管理网络安全设备

本章包含以下部分：

- 关于集中配置管理 , on page 1
- 确定正确的配置发布方法 , on page 2
- 使用主配置以集中管理网络安全设备 , on page 2
- 初始化并配置主配置, on page 5
- 设置为使用高级文件发布 , on page 15
- 将配置发布到网络安全设备, on page 15
- 查看发布作业的状态和历史记录 , on page 21
- 集中化升级管理， 第 21 页
- 查看网络安全设备状态， 第 25 页
- 准备和管理 URL 类别集更新 , on page 28
- 应用可视性与可控性 (AVC) 更新 , on page 29
- 使用 CLI 更新 WBRS 和 AVC 数据， 第 29 页
- 对配置管理问题进行故障排除 , on page 30

关于集中配置管理

集中配置管理允许从思科 安全邮件和 Web 管理器设备向相关网络安全设备发布配置，以便：

- 通过在安全管理设备（而不是各个网络安全设备）上一次性配置或更新设置，简化和加快网络安全策略管理。
- 确保跨分布式网络实施统一策略。

可通过两种方式向网络安全设备发布设置：

- 使用主配置
- 使用网络安全设备中的配置文件（使用“高级文件发布 (Advanced File Publishing)”）

确定正确的配置发布方法

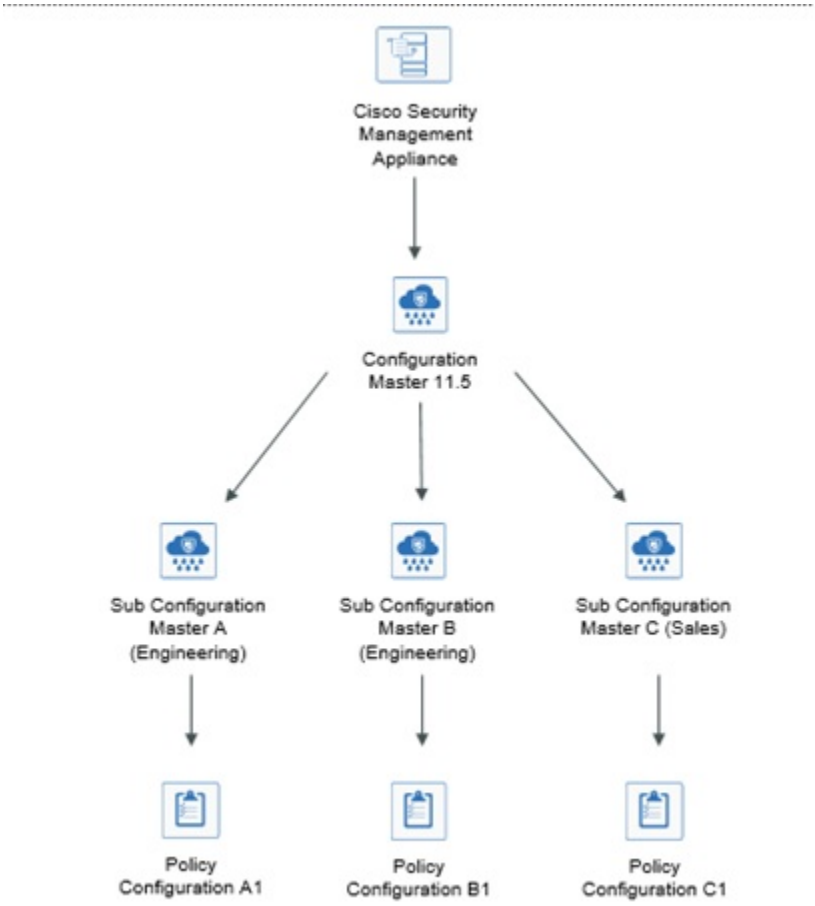
从安全邮件和网页管理器设备发布配置有两种不同的流程，每种流程发布不同的设置。有些设置不能集中管理。

配置	请
在网络安全设备上的“网络安全管理器 (Web Security Manager)”菜单下显示的功能，例如策略和自定义 URL 类别。 例外：主配置中不含“L4 流量监控器”(L4TM) 设置。 支持的确切功能取决于主配置版本，它与某个网络安全 AsyncOS 版本相对应。	发布主配置。 主配置中可配置的许多功能还要求直接在网络安全设备上配置，才能使用。例如，“SOCKS 策略 (SOCKS Policies)”可通过主配置进行配置，但“SOCKS 代理 (SOCKS Proxy)”必须首先在网络安全设备中直接配置。
注意：必须在每台网络安全设备上独立配置与思科身份服务引擎 (ISE) 的集成。Cisco 身份服务引擎设置无法从 Cisco 安全邮件和网页管理器 设备发布。	使用高级文件发布。
联邦信息处理标准 (FIPS) 模式、网络/接口设置、DNS、网络高速缓存通信协议 (WCCP)、上游代理组、证书、代理模式、时间设置（例如 NTP）、L4 流量监控器 (L4TM) 设置和身份验证重定向主机名。	在托管网络安全设备上直接配置设置。 请参阅思科网络安全设备 AsyncOS 用户指南

使用主配置以集中管理网络安全设备

安全管理设备提供多个不同的主配置版本，以便可以集中管理网络安全设备。每个主配置都支持其下方的多个子配置主机。通过子主配置，您可以在同一主配置中定义不同的策略配置。

假设您的工程和销售团队正在使用 AsyncOS 11.7 网络安全设备。您的组织策略要求您为这些团队定义不同的策略。在这种情况下，您可以在主配置 11.7 下创建两个子配置主机，并为每个子主配置定义不同的策略配置，如下图所示：



设置主配置以集中管理网络安全设备

下表提供了有关初始化和配置主配置和子主配置的说明。

步骤	相应操作	设备	更多信息
第 1 步	检查常规配置要求和警告。	—	请参阅 有关使用主配置的重要注意事项, on page 4。
第 2 步	确定要用于各个网络安全设备的主配置版本。	—	请参阅确定要使用的主配置版本, on page 5。
步骤 3	在所有目标网络安全设备上，启用并配置用于支持您将在安全管理设备的主配置中配置的策略和其他设置的必需特性和功能。	网络安全设备	—

步骤	相应操作	设备	更多信息
第 4 步	（**可选**）如果有一台网络安全设备正在运行，并可以将其用作所有网络安全设备的配置模型，则可以使用该网络安全设备中的配置文件加快安全管理设备中主配置的配置速度。	网络安全设备	有关从网络安全设备下载配置文件的说明，请参阅《思科网络安全设备 *AsyncOS* 用户指南》中的“保存和加载设备配置”。
第 5 步	启用并配置集中配置管理。	安全管理设备	请参阅在安全管理设备上启用集中配置管理, on page 5。
步骤 6	初始化主配置。	安全管理设备	请参阅初始化并配置主配置, on page 5。
步骤 7	（**可选**）配置子主配置	安全管理设备	请参阅配置子主配置, on page 8
第 8 步	（**可选**）选择子主配置作为活动配置	安全管理设备	请参阅 选择子主配置作为活动配置, on page 9
步骤 9	将网络安全设备关联到主配置。	安全管理设备	请参阅关于将网络安全设备与主配置关联, on page 6。
步骤 10	在主配置中导入和/或手动配置策略、自定义 URL 类别和/或网络代理绕行列表。	安全管理设备	请参阅 配置要发布的设置 , on page 9
步骤 11	确保各个网络安全设备上启用的功能与为分配到该设备的主配置启用的功能匹配。	安全管理设备	请参阅确保一致地启用功能 , on page 13。
第 12 步	在设置了所需的主配置并启用了相应功能之后，向网络安全设备发布配置。	安全管理设备	请参阅发布主配置 , on page 15。
第 13 步	为可能的 URL 类别集更新提前做准备，以便修改现有的主配置设置。	安全管理设备	准备和管理 URL 类别集更新 , on page 28

