思科网络安全设备 **AsyncOS 11.0** 用户指南

首次发布日期: 2017 年 4 月 28 日

上次修改日期: 2017 年 5 月 24 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。版权所有。版权所有 © 1981，加州大学董事会。

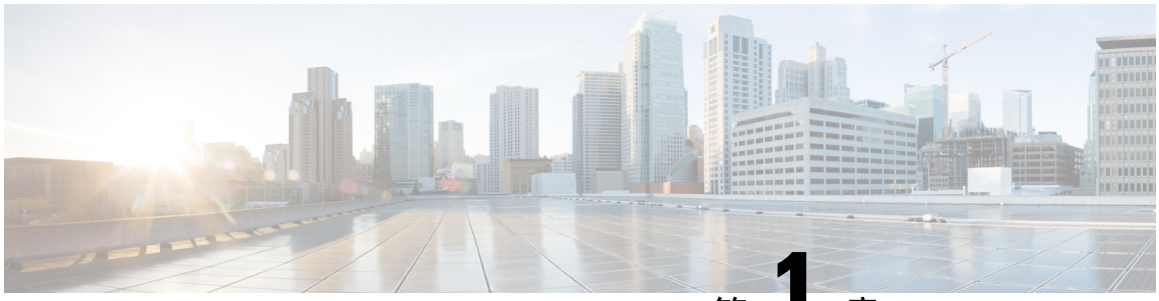
无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

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，请访问此网址：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)

目 录



第 1 章

产品和版本简介

本章包含以下部分：

网络安全设备简介

思科网络安全设备拦截和监控互联网流量并应用策略，以帮助保障内部网络安全，防范恶意软件、敏感数据丢失、工作效率损失和其他基于互联网的威胁。

新增内容

AsyncOS 11.0 中的新增内容

特性	说明
思科防御协调器集成	您可以将设备连接到思科防御协调器，并分析设备的安全策略配置，从而识别和解决策略不一致以及模型策略更改以验证其影响，同时协调策略更改以实现一致性并维持清晰的安全态势。思科防御协调器是一个基于云的平台，可帮助网络运营人员通过管理思科安全设备的安全策略来建立和维护端到端安全态势。 有关详细信息，请参阅将设备连接到思科防御协调器， 第 51 页。
CTA 上简化的设备注册	可以使用 **CTA 模板 (CTA Template)** 选项自动选择将 W3C 日志发送到思科认知威胁分析 (CTA) 系统所需的字段和条件。 有关详细信息，请参阅配置 CTA 特定的自定义 W3C 日志， 第 363 页。

特性	说明
辅助 DNS 服务器	还可以指定辅助 DNS 服务器来解析主名称服务器未解析的主机名查询。还可以设置服务器的优先级。当主DNS服务器返回以下错误时，辅助 DNS 服务器将接收主机名查询： • 没有错误，未收到应答部分。 • 服务器未能完成请求，没有应答部分。 • 名称错误，未收到应答部分。 • 函数未执行。 • 服务器拒绝应答查询。 有关详细信息，请参阅编辑 DNS 设置，第 41 页。
`supportrequest` 命令增强	如果您在使用 `supportrequest` 命令时，在可选步骤中指定服务请求编号，则可以发送需要自动附加到服务请求的一组系统和配置信息。 有关详细信息，请参阅网络安全设备 CLI 命令，第 457 页。
虚拟设备增强	虚拟设备现在可以部署在 Microsoft Hyper-V 5.0 版本上。 请参阅可从http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html中获取的《思科内容安全虚拟设备安装指南》。

相关主题

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

使用设备 Web 界面

Web 界面浏览器要求

要访问 Web 界面，您的浏览器必须支持并启用为接受 JavaScript 和 cookie。它必须能够呈现包含级联样式表 (CSS) 的 HTML 页面。

思科网络安全设备遵循 YUI 所设置的目标环境：http://yuilibrary.com/yui/environments/

会话在处于不活动状态 30 分钟后自动超时。

Web 界面中的某些按钮和链接会导致其他窗口打开。因此，您可能需要配置浏览器的弹出窗口阻止设置，以便使用 Web 界面。

注释 每次只能使用一个浏览器窗口或选项卡编辑设备配置。此外，不要同时使用 Web 界面和 CLI 来编辑设备。从多个位置并行编辑设备会导致意外行为，因此不予支持。

启用对虚拟设备上的 Web 界面访问

默认情况下，虚拟设备上未启用 HTTP 和 HTTPS 接口。要启用这些协议，必须使用命令行界面。

步骤 1 访问命令行界面。请参阅访问命令行界面，第 453 页。

步骤 2 运行 `suspendtransfers` 命令。

在提示符处按下 Enter 以接受默认值。

查找 HTTP 和 HTTPS 的提示符，并启用您要使用的协议。

访问设备 Web 界面

如果您正在使用虚拟设备，请参阅启用对虚拟设备上的 Web 界面访问，第 3 页。

步骤 1 打开浏览器并输入网络安全设备的 IP 地址（或主机名）。如果先前未配置设备，请使用默认设置：

`https://192.168.42.42:8443`

-或者-

`http://192.168.42.42:8080`

其中 `192.168.42.42` 是默认 IP 地址，`8080` 是用于 HTTP 的默认管理端口设置，`8443` 是用于 `HTTPS` 的默认管理端口。

否则，如果当前配置了设备，请使用 M1 端口的 IP 地址（或主机名）。

注释 在连接到设备时必须使用端口号（默认情况下为端口 `8080`）。在访问 Web 界面时未能指定端口号，将导致使用默认端口 80。系统将显示“代理未经许可”(Proxy Unlicensed) 错误页面。

步骤 2 当出现设备登录屏幕时，请输入用户名和密码以访问设备。

默认情况下，设备随附以下用户名和密码：

- 用户名：**admin**
- 密码：**ironport**

如果您是第一次使用默认 **admin** 用户名登录，系统会提示您要立即更改密码。

步骤 3 要查看使用您的用户名的最近设备访问尝试列表（包括成功和失败登录），点击应用窗口右上角“登录为”(Logged in as) 条目前面的最近活动图标（分别对应于成功或失败的 **i** 或 **!**）。

通过 Web 界面确认更改

步骤 1 点击**确认更改 (Commit Changes)** 按钮。

步骤 2 如果选择“注释”(Comment) 字段，请在该字段中输入注释。

步骤 3 点击**确认更改 (Commit Changes)**。

注释 您可以进行多个配置更改，然后再确认所有更改。

清除 Web 界面中的更改

步骤 1 点击**确认更改 (Commit Changes)** 按钮。

步骤 2 点击**放弃更改 (Abandon Changes)**。

支持的语言

AsyncOS 可使用以下任何语言显示其 GUI 和 CLI：

- 德语
- 英语
- 西班牙语
- 法语
- 意大利语
- 日语
- 韩语
- 葡萄牙语
- 俄语
- 中文

- 闽南语

思科 SensorBase 网络

Cisco SensorBase 网络是一个威胁管理数据库，用于跟踪全球数百万个域并维护互联网流量的全局监视列表。SensorBase 为思科提供对已知互联网域的可靠性的评估。网络安全设备使用 SensorBase 数据馈送提高 Web 信誉分数的准确性。

SensorBase 优势和隐私

参与 Cisco SensorBase 网络意味着思科收集数据并与 SensorBase 威胁管理数据库共享该信息。此数据包括有关请求属性以及设备如何处理请求的信息。

思科意识到维护隐私的重要性，因此不收集或使用个人或机密信息，例如用户名和密码。此外，主机名后跟的文件名和 URL 属性会进行模糊处理，以确保机密性。当提到已解密 HTTPS 事务时，SensorBase 网络仅在证书中收到服务器名称的 IP 地址、Web 信誉分数和 URL 类别。

如果您同意参与 SensorBase 网络，则从您的设备发送的数据使用 HTTPS 安全地进行传输。共享数据可改善思科应对基于 Web 的威胁和保护企业环境抵御恶意软件活动的能力。

启用思科 SensorBase 网络参与

注释 在系统设置期间，默认情况下将启用标准 SensorBase 网络参与。

步骤 1 依次选择**安全服务 (Security Services) > SensorBase**。

步骤 2 验证是否启用了 SensorBase 网络参与。

当其禁用时，不会将设备收集的任何数据发回到 SensorBase 网络服务器。

步骤 3 在“参与级别”(Participation Level) 部分中，选择以下级别之一：

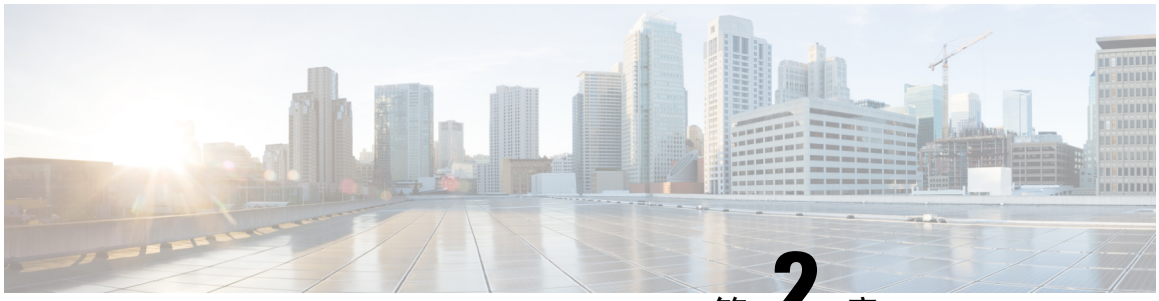
- **受限 (Limited)**。基本参与将概括服务器名称信息并将 MD5 散列的路径段发送到 SensorBase 网络服务器。
- **标准版 (Standard)**。增强的参与会将包含未模糊处理的路径段的整个 URL 发送到 SensorBase 网络服务器。此选项帮助提供更稳健的数据库，并且持续改善 Web 信誉分数的完整性。

步骤 4 在“AnyConnect 网络参与”(AnyConnect Network Participation) 字段中，选择是否包含从客户端（使用 Cisco AnyConnect 客户端连接到网络安全设备）收集的信息。

AnyConnect 客户端使用 Secure Mobility 功能将其 Web 流量发送到设备。

步骤 5 在“已排除的域和 IP 地址”(Excluded Domains and IP Addresses) 字段中，随意输入要从发送到 SensorBase 服务器的流量中排除的任何域或 IP 地址。

步骤 6 提交并确认更改。



第 2 章

连接、安装和配置

本章包含以下部分：

连接、安装和配置概述

网络安全设备提供三种操作模式：标准模式、云网络安全连接器模式和思科防御协调器模式。

- 网络安全设备的标准操作模式包括现场 Web 代理服务和第 4 层流量监控；这些服务在云网络安全连接器模式下不可用。
- 在云网络安全连接器模式下，设备连接到思科云网络安全 (CWS) 代理并将流量路由到思科云网络安全代理，在代理中执行网络安全策略。
- 在思科防御协调器模式下，设备装载到思科防御协调器上。策略管理和（可选）报告通过思科防御协调器实施。有关配置更改和限制的详细信息，请参阅思科防御编排器模式下的配置变更与约束， 第 52 页。

设备具有多个网络端口，其中分配的每个端口用于管理一个或多个特定数据类型。

设备使用网络路由、DNS、VLAN 以及其他设置和服务来管理网络连接和流量拦截。您可以通过系统设置向导配置基本的服务和设置，在设备的 Web 界面中修改设置并配置其他选项。

部署虚拟设备

要部署虚拟网络安全设备，请参阅位于以下位置的《思科内容安全虚拟设备安装指南》：http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html。

从物理设备迁移到虚拟设备

要将部署从物理设备迁移到虚拟设备，请参阅之前主题中引用的虚拟设备安装指南以及针对 AsyncOS 版本的版本说明。

比较操作模式

下表列出了标准和云连接器模式下可用的各种菜单命令，从而显示了每个模式下可用的各种功能。

要查看思科防御编排器模式下可用的功能，请参阅思科防御编排器模式下的配置变更与约束，第 52 页。

菜单	在标准模式下可用	在云连接器模式下可用
报告	系统状态 概述 用户 用户计数 网站 URL 类别 应用可视性 防恶意软件 高级恶意软件防护 文件分析 AMP 判定更新 客户端恶意软件风险 Web 信誉过滤器 第 4 层流量监控器 按用户地点分类的报告 Web跟踪 系统容量 系统状态 计划的报告 存档的报告	系统状态

菜单	在标准模式下可用	在云连接器模式下可用
Web安全管理器	识别配置文件 云路由策略 SaaS策略 解密策略 路由策略 访问策略 总体带宽限制 思科数据安全 出站恶意软件扫描 外部数据丢失预防 SOCKS 策略 自定义 URL 类别 定义时间范围和配额 旁路设置 第 4 层流量监控器	识别配置文件 云路由策略 外部数据丢失预防 自定义 URL 类别
安全服务	Web 代理 FTP代理 HTTPS代理 SOCKS 代理 PAC 文件托管 可接受的使用控制 防恶意软件和信誉 数据传输过滤器 AnyConnect 安全移动 终端用户通知 L4 通信监控 传感器群 报告 思科 Cloudlock 思科感知威胁分析	Web 代理

菜单	在标准模式下可用	在云连接器模式下可用
网络	接口 透明重定向 路由 DNS 高可用性 内部 SMTP 中继 上游代理 外部 DLP服务器 证书管理 身份验证 SaaS的标识提供程序 身份服务引擎	接口 透明重定向 路由 DNS 高可用性 内部 SMTP 中继 外部 DLP服务器 证书管理 身份验证 计算机 ID 服务 云连接器
系统管理	策略跟踪 告警信息 日志订阅 返回地址 SSL 配置 用户 网络接入 时区 时间设置 配置摘要 配置文件 功能密钥设置 功能密钥 升级和更新设置 系统升级 系统设置向导 FIPS 模式 后续步骤	告警信息 日志订阅 SSL 配置 用户 网络接入 时区 时间设置 配置摘要 配置文件 功能密钥 升级和更新设置 系统升级 系统设置向导

菜单	在标准模式下可用	在云连接器模式下可用
思科 CWS 门户（仅在混合网络安全模式下可用）	不适用	不适用

连接、安装和配置的任务概述

任务	更多信息
• 将设备连接到互联网流量。	连接设备，第 12 页
• 收集和记录设置信息。	收集设置信息，第 14 页
• 运行“系统设置向导”(System Setup Wizard)。	系统设置向导，第 16 页
• 配置 HTTPS 代理设置、身份验证领域和标识配置文件。必须为混合网络安全模式完成此步骤。	启用 HTTPS 代理，第 202 页 身份验证领域，第 86 页 标识配置文件和身份验证，第 120 页
• （可选）连接上游代理。	上游代理，第 23 页

连接设备

开始之前

- 要安装设备，请连接设备以进行管理，连接设备电源，遵守设备硬件指南中的说明。有关适用于您模型的此文档的位置，请参阅文档集，第 475 页。
- 如果计划将设备物理连接到 WCCP v2 路由器以进行透明重定向，请先验证 WCCP 路由器是否支持第 2 层重定向。
- 请注意思科配置建议：
  - 如有可能，请使用单工布线（对传入和传出流量使用不同电缆），以增强性能和安全性。

步骤 1 如果尚未连接管理接口，请执行此操作：

以太网端口	说明
第 1 个月	将 M1 连接到其可以执行以下操作的位置： • 发送和接收管理流量。 • （可选）发送和接收 Web 代理数据流量。 您可以将笔记本电脑直接连接到 M1 来管理设备。 要使用主机名 (http://hostname:8080) 连接到管理接口，请将设备主机名和 IP 地址添加到 DNS 服务器数据库。
P1 和 P2（可选）	• 可用于出站管理服务流量，但不可用于管理。 • 启用**将 M1 端口仅用于管理用途**（“网络”>“接口”页面）。 • 为使用数据接口的服务设置路由。

步骤 2 （可选）将设备直接或通过透明重定向设备连接到数据流量：

以太网端口	显式转发	透明重定向
P1/P2	仅 P1： • 启用**将 M1 端口仅用于管理用途**。 • 将 P1 和 M1 连接到不同的子网。 • 使用双工电缆将 P1 连接到内部网络和互联网，以同时接收入站和出站流量。 P1 和 P2 • 启用 P1。 • 将 M1、P1 和 P2 连接到不同的子网。 • 将 P2 连接到互联网以接收入站互联网流量。 在运行“系统设置向导”(System Setup Wizard) 后，启用 P2。	设备：WCCP v2 路由器： • 对于第 2 层重定向，请以物理方式将路由器连接到 P1/P2。 • 对于第 3 层重定向，请注意通用路由封装可能存在的性能问题。 • 在设备上创建 WCCP 服务。 设备：第 4 层交换机： • 对于第 2 层重定向，请以物理方式将交换机连接到 P1/P2。 • 对于第 3 层重定向，请注意通用路由封装可能存在的性能问题。 **注释** 设备不支持内联模式。
M1（可选）	如果禁用**将 M1 端口仅用于管理用途**，则 M1 是数据流量的默认端口。	不适用

步骤 3 （可选）要监控第 4 层流量，请将设备连接到位于代理端口之后和对客户端 IP 地址执行网络地址转换 (NAT) 的任何设备之前的 TAP、交换机或集线器：

以太网端口	说明
T1/T2	要允许第 4 层流量监控阻止，请将第 4 层流量监控置于网络安全设备所在的网络上。 **建议的配置：** **“设备”(Device)：“网络 TAP”(Network TAP)：** • **将 T1 连接到网络 TAP 以接收出站客户端流量。** • **将 T2 连接到网络 TAP 以接收入站互联网流量。** 其他选项： “设备”(Device)：“网络 TAP”(Network TAP)： • 在 T1 上使用双工电缆接收入站和出站流量。 “设备”(Device)：交换机上的跨网络端口或镜像端口 • 连接 T1 以接收出站客户端流量并连接 T2 以接收入站互联网流量。 • （优先级较低）使用半双工或全双工电缆连接 T1 以同时接收入站和出站流量。 “设备”(Device)：“集线器”(Hub)： • （优先级最低）使用双工电缆连接 T1 以同时接收入站和出站流量。 设备侦听这些接口上的所有 TCP 端口上的流量。

步骤 4 连接设备上游的外部代理以允许外部代理从设备接收数据。

下一步做什么

收集设置信息，第 14 页

相关主题

- 启用或更改网络接口，第 25 页
- 将 P2 数据接口用于 Web 代理数据，第 28 页
- 添加和编辑 WCCP 服务，第 34 页
- 配置透明重定向，第 31 页
- 上游代理，第 23 页

收集设置信息

您可以使用以下工作表记录您在运行“系统设置向导”(System Setup Wizard)时将需要的配置值。有关每个属性的详细信息，请参阅系统设置向导参考信息，第 17 页。

系统设置向导工作表			
特性	值	特性	值
设备详细信息 (Appliance Details)		**路由**	
默认系统主机名		**管理流量**	
本地 DNS 服务器 (Local DNS Server[s]) **（如果使用的不是互联网根服务器，则此属性必填）**		默认网关	
DNS 服务器 1		（可选）静态路由表名称 (Static Route Table Name)	
（可选）DNS 服务器 2 (DNS Server 2)		（可选）静态路由表目标网络 (Static Route Table Destination Network)	
（可选）DNS 服务器 3 (DNS Server 3)		（可选）标准服务路由器地址 (Standard Service Router Addresses)	
（可选）时间设置 (Time Settings)		**（可选）数据流量 (Data Traffic)**	
网络时间协议服务器 (Network Time Protocol Server)		默认网关	
（可选）外部代理详细信息 (External Proxy Details)		静态路由表名称 (Static Route Table Name)	
代理组名 (Proxy Group Name)		静态路由表目标网络 (Static Route Table Destination Network)	
代理服务器地址 (Proxy Server Address)		**（可选）WCCP 设置**	
代理端口号 (Proxy Port Number)		WCCP 路由器地址 (WCCP Router Address)	
接口详细信息		WCCP 路由器密码	

系统设置向导工作表			
特性	值	特性	值
管理 (M1) 端口 (Management [M1] Port)		**管理设置**	
IPv4 地址 (IPv4 Address)（必填） IPv6 地址 (IPv6 Address)（可选）		管理员密码	
Network Mask		系统警报收件人 (Email System Alerts To)	
Hostname		（可选）SMTP 中继主机 (SMTP Relay Host)	
（可选）数据 (P1) 端口 (Data [P1] Port)			
IPv4（可选） IPv6 地址 (IPv6 Address)（可选）			
Network Mask			
Hostname			

系统设置向导

开始之前

- 将设备连接到网络和设备。请参阅连接设备，第 12 页。
- 完成“系统设置向导”(System Setup Wizard) 工作表。请参阅收集设置信息，第 14 页。
- 如果要设置虚拟设备：
  - 使用 `loadlicense` 命令加载虚拟设备许可证。有关完整信息，请参阅位于以下位置的《思科内容安全虚拟设备安装指南》：http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html。
  - 启用 HTTP 和/或 HTTPS 接口：在命令行界面 (CLI) 中运行 `interfaceconfig` 命令。
- 请注意，“系统设置向导”(System Setup Wizard) 中使用的每个配置项的参考信息可在系统设置向导参考信息，第 17 页中获取。

警告 请仅在首次安装设备时或在要完全覆盖现有配置的情况下使用“系统设置向导”(System Setup Wizard)。

步骤 1 打开浏览器并输入网络安全设备的 IP 地址。首次运行“系统设置向导”(System Setup Wizard) 时，请使用默认 IP 地址：

`https://192.168.42.42:8443`

-或者-

`http://192.168.42.42:8080`

其中 `192.168.42.42` 是默认 IP 地址，`8080` 是用于 HTTP 的默认管理端口设置，`8443` 是用于 HTTPS 的默认管理端口。

否则，如果当前配置了设备，请使用 M1 端口的 IP 地址。

步骤 2 当出现设备登录屏幕时，请输入用户名和密码以访问设备。默认情况下，设备随附以下用户名和密码：

- 用户名：`admin`
- 密码：`ironport`

步骤 3 必须立即更改密码。

步骤 4 依次选择**系统管理 (System Administration) > 系统设置向导 (System Setup Wizard)**。

如果已经配置设备，系统将提示您需要重置配置。要继续使用系统设置向导，请选中**重置网络设置 (Reset Network Settings)**，然后点击**重置配置 (Reset Configuration)** 按钮。设备将重置并且浏览器将刷新为设备主屏幕。

步骤 5 阅读并接受最终用户许可协议的条款。

步骤 6 点击**开始设置 (Begin Setup)** 继续操作。

步骤 7 根据需要使用以下章节中提供的参考表来配置所有的设置。请参阅系统设置向导参考信息，第 17 页。

步骤 8 查看配置信息。如果您需要更改某个选项，请点击该部分中的**编辑 (Edit)** 按钮。

步骤 9 点击**安装这个配置 (Install This Configuration)**。

下一步做什么

安装配置后，应显示后续步骤 *(Next Steps)* 页面。但是，根据设置期间配置的 IP、主机名或 DNS 设置，在此阶段您可能会失去与设备的连接。如果浏览器中显示“找不到页面”(Page not found) 错误，请更改 URL 以反映任何新地址设置并重新加载页面。然后，继续执行要执行的任何设置后任务。

系统设置向导参考信息

- 网络/透明连接设置， 第 21 页
- 网络/管理设置， 第 21 页

网络/系统设置

属性	说明
默认系统主机名	系统主机名是用于在以下区域中标识设备的完全限定主机名： • 命令行界面 (CLI) • 系统警报 • 最终用户通知和确认页面 • 在网络安全设备加入 Active Directory 域的情况下形成计算机 NetBIOS 名称时。 系统主机名不直接对应接口主机名，并且未由客户端用于连接到设备。
DNS 服务器	• **使用互联网的根 DNS 服务器** - 当设备无权访问网络上的 DNS 服务器时，您可以选择使用互联网根 DNS 服务器进行域名服务查找。 注释 互联网根 DNS 服务器将不解析本地主机名。如果需要设备解析本地主机名，必须使用本地 DNS 服务器，或者使用 CLI 将相应的静态条目添加到本地 DNS。 • **使用这些 DNS 服务器** - 提供设备可用于解析主机名的本地 DNS 服务器的地址。 有关这些设置的详细信息，请参阅 DNS 设置， 第 40 页。
NTP 服务器	用于将系统时钟与网络或互联网上的其他服务器同步的网络时间协议(NTP)服务器。 默认设置为 time.sco.cisco.com。
时区	提供设备所在位置的时区信息；影响邮件信头和日志文件中的时间戳。
设备运行模式	• **标准** - 用于标准的内部策略实施。 • **云网络安全连接器** - 主要用于将流量定向到思科云网络安全服务以进行策略实施和威胁防御。 • **混合网络安全** - 与思科云网络安全服务一起用于云和内部策略实施和威胁防御。 有关这些操作模式的详细信息，请参阅比较操作模式， 第 8 页。

