设置和安装

本章包含以下部分：

安装规划

查看影响规划决策的信息

- 如果您要配置虚拟邮件网关，请先参阅思科内容安全虚拟设备安装指南，然后再继续阅读本章。
- 如果配置的是 M 系列思科安全邮件和 Web 管理器，请参阅在思科安全邮件和 Web 管理器（M 系列）上集中管理服务。
- 我们建议在安装之前先查看了解邮件通道，因为某些特性和功能可能会影响您的基础设施中邮件网关的放置。

计划将邮件网关放置在网络外围

您的邮件网关旨在用作SMTP网关，也称为邮件交换(MX)。为获得最佳效果，某些功能要求邮件网关是具有可直接访问互联网的 IP 地址的第一台机器（即它是外部 IP 地址）才能发送和接收邮件。

根据收件人的信誉过滤，反垃圾邮件、防病毒和病毒爆发过滤器功能（请参阅 IronPort 反垃圾邮件过滤、Sophos 防病毒过滤和病毒爆发过滤器）旨在处理互联网和内部网络邮件的直接流量。您可以

配置邮件网关，对传入及传出企业的所有邮件流量进行策略实施（有关定义允许连接哪些主机的概述）。

确保邮件网关可通过公共互联网访问，且是您的邮件基础设施中的“第一跳”。如果允许另一个 MTA 位于网络周界并处理所有外部连接，则邮件网关将无法确定发件人的 IP 地址。需要发件人的 IP 地址才能识别和区分邮件流监控中的发件人，以查询 IP 信誉服务 获得发件人的 IP 信誉得分，以及提高反垃圾邮件和病毒爆发过滤器功能的效果。

Note 如果无法将邮件网关配置为从互联网接收邮件的第一台机器，仍可以使用邮件网关上提供的一些安全服务。有关详细信息，请参阅 通过传入中继确定部署中的发件人 IP 地址。

当您将邮件网关用作 SMTP 网关时：

- 通过邮件流监控功能（请参阅使用邮件安全监控），可以全面了解贵企业中来自内部和外部发件人的所有邮件流量。
- LDAP 路由、别名和伪装查询（请参阅LDAP 查询）可以整合您的目基础设施并提供更简单的更新。
- 别名表（请参阅创建别名表）、基于域的路由（域映射功能）和伪装（配置伪装）等熟悉的工具可以让您更轻松地从开源 MTA 进行过渡。

在 DNS 中注册邮件安全设备

恶意邮件发件人会主动搜索公共DNS记录寻找新的受害者。为了充分利用反垃圾邮件、病毒爆发过滤器、McAfee 防病毒和 Sophos 防病毒功能，请确保在 DNS 中注册邮件网关。

要在 DNS 中注册邮件网关，请创建一条 A 记录，将邮件网关的主机名映射到其 IP 地址，再创建一条 MX 记录，将您的公共域映射到邮件网关的主机名。您必须为 MX 记录指定优先级，才能将邮件网关公布为域的主 MTA 或备用 MTA。

在下面的示例中，邮件网关 (ironport.example.com) 是域 example.com 的备用 MTA，因为其 MX 记录具有更高的优先级值 (20)。换句话说，该数值越大，MTA 的优先级越低。

```
$ host -t mx example.com
example.com mail is handled (pri=10) by mail.example.com
example.com mail is handled (pri=20) by ironport.example.com
```

通过在DNS中注册邮件网关，无论如何设置MX记录的优先级，都将吸引垃圾邮件攻击。但是，病毒攻击很少会瞄准备用MTA。在这种情况下，如果您最终分地挖掘出防病毒引擎的潜能，请将邮件网关的 MX 记录优先级值设置为等于或高于其他 MTA 值。

安装情景

您可以采用多种方式在现有网络基础设施中安装邮件网关。

以下情景代表了大多数客户的网络配置。如果您的网络配置有很大的差异，并且您需要获得有关安装规划方面的帮助，请联系思科客户支持（请参阅思科客户支持）。

配置概述

下图显示邮件网关在企业网络环境中的典型安装。

在某些情况下，邮件网关位于网络“DMZ”内，此时邮件网关和组件服务器之间会有一道额外的防火墙。

下面介绍以下网络方案：

- 防火墙背后：两个侦听程序配置（图 - 防火墙背后情景/2 个侦听程序配置）

选择与您的基础设施最匹配的配置。然后继续下一部分为系统设置做好准备, on page 8。

传入

- 您指定的本地域接受传入邮件。
- 所有其他域都将被拒绝。
- 外部系统直接连接到邮件网关以在本地域中传输邮件，邮件网关通过 SMTP 路由将邮件中继到适当的组件服务器（例如，Exchange™、Groupwise™、Domino™）。（请参阅路由本地域的邮件。）

传出

- 内部用户发送的传出邮件通过组件服务器路由邮件网关。
- 邮件网关根据私人侦听程序的主机访问表中的设置接受传出邮件。（有关详细信息，请参阅 使用侦听程序。）

以太网接口

在这些配置中，只需要邮件网关上的一个可用以太网接口。但是，您可以配置两个以太网接口，并将您的内部网络与外部互联网连接分开。

有关将多个 IP 地址分配到可用接口的详细信息，请参阅使用虚拟网关™ 技术为所有托管的域配置邮件网关和分配网络和 IP 地址。

硬件端口

硬件设备上端口的数量和类型取决于型号：

端口	Type	C190	C390	C690	C690F	C195	C395	C695	C695F
管理	以太网	0	1	1	1	0	1	1	1
数据	以太网	2*	5	5	3	2*	5	5	3
控制台	序列	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45
远程电源管理 (RPC)	以太网	支持	支持	支持	支持	支持	支持	支持	支持

*对于没有专用管理端口的设备，请使用 Data1 端口进行管理。

有关端口的详细信息，请参阅您的设备型号对应的硬件安装指南。

相关主题

- 配置网络接口, on page 20
- 通过串行连接访问邮件网关
- 启用远程电源循环

高级配置

除了图 - 防火墙后情景/2 个侦听程序配置和图 - 1 个侦听程序配置中显示的配置之外，还可以配置:

- 使用集中管理功能的多个邮件网关。请参阅 使用集群进行集中管理
- 网络接口卡级别的冗余，方法是使用 NIC 配对功能“组合”邮件网关上的两个以太网接口。请参阅 高级网络配置

防火墙设置（NAT，端口）

SMTP 和 DNS 服务必须具有互联网访问权限。其他服务可能也需要打开的防火墙端口。有关详细信息，请参阅防火墙资讯。

将邮件网关通过物理方式连接到网络

- 配置场景, on page 5

配置场景

邮件网关的典型配置情景如下：

- **接口** - 大多数网络环境只需要邮件网关上三个可用以太网接口中的一个。但是，您可以配置两个以太网接口，并将您的内部网络与外部互联网连接分开。
- **公共侦听程序（传入邮件）** - 公共侦听程序接收来自许多外部主机的连接并将邮件定向到数量有限的内部组件服务器。
  - 根据主机访问表 (HAT) 中的设置接受来自外部邮件主机的连接。默认情况下，HAT 配置为接受来自所有外部邮件主机的连接。
  - 仅当为收件人访问表 (RAT) 中指定的本地域寻址时接受传入邮件。所有其他域都将被拒绝。
  - 将邮件中继到适当的内部组件服务器，如 SMTP 路由所定义。
- **私人侦听程序（传出邮件）** - 私人侦听程序接收来自数量受限的内部组件服务器的连接，并将邮件定向到许多外部邮件主机。
  - 内部组件服务器配置为将传出邮件路由到思科 C 或 X 系列邮件网关。
  - 邮件网关根据 HAT 中的设置接受来自内部组件服务器的连接。默认情况下，HAT 配置为中继来自所有内部邮件主机的连接。

