合规名单

以下主题介绍如何在将合规 allow 名单添加到关联策略之前对其进行配置。

合规 允许 名单简介

合规 *allow* 名单，有时缩写为 an *allow* 名单，是指定允许在网络上的主机上运行的操作系统、应用（Web 和客户端）以及协议的一系列标准。如果主机不在名单，系统也会生成一个事件（违反）。

合规 allow 名单有两个主要组件：

- 目标 是您选择用于合规评估的主机。您可以评估所有或部分受监控的主机，按照子网、VLAN 和主机属性进行限制。在多域部署中，您可以将域以及域内或跨域的子网作为目标。
- 主机配置文件指定面向目标的合规标准。全局主机配置文件与操作系统无关。您也可以配置操作系统特定的主机配置文件，主机配置文件为一个 allow 名单独有或跨 allow 名单共享。

Talos 情报小组 提供配有建议设置的默认 allow 名单。您也可以创建自定义 allow 名单。简单的自定义名单可能只允许主机运行某一操作系统。较复杂的名单可能允许所有操作系统，但指定主机在特定端口上运行某一应用协议必须使用的操作系统。

注释 系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异。 此限制可能会影响创建合规 allow 名单的方式。

实施合规 允许 名单

要实施allow名单，请将该名单添加到活动关联策略。系统评估目标并给每个主机分配对应的属性：

- 合规 - 主机没有违反名单。
- 不合规 - 主机违反名单。
- 未评估 - 主机不是名单的目标，主机现在正在接受评估，或者系统没有足够的信息来确定主机是否合规。

注释 要删除主机属性，请删除其对应的 allow 名单。停用、删除或删除关联策略中的 an allow 名单**不** 会删除主机属性，也不会更改每个主机的属性值。

完成初始评估后，当受监控的主机不再符合活动 allow 名单时，系统会生成 an *allow* 名单事件；它会还记录 an *allow* 名单违规。

您可以使用工作流程、控制面板以及网络映射来监控整个系统的合规活动，并确定个别主机何时、以何种方式违反了您的 allow 名单。您也可以通过补救和警报自动对如违规做出响应。

示例：将 HTTP 限制为 Web 服务器

您的安全策略规定只有 Web 服务器可以运行 HTTP。您可以创建一份评估整个网络（不包括 Web 场）的 an allow 名单，以确定哪些主机正在运行 HTTP。

通过使用网络映射和控制面板，您可以获取您的网络合规性的概览摘要。只需几秒钟，便可以确定组织内的哪些主机违反了策略正在运行 HTTP，并采取相应的行动。

然后，使用关联功能配置系统，使系统在 Web 场之外的主机开始运行 HTTP 时发出警报。

相关主题

配置关联策略

合规 允许 名单目标网络

目标网络 指定要用于合规性评估的主机。An allow 名单可具有多个目标网络，并且会评估与其任何目标的条件相符的主机。

最初，您可通过 IP 地址或范围限制目标网络。在多域部署中，初始限制还包括一个域。

系统提供的默认 allow 名单针对所有受监控主机：0.0.0.0/0 和 ::/0。在多域部署中，默认 allow 名单限用于（且仅适用于）全局域。

如果修改目标网络或主机，致使该主机不再是 allow 名单的有效目标，则该主机不再通过名单进行评估，并且既不视为合规，也不视为不合规。

调查和优化目标网络

将目标网络添加到 an allow 名单中时，系统会提示您调查网络映射以帮助确定合规主机的特征。调查会将目标添加到表示已调查的主机的 allow 名单中。

您可以调查子网或单个主机。在多域部署中，您可以调查整个域，也可以跨域调查。调查祖先域会导致系统调查该域的后代。

除已添加的目标之外，调查还会对在该调查中检测到的每个操作系统都使用一个主机配置文件填充 allow 名单。这些主机配置文件允许系统在适用操作系统上检测到的所有客户端、应用协议、Web 应用和协议。

在调查目标网络（或跳过调查）后，请优化目标。您可以按 IP 地址排除主机，或者按主机属性或 VLAN 限制目标网络。

使用合规 允许 名单设定目标域

在多域部署中，域和目标网络紧密相连。

- 枝叶域管理员可以创建对其枝叶域内的主机进行评估的 allow 名单。
- 更高级别的域管理员可以创建跨域评估主机的 allow 名单。您可以在同一个 allow 名单中以不同域中的不同子网作为目标。