网络/网络环境

注释 当在包含其他代理服务器的网络中使用网络安全设备时，建议将网络安全设备放在代理服务器下游更靠近客户端的位置。

属性	说明
网络上是否有其他 Web 代理？(Is there another web proxy on your network?)	网络上是否有其他代理，以致 流量必须通过该代理？它是位于网络安全设备的上游吗？ 如果上述两点的答案均为是，请选中该复选框。这允许您为一个上游代理创建代理组。您可以稍后添加更多上游代理。
代理组名 (Proxy group name)	用于标识设备上的代理组的名称。
地址	上游代理服务器的主机名或 IP 地址。
端口	上游代理服务器的端口号。

相关主题

- 上游代理，第 23 页

网络/云连接器设置

需要确认页面名称和设置。

设置	说明
云网络安全代理服务器 (Cloud Web Security Proxy Servers)	云代理服务器 (CPS) 的地址，例如 proxy1743.scansafe.net。
故障处理 (Failure Handling)	如果 AsyncOS 无法连接到云网络安全代理，请选择**直接连接 (Connect directly)** 互联网，或者选择**丢弃请求 (Drop requests)**。
云网络安全授权方案 (Cloud Web Security Authorization Scheme)	授权事务的方法： • 网络安全设备公开 IPv4 地址。 • 每个事务随附的授权密钥。您可以在思科云网络安全门户中生成授权密钥。

网络/网络接口和连线

用于管理网络安全设备并在默认情况下用于代理（数据）流量的 IP 地址、网络掩码和主机名。

您可在连接到设备管理接口时使用此处（如果 M1 用于代理数据，则在浏览器代理设置中）指定的主机名，但是您必须在贵组织的 DNS 中注册主机名。

设置	说明
以太网端口 (Ethernet Port)	（可选）如果要对数据流量使用单独的端口，请选中**将 M1 端口仅用于管理**。 如果您仅配置用于管理流量的 M1 接口，则必须配置用于数据流量的 P1 接口。您还必须为管理流量和数据流量定义不同的路由。但是，即使 M1 接口同时用于管理和数据流量，您也可以配置 P1 接口。 只能在“系统设置向导”(System Setup Wizard) 中启用和配置 P1 端口。如果要启用 P2 接口，必须在完成“系统设置向导”(System Setup Wizard) 后执行此操作。
IP 地址/网络掩码 (IP Address / Netmask)	管理此网络接口上的网络安全设备时使用的 IP 地址和网络掩码。
主机名 (Hostname)	管理此网络接口上的网络安全设备时使用的主机名。

网络/L4 流量监控器接线

属性	说明
L4 流量监控器 (Layer-4 Traffic Monitor)	插入到“T”接口的有线连接的类型： • **双工 TAP (Duplex TAP)**。T1 端口同时接收传入和传出流量。 • **单工 TAP (Simplex TAP)**。T1 端口接收传出流量（从客户端到互联网），T2 端口接收传入流量（从互联网到客户端）。 思科建议尽可能使用单工，因为它可以提高性能和安全性。

管理流量和数据流量的网络/路由

注释 如果启用“将 M1 端口仅用于管理”(Use M1 port for management only)，则本节将具有单独的管理流量和数据流量部分；否则将显示联合部分。

属性	说明
默认网关	要用于通过管理接口和数据接口的流量的默认网关 IP 地址。

属性	说明
静态路由表	管理流量和数据流量的可选静态路由。可以添加多个路由。 • **名称** - 用于识别静态路由的名称。 • **内部网络** – 网络上此路由目标的 IPv4 地址。 • **内部网关** – 此路由的网关 IPv4 地址。路由网关必须与配置了该网关的管理接口或数据接口位于同一子网上。

网络/透明连接设置

注释 默认情况下，云连接器在透明模式下部署。这需要连接第 4 层交换机或第 2 版 WCCP 路由器。

属性	说明
第 4 层交换机或无设备 (Layer-4 Switch or No Device)	指定网络安全设备连接到第 4 层交换机以进行透明重定向，或者未使用任何透明重定向设备且客户端会将请求显式转发到设备。
WCCP v2 路由器	指定网络安全设备连接到第 2 版 WCCP 路由器。 如果将设备连接到第 2 版 WCCP 路由器，则必须至少创建一个 WCCP 服务。您可以在此屏幕上启用标准服务，或在完成“系统设置向导”(System Setup Wizard)（其中还可以创建多个动态服务）后启用此服务。 启用标准服务时，您还可以启用路由器安全性并输入密码。此处使用的密码必须用于同一服务组中的所有设备和 WCCP 路由器。 标准服务类型（也称为“网络缓存”服务）分配有固定 ID 0、固定重定向方法（按目标端口）和固定目标端口 80。 通过动态服务类型，您可以定义自定义 ID、端口号以及重定向和负载均衡选项。

网络/管理设置

属性	说明
管理员密码	用于访问网络安全设备以进行管理的密码。
系统警报收件人 (Email System Alerts To)	设备将系统警报发送到的邮件地址。
通过 SMTP 中继主机发送邮件 (Send Email via SMTP Relay Host)（可选）	AsyncOS 可用于发送系统生成的邮件的 SMTP 中继主机的地址和端口。 如果未定义 SMTP 中继主机，则 AsyncOS 会使用 MX 记录中列出的邮件服务器。

属性	说明
自动支持	指定设备是否向思科客户支持部门发送系统警报和每周状态报告。
SensorBase 网络参与 (SensorBase Network Participation)	指定是否参与思科 SensorBase 网络。如果参与，则可以配置有限或标准（完全）参与。默认值为“标准”(Standard)。 SensorBase 网络是一个威胁管理数据库，用于跟踪全球数百万个域并维护互联网流量的全局监视列表。当启用 SensorBase 网络参与时，网络安全设备向思科发送有关 HTTP 请求的匿名统计信息以提升 SensorBase 网络数据的价值。

安全/安全设置

选项	说明
全局策略默认操作 (Global Policy Default Action)	指定在完成“系统设置向导”(System Setup Wizard) 后默认情况下阻止还是监控所有 Web 流量。您可以稍后通过编辑全局访问策略的“协议”(Protocols) 和“用户代理”(User Agents) 设置来更改此行为。默认设置为监控流量。
L4 流量监控器 (L4 Traffic Monitor)	指定在完成“系统设置向导”(System Setup Wizard) 后默认情况下 L4 流量监控器应监控还是阻止可疑恶意软件。您可以稍后更改此行为。默认设置为监控流量。
可接受的使用控制 (Acceptable Use Controls)	指定是否启用“可接受的使用控制”(Acceptable Use Controls)。 如果启用，“可接受的使用控制”(Acceptable Use Controls) 允许您基于 URL 过滤配置策略。它们还提供应用可视性与可控性，以及相关选项（例如，安全搜索执行）。默认设置为已启用。
信誉过滤 (Reputation Filtering)	指定是否为全局策略组启用 Web 信誉过滤。 Web 信誉过滤器是一项安全功能，用于分析 Web 服务器行为并向 URL 分配信誉分数，以确定其包含基于 URL 的恶意软件的可能性。默认设置为已启用。
恶意软件和间谍软件扫描 (Malware and Spyware Scanning)	指定是否启用使用 Webroot、McAfee 或 Sophos 的恶意软件和间谍软件扫描。默认设置为启用全部三个选项。将自动启用/禁用大多数安全服务，以匹配通常对云策略可用的服务。同样，与策略相关的默认设置将不适用。必须至少启用一个扫描选项。 如果启用任何选项，另请选择是监控还是阻止检测到的恶意软件。默认设置是监控恶意软件。 完成“系统设置向导”(System Setup Wizard) 后，可以进一步配置恶意软件扫描。

选项	说明
思科数据安全过滤 (Cisco Data Security Filtering)	指定是否启用思科数据安全过滤器。 如果启用，则思科数据安全过滤器会评估离开网络的数据，并允许创建思科数据安全策略来阻止特定类型的上传请求。默认设置为已启用。

上游代理

Web 代理可以将 Web 流量直接转发到其目标 Web 服务器，或者使用路由策略将其重定向到外部上游代理。

- 上游代理任务概述， 第 23 页
- 为上游代理创建代理组， 第 23 页

上游代理任务概述

任务	更多信息
• 连接思科 Web 安全设备上游的外部代理。	连接设备， 第 12 页.
• 创建并配置上游代理的代理组。	为上游代理创建代理组， 第 23 页.
• 为代理组创建路由策略以管理将哪个流量路由到上游代理。	创建策略以控制互联网请求， 第 175 页

为上游代理创建代理组

步骤 1 依次选择**网络 (Network) > 上游代理 (Upstream Proxies)**。

步骤 2 点击**添加组 (Add Group)**。

步骤 3 完成代理组设置。

属性	说明
名称 (Name)	用于标识设备上的代理组的名称，例如在路由策略中。
代理服务器 (Proxy Servers)	组中的代理服务器的地址、端口和重新连接尝试（如果代理不响应）。根据需要，可以添加或删除每个代理服务器的对应行。 **注释** 您可以多次输入同一代理服务器，以允许在代理组中的代理之间分布不等的负载。

属性	说明
负载均衡 (Load Balancing)	Web 代理用于在多个上游代理之间对请求进行负载均衡的策略。选项包括： • 无（故障切换）(None [failover])。Web 代理将事务定向到组中的一个外部代理。它尝试按列出代理的顺序连接到这些代理。如果无法连接其中一个代理，则 Web 代理会尝试连接到列表中的下一个代理。 • 最小连接数 (Fewest connections)。Web 代理记录组中不同代理的活动请求数，并将事务定向到当前为最少数量的连接提供服务的代理。 • 基于散列 (Hash based)。最近最少使用 (Least recently used)。如果所有代理当前均处于活动状态，Web 代理将事务定向到最近最少接收事务的代理。此设置类似于轮询，不同之处是 Web 代理还考虑到代理作为其他代理组中的成员所收到的事务。即，如果一个代理在多个代理组中列出，“最近最少使用”(least recently used) 选项不太可能使该代理负担过重。 • 循环法 (Round robin)。Web 代理按列表顺序在组中的所有代理之间均衡地循环事务。 注释 在定义两个或多个代理之前，“负载均衡”(Load Balancing) 选项始终以灰色显示。
故障处理 (Failure Handling)	指定在此组中的所有代理都失败的情况下要采取的默认操作。选项包括： • 直接连接 (Connect directly)。将请求直接发送到其目标服务器。 • 丢弃请求 (Drop requests)。放弃请求，不进行转发。

步骤 4 提交并确认更改。

下一步做什么

- 创建策略，第 181 页

网络接口

IP 地址版本

在标准模式下，思科网络安全设备在大多数情况下都支持 IPv4 和 IPv6 地址。

注释 在云连接器模式下，思科网络安全设备仅支持 IPv4。

DNS 服务器可能会返回同时包含 IPv4 和 IPv6 地址的结果。DNS 设置包括用于在这些情况下配置 AsyncOS 行为的 IP 地址版本首选项。

接口/服务	IPv4	IPv6	说明
M1 接口	必填	可选	使用 IPv6 地址需要具备定义 IPv6 默认网关的 IPv6 路由表。根据网络，您可能还需要在路由表中指定静态 IPv6 路由。
P1 接口	可选	可选	如果 P1 接口已配置 IPv6 地址，并且设备使用拆分路由（单独的管理路由和数据路由），则 P1 接口无法使用管理路由上配置的 IPv6 网关。相反，为数据路由表指定 IPv6 网关。
P2 接口	可选	可选	—
数据服务	支持	支持	-
控制和管理服务	支持的	部分支持	映像（例如最终用户通知页面上的自定义徽标）需要 IPv4。
AnyConnect 安全移动 (MUS)	支持	不支持	-

相关主题

- 启用或更改网络接口， 第 25 页
- DNS 设置， 第 40 页

启用或更改网络接口

- 添加或修改接口 IP 地址
- 更改第 4 层流量监控连线类型
- 启用管理流量和数据流量的拆分路由

步骤 1 依次选择**网络 (Network) > 接口 (Interfaces)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 配置“接口”选项。

选项	说明
接口	根据需要，修改 M1、P1 或 P2 接口的 IPv4 或 IPv6 地址、网络掩码和主机名详细信息或者添加新的详细信息。 • **M1** - AsyncOS 需要一个 IPv4 地址作为 M1（管理）端口。除 IPv4 地址外，您还可以指定 IPv6 地址。默认情况下，管理接口用于管理设备和 Web 代理（数据）监控。但是，您可以配置 M1 端口以仅用于管理。 • **P1** 和 **P2** - 使用 IPv4 地址和/或 IPv6 地址作为数据端口。数据接口用于 Web 代理监控和 L4 流量监控阻止（可选）。您还可以将这些接口配置为支持出站服务，例如 DNS、软件升级、NTP 和跟踪路由数据流量。 **注释** 如果管理接口和数据接口都已配置，则必须在不同子网上为每个接口分配 IP 地址
分隔管理服务的路由 (Separate Routing for Management Services)	请选中**将 M1 端口限制为仅用于设备管理服务**，以将 M1 限制为仅用于管理流量，而数据流量则需要使用单独的接口。 **注释** 将 M1 仅用于管理流量时，请在其他子网上为代理流量至少配置一个数据接口。为管理流量和数据流量定义不同的路由。
设备管理服务 (Appliance Management Services)	启用/禁用以下网络协议的使用并为其指定默认端口号： • **FTP** - 默认情况下被禁用。 • **SSH** • **HTTP** • **HTTPS** 此外，还可以启用/禁用 HTTP 流量到 HTTPS 的重定向。

步骤 4 提交并确认更改。

下一步做什么

如果添加了 IPv6 地址，则添加 IPv6 路由表。

相关主题

- 连接设备，第 12 页.
- IP 地址版本，第 24 页
- 配置 TCP/IP 通信路由，第 29 页

配置高可用性故障切换组

WSA 使用通用地址冗余协议 (CARP) 在网络中启用多个主机来共享 IP 地址，从而提供 IP 冗余以确保这些主机提供的服务的高可用性。

故障切换只适用于代理服务。创建故障切换组时，代理会自动绑定到故障切换接口。因此，如果代理由于任何原因关闭，会触发故障切换。

在 CARP 中，主机有三种状态：

- 主用 – 每个故障切换组中仅有一个主用主机。
- 备用
- 初始

CARP 故障切换组中的主用主机定期发送通告到本地网络，以便备用主机知道主用主机仍处于“活动”状态。（可在 WSA 上配置通告间隔。）如果备用主机在指定时间段内未收到主用主机的通告（由于代理关闭、WSA 本身已关闭或 WSA 与网络断开），会触发故障切换，其中一个备用主机将接管主用主机的任务。

添加故障切换组

开始之前

- 确定将专门用于此故障切换组的虚拟 IP 地址。客户端将使用此 IP 地址以显式转发代理模式连接到故障切换组。
- 使用以下参数的相同值配置故障切换组中的所有设备：
  - 故障切换组 ID (Failover Group ID)
  - 主机名 (Hostname)
  - 虚拟 IP 地址 (Virtual IP Address)
- 如果您在虚拟设备上配置此功能，请确保每台设备特定的虚拟交换机和虚拟接口配置使用混合模式。有关详细信息，请参阅虚拟机监控程序相关文档。

步骤 1 依次选择**网络 (Network) > 高可用性 (High Availability)**。

步骤 2 点击**添加故障切换组 (Add Failover Group)**。

步骤 3 输入**故障切换组 ID (Failover Group ID)**，范围为 1 到 255。

步骤 4 （可选）输入说明。

步骤 5 输入**主机名 (Hostname)**，例如 www.example.com。

步骤 6 输入**虚拟 IP 地址和网络掩码 (Virtual IP Address and Netmask)**，例如 10.0.0.3/24 (IPv4) 或 2001:420:80:1::5/32 (IPv6)。

步骤 7 从**接口 (Interface)** 菜单中选择选项。**自动选择接口 (Select Interface Automatically)** 选项将基于您提供的 IP 地址选择接口。

注释 如果未选择**自动选择接口 (Select Interface Automatically)** 选项，您必须在提供的虚拟 IP 地址所在的子网中选择接口。

步骤 8 选择优先级。点击**主 (Master)** 将优先级设置为 255。或者，选择**备份 (Backup)** 并在**优先级 (Priority)** 字段中选择一个介于 1（最小）和 254 之间的优先级。

步骤 9 （可选）。要启用该服务的安全性，请选择**启用服务的安全性 (Enable Security for Service)** 复选框并输入将要在**共享密钥 (Shared Secret)** 和**重新键入共享密钥 (Retype Shared Secret)** 字段中用作共享密钥的字符串。

注释 对于故障切换组中的所有设备，共享密钥、虚拟 IP 和故障切换组 ID 必须相同。

步骤 10 在**广告间隔 (Advertisement Interval)** 字段中输入为其可用性做广告的主机之间的延迟秒数（1 到 255）。

步骤 11 提交并确认更改。

下一步做什么

相关主题

- 故障切换问题，第 428 页

编辑高可用性全局设置

步骤 1 依次选择**网络 (Network)** > **高可用性 (High Availability)**。

步骤 2 在**高可用性全局设置 (High Availability Global Settings)** 区域中，点击**编辑设置 (Edit Settings)**。

步骤 3 在**故障切换处理 (Failover Handling)** 菜单中，选择一个选项。

- **抢占式 (Preemptive)** - 最高优先级的主机将取得控制权（如果可用）。
- **非抢占式 (Non-preemptive)** - 即使有更高优先级的主机变为可用，控制中的主机将仍处于控制中。

步骤 4 点击**提交 (Submit)**。或者，点击**取消 (Cancel)** 放弃更改。

查看故障切换组的状态

依次选择**网络 (Network)** > **高可用性 (High Availability)**。故障切换组 (Failover Groups) 区域显示当前的故障切换组。可点击**刷新状态 (Refresh Status)** 来更新显示。还可以通过依次选择**网络 (Network)** > **接口 (Interfaces)** 或者**报告 (Report)** > **系统状态 (System Status)** 来查看故障切换详细信息。

将 P2 数据接口用于 Web 代理数据

默认情况下，Web 代理不侦听 P2 上的请求，即使在启用时也如此。但是，您可以将 P2 配置为侦听 Web 代理数据。

注释 如果使用 `advancedproxyconfig` > `miscellaneous` CLI 命令启用 P2 以侦听客户端请求，则可以选择将 P1 还是 P2 用于传出流量。要将 P1 用于传出流量，请更改数据流量的默认路由，以指定 P1 接口连接到的下一个 IP 地址。

开始之前

启用 P2（如果尚未启用 P1，您还必须启用 P1）（请参阅启用或更改网络接口，第 25 页）。

步骤 1 访问 CLI。

步骤 2 使用 `advancedproxyconfig > miscellaneous` 命令访问所需区域

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

步骤 3 []> **miscellaneous**

步骤 4 按 **Enter** 键跳过每个问题，直至出现以下问题：

```
是否要在 P2 上侦听？
```

对此问题输入“**y**”。

步骤 5 按 **Enter** 键跳过其余问题。

步骤 6 确认您的更改。

下一步做什么

相关主题

- 连接设备， 第 12 页.
- 配置 TCP/IP 通信路由， 第 29 页.
- 配置透明重定向， 第 31 页

配置 TCP/IP 通信路由

路由用于确定发送（或路由）网络流量的位置。网络安全设备路由以下类型的流量：

- **数据流量**。Web 代理处理的因终端用户浏览网络而产生的流量。
- **管理流量**。通过 Web 界面来管理设备而创建的流量和设备为管理服务（例如 AsyncOS 升级、组件更新、DNS、身份验证等等）创建的流量。

默认情况下，两种流量均使用为所有已配置的网络接口定义的路由。不过，您可以选择拆分路由，以便管理流量使用管理路由表，数据流量使用数据路由表。两种类型的流量拆分如下：

管理流量	数据流量
• WebUI • SSH • SNMP • NTLM 身份验证（使用域控制器） • 外部 DLP 服务器的 ICAP 请求 • 系统日志 • FTP 推送 • DNS（可配置） • 更新/升级/功能密钥（可配置）	• HTTP • HTTPS • FTP • WCCP 协商 • DNS（可配置） • 更新/升级/功能密钥（可配置）

网络 > **路由**页面包含多少个部分由是否启用拆分路由决定：

- **管理流量和数据流量对应不同的路由配置部分**（已启用拆分路由）。如果将管理接口仅用于管理流量（**限制 M1 端口仅用于设备管理服务**已启用），则此页面包含两个可以输入路由的部分，一个用于管理流量，一个用于数据流量。
- **一个路由配置部分用于所有流量**（未启用拆分路由）。将管理接口同时用于管理流量和数据流量（**限制 M1 端口仅用于设备管理服务**已禁用），则此页面包含一个部分来输入离开网络安全设备的所有流量（管理流量和数据流量）的路由。

注释 路由网关必须与配置了该网关的管理接口或数据接口位于同一子网上。如果启用多个数据端口，则 Web 代理在数据接口上发出事务，该接口与为数据流量配置的默认网关位于同一网络上。

出站服务流量

网络安全设备还使用管理接口和数据接口来路由 DNS、软件升级、NTP 以及 traceroute 数据流量等服务的出站流量。通过选择各服务用于出站流量的路由为各服务单独配置接口。默认情况下，管理接口用于所有服务。

相关主题

- 要启用管理流量和数据流量的拆分路由，请参阅启用或更改网络接口，第 25 页。

修改默认路由

步骤 1 依次选择**网络 (Network)** > **路由 (Routes)**。

步骤 2 根据需要，点击管理表或数据表中的**默认路由 (Default Route)**（如果未启用拆分路由，则使用组合的管理/数据表）。

步骤 3 在“网关”(Gateway) 列中，输入连接到待编辑网络接口的网络的下一跳上的计算机系统 IP 地址。

步骤 4 提交并确认更改。

添加路由

步骤 1 依次选择**网络 (Network) > 路由 (Routes)**。

步骤 2 点击正在为其创建路由的接口所对应的**添加路由 (Add Route)** 按钮。

步骤 3 输入“名称”(Name)、“目标网络”(Destination Network) 和“网关”(Gateway)。

步骤 4 提交并确认更改。

保存和加载路由表

依次选择**网络 (Network) > 路由 (Routes)**。

要保存路由表，请点击**保存路由表 (Save Route Table)** 并指定保存文件的位置。

要加载已保存的路由表，请点击**加载路由表 (Load Route Table)**，导航到文件，将其打开，然后提交并确认更改。

注释 当目标地址与其中一个物理网络接口位于同一子网上时，AsyncOS 使用具有相同子网的网络接口来发送数据。AsyncOS 不查询路由表。

删除路由

步骤 1 依次选择**网络 (Network) > 路由 (Routes)**。

步骤 2 选择“删除”(Delete) 列中相应路由的对应复选框。

步骤 3 点击**删除 (Delete)** 并确认。

步骤 4 提交并确认更改。

下一步做什么

相关主题

- 启用或更改网络接口， 第 25 页.

配置透明重定向

- 指定透明重定向设备， 第 32 页

- 配置 WCCP 服务，第 33 页

指定透明重定向设备

开始之前

将设备连接到第 4 层交换机或 WCCP v2 路由器。

步骤 1 依次选择**网络 (Network) > 透明重定向 (Transparent Redirection)**。

步骤 2 点击**编辑设备 (Edit Device)**。

步骤 3 从“类型”下拉列表中选择透明地将流量重定向到设备的设备类型：**第 4 层交换机或无设备**或 **WCCP v2 路由器**。

步骤 4 提交并确认更改。

步骤 5 对于 WCCP v2 设备，请完成以下附加步骤：

a) 使用设备文档配置 WCCP 设备。

b) 在 WSA 的“透明重定向”页面上，点击**添加服务**以添加 WCCP 服务，如添加和编辑 WCCP 服务，第 34 页中所述。

c) 如果在设备上启用了 IP 欺骗，请创建第二个 WCCP 服务。

下一步做什么

相关主题

- 连接设备，第 12 页.
- 配置 WCCP 服务，第 33 页.