相关主题

- 将传入和传出邮件分离, on page 5

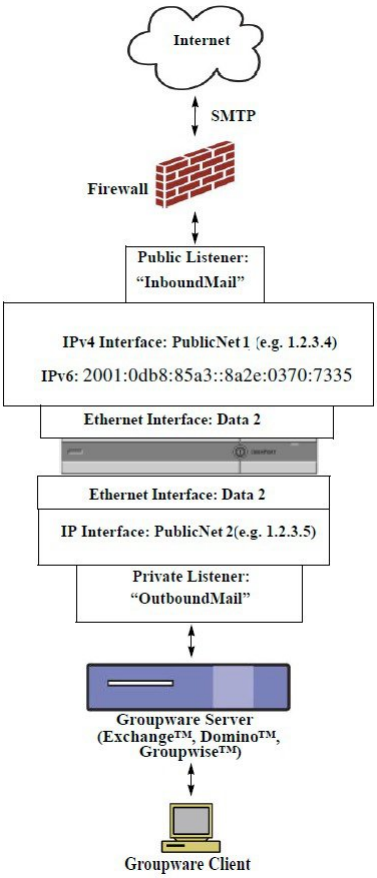
将传入和传出邮件分离

您可以通过单独的侦听程序以及在单独的 IP 地址上分离传入和传出邮件流量。您可以使用互联网协议第 4 版 (IPv4) 和第 6 版 (IPv6) 地址。但是，邮件网关上的系统设置向导支持下列初始配置：

- 在独立的物理接口上配置的 2 个逻辑 IPv4 和 2 个 IPv6 地址上的 2 个独立侦听程序
  - 分离传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址分配到每个侦听程序
- 在一个物理接口配置的 1 个逻辑 IPv4 地址上的 1 个侦听程序
  - 合并传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址都分配到侦听程序

下面包括了一个和两个侦听程序配置的配置工作表（请参阅收集设置信息, on page 11）。大多数配置情景都通过以下三个图之一表示。

Figure 1: 防火墙保护的场景/*2* 个侦听程序配置



说明：

- 2 个侦听程序
- 2 个 IPv4 地址
- 2 个 IPv6 地址
- 1 个或 2 个以太网接口（仅显示了 1 个接口）
- 配置的 SMTP 路由

入站侦听程序：“InboundMail”（公共）

- IPv4 地址：1.2.3.4
- IPv6 地址：2001:0db8:85a3::8a2e:0370:7334
- Data2 接口上的侦听程序侦听端口 25
- HAT（全部接受）
- RAT（接受本地域的邮件；全部拒绝）

出站侦听程序：“**OutboundMail**”（专用）

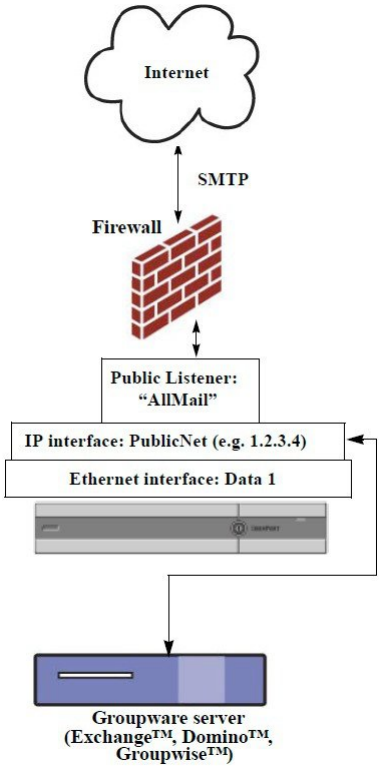
- IP 地址：1.2.3.5
- IPv6 地址：2001:0db8:85a3::8a2e:0370:7335
- Data2 接口上的侦听程序侦听端口 25
- HAT（中继本地域；全部拒绝）

DNS 可配置为使用互联网根服务器或内部 DNS 服务器

SMTP 将邮件直接路由到适当的组件服务器

为适当的服务打开的防火墙端口，用于在与邮件网关之间传输数据

Figure 2: 一个侦听程序配置



说明：

- 1 个侦听程序
- 1 个 IP 地址
- 1 个以太网接口
- 配置的 SMTP 路由

入站侦听程序：“**InboundMail**”（公共）

- IP 地址：1.2.3.4
- Data2 接口上的侦听程序侦听端口 25
- HAT（接受 ALL）包括 RELAYLIST 中组件服务器的条目
- RAT（接受本地域的邮件；全部拒绝）

DNS 可配置为使用互联网根服务器或内部 DNS 服务器

SMTP 将邮件直接路由到适当的组件服务器

为适当的服务打开的防火墙端口，用于在与邮件网关之间传输数据。

为系统设置做好准备

- 确定连接邮件网关的方式, on page 9
- 确定网络和 IP 地址分配, on page 10
- 收集设置信息, on page 11

Procedure

	Command or Action	Purpose
步骤 1	确定如何连接到邮件网关。	请参阅确定连接邮件网关的方式, on page 9
步骤 2	确定网络和 IP 地址分配。 • 如果您已将邮件网关用电缆连接到您的网络，请确保该邮件网关的默认 IP 地址与您网络中的其他 IP 地址未发生冲突。	请参阅 确定连接邮件网关的方式, on page 9 和 确定网络和 IP 地址分配, on page 10
步骤 3	收集系统设置的相关信息。	请参阅收集设置信息, on page 11。
步骤 4	查看邮件网关的最新产品版本说明。	有关版本说明，请访问文档中的链接。
步骤 5	打开邮件网关包装，在机架中对设备进行物理安装，然后将其打开。	请参阅邮件网关的《快速入门指南》。如需该指南，请访问文档中的链接。
步骤 6	如果使用命令行界面 (CLI) 运行安装向导，请访问 CLI。	请参阅运行命令行界面 (CLI) 系统设置向导, on page 26）
步骤 7	如果使用 Web 界面运行安装向导，请执行以下操作：	**a.** （仅限虚拟设备）使用 `interfaceconfig` 命令访问命令行界面并启用 HTTP 和/或 HTTPS。 **b.** 启动网络浏览器并输入邮件网关的 IP 地址。

	Command or Action	Purpose
步骤 8	如果设置的是虚拟邮件网关，请加载虚拟邮件网关许可证。	使用 `loadlicense` 命令。有关详细信息，请参阅思科内容安全虚拟设备安装指南，该指南在文档中的链接中提供。
步骤 9	配置系统的基本设置。	请参阅 使用系统设置向导 , on page 14

确定连接邮件网关的方式

要在您的环境中成功设置邮件网关，您必须从网络管理员那里收集有关您想如何将邮件网关连接到网络的重要网络信息。

相关主题

- 连接到邮件网关, on page 9

连接到邮件网关

在初始设置过程中，您可以通过以下两种方式之一连接到邮件网关：

Table 1: 邮件网关的连接选项

以太网	PC 和网络之间以及网络和管理端口之间的以太网连接。出厂时分配给 Management 端口的 IPv4 地址是 192.168.42.42。这是使用网络配置时最容易的连接方式。
序列	PC 与串行控制台端口之间的串行通信连接。如果您无法使用以太网连接方法，而且暂时无法对管理端口应用其他网络设置，您可以直接在计算机与邮件网关之间建立串行端口到串行端口的连接。有关引出线信息，请参阅通过串行连接访问邮件网关。串行端口的通信设置具体如下： **每秒位数**：9600 **数据位**：8 **奇偶校验**：无 **停止位**：1 **流量控制**：硬件

Note 请记住，初始连接方法不是最终的。此过程仅适用于初始配置。您只能稍后更改网络设置，以允许不同的连接方式。（有关详细信息，请参阅FTP、SSH 和 SCP 访问。）您还可以使用不同的管理权限创建多个用户账号来访问邮件网关。（有关详细信息，请参阅 添加用户。）

确定网络和 IP 地址分配

您可以使用 IPv4 和 IPv6 地址。

管理和数据端口的默认 IP 地址

在管理端口（C170 和 C190 邮件网关上的 Data 1 端口）上预配置的 IP 地址是 192.168.42.42。

选择接收和传送邮件的网络连接

大多数用户会从邮件网关连接到两个网络，充分利用邮件网关的两个数据以太网端口：

- 专用网络接受邮件并将其传送到内部系统。
- 公共网络接受邮件并将其传送到互联网。

其他用户可能希望仅使用一个数据端口来提供两种功能。尽管管理以太网端口可支持任何功能，但它预配置为访问图形用户界面和命令行界面。

将逻辑 IP 地址绑定到物理以太网端口

您可以通过单独的侦听程序以及在单独的 IP 地址上分离传入和传出邮件流量。您可以使用互联网协议第 4 版 (IPv4) 和第 6 版 (IPv6) 地址。但是，邮件网关上的系统设置向导支持下列初始配置：