有关使用主配置的重要注意事项

Important 在升级到 AysncOS 12.0 及更高版本之前，您可能需要备份主配置设置。主配置版本10.0 及更早版本将替换为主配置版本 11.7 及更高版本。

升级到此版本后，必须初始化新的主配置或从现有主配置导入配置。如果您已有先前版本（例如，9.1）的主配置，则可以将设置复制到新的主配置（例如，11.5）。

由于主配置版本发生变化，“设备列表”将从身份和策略中丢失。您必须将网络安全设备与相应的主配置重新关联。

Note 在集中管理的各个网络安全设备上，检查确保“网络 (Network)”>“身份验证 (Authentication)”中的所有领域名称在整个设备范围内是唯一的，除非同名领域的设置相同。

确定要使用的主配置版本

安全管理设备提供多个主配置，以便可以集中管理运行不同版本的 AsyncOS for Web Security（支持不同的功能）的网络安全设备。

每个主配置包含要用于一个或多个特定网络安全 AsyncOS 版本的配置。

要确定哪些主配置版本适用于您的AsyncOS网络安全版本，请参阅位于以下网站的“兼容性矩阵”：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

Note 主配置版本应与网络安全设备上的 AsyncOS 版本相匹配，如兼容性矩阵所指定。如果网络安全设备中的设置与主配置中的设置不匹配，向更新的网络安全设备发布较早的主配置版本可能会失败。即使“网络设备状态”(Web Appliance Status) 详细信息页面未指明任何差异，也可能发生这种情况。在这种情况下，您必须手动比较每台设备上的配置。

在安全管理设备上启用集中配置管理

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 网络 (Web) >集中配置管理器 (Centralized Configuration Manager)**。

步骤 2 单击**启用 (Enable)**。

步骤 3 如果您在运行“系统设置向导”后首次启用集中配置管理，请查看最终用户许可协议，然后单击**接受 (Accept)**。

步骤 4 提交并确认更改。

初始化并配置主配置

- 初始化主配置 , on page 5
- 从网络安全设备中导入设置 , on page 10
- 配置要发布的设置 , on page 9

初始化主配置

注意：在初始化主配置后，“初始化”选项不可用。相反，请使用配置要发布的设置 , on page 9介绍的其中一种方法填充主配置。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

步骤 2 在“选项”(Options) 列中单击**初始化 (Initialize)**。

步骤 3 在“初始化主配置”(Initialize Configuration Master) 页面上：

- 如果您有某个以前版本的现有主配置，并且希望将相同的设置用于新的主配置或从相同的设置开始，请选择**复制主配置 (Copy Configuration Master)**。您稍后还可以从现有的主配置中导入设置。
- 否则，请选择**使用默认设置 (Use default settings)**。

步骤 4 单击**初始化 (Initialize)**。

主配置现在可用。

步骤 5 为每个主配置版本重复上述初始化步骤。

关于将网络安全设备与主配置关联

有关主配置与网络安全版本兼容性的信息，请参阅确定要使用的主配置版本, on page 5。

将设备添加到主配置的最简单过程取决于具体情况：

如果	使用以下程序
您尚未将网络安全设备添加至安全管理设备	添加网络安全设备并将其与主配置版本关联 , on page 6
您已经添加网络安全设备	将主配置与网络安全设备关联 , on page 7
您想要在设备列表中查看关联的主配置	在设备列表中查看关联的主配置, on page 8

添加网络安全设备并将其与主配置版本关联

如果您尚未添加要集中管理的网络安全设备，请使用以下程序。

Before you begin

- 选择适合各个网络安全设备的正确主配置版本。请参阅 确定要使用的主配置版本, on page 5
- 在您打算添加到安全管理设备的网络安全设备上启用以下密钥交换和密码算法：
  - 密钥交换算法：

    `diffie-hellman-group1-sha1,diffie-hellman-group14-sha1`
  - Cipher Algorithms:

    `3des-cbc,blowfish-cbc`

要启用算法，请在网络安全设备上的 CLI 中使用 `sshconfig > sshd` 命令。

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **安全设备 (Security Appliances)**。

步骤 2 单击“添加网络设备”(Add Web Appliance)。

步骤 3 在“设备名称 (Appliance Name)”和“IP 地址 (IP Address)”文本字段，键入设备名称和网络安全设备管理接口的 IP 地址或可解析主机名。

Note 如果在“IP 地址 (IP Address)”文本字段中输入 DNS 名称，则单击**提交 (Submit)** 后，该名称将立即解析为 IP 地址。

步骤 4 “集中配置管理器”(Centralized Configuration Manager) 服务已预先选择。

步骤 5 单击**建立连接 (Establish Connection)**。

步骤 6 在要托管的设备上输入管理员账户的用户名和口令，然后单击**建立连接 (Establish Connection)**。

Note 输入登录凭证，以便将文件传输的公共 SSH 密钥从安全管理设备传递到远程设备。登录凭证不会存储在安全管理设备上。

步骤 7 等待该页面表格上方显示成功消息。

步骤 8 选择您要将设备分配至哪个主配置版本。

Note 如果配置了特定版本的主配置和分配网络安全设备的子集，则会在下拉列表中显示与 Web 安全设备关联的子主配置版本。

步骤 9 提交并确认更改。

步骤 10 对于您要为其启用“集中配置管理”(Centralized Configuration Management) 的每台网络安全设备，请重复上述操作程序。

将主配置与网络安全设备关联

如果已将网络安全设备添加到安全管理设备，则可以使用以下程序快速将网络安全设备与主配置版本关联。

Before you begin

如果尚未添加，请选择适合各个网络安全设备的正确主配置版本。请参阅确定要使用的主配置版本, on page 5。

步骤 1 在安全管理设备上，依次选择**网络 (Web)** > **实用程序 (Utilities)** > **主配置 (Configuration Masters)**。

Note 如果主配置显示为“已禁用”(Disabled)，可以单击 **网络 (Web)** > **实用程序 (Utilities)** > **安全服务显示 (Security Services Display)**将其启用，然后单击**编辑显示设置 (Edit Display Settings)**。选中该主配置的复选框可启用它。有关详细信息，请参阅启用要发布的功能 , on page 14。

步骤 2 单击**安全设备 (Security Appliances)**。

步骤 3 单击所需的网络安全设备。

步骤 4 选择主配置的所需配置。

您可以在**Web > 实用程序 > 主配置**页面中查看主配置的不同配置。

步骤 5 提交并确认更改。

配置子主配置

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

注释 如果主配置显示为“已禁用”(Disabled)，可以单击 **网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**将其启用，然后单击**编辑显示设置 (Edit Display Settings)**。选中该主配置的复选框可启用它。有关详细信息，请参阅启用要发布的功能 ，第 14 页。

步骤 2 在“新建主配置”(New Configuration Master) 页面中，单击**新建 (New)**。

步骤 3 输入主配置的唯一名称（例如，11_5_new）。

注释 名称必须仅包含字母、数字和下划线。它不能以下划线开头。

步骤 4 从下拉列表中选择主配置版本。

步骤 5 对于“选择配置来源”(Select Configuration Source)，请从下拉列表中选择一个主配置。

步骤 6 单击**提交 (Submit)** 并确认更改。

在设备列表中查看关联的主配置

开始之前

如果尚未添加，请选择适合各个网络安全设备的正确主配置版本。请参阅确定要使用的主配置版本 ，第 5 页。

如果已将网络安全设备添加到安全管理设备，则可以使用以下程序查看网络安全设备列表中的相关主配置版本。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