使用第 4 层交换机

如果使用第4层交换机进行透明重定向，根据配置情况，您可能需要在WSA上配置几个其他选项。

- 通常情况下，请勿启用 IP 欺骗；如果伪造上游 IP 地址，您可能创建一个异步路由循环。
- 在“编辑 Web 代理设置”(Edit Web Proxy Settings) 页面（“安全服务”(Security Services) > “Web 代理”(Web Proxy)），勾选**使用接收的报头 (Use Received Headers)** 部分（“高级设置”(Advanced Settings) 中的**使用 X-Forwarded-For 启用客户端 IP 地址的标识 (Enable Identification of Client IP Addresses using X-Forwarded-For)**。然后将一个或多个出口 IP 地址添加到**受信任的下游代理或负载均衡器 (Trusted Downstream Proxy or Load Balancer)** 列表。
- 或者，您可以使用 CLI 命令 `advancedproxyconfig > miscellaneous` 根据需要配置代理相关的以下参数：
  - `是否希望代理响应来自第 4 层交换机的运行状况检查（如果 WSA 处于第 4 层透明模式时始终启用）？` - 如果想要允许 WSA 响应运行状况检查，则输入 Y。
  - `是否希望代理对 TCP 接收窗口大小执行动态调整？` - 多数情况下使用默认 Y 即可；如果 WSA 的上游有另一个代理设备，则输入 N。

- 是否要为信头发送转发的 HTTP X? - 不需要，除非上游对 X-Forwarded-For (XFF) 报头有要求。
- 是否希望代理在传入连接 IP 地址的位置上记录 X 转发标题的值? - 为了协助排除故障，您可以输入 Y；客户端 IP 地址会显示在访问日志中。
- 是否希望代理使用 X-Forwarded-For 报头中的客户端 IP 地址? 同样，为协助策略配置和报告，您可以输入 Y。

- 如果使用 X-Forwarded-For (XFF) 报头，则添加 %f 到访问日志订用，以记录 XFF 报头。对于 W3C 日志格式，添加 cs(X-Forwarded-For)。

配置 WCCP 服务

WCCP 服务是用于将服务组定义到 WCCP v2 路由器的设备配置。该服务包括所使用的服务 ID 和端口等信息。通过服务组，Web 代理可以与 WCCP 路由器建立连接并处理来自路由器的已重定向流量。

如果启用了 WCCP 代理运行状况检查，则 WSA 的 WCCP 后台守护程序将会每 10 秒钟向 Web 代理上运行的 xmlrpc 服务器发送一次代理运行状况检查邮件（xmlrpc 客户端请求）。如果代理已启动并正在运行，WCCP 服务将接收来自代理的响应，并且 WSA 将会每 10 秒钟向启用了 WCCP 的指定路由器发送一封 WCCP“我这这里”(HIA) 的邮件。如果 WCCP 服务没有收到代理的答复，则 HIA 邮件不会发送到 WCCP 路由器。

在 WCCP 路由器错过了连续三封 HIA 邮件后，路由器将从其服务组中删除该 WSA，并且流量不再转发到该 WSA。

您可以使用 CLI 命令 advancedproxyconfig > miscellaneous > Do you want to enable WCCP proxy health check? 启用和禁用代理运营状况检查邮件；运行状况检查默认情况下将被禁用。

注释 可以在单个设备上配置最多 15 个服务组。

- 关于 WCCP 负载均衡，第 33 页
- 添加和编辑 WCCP 服务，第 34 页
- 创建用于 IP 欺骗的 WCCP 服务，第 36 页

关于 WCCP 负载均衡

WCCP 服务定义中的**分配权重**参数用于在本 WSA 上的负载作为 WCCP 池或服务组的成员运行时调整该负载。此权重表示可发送到此 WSA 以进行处理的 WCCP 总流量的比例。

只有当不同类型的网关设备是同一 WCCP 池的成员，并且您需要将更多流量转移到更强的设备时，才需要进行分配权重调整。

注释 所有作为 WCCP 池成员的 WSA 都必须运行支持分配权重的 AsyncOS 版本，以从 WCCP 负载均衡中获益。

有关**分配权重**参数的详细信息，请参阅添加和编辑 WCCP 服务，第 34 页。

添加和编辑 WCCP 服务

开始之前

将设备配置为使用 WCCP v2 路由器（请参阅指定透明重定向设备，第 32 页）。

步骤 1 依次选择**网络 (Network) > 透明重定向 (Transparent Redirection)**。

步骤 2 点击**添加服务 (Add Service)**，或者，要编辑 WCCP 服务，请点击“服务配置文件名称”(Service Profile Name) 列中的 WCCP 服务的名称。

步骤 3 按照说明配置 WCCP 选项：

WCCP 服务选项	说明
服务配置文件名称	WCCP 服务的名称。 **注释** 如果将此选项留空并选择标准服务（如下所示），则此处会自动分配名称“web_cache”。
服务	路由器的服务组类型。选项包括： **标准服务 (Standard service)**。此服务类型分配有固定 ID 0、固定重定向方法（按目标端口）和固定目标端口 80。只能创建一个标准服务。如果在设备上已存在标准服务，则此选项以灰色显示。 **动态服务 (Dynamic service)**。通过此服务类型，您可以定义自定义 ID、端口号以及重定向和负载均衡选项。在 WCCP 路由器上创建服务时输入与为动态服务所输入相同的参数。 如果创建动态服务，请输入以下信息： • **服务 ID (Service ID)**。您可以在“动态服务 ID”字段中输入 0 到 255 的任意数值。但是请注意，您可以在该设备上最多配置 15 个服务组。 • **端口号 (Port number[s])**。在“端口号”(Port Numbers) 字段中为要重定向的流量输入最多 8 个端口号。 • **重定向基础 (Redirection basis)**。选择基于源端口或目标端口来重定向流量。默认值为目标端口。 **注释** 要使用透明重定向和 IP 欺骗来配置本地 FTP，请选择“基于源端口（返回路径）重定向”，并将源端口设置为 13007。 • **负载均衡基础 (Load balancing basis)**。当网络使用多个网络安全设备时，您可以选择如何在设备之间分配数据包。您可以基于服务器或客户端地址来分配数据包。当选择客户端地址时，来自客户端的数据包始终分配到同一设备。默认设置为服务器地址。
路由器 IP 地址	一个或多个支持 WCCP 功能的路由器的 IPv4 或 IPv6 地址。使用每个路由器的唯一 IP；不能输入组播地址。不能在服务组内混用 IPv4 和 IPv6 地址。

WCCP 服务选项	说明
路由器安全	选中**启用服务安全性**可要求此服务组使用密码。如果启用，使用服务组的每个设备和 WCCP 路由器必须使用相同的密码。 提供并确认要使用的密码。
高级	**负载均衡方法 (Load-Balancing Method)**。这确定路由器如何在多个网络安全设备之间执行数据包的负载均衡。选项包括： • **仅允许掩码 (Allow Mask Only)**。WCCP 路由器使用路由器中的硬件制定决策。相比于散列方法，此方法可以提高路由器性能。但是，并非所有 WCCP 路由器都支持掩码分配。（仅 IPv4。） • **仅允许散列**。此方法依靠散列函数来做出重定向决策。此方法可能没有掩码方法高效，但可能是路由器支持的唯一选项。（IPv4 和 IPv6。） • **允许散列或掩码 (Allow Hash or Mask)**。允许 AsyncOS 与路由器协商方法。如果路由器支持掩码，则 AsyncOS 使用掩码，否则使用散列。 **掩码自定义**。如果选择“仅允许掩码”(Allow Mask Only) 或“允许散列或掩码”(Allow Hash or Mask)，则可以自定义掩码或指定位数： • **自定义掩码（最多 6 位）(Custom mask [max 5 bits])**。您可以指定掩码。Web 界面显示与提供的掩码关联的位数。您可以为 IPv4 路由器使用多达五个位，或为 IPv6 路由器使用多达六个位。 • **系统生成的掩码 (System generated mask)**。您可以让系统为您生成掩码。或者，您可以指定系统生成的掩码的位数，介于 1 位和 5 位之间。 **分配权重** – 此 WSA 的 WCCP 加权；有效数值为零到 255。此加权表示可发送到此 WSA 作为 WCCP 服务组的成员进行处理的总流量比例。值为零表示此 WSA 将是服务组的一部分，但不会从路由器接收任何重定向的流量。有关详细信息，请参阅关于 WCCP 负载均衡，第 33 页。 **转发方法 (Forwarding method)**。这是已重定向的数据包从路由器传输到 Web 代理所采用的方法。 **返回方法 (Return Method)**。这是已重定向的数据包从 Web 代理传输到路由器所采用的方法。

WCCP 服务选项	说明
	转发方法和返回方法使用以下方法类型之一： • **第 2 层 (L2)**。此方法通过将数据包的目标 MAC 地址替换为目标 Web 代理的 MAC 地址来重定向第 2 层的流量。L2 方法在硬件级别运行，并且通常提供最佳性能。但是，并非所有 WCCP 路由器都支持 L2 转发。此外，WCCP 路由器仅允许与直接（物理）连接的网络安全设备进行 L2 协商。 • **通用路由封装 (GRE)(Generic Routing Encapsulation [GRE])**。此方法通过使用 GRE 报头和重定向报头封装 IP 数据包来重定向第 3 层的流量。GRE 在软件级别运行，这可能会影响性能。 • **L2 或 GRE (L2 or GRE)**。通过此选项，设备使用路由器表明其支持的方法。如果路由器和设备都支持 L2 和 GRE，则设备使用 L2。 如果路由器不直接连接到设备，则您必须使用 GRE。

步骤 4 提交并确认更改。

创建用于 IP 欺骗的 WCCP 服务

步骤 1 如果已在 Web 代理上启用了 IP 欺骗，请创建两个 WCCP 服务。创建一个标准 WCCP 服务，或者创建一个基于目标端口重定向流量的动态 WCCP 服务。

步骤 2 创建基于源端口重定向流量的动态 WCCP 服务。

使用与对步骤 1 中创建的服务所使用相同的端口号、路由器 IP 地址和路由器安全设置。

注释 思科建议对用于返回路径的 WCCP 服务使用从 90 到 97 的服务 ID 号（基于源端口）。

下一步做什么

相关主题

- Web 代理缓存，第 63 页.

使用 VLAN 增加接口容量

您可以配置一个或多个 VLAN 来增加思科网络安全设备可以连接到的除包含的物理接口数以外的网络数。

VLAN 显示为以“VLAN DDDD”格式标记的动态“数据端口”，其中“DDDD”是 ID，是长度最多为 4 位数的整数（例如 VLAN 2 或 VLAN 4094）。AsyncOS 最多支持 30 个 VLAN。

物理端口不需要为了进入 VLAN 而配置 IP 地址。其上创建了 VLAN 的物理端口可具有将接收非 VLAN 流量的 IP，因此在同一接口上可同时有 VLAN 流量和非 VLAN 流量。

只能在管理端口和 P1 数据端口上创建 VLAN。

配置和管理 VLAN

您可以通过 `etherconfig` 命令创建、编辑和删除 VLAN。创建之后，即可在 CLI 中通过 `interfaceconfig` 命令来配置 VLAN。

示例 1：创建新的 VLAN

在此示例中，在 P1 端口上创建两个 VLAN（命名为 VLAN 31 和 VLAN 34）：

注释 不在 T1 或 T2 接口上创建 VLAN。

步骤 1 访问 CLI。

步骤 2 按照显示的步骤操作。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN   31 (P1)
2. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
```

```
- DELETE - Delete a VLAN.
[]>
```

步骤 3 确认您的更改。

示例 2：在 VLAN 上创建 IP 接口

在此示例中，在 VLAN 34 以太网接口上创建新 IP 接口。

注释 对接口进行更改可能会关闭与设备的连接。

步骤 1 访问 CLI。

步骤 2 按照所示步骤操作：

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new
IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10
Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN   34
[1]> 4
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>
Hostname:
[]> v.example.com
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN   34 (10.10.31.10 on VLAN  34: v.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
example.com> commit
```

步骤 3 确认您的更改。

下一步做什么

相关主题

- 启用或更改网络接口，第 25 页.
- 配置 TCP/IP 通信路由，第 29 页.

重定向主机名和系统主机名

在运行“系统设置向导”(System Setup Wizard) 后，系统主机名和重定向主机名相同。但是，使用 `sethostname` 命令更改系统主机名并不会更改重定向主机名。因此，设置可能具有不同的值。

AsyncOS 将重定向主机名用于最终用户通知和确认。

系统主机名是用于在以下区域中识别设备的完全限定主机名：

- 命令行界面 (CLI)
- 系统警报
- 在网络安全设备加入 Active Directory 域的情况下形成计算机 NetBIOS 名称时。

系统主机名不直接对应接口主机名，并且未由客户端用于连接到设备。

更改重定向主机名

步骤 1 在 Web 用户界面上，导航到**网络 (Network)** > **身份验证 (Authentication)**。

步骤 2 点击“编辑全局设置”(Edit Global Settings)。

步骤 3 为“重定向主机名”(Redirect Hostname) 输入新值。

更改系统主机名

步骤 1 访问 CLI。

步骤 2 使用 `sethostname` 命令更改网络安全设备的名称：

```
example.com> sethostname

example.com> hostname.com

example.com> commit
...
hostname.com>
```

步骤 3 确认您的更改。

配置 SMTP 中继主机设置

AsyncOS会定期发送系统生成的邮件，例如通知、警报和思科客户支持请求。默认情况下，AsyncOS使用域上的 MX 记录中列出的信息来发送邮件。但是，如果设备无法直接访问 MX 记录中列出的邮件服务器，则必须至少在设备上配置一个 SMTP 中继主机。

注释 如果网络安全设备无法与 MX 记录中列出的邮件服务器或任何已配置的 SMTP 中继主机通信，则其无法发送邮件，并会在日志文件写入一条消息。

您可以配置一个或多个 SMTP 中继主机。当配置多个 SMTP 中继主机时，AsyncOS 使用最前面的可用 SMTP 中继主机。如果 SMTP 中继主机不可用，则它会尝试使用列表中位于下方的中继主机。

配置 SMTP 中继主机

步骤 1 依次选择**网络 (Network) > 内部 SMTP 中继 (Internal SMTP Relay)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 完成“内部 SMTP 中继”(Internal SMTP Relay) 设置。

属性	说明
中继主机名或 IP 地址 (Relay Hostname or IP Address)	要用于 SMTP 中继的主机名或 IP 地址
端口 (Port)	用于连接到 SMTP 中继的端口。如果此属性留空，则设备使用端口 25。
用于 SMTP 的路由表 (Routing Table to Use for SMTP)	与用于连接到 SMTP 中继的设备网络接口关联（管理或数据）的路由表。选择与中继系统位于同一网络上的任何一个接口。

步骤 4 （可选）点击**添加行 (Add Row)** 可添加额外的 SMTP 中继主机。

步骤 5 提交并确认更改。

DNS 设置

AsyncOS for Web 可以使用互联网根 DNS 服务器或您自己的 DNS 服务器。当使用互联网根服务器时，您可以指定用于特定域的备用服务器。由于备用DNS服务器应用于单个域，因此其必须能够对该域授权（提供限定的 DNS 记录）。

还可以指定辅助 DNS 名称服务器来解析主名称服务器未解析的查询。辅助 DNS 服务器不用作故障切换 DNS 服务器。当主 DNS 服务器返回 编辑 DNS 设置，第 41 页 中指定的错误时，将根据优先级对它们进行查询。

拆分 DNS

AsyncOS 支持拆分 DNS，其中为特定域配置了内部服务器，并为其他域配置了外部服务器或根 DNS 服务器。如果您使用的是自己的内部服务器，则还可以指定异常域和关联的 DNS 服务器。

清除 DNS 缓存

开始之前

请注意，使用此命令可能会导致性能暂时降低，而缓存则会重新填充。

步骤 1 依次选择**网络 (Network) > DNS**。

步骤 2 点击**清除 DNS 缓存 (Clear DNS Cache)**。

编辑 DNS 设置

步骤 1 依次选择**网络 (Network) > DNS**

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 根据需要配置 DNS 设置。

属性	说明
主 DNS 服务器 (Primary DNS Servers)	**使用这些 DNS 服务器 (Use these DNS Servers)**。设备可用于解析主机名的本地 DNS 服务器。 **备用 DNS 服务器覆盖（可选） (Alternate DNS servers Overrides [Optional])**。特定域的授权 DNS 服务器 **使用互联网的根 DNS 服务器 (Use the Internet's Root DNS Servers)**。当设备无权访问网络上的 DNS 服务器时，您可以选择使用互联网根 DNS 服务器进行域名服务查找。 注释 互联网根 DNS 服务器将不解析本地主机名。如果需要设备解析本地主机名，必须使用本地 DNS 服务器，或者使用命令行界面将相应的静态条目添加到本地 DNS。

属性	说明
辅助 DNS 服务器 (Secondary DNS Servers)	设备可用于解析主名称服务器未解析的主机名的辅助 DNS 服务器。 注释 当主 DNS 服务器返回以下错误时，辅助 DNS 服务器将接收主机名查询： • 没有错误，未收到应答部分。 • 服务器未能完成请求，没有应答部分。 • 名称错误，未收到应答部分。 • 函数未执行。 • 服务器拒绝应答查询。
DNS 流量的路由表 (Routing Table for DNS Traffic)	指定 DNS 服务路由流量将采用的接口。
IP 地址版本首选项 (IP Address Version Preference)	当 DNS 服务器同时提供 IPv4 和 IPv6 地址时，AsyncOS 使用此首选项选择 IP 地址版本。 注释 AsyncOS 不支持透明 FTP 请求的版本首选项。
在反向 DNS 查找超时之前等待 (Wait Before Timing out Reverse DNS Lookups)	在无响应的反向 DNS 查找超时之前的等待时间（以秒为单位）。
域搜索列表 (Domain Search List)	在请求发送到裸主机名（没有“.”字符）时使用的DNS域搜索列表。将按照输入顺序依次尝试指定的每个域，以查看是否可以找到主机名以及域的 DNS 匹配项。

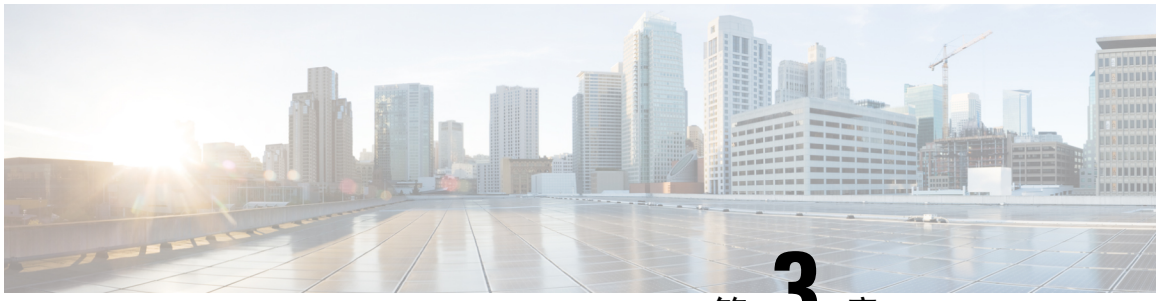
步骤 4 提交并确认更改。

下一步做什么

相关主题

- 配置 TCP/IP 通信路由， 第 29 页
- IP 地址版本， 第 24 页

连接、安装和配置故障排除



第 3 章

将设备连接到思科云网络安全代理

本章包含以下部分：

如何在云连接器模式下配置和使用功能

除非另有说明，否则对云连接器子网中功能的使用与在标准模式下的使用相同。有关其他信息，请参阅比较操作模式， 第 8 页。

本章包含一些可以转到本文档中其他位置的链接，用于提供有关网络安全设备在标准模式和云网络安全连接器模式下均常见的某些主要功能的信息。除了有关云连接器配置设置以及向云发送目录组的信息外，其他相关信息位于本文档的其他位置。

本章包含有关配置不适用于标准模式的云网络安全连接器的信息。

本文档不含有关思科云网络安全产品的信息。可从以下位置获取思科云网络安全文档：
http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

在云连接器模式下部署

初始设置设备时，选择是在云连接器模式还是标准模式下部署。如果您拥有所需的许可，还可以在当前已在标准模式下部署的设备上运行系统设置向导，以便在云连接器模式下重新部署该设备。运行系统设置向导将会覆盖现有配置，并删除所有现有数据。

在标准模式和云安全模式下，设备的部署是相同的，只是在云网络安全连接器模式下，现场 Web 代理服务和第 4 层流量监控器不可用。

您可以在显式转发模式或透明模式下部署云网络安全连接器。

要在初始设置后修改云连接器设置，请选择**网络 (Network)** > **云连接器 (Cloud Connector)**。

相关主题

- 连接、安装和配置 ， 第 7 页

配置云连接器

开始之前

请参阅启用对虚拟设备上的 Web 界面访问 ， 第 3 页。

步骤 1 访问网络安全设备的 Web 界面：

在因特网浏览器中输入网络安全设备的 IPv4 地址。

首次运行“系统设置向导”(System Setup Wizard) 时，请使用默认 IPv4 地址：

```
https://192.168.42.42:8443
```

-或者-

```
http://192.168.42.42:8080
```

其中 `192.168.42.42` 是默认 IPv4 地址，`8080` 是用于 HTTP 的默认管理端口设置，`8443` 是用于 HTTPS 的默认管理端口。

步骤 2 依次选择**系统管理 (System Administration)** > **系统设置向导 (System Setup Wizard)**。

步骤 3 接受许可协议条款。

步骤 4 点击**开始安装 (Begin Setup)**。

步骤 5 配置系统设置：

设置	说明
默认系统主机名 (Default System Hostname)	网络安全设备的完全限定主机名。
DNS 服务器 (DNS Server(s))	用于域名服务查找的互联网根 DNS 服务器。 另请参阅 DNS 设置 ， 第 40 页。
NTP 服务器 (NTP Server)	用于同步系统时钟的服务器。默认设置为 time.ironport.com。
时区 (Time Zone)	在设备上设置时区，以便邮件头和日志文件中的时间戳是正确的。

步骤 6 对设备模式选择**云网络安全连接器 (Cloud Web Security Connector)**。

步骤 7 配置云连接器设置：

设置	说明
云网络安全代理服务器 (Cloud Web Security Proxy Servers)	云代理服务器 (CPS) 的地址，例如 proxy1743.scansafe.net。
故障处理 (Failure Handling)	如果 AsyncOS 无法连接到 Cloud Web Security 代理，请选择**直接连接 (Connect directly)** 到互联网，或者选择**丢弃请求 (Drop requests)**。
云网络安全授权方案 (Cloud Web Security Authorization Scheme)	授权事务的方法： • 网络安全设备公开 IPv4 地址 • 每个事务随附的授权密钥。您可以在思科云网络安全门户中生成授权密钥。

步骤 8 配置网络接口和接线：

设置	说明
以太网端口 (Ethernet Port)	如果您仅配置用于管理流量的 M1 接口，则必须配置用于数据流量的 P1 接口。但是，即使在 M1 接口同时用于管理流量和数据流量时，也可以配置 P1 接口。
IP 地址 (IP Address)	用于管理网络安全设备的 IPv4 地址。
网络掩码 (Network Mask)	管理此网络接口上的网络安全设备时使用的网络掩码。
主机名 (Hostname)	管理此网络接口上的网络安全设备时使用的主机名。

步骤 9 配置用于管理和数据流量的路由：

设置	说明
默认网关 (Default Gateway)	用于管理和/或数据接口流量的默认网关 IPv4 地址。
名称 (Name)	用于识别静态路由的名称。
内部网络 (Internal Network)	网络上此路由目标的 IPv4 地址。
内部网关 (Internal Gateway)	此路由的网关 IPv4 地址。路由网关必须位于与所配置的管理或数据接口相同的子网。

步骤 10 配置透明连接设置：

注释 默认情况下，云连接器在透明模式下部署。这需要连接第 4 层交换机或第 2 版 WCCP 路由器。

设置	说明
第 4 层交换机 (Layer-4 Switch) 或 无设备 (No Device)	• 网络安全设备连接到第 4 层交换机。 或 • 您将在显式转发模式下部署云连接器。
WCCP v2 路由器 (WCCP v2 Router)	网络安全设备连接到第 2 版 WCCP 路由器。 注：密码最多可以包含七个字符并且是可选项。

步骤 11 配置管理设置：

设置	说明
管理员密码 (Administrator Passphrase)	用于访问网络安全设备的密码。密码必须至少包含六个字符。
系统警报收件人 (Email system alerts to)	设备发送警报的邮件地址。
通过 SMTP 中继主机发送邮件 (Send Email via SMTP Relay Host)	（可选）AsyncOS 用来发送系统邮件的 SMTP 中继主机的主机名或地址。 默认 SMTP 中继主机为 MX 记录中列出的邮件服务器。 默认端口号为 25。
自动支持 (AutoSupport)	设备可以向思科客户支持发送系统警报和每周状态报告。

步骤 12 查看和安装：

a) 查看安装。

b) 点击**上一步 (Previous)** 返回相关设置进行修改。

c) 点击**安装此配置 (Install This Configuration)** 继续使用您提供的信息。

下一步做什么

相关主题

- 防止安全数据丢失，第 48 页
- 网络接口，第 24 页
- 配置 TCP/IP 通信路由，第 29 页
- 配置透明重定向，第 31 页
- 管理警报，第 392 页

