



## 快速入门指南



# Cisco S380 和 Cisco S680 网络安全设备

- 1 欢迎
- 2 准备工作
- 3 记录网络设置
- 4 规划安装
- 5 在机架中安装设备
- 6 插入设备
- 7 暂时更改 IP 地址
- 8 连接至设备
- 9 开启设备电源
- 10 登录设备
- 11 运行“系统安装向导”
- 12 配置网络设置
- 13 配置摘要
- 14 大功告成！
- 15 接下来可以做的事情

部件号：78-21150-01

# 1 欢迎

感谢您选择 Cisco S380 和 Cisco S680 网络安全设备（Cisco S380 和 Cisco S680）。网络安全设备可保护企业安全并控制网络流量。

本指南描述如何实际安装 S380 和 S680 设备及如何使用“系统安装向导”为设备配置基本设置。还可参阅 *Cisco IronPort AsyncOS for Web User Guide*（*Cisco IronPort AsyncOS for Web 用户指南*）中的“部署” (Deployment) 一章以了解有关配置设备设置的信息。

## 2 准备工作

开始安装之前，确保您具有所需物品。Cisco S380 和 Cisco S680 网络安全设备附带以下物品：

- 快速入门指南（本指南）
- 滑轨套件
- 电源线（2 条）
- 用于将设备连接至网络的以太网电缆
- 用于将计算机连接至控制台端口的 RJ45 转 DB9 电缆
- 思科内容安全文档指针卡



### 注意

---

Cisco S680 设备上的锁定面板版本附带了两个锁定密钥。请保存好这些密钥，因为丢失密钥时您需要 4 位数字密钥代码进行更换。

---

您自己需要提供以下物品：

- 机架机柜外壳（如果以机架方式安装该设备）
- 10/100/1000 Base-TX TCP/IP LAN
- 台式计算机或笔记本电脑
- 网络浏览器（或 SSH 和终端软件）
- [第 4 页上的“记录网络设置”一节](#)的网络和管理员信息

## 3 记录网络设置

开始之前，请写下有关您的网络和管理员设置的以下信息。

| 部署选项                                                                                                             |                                                                                               |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Web 代理： <ul style="list-style-type: none"><li>带第 4 层交换机的透明代理</li><li>带 WCCP 路由器的交换机透明代理</li><li>显式转发代理</li></ul> | 第 4 层流量监测器： <ul style="list-style-type: none"><li>单工接头/SPAN 端口</li><li>双工接头/SPAN 端口</li></ul> |
| 网络上下文                                                                                                            |                                                                                               |
| 网络上是否有另一代理：                                                                                                      | 是                                                                                             |
| 其他代理的 IP 地址：                                                                                                     |                                                                                               |
| 其他代理的端口：                                                                                                         |                                                                                               |
| 网络配置                                                                                                             |                                                                                               |
| 默认系统主机名：                                                                                                         |                                                                                               |
| DNS 服务器：                                                                                                         | 使用互联网根 DNS 服务器。<br>使用 DNS 服务器（最多 3 台）：<br>1.<br>2.<br>3.                                      |
| 网络时间协议 (NTP) 服务器：                                                                                                |                                                                                               |
| 时区 - 区域：                                                                                                         |                                                                                               |
| 时区 - 国家/地区：                                                                                                      |                                                                                               |
| 时区 - GMT 时差：                                                                                                     |                                                                                               |