假设您是全局域管理员，并且要将同一合规性标准应用于整个部署中的 Web 服务器。您可以在全局域中创建用于定义合规性标准的 allow 名单。然后，使用指定各枝叶域中 Web 服务器的 IP 空间（或单个 IP 地址）的目标网络来限制 allow 名单。

注释 除将枝叶域中的IP地址和范围设定为目标之外，您还可以使用更高级别的域来限制目标网络。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字IP地址限制此配置可能会出现意外结果。

合规 允许 名单主机配置文件

在合规 allow 名单中，主机配置文件指定允许在目标主机上运行的操作系统、客户端、应用协议、Web 应用和协议。有三种类型的主机配置文件可在合规 allow 名单中使用；每个类型在合规名单编辑器中以不同方式显示。

表 *1:* 合规 允许 名单主机配置文件类型

主机配置文件类型	外观	说明
全局	任何操作系统	指定允许在目标主机上运行的内容，而不考虑操作系统
特定于操作系统	以纯文本列示	指定允许在特定操作系统的目标主机上运行的内容
共享	以斜体形式列示	指定可以在多个 allow 名单中使用的操作系统条件

操作系统特定主机配置文件

在合规 allow 名单中， 特定操作系统主机配置文件 不仅指定了允许在网络上运行的操作系统，还指定了允许在这些操作系统上运行的应用协议、客户端、Web 应用及通信协议。

例如，可以要求合规主机运行特定版本的 Microsoft Windows。再例如，可以允许 SSH 于端口 22 在 Linux 主机上运行，并进一步限制 SSH 客户端的供应商和版本。

请为允许在网络上运行的各个操作系统创建一个主机配置文件。要禁止网络上的某个操作系统，则不要创建该操作系统的主机配置文件。例如，为了确保网络上的所有主机均运行 Windows，请将 allow 名单配置为只包含该操作系统的主机配置文件。

注释 未识别的主机在被识别之前，一直处于符合所有 allow 名单条件的状态。但是，可以为未知主机创建一份 an allow 名单主机配置文件。未识别的主机是指系统尚未收集足够的信息识别其操作系统的主机。未知主机是指其操作系统与已知指纹不匹配的主机。

共享主机配置文件

在合规 allow 名单中，共享主机配置文件绑定到特定操作系统，但是您可以在多个 allow 名单中使用每个共享主机配置文件。

例如，您可能在全球具有多个办事处，其中每个位置对应单独的 allow 名单，但是要对运行 Apple Mac OS X 的所有主机都使用同一配置文件。您可以为该操作系统创建共享配置文件，并将其用于所有 allow 名单中。

默认 allow 名单使用共享主机配置文件的一个特殊类别，即 内置主机配置文件。这些配置文件使用内置应用协议、Web 应用、协议和客户端。在合规 allow 名单编辑器中，系统使用 **内置主机配置文件图标**标记这些配置文件。

在多域部署中，系统会显示在当前域中创建的共享主机配置文件，您可以对其进行编辑。系统还会显示祖先域中的共享主机配置文件，您不可以对其进行编辑。要查看和编辑在较低域中创建的共享主机配置文件，请切换至该域。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个 allow 名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

允许 违规触发器

当系统出现以下情况时，主机的 allow 名单合规情况会发生变化：

- 检测到主机的操作系统发生变化
- 检测到主机的操作系统或主机上的应用协议存在身份冲突

- 检测到主机上有新的TCP服务器端口（例如，SMTP或网络服务器使用的端口）处于活动状态，或主机上有新的 UDP 服务器正在运行
- 检测到主机上运行的 TCP 或 UDP 服务器发生变化，例如由于升级导致版本发生变化
- 检测主机上有新的客户端或 Web 应用正在运行
- 从其数据库中丢弃不活动的客户端或 Web 应用
- 检测到主机正使用新的网络或传输协议进行通信
- 检测到新的破解移动设备
- 检测到主机上的某个 TCP 或 UDP 端口已关闭或超时

此外，您还可以使用主机输入功能或主机配置文件执行以下操作来触发主机合规性的改变：

- 向主机添加客户端、协议或服务器
- 从主机中删除客户端、协议或服务器
- 设置主机的操作系统定义
- 更改主机的主机属性，这样该主机便不再是一个有效目标

注释 为避免事件数量过多而使系统不堪重负，系统在初始评估时不会为违规主机生成 allow 名单事件，也不会对由于修改了有效 allow 名单或共享主机配置文件而导致违规的主机生成不合规名单事件。但是，仍会记录违规情况。如果要为所有违规目标生成 allow 名单事件，请清除发现数据。重新发现网络资产可能会触发 allow 名单事件。