- 配置 SMTP 中继主机， 第 40 页

在云中使用目录组控制 Web 访问

您可以使用思科云网络安全控制基于目录组的 Web 访问。当进入思科云网络安全的流量通过云连接器模式下的网络安全设备路由时，思科云网络安全需要从云连接器接收事务的目录组信息，以便应用基于组的云策略。

开始之前

向网络安全设备配置添加身份验证领域。

步骤 1 导航到**网络 (Network)** > **云连接器 (Cloud Connector)**。

步骤 2 在**云策略目录组 (Cloud Policy Directory Groups)** 区域中，点击**编辑组 (Edit Groups)**。

步骤 3 选择在思科云网络安全中已创建云策略的用户组 (User Groups) 和计算机组 (Machine Groups)。

步骤 4 点击**添加 (Add)**。

步骤 5 点击**完成 (Done)** 并确认更改。

下一步做什么

相关信息

- 身份验证领域， 第 86 页

绕过云代理服务器

通过云路由策略，您可以根据以下特征将 Web 流量路由到思科云网络安全代理或直接路由到互联网：

- **标识配置文件**
- 代理端口
- 子网
- URL 类别
- 用户代理

在云连接器模式下创建云路由策略的流程与使用标准模式创建路由策略的流程相同。

相关主题

- 创建策略， 第 181 页

在云连接器模式下对 FTP 和 HTTPS 的部分支持

云连接器模式下的网络安全设备不完全支持 FTP 或 HTTPS。

FTP

云连接器不支持 FTP。如果设备配置为云连接器模式，AsyncOS 会丢弃本地 FTP 流量。

在云连接器模式下支持 FTP over HTTP。

HTTPS

云连接器不支持解密。它可以在不解密的情况下传递 HTTPS 流量。

因为云连接器不支持加密，所以 AsyncOS 通常无法访问 HTTPS 流量客户端报头中的信息。因此，AsyncOS 通常无法执行依赖于加密报头信息的路由策略。透明 HTTPS 事务始终是这种情况。例如，对于透明 HTTPS 事务，AsyncOS 无法访问 HTTPS 客户端报头中的端口号，因此无法根据端口号匹配路由策略。在这种情况下，AsyncOS 会使用默认路由策略。

显式 HTTPS 事务有两种例外情况。AsyncOS 可以访问显式 HTTPS 事务的以下信息：

- URL
- 目标端口号

对于显式 HTTPS 事务，可以根据 URL 或端口号匹配路由策略。

防止安全数据丢失

您可以通过选择**网络 (Network)** > **外部 DLP 服务器 (External DLP Servers)**，将云连接器与外部防数据丢失服务器集成到一起。

相关主题

- 防止敏感数据丢失，第 263 页

查看组名称、用户名称和 IP 地址

要查看已配置的组名称、用户名称和 IP 地址，请转到 whoami.scansafe.net。

订用云连接器日志

云连接器日志提供有关云连接器（例如，用户和组身份验证、云报头和授权密钥）故障排除的有用信息。

步骤 1 导航到**系统管理 (System Administration)** > **日志订阅 (Log Subscriptions)**。

步骤 2 从**日志类型 (Log Type)** 菜单中选择**云连接器日志 (Cloud Connector Logs)**。

步骤 3 在**日志名称 (Log Name)** 字段中输入名称。

步骤 4 设置日志级别。

步骤 5 提交并确认更改。

下一步做什么

相关主题

- 通过日志监控系统活动，第 331 页

标识配置文件和采用云网络安全连接器模式的身份验证

云网络安全连接器支持基本身份验证和 NTLM。您还可以绕过某些目标的身份验证。

在云连接器模式下，您可以使用 Active Directory 领域将事务请求识别为由特定计算机发出。计算机 ID 服务在标准模式下不可用。

无论是在标准配置下，还是在云连接器配置下，网络安全设备都以相同方式执行身份验证，但是有以下两种例外情况。例外情况：

- 计算机 ID 服务在标准模式下不可用。
- 如果设备配置为云连接器模式，AsyncOS 不支持 Kerberos。

注释 对于 HTTPS 流量，设备不支持基于用户代理或目标 URL 的标识配置文件。

相关主题

- 识别用于策略应用的计算机，第 49 页
- 未通过身份验证的用户的访客访问，第 50 页
- 对最终用户进行分类以应用策略，第 113 页
- 获取最终用户凭证，第 77 页

识别用于策略应用的计算机

启用计算机 ID 服务后，AsyncOS 可以基于发起事务请求的计算机应用策略，而不是基于已验证用户、IP 地址或其他标识符应用策略。AsyncOS 使用 NetBIOS 获取计算机 ID。

注释 请注意，只有在使用 Active Directory 领域的情况下，计算机 ID 服务才可用。如果您未配置 Active Directory 领域，此服务将被禁用。

步骤 1 依次选择**网络 (Network) > 计算机 ID 服务 (Machine ID Service)**。

步骤 2 点击**启用和编辑设置 (Enable and Edit Settings)**。

步骤 3 配置下列计算机身份设置：

设置	说明
为计算机身份启用 NetBIOS (Enable NetBIOS for Machine Identification)	选择此项可启用计算机身份服务。
领域 (Realm)	用于识别发起事务请求的计算机的 Active Directory 领域。
故障处理 (Failure Handling)	此项用于指定当 AsyncOS 无法识别计算机时，是丢弃事务还是继续匹配策略。

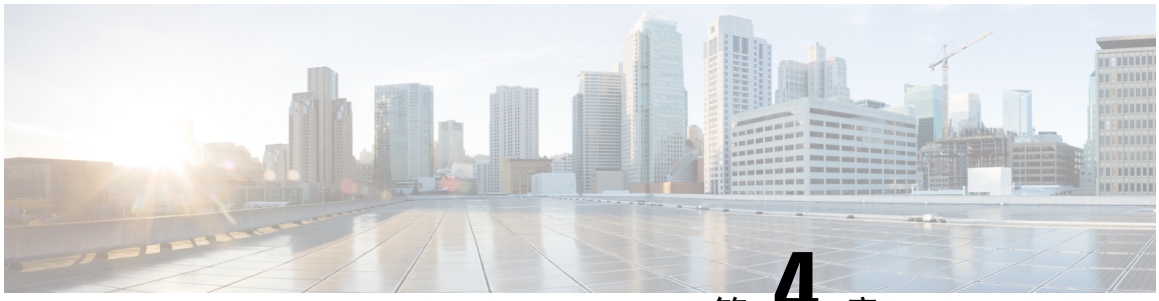
步骤 4 提交并确认更改。

未通过身份验证的用户的访客访问

如果网络安全设备配置为向未通过身份验证的用户提供访客接入，在云连接器模式下，AsyncOS 会将访客用户分配到组 __GUEST_GROUP__，并将该信息发送到思科云网络安全。使用身份向未通过身份验证的用户提供访客接入。使用思科云网络安全策略控制这些访客用户。

相关主题

- 身份验证失败后授予访客接入权限， 第 106 页



第 4 章

将设备连接到思科防御协调器

本章包含以下部分：

思科防御协调器集成概述

思科防御协调器是一个基于云的平台，可帮助网络运营人员通过管理思科安全设备的安全策略来建立和维护端到端安全态势。您可以将设备连接到思科防御协调器，并分析设备的安全策略配置，从而识别和解决策略不一致以及模型策略更改以验证其影响，同时协调策略更改以实现一致性并维持清晰的安全态势。

如何在思科防御协调器模式下配置和使用功能

除非另有说明，否则对思科防御协调器子网中功能的使用与在标准模式下的使用相同。有关其他信息，请参阅思科防御编排器模式下的配置变更与约束， 第 52 页。

本章包含一些可以转到本文档中其他位置的链接，用于提供有关网络安全设备在标准模式和思科防御协调器模式下均常见的某些主要功能的信息。

本章包含有关配置在标准模式下不适用的思科防御协调器的信息。

本文档不含有关思科防御协调器的信息。可从https://docs.defenseorchestrator.com获取思科防御协调器文档。

在思科防御协调器模式下部署

您可以根据自身需求使用以下方法之一在思科防御协调器模式下配置设备：

- **使用系统设置向导**。可对新设备使用此选项。运行系统设置向导时，选择思科防御协调器运行模式。有关说明，请参阅使用系统设置向导在思科防御协调器模式下配置设备，第 53 页。
- **在 Web 界面中使用思科防御协调器设置页面**。如果现有设备处于标准模式并且已配置策略，请使用此选项。您将能够使用思科防御协调器管理这些策略。有关说明，请参阅使用 Web 界面在思科防御协调器模式下配置标准模式设备，第 54 页。

思科防御编排器模式下的配置变更与约束

本部分指定在将网络安全设备注册到思科防御编排器之后，网络安全设备中将发生的配置更改。同时，还指定可配置的选项和约束。

注释 除了下面指定的内容之外，Web 界面中没有限制。思科防御编排器不支持进行身份验证。

注册后网络安全设备中的约束：

在设备中，您将无法配置通过思科防御编排器管理的功能。当设备注册时，这些功能的配置将迁移到思科防御编排器。设备中的所有其他配置设置都设置为默认设置。

除通过思科防御编排器管理的功能，其他所有功能都在您的设备中都可用。

注册后，访问策略通过思科防御编排器控制。例外情况如下所示。您只能在网络安全设备中配置以下访问策略功能：

- 访问策略 - 策略定义
  - 协议和用户代理
  - 防恶意软件和信誉 (Anti-Malware and Reputation)
- 自定义 URL 类别（外部实时源类别）

您只能在思科防御编排器中配置以下功能：

- 自定义 URL 类别（本地自定义类别）
- URL 过滤、应用和对象（大小和自定义 MIME 类型除外）
- 全局和非全局访问策略
- 访问策略支持
  - 支持添加多个访问策略。

- 支持添加、重新排序、删除访问策略。
- URL 过滤（预定义的 URL 类别过滤）、应用和对象（对象类型），具有以下限制：
  - 不支持应用和应用类型的带宽设置。
  - 不支持存档对象检查。
  - 不支持访问策略和身份的高级成员资格定义。
  - 不支持范围请求转发。
  - 不支持时间和量配额管理。
  - 不支持进行 URL 安全搜索、引用的异常、站点内容分级

如果启用了通过思科防御编排器进行报告：

- 思科防御编排器中的摘要报告将会可用。
- 报告在网络安全设备中也将可用。
- 报告在安全管理设备中将不可用。

使用系统设置向导在思科防御协调器模式下配置设备

安装新设备时，您可以使用系统设置向导在思科防御协调器模式下配置设备。

开始之前

参考思科防御编排器模式下的配置变更与约束，第 52 页，了解更多有关在将网络安全设备装载到思科防御协调器后网络安全设备中的配置变化的信息。

步骤 1 打开浏览器并输入网络安全设备的 IP 地址。第一次运行系统设置向导时，请使用默认 IP 地址：

`https://192.168.42.42:8443`

-或者-

`http://192.168.42.42:8080`

其中 `192.168.42.42` 是默认 IP 地址，`8080` 是用于 HTTP 的默认管理端口设置，`8443` 是用于 HTTPS 的默认管理端口。

否则，如果当前配置了设备，请使用 M1 端口的 IP 地址。

步骤 2 当出现设备登录屏幕时，请输入用户名和密码以访问设备。默认情况下，设备随附以下用户名和密码：

- 用户名：`admin`
- 密码：`ironport`

步骤 3 依次选择**系统管理 (System Administration)** > **系统设置向导 (System Setup Wizard)**。

步骤 4 接受许可协议条款。

步骤 5 点击**开始安装 (Begin Setup)**。

步骤 6 选择设备模式为**思科防御协调器 (Cisco Defense Orchestrator)**。

步骤 7 根据需要使用以下章节中提供的参考表来配置所有的设置。请参阅系统设置向导参考信息，第 17 页（第 2-11 页）。

步骤 8 查看和安装：

a) 查看安装。

b) 点击**上一步 (Previous)** 返回相关设置进行修改。

c) 点击**安装此配置 (Install This Configuration)** 继续使用您提供的信息。

根据设置期间配置的 IP、主机名或 DNS 设置，在此阶段您可能会失去与设备的连接。如果浏览器中显示“找不到页面”(Page not found) 错误，请更改 URL 以反映任何新地址设置并重新加载页面。出现提示时，请输入您的凭证。

步骤 9 点击**思科防御协调器门户 (Cisco Defense Orchestrator Portal)**。根据浏览器的设置，门户会在一个新窗口或选项卡中打开。

步骤 10 在思科防御协调器门户上，请执行以下步骤：

a) 登录思科防御协调器门户。

b) 在门户上装载网络安全设备。

c) 复制注册令牌（密钥）。

步骤 11 在网络安全设备上完成思科防御协调器注册。执行以下步骤：

a) 选择**网络 (Network)** > **思科防御协调器 (Cisco Defense Orchestrator)**。

b) 输入注册令牌（密钥），然后点击**注册 (Register)**。

c) 注册成功后会显示一条成功消息。

注释 执行此步骤后，用于策略实施的任何内容安全管理设备将无法在思科网络安全设备上实现策略更改。

下一步做什么

- （可选）配置设备，以将报告发送到思科防御协调器。请参阅如何启用思科防御协调器报告，第 57 页。
- 在思科防御协调器上配置访问策略。请参阅https://docs.defenseorchestrator.com/。

相关主题

排除思科防御协调器模式故障，第 57 页

使用 Web 界面在思科防御协调器模式下配置标准模式设备

如果您设备上存在现有策略，并且您希望使用思科防御协调器管理这些策略，请使用此程序。

开始之前

参考思科防御编排器模式下的配置变更与约束，第 52 页，了解更多有关在将网络安全设备装载到思科防御协调器后网络安全设备中的配置变化的信息。

步骤 1 选择**网络 (Network) > 思科防御协调器 (Cisco Defense Orchestrator)**。

步骤 2 在思科防御协调器设置下，点击**编辑设置 (Edit Settings)**。

步骤 3 选择**启用 (Enable)**，然后点击**提交 (Submit)**。

步骤 4 确认您的更改。

注释 执行此步骤后，用于策略实施的任何内容安全管理设备将无法在思科网络安全设备上实现策略更改。

步骤 5 点击**思科防御协调器门户 (Cisco Defense Orchestrator Portal)**。根据浏览器的设置，门户会在一个新窗口或选项卡中打开。

步骤 6 在思科防御协调器门户上，请执行以下步骤：

a) 登录思科防御协调器门户。
b) 在门户上装载网络安全设备。
c) 复制注册令牌（密钥）。

步骤 7 在网络安全设备上完成思科防御协调器注册。执行以下步骤：

a) 选择**网络 (Network) > 思科防御协调器 (Cisco Defense Orchestrator)**。
b) 输入注册令牌（密钥），然后点击**注册 (Register)**。
c) 注册成功后会显示一条成功消息。

下一步做什么

- （可选）配置设备，以将报告发送到思科防御协调器。请参阅如何启用思科防御协调器报告，第 57 页。
- 分析思科防御协调器上您的设备的访问策略。请参阅https://docs.defenseorchestrator.com/。

相关主题

排除思科防御协调器模式故障，第 57 页

禁用思科防御协调器

开始之前

在禁用思科防御协调器后，如果您需要启用它，需从思科防御协调器门户重新生成注册令牌（密钥），然后再次装载设备。请参阅启用思科防御协调器，第 56 页。

步骤 1 选择**网络 (Network) > 思科防御协调器 (Cisco Defense Orchestrator)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 取消选中**启用 (Enable)**。

步骤 4 提交并确认更改。

启用思科防御协调器

开始之前

确保您已连接到思科防御协调器门户。

步骤 1 选择**网络 (Network) > 思科防御协调器 (Cisco Defense Orchestrator)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用 (Enable)**。

步骤 4 提交并确认更改。

步骤 5 点击**思科防御协调器门户 (Cisco Defense Orchestrator Portal)**。根据浏览器的设置，门户会在一个新窗口或选项卡中打开。

步骤 6 在思科防御协调器门户上，请执行以下步骤：

a) 登录思科防御协调器门户。

b) 在门户上装载网络安全设备。

c) 复制注册令牌（密钥）。

步骤 7 在网络安全设备上完成思科防御协调器注册。执行以下步骤：

a) 导航到**思科防御协调器注册 (Cisco Defense Orchestrator Registration)** 部分。

b) 输入注册令牌（密钥），然后点击**注册 (Register)**。

c) 注册成功后会显示一条成功消息。

注释 执行此步骤后，用于策略实施的任何内容安全管理设备将无法在思科网络安全设备上实现策略更改。

思科防御协调器报告

在思科防御协调器模式下部署设备后，您可以配置设备以向思科防御协调器发送报告。

要启用思科防御协调器报告，请参阅如何启用思科防御协调器报告，第 57 页。您也将无法查看和管理安全管理设备上的报告数据。

如何启用思科防御协调器报告

开始之前

在思科防御协调器模式下部署您的设备。有关说明，请参阅在思科防御协调器模式下部署，第 52 页。

步骤 1 依次选择**安全服务 (Security Services)** > **报告 (Reporting)**，并点击**编辑设置 (Edit Settings)**。

步骤 2 选择**本地报告 (Local Reporting)**。

步骤 3 选择**思科防御协调器报告 (Cisco Defense Orchestrator Reporting)**。

步骤 4 提交并确认更改。

注释 一旦您启用思科防御协调器报告功能，采用安全管理设备进行的集中报告将不再起作用。但是，您可以继续使用高级网络安全报告应用进行集中报告。

下一步做什么

在思科防御协调器上查看您的设备的摘要报告。请参阅 https://docs.defenseorchestrator.com/。

排除思科防御协调器模式故障

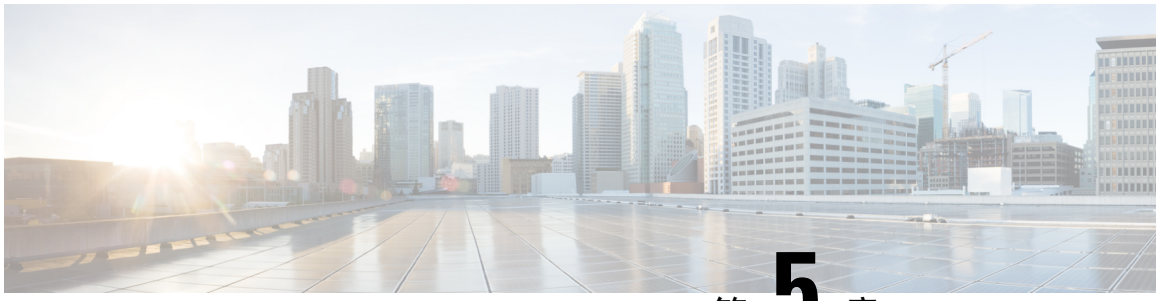
无法注册思科防御协调器

在设备上启用思科防御协调器模式后，如果您无法注册思科防御协调器，请执行以下操作：

步骤 1 确保从思科防御协调器门户获取的注册密钥正确。

步骤 2 确保从思科防御协调器门户获取的注册密钥有效。

如果注册密钥已过期，则在思科防御协调器上生成新的注册密钥。有关详细信息，请参阅 https://docs.defenseorchestrator.com。



第 5 章

拦截 Web 请求

本章包含以下部分：

拦截 Web 请求概述

网络安全设备会拦截客户端或其他设备通过网络转发来的请求。

该设备与其他网络设备配合工作以拦截流量。这些设备可能是普通交换机、透明重定向设备、网络分路器和其他代理服务器或网络安全设备。

拦截 Web 请求的任务

步骤	任务	相关主题和程序的链接
第 1 步	查看最佳实践。	• 拦截 Web 请求的最佳实践， 第 60 页
第 2 步	（可选）执行后续网络任务： • 连接并配置上游代理。 • 配置网络接口端口。 • 配置透明重定向设备。 • 配置 TCP/IP 路由。 • 配置 VLAN。	• 上游代理， 第 23 页 • 网络接口， 第 24 页 • 配置透明重定向， 第 31 页 • 配置 TCP/IP 通信路由， 第 29 页 • 使用 VLAN 增加接口容量， 第 36 页

步骤	任务	相关主题和程序的链接
第 3 步	（可选）执行后续 Web 代理任务。 • 将 Web 代理配置为在转发模式或透明模式下工作。 • 决定要拦截的协议类型是否需要额外服务。 • 配置 IP 欺骗。 • 管理 Web 代理缓存。 • 使用自定义 Web 请求报头。 • 绕过某些请求的代理。	• 用于拦截 Web 请求的 Web 代理选项，第 60 页 • 配置 Web 代理设置，第 61 页 • 用于拦截 Web 请求的 Web 代理选项，第 60 页 • Web 代理缓存，第 63 页 • Web 代理 IP 欺骗，第 66 页 • Web 代理绕行，第 67 页
第 4 步	执行客户端任务： • 决定客户端应如何将请求重定向到 Web 代理。 • 配置客户端和客户端资源。	• 重定向 Web 请求的客户端选项，第 68 页 • 通过客户端应用使用 PAC 文件，第 69 页
第 5 步	（可选）启用并配置 FTP 代理。	• FTP 代理服务，第 71 页

拦截 Web 请求的最佳实践

- 仅启用所需的代理服务。
- 为网络安全设备中定义的所有 WCCP 服务使用相同的转发和返回方法（L2 或 GRE）。这可以使代理绕行列表保证其运行一致。
- 确保用户无法从公司网络外访问 PAC 文件。这允许移动员工在处于公司网络中时使用 Web 代理，而在其他时间则可以直接连接到 Web 服务器。
- 仅允许 Web 代理从可信的下游代理或负载均衡器接收 X-Forwarded-For 报头。
- 将 Web 代理置于默认透明模式下，即使最初仅使用显式转发。透明模式也接受显式转发的请求。

用于拦截 Web 请求的 Web 代理选项

Web 代理自身可以拦截使用 HTTP（包括 FTP over HTTP）和 HTTPS 的 Web 请求。额外的代理模块可用于加强协议管理：

- **FTP 代理**。FTP 代理允许拦截本地 FTP 流量（而不是仅拦截 HTTP 中的编码 FTP 流量）。
- **HTTPS 代理**。HTTPS 代理支持解密 HTTPS 流量并允许 Web 代理将未加密的 HTTPS 请求传递到内容分析策略。

注释 在透明模式下，如果未启用 HTTPS 代理，Web 代理会丢弃所有透明重定向的 HTTPS 请求。系统不会为已丢弃的透明重定向 HTTPS 请求创建日志条目。

- **SOCKS 代理 (SOCKS Proxy)**。SOCKS 代理允许拦截 SOCKS 流量。

这些额外的代理都需要 Web 代理才能运行。如果禁用 Web 代理，则无法启用它们。

注释 默认情况下启用 Web 代理。默认情况下禁用所有其他代理。

相关主题

- FTP 代理服务，第 71 页
- SOCKS 代理服务，第 73 页

配置 Web 代理设置

开始之前

启用 Web 代理。

步骤 1 依次选择**安全服务 (Security Services)** > **Web 代理 (Web Proxy)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 按需配置基本的 Web 代理设置。

属性	说明
代理的 HTTP 端口 (HTTP Ports to Proxy)	Web 代理将会侦听其 HTTP 连接的端口。
缓存 (Caching)	指定启用还是禁用 Web 代理缓存。 Web 代理会缓存数据来提高性能。
代理模式 (Proxy mode)	• **转发 (Forward)** - 允许客户端浏览器命名互联网目标。要求每个 Web 浏览器单独配置为使用 Web 代理。Web 代理可以在此模式下拦截仅显式转发的 Web 请求。 • **透明 (Transparent)**（推荐）- 允许 Web 代理命名互联网目标。在此模式下，Web 代理可以拦截透明转发和显式转发的 Web 请求。
IP 欺骗 (IP Spoofing)	• **禁用 IP 欺骗 (IP Spoofing disabled)** - Web 代理更改请求源 IP 地址以匹配其自身的地址，以此来提升安全性。 • **启用 IP 欺骗 (IP Spoofing enabled)** - Web 代理保留源地址，以便其显示为来自源客户端而不是来自网络安全设备。