| 界面设置                                                                                                                                               |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>管理端口</b>                                                                                                                                        |  |
| IP 地址:                                                                                                                                             |  |
| 网络掩码:                                                                                                                                              |  |
| 主机名:                                                                                                                                               |  |
| <b>数据端口（可选，请参阅“注释”）</b>                                                                                                                            |  |
| IP 地址:                                                                                                                                             |  |
| 网络掩码:                                                                                                                                              |  |
| 主机名:                                                                                                                                               |  |
|  <b>注意</b> Web 代理可以共享管理界面。如果单独配置，那么数据界面 IP 地址和管理界面 IP 地址不能共享同一子网。 |  |
| 路由                                                                                                                                                 |  |
| <b>用于管理的内部路由</b>                                                                                                                                   |  |
| 默认网关:                                                                                                                                              |  |
| 静态路由名称:                                                                                                                                            |  |
| 静态路由目标网络:                                                                                                                                          |  |
| 静态路由网关:                                                                                                                                            |  |
| <b>用于数据的内部路由</b>                                                                                                                                   |  |
| 默认网关:                                                                                                                                              |  |
| 静态路由名称:                                                                                                                                            |  |
| 静态路由目标网络:                                                                                                                                          |  |
| 静态路由网关:                                                                                                                                            |  |

## 透明路由设备

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 设备类型： | <ul style="list-style-type: none"> <li>第 4 层交换机或无设备</li> <li>WCCP 路由器                             <ul style="list-style-type: none"> <li>启用标准服务 ID（网络高速缓存）。                                     <ul style="list-style-type: none"> <li>路由器地址：                                             <div></div> </li> </ul> </li> <li>启用路由器安全性。                                     <ul style="list-style-type: none"> <li>密码：                                             <div></div> </li> </ul> </li> </ul> </li> </ul> |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



**注意** 将设备连接到 WCCP 路由器时，您可能需要配置网络安全设备，以在运行系统设置向导后创建 WCCP 服务。

## 管理设置

|                  |                                                                     |
|------------------|---------------------------------------------------------------------|
| 管理员密码：           |                                                                     |
| 通过邮件将系统告警发送至：    |                                                                     |
| SMTP 中继主机：       | （可选）                                                                |
| 自动支持：            | 启用                                                                  |
| SenderBase 网络参与： | 启用 <ul style="list-style-type: none"> <li>有限</li> <li>标准</li> </ul> |

| 安全服务                      |                                                                                                          |
|---------------------------|----------------------------------------------------------------------------------------------------------|
| L4 流量监视器：                 | <ul style="list-style-type: none"> <li>• 仅监测</li> <li>• 拦截</li> </ul>                                    |
| 可接受使用控制：                  | 启用 <ul style="list-style-type: none"> <li>• Cisco IronPort 网络使用控制</li> </ul>                             |
| 网络信誉过滤器：                  | 启用                                                                                                       |
| 恶意软件和间谍软件扫描：              | <ul style="list-style-type: none"> <li>• 启用 Webroot</li> <li>• 启用 McAfee</li> <li>• 启用 Sophos</li> </ul> |
| 针对检测到的恶意软件采取的措施：          | <ul style="list-style-type: none"> <li>• 仅监测</li> <li>• 拦截</li> </ul>                                    |
| IronPort 数据安全过滤：          | 启用                                                                                                       |
| 锁定面板                      |                                                                                                          |
| 4 位代码（适用于 S680 - LKFP 设备） |                                                                                                          |

## 4 规划安装

决定如何在网络中配置 Cisco S380 和 Cisco S680 网络安全设备。

Cisco S380 和 Cisco S680 通常安装为网络中的客户端与互联网之间的附加层。您部署设备的方式决定了您是否需要第 4 层 (L4) 交换机或 WCCP 路由器将客户端流量传送至设备。

部署选项包括：

- 透明代理 - 带 L4 交换机的 Web 代理
- 透明代理 - 带 WCCP 路由器的 Web 代理
- 显式转发代理 - 连接至网络交换机
- 第 4 层流量监测器 - 以太网接头（单工或双工）
  - 单工模式：端口 T1 接收所有传出流量，端口 T2 接收所有传入流量。
  - 双工模式：端口 T1 接收所有传入和传出流量。