- 在独立的物理接口上配置的 2 个逻辑 IPv4 和 2 个 IPv6 地址上的 2 个独立侦听程序
  - 分离传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址分配到每个侦听程序
- 在一个物理接口配置的 1 个逻辑 IPv4 地址上的 1 个侦听程序
  - 合并传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址都分配到侦听程序

邮件网关可以在单个侦听程序上同时支持 IPv4 和 IPv6 地址。侦听程序将接受两种地址的邮件。侦听程序的所有设置均适用于 IPv4 和 IPv6 地址。

选择连接的网络设置

您将需要有关您选择使用的每个以太网端口的以下网络信息：

- IP 地址（IPv4 或/或 IPv6）
- CIDR 格式的 IPv4 地址的网络掩码
- CIDR 格式的 IPv6 地址的前缀

此外，还需要有关整个网络的以下信息：

- 网络上默认路由器（网关）的 IP 地址
- DNS 服务器的 IP 地址和主机名（如果要使用互联网根服务器，则无需此信息）
- NTP 服务器的主机名或 IP 地址（如果要使用思科的时间服务器，则无需此信息）

有关详细信息，请参阅分配网络和 IP 地址。

Note 如果您是在网络上的互联网与邮件网关之间运行防火墙，则可能需要打开特定端口以使邮件网关设备正常运行。有关详细信息，请参阅防火墙资讯。

收集设置信息

既然您已了解在系统设置向导中进行必要选择时的需求和策略，请在阅读本节时使用下表收集有关系统设置的信息。

有关网络和 IP 地址的详细信息，请参阅分配网络和 IP 地址。如果配置的是思科安全邮件和 Web 管理器，请参阅在思科安全邮件和 Web 管理器（M 系列）上集中管理服务。

Table 2: 系统设置工作表：用于分离邮件流量的 *2* 个侦听程序

系统设置		
默认系统主机名：		
通过电子邮件将系统警告发送至:		
将计划报告发送到:		
时区信息：		
时钟同步服务器:		
管理员密码：		
SenderBase 网络参与：	启用/禁用	
自动支持:	启用/禁用	
网络集成		
网关：		
DNS（互联网或指定自有 DNS）：		
接口		
Data 1 端口		

系统设置		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**系统**	
Data 2 端口		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**系统**	
管理端口		
IP 地址：		
网络掩码:		
IPv6 Address:		
前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**系统**	
邮件安全		
IP 信誉过滤：	启用/禁用	
反垃圾邮件扫描引擎	无/IronPort	
McAfee 防病毒扫描引擎	启用/禁用	
Sophos 防病毒扫描引擎	启用/禁用	
病毒爆发过滤器	启用/禁用	

Table 3: 系统设置工作表：用于所有邮件流量的 *1* 个侦听程序

系统设置		
默认系统主机名：		
通过电子邮件将系统警告发送至:		
将计划报告发送到:		
时区：		
时钟同步服务器:		
管理员密码：		
SenderBase 网络参与：	启用/禁用	
自动支持:	启用/禁用	
网络集成		
网关：		
DNS（互联网或指定自有 DNS）：		
接口		
Data 2 端口		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**系统**	
Data 1 端口		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
邮件安全		
IP 信誉过滤：	启用/禁用	

系统设置		
反垃圾邮件扫描引擎	无/IronPort	
McAfee 防病毒扫描引擎	启用/禁用	
Sophos 防病毒扫描引擎	启用/禁用	
病毒爆发过滤器	启用/禁用	

使用系统设置向导

您必须使用系统设置向导进行初始设置才能确保配置完整。之后，您可以配置系统设置向导中未提供的自定义选项。

您可以使用浏览器或命令行界面 (CLI) 运行系统设置向导。有关详细信息，请参阅访问基于 Web 的图形用户界面 (GUI), on page 15或运行命令行界面 (CLI) 系统设置向导, on page 26

开始之前，请完成为系统设置做好准备, on page 8中的先决条件。

Caution 如果要设置虚拟邮件网关，您必须在运行系统设置向导之前使用 loadlicense 命令加载您的虚拟邮件网关许可证。有关详细信息，请参阅思科内容安全设备安装指南。

Caution 系统设置向导将完全重新配置您的系统。第一次安装邮件网关时，或者您要完全覆盖现有配置时，您只能使用系统设置向导。

Caution 邮件网关在所有硬件的管理端口上配置默认 IP 地址 192.168.42.42，C170 和 C190 邮件网关除外，其使用 Data 1 端口。在将邮件网关连接到网络之前，请确保其他设备的 IP 地址与此出厂默认设置都不冲突。如果配置的是思科安全邮件和 Web 管理器，请参阅在思科安全邮件和 Web 管理器（M 系列）上集中管理服务。

如果要将多个出厂配置的内容安全设备连接到网络，请一次添加一个，然后对应重新配置每个设备的默认 IP 地址。

访问基于 Web 的图形用户界面 (GUI)

邮件网关采用基于 Web 的标准图形用户界面。这一基于 Web 的新界面可用于管理“邮件安全监控”功能（监控、跟踪和隔离）和命令行界面。

要访问基于 Web 的图形用户界面 (GUI)，请打开浏览器并将其指向 192.168.42.42。

[仅限新 Web 界面] 您可以通过以下方式之一访问新 Web 界面：

Note 邮件网关的新 Web 界面使用 AsyncOS API HTTP/HTTPS 端口 (6080/6443) 和 trailblazer HTTPS 端口 (4431)。您可以在 CLI 中使用 `trailblazerconfig` 命令来配置 trailblazer HTTPS 端口。确保在防火墙中打开 trailblazer HTTPS 端口。

- 当 `trailblazerconfig` CLI 命令启用后，请使用以下 URL - `https://example.com:<trailblazer-https-port>/ng-login`

  其中，`example.com`是邮件网关主机名，`<trailblazer-https-port>` 是在邮件网关上已配置的 trailblazer HTTPS 端口。

  有关 trailblazerconfig CLI 命令的详细信息，请参阅《思科安全邮件命令参考指南》。

- 登录到旧 Web 界面，然后单击 **安全邮件网关将以全新的面貌出现。试用！！访问新 Web 界面的** 链接。

重要说明

- 请确保邮件网关上已启用 AsyncOS API。
- 请确保未在多个接口上启用 AsyncOS HTTPS API 端口。
- 您必须再次登录到邮件网关的旧版 Web 界面。
- 如果已启用 `trailblazerconfig`，则必须在防火墙上打开配置的 HTTPS 端口。默认 HTTPS 端口为 4431。

  确保 DNS 服务器可以解析为访问邮件网关指定的主机名。

相关主题

- 出厂默认用户名和密码, on page 15
- 在黄昏模式下访问新 Web 界面, on page 16

出厂默认用户名和密码

如果安装新的虚拟或硬件邮件网关，则必须更改默认密码才能获得设置邮件网关设备的完整访问权限。首次登录邮件网关时，Web 界面会提示您更改默认密码，并且 CLI 会在您更改默认密码之前限制对以下命令的访问。

- Commit

- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense（适用于虚拟邮件网关）
- 功能密钥
- Ping
- Telnet
- netstat
- 用户名：**admin**
- 密码：**ironport**

例如：

```
login: admin
passphrase: ironport
```

Note 如果会话超时，系统会要求您重新输入用户名和密码。如果在运行系统设置向导时会话超时，您将必须重新启动。

访问旧 Web 界面

要从新 Web 界面访问旧 Web 界面，请单击齿轮图标 ，如下图所示：

图 *3:* 访问旧 *Web* 界面

旧 Web 界面将在新浏览器窗口中打开。您必须重新登录，才能访问该页面。

如果要完全注销该设备，则需要注销邮件网关的新旧 Web 界面。

在黄昏模式下访问新 Web 界面

黄昏模式是一种反向配色方案，在深色背景上使用浅色字体、用户界面元素和图标。

现在，您可以使用黄昏模式来访问邮件网关的新 Web 界面。

要切换到黄昏模式，请单击新 Web 界面右上角的用户图标，然后选择**黄昏模式 (Dusk Theme)**。

使用基于 Web 的系统设置向导定义基本配置

Procedure

步骤 1 启动系统设置向导

- 按照访问基于 Web 的图形用户界面 (GUI), on page 15中的说明登录到图形用户界面。
- 开始使用全新（并非从旧版 AsyncOS 升级）系统时，会将您的浏览器会自动重新定向到系统设置向导。
- 否则，在“系统管理”(System Administration) 选项卡中，单击左侧链接列表中的“系统设置向导”(System Setup Wizard)。