操作系统合规性

如果 allow 名单指定只允许在网络上运行 Microsoft Windows 主机，但系统检测到主机正在运行 Mac OS X，则系统会生成 an allow 名单事件。此外，该主机与 allow 名单关联的主机属性从“合规”更改为“违规”。

要将本示例中主机的合规属性恢复为合规，必须发生下列任一情况：

- 您编辑 allow 名单，以允许 Mac OS X 操作系统的运行
- 您手动将主机的操作系统定义更改为 Microsoft Windows
- 系统检测到操作系统已更改回 Microsoft Windows

从网络映射中删除违规资产

如果 allow 名单禁止使用 FTP，并且您从应用协议网络映射或事件视图中删除了 FTP，则运行 FTP 的主机的属性变为合规。但如果系统再次检测到该应用协议，则会生成 an allow 名单事件，且该主机的属性变为违规。

仅对完整信息触发

如果 allow 名单仅在端口 21 上允许 TCP FTP 流量，且系统检测到端口 21/TCP 上存在不确定的活动，则 allow 名单不会触发。仅当系统将该流量识别为除 FTP 流量以外的其他流量，或者您使用主机输入功能将该流量指定为非 FTP 流量时， allow 名单才会触发。系统不会记录仅含部分信息的违规。

合规的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

创建合规 允许 名单

当创建合规 allow 名单时，系统会提示您调查网络，创建初始目标并帮助确定合规主机的特征。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 点击 **New允许列表**。

步骤 3 或者，输入初始目标网络的 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。在多域部署中，在**域 (Domain)** 中选择目标网络所在的域。

提示 要调查整个受监控网络，请使用默认值 0.0.0.0/0 和 ::/0。

注释　在为目标网络选择域之后，不能更改该域。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 添加目标网络：

- 添加 - 要添加目标网络而无需调查，请点击**添加 (Add)**。
- 添加并调查网络 - 要添加并调查目标网络，请点击**添加并调查网络 (Add and Survey Network)**。
- 跳过 - 要创建 an allow 名单而不调查网络，请点击 **跳过**。

步骤 5 或者，为 allow 名单输入新的 **名称** 和 **说明** 。

步骤 6 或者，在网络上**允许破解的移动设备 (Allow Jailbroken Mobile Devices)**。禁用此选项会导致破解设备生成 allow 名单违规。

步骤 7 向 allow 名单中至少添加一个 **目标网络** ，如 为合规 允许 名单创建目标网络 ， 第 8 页中所述。

步骤 8 使用**允许的主机配置文件 (Allowed Host Profiles)** 确定合规主机的特征：

- 全局主机配置文件 - 要编辑 allow 名单的全局主机配置文件，请点击 **任何操作系统** ，然后如 构建 允许 列表主机配置文件 ， 第 9 页中所述继续操作。
- 编辑已调查的配置文件 - 要编辑由网络调查创建的现有操作系统特定主机配置文件，请点击其名称，然后如构建 允许 列表主机配置文件 ， 第 9 页中所述继续操作。
- 创建新配置文件 - 要为此 allow 名单创建新的操作系统特定主机配置文件，请点击 **允许的主机配置文件**旁边的 **添加**（＋），然后如 构建 允许 列表主机配置文件 ， 第 9 页中所述继续操作。
- 添加共享主机配置文件 - 要向 allow 名单中添加现有共享主机配置文件，请点击 **添加共享主机配置文件**，选择要添加的共享主机配置文件，然后点击 **确定**。共享主机配置文件以斜体显示。

步骤 9 单击**保存 (Save)允许列表**。

下一步做什么

- 将 allow 名单添加到活动关联策略中，如配置关联策略中所述。系统立即开始评估 allow 名单并生成违规。

相关主题

合规 允许 名单目标网络 ， 第 2 页
根据所选主机创建合规 允许 名单
Firepower 系统 IP 地址约定

为合规 允许 名单创建目标网络

添加目标网络时，可以对其进行调查以确定合规主机的特征。此调查会对调查中检测到的每个操作系统都使用一个主机配置文件来填充 allow 名单。这些主机配置文件允许系统在适用操作系统上检测到的所有客户端、应用协议、Web 应用和协议。

过程

步骤 1 在合规 allow 名单编辑器中，点击 **添加目标网络**。

步骤 2 为目标网络输入 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。

步骤 3 在多域部署中，在**域 (Domain)** 中选择目标网络所在的域。

注释 在为目标网络选择域之后，不能更改该域。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 添加目标网络：