### 注意

---

要监测真正的客户端 IP 地址，第 4 层流量监测器应始终配置在防火墙内部及 NAT（网络地址转换）之前。

---

## 5 在机架中安装设备

使用所提供的滑轨安装 Cisco S380 和 Cisco S680 网络安全设备。有关在机架中安装设备的信息，请参阅 *Cisco 380 and Cisco 680 Series Hardware Installation Guide*（Cisco 380 和 Cisco 680 系列硬件安装指南）。

### 设备放置

- 环境温度 - 为防止设备过热，请勿在环境温度超过 104°F (40°C) 的区域操作设备。
- 气流 - 确保设备周围有足够的气流。
- 机械负荷 - 确保设备保持平稳，以避免出现任何危险情况。



## 6 插入设备

将每条直电源线的插口端插入设备后面板上的冗余电源。  
将插头端插入电源插座。



## 7 暂时更改 IP 地址

要连接至 Cisco S380 和 Cisco S680，必须暂时更改计算机的 IP 地址。



### 注意

---

请记住当前 IP 配置设置，因为您在完成配置后需要恢复为这些设置。

---

### 对于 Windows

---

**步骤 1** 使用系统箱中包括的以太网电缆将笔记本电脑连接至管理端口。Cisco S380 和 Cisco S680 设备仅使用管理端口。请参阅第 8 页上的“规划安装”一节。

**步骤 2** 转至“开始”菜单并选择**控制面板**。

**步骤 3** 双击**网络和共享中心**。

**步骤 4** 点击**本地连接**，然后点击**属性**。

**步骤 5** 选择 **Internet 协议 (TCP/IP)**，然后点击**属性**。

**步骤 6** 选择**使用下面的 IP 地址**。

**步骤 7** 输入以下更改：

- IP 地址：192.168.42.43
- 子网掩码：255.255.255.0
- 默认网关：192.168.42.1

**步骤 8** 点击**确定**，然后点击**关闭**以退出对话框。

---

## 对于 MAC

---

- 步骤 1** 启动 Apple 菜单并选择**系统预置**。
- 步骤 2** 点击**网络**。
- 步骤 3** 点击锁定图标以允许更改。
- 步骤 4** 选择带有绿色图标的以太网网络配置。这是您的活动连接。然后点击**高级**。
- 步骤 5** 点击 TCP/IP 选项卡，然后在以太网设置的下拉列表中选择**手动**。
- 步骤 6** 输入以下更改：
- IP 地址：**192.168.42.43**
  - 子网掩码：**255.255.255.0**
  - 路由器：**192.168.42.1**
- 步骤 7** 点击**确定**。
-

## 8 连接至设备

将以太网电缆连接至 Cisco S380 和 Cisco S680 设备后面板上的相应端口。

- 代理端口标签为 P1 和 P2。
  - 仅启用 P1: 如果仅启用了 P1, 那么必须将 P1 连接至网络以用于传入和传出流量。
  - 启用 P1 和 P2: 如果同时启用了 P1 和 P2, 那么必须将 P1 连接至内部网络, 将 P2 连接至互联网。
- 流量监测器端口标签为 T1 和 T2。
  - 单工接头: 端口 T1 和 T2 ; 一条电缆 (T1) 用于发往互联网的所有数据包, 一条电缆 (T2) 用于来自互联网的所有数据包。
  - 双工接头: 端口 T1; 一条电缆用于所有传入和传出流量。



| 项 | 端口 | 说明                                                                                       |
|---|----|------------------------------------------------------------------------------------------|
| 1 | P1 | 表示代理端口。将 P1 连接至网络以用于所有传入和传出流量。                                                           |
| 2 | P2 | 表示代理端口。如果同时启用了 P1 和 P2，那么必须将 P1 连接至内部网络，将 P2 连接至互联网。P1 和 P2 可以连接至 L4 交换机、WCCP 路由器或网络交换机。 |
| 3 | T1 | 表示双工以太网接头的流量监测器端口<br>T1：一条电缆用于所有传入和传出流量。                                                 |
| 4 | T2 | 表示流量监测器端口。单工以太网接头：端口 T1 和 T2。一条电缆 (T1) 用于发往互联网的所有数据包，一条电缆 (T2) 用于来自互联网的所有数据包。            |