步骤 4 按需完成高级 Web 代理设置。

属性	说明
持久性连接超时 (Persistent Connection Timeout)	在事务完成后并且未接测到进一步活动的情况下，Web代理与客户端或服务器保持开放连接的最长时间（以秒为单位）。 • **客户端 (Client side)**。连接到客户端的超时值。 • **服务器端 (Server side)**。与服务器的连接超时值。 如果添加这些值，连接保持打开的时间将变长，用于重复打开和关闭连接的开销会降低。然而，如果达到同时打开的持久连接数，这也会限制 Web 代理打开新连接的能力。 思科建议保留默认值。
使用中连接超时 (In-Use Connection Timeout)	在当前事务尚未完成的情况下，Web 代理等待闲置客户端或服务器详细数据的最长时间（以秒为单位）。 • **客户端 (Client side)**。连接到客户端的超时值。 • **服务器端 (Server side)**。与服务器的连接超时值。
同时的持久连接数（服务器最大数量）(Simultaneous Persistent Connections [Server Maximum Number])	Web 代理与服务器保持打开的最大连接数（插槽数）。
生成报头 (Generate Headers)	生成并添加编码请求相关信息的报头。 • **X-Forwarded-For** 报头对发出 HTTP 请求的客户端 IP 地址编码。 注释 要开启或关闭请求头转发，请使用 CLI 命令 `advancedproxyconfig` 访问“其他设置”(Miscellaneous) 选项，并更改“是否需要传递 HTTP X-Forwarded-For 请求头？”(Do you want to pass HTTP X-Forwarded-For headers?) 的设置。 使用显式转发上游代理管理代理身份验证需要转发以下报头的用户身份验证或访问控制。 • **请求方 VIA (Request Side VIA)** 请求头用于编码将请求从客户端传递到服务器的代理。 • **应答方 VIA (Response Side VIA)** 请求头用于编码将请求从服务器传递到客户端的代理。
使用接收的报头 (Use Received Headers)	允许部署为上游代理的 Web 代理使用下游代理发送的 X-Forwarded-For 报头识别客户端。Web 代理将不会接受此列表之外来源的 X-Forwarded-For 报头中的 IP 地址。 如果启用此项，则必须使用下游代理或负载均衡器的 IP 地址（即不能输入子网或主机名）。
范围请求转发 (Range Request Forwarding)	使用**启用范围请求转发 (Enable Range Request Forwarding)** 复选框可启用或禁用范围请求转发。有关详细信息，请参阅管理对 Web 应用的访问 ， 第 253 页。

步骤 5 提交并确认更改。

下一步做什么

- Web 代理缓存，第 63 页
- 配置透明重定向，第 31 页

Web 代理缓存

Web 代理缓存数据以提高性能。AsyncOS 包括多种已定义的缓存模式（从安全模式到积极模式），而且支持自定义缓存。您可以通过两种方式，从正在缓存的 URL 中排除特定 URL：将特定 URL 从缓存中删除；通过配置缓存忽略特定 URL。

清除 Web 代理缓存

步骤 1 依次选择**安全服务 (Security Services)** > **Web 代理 (Web Proxy)**。

步骤 2 点击**清除缓存 (Clear Cache)**，然后确认您的操作。

从 Web 代理缓存删除 URL

步骤 1 访问 CLI。

步骤 2 使用 `webcache > evict` 命令访问所需的缓存区域：

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

步骤 3 输入需要从缓存中删除的 URL。

注释 如果您在输入 URL 时没有提供协议，系统会自动在 URL 前追加 `http://`（即 `www.cisco.com` 会变为 `http://www.cisco.com`）。

指定 Web 代理从不缓存的域或 URL

步骤 1 访问 CLI。

步骤 2 使用 `webcache -> ignore` 命令访问所需的子菜单：

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

步骤 3 输入您要管理的地址的类型：`DOMAINS` 或 `URLS`。

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

步骤 4 输入 **add** 以添加新条目：

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

步骤 5 输入域或 URL（每项单独占一行），例如：

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

在指定域或 URL 时，您可以输入某些正则表达式 (regex) 字符。 在 `DOMAINS` 选项下，您可以使用前句点字符，将整个域及其子域从缓存中排除。例如，您可以输入 `.google.com` 而非 `google.com`，以排除 www.google.com、docs.google.com 及其他 google.com 相关域。

在 `URLS` 选项下，您可以使用整套正则表达式字符。有关使用正则表达式的更多信息，请参阅正则表达式，第 161 页。

步骤 6 输入所需值后，按 Enter 键，直至返回主命令行界面。

步骤 7 确认您的更改。

选择 Web 代理缓存模式

步骤 1 访问 CLI。

步骤 2 使用 `advancedproxyconfig -> caching` 命令访问所需子菜单：

```
example.com> advancedproxyconfig
```

```
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

步骤 3 输入与所需的 Web 代理缓存设置对应的数字：

入门级	模式	说明
1	安全模式 (Safe)	与其他模式相比，最少缓存，最遵循 RFC #2616。
2	优化模式 (Optimized)	中等缓存，适度遵循 RFC #2616。与安全模式的不同点在于，在优化模式下，Web 代理会在未指定缓存时间且存在“Last-Modified”请求头的情况下缓存对象。Web 代理会缓存负响应。
3	积极模式 (Aggressive)	最多缓存，最不遵循 RFC #2616。与最优化模式相比，主动模式缓存通过身份验证的内容、ETag 不匹配项以及没有 Last-Modified 报头的内容。Web 代理会忽略无缓存参数。
4	自定义模式 (Customized mode)	逐个配置每个参数。

步骤 4 如果选择选项 4（自定义模式），请为每个自定义设置输入值（或保留默认值）。

步骤 5 按 **Enter** 键，直至返回到主命令界面。

步骤 6 确认您的更改。

下一步做什么

相关主题

- Web 代理缓存，第 63 页.

Web 代理 IP 欺骗

默认情况下，Web 代理转发请求时，会更改请求源 IP 地址以匹配其自身的地址。这提升了安全性，但您可以通过实施 IP 欺骗来更改此行为，以让请求保留源地址，显示为来自源客户端而不是来自网络安全设备。

IP 欺骗适用于透明和显式转发的流量。在透明模式下部署 Web 代理时，您可以选择仅对透明重定向的连接或对（透明重定向和显式转发的）所有连接启用 IP 欺骗。如果显示转发连接使用 IP 欺骗，您应该确定有将返回的数据包路由到网络安全设备上的适当网络设备。

当 IP 欺骗启用并且设备连接到 WCCP 路由器时，您必须配置两项 WCCP 服务：一项基于源端口，另一项基于目标端口。

相关主题

- 配置 Web 代理设置，第 61 页
- 配置 WCCP 服务，第 33 页

Web 代理自定义报头

您可以向特定传出事务添加自定义报头以请求目标服务器进行特殊处理。例如，如果您与 YouTube for Schools 建立了联系，可以使用自定义报头来识别传到 YouTube.com 的事务请求，确定其来自您的网络还是需要特殊处理。

将自定义报头添加到 Web 请求中

步骤 1 访问 CLI。

步骤 2 使用 `advancedproxyconfig -> customheaders` 命令访问所需的子菜单：

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

步骤 3 输入以下所需子命令：

选项	说明
删除 (Delete)	删除您指定的自定义报头。使用与命令返回的列表中的报头相关联的编号，确定要删除的报头。
新建 (New)	创建您提供用于所指定域的报头。 报头示例： X-YouTube-Edu-Filter：ABCD1234567890abcdef （本例中的值是 YouTube 提供的唯一密钥。） 域示例： youtube.com
编辑 (Edit)	用您指定的报头替换现有的报头。使用与命令返回的列表中的报头相关联的编号，确定要删除的报头。

步骤 4 按 **Enter** 键，直至返回到主命令界面。

步骤 5 确认您的更改。

Web 代理绕行

用于 Web 请求的 Web 代理绕行

您可以配置网络安全设备，让来自特定客户端或面向特定目标的透明请求绕过 Web 代理。

绕过 Web 代理使您能够：

- 防止与不遵循 HTTP（或者专有）的协议（使用 HTTP 端口但是连接到代理服务器时无法正常工作）相冲突。
- 确保来自网络内部特定计算机（如恶意软件测试计算机）的流量绕过 Web 代理及其所有内置安全防护。

绕行仅适用于透明重定向到 Web 代理的请求。Web 代理处理客户端显示转发来的所有请求，无论代理处于透明模式还是转发模式。

为 Web 请求配置 Web 代理绕行

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 绕过设置 (Bypass Settings)**。

步骤 2 点击**编辑绕过设置 (Edit Bypass Settings)**。

步骤 3 输入要绕过 Web 代理的地址。

步骤 4 提交并确认更改。

为应用配置 Web 代理绕行

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 绕过设置 (Bypass Settings)**。

步骤 2 点击**编辑应用绕过设置 (Edit Application Bypass Settings)**。

步骤 3 选择要绕过扫描的应用。

步骤 4 提交并确认更改。

Web 代理使用协议

您可以将网络安全设备配置为通知用户其正在过滤和监控 Web 活动。应用可以通过以下方式实现此操作：当用户在一定时间段后首次访问浏览器时，应用显示最终用户确认页面。当出现最终用户确认页面时，用户必须点击链接才能访问所请求的原始站点或任何其他网站。

相关主题

- 通知最终用户代理操作，第 275 页

重定向 Web 请求的客户端选项

如果选择让客户端将请求显式转发到 Web 代理，还必须决定如何配置客户端执行此操作。从以下方法中选择：

- **使用显式设置配置客户端**。通过 Web 代理主机名和端口号配置客户端。有关如何操作的详细信息，请参阅每个客户端文档。

注释 默认情况下，Web 代理端口使用端口号 80 和 3128。客户端可以使用其中任一端口。

- **使用代理自动配置 (PAC) 文件配置客户端**。PAC 文件为客户端提供有关将 Web 请求定向到哪里的说明。此选项让您可以集中管理代理详细信息的后续变更。

如果选择使用 PAC 文件，还必须选择这些文件的存储位置以及客户端查找这些文件的方式。

相关主题

- 通过客户端应用使用 PAC 文件，第 69 页

通过客户端应用使用 PAC 文件

发布代理自动配置 (PAC) 文件的选项

您必须在客户端可以访问的位置发布 PAC 文件。有效位置为：

- **Web 服务器**。
- **网络安全设备**。您可以将 PAC 文件放在网络安全设备上，其对于客户端就像是 Web 浏览器。设备还提供其他选项来管理 PAC 文件，包括能够管理使用不同主机名、端口和文件名的服务请求。
- **本地计算机**。您可以将 PAC 文件放在客户端本地硬盘。思科不建议将其作为通用解决方案，并且它不适用于自动 PAC 文件检测方法，但可用于测试。

相关主题

- 在网络安全设备上托管 PAC 文件，第 69 页
- 在客户端应用中指定 PAC 文件，第 70 页

查找代理自动配置 (PAC) 文件的客户端选项

如果选择使用客户端的 PAC 文件，还必须选择客户端查找这些文件的方式。此时您有两种选择：

- **配置客户端的 PAC 文件位置 (Configure client with the PAC file location)**。通过指向具体 PAC 文件的 URL 配置客户端。
- **将客户端配置为自动检测 PAC 文件位置 (Configure clients to detect the PAC file location automatically)**。将客户端配置为使用 WPAD 协议以及 DHCP 或 DNS 自动查找 PAC 文件。

PAC 文件自动检测

WPAD 是允许浏览器使用 DHCP 和 DNS 确定 PAC 文件位置的协议。

- **要将 WPAD 与 DHCP 配合使用**，您必须用 PAC 文件位置的 URL 在 DHCP 服务器上设置选项 252。但是，并不是所有的浏览器都支持 DHCP。
- **要将 WPAD 与 DNS 配合使用**，则必须将 DNS 记录配置为指向 PAC 文件的主服务器。

您可以配置其中一个选项或同时配置这两个选项。WPAD 将首先尝试使用 DHCP 查找 PAC 文件，如果找不到，将尝试使用 DNS。

相关主题

- 在客户端上自动检测 PAC 文件，第 71 页

在网络安全设备上托管 PAC 文件

步骤 1 依次选择**安全服务 (Security Services) > PAC 文件托管 (PAC File Hosting)**。

步骤 2 点击**启用和编辑设置 (Enable and Edit Settings)**。

步骤 3 （可选）完成以下基本设置：

选项	说明
PAC 服务器端口 (PAC Server Ports)	网络安全设备将用来侦听 PAC 文件请求的端口。
PAC 文件过期 (PAC File Expiration)	允许 PAC 文件在指定分钟数后在浏览器缓存中过期。

步骤 4 点击“PAC 文件”(PAC Files) 部分中的**浏览 (Browse)**，从本地计算机中选择要上传到网络安全设备的 PAC 文件。

注释 如果所选择的文件名为 `default.pac`，则在浏览器中配置其位置时无需指定文件名。如果未指定名称，网络安全设备会查找名为 `default.pac` 的文件。

步骤 5 点击**上传 (Upload)**，将在步骤 4 中选择的 PAC 文件上传到网络安全设备。

步骤 6 （可选）在“直接提供 PAC 文件的主机名”(Hostnames for Serving PAC Files Directly) 部分中，为不含端口号的 PAC 文件请求配置主机名和关联文件名。

选项	说明
主机名 (Hostname)	如果网络安全设备用于请求服务，则必须包括 PAC 文件请求的主机名。因为请求不包含端口号，所以请求将通过 Web 代理的 HTTP 端口（如端口 80）进行处理，而且必须能通过此主机名值被识别为 PAC 文件请求。
通过代理端口的“Get/”请求的默认 PAC 文件 (Default PAC File for "Get/" Request through Proxy Port)	将与同一行的主机名关联的 PAC 文件名。对主机名的请求会返回此处指定的 PAC 文件。 仅已上传的 PAC 文件才可供选择。
添加行 (Add Row)	添加另一行以指定其他主机名和 PAC 文件名。

步骤 7 提交并确认更改。

在客户端应用中指定 PAC 文件

在客户端上手动配置 PAC 文件位置

步骤 1 创建并发布一个 PAC 文件。

步骤 2 在浏览器中指向 PAC 文件位置的 PAC 文件配置区域中输入 URL。

如果网络安全设备托管 PAC 文件，有效 URL 格式如下：

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

其中，*WSAHostname* 是在网络安全设备上托管 PAC 文件时配置的**主机名(hostname)** 值。否则 URL 格式将取决于存储位置，在某些情况下，取决于客户端。

下一步做什么

- 在网络安全设备上托管 PAC 文件，第 69 页

在客户端上自动检测 PAC 文件

步骤 1 创建一个名为 wpad.dat 的 PAC 文件并将其发布到 Web 服务器或网络安全设备（如果要使用 WPAD 以及 DNS，必须将该文件放在 Web 服务器的根文件夹中）。

步骤 2 配置 Web 服务器，使用下面的 MIME 类型设置 .dat 文件：