- 添加 - 要在不调查的情况下添加目标网络，请点击**添加 (Add)**。
- 添加并调查网络 - 要添加并调查目标网络，请点击**添加并调查网络 (Add and Survey Network)**。

步骤 5 或者，点击新目标以进一步对其进行配置：

- 名称 - 在**名称 (Name)** 中输入新名称。
- 添加网络 - 要以其他主机为目标，请点击 **添加**（+），然后输入 **IP 地址** 和 **网络掩码**。要从 allow 名单合规性中排除网络，请选择 **排除**。
- 添加主机属性 - 要以具有特定主机属性的主机为目标，请点击 **添加**（+），然后指定 **属性** 及其 **值** 。
- 添加 VLAN - 要以 VLAN 为目标，请点击 **添加**（+），然后键入 VLAN 编号（对于 802.1q VLAN）。
- 删除 - 要删除目标限制，请点击 **删除**（🗑）。

步骤 6 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

相关主题

合规 允许 名单目标网络 ，第 2 页

Firepower 系统 IP 地址约定

构建 允许 列表主机配置文件

主机配置文件 指定 allow 名单的合规性标准，即允许在目标主机上运行的操作系统、客户端、应用协议、Web 应用和协议。

每个allow名单都有一个与操作系统无关的全局主机配置文件。例如，无需编辑多个Microsoft Windows和Linux主机配置文件以允许Mozilla Firefox，可以将全局主机配置文件配置为允许Firefox，无论检测到该主机使用的是什么操作系统。

您也可以配置操作系统特定的主机配置文件，主机配置文件为一个 allow 名单独有或跨 allow 名单共享。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个 allow 名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

开始之前

- 如 编辑合规 允许 名单，第 13 页中所述在 an allow名单内创建或编辑主机配置文件，或者如 管理共享主机配置文件，第 14 页中所述创建或编辑共享主机配置文件。

过程

步骤 1 在合规 allow 名单主机配置文件编辑器中，配置主机配置文件：

- 名称 - 输入**名称 (Name)**。
- 操作系统 - 要将主机配置文件限制为特定的操作系统，请使用**操作系统供应商 (OS Vendor)**、**操作系统名称 (OS Name)** 和**版本 (Version)** 下拉列表。由于其目的是应用到运行任何操作系统的主机，因此无法限制全局主机配置文件。
- 应用协议 - 要允许应用协议，请点击 **添加**（+），并如 将应用协议添加到合规 允许 列表，第 10 页中所述继续操作。
- 客户端 - 要允许客户端，请点击 **添加**（+），并如 将客户端添加到合规 允许 列表，第 10 页中所述继续操作。
- Web 应用 - 要允许 Web 应用，请点击 **添加**（+），并如 将 Web 应用添加到合规 允许 列表，第 11 页中所述继续操作。
- 协议 - 要允许协议，请点击 **添加**（+），并如 将协议添加到合规 允许 列表，第 11 页中所述继续操作。
- 删除 - 要禁止之前允许的项目，请点击 **删除**（🗑）。

- 编辑属性 - 要编辑允许的应用协议、客户端或协议的属性，请点击其名称。进行的更改反映在使用该元素的所有主机配置文件中。

提示　选中相应的**全部允许...(Allow all...)**复选框，以允许与此配置文件匹配的主机的所有应用协议、客户端或 Web 应用。

步骤 2 要立即实施自上次保存后进行的所有更改，请点击**保存允许列表**（或如果您编辑的是共享主机配置文件，则点击 **保存所有配置文件** ）。

将应用协议添加到合规 允许 列表

使用 allow 名单主机配置文件，您可以在全局范围或在特定操作系统上将应用协议允许。或者，可以按端口、供应商或版本限制应用协议。例如，可以允许特定版本的SSH在Linux主机的端口22/TCP上运行。

过程

步骤 1 创建或修改合规 allow 列表主机配置文件时，点击 **允许的应用协议** 旁边的 **添加**（＋）（或者，如果修改的是全局主机配置文件，则点击 **全局允许的应用协议** 旁边的添加图标）。

步骤 2 此时您有两种选择：

- 如果列出了要允许的应用协议，请选择这些协议。Web 界面列出 allow 名单已允许或当前允许的应用协议。
- 要允许列表中未包含的应用协议，请选择**<新应用协议> (<New Application Protocol>)**，然后点击**确定 (OK)** 显示应用协议编辑器。选择要允许的应用协议**类型 (Type)** 和**协议 (Protocol)**。或者，按**端口 (port)**、**供应商 (Vendor)** 和**版本 (Version)** 限制应用协议。