#### 注意

如果随设备订购了网络接口卡 (NIC)，请参阅 *Cisco 380 and Cisco 680 Series Hardware Installation Guide*（Cisco 380 和 Cisco 680 系列硬件安装指南）中的“PCI NIC Slot Configurations”（PCI NIC 插槽配置）一节中的详细信息。

## 9 开启设备电源

按 Cisco S380 和 Cisco S680 前面板上的开关接通设备电源。每次接通系统电源时，必须等待五分钟以便系统初始化。机器接通电源后，绿灯常亮表示设备正在运行。



### 注意

---

如果设备连接电源后快速开启，那么设备会接通电源，并且风扇会旋转，LED 会亮起。在 30 到 60 秒的时间内，风扇会停止，所有 LED 会熄灭。设备在 31 秒后通电。此行为旨在使系统固件和控制器同步。

---

# 10 登录设备

可使用两个界面登录 Cisco S380 和 Cisco S680：基于网络的界面或命令行界面。

## 基于网络的界面

---

**步骤 1** 要通过以太网端口进行网络浏览器访问（请参阅第 13 页上的“连接至设备”一节），请在网络浏览器中输入以下 URL 以访问设备管理界面：  
`http://192.168.42.42:8080`



**步骤 2** 输入以下登录信息：

- 用户名：admin
- 密码：ironport



**注意** 主机名参数是在设置系统时分配的。使用主机名 (`http://hostname:8080`) 连接至管理界面之前，必须将设备主机名和 IP 地址添加至 DNS 服务器数据库。

---

**步骤 3** 点击**登录**。

---

## 命令行界面

---

- 步骤 1** 要通过串行端口进行命令行界面访问（请参阅[第 13 页上的“连接至设备”一节](#)），请使用 9600 位、8 位、无奇偶校验和 1 个停止位 (9600, 8, N, 1) 和 “Hardware” 流量控制设置来访问命令行界面终端仿真程序。
- 步骤 2** 启动与 IP 地址 192.168.42.42 的 telnet 或 SSH 会话。
- 步骤 3** 以 admin 身份登录并使用密码 ironport。
- 步骤 4** 在提示符下，运行 systemsetup 命令。
-

# 11 运行“系统安装向导”

运行“系统安装向导”以配置基本设置并启用一组系统默认值。当您通过基于网络的界面访问设备（或从命令行界面运行 **systemsetup** 命令）时，“系统安装向导”自动启动并显示最终用户许可协议（又称为 EULA）。

---

**步骤 1** 启动“系统安装向导”。

**步骤 2** 接受最终用户许可协议。

**步骤 3** 输入注册信息。

**步骤 4** 输入第 4 页上的“记录网络设置”一节中的信息。

**步骤 5** 设置网络安全设置。

**步骤 6** 检查配置摘要页面。

**步骤 7** 使用用户名 **admin** 和您在“系统安装向导”中设置的新密码登录设备。

Cisco S380 和 Cisco S680 网络安全设备使用自签名证书，此证书可能会导致网络浏览器发出警告。您可以直接接受证书并忽略此警告。

**步骤 8** 写下新的管理员密码并将其保存在安全的位置。

---

## 12 配置网络设置

根据网络配置，可能需要将防火墙配置为允许使用以下端口进行访问。SMTP 和 DNS 服务必须能够访问互联网。

网络安全设备必须能够侦听以下端口：

- FTP：端口 21，数据 TCP 端口 1024 及更高端口号
- HTTP：端口 80
- HTTPS：端口 443
- 管理访问端口：8443 (HTTPS) 和 8080 (HTTP)
- SSH：端口 22

