

Please enter host name or IP address of the RADIUS server:
[]> radius.example.com

Please enter port number of the RADIUS server:
[1812]>

Please enter the shared password:
>
Please enter the new password again.
>

Please enter timeout in seconds for receiving a valid reply from the server:
[5]>

1.CHAP
2.PAP
Select authentication type:
[2]>

Configured RADIUS servers:
Host                      Port  Timeout (s) Auth type
------------------------- ----- ---------- ----------
radius.example.com        1812  5          pap

Choose the operation you want to perform:
- NEW - Add a RADIUS server configuration.
- EDIT - Modify a RADIUS server configuration.
- DELETE - Remove a RADIUS server configuration.
- CLEAR - Remove all RADIUS server configurations.
[]>
```

password or passwd

说明

更改密码。

Usage

提交：此命令需要 “提交”。

集群管理：此命令仅限在集群模式下使用。

注　passwd 命令是一个特例，因为它需要对仅能使用计算机模式的访客用户可用。如果访客用户在集群模式下在一台计算机上发出 passwd 密码，则它不会输出警告消息，而只是以静默方式操作集群级别的数据，而不会更改用户的模式。所有其他用户都将体验到上面提到的情况 （与其他受限制的配置命令一致）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> password


Old password: your_old_password
New password: your_new_password
Retype new password: your_new_password
Password changed.
```

last

说明

last 命令显示最近一次登录到系统的人。默认情况下，它显示登录过系统的所有用户。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。

批处理命令：此命令不支持批处理格式。

示例

```
elroy.run> last

Username  Remote Host    Login Time         Logout Time        Total Time
========  =============  =================  =================  ==========
admin     10.251.23.186  Thu Sep 01 09:14   still logged in    1h 5m
admin     10.251.23.186  Wed Aug 31 14:00   Wed Aug 31 14:01   1m
admin     10.251.16.231  Wed Aug 31 13:36   Wed Aug 31 13:37   0m
admin     10.251.23.186  Wed Aug 31 13:34   Wed Aug 31 13:35   0m
admin     10.251.23.142  Wed Aug 31 11:26   Wed Aug 31 11:38   11m
admin     10.251.23.142  Wed Aug 31 11:05   Wed Aug 31 11:09   4m
admin     10.251.23.142  Wed Aug 31 10:52   Wed Aug 31 10:53   1m
admin     10.251.60.37   Tue Aug 30 01:45   Tue Aug 30 02:17   32m
admin     10.251.16.231  Mon Aug 29 10:29   Mon Aug 29 10:41   11m
shutdown                                    Thu Aug 25 22:20
```

who

说明

who 命令列出通过 CLI 登录过系统的所有用户、登录时间、空闲时间以及用户登录时所在的远程主机。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。此命令需要访问本地文件系统。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> who

Username  Login Time  Idle Time  Remote Host  What
========  ==========  =========  ===========  ====
admin     03:27PM     0s         10.1.3.201   cli
```

whoami

说明

whoami 命令显示当前登录用户的用户名和全名，以及该用户所属的组。

Usage

提交：此命令需要 “提交”。

集群管理：此命令可用于所有三种计算机模式 （集群、分组、计算机）。

批处理命令：此命令不支持批处理格式。

示例

```
mail3.example.com> whoami

用户名: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

虚拟设备管理

loadlicense

说明

Loads an XML license for a virtual appliance.您可以从文件中加载，或者可以复制并粘贴。有关完整信息，请参阅以下位置的 《*思科内容安全虚拟设备安装指南*》：
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html。

此命令面向具有 Admin 或 Operator 权限的用户。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令不支持批处理格式。

示例

```
mail.example.com> loadlicense

1 Paste via CLI
2 Load from file
How would you like to load a license file?
[1]> 2

Enter the name of the file in /configurations to import:
[]> <filename>

TERMS AND CONDITIONS OF USE
<Terms and conditions>

Do you accept the above license agreement?
[]> y
The license agreement was accepted.

The following feature key have been added:
<feature keys>
```

还可能显示错误和硬件错误配置。

showlicense

说明

显示当前虚拟设备许可的信息。使用 `featurekey` 命令可以查看更多详细信息。

此命令面向具有 Admin 或 Operator 权限的用户。

Usage

提交：此命令不需要 “提交”。

集群管理：此命令仅限在计算机模式下使用。它被进一步限制为在登录主机 （例如，您登录的特定计算机）上使用。

批处理命令：此命令支持批处理格式。

批处理格式

此命令的语法为：`showlicense`

示例

```
mail.example.com> showlicense

company: Example Inc.
org: Widget Division
unit: Portland Data Center
seats: 1000
city: Portland
state: Oregon
country: US
email: mailadmin@example.com
begin_date: Tue Dec 6 17:45:19 2011
end_date: Mon Sep 1 17:45:19 2014
vln: ABC-123423123
serial: 1003385
```