  注释　必须完全按照供应商和版本在应用的表视图中的显示键入该供应商和版本。如果不指定供应商或版本，则只要类型与协议匹配， allow 名单便允许所有供应商和版本。

步骤 3 点击**确定**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

将客户端添加到合规 允许 列表

使用 allow 名单主机配置文件时，可以在全局或在特定操作系统上将客户端允许。或者，要求客户端的特定版本。例如，可以只允许 Microsoft Internet Explorer 10 在 Microsoft Windows 主机上运行。

过程

步骤 1 创建或修改合规 allow 名单主机配置文件时，点击 **允许的客户端** 旁边的 **添加**（＋） 或者，如果修改的是全局主机配置文件，则点击 **全局允许的客户端** 旁边的图标）。

步骤 2 此时您有两种选择：

- 如果要允许的客户端已列出，请选择这些客户端。Web 界面列出已被 allow 名单允许或当前允许的客户端。
- 要允许不在列表中的客户端，请选择**<新建客户端> (<New Client>)** 并点击**确定 (OK)** 以显示客户端编辑器。从下拉列表中选择要允许的**客户端 (Client)**，或者将客户端限制为允许的**版本 (Version)**。

  注释　必须准确地输入版本，因为它会显示在客户端表视图中。如果不指定版本，则允许所有版本。

步骤 3 点击**确定**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

将 Web 应用添加到合规 允许 列表

使用 allow 名单主机配置文件，您可以在全局范围或在特定操作系统上将 web 应用允许。

过程

步骤 1 创建或修改合规 allow 名单主机配置文件时，点击 **允许的 Web 应用** 旁边的 **添加**（＋） （或者，如果修改的是全局主机配置文件，则点击 **全局允许的 Web 应用** 旁边的图标）。

步骤 2 选择要允许的 Web 应用。

步骤 3 点击 **OK**

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

将协议添加到合规 允许 列表

使用 allow 名单主机配置文件，您可以在全局范围或在特定操作系统上将协议允许。始终允许在任何主机上运行 ARP、IP、TCP 和 UDP；不能禁用这些协议。

过程

步骤 1 创建或修改合规 allow 列表主机配置文件时，点击 **允许的协议** 旁边的 **添加**（＋） （或者，如果修改的是全局主机配置文件，则点击 **全局允许的协议** 旁边的添加图标）。

步骤 2 此时您有两种选择：

- 如果列出了要允许的协议，请选择这些协议。Web 界面列出 allow 名单已允许或当前允许的协议。
- 要允许列表中未包含的协议，请选择**<新协议> (<New Protocol>)**，然后点击**确定 (OK)** 显示协议编辑器。从**类型 (Type)** 下拉列表中，选择协议类型（**网络 [Network]** 或**传输 [Transfer]**），然后从下拉列表中选择**协议 (Protocol)**。

  提示 选择 **Other (manual entry)** 以指定不在列表中的通信协议。对于网络协议，请键入 http://www.iana.org/assignments/ethernet-numbers/ 中所列的相应编号。对于传输协议，请键入 http://www.iana.org/assignments/protocol-numbers/ 中所列的相应编号。

步骤 3 点击 **OK**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

管理合规 允许 名单

可以使用 允许 名单页面管理合规allow名单和共享主机配置文件。默认allow名单表示建议的设置，并使用共享主机配置文件的一个特殊类别，即 内置主机配置文件。

在多域部署中，系统会显示在当前域中创建的合规 allow 名单，您可以对其进行编辑。系统还会显示祖先域中的选定 allow 名单，您不可以对其进行编辑。要查看和编辑在较低域中创建的 allow 名单，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。 默认 allow 名单仅在全局域中可用。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 管理合规 allow 名单：

- 创建 - 要创建新的 allow 名单，请点击 **新建允许列表**，然后如 创建合规 允许 名单，第 6 页 中所述继续操作。
- 删除 - 要删除未使用的 an allow 名单，请点击 **删除**（）），然后确认要删除该 allow 名单。删除 an allow 名单还会从网络上所有主机中删除其关联的主机属性。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 编辑 - 要修改现有 allow 名单，请点击 **编辑**（），然后如 编辑合规 允许 名单，第 13 页中所述继续操作。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

- 共享主机配置文件 - 要管理 allow 名单的共享主机配置文件，请点击 **编辑共享配置文件** ，然后如 管理共享主机配置文件 ， 第 14 页中所述继续操作。