网络安全设备必须能够在以下端口上建立出站连接：

- DNS：端口 53
- FTP：端口 21，数据 TCP 端口 1024 及更高端口号
- HTTP：端口 80
- HTTPS：端口 443
- LDAP：端口 389 或 3268
- 基于 SSL 的 LDAP：端口 636
- 基于 SSL 的 LDAP（用于全局目录查询）：端口 3269
- NTP：端口 123
- SMTP：端口 25



### 注意

---

如果未打开端口 80 和 443，那么无法下载功能密钥。

---

## 13 配置摘要

| 项  | 说明                                                                                                                                                                                                                                                                                         |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理 | <p>在完成“系统安装向导”后，可通过以下方法从管理端口对网络安全设备进行管理：输入 <code>http://192.168.42.42:8080</code> 或使用分配给管理界面的 IP 地址。</p> <p>如果将配置重置为出厂默认设置（例如通过重新运行“系统安装向导”），那么您只能通过管理端口 (<code>http://192.168.42.42:8080</code>) 访问管理界面，因此请确保可连接至管理端口。</p> <p>此外，请确认您已在管理界面上打开防火墙端口 80 和 443。</p>                         |
| 数据 | <p>运行“系统安装向导”后，设备上的至少一个端口配置为接收来自网络上的客户端的网络流量：仅 M1；M1 和 P1；M1、P1 和 P2；仅 P1；或 P1 和 P2。</p> <div><b>注意</b><p>如果您已按显式转发模式配置了 Web 代理，则客户端机器上的应用必须配置成使用为数据配置的 IP 地址（M1 或 P1）将网络流量显式转发至网络安全设备的 Web 代理。</p></div> |

| 项     | 说明                                                                                                                                                                                                                                                                    |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 流量监测器 | 运行“系统安装向导”后，一个或两个第 4 层流量监测器端口（仅 T1 或 T1 和 T2）配置为侦听所有 TCP 端口上的流量。第 4 层流量监测器的默认设置为仅监测。在安装期间或之后，可将第 4 层流量监测器配置为监测并拦截可疑流量。                                                                                                                                                |
| 计算机地址 | <p>请记得将计算机 IP 地址改回您在第 11 页上的“暂时更改 IP 地址”一节中记下的原始设置。</p> <div>  <div> <b>注意</b> 可在<b>系统管理 &gt; 配置摘要 (System Administration &gt; Configuration Summary)</b> 页面中检查系统设置摘要。 </div> </div> |

## 14 大功告成！

祝贺您！您现在已准备好开始使用 Cisco S380 和 Cisco S680 网络安全设备。您可能希望考虑执行下列某些步骤以便更好地利用设备：

### 用户策略

使用网络界面以根据需要创建一些策略，定义哪些用户可访问哪些网络资源。

- 标识用户 - 请选择**网络安全管理器 > 身份 (Web Security Manager > Identities)**，定义可访问互联网的用户组。
- 定义访问策略 - 请选择**网络安全管理器 > 访问策略 (Web Security Manager > Access Policies)**，通过配置要允许或阻止的对象和应用、要监视或阻止的 URL 类别以及网络信誉和反恶意软件设置来控制用户对互联网的访问。

您还可以定义多种其他策略类型，通过控制对互联网的访问来实施贵公司的可接受使用策略。例如，您可以定义用于解密 HTTPS 事务的策略及用于控制上传请求的其他策略。

有关在 Cisco S380 和 Cisco S680 设备上配置策略的信息，请参阅 *Cisco IronPort AsyncOS for Web User Guide*（*Cisco IronPort AsyncOS for Web 用户指南*）中的“Working with Policies”（使用策略）一章。

## 报告

通过查看网络界面中提供的报告，您可以了解有关网络上已阻止和已监测的网络流量的统计信息。还可查看有关被阻止的前若干种 URL 类别、客户端活动、系统状态及其他信息的报告。

## 更多信息

您可能还想为 Cisco S380 和 Cisco S680 设备配置其他功能。有关配置功能密钥、最终用户通知和日志记录的更多信息，以及有关其他可用网络安全设备功能的详细信息，请参阅 Cisco S380 和 Cisco S680 网络安全设备文档。