步骤 2 开始。请参阅第 1 步：开始, on page 18。

- 阅读并接受许可协议

步骤 3 系统。请参阅第 2 步：系统, on page 18。

- 设置邮件网关的主机名
- 配置警告设置、报告交付设置和自动支持
- 设置系统时间设置和 NTP 服务器
- 重新设置管理员密码
- 启用服务日志

步骤 4 网络。请参阅第 3 步：网络, on page 19。

- 定义默认路由器和 DNS 设置
- 启用和配置网络接口，包括：配置传入邮件（入站侦听程序）、定义 SMTP 路由（可选）、配置传出邮件（出站侦听程序）和定义允许通过邮件网关中继邮件的系统（可选）

步骤 5 安全性请参阅第 4 步：安全, on page 23。

- 启用 IP 信誉过滤
- 启用反垃圾邮件服务
- 启用垃圾邮件隔离区
- 启用防病毒服务
- 启用高级恶意软件防护（文件信誉和分析服务）
- 启用病毒爆发过滤器服务

步骤 6 审查。请参阅第 5 步：审查, on page 24。

- 审查您的设置和安装配置
- 在该过程结束时，系统会提示

步骤 7 提交您做出的更改。

在您提交后更改才会生效。

第 1 步：开始

首先阅读许可协议。阅读并接受许可协议后，请选中指示您同意的框，然后单击**开始设置** (Begin Setup) 执行。

您还可以在以下位置查看协议的文本：https://support.ironport.com/license/eula.html

第 2 步：系统

- 设置主机名, on page 18
- 配置系统警报, on page 18
- 配置报告交付, on page 18
- 设置时间, on page 18
- 设置密码, on page 19
- 使用服务日志来提高网络钓鱼检测效率
- 启用自动支持, on page 19

设置主机名

为邮件网关定义完全限定主机名。此名称应由网络管理员分配。

配置系统警报

如果存在需要用户干预的系统错误，则 Cisco AsyncOS 会通过邮件发送警报消息。输入接收这些警报的邮件地址。

您必须至少添加一个接收系统警报的邮件地址。输入一个邮件地址或用逗号分隔多个地址。邮件收件人最初会收到所有级别的所有类型的警报，但不会收到目录收割攻击预防警报。您可以稍后进一步细化警报配置。有关详细信息，请参阅警报。

配置报告交付

输入接收默认计划报告的地址。如果您将此值留空，仍会运行计划报告。计划报告将在邮件网关上存档而非通过设备交付。

设置时间

在邮件网关上设置时区，以便邮件头和日志文件中的时间戳是正确的。使用下拉菜单找到您所在的时区或通过 GMT 偏移定义时区（有关详细信息，请参阅选择 GMT 偏移）。

您可以之后手动设置系统时钟时间，也可以使用网络时间协议 (NTP) 来与网络或互联网中的其他服务器同步。默认情况下，已配置用于同步邮件网关时间的思科系统时间服务器(**time.ironport.com**)的一个条目。

设置密码

设置管理员账户的密码。这是必需的步骤。在更改 Cisco AsyncOS 管理员账户的密码时，新密码的长度必须为六个或以上字符。请务必将密码保存在安全的位置。

除了手动创建登录密码之外，您还可以创建系统生成的密码以登录邮件网关。

启用服务日志

“服务日志”会被发送到思科 Talos 云服务，以改进网络钓鱼检测。

如果启用服务日志，思科邮件安全网关只会从客户邮件中收集有限的个人数据，并提供大量有用的威胁检测功能，这些功能可与专用分析系统结合使用，来收集观察到的威胁活动，然后分析其趋势并建立关联。思科会将这些个人数据用于改进思科安全邮件云网关的功能，以分析威胁形势、提供对恶意邮件的威胁分类解决方案，以及保护邮件网关免受新威胁（例如垃圾邮件、病毒和目录搜集攻击）的攻击。

有关详细信息，请参阅使用服务日志来提高网络钓鱼检测效率。

启用自动支持

自动支持功能（默认已启用）使思科客户支持团队能够及时了解邮件网关的问题，以便可以更好地为您提供支持。（有关详细信息，请参阅 自动支持。）

单击**下一步 (Next)** 继续操作。

第 3 步：网络

第 3 步，定义默认路由器（网关）并配置 DNS 设置，然后通过配置 Data 1、Data 2 和管理接口设置邮件网关来接收和或回复邮件。

- 配置 DNS 和默认网关, on page 19
- 配置网络接口, on page 20
- 接受邮件, on page 20
- 中继邮件（可选）, on page 21
- C170 和 C190 安装, on page 22

配置 DNS 和默认网关

输入网络中默认路由器（网关）的 IP 地址。您可以使用 IPv4 地址、IPv6 地址或以上两者。

接下来，配置 DNS（域名服务）设置。Cisco AsyncOS 包含可以直接查询互联网根服务器的高性能内部 DNS 解析程序/缓存，或者系统可以使用您指定的 DNS 服务器。如果选择使用自己的服务器，将需要提供每个 DNS 服务器的 IP 地址和主机名。您可以通过系统设置向导最多输入四个 DNS 服务器。请注意，您输入的 DNS 服务器的初始优先级为 0。有关详细信息，请参阅配置域名系统 (DNS) 设置。

Note 邮件网关需要访问正在工作的 DNS 服务器才能对传入连接执行 DNS 查找。如果您在设置邮件网关时无法指定邮件网关可访问的正在工作的 DNS 服务器，解决方法是选择“使用互联网根 DNS 服务器”(Use Internet Root DNS Servers)，或临时指定管理接口的 IP 地址，以便完成系统设置向导。

配置网络接口

您的邮件网关具有与计算机的物理以太网端口关联的网络接口。

要使用某个接口，请选中“启用”(Enable) 复选框，然后指定 IP 地址、网络掩码和完全限定的主机名。您输入的 IP 地址应当是您的 DNS 记录反映的入站邮件的 IP 地址。此地址通常具有与 DNS 中的记录关联的 MX记录。您可以使用 IPv4 地址、IPv6 地址或以上两者。如果使用以上两者，接口将接受两种类型的连接。

每个接口都可配置为接受邮件（传入）、中继邮件（传出）或设备管理。在设置过程中，每个接口只能限制为配置一种功能。在大多数邮件网关上，通常一个接口用于传入邮件，一个接口用于传出邮件，一个接口用于设备管理。在 C170 和 C190 邮件网关上，通常一个接口用于传入和传出邮件，另一个接口用于管理。

您必须将一个接口配置为接收邮件。

向邮件网关上的其中一个物理以太网接口分配和配置逻辑 IP 地址。如果决定同时使用 Data 1 以太网端口和 Data 2 以太网端口，则两个连接都需要此信息。

对于 C390 和 C690 设备：思科建议使用其中一个物理以太网端口直接连接到互联网，以通过公共侦听程序接收入站邮件；建议使用另一个物理以太网端口直接连接到您的内部网络，以通过专用侦听程序中继出站邮件。

对于 C190 设备：通常，系统设置向导仅配置一个物理以太网端口和一个侦听程序，同时用于接收入站邮件和中继出站邮件。

请参阅将逻辑 IP 地址绑定到物理以太网端口, on page 10。

需要提供以下信息：

- 由网络管理员分配的 **IP 地址**。这可以是 IPv4 地址、IPv6 地址或以上两者。
- 对于 IPv4 地址：接口的**网络掩码**。AsyncOS 仅接受 CIDR 格式的网络掩码。例如，`255.255.255.0` 子网的网络掩码为 `/24`。