```
application/x-ns-proxy-autoconfig
```

注释 网络安全设备自动为您执行此操作。

步骤 3 要支持 DNS 搜索，请创建一个以“`wpad`”开头的可内部解析的 DNS 名称（例如 `wpad.example.com`），并将其关联到 `wpad.dat` 文件托管服务器的 IP 地址。

步骤 4 如需支持 DHCP 搜索，请将 DHCP 服务器的 252 选项配置为 wpad.dat 文件位置的 URL（例如 `http://wpad.example.com/wpad.dat`）。URL 可以使用任何有效主机地址，包括 IP 地址，并且不需要特定 DNS 条目。

下一步做什么

- 通过客户端应用使用 PAC 文件，第 69 页
- 在网络安全设备上托管 PAC 文件，第 69 页
- WPAD 在 Firefox 中无法正常运行，第 427 页

FTP 代理服务

- FTP 代理服务概述，第 71 页
- 启用和配置 FTP 代理，第 72 页

FTP 代理服务概述

Web 代理可以拦截两种类型的 FTP 请求：

- **本地 FTP (Native FTP)**。本地 FTP 请求由专用 FTP 客户端（或由使用内置 FTP 客户端的浏览器）生成。需要 FTP 代理。
- **FTP over HTTP**。浏览器有时会编码 HTTP 请求中的 FTP 请求，而不是使用本地 FTP。不需要 FTP 代理。

相关主题

- 启用和配置 FTP 代理，第 72 页
- 配置 FTP 通知消息，第 284 页

启用和配置 FTP 代理

注释　要配置适用于 FTP over HTTP 连接的代理设置，请参阅配置 Web 代理设置，第 61 页。

步骤 1　依次选择**安全服务 (Security Services)** > **FTP 代理 (FTP Proxy)**。

步骤 2　点击**启用和编辑设置 (Enable and Edit Settings)**（如果只有**编辑设置 [Edit Settings]** 选项可用，则说明 FTP 代理已经启用）。

步骤 3　（可选）配置基本 FTP 代理设置。

属性	说明
代理侦听端口 (Proxy Listening Port)	FTP 代理将会侦听其 FTP 控制连接的端口。客户端在配置 FTP 代理时将使用此端口（不作为连接到 FTP 服务器的端口，该连接通常使用端口 21）。
缓存 (Caching)	是否缓存来自匿名用户的数据连接。 注释　从不缓存来自非匿名用户的数据。
服务器端 IP 欺骗 (Server Side IP Spoofing)	允许 FTP 代理模拟 FTP 服务器的 IP 地址。这样，在 IP 地址与控制和数据连接不同时，可支持不允许事务的 FTP 客户端。
身份验证格式 (Authentication Format)	允许选择 FTP 代理在与 FTP 客户端通信时可以使用的身份验证格式。
被动模式数据端口范围 (Passive Mode Data Port Range)	FTP 客户端将用于在被动模式连接下建立与 FTP 代理的数据连接的 TCP 端口范围。
激活模式数据端口范围 (Active Mode Data Port Range)	FTP 服务器将用于在主用模式连接下建立与 FTP 代理的数据连接的 TCP 端口范围。此设置适用于本地 FTP 和 FTP over HTTP 连接。 增大端口范围可容纳来自同一 FTP 服务器的更多请求。由于 TCP 会话存在 TIME-WAIT 延迟（通常为几分钟），所以对于同一个 FTP 服务器，端口在使用完毕后不会立即变为可用状态。因此，任何指定 FTP 服务器在较短的时间内都无法以活动模式连接到 FTP 代理 *n* 次以上（*n* 为此字段中指定的端口数）。

属性	说明
欢迎横幅 (Welcome Banner)	连接过程中显示在 FTP 客户端中的欢迎横幅。选项包括： • **FTP 服务器消息 (FTP server message)**。该消息将通过目标 FTP 服务器提供。仅当为透明模式配置 Web 代理时，此选项才可用，并且此选项仅适用于透明连接。 • **自定义消息 (Custom message)**。选择后，所有本地 FTP 连接均显示此自定义消息。如果未选择，此选项仍适用于显式转发本地 FTP 连接。

步骤 4 （可选）配置高级 FTP 代理设置：

属性	说明
控制连接超时 (Control Connection Timeouts)	在当前事务尚未完成的情况下，FTP 代理等待来自闲置 FTP 客户端或 FTP 服务器控制连接的进一步通信的最长时间（以秒为单位）。 • **客户端 (Client side)**。与闲置 FTP 客户端的控制连接超时值。 • **服务器端 (Server side)**。与闲置 FTP 服务器的控制连接超时值。
数据连接超时 (Data Connection Timeouts)	在当前事务尚未完成的情况下，FTP 代理等待来自闲置 FTP 客户端或 FTP 服务器数据连接的进一步通信的时间。 • **客户端 (Client side)**。与闲置 FTP 客户端的数据连接超时值。 • **服务器端 (Server side)**。与闲置 FTP 服务器的数据连接超时值。

步骤 5 提交并确认更改。

下一步做什么

• FTP 代理服务概述， 第 71 页

SOCKS 代理服务

SOCKS 代理服务概述

网络安全设备包含 SOCKS 代理，用于处理 SOCKS 流量。SOCKS 策略等同于控制 SOCKS 流量的访问策略。类似于访问策略，您可以利用标识配置文件指定每个 SOCKS 策略管理哪些事务。SOCKS 策略应用于事务后，路由策略便可以管理流量的路由。

请注意以下关于 SOCKS 代理的内容：

- SOCKS 协议仅支持直接转发连接。
- SOCKS 代理不支持（不会转发至）上游代理。
- SOCKS 代理不支持应用可视性与可控性使用 (AVC)、数据丢失 (DLP) 和恶意软件检测所使用的扫描服务。
- SOCKS 代理不支持策略跟踪。
- SOCKS 代理不对 SSL 流量进行解密；它通过隧道将其从客户端发送到服务器。

启用 SOCKS 流量处理

开始之前

启用 Web 代理。

步骤 1 依次选择**安全服务 (Security Services)** > **SOCKS 代理 (SOCKS Proxy)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择**启用 SOCKS 代理 (Enable SOCKS Proxy)**。

步骤 4 **提交 (Submit)** 并**确认更改 (Commit Changes)**。

配置 SOCKS 代理

步骤 1 依次选择**安全服务 (Security Services)** > **SOCKS 代理 (SOCKS Proxy)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择**启用 SOCKS 代理 (Enable SOCKS Proxy)**。

步骤 4 配置基本和高级 SOCKS 代理设置。

SOCKS 代理 (SOCKS Proxy)	已启用。
SOCKS 控制端口 (SOCKS Control Ports)	接受 SOCKS 请求的端口。默认值为 1080。
UDP 请求端口 (UDP Request Ports)	SOCKS 服务器应侦听的 UDP 端口。默认值为 16000-16100。
代理协商超时 (Proxy Negotiation Timeout)	协商阶段从 SOCKS 客户端发送或接收数据的等待时间（秒）。默认值为 60。
UDP 隧道超时 (UDP Tunnel Timeout)	来自 UDP 客户端或服务器的数据在关闭 UDP 隧道之前的等待时间（秒）。默认值为 60。

创建 SOCKS 策略

步骤 1 依次选择**网络安全管理器 (Web Security Manager)** > **SOCKS 策略 (SOCKS Policies)**。

步骤 2 点击**添加策略 (Add Policy)**。

步骤 3 在**策略名称 (Policy Name)** 字段中指定一个名称。

注释 每个策略组名称都必须唯一，并且仅包含字母数字字符或空格字符。

步骤 4 （可选）添加说明。

步骤 5 在**插入到策略上面 (Insert Above Policy)** 字段中，选择此 SOCKS 策略所要插入到的 SOCKS 策略表。

注释 当配置多个 SOCKS 策略时，确定每个策略的逻辑顺序。为策略排序，确保发生正确的匹配。

步骤 6 在**身份和用户 (Identities and Users)** 部分，选择一个或多个要应用到此策略组的身份。

步骤 7 （可选）展开“高级”(Advanced) 部分，定义其他成员身份要求。

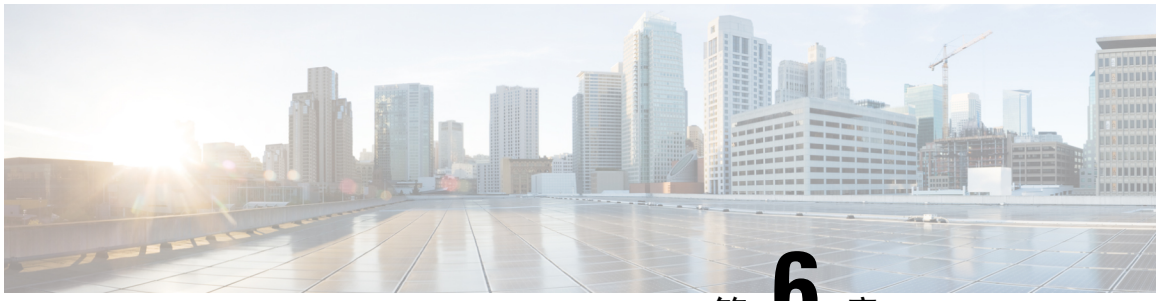
代理端口 (Proxy Ports)	在浏览器中配置的端口。 （可选）由用于访问 Web 代理的代理端口定义策略组成员身份。在“代理端口”(Proxy Ports) 字段中输入一个或多个端口号。使用逗号分隔多个端口。 如果您将一组客户端配置为在某个端口上显式转发请求，并将另一组客户端配置为在另一个端口上显式转发请求，则您可能要在代理端口上定义策略组成员身份。 **注释** 如果与此策略组关联的身份按此高级设置定义身份成员身份，不会在 SOCKS 策略组级别配置此设置。
子网 (Subnets)	（可选）按子网或其他地址定义策略组成员身份。 您可以选择使用可通过关联**身份 (Identity) 定义 (defined)** 的**地址 (addresses)**，也可以在此处输入**具体地址 (specific addresses)**。 **注释** 如果与此策略组相关的身份按地址定义其成员身份，则在此策略组中，您必须输入作为身份地址组成部分的地址。在策略组中添加地址会进一步缩小与此策略组匹配的事务列表的范围。
时间范围（Time Range）	（可选）按时间范围定义策略组成员身份： 1. 在**时间范围 (Time Range)** 字段中，选择一个时间范围。 2. 指定此策略组将应用于所选时间范围之内还是之外的时间。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

- （可选）添加与 SOCKS 策略配合使用的身份。
- 添加一个或多个 SOCKS 策略以管理 SOCKS 流量。

拦截请求故障排除



第 6 章

获取最终用户凭证

本章包含以下部分：

获取最终用户凭证概述

服务器类型/领域	身份验证方案	支持的网络协议	备注
Active Directory	Kerberos NTLMSSP 基本	HTTP，HTTPS 本地 FTP，FTP over HTTP SOCKS（基本身份验证）	仅标准模式支持 Kerberos。在云连接器模式下不受支持。
LDAP	基本	HTTP，HTTPS 本地 FTP，FTP over HTTP SOCKS	—

身份验证任务概述

步骤	任务	相关主题和程序的链接
1	创建身份验证领域。	• 如何创建 Active Directory 身份验证领域（NTLMSSP 和基本），第 90 页 • 创建 LDAP 身份验证领域，第 92 页
2	配置全局身份验证设置。	• 配置全局身份验证设置，第 96 页
3	配置外部身份验证。 可通过外部 LDAP 或 RADIUS 服务器对用户进行身份验证。	• 外部身份验证，第 86 页
4	（可选）创建其他身份验证领域并对其进行排序。 为每一个身份验证协议以及计划使用的方案组合创建至少一个身份验证领域。	• 创建身份验证序列，第 102 页
5	（可选）配置凭证加密。	• 配置凭证加密，第 111 页
6	创建身份标识配置文件以根据身份验证要求对用户和客户端软件进行分类。	• 用户和客户端软件分类，第 115 页
7	创建策略以管理来自您为其创建身份标识配置文件的用户和用户组的 Web 请求。	• 通过策略管理 Web 请求的最佳实践，第 177 页

身份验证最佳实践

- 尽可能少地创建 Active Directory 领域。多个 Active Directory 领域在进行身份验证时需占用更多内存。
- 如果使用 NTLMSSP，则利用网络安全设备或上游代理服务器对用户进行身份验证，但不可同时利用两者。（推荐使用网络安全设备）
- 如果使用 Kerberos，请利用网络安全设备进行身份验证。
- 为了获得最佳性能，使用单个领域在同一子网上进行客户端身份验证。
- 已知一些用户代理具有计算机凭证或身份验证失败问题，这些问题可能会对正常操作产生负面影响。应绕过使用这些用户代理的身份验证。请参阅绕过有问题的用户代理的身份验证，第 104 页。

身份验证计划

- Active Directory/Kerberos，第 79 页
- Active Directory/基本，第 80 页

- Active Directory/NTLMSSP， 第 81 页
- LDAP/基本， 第 81 页
- 透明地识别用户， 第 82 页

Active Directory/Kerberos

显式转发	透明，基于 IP 的缓存	透明，基于 Cookie 的缓存
优点： • 与 NTLM 相比，性能和互操作性更佳 • 适用于已加入域的 Windows 和非 Windows 客户端 • 所有浏览器和大多数其他应用均支持 • 基于 RFC • 开销小 • 适用于 HTTPS (CONNECT) 请求 • 由于未将密码传输至身份验证服务器，故更安全 • 对连接，而不是主机或 IP 地址进行身份验证 • 将客户端应用配置为信任网络安全设备时，在 Active Directory 环境中实现真正的单点登录	优点： • 与 NTLM 相比，性能和互操作性更佳 • 适用于已加入域的 Windows 和非 Windows 客户端 • 适用于所有主要浏览器 • 利用不支持身份验证的用户代理，用户仅需要首先在受支持浏览器中进行身份验证 • 开销相对较低 • 适用于 HTTPS 请求（如果用户之前已利用 HTTP 请求进行身份验证）	优点： • 与 NTLM 相比，性能和互操作性更佳 • 适用于已加入域的 Windows 和非 Windows 客户端 • 适用于所有主要浏览器 • 身份验证与用户而不是主机或 IP 地址相关联 缺点： • 各个新的 Web 域均需要整个身份验证过程，因为 Cookie 特定于域 • 需要启用 Cookie • 对于 HTTPS 请求不起作用

Active Directory/基本

显式转发	透明，基于 **IP** 的缓存	透明，基于 **Cookie** 的缓存
优点： • 所有浏览器和大多数其他应用均支持 • 基于 RFC • 开销小 • 适用于 HTTPS (CONNECT) 请求 • 由于未将密码传输至身份验证服务器，故更安全 • 对连接，而不是主机或 IP 地址进行身份验证 • 将客户端应用配置为信任网络安全设备时，在 Active Directory 环境中实现真正的单点登录 缺点： • 以明文 (Base64) 形式发送各请求的密码 • 无单点登录 • 中等开销：需要对各个新连接重新进行身份验证 • 主要是仅在 Windows 和主要浏览器上受支持	优点： • 适用于所有主要浏览器 • 利用不支持身份验证的用户代理，用户仅需要首先在受支持浏览器中进行身份验证 • 开销相对较低 • 适用于HTTPS请求（如果用户之前已利用 HTTP 请求进行身份验证） 缺点： • 身份验证凭证与 IP 地址而不是用户相关联（不适用于 Citrix 和 RDP 环境；或者，用户如更改 IP 地址，亦不适用） • 无单点登录 • 以明文 (Base64) 形式发送密码	优点： • 适用于所有主要浏览器 • 身份验证与用户而不是主机或 IP 地址相关联 缺点： • 各个新的 Web 域均需要整个身份验证过程，因为 Cookie 特定于域 • 需要启用 Cookie • 对于 HTTPS 请求不起作用 • 无单点登录 • 以明文 (Base64) 形式发送密码

Active Directory/NTLMSSP

显式转发	透明
优点： • 由于未将密码传输至身份验证服务器，故更安全 • 对连接，而不是主机或 IP 地址进行身份验证 • 将客户端应用配置为信任网络安全设备时，在 Active Directory 环境中实现真正的单点登录 缺点： • 中等开销：需要对各个新连接重新进行身份验证 • 主要是仅在 Windows 和主要浏览器上受支持	优点： • 更灵活 透明NTLMSSP身份验证类似于透明基本身份验证，除了 Web 代理使用质询和响应而不是基本明文用户名和密码与客户端进行通信。 使用透明 NTLM 身份验证的优点和缺点与使用透明基本身份验证的优点和缺点相同，除了**透明 NTLM 身份验证具备不向身份验证服务器发送密码的新增优势，且将客户端应用配置为信任网络安全设备时，可实现单点登录**。

LDAP/基本

显式转发	透明
优点： • 基于 RFC • 较之 NTLM，支持更多浏览器 • 开销小 • 适用于 HTTPS (CONNECT) 请求 缺点： • 无单点登录 • 以明文 (Base64) 形式发送各请求的密码 解决方法： • 身份验证失败，第 103 页	优点： • 与显式转发比较，更灵活 • 较之 NTLM，支持更多浏览器 • 利用不支持身份验证的用户代理，用户仅需要首先在受支持浏览器中进行身份验证 • 开销相对较低 • 适用于 HTTPS 请求（如果用户之前已利用 HTTP 请求进行身份验证） 缺点： • 无单点登录 • 以明文 (Base64) 形式发送密码 • 身份验证凭证与 IP 地址而不是用户相关联（不适用于 Citrix 和 RDP 环境；或者，用户如更改 IP 地址，亦不适用） 解决方法： • 身份验证失败，第 103 页

透明地识别用户

按传统方式，系统通过提示用户输入用户名和密码来识别用户并对其进行身份验证。系统根据身份验证服务器来验证这些凭证，Web 代理随后再根据通过身份验证的用户名，将合适的策略应用于事务。

但是，您可以配置网络安全设备以透明方式验证用户身份，即不提示最终用户输入凭证。透明标识通过从另一受信任源获取的凭证对用户进行身份验证（假定该受信任源已对用户进行身份验证），然后应用适当的策略。

您可能希望透明地标识用户以便：

- 创建单点登录环境，以便用户并不知悉网络上存在代理。
- 要将基于身份验证的策略应用至来自客户端应用（无法向最终用户显示身份验证提示）的事务。

透明标识用户仅影响 Web 代理获取用户名和分配标识配置文件的方式。获取用户名并分配标识配置文件后，Web 代理正常情况下会应用所有其他策略，而不考虑分配标识配置文件的方式。

如果透明身份验证失败，则可以配置如何处理事务：可以授予用户访客接入权限，或者可以强制执行向用户显示身份验证提示。

由于透明用户识别失败而向最终用户显示身份验证提示，并且由于凭证无效而无法对用户进行身份验证时，可选择是否允许用户访客接入。

注释 启用重新身份验证并通过URL过滤阻止事务时，系统将显示最终用户通知页面，其中包含用于以不同用户登录的选项。用户点此链接则会收到进行身份验证的提示。有关详细信息，请参阅授权失败：允许使用不同凭证进行重新验证，第 107 页。

了解透明用户识别

可用的透明用户识别方法有：

- **利用 ISE 透明识别用户** - 在启用身份服务引擎 (ISE) 服务（“网络”(Network) >“身份服务引擎”(Identity Services Engine)）后可用。对于这些事务，将从身份服务引擎服务器获取用户名和相关联安全组标记。请参阅认证和集成 ISE 服务任务，第 131 页。
- **利用 ASA 透明标识用户** - 用户按从思科适应安全设备收到的当前 IP 地址到用户名的映射进行标识（仅适用于远程用户）。启用 AnyConnect 安全移动并与 ASA 集成时，该选项可用。将从 ASA 获取用户名，并从网络安全设备上指定的身份验证领域或序列获取关联的目录组。请参阅远程用户，第 195 页。
- **利用身份验证领域透明标识用户** - 使用以下身份验证服务器之一配置一个或多个身份验证领域以支持透明识别时，此选项可用。
  - **Active Directory** - 创建 NTLM 或 Kerberos 身份验证领域，然后启用透明用户识别。此外，必须部署单独的 Active Directory 代理，例如 Cisco Context Directory Agent。有关详细信息，请参阅利用 Active Directory 进行透明用户识别，第 83 页。
  - **LDAP** - 创建配置为 eDirectory 的 LDAP 身份验证领域，然后启用透明用户识别。有关详细信息，请参阅利用 LDAP 进行透明用户识别，第 84 页。

AsyncOS for Web 定期与 eDirectory 或 Active Directory 代理通信，以维持将经身份验证用户名与其当前 IP 地址匹配的映射。

利用 Active Directory 进行透明用户识别

Active Directory 并不会以易于其他系统（例如网络安全设备）查询的格式记录用户登录信息。如要在 Active Directory 安全事件日志中查询已通过身份验证的用户的相关信息，思科 Context Directory Agent (CDA) 等 Active Directory 代理必不可少。

AsyncOS for Web 与 Active Directory 代理进行通信以维护 IP 地址到用户名映射的本地副本。AsyncOS for Web 需要将 IP 地址与用户名相关联时，首先检查其映射本地副本。如果未发现匹配项，则查询 Active Directory 代理找到匹配项。

有关安装和配置 Active Directory 代理的详细信息，请参阅下文中的“设置 Active Directory 代理以向网络安全设备提供信息”一节。

利用 Active Directory 透明地识别用户时，请注意：

- 利用 Active Directory 的透明用户识别仅适用于 NTLM 或 Kerberos 身份验证方案。无法将其与对应于 Active Directory 实例的 LDAP 身份验证领域结合使用。
- 透明用户识别适用于 Active Directory 代理支持的 Active Directory 版本。
- 可以在另一台计算机上安装第二个 Active Directory 代理实例以获取高可用性。执行此操作时，各个 Active Directory 代理均独立于其他代理维护 IP 地址到用户名的映射。如果主代理 3 次 ping 不通，AsyncOS for Web 则会使用备用 Active Directory 代理。
- Active Directory 代理与网络安全设备通信时使用按需模式。
- Active Directory 代理将用户注销信息推送至网络安全设备。有时，某些用户注销信息并未记录在 Active Directory 安全日志中。如果客户端计算机崩溃或如果用户关闭计算机但未注销，则可能出现这种情况。如果安全日志中无用户注销信息，则 Active Directory 代理无法告知设备不再将 IP 地址分配给该用户。要消除这种可能性，可以定义 AsyncOS 缓存 IP 地址到用户映射的时间，在该时间，无来自 Active Directory 代理的更新。有关详细信息，请参阅使用 CLI 配置高级透明用户识别设置，第 85 页。
- Active Directory 代理记录从特定 IP 地址登录的各用户 `sAMAccountName`以确保用户名唯一。
- 客户端计算机向 Active Directory 服务器和网络安全设备呈现的客户端 IP 地址必须相同。
- AsyncOS for Web 仅搜索用户直接父组。不搜索嵌套组。

设置 Active Directory 代理以向网络安全设备提供信息

由于 AsyncOS for Web 无法直接从 Active Directory 获取客户端 IP 地址，必须从 Active Directory 代理获取 IP 地址到用户名映射信息。

将 Active Directory 代理安装在网络中的计算机上，该计算机能够从网络安全设备访问并且能够与所有可见 Windows 域控制器进行通信。为获取最佳性能，该代理在物理连接上应尽可能地靠近网络安全设备。在小型网络环境中，可能希望将 Active Directory 代理直接安装到 Active Directory 服务器上。

注释 用于与网络安全设备进行通信的 Active Directory 代理实例也可支持其他设备，包括思科自适应安全设备和其他网络安全设备。

获取、安装和配置思科 Context Directory Agent

可以在此处找到关于下载、安装和配置思科 Context Directory Agent 的信息：http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html。

注释 网络安全设备和 Active Directory 代理使用 RADIUS 协议与彼此通信。设备和代理必须配置相同的共享密钥以模糊处理用户密码。其他用户属性不模糊处理。

利用 LDAP 进行透明用户识别

AsyncOS for Web 能够与 eDirectory 服务器（配置为维持 IP 地址到用户名映射的轻量级目录访问协议 (LDAP) 领域）进行通信。用户通过 eDirectory 客户端登录时，根据 eDirectory 服务器对用户进行身份验证。身份验证成功后，客户端 IP 地址即作为登录用户的一个属性（网络地址）记录于 eDirectory 服务器中。

使用 LDAP (eDirectory) 透明标识用户时，考虑以下选项：

- 必须将 eDirectory 客户端安装在各客户端工作站上，且最终用户必须根据 eDirectory 服务器将其用于身份验证。
- eDirectory 客户端登录所使用的 LDAP 树必须与身份验证领域中所配置的 LDAP 树相同。
- 如果 eDirectory 客户端使用多个 LDAP 树，则创建用于各个树的身份验证领域，然后创建使用各个 LDAP 身份验证领域的身份验证序列。
- 将 LDAP 身份验证领域配置为 eDirectory 时，必须指定用于查询凭证的 Bind DN。
- 用户登录时必须配置 eDirectory 服务器以更新用户对象的 NetworkAddress 属性。
- AsyncOS for Web 仅搜索用户直接父组。不搜索嵌套组。
- 可以使用 eDirectory 用户的 NetworkAddress 属性确定用户的最近登录 IP 地址。

关于透明用户识别的规则和准则

将透明用户识别与任何身份验证服务器结合使用时，请考虑以下规则和准则：

- 使用 DHCP 将 IP 地址分配至客户端计算机时，确保网络安全设备上的 IP 地址到用户名映射的更新比 DHCP 租用的更新更频繁些。使用 `tuiconfig` CLI 命令更新映射更新间隔。有关详细信息，请参阅使用 CLI 配置高级透明用户识别设置，第 85 页。
- 如果在网络安全设备上的 IP 地址到用户名映射更新前，用户退出计算机而另一用户登录到同一计算机，则 Web 代理将此客户端记录为上一个用户。
- 可以配置透明用户识别失败时 Web 代理处理事务的方式。可以授予用户访客接入权限，或者可以强制向最终用户显示身份验证提示。
- 由于透明用户识别失败而向用户显示身份验证提示，并且由于凭证无效而无法对用户进行身份验证时，可选择是否允许用户以访客身份接入。
- 分配的标识配置文件将身份验证序列与用户存在于其中的多个领域结合使用时，AsyncOS for Web 从领域中获取用户组，顺序如其出现在序列中的顺序。
- 配置标识配置文件透明识别用户时，身份验证代理必须为 IP 地址。无法选择不同的代理类型。
- 查看用户事务详细信息时，“网络跟踪”(Web Tracking) 页面会显示已透明识别哪些用户。

- 可使用 %m 和 x-auth-mechanism 自定义字段将透明标识用户记录到访问和 WC3 日志中。SSO_TUI 日志条目表示用户名通过将客户端 IP 地址与使用透明用户识别完成身份验证的用户名匹配获取。（同样，SSO_ASA 值表示用户是远程用户，用户名从使用 AnyConnect 安全移动的思科 ASA 中获取。）

配置透明用户识别

有关配置透明用户识别和授权的详细信息，请参见获取最终用户凭证，第 77 页。基本步骤是：

- 创建身份验证领域并对其进行排序。
- 创建身份标识配置文件以对用户和客户端软件进行分类。
- 创建策略以管理来自已标识用户和用户组的 Web 请求。

使用 CLI 配置高级透明用户识别设置

AsyncOS for Web 提供以下 TUI 相关 CLI 命令：

- **tuiconfig** – 配置与透明用户识别相关的高级设置。批量模式可用于同时配置多个参数。
  - **配置 Active Directory 代理映射超时** - 以分钟为单位的时间长度。当无来自代理的更新时，将在此时间里为 AD 代理检索的 IP 地址缓存“IP 地址-用户”映射。
  - **配置 Active Directory 代理的代理缓存超时** - 以秒为单位的时间长度，将在此时间里缓存特定代理的“IP 地址-用户”映射；有效值范围为 5 到 1200 秒。默认值和建议值均为 120 秒。指定较低值可能会对代理性能产生不利影响。
  - **配置 Novell eDirectory 映射超时** - 以分钟为单位的时间长度。当无来自服务器的更新时，将在此时间里为从 eDirectory 服务器检索的 IP 地址缓存 IP 地址-用户映射。
  - **配置 Active Directory 代理查询等待时间** - 等待 Active Directory 代理应答的时间长度（以秒为单位）。查询时间超过该值时，则认为透明用户识别已失败。这限制最终用户所经历的身份验证延迟。
  - **配置 Novell eDirectory 查询等待时间** - 等待 eDirectory 服务器应答的时间长度（以秒为单位）。查询时间超过该值时，则认为透明用户识别已失败。这限制最终用户所经历的身份验证延迟。

Active Directory 设置适用于所有使用 AD 代理进行透明用户识别的 AD 领域。eDirectory 设置适用于所有使用 eDirectory 进行透明用户识别的 LDAP 领域。

如果验证对于任一参数均无效，则所有值均不变。

- **tuistatus** - 该命令提供以下 AD 相关子命令：
  - **adagentstatus** - 显示所有 AD 代理当前状态，及其与 Windows 域控制器连接的相关信息。
  - **listlocalmappings** - 列出存储在网络安全设备上的所有 IP 地址到用户名映射，可以通过 AD 代理进行检索。但并未列出存储于代理上的条目，也未列出当前正在进行查询的映射。

配置单点登录

透明地获取凭证有利于单点登录环境。透明用户识别是一项身份验证领域设置。