注释 如果主配置显示为“已禁用”(Disabled)，可以点击 **网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**将其启用，然后点击**编辑显示设置 (Edit Display Settings)**。选中该主配置的复选框可启用它。有关详细信息，请参阅启用要发布的功能 ，第 14 页。

步骤 2 点击**安全设备 (Security Appliances)**。

“安全设备”(Security Appliances) 页面与**管理设备 (Management Appliances) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**页面相同。如果已向其添加网络安全设备和关联的主配置，则可以查看与网络安全设备关联的主配置和 AsyncOS 版本。

删除子主配置

如果您在配置子主配置 ， 第 8 页中配置了子主配置，请使用以下程序删除配置。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

注释 如果主配置显示为“已禁用”(Disabled)，可以点击 **网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**将其启用，然后点击**编辑显示设置 (Edit Display Settings)**。选中该主配置的复选框可启用它。有关详细信息，请参阅启用要发布的功能 ， 第 14 页。

步骤 2 点击所需的子主配置上的垃圾桶图标。

注释 您无法删除与网络安全设备关联的主配置。

步骤 3 提交并确认更改。

选择子主配置作为活动配置

在配置子主配置时，必须将所需配置分配为活动配置。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

步骤 2 在主配置的所需配置版本上点击**编辑 (Edit)**。选择主配置版本将替换主配置的现有配置。

步骤 3 确认您的更改。

在您提交更改后，您可以看到主配置下拉列表的标签已更改为所选主配置版本。

配置要发布的设置

使用要发布的设置来设置您的主配置。

有几种方法可以设置主配置：

If	相应操作
您从以前的安全管理 AsyncOS 版本进行升级 和 您未通过将较早的现有主配置版本复制到新的主配置版本来初始化新版本。	导入旧版本。请参阅从现有主配置导入 , on page 10。
已经配置了一台网络安全设备，并希望对于多台网络安全设备采用相同的配置	将您保存的配置文件从该网络安全设备导入到主配置。 在您查看使用主配置以集中管理网络安全设备 , on page 2时，可能已保存了此配置文件。 要导入，请参阅从网络安全设备中导入设置 , on page 10。
您需要修改导入的设置	请参阅直接在主配置中配置网络安全功能, on page 11。
尚未在网络安全设备上配置策略设置、URL 类别或旁路设置。	直接在安全管理设备上相应的主配置中配置这些设置。 请参阅直接在主配置中配置网络安全功能, on page 11。

从现有主配置导入

您可以将现有的主配置升级到新的、更高的主配置版本。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

步骤 2 在“选项”(Options) 列中，点击**导入配置 (Import Configuration)**。

步骤 3 对于**选择配置来源 (Select Configuration Source)**，请从列表中选择一个主配置。

步骤 4 选择是否在此配置中包括现有的自定义用户角色。

步骤 5 点击**导入**。

What to do next

关于自定义网络用户角色

从网络安全设备中导入设置

如果想要使用其中一台网络安全设备当前正在运行的配置，可以将配置文件导入到安全管理设备来创建主配置中的策略设置。

Before you begin

验证配置文件和主配置版本的兼容性。请参阅确定要使用的主配置版本, on page 5。

Caution 即使已向托管的网络安全设备发布配置，也可以根据自己的需要决定导入兼容网络配置文件的频率。将配置文件导入主配置将完全覆盖与所选主配置关联的设置。此外，“安全服务显示(Security Services Display)”页面的安全服务设置将设置为与导入的配置匹配。

Note 如果您尝试导入的配置文件使用的 URL 类别集比安全管理设备具有的 URL 类别集更旧，加载将失败。

步骤 1 从网络安全设备保存配置文件。

步骤 2 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置 (Configuration Masters)**。

步骤 3 在“选项”(Options) 列中，点击**导入配置 (Import Configuration)**。

步骤 4 从“选择配置”(Select Configuration) 下拉列表中，选择**网络配置文件 (Web Configuration File)**。

步骤 5 在“新主配置默认值”(New Master Defaults) 部分，点击**浏览 (Browse)** 并从网络安全设备中选择有效的配置文件。

步骤 6 点击**导入文件 (Import File)**。

步骤 7 点击**导入 (Import)**。

直接在主配置中配置网络安全功能

您可以在主配置中配置以下功能，具体取决于版本：

• 身份/识别配置文件 • SaaS 策略 • 解密策略 • 路由策略 • 访问策略 • 网络流量分流策略 **Note** 若要定义网络流量分流策略，必须在网络安全设备中启用网络流量分流功能。 • 总体带宽限制	• 思科数据安全 • 出站恶意软件扫描 (Outbound Malware Scanning) • 外部数据丢失防护	• SOCKS 策略 • 自定义 URL类别 • 定义的时间范围和/或配额 • 绕行设置 • L4通信监控

要直接在主配置中配置每项功能的设置，请依次选择**网络 (Web) > 主配置 (Configuration Master)** < 版本> > <功能>。

除在主配置中配置功能时特定于 SMA 的差异 , on page 12中所述的几项外，在主配置中配置功能的说明与在网络安全设备上配置相同功能的说明相同。有关说明，请参阅网络安全设备的在线帮助，或者与主配置版本相对应的 AsyncOS 版本的《思科网络安全设备 AsyncOS 用户指南》。如果需要，请查阅以下主题确定适合您的网络安全设备的正确主配置：确定要使用的主配置版本, on page 5

网络安全用户指南的所有版本均可从https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html获取。

在主配置中配置功能时特定于 SMA 的差异

在主配置中配置功能时，请注意以下与直接在网络安全设备上配置相同功能的差异。

Table 1: 功能配置：主配置与网络安全设备之间的差异

功能或页面	详细信息
所有功能，特别是每个版本中的新功能	对于在主配置中配置的每项功能，必须在安全管理设备的“网络”(Web)>“实用程序”(Utilities) >“安全服务显示”(Security Services Display) 下启用功能。有关详细信息，请参阅确保一致地启用功能 , on page 13。
身份/识别配置文件	• 请参阅关于在主配置中使用身份/识别配置文件的提示 , on page 13。 • 在添加或编辑身份/识别配置文件时，如果具有身份验证领域且支持透明用户识别的网络安全设备已添加为托管设备，则**透明地识别用户**选项可用。
使用思科身份服务引擎 (ISE) 识别用户的策略	约每五分钟从网络安全设备更新一次安全组标签 (SGT) 信息。管理设备不与 ISE 服务器直接通信。 要按需更新 SGT 列表，请选择**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，点击某台连接到 ISE 服务器的网络安全设备，然后点击**刷新数据 (Refresh Data)**。根据需要对其他设备重复此步骤。 最常见的部署方案是一家公司只有一台所有 WSA 连接至的 ISE 服务器（这是 ISE 的全部要点）。不支持具有不同数据的多台 ISE 服务器。
“访问策略”(Access Policies)>“编辑组”(Edit Group)	在“策略成员定义”(Policy Member Definition) 部分中配置“身份/识别配置文件”(Identities /Identification Profiles) 和“用户”(Users) 选项时，如果您使用外部目录服务器，则以下内容适用： 当您在“编辑组”(Edit Group) 页面上搜索组时，只会显示前 500 项匹配的结果。如果没有看到所需的组，可以在“目录”(Directory) 搜索字段中输入该组并点击**添加 (Add)** 按钮，将其添加到“授权组”(Authorized Groups) 列表。
访问策略 (Access Policies) > 网络信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)	
SaaS 策略	只有作为托管设备添加了身份验证领域支持透明用户身份识别的网络安全设备，身份验证选项“提示透明用户身份识别功能发现的 SaaS 用户 (Prompt SaaS users who have been discovered by transparent user identification)”才可用。