  对于 IPv6 地址：CIDR 格式的**前缀**。例如 64 位前缀为 `/64`。
- （可选）IP 地址的完全限定主机名。

Note 无法在单独的物理以太网接口上配置相同子网内的 IP 地址。有关网络和 IP 地址配置的详细信息，请参阅分配网络和 IP 地址。

接受邮件

在配置接口接收邮件时，需要定义：

- 为其接受邮件的域
- 每个域的目标（SMTP 路由），这是可选选项

选中“接受传入邮件”(Accept Incoming Mail) 复选框以将接口配置为接受邮件。输入为其接受邮件的域名。

输入目标。这是要为指定的域路由邮件所在计算机的 SMTP 路由或名称。

这是第一个 SMTP 路由条目。SMTP 路由表可让您为输入到特定邮件交换 (MX) 主机的每个域（也称为收件人访问表 [RAT] 条目）重定向所有邮件。在典型安装中，SMTP 路由表定义特定组件（例如，Microsoft Exchange）服务器或基础设施的邮件传送中的“下一跳”。

例如，您可以定义一个路由，指定为域 `example.com` 和所有其子域 `.example.com` 接受的邮件路由到组件服务器 `exchange.example.com`。

您可以输入多个域和目标。单击**添加行 (Add Row)** 添加另一个域。单击垃圾箱图标可删除行。

Note 在此步骤中配置 SMTP 是可选操作。如果未定义任何 SMTP 路由，系统将使用 DNS 查找并确定侦听程序收到的传入邮件的传输主机。（请参阅路由本地域的邮件。）

您必须至少添加一个域到收件人访问表。例如，输入域 `example.com`。要确保发往 `example.net` 任何子域的邮件在收件人访问表中匹配，请输入 `.example.net` 以及域名。有关详细信息，请参阅定义收件人地址。

中继邮件（可选）

在配置邮件中继接口时，要定义系统，允许通过邮件网关中继邮件。

这些是侦听程序的主机访问表的 RELAYLIST 中的条目。有关详细信息，请参阅发件人组语法。

选中“中继传出邮件”(Relay Outgoing Mail) 复选框以将接口配置为中继邮件。输入可以通过邮件网关中继邮件的主机。

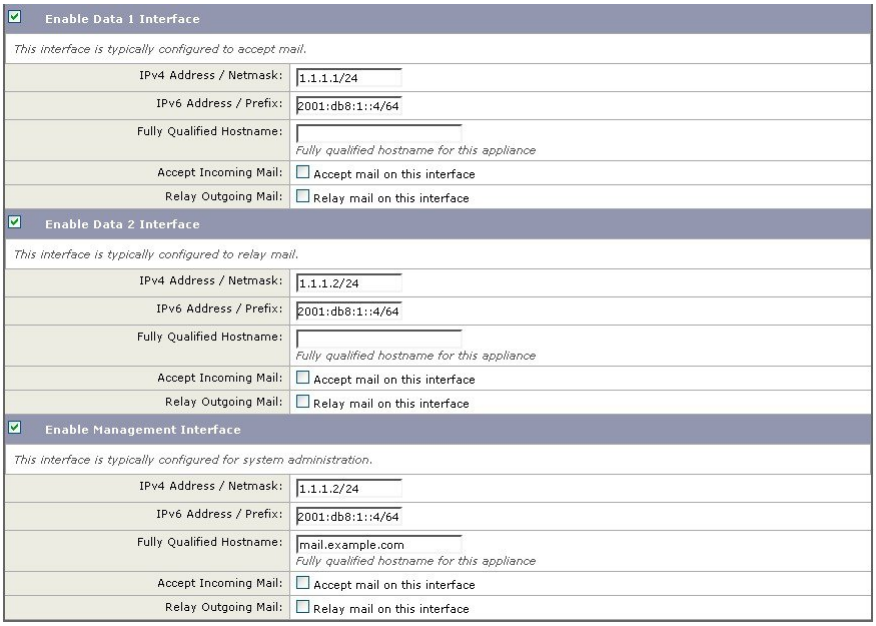
当您配置中继出站邮件的接口时，只要没有公共侦听程序配置为使用该接口，系统设置向导就会打开该接口的 SSH。

在下面的示例中，创建两个具有 IPv4 地址的接口：

- 管理接口依然配置为 192.168.42.42。
- 在 Data 1 以太网接口上启用 192.168.1.1。它配置为接受以 .example.com 结尾的域的邮件，SMTP 路由为 exchange.example.com 定义。
- 在 Data 2 以太网接口上启用 192.168.2.1。它配置为从 exchange.example.com 中继邮件。

C390 和 C690 安装

Figure 4: 网络接口：除了管理接口（已分流的流量）之外的 ***2*** 个接口

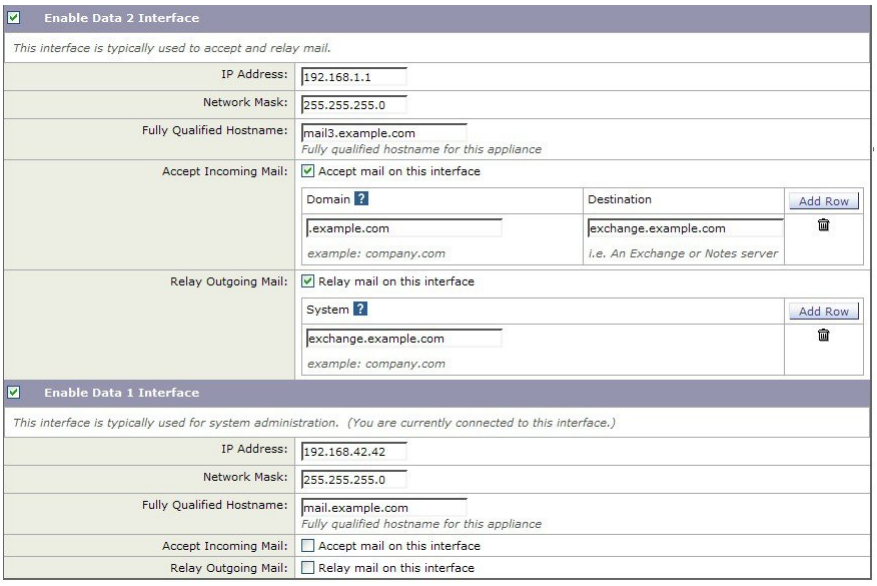


C170 和 C190 安装

对于 C170 和 C190 设备，Data 1 接口通常配置为用于传入邮件和传出邮件，而 Data 2 接口用于设备管理。

当配置单一 IP 地址用于所有邮件流量（未分流的流量）时，系统设置向导的第 3 步如下所示：

Figure 5: 网络接口：用于传入和传出（未分流）流量的 ***1*** 个 ***IP*** 地址



单击**下一步 (Next)** 继续操作。

第 4 步：安全

步骤 4，配置反垃圾邮件和防病毒设置。反垃圾邮件选项包括 IP 信誉过滤和选择反垃圾邮件扫描引擎。对于防病毒，您可以启用病毒爆发过滤器和 Sophos 或 McAfee 防病毒扫描。

- 启用 IP 信誉过滤, on page 23
- 启用反垃圾邮件扫描, on page 23
- 启用防病毒扫描, on page 23
- 启用高级恶意软件防护（文件信誉和分析服务） , on page 23
- 启用病毒爆发过滤器, on page 24

启用 IP 信誉过滤

IP 信誉服务可以用作独立的反垃圾邮件解决方案，但是，它主要用于提高基于内容的反垃圾邮件系统（例如反垃圾邮件）的效率。

IP 信誉服务为用户提供基于远程主机的连接 IP 地址，准确、灵活地拒绝或“限制”可疑垃圾邮件的方法。IP 信誉服务根据从指定源发送的邮件是垃圾邮件的概率返回一个分数。IP 信誉服务的独特之处在于它提供邮件量的全局视图且数据组织方式易于识别和分组邮件的相关源。思科强烈建议您启用 IP 信誉过滤。

启用后，IP 信誉过滤会应用到传入（接受）侦听程序。

启用反垃圾邮件扫描

您的邮件网关可能随附反垃圾邮件软件的30天试用版密钥。在系统设置向导的这一部分，您可以选择在邮件网关上全局启用反垃圾邮件。您还可以选择不启用该服务。

如果您选择启用反垃圾邮件服务，则可以将 AsyncOS 配置为将垃圾邮件和可疑垃圾邮件发送到本地垃圾邮件隔离区。垃圾邮件隔离区用作邮件网关的最终用户隔离区。在配置最终用户访问权限之前，只有管理员可以访问隔离区。