编辑合规 允许 名单

当修改并保存活动关联策略中包含的合规 allow 名单时，系统会立即重新评估 allow 名单的目标网络中主机的合规性。尽管此重新评估可能会使某些主机合规或不合规，但是系统不会生成任何 allow 名单事件。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 在要修改的 allow 名单旁，点击 **编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑合规 allow 名单：

- 名称和说明 - 要更改名称或说明，请点击左侧面板中的 allow 名单名称以显示基本 allow 名单信息，然后键入新信息。
- 允许破解的设备 - 要在网络上允许破解的移动设备，请点击左侧面板中的 allow 名单名称以显示基本 allow 名单信息，然后启用 **允许破解的移动设备**。禁用此选项会导致破解设备生成 allow 名单违规。
- 添加允许的主机配置文件 - 要为此 allow 名单创建操作系统特定主机配置文件，请点击“允许的主机配置文件”旁边的 **添加**（ ），然后如 构建 允许 列表主机配置文件 ， 第 9 页中所述继续操作。
- 添加共享主机配置文件 - 要向 allow 名单中添加现有共享主机配置文件，请点击 **添加共享主机配置文件**，选择要添加的共享主机配置文件，然后点击 **确定**。共享主机配置文件以斜体显示。
- 添加目标网络 - 要添加新的目标网络而不调查其主机，请点击“目标网络”旁边的 **添加**（ ），然后如 为合规 允许 名单创建目标网络 ， 第 8 页中所述继续操作。
- 删除主机配置文件 - 要从 allow 名单中删除共享主机配置文件或操作系统特定主机配置文件，请点击主机配置文件旁边的 **删除**（ ），然后确认选择。删除共享主机配置文件会从 allow 名单中将其移除，但是不会删除该配置文件，也不会从使用它的任何其他 allow 名单中将其移除。您无法删除 an allow 名单的全局主机配置文件。
- 删除目标网络 - 要从 allow 名单中移除目标网络，请点击网络旁边的 **删除**（ ），然后确认选择。
- 编辑全局主机配置文件 - 要编辑 allow 名单的全局主机配置文件，请点击 **任何操作系统** ，然后如 构建 允许 列表主机配置文件 ， 第 9 页中所述继续操作。

- 编辑其他主机配置文件 - 要编辑共享主机配置文件或操作系统特定主机配置文件，请点击该主机配置文件的名称，然后如构建 允许 列表主机配置文件，第 9 页中所述继续操作。
- 编辑目标网络 - 要编辑目标网络，请点击网络的名称，然后如为合规 允许 名单创建目标网络，第 8 页中所述继续操作。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

管理共享主机配置文件

在合规 allow 名单中，共享主机配置文件绑定到特定操作系统，但是您可以在多个 allow 名单中使用每个共享主机配置文件。如果创建了多个allow名单，但要使用相同的主机配置文件来评估运行allow名单中规定的特定操作系统的主机，可使用共享主机配置文件。

在多域部署中，系统会显示在当前域中创建的共享主机配置文件，您可以对其进行编辑。系统还会显示祖先域中的共享主机配置文件，您不可以对其进行编辑。要查看和编辑在较低域中创建的共享主机配置文件，请切换至该域。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个 allow 名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 点击 **Edit Shared Profiles**。

步骤 3 管理共享主机配置文件：

- 创建共享主机配置文件 - 要创建新的共享主机配置文件而不调查主机，请点击共享主机配置文件旁边的 **添加**（＋），然后如 构建 允许 列表主机配置文件，第 9 页中所述继续操作。
- 通过调查创建共享主机配置文件 - 要通过调查网络创建多个新的共享主机配置文件，请点击**添加目标网络 (Add Target Network)**，然后如为合规 允许 名单创建目标网络，第 8 页中所述继续操作。
- 删除 - 要删除共享主机配置文件，请点击 **删除**（🗑），然后确认您的选择。
- 编辑 - 要修改现有的共享主机配置文件（包括内置共享主机配置文件），请点击其名称，然后如构建 允许 列表主机配置文件，第 9 页中所述继续操作。

- 重置内置主机配置文件 - 要将所有内置主机配置文件重置为出厂默认设置，请点击**内置主机配置 (Built-in Host Profiles)**，然后点击**重置为出厂默认设置 (Reset to Factory Defaults)** 并确认您的选择。

步骤 4 要立即实施自上次保存后做出的所有更改，请点击**保存所有配置文件 (Save All Profiles)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。