关于在主配置中使用身份/识别配置文件的提示

在安全管理设备上创建身份/识别配置文件时，可以选择使其仅适用于特定设备。例如，您购买了一台安全管理设备，并希望保留为每台网络安全设备创建的现有网络安全设备配置和策略，则必须向计算机加载一个文件，然后从其他计算机手动添加策略。

完成此任务的一种方法是为每台设置建立一组身份/识别配置文件，然后拥有引用这些身份/识别配置文件的策略。当安全管理设备发布配置时，将自动删除和禁用引用它们的身份/识别配置文件和策略。使用此方法，您不必手动配置任何设置。这实际上是一个“按设备”的身份/识别配置文件。

使用此方法的唯一挑战：您具有一个在站点之间不同的默认策略或身份/识别配置文件。例如，您在一个站点具有为“默认允许及身份验证”(default allow with auth) 设置的策略，在另一个站点具有为“默认拒绝”(default deny) 设置的策略。此时，您将需要在默认设置上创建按设备的身份/识别配置文件和策略；实际上是创建您自己的“默认”策略。

确保一致地启用功能

在发布主配置之前，您应该确保将发布该主配置，并确保在发布后将按照您的期望启用并配置预期的功能。

为此，请执行以下两项操作：

- 比较启用的功能 , on page 13
- 启用要发布的功能 , on page 14

Note 如果为同一主配置分配了多个启用不同功能的网络安全设备，应单独向每台设备发布，并在每次发布前执行以下操作。

比较启用的功能

确认各个网络安全设备上启用的功能与为分配到该设备的主配置启用的功能匹配。

Note 如果为同一主配置分配了多个启用不同功能的网络安全设备，应单独向每台设备发布，并在每次发布前执行此检查。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**。

步骤 2 点击要将主配置发布到的网络安全设备的名称。

步骤 3 滚动到**安全服务 (Security Services)** 表。

步骤 4 验证所有已启用功能的功能密钥处于活动状态且未过期。

步骤 5 比较**服务 (Services)** 列中的设置：

网络设备服务 (Web Appliance Service) 列和**服务是否显示在管理设备上？(Is Service Displayed on Management Appliance?)** 列应该一致。

- 已启用 = 是
- 已禁用和未配置 = 否或已禁用。
- N/A=不适用。例如，可能无法使用主配置对该选项进行配置，但是会列出该选项，使您可以查看功能密钥状态。

配置不匹配将以红色文本显示。

What to do next

如果某项功能的已启用/已禁用设置不匹配，请执行以下操作之一：

- 更改主配置的相关设置。请参阅启用要发布的功能 , on page 14。
- 在网络安全设备上启用或禁用该功能。某些更改可能影响多个功能。有关相关功能的信息，请参阅《适用于思科网络安全设备的 AsyncOS 用户指南》。

启用要发布的功能

启用您要使用主配置发布其设置的功能。

Before you begin

确定必须启用和禁用哪些功能。请参阅比较启用的功能 , on page 13。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**。

步骤 2 单击**编辑设置 (Edit Settings)**。

“编辑安全服务显示”(Edit Security Services Display) 页面列出了每个主配置中出现的功能。

功能旁边的“N/A”表示该功能在此主配置版本中不可用。

Note 网络代理不作为功能列出，因为假定已启用网络代理，以便在网络安全设备上执行任何托管的策略类型。如果网络代理被禁用，将忽略发布到该网络安全设备中的任何策略。

步骤 3 （可选）隐藏不使用的主配置。有关说明和注意事项，请参阅禁用未使用的主配置 , on page 15。

步骤 4 对于您将使用的每个主配置，请为要启用的每项功能选中或取消选中“是”复选框。

某些功能的特殊注意事项（可用的选项因主配置版本而异）：

- 透明模式。如果使用“转发”(Forward) 模式，则代理绕行功能将不可用。
- HTTPS 代理。要配置解密策略，必须启用 HTTPS 代理。
- 上游代理组。如果希望使用路由策略，则上游代理组必须在网络安全设备上可用。

步骤 5 单击**提交 (Submit)**。如果对安全服务设置的更改会影响网络安全设备上配置的策略，则 GUI 将显示特定的警告消息。如果确定要提交更改，请单击**继续 (Continue)**。

步骤 6 在**安全服务显示 (Security Services Display)** 页面上，确认**是 (Yes)** 出现在您选择的每个选项旁边。

步骤 7 确认您的更改。

What to do next

- 验证现在已经为您将发布到的设备正确启用或禁用所有功能。请参阅比较启用的功能 , on page 13。
- 在主配置接收设备的每个网络安全设备上，确保启用的功能与为主配置启用的功能一致。

禁用未使用的主配置

您可以选择不显示未使用的主配置。

但是，必须启用至少一个主配置。

Note 当某个主配置被禁用时，将从 GUI 中删除所有对它的引用，包括相对应的“主配置 (Configuration Master)”选项卡。使用该主配置的待发布作业将被删除，而所有分配到该隐藏主配置的网络安全设备将重新归类为“未分配”。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 取消选中未使用的主配置的复选框

步骤 4 提交并确认更改。

设置为使用高级文件发布

如果您的系统设置为使用主配置，则它已设置高级文件发布。

否则，请完成以下主题中的操作程序，这些操作程序适用于高级文件发布以及主配置发布。

- 在安全管理设备上启用集中配置管理, on page 5
- 初始化主配置 , on page 5
- 关于将网络安全设备与主配置关联, on page 6

将配置发布到网络安全设备

- 发布主配置 , on page 15
- 使用高级文件发布功能发布配置, on page 19

发布主配置

在主配置中编辑或导入设置后，可以将它们发布到与主配置关联的网络安全设备。

- 在发布主配置之前 , on page 16

- 立即发布主配置 , on page 17
- 稍后发布主配置 , on page 18
- 使用命令行界面发布主配置, on page 19

在发布主配置之前

发布主配置将覆盖与该主配置关联的网络安全设备上的现有策略信息。

有关可使用主配置进行配置的设置信息，请参阅确定正确的配置发布方法 , on page 2。

所有发布作业

- 目标网络安全设备上的 AsyncOS 版本应与主配置版本相同，或者是在 SMA 兼容性值表中确定为兼容的版本。
- （仅限首次）必须遵循使用主配置以集中管理网络安全设备 , on page 2中的程序。
- 要确保主配置将会发布且发布后将启用预期的功能集，请验证每个网络安全设备的功能集及相关主配置，并进行任何所需的更改。请参阅比较启用的功能 , on page 13，如有必要，请参阅启用要发布的功能 , on page 14。如果您为未在目标设备上启用的功能发布配置，则不会应用这些配置。

如果在分配到同一主配置的不同网络安全设备上启用了不同的功能，则必须单独向每台设备发布，并在每次发布前验证和启用功能。

要识别在发布时遇到的配置不匹配，请参阅查看发布历史记录, on page 21。

- 在发布之前从每台目标网络安全设备中保存配置文件，以便在发布的配置出现问题时可以恢复现有配置。有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。
- 如果在网络安全设备上确认任何更改后，可能会导致网络代理重启，则从安全管理设备发布这些更改时，也会导致代理重启。在这些情况下，您会收到一条警告。

网络代理重新启动会暂时中断网络安全服务。

- 在将任何更改发布到身份/识别配置文件时，所有最终用户必须重新进行身份验证。

特殊情况

- 如果在目标网络安全设备上恢复了 AsyncOS，可能需要将不同的主配置与该设备相关联。
- 如果将主配置发布到的网络安全设备没有在启用“透明用户身份识别”的情况下配置的领域，但已在身份/识别配置文件或 SaaS 策略中选择“透明用户身份识别”：
  - 对于身份/识别配置文件，“透明用户识别”(Transparent User Identification) 已禁用，改为选中“需要身份验证”(Require Authentication) 选项。
  - 对于 SaaS 策略，“透明用户识别”(Transparent User Identification) 选项已禁用，改为选中默认选项“始终提示 SaaS 用户进行代理身份验证”(Always prompt SaaS users for proxy authentication)。