对于 Internet Explorer，请确保“重定向主机名”(Redirect Hostname) 是短主机名（不含点号）或 NetBIOS 名称，而非完全限定域名。或者，可以将设备主机名添加至 Internet Explorer 的本地内联网区域（“工具”(Tools) > “互联网选项”(Internet options) > “安全”(Security) 选项卡）；然而，这在每个客户端上均需完成。有关与此相关的详细信息，请参阅如何利用 SSO 准确设置 NTLM（透明发送凭据）？

使用 Firefox 和其他非 Microsoft 浏览器时，必须将参数 **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris** 和 **network.automatic-ntlm-auth.trusted-uris** 设置为透明模式重定向主机名。还可参阅 Firefox 不透明发送身份验证凭证 (SSO)。该文章提供有关更改 Firefox 参数的一般信息。

有关重定向主机名的信息，请参阅配置全局身份验证设置，第 96 页或 CLI 命令 `sethostname`。

身份验证领域

身份验证领域定义联系身份验证服务器所需详细信息，并指定与客户端通信时使用的身份验证方案。AsyncOS 支持多个身份验证领域。领域也可以分组为允许通过相同策略管理具有不同身份验证要求的用户的身份验证序列。

- 外部身份验证，第 86 页
- 创建用于 Kerberos 身份验证方案的 Active Directory 领域，第 87 页
- 如何创建 Active Directory 身份验证领域（NTLMSSP 和基本），第 90 页
- 创建 LDAP 身份验证领域，第 92 页
- 有关删除身份验证领域，第 96 页
- 配置全局身份验证设置，第 96 页

相关主题

- 身份验证序列，第 101 页
- RADIUS 用户身份验证，第 387 页

外部身份验证

可通过外部 LDAP 或 RADIUS 服务器对用户进行身份验证。

通过 LDAP 服务器配置外部身份验证

开始之前

创建 LDAP 身份验证领域，并利用一个或多个外部身份验证查询进行配置。创建 LDAP 身份验证领域，第 92 页。

步骤 1 在设备上启用外部身份验证：

a) 导航至**系统管理 (System Administration)** > **用户 (Users)**。

b) 点击“外部身份验证”(External Authentication) 部分中的**启用 (Enable)**。

c) 配置选项：

选项	说明
启用外部身份验证 (Enable External Authentication)	—
身份验证类型 (Authentication Type)	选择 LDAP。
外部身份验证缓存超时 (External Authentication Cache Timeout)	AsyncOS 再次联系 LDAP 服务器以重新进行身份验证前存储外部身份验证凭证的秒数。默认值为零 (0)。
LDAP 外部身份验证查询 (LDAP External Authentication Query)	利用 LDAP 领域配置的查询。
等待服务器的有效响应超时 (Timeout to wait for valid response from server)	AsyncOS 等待向服务器查询做出响应的秒数。
组映射 (Group Mapping)	对于目录中各用户组名称，分配一个角色。

步骤 2 提交并确认更改。

启用 RADIUS 外部身份验证

请参阅使用 RADIUS 启用外部身份验证，第 387 页。

创建用于 Kerberos 身份验证方案的 Active Directory 领域

开始之前

- 确保在标准模式（而不是云连接器模式）中配置设备。
- 准备 Active Directory 服务器。
  - 在以下服务器之一上安装 Active Directory：Windows 服务器 2003、2008、2008R2 或 2012。
  - 在 Active Directory 服务器上创建用户：
    - 在 Active Directory 服务器上创建一个用户，此用户是域管理员组或帐户操作员组的成员。

      或

    - 创建具有以下权限的用户名：
      - Active Directory 重置密码权限
      - 已验证写入 servicePrincipalName 权限
      - 写帐户限制

- 写 dNShost 名称
- 写 servicePrincipalName

  这些是用户名所需的最低 Active Directory 权限，以便将设备加入域并确保其完全正常运行。

- 将您的客户端加入该域。支持的客户端包括 Windows XP、Windows 7 和 Mac OS 10.5 及更高版本。
- 利用 Windows 资源套件中的 kerbtray 工具验证客户端上的 Kerberos 票证：http://www.microsoft.com/en-us/download/details.aspx?id=17657。
- 可通过主菜单 >“密钥串访问”(KeyChain Access)，查看 Kerberos 票证，访问 Mac 客户端上的票证查看应用。

- 确保您拥有将网络安全设备加入到要根据其完成身份验证的 Active Directory 域所需的权限和域信息。
- 将网络安全设备上的当前时间与 Active Directory 服务器上的当前时间进行比较，验证差异不超过 Active Directory 服务器“计算机时钟同步最高容差”(Maximum tolerance for computer clock synchronization) 选项指定的时间。
- 如果安全管理设备托管网络安全设备，请做好准备，确保不同网络安全设备上相同名称的身份验证领域在每个设备上都有一致的已定义属性。
- 网络安全设备配置：
  - 在显式模式下，在浏览器中配置的 WSA 主机名（CLI 命令 `sethostname`）和代理名称必须相同。
  - 在透明模式下，WSA 主机名必须与重定向主机名相同（请参阅配置全局身份验证设置，第 96 页）。此外，创建 Kerberos 领域前，必须配置 WSA 主机名和重定向主机名。
- 请注意，确认新领域后即无法更改领域的身份验证协议。
- 请注意，必须在客户端浏览器上配置单点登录 (SSO)；请参阅配置单点登录，第 85 页。
- 为简化日志使用过程，可自定义访问日志，以使用 %m 自定义字段参数。请参阅自定义访问日志，第 361 页。

步骤 1 在思科网络安全设备界面中，依次选择 **网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击**添加领域 (Add Realm)**。

步骤 3 将仅使用字母数字和空格字符的唯一名称分配给身份验证领域。

步骤 4 在“身份验证协议”(Authentication Protocol) 字段中，选择 **Active Directory** 。

步骤 5 最多输入三个适用于 Active Directory 服务器的完全限定域名或 IP 地址。

示例：`ntlm.example.com`。

仅当在设备上配置的 DNS 服务器无法解析 Active Directory 服务器主机名时，才需要 IP 地址。

在领域中配置多个身份验证服务器时，无法授权该领域内事务前，设备尝试授权多达三个身份验证服务器。

步骤 6 将设备连接至域：

a) 配置 Active Directory 帐户：

设置	说明
Active Directory 域	Active Directory 服务器第 3 个域名。也称为 DNS 域或领域。
NetBIOS 域名 (NetBIOS domain name)	如果网络使用 NetBIOS，则提供域名。 **提示** 如果此选项不可用，请使用 `setntlmsecuritymode` CLI 命令验证 NTLM 安全模式是否已设置为“domain”。
计算机帐户	指定在 Active Directory 域内的位置，其中，AsyncOS 将创建 Active Directory 计算机帐户（也称为“计算机信任帐户”）以唯一标识域上的计算机。 如果 Active Directory 环境以特定时间间隔自动删除计算机对象，则指定位于容器内的计算机帐户的位置，以防自动删除。

b) 点击**连接域 (Join Domain)**。

注释 如果尝试加入您已加入的域（即使使用相同的凭证），现有连接将会关闭，因为 Active Directory 会将一组新密钥发送到所有客户端，包括此 WSA。受影响的客户端将需要注销并再次重新登录。

c) 为 Active Directory 中的帐户提供登录凭证（用户名和密码），然后点击“创建帐户”(Create Account)。

步骤 7 （可选）配置透明用户识别。

设置	说明
使用 Active Directory 代理启用透明用户标识 (Enable Transparent User Identification using Active Directory agent)	输入已安装主 Context Directory 代理的计算机的服务器名称及访问该计算机的共享密钥。 （可选）输入已安装备份 Context Directory 代理的计算机的服务器名称及其共享密钥。

步骤 8 配置网络安全：

设置	说明
需要客户端签名 (Client Signing Required)	如果将 Active Directory 服务器配置为需要客户端签名，则选择该选项。 如选中此选项，与 Active Directory 服务器通信时，AsyncOS 会使用传输层安全。

步骤 9 （可选）点击**开始测试 (Start Test)**。这将测试您输入的设置，在实际用户使用它们进行身份验证之前确保其正确性。有关进行测试的详细信息，请参阅使用多个 NTLM 领域和域，第 96 页。

步骤 10 对在测试期间发现的任何问题进行故障排除。请参阅排除身份验证工具故障，第 425 页

步骤 11 提交并确认更改。

下一步做什么

创建使用 Kerberos 身份验证方案的标识配置文件。用户和客户端软件分类，第 115 页。

如何创建 Active Directory 身份验证领域（NTLMSSP 和基本）

创建 Active Directory 身份验证领域（NTLMSSP 和基本）的先决条件

- 确保您拥有将网络安全设备加入到要根据其完成身份验证的 Active Directory 域所需的权限和域信息。
- 如果您计划使用“domain”作为 NTLM 安全模式，仅可使用 Active Directory 嵌套组。如果 Active Directory 组未嵌套，则使用默认值“ads”。请参阅本指南“命令行界面”附录中的 `setntlmsecuritymode`。
- 将网络安全设备上的当前时间与 Active Directory 服务器上的当前时间进行比较，验证差异不超过 Active Directory 服务器“计算机时钟同步最高容差”(Maximum tolerance for computer clock synchronization) 选项指定的时间。
- 如果安全管理设备托管网络安全设备，请做好准备，确保不同网络安全设备上相同名称的身份验证领域在每个设备上都有一致的已定义属性。
- 请注意，确认新领域后即无法更改领域的身份验证协议。
- WSA 需要连接到所有受信任域的域控制器，以及连接到 NTLM 领域的配置的域控制器。为了能正确执行身份验证，您需要对内部域和外部域上的所有域控制器打开以下端口：
  - LDAP（389 UDP 和 TCP）
  - Microsoft SMB (445 TCP)
  - Kerberos (88 UDP)
  - 终端分辨率 - 端口映射程序 (135 TCP) 网络登录固定端口
- 对于 NTLMSSP，可以在客户端浏览器上配置单点登录 (SSO)。请参阅配置单点登录，第 85 页。

关于使用多个 NTLM 领域和域

下列规则适用于使用多个 NTLM 领域和域的情况：

- 最多可创建 10 个 NTLM 身份验证领域。
- 一个 NTLM 领域中的客户端 IP 地址不得与另一 NTLM 领域的客户端 IP 地址重叠。
- 每个 NTLM 领域只能加入一个 Active Directory 域，但可以通过该域信任的任何域对用户进行身份验证。默认情况下，这种信任适用于同一域林中的其他域以及至少存在一个单向信任的林外域。
- 创建更多 NTLM 领域以对不受现有 NTLM 领域信任的域中的用户进行身份验证。

创建 Active Directory 身份验证领域（NTLMSSP 和基本）

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击**添加领域 (Add Realm)**。

步骤 3 将仅使用字母数字和空格字符的唯一名称分配给身份验证领域。

步骤 4 在“身份验证协议和方案”(Authentication Protocol and Scheme(s)) 字段中，选择 **Active Directory**。

步骤 5 最多输入三个适用于 Active Directory 服务器的完全限定域名或 IP 地址。

示例：`active.example.com`。

仅当在设备上配置的 DNS 服务器无法解析 Active Directory 服务器主机名时，才需要 IP 地址。

在领域中配置多个身份验证服务器时，无法授权该领域内事务前，设备尝试授权多达三个身份验证服务器。

步骤 6 将设备连接至域：

a) 配置 Active Directory 帐户：

设置	说明
Active Directory 域	Active Directory 服务器域名。也称为 DNS 域或领域。
NetBIOS 域名 (NetBIOS domain name)	如果网络使用 NetBIOS，则提供域名。
计算机帐户	指定一个在 Active Directory 域内的位置，其中，AsyncOS 将创建 Active Directory 计算机帐户（也称为“计算机信任帐户”）以唯一地标识域中计算机。 如果 Active Directory 环境以特定时间间隔自动删除计算机对象，则指定位于容器内的计算机帐户的位置，以防自动删除。

b) 点击**连接域 (Join Domain)**。

注释 如果尝试加入您已加入的域（即使使用相同的凭证），现有连接将会关闭，因为 Active Directory 会将一组新密钥发送到所有客户端，包括此 WSA。受影响的客户端将需要注销并再次重新登录。

c) 输入具有在域中创建计算机帐户权限的现有 Active Directory 用户的 sAMAccountName 用户名和密码。

例如：“`jazzdoe`”。请勿使用“`DOMAIN\jazzdoe`”或“`jazzdoe@domain`”。

此信息仅在建立计算机帐户时使用一次，而且不保存。

d) 点击**创建帐户 (Create Account)**。

步骤 7 （可选）配置透明身份验证。

设置	说明
使用 Active Directory 代理启用透明用户标识 (Enable Transparent User Identification using Active Directory agent)	输入已安装主 Context Directory 代理的计算机的服务器名称及访问该计算机的共享密钥。 （可选）输入已安装备份 Context Directory 代理的计算机的服务器名称及其共享密钥。

步骤 8 配置网络安全：

设置	说明
需要客户端签名 (Client Signing Required)	如果将 Active Directory 服务器配置为需要客户端签名，则选择该选项。 如选中此选项，与 Active Directory 服务器通信时，AsyncOS 会使用传输层安全。

步骤 9 （可选）点击**开始测试 (Start Test)**。这会测试已输入的设置，确保真实用户将这些设置用于身份验证前正确。

步骤 10 提交并确认更改。

创建 LDAP 身份验证领域

开始之前

- 获取有关贵组织中 LDAP 的以下信息：
  - LDAP 版本
  - 服务器地址
  - LDAP 端口
- 如果安全管理设备托管网络安全设备，请确保不同网络安全设备上相同名称的身份验证领域在每个设备上都有一致的已定义属性。

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击**添加领域 (Add Realm)**。

步骤 3 将仅使用字母数字和空格字符的唯一名称分配给身份验证领域。

步骤 4 在“身份验证协议和方案”(Authentication Protocol and Scheme(s)) 字段中，选择 **LDAP**。

步骤 5 输入 LDAP 身份验证设置：

设置	说明
LDAP 版本 (LDAP Version)	选择 LDAP 版本，并选择是否使用安全 LDAP。 设备支持 LDAP 版本 2 和版本 3。安全 LDAP 需要 LDAP 版本 3。 选择该 LDAP 服务器是否支持 Novell eDirectory 与透明用户识别结合使用。

设置	说明
LDAP 服务器 (LDAP Server)	输入 LDAP 服务器的 IP 地址或主机名及其端口号。最多可指定 3 个服务器。 主机名必须是完全限定域名。例如，`ldap.example.com`。只有在设备配置的 DNS 服务器无法解析 LDAP 服务器主机名的情况下，才需要 IP 地址。 标准 LDAP 的默认端口号为 389。安全 LDAP 的默认端口号为 636。 如果 LDAP 服务器为 Active Directory 服务器，请在此输入主机名或 IP 地址，以及域控制器的端口。请尽可能输入全局目录服务器的名称并使用 3268 端口。但是，如果全局目录服务器物理距离远并且您只需要对本地域控制器上的用户进行身份验证时，您可能想要使用本地域控制器。 **注：**领域中配置多个身份验证服务器时，在该领域内事务授权失败之前，设备最多会尝试使用 3 个身份验证服务器进行授权。
LDAP 持久性连接 (LDAP Persistent Connections) （位于“高级”(Advanced) 部分下）	选择以下其中一个值： • **使用持久性连接（无限制）(Use persistent connections [unlimited])**。使用现有连接。如果无连接可用，则打开新连接。 • **使用永久性连接 (Use persistent connections)**。使用现有连接来满足指定请求的数量。达到最大值时，建立与 LDAP 服务器的新连接。 • **不使用持久性连接 (Do not use persistent connections)**。始终创建与 LDAP 服务器的新连接。
用户身份验证 (User Authentication)	在以下字段中输入值： **基础可分辨名称（基础 DN）(Base Distinguished Name [Base DN])** LDAP 数据库为树型目录结构，设备使用基础 DN 导航到 LDAP 目录树的正确位置后开始搜索。有效的基础 DN 过滤器字符串由一个或多个表单 `object-value` 组件构成。例如 `dc=companyname, dc=com`。 **用户名属性 (User Name Attribute)** 选择以下其中一个值： • **Uid**、**cn** 和 **sAMAccountName**。LDAP 目录中指定用户名的唯一标识符。 • **自定义 (custom)**。自定义标识符，例如 `UserAccount`。 **用户过滤器查询 (User Filter Query)** 用户过滤器查询是一种查找用户基础 DN 的 LDAP 搜索过滤器。如果用户目录位于基础 DN 以下的层次结构，或登录名未包含在该用户基础 DN 的用户特定组件中，则用户过滤器查询必不可少。 选择以下其中一个值： • **无 (none)**。过滤所有用户。 • **自定义 (custom)**。过滤某特定用户组。

设置	说明
查询凭证 (Query Credentials)	选择身份验证服务器是否接受匿名查询。 如果身份验证服务器接收匿名查询，则选择**服务器接受匿名查询 (Server Accepts Anonymous Queries)**。 如果身份验证服务器不接收匿名查询，则选择**使用 Bind DN (Use Bind DN)**，然后输入以下信息： • **绑定 DN (Bind DN)**。允许外部 LDAP 服务器上的用户搜索 LDAP 目录。通常应允许绑定 DN 搜索整个目录。 • **密码 (Passphrase)**。密码与在“绑定 DN”(Bind DN) 字段中输入的用户相关联。 下列文本列出“绑定 DN”(Bind DN) 字段的某些示例用户： cn=administrator，cn=Users，dc=domain，dc=com sAMAccountName=jdoe，cn=Users，dc=domain，dc=com。 如果 LDAP 服务器是 Active Directory 服务器，也可以输入“绑定 DN”(Bind DN) 用户名作为“DOMAIN\username”。

步骤 6 （可选）请通过组对象或用户对象启用组身份验证，并相应地完成所选选项的相关设置：

组对象设置	说明
组对象中组成员属性 (Group Membership Attribute Within Group Object)	选择列出属于该组的所有用户的 LDAP 属性。 选择以下其中一个值： • **成员 (member)** 和**唯一成员 (uniquemember)**。指定组成员于 LDAP 目录中的唯一标识符。 • **自定义 (custom)**。自定义标识符，例如 `UserInGroup`。
包含组名的属性 (Attribute that Contains the Group Name)	选择指定可用于策略组配置中的组名的 LDAP 属性。 选择以下其中一个值： • **cn**。LDAP 目录中指定组名的唯一标识符。 • **自定义 (custom)**。自定义标识符，例如 `FinanceGroup`。
确定对象是否为组的查询字符串 (Query String to Determine if Object is a Group)	选择一个可确定 LDAP 对象是否表示用户组的 LDAP 搜索过滤器。 选择以下其中一个值： • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.**自定义过滤器，例如 `objectclass=person`。 **注意**：查询定义可用于策略组的身份验证组集。

用户对象设置	说明
用户对象中的组成员身份属性 (Group Membership Attribute Within User Object)	选择列出该用户所属所有组的属性。 选择以下其中一个值： • **memberOf**。LDAP 目录中指定用户成员的唯一标识符。 • **自定义 (custom)**。自定义标识符，例如 `UserInGroup`。
组成员属性为 DN (Group Membership Attribute is a DN)	指定组成员属性是否为指代某 LDAP 对象的可区别名称 (DN)。对于 Active Directory 服务器，请启用该选项。 启用该选项时，必须配置后续设置。
包含组名的属性 (Attribute that Contains the Group Name)	组成员身份属性为 DN 时，这指定可用作为策略组配置中组名称的属性。 选择以下其中一个值： • **cn**。LDAP 目录中指定组名的唯一标识符。 • **自定义 (custom)**。自定义标识符，例如 `FinanceGroup`。
确定对象是否为组的查询字符串 (Query String to Determine if Object is a Group)	选择一个可确定 LDAP 对象是否表示用户组的 LDAP 搜索过滤器。 选择以下其中一个值： • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.**自定义过滤器，例如 `objectclass=person`。 **注**：此查询定义了可在网络安全管理器策略中使用的身份验证组的集合。

步骤 7 （可选）配置用户的外部 LDAP 身份验证

a) 选择**外部身份验证查询 (External Authentication Queries)**。

b) 标识用户帐户：

基本 **DN**	导航至 **LDAP** 目录树中的正确位置以开始搜索的基本 **DN**。

查询字符串 (Query String)	返回身份验证组集的查询，例如：
	`(&(objectClass=posixAccount)(uid={u}))`
	或
	`(&(objectClass=user)(sAMAccountName={u}))`

包含用户全名的属性	LDAP 属性，例如 displayName 或 gecos。

c) （可选）根据 RFC 2307 帐户过期 LDAP 属性，拒绝登录到过期帐户。

d) 提供检索用户组信息的查询。

如果用户属于具有不同用户角色的多个 LDAP 组，AsyncOS 会为用户授予最受限制角色的权限。

基本 DN (Base DN)	导航至 LDAP 目录树中的正确位置以开始搜索的基本 DN。
查询字符串 (Query String)	`(&(objectClass=posixAccount)(uid={u}))`
包含用户全名的属性	`gecos`

步骤 8 （可选）点击**开始测试 (Start Test)**。这将测试您输入的设置，在实际用户使用它们进行身份验证之前确保其正确性。有关进行测试的详细信息，请参阅使用多个 NTLM 领域和域，第 96 页。

注释 一旦提交并确认更改，稍后则无法更改领域身份验证协议。

步骤 9 提交并确认更改。

下一步做什么

创建使用 Kerberos 身份验证方案的标识配置文件。请参阅用户和客户端软件分类，第 115 页。

相关主题

- 外部身份验证，第 86 页

使用多个 NTLM 领域和域

有关使用多个 NTLM 领域和域，以下规则适用：

- 最多可创建 10 个 NTLM 身份验证领域。
- 一个 NTLM 领域中的客户端 IP 地址不得与另一 NTLM 领域的客户端 IP 地址重叠。
- 每个 NTLM 领域只能加入一个 Active Directory 域，但可以通过该域信任的任何域对用户进行身份验证。默认情况下，这种信任适用于同一林中的其他域以及至少存在一个单向信任的林外域。
- 创建更多 NTLM 领域以对不受现有 NTLM 领域信任的域中的用户进行身份验证。

有关删除身份验证领域

删除身份验证领域会禁用相关身份，这反过来会从相关联策略中删除那些身份。

删除身份验证领域会将其从序列中移除。

配置全局身份验证设置

将全局身份验证设置配置为独立于其身份验证协议，将设置应用于所有身份验证领域。

Web 代理的部署模式会影响到可以配置的全局身份验证设置。与显式转发模式相比，以透明模式部署时可用的设置更多。

开始之前

- 熟悉以下概念：

- 身份验证失败，第 103 页
- 授权失败：允许使用不同凭证进行重新验证，第 107 页

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 编辑“全局身份验证设置”(Global Authentication Settings) 部分的设置：

设置	说明
身份验证服务不可用时的操作 (Action if Authentication Service Unavailable)	选择以下其中一个值： • **允许流量在未经身份验证的情况下继续 (Permit traffic to proceed without authentication)**。如用户已通过身份验证一样继续处理。 • **如果用户身份验证失败，则阻止所有流量 (Block all traffic if user authentication fails)**。中断处理，并阻止所有流量。
身份验证失败处理 (Failed Authentication Handling)	在标识配置文件策略中授予用户访客接入权限时，该设置确定 Web 代理如何标识作为访客的用户及将其记录至访问日志中。 有关授予用户访客接入权限的详细信息，请参阅身份验证失败后授予访客接入权限，第 106 页。
重新进行身份验证 (Re-authentication) （“最终用户被URL类别或用户会话限制阻止时启用重新身份验证提示”(Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction)）	如用户因限制性 URL 过滤策略或不允许登录另一 IP 地址而被网站阻止，此设置允许用户重新进行身份验证。 用户会看到一个阻止页面，其中包含可供其输入新身份验证凭证的链接。如果用户输入更高权限的凭证，请求的页面即会显示于浏览器中。 **注**：此设置只适用于因限制性 URL 过滤策略或用户会话限制而被阻止的已通过身份验证的用户。不适用于被无身份验证子网阻止的事务。 有关详细信息，请参阅授权失败：允许使用不同凭证进行重新验证，第 107 页。
基本身份验证令牌 TTL (Basic Authentication Token TTL)	控制用户凭证通过身份验证服务器重新验证之前在缓存中的存储时长。这包括用户名和密码，以及与用户相关联的目录组。 推荐采用默认值设置。如果已配置“代理超时”(Surrogate Timeout) 设置且该值大于“基本身份验证令牌 TTL”(Basic Authentication Token TTL)，则“代理超时”(Surrogate Timeout) 值优先，Web 代理会在代理超时到期后联系身份验证服务器。

其余身份验证设置可否配置，取决于 Web 代理是在透明还是显式转发模式下部署。

步骤 4 如果在透明模式下部署 Web 代理，则编辑以下设置：

设置	说明
凭证加密 (Credential Encryption)	此设置指定客户端是否通过加密 HTTPS 连接向 Web 代理发送登录凭证。 该设置适用于基础身份验证方案和 NTLMSSP 身份验证方案，但特别适用于基础身份验证方案，因为用户凭证以纯文本形式进行发送。 有关详细信息，请参阅身份验证失败，第 103 页。
HTTPS 重定向端口 (HTTPS Redirect Port)	为通过 HTTPS 连接验证用户身份的重定向请求指定一个可用 TCP 端口。 此设置可指定客户端将通过哪个端口使用 HTTPS 打开 Web 代理的连接。启用凭证加密或使用访问控制并提醒用户进行身份验证时，会出现这种情况。