请参阅管理垃圾邮件和灰色邮件，了解邮件网关上提供的所有反垃圾邮件配置选项。请参阅策略、病毒和病毒爆发隔离区。

启用防病毒扫描

您的邮件网关可能随附 Sophos 防病毒或 McAfee 防病毒扫描引擎的 30 天试用版密钥。在系统设置向导的这一部分，您可以选择在邮件网关上全局启用防病毒扫描引擎。

如果选择启用防病毒扫描引擎，则会为默认传入邮件和默认传出邮件策略都启用该引擎。邮件网关会扫描邮件以查看是否存在病毒，但不修复受感染的附件。邮件网关会丢弃感染的邮件。

请参阅防病毒，了解邮件网关上提供的所有反垃圾邮件配置选项。

启用高级恶意软件防护（文件信誉和分析服务）

高级恶意软件防护可获取有关基于云的服务所附加文件的相关信誉信息。

有关详细信息，请参阅文件信誉过滤和文件分析：

启用病毒爆发过滤器

您的邮件网关可能随附病毒爆发过滤器的30天试用版密钥。病毒爆发过滤器会在传统的防病毒安全服务更新为新的病毒签名文件之前隔离可疑邮件，提供防新病毒爆发的“第一道防线”。

有关详细信息，请参阅病毒爆发过滤器。

单击**下一步 (Next)** 继续操作。

第 5 步：审查

配置信息的摘要已显示。您可以单击**旧版 (Previous)** 按钮或单击每部分右上角的**编辑 (Edit)** 链接编辑系统设置、网络集成和邮件安全信息。当您返回某步进行更改时，您必须继续完成所有剩余步骤，一直到此审查页面。您之前输入的所有设置都会保留。

您对显示的信息满意后，请单击**安装此配置 (Install This Configuration)**。

系统会显示确认对话框。单击**安装 (Install)** 安装新配置。

您的邮件网关现已就绪，可以发送邮件。

Note 如果已更改用于连接到邮件网关的接口的默认 IP 地址，则单击**安装 (Install)** 将导致与当前 URL (http://192.168.42.42) 的连接丢失。但是，您的浏览器将重新定向到新的 IP 地址。

系统设置完成后，系统会发送多条警报消息。有关详细信息，请参阅即时警报, on page 39。

设置与 Active Directory 的连接

如果系统设置向导在邮件网关上正确安装了该配置，则会显示 Active Directory 向导。如果要在您的网络中运行 Active Directory 服务器，请使用 Active Directory 向导为 Active Directory 服务器配置 LDAP 服务器配置文件，并分配侦听程序进行收件人验证。如果没有使用 Active Directory 或者希望稍后再进行配置，请单击“跳过此步骤”(Skip this Step)。您可以在**系统管理 (System Administration) > Active Directory 向导 (Active Directory Wizard)** 页面上运行 Active Directory 向导。您还可以在**系统管理 (System Administration) > LDAP** 页面上配置 Active Directory 和其他 LDAP 配置文件。

Active Directory 向导会检索创建 LDAP 服务器配置文件所需的系统信息，例如身份验证方法、端口、基本 DN 以及是否支持 SSL。Active Directory 向导还创建 LDAP 服务器配置文件的 LDAP 接受和分组查询。

Active Directory 向导创建 LDAP 服务器配置文件后，请使用 **系统管理 (System Administration) > LDAP** 页面查看新的配置文件并进行其他更改。建议您不要更改 思科安全邮件云网关上的 LDAP 设置。

Procedure

步骤 1 在“Active Directory 向导”(Active Directory Wizard) 页面上，单击**运行 Active Directory 向导 (Run Active Directory Wizard)**。

步骤 2 输入 Active Directory 服务器的主机名。

步骤 3 输入身份验证请求的用户名和密码。

步骤 4 单击**下一步 (Next)** 继续操作。

Active Directory 向导会测试与 Active Directory 服务器的连接。如果成功，则会显示“测试目录设置”(Test Directory Settings) 页面。

步骤 5 输入您知道存在于 Active Directory 中的邮件地址并单击**测试 (Test)**，来测试目录设置。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 6 单击**完成 (Done)**。

继续执行后续步骤

在您已成功将邮件网关配置为与 Active Directory 向导配合使用或跳过该流程后，系统会显示“系统设置后续步骤”(System Setup Next Steps) 页面。

单击“系统设置后续步骤”(System Setup Next Steps) 页面上的链接，继续配置您的邮件网关。

访问命令行界面 (CLI)

对 CLI 的访问因您在连接到邮件网关, on page 9中选择的管理连接方式而异。出厂默认用户名和口令在后面列出。最初，只有管理员用户账户具有访问 CLI 的权限。在您通过管理员账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。（有关添加用户的信息，请参阅添加用户。）“系统设置向导”会要求您更改管理员账户的口令。还可以随时使用 `passphrase` 命令直接重置管理员账户的口令。

通过以太网连接：使用出厂默认 IP 地址 192.168.42.42 启动 SSH 会话。SSH 配置为使用端口 22。在下面输入您的用户名和口令。

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。对连接到邮件网关, on page 9中所述的串行端口使用设置。在下面输入您的用户名和口令。

通过输入用户名和口令登录邮件网关。

相关主题

- 出厂默认用户名和密码, on page 15

出厂默认用户名和密码

如果安装新的虚拟或硬件邮件网关，则必须更改默认密码才能获得设置邮件网关设备的完整访问权限。首次登录邮件网关时，Web 界面会提示您更改默认密码，并且 CLI 会在您更改默认密码之前限制对以下命令的访问。

- Commit
- Interfaceconfig

- passphrase
- Loadconfig
- Systemsetup
- loadlicense（适用于虚拟邮件网关）
- 功能密钥
- Ping
- Telnet
- netstat
- 用户名：**admin**
- 密码：**ironport**

例如：

```
login: admin
passphrase: ironport
```

Note 如果会话超时，系统会要求您重新输入用户名和密码。如果在运行系统设置向导时会话超时，您将必须重新启动。

运行命令行界面 (CLI) 系统设置向导

CLI 版系统设置向导与 GUI 版中的步骤基本一致，只有少数例外情况：

- CLI 版包括启用 Web 界面的提示。
- CLI 版允许您编辑自己创建的每个侦听程序的默认邮件流策略。
- CLI 版包含配置全局防病毒和病毒爆发过滤器安全设置的提示。
- 在系统设置完成后，CLI 版不提示您创建 LDAP 配置文件。使用 `ldapconfig` 命令创建 LDAP 配置文件。

要运行系统设置向导，请在命令提示符下键入 `systemsetup`。

```
IronPort> systemsetup
```

系统设置向导会警告您将重新配置您的系统。如果这是您第一次安装邮件网关，或者如果您要完全覆盖现有配置，请对以下问题回答“是”(Yes)。

```
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
```

Note 其他系统设置步骤如下所述。只有与使用基于 Web 的系统设置向导定义基本配置 , on page 17中所述的 GUI 系统设置向导存在偏差的部分才会包含 CLI 系统设置向导对话框示例。

相关主题

- 更改管理员密码, on page 27
- 接受许可协议, on page 27
- 设置主机名 , on page 27
- 分配并配置逻辑 IP 接口, on page 28
- 指定默认网关, on page 28
- 启用 Web 界面, on page 29
- 配置 DNS 设置, on page 29
- 创建侦听程序, on page 29
- 启用反垃圾邮件, on page 36
- 选择默认反垃圾邮件扫描引擎, on page 37
- 启用垃圾邮件隔离区, on page 37
- 启用防病毒扫描, on page 37
- 启用病毒爆发过滤器, on page 37
- 配置警报设置和自动支持, on page 37
- 配置计划报告, on page 38
- 配置时间设置, on page 38
- 确认更改, on page 38
- 测试配置, on page 38
- 即时警报, on page 39

更改管理员密码

首先，更改 AsyncOS 管理员帐户的密码。您必须输入旧密码才能继续。新密码必须至少为 6 个或以上字符。请务必将密码保存在安全的位置。密码更改在系统设置完成后生效。

除了手动创建登录密码之外，您还可以创建系统生成的密码以登录邮件网关。

接受许可协议

阅读并接受显示的软件许可协议。

设置主机名

接下来，为邮件网关定义完全限定主机名。此名称应由网络管理员分配。

分配并配置逻辑 IP 接口

下一步将在名为 Management（在 C390 和 C690 设备上）或名为 Data 1（在 C190 设备上）的物理以太网接口上分配和配置逻辑 IP 接口，然后提示您在邮件网关的任何其他可用物理以太网接口上配置逻辑 IP 接口。