- 从安全管理设备向多个并非为 RSA 服务器配置的网络安全设备发布外部 DLP 策略时，安全管理设备将发送以下发布状态警告：

“为主配置 <版本>配置的安全服务显示设置当前未反映与此发布请求相关联的网络设备上的一个或多个安全服务的状态。受影响的设备是：“<*WSA* 设备名称>”。这可能表示此特定主配置的安全服务显示设置的配置不正确。转到每台设备的网络设备状态 (Web Appliance Status) 页面可获得有助于对该问题进行故障排除的详细视图。现在是否要继续发布配置？”

如果决定继续发布，则并非为 RSA 服务器配置的网络安全设备将收到外部 DLP 策略，但这些策略将被禁用。如果未配置外部 DLP 服务器，网络安全设备的“外部 DLP (External DLP)”页面不会显示发布的策略。

如果主配置中身份/识别配置文件中的方案为：	则网络安全设备上的身份/识别配置文件中的方案变成
使用 Kerberos	使用 NTLMSSP 或基本
使用 Kerberos 或 NTLMSSP	使用 NTLMSSP
使用 Kerberos 或 NTLMSSP 或 Basic	使用 NTLMSSP 或基本

如果您是外部身份验证用户，则只能查看分配给网络安全设备的所有主配置的列表，并发布当前已初始化的配置。如果要发布主配置的不同子集，请与管理员联系。

Note 不要同时使用以下内容编辑、加载或发布主配置：

- 同一浏览器上的多个选项卡。
- 同一系统或两个不同系统上的多个浏览器。

立即发布主配置

Before you begin

请参阅在发布主配置之前 , on page 16中的重要要求和信息。

步骤 1 在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 2 单击**立即发布配置 (Publish Configuration Now)**。

步骤 3 “系统生成的作业名称”(System-generated job name) 在默认情况下处于选中状态，或者请输入自定义的作业名称（不超过 80 个字符）。

步骤 4 选择要发布的主配置。

Note 如果配置了特定版本的主配置和分配网络安全设备的子集，则会在下拉列表中显示与 Web 安全设备关联的子主配置版本。

步骤 5 选择要将主配置发布到的网络安全设备。选择“所有已分配设备 (All assigned appliances)”，将配置发布到分配到该主配置的所有设备。

或

选择“在列表中选择设备”(Select appliances in list) 以显示分配给主配置的设备列表。选择要将配置发布到的设备。

步骤 6 单击**发布 (Publish)**。

“正在发布”(Publish in Progress) 页面上的红色进度条和文本表示在发布期间出错。如果另一个作业当前正在发布，则您的请求将在上一个作业完成时执行。

Note 正在进行的作业的详细信息还会出现在**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)** 页面上。单击**检查进度 (Check Progress)** 访问“正在发布”(Publish in Progress) 页面。

What to do next

检查以确保发布完全成功。请参阅查看发布历史记录, on page 21。系统将记录未完全发布的项目。

稍后发布主配置

Before you begin

请参阅在发布主配置之前 , on page 16中的重要要求和信息。

步骤 1 在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 2 点击**安排作业 (Schedule a Job)**。

步骤 3 “系统生成的作业名称”(System-generated job name) 在默认情况下处于选中状态，或者请输入自定义的作业名称（不超过 80 个字符）。

步骤 4 输入要发布主配置的日期和时间。

步骤 5 选择要发布的主配置。

步骤 6 选择要将主配置发布到的网络安全设备。选择“所有已分配设备 (All assigned appliances)”，将配置发布到分配到该主配置的所有设备。

或

选择“在列表中选择设备”(Select appliances in list) 以显示分配给主配置的设备列表。选择要将配置发布到的设备。

步骤 7 点击**提交 (Submit)**。

步骤 8 在**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)** 页面上查看已安排的作业列表。要编辑已安排的作业，请点击作业的名称。要取消待定的作业，请点击对应的垃圾桶图标并确认您要删除该作业。

步骤 9 您可能需要为自己创建提醒（例如，在日历中），以便在安排的发布时间过后进行检查，确保成功完成发布。

Note 如果在安排的作业发布前重启或升级设备，则必须重新安排作业。

What to do next

检查以确保发布完全成功。请参阅查看发布历史记录, on page 21。系统将记录未完全发布的项目。

使用命令行界面发布主配置

Note 请参阅在发布主配置之前 , on page 16中的重要要求和信息。

安全管理设备提供使用以下 CLI 命令，通过主配置发布更改的功能：

publishconfig config_master [*--job_name*] [*--host_list* | *host_ip*]

其中 **config_master** 是受支持的主配置版本。此关键字是必需的。选项 *job_name* 是可选的，如果未指定该选项，系统将生成它。

host_list 选项是要发布的网络安全设备的主机名或 IP 地址列表，将发布到分配到主配置的所有主机（如果未指定）。选项 *host_ip* 可以是用逗号分隔的多个主机 IP 地址。

要验证 **publishconfig** 命令是否成功，请检查 **smad_logs** 文件。还可以选择网络 (Web) > **用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，从安全管理设备 GUI 确认发布历史记录是否成功。在此页面选择想要获取其发布历史记录详细信息的网络设备。此外，您可以转到“发布历史记录”(Publish History) 页面：依次选择**网络 (Web) > 实用程序 (Utilities) > 发布 (Publish) > 发布历史记录 (Publish History)**。

使用高级文件发布功能发布配置

使用高级文件发布可从本地文件系统向托管网络安全设备推送兼容的 XML 配置文件。

有关可使用高级文件发布配置的设置的信息，请参阅确定正确的配置发布方法 , on page 2。

要执行高级文件发布，请执行以下操作：

- 高级文件发布：立即发布配置, on page 19
- 高级文件发布：稍后发布, on page 20

高级文件发布：立即发布配置

Before you begin

- 验证您将发布的配置版本与您发布到的设备的 AsyncOS 版本是否兼容。请参阅位于以下网址的兼容性矩阵：
  http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。
- 在每个目标网络安全设备上，将网络安全设备上的现有配置备份到一个配置文件。有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

步骤 1 在源网络安全设备中保存配置文件。

有关保存来自网络安全设备的配置文件的说明，请参阅《思科网络安全设备 AsyncOS 用户指南》。

步骤 2 在安全管理设备窗口中，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 3 点击**立即发布配置 (Publish Configuration Now)**。

步骤 4 “系统生成的作业名称”(System-generated job name) 在默认情况下处于选中状态，或者请输入作业名称（不超过 80 个字符）。

步骤 5 对于**要发布的主配置 (Configuration Master to Publish)**，请选中**高级文件选项 (Advanced file options)**。

步骤 6 点击**浏览 (Browse)** 以选择在步骤 1 中保存的文件。

步骤 7 从“网络设备”(Web Appliances) 下拉列表中，选择**在列表中选择设备 (Select appliances in list)** 或**分配给主配置的所有设备 (All assigned to Master)**，然后选择您要将配置文件发布到的设备。

步骤 8 点击**发布 (Publish)**。

高级文件发布：稍后发布

Before you begin

- 验证您将发布的配置版本与您发布到的设备的 AsyncOS 版本是否兼容。请参阅位于以下网址的兼容性矩阵：
  http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。
- 在每个目标网络安全设备上，将网络安全设备上的现有配置备份到一个配置文件。有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