## 15 接下来可以做的事情

| 支持                                                                                                                              |                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 思科支持门户                                                                                                                          | <a href="http://www.cisco.com/support">http://www.cisco.com/support</a>                                                                                                                                                                                           |
| 美国和加拿大免费电话                                                                                                                      | 800-553-2447                                                                                                                                                                                                                                                      |
| 国际联系信息                                                                                                                          | 全球电话号码                                                                                                                                                                                                                                                            |
| 邮件:                                                                                                                             | <a href="mailto:tac@cisco.com">tac@cisco.com</a>                                                                                                                                                                                                                  |
| 思科网络安全设备支持社区                                                                                                                    | <a href="https://supportforums.cisco.com/community/netpro/security/web">https://supportforums.cisco.com/community/netpro/security/web</a>                                                                                                                         |
| 产品文档                                                                                                                            |                                                                                                                                                                                                                                                                   |
| <i>Cisco S380 和 Cisco S680 网络安全设备快速入门指南</i> （本文档）                                                                               | <a href="http://www.cisco.com/en/US/docs/security/wsa/hw/S380_S680_QSG_78_21150.pdf">http://www.cisco.com/en/US/docs/security/wsa/hw/S380_S680_QSG_78_21150.pdf</a>                                                                                               |
| <i>Cisco 380 and Cisco 680 Series Hardware Installation Guide</i><br>(Cisco 380 和 Cisco 680 系列硬件安装指南)<br>包含有关 LED、技术规格和安全选项的信息。 | <a href="http://www.cisco.com/en/US/docs/security/esa/hw/380_680_Series_HW_Install.pdf">http://www.cisco.com/en/US/docs/security/esa/hw/380_680_Series_HW_Install.pdf</a>                                                                                         |
| 思科网络安全设备文档<br>包含有关配置设备功能、CLI 命令和版本说明的文档。                                                                                        | <a href="http://www.cisco.com/en/US/customer/products/ps10164/tsd_products_support_series_home.html">http://www.cisco.com/en/US/customer/products/ps10164/tsd_products_support_series_home.html</a>                                                               |
| “Safety and Compliance Guide”<br>(安全和合规性指南)                                                                                     | <a href="http://www.cisco.com/en/US/docs/security/content_security/compliance/ContentSecurity_regulatory_compliance_information.fm">http://www.cisco.com/en/US/docs/security/content_security/compliance/ContentSecurity_regulatory_compliance_information.fm</a> |
| MIB                                                                                                                             |                                                                                                                                                                                                                                                                   |
| 思科网络安全设备的 AsyncOS MIB<br>(“Related Tools”<br>(相关工具) 部分)                                                                         | <a href="http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html</a>                                                                                 |

# 获取文档和提交服务请求

有关获取文档、提交服务请求和收集更多信息的相关内容，请参阅 *思科产品文档更新*，网址为：

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>。

通过 RSS 源的方式订阅 *思科产品文档更新*（其中列出所有新的和修订过的思科技术文档），并将相关内容通过阅读器应用直接发送至您的桌面。RSS 源是一种免费服务。

---

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此 URL：[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

本文档中使用的任何 Internet 协议 (IP) 地址都不是有意使用的真实地址。本文档中所含的任何示例、命令显示输出和图形仅供说明之用。说明内容中用到的任何真实 IP 地址都纯属巧合，并非有意使用。

© 2013 思科系统公司。版权所有。









---

**美洲总部**

思科系统公司  
加州圣荷西

**亚太总部**

Cisco Systems (USA) Pte.Ltd.  
新加坡

**欧洲总部**

Cisco Systems International BV  
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站 [www.cisco.com/go/offices](http://www.cisco.com/go/offices) 上列有各办事处的地址、电话和传真号码。

---

本文档使用含 10% 用后废料的再生纸在美国印制出版。

部件号: 78-21150-01