每个以太网接口可分配有多个 IP 接口。IP 接口是一个将 IP 地址和主机名与物理以太网接口相关联的逻辑结构。如果您决定同时使用 Data 1 和 Data 2 以太网端口，则您需要两个连接的 IP 地址和主机名。

对于 C390 和 C690 设备：思科建议使用其中一个物理以太网端口直接连接到互联网，以通过公共侦听程序接收入站邮件；建议使用另一个物理以太网端口直接连接到您的内部网络，以通过专用侦听程序中继出站邮件。

对于 C170 和默认情况下，`systemsetup` 命令将通过一个侦听程序仅配置一个物理以太网端口，既可以接收入站邮件，也可以中继出站邮件。

Note 当您配置转发出站邮件的接口时，只要未将任何公共侦听程序配置为使用接口，系统就会打开接口的 SSH。

需要提供以下信息：

- 您创建的用于稍后指代 IP 接口的**名称**（昵称）。例如，如果您将一个以太网端口用于专用网络，另一个用于公共网络，您可能想要将它们分别命名为 PrivateNet 和 PublicNet。

  Note 为接口定义的名称区分大小写。AsyncOS 将不允许创建两个相同的接口名称。例如，名称 **`Privatenet`** 和 **`PrivateNet`** 被视为两个不同（唯一）的名称。

- 由网络管理员分配的 **IP 地址**。这可以是 IPv4 或 IPv6 地址，您可以为单一 IP 接口分配两种类型的 IP 地址。
- 接口的**网络掩码**。网络掩码必须采用 CIDR 格式。例如，使用 `/24` 作为 `255.255.255.0` 子网的网络掩码。

  Note 无法在单独的物理以太网接口上配置相同子网内的 IP 地址。有关网络和 IP 地址配置的详细信息，请参阅分配网络和 IP 地址。

  对于 C190 设备，最先配置 Data 2 接口。

指定默认网关

在 `systemsetup` 命令的下一部分中，键入网络上默认路由器（网关）的 IP 地址。

启用 Web 界面

在 systemsetup 命令的后面部分，为邮件网关启用 Web 界面（适用于管理以太网接口）。您还可以选择通过安全的 HTTP (https) 运行 Web 界面。如果选择使用 HTTPS，则系统将使用演示证书，直至您上传自己的证书为止。

配置 DNS 设置

接下来，配置 DNS（域名服务）设置。Cisco AsyncOS 具有可直接查询互联网根服务器的高性能内部 DNS 解析程序/缓存，系统还可以使用您自己的 DNS 服务器。如果您选择使用自己的服务器，您将需要提供每个 DNS 服务器的 IP 地址和主机名。您可以输入所需数量的 DNS 服务器（每个服务器将具有优先级 0）。默认情况下，systemsetup 会提示您输入您自己的 DNS 服务器的地址。

创建侦听程序

“侦听程序”管理在特定 IP 接口上配置的入站邮件处理服务。侦听程序仅适用于从您的内部系统或从互联网进入邮件网关的邮件。Cisco AsyncOS 使用侦听程序指定邮件为获得接受和转发到收件人主机所必须满足的条件。您可以将侦听程序视为针对以上指定的 IP 地址运行的邮件侦听程序（甚至“SMTP 后台守护程序”）。

对于 、C390 和 C690 设备：默认情况下，systemsetup 命令配置两个侦听程序 - 一个公共侦听程序，一个专用侦听程序。（有关可用侦听程序类型的详细信息，请参阅配置网关以接收邮件。）

对于 C190 设备：默认情况下，systemsetup 命令配置一个公共侦听程序，既接收来自互联网的邮件，也中继来自内部网络的邮件。请参阅C190 设备的侦听程序示例 , on page 34。

当您定义侦听程序时，您应指定以下属性：

- 您创建的用于稍后指代侦听程序的**名称**（昵称）。例如，从您的内部系统接收即将传送到互联网的邮件的侦听程序可能被称为 OutboundMail。
- 用于接收邮件的其中一个 IP 接口（您之前使用 systemsetup 命令创建的接口）。
- 要向其路由邮件的机器的名称（仅限公共侦听程序）。（这是第一个 smtproutes 条目。请参阅路由本地域的邮件。）
- 根据公共侦听程序的 IP 信誉分数确定是否启用过滤。如果启用，系统还会提示您在“保守”(Conservative)、“中等”(Moderate) 或“主动”(Aggressive) 设置之间进行选择。
- 每台主机的速率限制：每小时您愿意从远程主机接收的最大收件人数量（仅限公共侦听程序）。
- 您要为其接收邮件的收件人域或特定地址（公共侦听程序）或允许通过邮件网关转发邮件的系统（专用侦听程序）。（这些是侦听程序的第一个收件人访问表和主机访问表条目。如需更多信息，请参阅发件人组语法和添加为其接受邮件的域和用户。）

相关主题

- 公共侦听程序, on page 30
- 专用侦听程序, on page 32
- C190 设备的侦听程序示例 , on page 34

公共侦听程序

Note 创建公共和专用侦听程序的以下示例仅适用于 设备。对于 C190 设备，请跳到下一部分C190 设备的侦听程序示例 , on page 34。

在 `systemsetup` 命令的此示例部分中，名为 InboundMail 的公共侦听程序配置为在 PublicNet IP 接口上运行。然后，该侦听程序配置为接受 `example.com` 域的所有邮件。配置到邮件交换 `exchange.example.com` 的初始 SMTP 路由。已启用速率限制，并为公共侦听程序指定了单个主机每小时 4500 个收件人的最大值。

Note 您为希望从远程主机每小时接收的最大邮件数输入的值是完全随机值，通常相对于您要为其管理邮件的企业规模。例如，在 1 小时内发送 200 封邮件的发件人可能被视为“垃圾邮件制造者”（垃圾邮件发送者），但如果您将邮件网关配置为处理一家 10,000 人的公司的所有邮件，每小时从远程主机收到 200 封邮件可能很合理。相反，在一家 50 人的公司中，在一小时内向您发送 200 封邮件的人很显然就是一个垃圾邮件制造者。当您为设备启用公共侦听程序（限制）入站邮件的速率限制时，必须选择适当的值。有关默认主机访问策略的详细信息，请参阅发件人组语法。

之后，系统接受侦听程序的默认主机访问策略。

```
You are now going to configure how the appliance accepts mail by

creating a "Listener".

Please create a name for this listener (Ex: "InboundMail"):

[]> InboundMail


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]> 3


Enter the domains or specific 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


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server which you want mail for example.com to be delivered.
Separate multiple entries with commas.

[]> exchange.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.) [Y]> y


Enter the maximum number of recipients per hour to accept from a remote domain.

[]> 4500


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 1,000

Maximum Number Of Messages Per Connection: 1,000

Maximum Number Of Recipients Per Message: 1,000

Maximum Number Of Recipients Per Hour: 4,500

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour
```

```
Use SenderBase for Flow Control:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: 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.

*****
```

专用侦听程序

在 systemsetup 命令的此示例部分中，名为 OutboundMail 的专用侦听程序配置为在 PrivateNet IP 接口上运行。然后，配置为中继 `example.com` 域内所有主机的所有邮件。（请注意，条目开始处的句点：`.example.com`）

然后，将会接受速率限制（未启用）的默认值和此侦听程序的默认主机访问策略。

请注意，专用侦听程序的默认值与之前创建的公共侦听程序的不同。有关详细信息，请参阅使用侦听程序。

```
Do you want to configure the appliance to relay mail for internal hosts?  [Y]> y


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


Please specify the systems allowed to relay email through the appliance.
```

```
Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed 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

Virus Detection Enabled:  Yes

Allow TLS Connections: 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.

*****
```

C190 设备的侦听程序示例

Note 创建侦听程序的以下示例仅适用于 C170 和 C190 设备。

在 systemsetup 命令的此示例部分中，名为 MailInterface 的侦听程序配置为在 MailNet IP 接口上运行。然后，该侦听程序配置为接受 example.com 域的所有邮件。配置到邮件交换 exchange.example.com 的初始 SMTP 路由。然后，同一侦听程序会配置为中继 example.com 域内所有主机的所有邮件。（请注意，条目开始处的句点：.example.com）