步骤 1 在源网络安全设备中保存配置文件。

有关保存来自网络安全设备的配置文件的说明，请参阅《思科网络安全设备 AsyncOS 用户指南》。

步骤 2 在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 3 单击**安排作业 (Schedule a Job)**。

步骤 4 **系统生成的作业名称 (System-generated job name)** 在默认情况下处于选中状态，或者请输入作业名称（不超过 80 个字符）。

步骤 5 输入要发布配置的日期和时间。

步骤 6 对于**要发布的主配置 (Configuration Master to Publish)**，请选择**高级文件选项 (Advanced file options)**，然后单击**浏览 (Browse)**，以选择在步骤 1 中保存的配置文件。

步骤 7 从“网络设备”(Web Appliances) 下拉列表中，选择**在列表中选择设备 (Select appliances in list)** 或**分配给主配置的所有设备 (All assigned to Master)**，然后选择您要将配置文件发布到的设备。

步骤 8 单击**发布 (Publish)**。

查看发布作业的状态和历史记录

要查看	相应操作
已安排但尚未发生的发布作业的列表	依次选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**，然后查看**待定作业 (Pending Jobs)** 部分。
每台设备的最后发布的配置列表	依次选择**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，然后查看**最后发布的配置 (Last Published Configuration)** 信息。
当前正在进行的发布作业的状态	依次选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**，然后查看**发布进度 (Publishing Progress)** 部分。
至所有或任何设备的所有或任何发布作业的历史记录	请参阅查看发布历史记录

查看发布历史记录

查看发布历史记录有利于检查在发布期间可能发生的错误，或识别在配置的功能与目标设备上启用的功能之间的不匹配。

步骤 1 在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布历史记录 (Publish History)**。

步骤 2 要查看关于特定作业的其他详细信息，请单击“作业名称”(Job Name) 列中的特定任务名称。

步骤 3 查看更多信息：

- 要查看关于作业中的特定设备的状态详细信息，请单击**详细信息 (Details)** 链接。

此时将出现“网络设备发布详细信息”(Web Appliance Publish Details) 页面。

- 要查看关于作业中的特定设备的其他详细信息，请单击设备名称。

此时将出现**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)** 页面。

集中化升级管理

您可以使用单个安全管理设备 (SMA) 同时升级多个网络安全设备 (WSA)。您还可以为每台 WSA 应用不同软件升级。

- 为网络安全设备设置集中升级管理，第 22 页
- 选择并下载 WSA 升级，第 23 页

• 使用安装向导，第 24 页

为网络安全设备设置集中升级管理

请按照以下步骤，继续在此安全管理设备上配置集中升级服务。

• 启用集中升级管理器，第 22 页
• 将集中升级服务添加到每个托管 Web 安全设备，第 22 页

启用集中升级管理器

开始之前

- 在启用集中升级管理之前，应配置所有网络安全设备并确保其按预期工作。
- 您必须在每个将要接收集中升级的托管网络安全设备上逐一启用集中升级。

注释 要在 CLI 中启用集中升级，请使用

```
applianceconfig > services > [...] > 启用集中升级 > Y
```

- 请确保在安全管理设备上安装相应的功能密钥。

步骤 1 在安全管理设备上，选择**管理设备**页面，然后依次选择**集中服务 > 集中升级管理器**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用**。

步骤 4 提交并确认更改。

将集中升级服务添加到每个托管 Web 安全设备

在安全管理设备上启用集中升级管理器后，必须通过在各个托管 WSA 上启用集中升级，将所需的网络安全设备添加到升级管理器名录。

步骤 1 在安全管理设备上，选择**管理设备**页面，然后选择**集中服务 > 安全设备**。

步骤 2 如果您尚未添加网络安全设备，或者您需要为集中升级管理添加其他设备：

a) 点击**添加网络设备 (Add Web Appliance)**。

b) 在“设备名称 (Appliance Name)”和“IP 地址 (IP Address)”文本字段，键入设备名称和网络安全设备管理接口的 IP 地址。

注释 可以在“IP 地址”文本字段中输入 DNS 名称，但是当您点击**提交** 时，该名称将解析为 IP 地址。

c) 请务必选中**集中升级**。
d) 点击**建立连接 (Establish Connection)**。
e) 在要托管的设备上输入管理员账户的用户名和口令，然后点击**建立连接 (Establish Connection)**。

注释 输入登录凭证，以便将文件传输的公共 SSH 密钥从安全管理设备传递到远程设备。登录凭证不会存储在安全管理设备上。

等待该页面表格上方显示成功消息。

f) 点击“测试连接”(Test Connection)。

阅读表格上方的测试结果。

g) 点击**提交 (Submit)**。

对您希望添加到托管网络安全设备列表中的每个 WSA 重复此程序，同时启用集中升级管理。

步骤 3 要在已添加到托管设备列表中的 WSA 上启用集中升级管理：

a) 点击网络安全设备名称，打开“编辑网络安全设备设置”(Edit Web Security Appliance Settings) 页面。
b) 在“WSA 集中服务”部分选择**集中升级**。
c) 点击**提交 (Submit)**。

对您希望启用集中升级管理的每个 WSA 重复此程序。

步骤 4 确认您的更改。

下一步做什么

有关向托管设备列表添加设备和编辑托管设备列表的详细信息，请参阅关于添加托管设备。

选择并下载 WSA 升级

步骤 1 在安全管理设备上，选择**网络**页面，然后依次选择**实用程序 > 集中升级**。

列出最近为升级选择的任何设备以及升级状态。

步骤 2 点击“集中升级”(Centralized Upgrade) 页面上的**升级设备 (Upgrade Appliances)** 按钮。

列出可升级的所有托管 WSA。

步骤 3 通过勾选列表中名称前面的框，选择要升级的每个网络安全设备。

步骤 4 点击**下载向导 (Download Wizard)** 或**下载并安装向导 (Download and Install Wizard)**。

“下载向导”可用于选择要下载到所选 WSA 的升级软件包；此操作仅供下载 - 您可以安装下载的软件包并稍后重新启动每个系统。

“下载和安装向导”可用于选择要下载的升级软件包并在所选 WSA 上立即进行安装。安装后，每个系统都会自动重启。

步骤 5 系统将显示已启动向导的“获取升级”(Fetch Upgrades) 页面；为所选 WSA获取所有可用的升级（“已完成获取可用升级”(Completed Fetching Available Upgrades) 显示在 WSA 矩阵的**状态 (Status)** 列）后，点击**下一步 (Next)** 继续。

步骤 6 “可用升级”(Available Upgrades) 页面列出每个所选 WSA 的所有可用升级版本；最多可以选择五个版本进行比较，然后点击**下一步 (Next)**。

步骤 7 向导的“升级选择”(Upgrade Selection) 页面会为每个 WSA 提供所选升级兼容性列表；请为每个 WSA 选中所需的升级版本，然后点击**下一步 (Next)**。

步骤 8 “摘要”(Summary) 页面列出每个所选 WSA 和升级版本的摘要信息；点击**下一步 (Next)** 继续向导。

步骤 9 完成一系列的下载检查后，例如连接状态，“审核”(Review) 页面将提供每个 WSA 的下载状态列表。点击**开始下载 (Summary)** 即可将升级软件包下载到每个所选 WSA。

“集中升级”(Centralized Upgrade) 页面在整个过程中显示下载状态信息。

下一步做什么

- **下载向导 (Download Wizard)** - 如果在此程序开始时点击此按钮，当下载完成时，依次选择**网络 (Web) > 实用程序 (Utilities) > 集中升级 (Centralized Upgrade)**，或点击浏览器窗口中的刷新页面按钮，可以刷新“集中升级”(Centralized Upgrade) 页面。