已启用速率限制，并为公共侦听程序指定了单个主机每小时 450 个收件人的最大值。

Note 您为希望从远程主机每小时接收的最大邮件数输入的值是完全随机值，通常相对于您要为其管理邮件的企业规模。例如，在 1 小时内发送 200 封邮件的发件人可能被视为“垃圾邮件制造者”（垃圾邮件发送者），但如果您将邮件网关配置为处理一家 10,000 人的公司的所有邮件，每小时从远程主机收到 200 封邮件可能很合理。相反，在一家 50 人的公司中，在一小时内向您发送 200 封邮件的人很显然就是一个垃圾邮件制造者。当您为设备启用公共侦听程序（限制）入站邮件的速率限制时，必须选择适当的值。有关默认主机访问策略的详细信息，请参阅发件人组语法。

之后，系统接受侦听程序的默认主机访问策略。

```
You are now going to configure how the appliance accepts mail by creating a "Listener".

Please create a name for this listener (Ex: "MailInterface"):

[]> MailInterface


Please choose an IP interface for this Listener.

1. MailNet (10.1.1.1/24: mail3.example.com)

2. Management (192.168.42.42/24: mail3.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


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server where you want mail for example.com to be delivered.
Separate multiple entries with commas.

[]> exchange.example.com


Please specify the systems allowed to relay email through the appliance.

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.)  [Y]> y


Enter the maximum number of recipients per hour to accept from a remote domain.

[]> 450


Default Policy Parameters

==========================

Maximum Message Size: 10M

Maximum Number Of Connections From A Single IP: 50
```

```
Maximum Number Of Messages Per Connection: 100

Maximum Number Of Recipients Per Message: 100

Maximum Number Of Recipients Per Hour: 450

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

Would you like to change the default host access policy?  [N]>


Listener MailInterface created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

Note 由于 `systemsetup` 命令仅配置一个侦听程序，用于处理 C170 和 C190 设备的入站和出站邮件，所有传出邮件将采用邮件流监控功能计算（通常用于入站邮件）。请参阅 使用邮件安全监控

启用反垃圾邮件

您的邮件网关随附反垃圾邮件软件的30天试用版密钥。在**systemsetup**命令的此部分中，您可以选择接受许可协议，并且在邮件网关上全局启用反垃圾邮件功能。

然后，将会在传入邮件策略上启用反垃圾邮件扫描。

Note 如果未接受许可协议，则不会在邮件网关上启用反垃圾邮件功能。

请参阅管理垃圾邮件和灰色邮件，了解邮件网关上提供的所有反垃圾邮件配置选项。

选择默认反垃圾邮件扫描引擎

如果您启用了多个反垃圾邮件扫描引擎，系统会提示您选择启用哪个引擎以对默认传入邮件策略使用。

启用垃圾邮件隔离区

如果您选择启用反垃圾邮件服务，您可以启用传入邮件策略以将垃圾邮件和可疑的垃圾邮件发送到本地垃圾邮件隔离区。启用垃圾邮件隔离区还会在邮件网关上启用终端用户隔离区。在配置最终用户访问权限之前，只有管理员可以访问最终用户隔离区。

请参阅设置本地垃圾邮件隔离区。

启用防病毒扫描

您的邮件网关随附病毒扫描引擎的 30 天试用版密钥。在 `systemsetup` 命令的这一部分，您可以选择接受一个或多个许可协议并在邮件网关启用防病毒扫描。您必须接受您要对邮件网关启用的每个防病毒扫描引擎的许可协议。

接受协议后，将会在传入邮件策略上启用所选择的防病毒扫描引擎。邮件网关会扫描传入邮件以查看是否存在病毒，但不修复受感染的附件。设备会丢弃感染的邮件。

请参阅防病毒，了解邮件网关上提供的反垃圾邮件配置选项。

启用病毒爆发过滤器

下一步，提示您启用 病毒爆发过滤器。您的邮件网关随附病毒爆发过滤器的 30 天试用版密钥。

相关主题

- 病毒爆发过滤器, on page 37

病毒爆发过滤器

病毒爆发过滤器会在传统的防病毒安全服务更新为新的病毒签名文件之前隔离可疑邮件，提供防新病毒爆发的“第一道防线”。如果启用，将对默认传入邮件策略启用病毒爆发过滤器。

如果您选择启用病毒爆发过滤器，请输入阈值以及您是否要接收病毒爆发过滤器警报。有关病毒爆发过滤器和阈值的更多信息，请参阅病毒爆发过滤器。

配置警报设置和自动支持

如果存在需要用户干预的系统错误，则 Cisco AsyncOS 会通过邮件向用户发送警报消息。添加至少一个接收系统警报的邮件地址。多个地址之间用逗号分隔。您输入的邮件地址最初会接收所有级别的所有类型的警报，目录搜集攻击预防警报除外。之后您可以使用 CLI 中的 `alertconfig` 命令和 GUI 中的**系统管理 (System Administration) > 警报 (Alerts)** 页面进一步细化警报配置。有关详细信息，请参阅《思科安全邮件网关指南》的分发管理任务一章的警报一节。

自动支持功能使思科客户支持团队能够及时了解邮件网关的问题，以便思科可以为您提供行业领先的支持。回答“是”(Yes) 可发送思科支持警告和每周状态更新。有关详细信息，请参阅《思科安全邮件网关指南》的分发管理任务一章的自动支持一节。

配置计划报告

输入要接收默认计划报告的地址。您可以将此值留为空白，报告将在邮件网关上存档，而不是通过邮件发送。

配置时间设置

通过 Cisco AsyncOS，您可以使用网络时间协议 (NTP) 将时间与网络上的其他服务器或互联网同步，或者手动设置系统时钟。您还必须在邮件网关上设置时区，以便邮件信头和日志文件中的时间戳正确。您还可以使用思科系统时间服务器来同步邮件网关上的时间。

选择洲、国家/地区和时区以及是否使用 NTP（包括要使用的 NTP 服务器的名称）。

确认更改

最后，系统设置向导会要求您使用 `commit` 命令，提交在程序中所做的配置修改。如果您要提交更改，请回答“是”(Yes)。

在您成功完成系统设置向导后，系统将显示以下信息，并将显示命令提示符：

```
Congratulations! System setup is complete. For advanced configuration, please refer to the
 User Guide.

mail3.example.com>
```

邮件网关现已就绪，可以发送邮件。

测试配置

要测试思科 AsyncOS 配置，您可以使用 mailconfig 命令立即发送包含您刚通过 `systemsetup` 命令创建的系统配置数据的测试邮件：

```
mail3.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


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

mail3.example.com>
```

将配置发送到您有权访问的邮箱，以确认系统能够在您的网络中发送邮件。

即时警报

邮件网关使用功能没要启用功能。第一次使用 `systemsetup` 命令创建侦听程序、启用反垃圾邮件、启用 Sophos 或 McAfee 防病毒或启用病毒爆发过滤器时，系统会生成警报并发送至您在第 2 步：系统, on page 18中指定的地址。

警报会定期通知您密钥的剩余时间。例如：

```
Your "Receiving" key will expire in under 30 day(s).
Please contact IronPort Customer Support.


Your "Sophos" key will expire in under 30 day(s).
Please contact IronPort Customer Support.


Your "Outbreak Filters" key will expire in under 30 day(s).
Please contact IronPort Customer Support.
```

有关在30天试用期过后如何启用该功能的信息，请与思科销售代表联系。可以通过**系统管理 (System Administration) > 功能密钥 (Feature Keys)** 页面或发出 `featurekey` 命令来查看密钥的剩余时间。（有关详细信息，请参阅功能密钥。）

将系统配置为企业网关

要将系统配置为企业网关（接受来自互联网的邮件），请先完成本章，然后参阅配置网关以接收邮件了解更多信息。

验证您的配置和后续步骤

系统设置完成后，您的邮件网关应该可以发送和接收邮件。如果您已启用防病毒、反垃圾邮件和病毒爆发过滤器安全功能，系统还将扫描传入和传出邮件，以查找是否存在垃圾邮件和病毒。

下一步是了解如何自定义邮件网关的配置。了解邮件通道提供了有关如何通过系统路由邮件的详细概述。每项功能会按顺序处理（从上到下），会在本指南的剩余章节中介绍。