  除所有可升级的托管 WSA 列表之外，“集中升级”(Centralized Upgrade) 页面的另一部分现在会列出已下载升级软件包的所有 WSA。（您可以点击每个条目旁边显示的垃圾桶按钮，从该 WSA 中删除已下载的升级软件包。）

  任何时候，您都可以选择此列表中的一个或多个 WSA，然后点击“安装向导”(Install Wizard)，以开始在每个所选 WSA 上安装已下载的升级软件包；在 WSA 上完成安装后，将重新启动设备。有关使用此向导的信息，请参阅使用安装向导，第 24 页。

- **下载和安装向导 (Download and Install Wizard)** - 如果在此程序开始时点击此按钮，当下载完成时，会自动开始升级安装；有关此程序的信息，请参阅使用安装向导，第 24 页（从步骤 2 开始）。安装完成后，重新启动 WSA。

使用安装向导

“安装向导”(Install Wizard) 开始时，无论是自动作为下载和安装过程的一部分，还是在选择一个或多个具备已下载但尚未安装的升级软件包的 WSA 后点击“集中升级”(Centralized Upgrade) 页面上的“安装向导”按钮，请按照以下步骤继续安装。

步骤 1 如果安装之前下载的升级软件包：

a) 在“集中升级”(Centralized Upgrade) 页面的“具有已下载 AsyncOS 版本的网络设备”部分选择所需的 WSA（**网络 (Web) > 实用程序 (Utilities) > 集中升级 (Centralized Upgrade)**）。

b) 点击**安装向导 (Install Wizard)**。

步骤 2 在向导的“升级准备”(Upgrade Preparation) 页面上，对于每个所选 WSA：

- 如果要将 WSA 当前配置的备份副本保存到系统的配置目录，请勾选**升级之前将当前配置保存到配置目录**。
- 如果已选中**保存当前配置**选项，您可以勾选在**配置文件**中**屏蔽口令**，以在备份副本中屏蔽所有当前配置口令。请注意，不能使用 **Load Configuration** 命令来重新加载已屏蔽口令的备份文件。
- 如果已勾选**保存当前配置**选项，您可以在**通过邮件将文件发送到**字段中输入一个或多个邮件地址；备份配置文件副本会通过邮件发送至每个地址。多个地址之间用逗号分隔。

步骤 3 点击**下一步 (Next)**。

步骤 4 “升级摘要”(Upgrade Summary) 页面将列出每个所选 WSA 的升级准备信息；点击**下一步 (Next)** 继续向导。

步骤 5 完成一系列的设备检查后，例如连接状态，“审核”(Review) 页面将提供每个 WSA 的安装状态列表。您可以取消选择显示错误的设备。点击**开始安装 (Begin Install)**，以开始将升级软件包安装到每个所选 WSA。

您将返回“集中升级”(Centralized Upgrade) 页面，此页面显示安装状态信息。

注释 安装完成后，将重新启动每个 WSA。

下一步做什么

注释 或者，您也可以为任何之前从 WSA 下载的软件包运行安装程序。也就是说，WSA 的**系统管理 > 系统升级**页面上将列出已下载的升级软件包以及“安装”按钮。有关详细信息，请参阅《思科网络安全设备用户指南》中的“升级和更新 AsyncOS 和安全服务组件”。

查看网络安全设备状态

- 比较启用的功能 ， 第 13 页
- 查看网络设备的状态摘要 ， 第 25 页
- 查看各台网络安全设备的状态 ， 第 25 页
- 网络设备状态详细信息 ， 第 26 页

查看网络设备的状态摘要

网络 > 实用程序 > 网络设备状态页面提供连接到您的安全管理设备的网络安全设备的全面概要。

“网络设备状态”(Web Appliance Status) 页面显示连接的网络安全设备列表，包括设备名称、IP 地址、AsyncOS 版本、上次发布的配置信息（用户、作业名称和配置版本）、启用或禁用的安全服务数和连接的设备总数。警告图标指示何时需要注意连接的某台设备。

查看各台网络安全设备的状态

“设备状态”(Appliance Status) 页面提供每台连接设备的状态的详细视图。

要在“网络设备状态”(Web Appliance Status) 页面查看管理的网络安全设备的详细信息，请点击设备的名称。

状态信息包括关于连接的网络安全设备的常规信息、其发布的配置、发布历史记录、功能密钥状态等。

Note 只有支持集中管理的计算机才会显示数据。

Note 如果网络安全设备上不同版本的“可接受的使用控制引擎”与安全管理设备上的版本不匹配，将显示警告消息。如果网络安全设备上禁用或不存在该服务，将显示“N/A”。

网络设备状态详细信息

此页面上的大多数信息都由网络安全设备推送：

- 系统状态信息（正常运行时间、设备型号和序列号、AsyncOS 版本、构建日期、AsyncOS 安装日期和时间以及主机名）
- 配置发布历史记录（发布日期/时间、作业名称、配置版本、发布结果和用户）
- 集中报告状态，包括上次尝试传输数据的时间
- 网络安全设备中的功能状态（各项功能是否已启用、功能密钥状态）
- 托管和管理设备上可接受的使用控制引擎版本
- 网络安全设备上的“AnyConnect 安全移动 (AnyConnect Secure Mobility)”设置
- 此网络安全设备连接的思科身份服务引擎 (ISE) 服务器。
- 网络安全设备的代理设置（上游代理和代理的 HTTP 端口）
- 身份验证服务信息（服务器、方案、领域和顺序；是否支持透明用户身份识别；以及如果身份验证失败，是阻止还是允许通信）

Tip “网络设备状态”(Web Appliance Status) 页面可能需要几分钟，才会反映网络安全设备中最近发生的配置更改。要立即刷新数据，请点击**刷新数据 (Refresh Data)** 链接。页面上的时间戳将向您告知最后刷新数据的时间。

新 Web 界面中的系统运行状况控制面板

在设备上，选择**监控 (Monitoring)** > **系统运行状况 (System Health)** 以监控系统状态。该页面显示网络安全设备的当前状态和配置。

注释 包含所有严重和警告警报的系统运行状况控制面板仅在 AsyncOS 14.0 及更高版本中可用。

您可以根据时间范围（日期、昨天、自定义范围）对页面内容进行排序。在使用自定义范围时，设备允许选择一周的日期。

该页面显示了连接到 AsyncOS 的网络安全设备总数，设备上的严重和警告警报的计数。

要搜索所选设备，必须使用**搜索**功能。

要按升序和降序对设备进行排序，点击**代理名称 (Proxy Name)**。但是，您只能根据**代理名称 (Proxy Name)** 字段按升序和降序对行进行排序。

注释 如果设备尚未与思科安全管理器建立连接，则该行会突出显示，如果将鼠标悬停在该行上，则会显示停止图标。

显示的详细信息包括：

- 代理名称 (Proxy Name) - 显示网络安全设备代理名称。
- 硬件 (Hardware) - 显示设备的所有硬件严重和警告警报。您必须点击警报才能查看包含所选警报信息的弹出窗口。要获取有关警报的详细信息，您必须点击弹出窗口中可用的**硬件 (Hardware)** 链接。要导航到所选设备的系统状态页面，请选择弹出窗口中显示的**转到设备 (Go To Appliance)** 链接。但是，您必须要登录才能查看状态页面。
- 服务 (Services) - 显示设备的所有服务关键和警告警报。您必须点击警报才能查看有关所选警报的其他信息。您必须点击警报才能查看包含所选警报信息的弹出窗口。要获取有关警报的详细信息，您必须点击弹出窗口中的**系统 (System)** 链接。要导航到所选设备的系统状态页面，请选择弹出窗口中显示的**转到设备 (Go To Appliance)** 链接。但是，您必须要登录才能查看状态页面。
- 峰值 RPS (Peak RPS) - 显示所选设备的每秒请求数。
- 峰值加密 RPS (Peak Decrypted RPS) - 显示所选时间段内设备上已解密请求的峰值 RPS。
- 峰值客户端连接数 (Peak Client Connections) - 显示设备上的客户端峰值连接数。
- 峰值服务器连接 (Peak Server Connections) - 显示设备上的服务器端峰值连接数。

在 AsyncOS 14.0 中，您现在可以在页面中查看网络安全设备的当前状态和配置。您必须选择**监控 (Monitoring)** > **系统运行状况 (System Health)** 来监控网络安全设备的系统状态。

- 在 AsyncOS 14.1.0 中，根据所选 WSA 的活动日期来显示接口上可用的网络安全设备跟踪数据。根据设备可用的日期来显示所选设备的所有状态消息。
- AsyncOS 14.1.0 使用颜色代码来显示网络安全设备状态。使用的颜色代码如下：
  - 绿色状态 - API 服务器和 trailblazer 已启动并正在运行
  - 灰色状态 - API 服务器状态或和 trailblazer 状态为正常运行。但是，设备连接未使用思科安全邮件和 Web 管理器来建立。
  - 红色状态 - API 服务器状态和 trailblazer 状态为关闭或两者均关闭。

准备和管理 URL 类别集更新

要确保系统具有可用于管理网络使用的最新预定义 URL 类别集，可以不定期更新网络使用控制 (WUC) 的 URL 类别集：默认情况下，网络安全设备自动从思科下载 URL 类别集更新，并且安全管理设备可在几分钟内自动从托管网络安全设备接收这些更新。

由于这些更新可能会影响现有的配置和设备行为，因此您应提前准备这些更新，并在进行更新后采取相应操作。

您应该采取的行动包括：

- 了解 URL 类别集更新的影响 , on page 28
- 确保您将收到关于 URL 类别集更新的通知和警报 , on page 28
- 为新类别和已更改的类别指定默认设置 , on page 28
- 在更新 URL 类别集时，检查您的策略和身份/识别配置文件设置 , on page 29

了解 URL 类别集更新的影响

当 URL 类别集更新发生时，它们可能更改主配置中现有策略的行为。

有关更新 URL 类别集前后应采取的操作的重要信息，请参阅《思科网络安全设备 AsyncOS 用户指南》中“URL 过滤器”一章的“管理 URL 类别集的更新”部分（见文档中提供的链接）。类别说明在同一章的“URL 类别说明”部分。

确保您将收到关于 URL 类别集更新的通知和警报

要接收	相应操作
URL 类别集更新的提前通知	立即注册以接收有关您的 Cisco 安全邮件和网页管理器设备的通知，通知将包括关于 URL 类别集更新的通知。请参阅思科通知服务。
警报（当URL类别集更新已影响现有策略设置时）	转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报**，并确保将您配置为接收“系统”(System) 类别中的警告级别警报。有关警报的详细信息，请参阅管理警报

为新类别和已更改的类别指定默认设置

在更新 URL 类别集之前，应指定提供 URL 过滤的各个策略中新合并类别的默认操作，或从已配置这些设置的网络安全设备中导入配置。

有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》或网络安全设备在线帮助“URL 过滤器”章节中的“选择新类别和已更改类别的默认设置”部分。

在更新 URL 类别集时，检查您的策略和身份/识别配置文件设置

URL 类别集更新触发两种类型的警报：

- 有关类别更改的警报
- 有关策略因类别更改而发生更改或被禁用的警报

在接收关于 URL 类别集更改的警报时，您应该检查基于 URL 类别的现有策略和身份/识别配置文件，以确保其仍然符合您的策略目标。

有关可能需要您注意的更改类型的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》中的“响应关于 URL 类别集更新的警报”部分。

应用可视性与可控性 (AVC) 更新

SMA 将自动使用它管理的大多数网络安全设备上存在的 AVC 引擎版本。

使用 CLI 更新 WBRS 和 AVC 数据

您可以使用 `wsa_updatesconfig` 命令通过使用 CLI 来更新 WBRS、AVC 或 WBRS 和 AVC 数据。

wsa_updatesconfig

说明

该命令会强制更新安全邮件和 Web 管理器上的 WBRS、AVC 或 WBRS 和 AVC 数据。以下子命令可用：

- WBRS - 强制更新思科安全邮件和 Web 管理器上的 WBRS 数据。
- AVC - 强制更新思科安全邮件和 Web 管理器上的 AVC 数据。
- BOTH - 强制更新思科安全邮件和 Web 管理器上的 WBRS 和 AVC 数据。

使用情况

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

```
mail1.example.com> wsa_updatesconfig
Choose the operation you want to perform:
- WBRS - force an update of WBRS data on this appliance.
- AVC - force an update of AVC data on this appliance.
- BOTH - force an update for WBRS and AVC on this appliance
```

对配置管理问题进行故障排除

- 在主配置身份/识别配置文件中，组不可用 , on page 30
- 主配置、访问策略、Web 信誉和防恶意软件设置页面设置不符合预期, on page 30
- 配置发布失败故障排除 , on page 31

在主配置身份/识别配置文件中，组不可用

问题

在**网络 (Web) > 主配置 (Configuration Master) > 身份/识别配置文件 (Identities/Identification Profiles)** 中，“策略成员身份定义”(Policy membership definition) 页面不显示“选定的组和用户”(Selected groups and Users) 下的“组”(Groups) 选项。

解决方案

如果您有多个网络安全设备：在每个 WSA 上，在“网络”>“身份验证”中，请确保领域名称在所有 WSA 间是唯一的，除非同名领域的所有设置都是相同的。

Tip 要查看各个 WSA 的领域名称，请转到**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，点击每个设备名称，然后滚动至“详细信息”(Details) 页面底部。

主配置、访问策略、Web 信誉和防恶意软件设置页面设置不符合预期

问题

主配置中的**访问策略 > 网络信誉和防恶意软件设置**页面缺少预期的设置，包括“网络信誉得分”阈值设置和选择防恶意软件扫描引擎的功能。或者，在网络安全设备上使用自适应安全时包括这些设置。

解决方案

可用的选项取决于是否在“网络”(Web)>“实用程序”(Utilities)>“安全服务显示”(Security Services Display) 设置中为该主配置选择了“自适应安全”(Adaptive Security)。

排除在为主配置导入现有配置时的问题

问题

升级到主配置 11.8 后，如果将现有配置导入到新的主配置，设备将重定向到网络安全设备 (WSA_Sandbox) 登录页面。

解决方案

将设备升级到支持主配置 11.8 的版本后，必须将网络安全设备关联到安全管理设备才能从现有主配置导入配置。

注释 如果在加载配置文件时遇到任何与策略相关的问题，请检查设备上的 GUI 日志。

配置发布失败故障排除

问题

发布配置失败。

解决方案

查看**网络 > 实用程序 > 网络设备状态**页面。在下列情况下，发布将失败：

- “网络设备服务”(Web Appliance Service) 列中的状态与“服务是否显示在管理设备上？”(Is Service Displayed on Management Appliance?) 列中的状态之间存在差异。
- 两列都显示已启用功能，但相应的功能密钥未处于活动状态（例如，已过期）。
- 主配置版本应与网络安全设备上的 AsyncOS 版本匹配。如果网络安全设备中的设置与主配置中的设置不匹配，向更新的网络安全设备发布较早的主配置版本可能会失败。即使“网络设备状态”(Web Appliance Status) 页面未指示任何差异，也可能会出现失败。

后续操作：

- 查看发布历史记录, on page 21
- 比较启用的功能 , on page 13
- 启用要发布的功能 , on page 14

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。