重定向主机名 (Redirect Hostname)	输入网络接口短主机名，在该网络接口上，Web 代理侦听传入连接。 当在透明模式下部署的设备上配置身份验证时，Web 代理将该主机名用于发送至客户端以对用户进行身份验证的重定向 URL 中。 可以输入以下值之一： • **单字主机名 (Single word hostname)**。您可以输入可由客户端和网络安全设备进行 DNS 解析的单个单词的主机名。这让客户端能够利用 Internet Explorer 实现真正的单点登录，而无需更多浏览器端设置。请务必输入可由客户端和网络安全设备进行 DNS 解析的单字主机名。例如，如果您的客户端在域 mycompany.com 且 Web 代理侦听的接口具有完整主机名 **`proxy.mycompany.com`**，则应该在此字段中输入 **`代理 (Proxy)`**。客户端在代理上执行查找，并应能够解析 **`proxy.mycompany.com`**。 • **完全限定域名 (FQDN) (Fully qualified domain name [FQDN])**。也可以在该字段中输入 FQDN 或 IP 地址。但是，如果您在这种情况下还想实现 Internet Explorer 和 Firefox 浏览器真正的单点登录，则必须确保已将 FQDN 或 IP 地址添加到客户端浏览器列出的“受信任站点”(Trusted Sites) 中。根据代理流量所用的接口，默认值为 M1 或 P1 接口的 FQDN。
凭证缓存选项：(Credential Cache Options:) 替代超时 (Surrogate Timeout)	此设置指定 Web 代理再次向客户端请求身份验证凭证之前的等待时长。Web 代理使用代理中的存储值（IP 地址或 Cookie），直到再次请求凭证。 浏览器等用户代理通常会缓存身份验证凭证，所以无需每次都提示用户输入凭证。
凭证缓存选项：(Credential Cache Options:) 客户端 IP 空闲超时时间 (Client IP Idle Timeout)	将 IP 地址用作身份验证代理时，该设置指定 Web 代理在客户端空闲时再次向客户端请求身份验证凭证前等待的时间。 该值大于代理超时值时，该设置没有任何作用，并在达到代理超时后提示客户端进行身份验证。 您可能想要使用该设置减少离开计算机的用户的安全隐患。

设置	说明
凭证缓存选项：(Credential Cache Options:) 缓存大小 (Cache Size)	指定身份验证缓存中存储条目的数量。设置该值以足够容纳使用此设备的实际用户数。推荐采用默认值设置。
用户会话限制 (User Session Restrictions)	此设置指定已通过身份验证的用户是否可通过多个 IP 地址同时访问互联网。 您可能需要限制对某计算机的访问，以防止用户与非授权用户共享其身份验证凭证。阻止用户在不同计算机上登录时，出现最终用户通知页面。您可以利用此页面上“重新身份验证”(Re-authentication) 设置，选择用户可否点击某个按钮以不同的用户名登录。 如果启用此设置，请输入超时限值，确定用户在可以通过不同的 IP 地址登录计算机之前必须等待的时长。超时限值必须大于代理超时值。 可以使用 `authcache` CLI 命令从身份验证缓存中删除特定用户或所有用户。
高级 (Advanced)	使用凭证加密或访问控制时，可以选择设备是使用自带数字证书和密钥（思科网络安全设备演示证书）还是在此处上传的数字证书和密钥。

步骤 5 如果在显式转发模式下部署 Web 代理，则编辑以下设置：

设置	说明
凭证加密 (Credential Encryption)	此设置指定客户端是否通过加密 HTTPS 连接向 Web 代理发送登录凭证。要启用凭证加密，请选择“HTTPS 重定向（安全）”(HTTPS Redirect [Secure])。如果启用凭证加密，则会显示可用于配置如何将客户端重定向到 Web 代理以进行身份验证的其他字段。 该设置适用于基础身份验证方案和 NTLMSSP 身份验证方案，但特别适用于基础身份验证方案，因为用户凭证以纯文本形式进行发送。 有关详细信息，请参阅身份验证失败，第 103 页。
HTTPS 重定向端口 (HTTPS Redirect Port)	为通过 HTTPS 连接验证用户身份的重定向请求指定一个可用 TCP 端口。 此设置可指定客户端将通过哪个端口使用 HTTPS 打开 Web 代理的连接。启用凭证加密或使用访问控制并提醒用户进行身份验证时，会出现这种情况。

设置	说明
重定向主机名 (Redirect Hostname)	输入网络接口短主机名，在该网络接口上，Web 代理侦听传入连接。 启用上述身份验证模式后，Web代理将该主机名用于发送至客户端以对用户进行身份验证的重定向 URL 中。 可以输入以下值之一： • **单字主机名 (Single word hostname)**。您可以输入可由客户端和网络安全设备进行 DNS 解析的单个单词的主机名。这让客户端能够利用 Internet Explorer 实现真正的单点登录，而无需更多浏览器端设置。请务必输入可由客户端和网络安全设备进行 DNS 解析的单字主机名。例如，如果您的客户端在域 mycompany.com 且 Web 代理侦听的接口具有完整主机名 `proxy.mycompany.com`，则应该在此字段中输入`代理(Proxy)`。客户端在代理上执行查找，并应能够解析 `proxy.mycompany.com`。 • **完全限定域名 (FQDN) (Fully qualified domain name [FQDN])**。也可以在该字段中输入 FQDN 或 IP 地址。但是，如果您在这种情况下还想实现 Internet Explorer 和 Firefox 浏览器真正的单点登录，则必须确保已将 FQDN 或 IP 地址添加到客户端浏览器列出的“受信任站点”(Trusted Sites) 中。根据代理流量所用的接口，默认值为 M1 或 P1 接口的 FQDN。
凭证缓存选项：(Credential Cache Options:) 替代超时 (Surrogate Timeout)	此设置指定 Web 代理再次向客户端请求身份验证凭证之前的等待时长。Web代理使用代理中的存储值（IP地址或Cookie），直到再次请求凭证。 请注意，浏览器等用户代理通常会缓存身份验证凭证，所以无需每次都提示用户输入凭证。
凭证缓存选项：(Credential Cache Options:) 客户端 IP 空闲超时时间 (Client IP Idle Timeout)	将 IP 地址用作身份验证代理时，该设置指定 Web 代理在客户端空闲时再次向客户端请求身份验证凭证前等待的时间。 该值大于代理超时值时，该设置没有任何作用，并在达到代理超时后提示客户端进行身份验证。 您可能想要使用该设置减少离开计算机的用户的安全隐患。
凭证缓存选项：(Credential Cache Options:) 缓存大小 (Cache Size)	指定身份验证缓存中存储条目的数量。设置该值以足够容纳使用此设备的实际用户数。推荐采用默认值设置。

设置	说明
用户会话限制 (User Session Restrictions)	此设置指定已通过身份验证的用户是否可通过多个 IP 地址同时访问互联网。 您可能需要限制对某计算机的访问，以防止用户与非授权用户共享其身份验证凭证。阻止某用户在不同的计算机上登录时，会显示一个最终用户通知页面。您可以利用此页面上“重新身份验证”(Re-authentication) 设置，选择用户可否点击某个按钮以不同的用户名登录。 如果启用此设置，请输入超时限值，确定用户在可以通过不同的IP地址登录计算机之前必须等待的时长。超时限值必须大于代理超时值。 可以使用 `authcache` CLI 命令从身份验证缓存中删除特定用户或所有用户。
高级 (Advanced)	使用凭证加密或访问控制时，可以选择设备是使用自带数字证书和密钥（思科网络安全设备演示证书）还是在此处上传的数字证书和密钥。 要上传数字证书和密钥，请点击**浏览 (Browse)** 并导航到本地计算机中的必要文件。选择目标文件后，点击**上传文件 (Upload Files)**。

步骤 6 提交并确认更改。

身份验证序列

关于身份验证序列

使用身份验证序列，允许一个身份通过不同的身份验证服务器或协议来对用户进行身份验证。如果主身份验证选项不可用，身份验证序列亦可用于提供备用选项。

身份验证序列是两个或多个身份验证领域的集合。所采用的领域可拥有不同的验证服务器和不同的身份验证协议。有关身份验证领域的详细信息，请参阅身份验证领域， 第 86 页。

创建第二身份验证领域后，设备会在“网络”(Network) >“身份验证”(Authentication) 下自动显示一个“领域序列”(Realm Sequences) 部分，且包含一个名为“所有领域”(All Realms) 的默认身份验证序列。“所有领域”(All Realms) 序列会自动包含您定义的每个领域。您可以更改各领域在“所有领域”(All Realms) 序列中的顺序，但无法删除“所有领域”(All Realms) 序列或从中删除任何领域。

定义多个NTLM身份验证领域时，网络安全设备使用的是每个序列仅有一个NTLM身份验证领域的NTLMSSP 身份验证方案。您可以为每个序列中的 NTLMSSP 选择要使用的 NTLM 身份验证领域，其中包括“所有领域”(All Realms) 序列。要将 NTLMSSP 与多个 NTLM 领域结合使用，请为各领域定义单独的身份标识配置文件。

身份验证过程中采用序列中的哪些身份验证领域取决于：

- 使用的身份验证方案。这通常由在客户端输入的凭证类型决定。
- 各领域在序列中列出的顺序（仅适用于基本领域，因为只能有一个 NTLMSSP）。

提示　为了获得最佳性能，使用单个领域在同一子网上进行客户端身份验证。

创建身份验证序列

开始之前

- 创建两个或多个身份验证领域（请参阅身份验证领域，第 86 页）。
- 如果安全管理设备托管网络安全设备，请确保不同网络安全设备上相同名称的身份验证领域在每个设备上都有一致的已定义属性。
- 请注意，AsyncOS 将从列表中的第一个领域开始，按顺序利用各个领域处理身份验证。

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**

步骤 2 点击**添加序列 (Add Sequence)**。

步骤 3 输入使用字母数字和空格字符的唯一序列名称。

步骤 4 在“基础方案领域序列”(Realm Sequence for Basic Scheme) 区域的第一行中，选择要包括在序列中的首个身份验证领域。

步骤 5 在“基础方案领域序列”(Realm Sequence for Basic Scheme) 区域的第二行中，选择要包括在序列中的下一个领域。

步骤 6 （可选）点击**添加列 (Add Row)** 包括使用基础凭证的其他领域。

步骤 7 如果定义 NTLM 领域，则在“NTLMSSP 方案领域”(Realm for NTLMSSP Scheme) 字段中选择 NTLM 领域。

客户端发送 NTLMSSP 身份验证凭证时，Web 代理使用该 NTLM 领域。

步骤 8 提交并确认更改。

编辑和重新排序身份验证序列

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击要编辑或重新排序顺序的序列的名称。

步骤 3 根据想让该领域在序列中呈现的顺序，从其位置编号对应行的“领域”(Realms) 下拉列表中选择一个领域名称。

注释　对于“所有领域”(All Realms) 序列，只能更改其领域顺序，无法更改领域本身。要更改领域在“所有领域”(All Realms) 序列中的排序，请点击“排序”(Order) 列中的箭头改变相应领域的位置。

步骤 4 重复**步骤 3** 直至按需列出和排序所有领域，确保一行中仅显示各领域名称。

步骤 5 提交并确认更改。

删除身份验证序列

开始之前

请注意，删除某身份验证序列同时会禁用关联身份，反过来又会从关联策略中删除这些身份。

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击序列名称对应的垃圾桶图标。

步骤 3 点击**删除 (Delete)** 确认想要删除序列。

步骤 4 确认您的更改。

身份验证失败

关于身份验证失败

由于下列原因导致的身份验证失败，可能会阻止用户访问网络：

- **客户端/用户代理限制**。某些客户端应用可能无法正常支持身份验证。可以通过配置无需授权的身份标识配置文件以及将其标准设定在客户端的基础上（以及需访问的 URL（可选））来绕过这些客户端的身份验证。
- **身份验证服务不可用**。身份验证服务可能因网络或服务器问题不可用。这种情况下，您可以选择允许未经身份验证的流量。
- **凭证无效**。某些用户可能无法提供正常身份验证所需的有效凭证（例如访客或等待凭证的用户）。可以选择授予这些用户有限的 Web 访问权限。

相关主题

- 绕过有问题的用户代理的身份验证， 第 104 页
- 绕过身份验证， 第 105 页
- 身份验证服务不可用时允许未经身份验证的流量， 第 105 页
- 身份验证失败后授予访客接入权限， 第 106 页

绕过有问题的用户代理的身份验证

已知有些用户代理存在可能会影响正常操作的身份验证问题。

应通过以下用户代理绕过身份验证：

- Windows-Update-Agent
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession 接口
- Microsoft-CryptoAPI
- NCSI
- MSDW
- Gnotify
- msde
- Google Update

注释 访问策略仍将根据访问策略设置（基于 URL 类别）过滤和扫描（McAfee，Webroot）流量。

步骤 1 配置标识配置文件以绕过指定用户代理中的身份验证：

a) 依次选择**网络安全管理器 (Web Security Manager) > 标识配置文件 (Identification Profiles)**。

b) 点击**添加身份标识配置文件 (Add Identification Profile)**。

c) 输入信息：

选项	值
名称 (Name)	用户代理身份验证豁免标识配置文件 (User Agent AuthExempt Identification Profile)
在上方插入 (Insert Above)	设置为处理顺序中的第一个配置文件
按子网定义成员 (Define Members by Subnet)	留空。
按身份验证定义成员 (Define Members by Authentication)	无需身份验证 (No Authentication Required)。

d) 点击**高级 (Advanced) > 用户代理 (User Agents)**。

e) 点击**未选择 (None Selected)**。

f) 在“自定义用户代理”(Custom user Agents) 下，指定有问题的用户代理字符串。

步骤 2 配置访问策略：

a) 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

b) 点击**添加策略 (Add Policy)**。

c) 输入信息：

选项	值
策略名称	用户代理身份验证豁免 (Auth Exemption for User Agents)
插入以上策略 (Insert Above Policy)	设置为处理顺序中的第一个策略
标识配置文件条件 (Identification Profile Policy)	用户代理身份验证豁免标识配置文件 (User Agent AuthExempt Identification Profile)
高级 (Advanced)	无 (None)

步骤 3 提交并确认更改。

绕过身份验证

	步骤	更多信息
1	通过配置“高级”(Advanced) 属性，创建一个包含受影响网站的自定义 URL 类别。	创建和编辑自定义 URL 类别，第 151 页
2	创建具有以下特征的身份标识配置文件： • 高于需要身份验证的所有身份。 • 包括自定义 URL 类别。 • 包括受影响客户端应用。 • 无需身份验证。	用户和客户端软件分类，第 115 页
3	为身份标识配置文件创建策略。	创建策略，第 181 页

相关主题

- 绕过 Web 代理

身份验证服务不可用时允许未经身份验证的流量

注释 仅在身份验证服务不可用时，才适用此配置。此操作并非永久绕过身份验证。有关替代选项，请参阅 关于身份验证失败，第 103 页

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 点击“身份验证服务不可用时操作”(Action If Authentication Service Unavailable) 字段中的**允许流量继续而不进行身份验证 (Permit Traffic To Proceed Without Authentication)**。

步骤 4 提交并确认更改。

身份验证失败后授予访客接入权限

授予访客接入权限需要完成以下程序：

1. 定义可支持访客接入的标识配置文件，第 106 页
2. 使用策略中支持访客接入的标识配置文件，第 106 页
3. （可选） 配置访客用户详细信息记录方式，第 107 页

注释 如果身份标识配置文件允许访客接入且没有使用该身份标识配置文件的用户定义策略，则身份验证失败的用户匹配适用策略类型的全局策略。例如，如果身份标识配置文件 MyIdentificationProfile 允许访客接入且没有使用此配置文件的用户定义访问策略，则身份验证失败的用户匹配全局访问策略。如果不希望访客用户匹配全局策略，则创建高于全局策略的一个策略，适用于访客用户并阻止所有接入。

定义可支持访客接入的标识配置文件

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 标识配置文件 (Identification Profiles)**。

步骤 2 点击**添加身份标识配置文件 (Add Identification Profile)** 可添加新身份，或点击要使用的现有身份名称。

步骤 3 选中**支持访客权限 (Support Guest Privileges)** 复选框。

步骤 4 提交并确认更改。

使用策略中支持访客接入的标识配置文件

步骤 1 从“网络安全管理器”(Web Security Manager) 菜单中选择策略类型。

步骤 2 点击策略表中的策略名称。

步骤 3 从“标识配置文件和用户”(Identification Profiles And Users) 下拉列表中，选择**选择一个或多个标识配置文件 (Select One Or More Identification Profiles)**（如果尚未选择）。

步骤 4 从“标识配置文件”(Identification Profile) 列的下拉列表中，选择可支持访客访问的**配置文件**。

步骤 5 点击**访客（用户身份验证失败）(Guests [Users Failing Authentication])**单选按钮。

注释 如果该选项不可用，则意味着并未将所选**配置文件 (profile)** 配置为支持访客访问。返回第步骤4，选择其他配置文件，或参阅定义可支持访客接入的标识配置文件，第 106 页定义一个新的配置文件。

步骤 6 提交并确认更改。

配置访客用户详细信息记录方式

步骤 1 依次选择网络 (Network) > 身份验证 (Authentication)。

步骤 2 点击编辑全局设置 (Edit Global Settings)。

步骤 3 点击“身份验证处理失败”(Failed Authentication Handling) 字段中的“访客用户记录方式”(Log Guest User By) 单选按钮（如下所述）。

单选按钮	说明
IP 地址 (IP Address)	访客用户客户端的 IP 地址将被记录到访问日志中。
最终用户输入的用户名 (User Name As Entered By End-User)	最初身份验证失败的用户名将记录在访问日志中。

步骤 4 提交并确认更改。

授权失败：允许使用不同凭证进行重新验证

有关允许使用不同凭证进行重新身份验证

如果之前使用的凭证未能通过身份验证，重新身份验证允许用户使用不同的凭证重新进行身份验证。如果未获得相关授权，即便用户已成功通过身份验证，也仍有可能无法访问网络资源。这是因为，身份验证只是出于将用户的已验证凭证传达给策略的目的而对用户进行识别，而是否授权用户访问资源则由策略负责。

用户必须成功通过身份验证，才能重新进行身份验证。

- 要将重新身份验证功能与用户定义的最终用户通知页面配合使用，解析重定向 URL 的 CGI 脚本必须具备解析能力并采用 Reauth_URL 参数。

允许使用不同凭证进行重新身份验证

步骤 1 依次选择网络 (Network) > 身份验证 (Authentication)。

步骤 2 点击编辑全局设置 (Edit Global Settings)。

步骤 3 选中最终用户被 URL 类别或用户会话限制阻止时启用重新身份验证提示 (Re-Authentication Prompt If End User Blocked by URL Category Or User Session Restriction) 复选框。

步骤 4 点击提交 (Submit)。

跟踪已识别用户

注释 如果设备配置为使用基于 Cookie 的身份验证代理，则不会从 HTTPS 和 FTP over HTTP 请求客户端获取 Cookie 信息。因此，无法从 Cookie 获取用户名。

受支持的显式请求身份验证代理

代理类型	禁用凭证加密			启用凭证加密		
协议：	HTTP	HTTPS 和 FTP over HTTP	本地 FTP	HTTP	HTTPS 和 FTP over HTTP	本地 FTP
无代理	是	是	是	NA	NA	NA
基于 IP	是	是	是	是	是	是
基于 Cookie	是	是***	是***	是	否/是**	是***

受支持的透明请求身份验证代理

注释 另请参阅用户和客户端软件分类，第 115 页中关于“身份验证代理”选项的说明。

代理类型	凭证加密已禁用			凭证加密已启用		
协议：	HTTP	HTTPS	本地 FTP	HTTP	HTTPS	本地 FTP
无代理	不适用	不适用	不适用	不适用	不适用	不适用
基于 IP	是	否/是*	否/是*	是	否/是*	否/是*
基于 Cookie	是	否/是**	否/是**	是	否/是**	否/是**

* 在客户端向某 HTTP 站点提出请求并通过身份验证后生效。在此之前，相关行为取决于事务类型：

- **本地 FTP 事务**。事务绕过身份验证。
- **HTTPS 事务**。丢弃事务。但是，可以配置 HTTPS 代理解密首个 HTTPS 请求以便进行身份验证。

** 使用基于 Cookie 的身份验证时，Web 代理无法对 HTTPS、本地 FTP 以及 FTP over HTTP 事务的用户进行身份验证。由于此限制，所有 HTTPS、本地 FTP 以及 FTP over HTTP 请求都会绕过身份验证，根本不请求身份验证。

*** 在这种情况下，即使配置基于 Cookie 的代理，也不使用代理。

相关主题

- 标识配置文件和身份验证，第 120 页

跟踪重新进行身份验证的用户

借助重新进行身份验证，如果某具有更高权限的用户进行身份验证并获得授权，则 Web 代理会根据配置的身份验证代理，为该用户提供不同时长的身份缓存：

- **会话 Cookie**。具有权限的用户身份一直持续到浏览器关闭或会话超时。
- **持久性 Cookie**。具有权限的用户身份一直持续到代理超时。
- **IP 地址**。具有权限的用户身份一直持续到代理超时。
- **无代理**。Web 代理默认为每个新连接请求身份验证，但是如果启用重新进行身份验证，Web 代理即为每个新请求请求身份验证，所以使用NTLMSSP时，身份验证服务器的负载会越来越大。但身份验证活动的增加对用户而言可能不太明显，因为大多数的浏览器会一直无提示地缓存具有权限的用户凭证及身份验证，直到浏览器关闭。此外，在透明模式下部署 Web 代理且“将同一代理设置应用至显式转发请求”(Apply same surrogate settings to explicit forward requests) 选项未启用时，无用于显式转发请求的身份验证代理，且在重新身份验证时出现负载增加。

注释 如果网络安全设备使用身份验证代理 Cookie，思科建议启用凭证加密。

凭证

从用户获取身份验证凭证的方式如下：提示用户通过浏览器或其他客户端应用输入凭证，或从其他源透明地获取凭证。

- 会话期间跟踪凭证以便重新使用，第 109 页
- 身份验证和授权失败，第 110 页
- 凭证格式，第 110 页
- 基础身份验证凭证加密，第 110 页

会话期间跟踪凭证以便重新使用

使用身份验证代理，待用户于某次会话中完成用户身份验证后，即可跟踪整个会话期间重复使用的凭证，而无需要求用户每次新请求都进行身份验证。身份验证代理可能基于用户工作站的 IP 地址，或是分配给该会话的 Cookie。

对于 Internet Explorer，请确保“重定向主机名”(Redirect Hostname) 是短主机名（不含点号）或 NetBIOS 名称，而非完全限定域名。或者，可以将设备主机名添加至 Internet Explorer 的本地内联网区域（“工具”(Tools) > “互联网选项”(Internet options) > “安全”(Security) 选项卡）；然而，这在每个客户端上均需完成。有关与此相关的详细信息，请参阅如何利用 SSO 准确设置 NTLM（透明发送凭证）？

使用 Firefox 和其他非 Microsoft 浏览器时，必须将参数 **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris** 和 **network.automatic-ntlm-auth.trusted-uris** 设置为透明模式重定向主机名。还可参阅 Firefox 不透明发送身份验证凭证 (SSO)。该文章提供有关更改 Firefox 参数的一般信息。

有关重定向主机名的信息，请参阅配置全局身份验证设置，第 96 页或 CLI 命令 `sethostname`。

身份验证和授权失败

如果身份验证因客户端应用不兼容等可接受的原因失败，则您可以授予访客接入权限。

如果身份验证成功但授权失败，则可能允许利用一组已授权访问请求资源的不同凭证重新进行身份验证。

相关主题

- 身份验证失败后授予访客接入权限，第 106 页
- 允许使用不同凭证进行重新身份验证，第 107 页

凭证格式

身份验证方案	凭证格式
NTLMSSP	**MyDomain\jsmith**
基本	**jsmith** **MyDomain\jsmith** 注释　如果用户未输入 Windows 域，则 Web 代理会在前面加上默认 Windows 域。

基础身份验证凭证加密

关于基本身份验证的凭证加密

启用凭证加密，以加密形式通过 HTTPS 传输凭证。如此可提升基本身份验证过程的安全性。

网络安全设备默认使用自有证书和私钥来创建出于安全身份验证目的与客户端建立的HTTPS连接。但大多数浏览器会警告用户此证书无效。为防止用户看到此无效证书消息，您可以上传贵组织使用的有效证书和密钥对。

配置凭证加密

开始之前

- 将设备配置为使用 IP 代理。
- （可选）获取一份证书和未加密的私钥。此处配置的证书和密钥也会被“访问控制”(Access Control) 使用。

步骤 1 依次选择**网络 (Network) > 身份验证 (Authentication)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 选中“凭证加密”(Credential Encryption) 字段中的**将加密 HTTPS 连接用于身份验证 (Use Encrypted HTTPS Connection For Authentication)** 复选框。

步骤 4 （可选）身份验证期间，编辑适用于客户端 HTTP 连接的“HTTPS 重定向端口”(HTTPS Redirect Port) 字段中的默认端口号 (443)。

步骤 5 （可选）上传证书和密钥：

a) 展开“高级”(Advanced) 部分。
b) 点击“证书”(Certificate) 字段中的**浏览 (Browse)** 并找到要上传的证书文件。
c) 点击“密钥”(Key) 字段中的**浏览 (Browse)** 并找到要上传的私钥文件。
d) 点击**上传文件 (Upload Files)**。

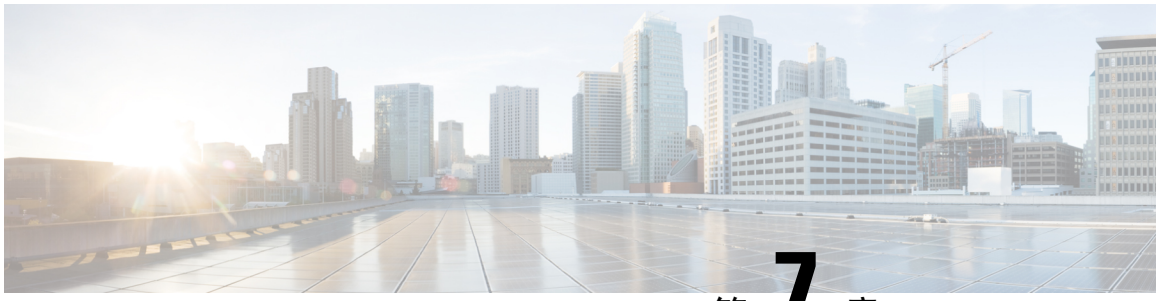
步骤 6 提交并确认更改。

下一步做什么

相关主题

- 证书管理， 第 406 页.

身份验证故障排除



第 7 章

对最终用户进行分类以应用策略

本章包含以下部分：

用户和客户端软件分类概述

出于以下目的，标识配置文件允许您对用户和用户代理（客户端软件）进行分类：

- 对事务请求进行分组，以应用策略（SaaS 除外）
- 规范身份识别和身份验证要求

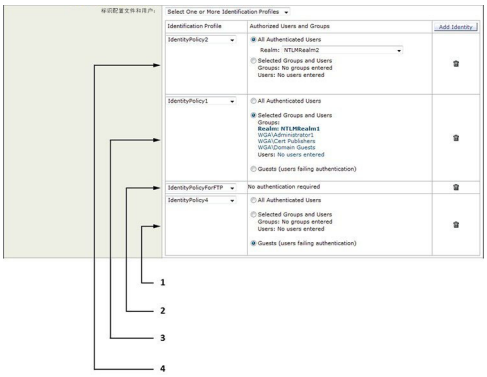
AsyncOS 为每个事务分配一个标识配置文件：

- “自定义标识配置文件”(Custom Identification Profiles) - AsyncOS 根据相应身份的条件分配自定义配置文件。
- “全局标识配置文件”(The Global Identification Profile) - AsyncOS 为不符合任何自定义配置文件的条件的事务分配全局配置文件。默认情况下，全局配置文件不需要进行身份验证。

AsyncOS 从第一个开始依次处理标识配置文件。全局配置文件是最后一个处理的配置文件。

一个标识配置文件只能包含一个条件。或者，包含多个条件的配置文件要求所有的条件都得到满足。

一个策略可能需要多个标识配置文件：



1	此标识配置文件允许访客接入，并会应用于身份验证失败的用户。
2	身份验证不用于此标识配置文件。
3	此标识配置文件中的指定用户组会被授权使用此策略。
4	此标识配置文件使用一个身份验证序列，并且此策略会应用于序列中的一个领域。

用户和客户端软件分类：最佳实践

- 创建适用于所有用户或更少或更大用户组的更少、更通用的标识配置文件。使用策略（而不是配置文件）提供更精细的管理。
- 创建具有唯一条件的标识配置文件。
- 如果在透明模式下部署，请为不支持身份验证的站点创建标识配置文件。请参阅绕过身份验证，第 105 页。

标识配置文件条件

下列事务特征可用于定义标识配置文件：

选项	说明
子网 (Subnet)	客户端子网必须与策略中的子网列表匹配。
协议 (Protocol)	用于事务的协议：HTTP、HTTPS、SOCKS 或本地 FTP。
端口 (Port)	请求的代理端口必须包含在标识配置文件的端口列表中（如果列出了任何端口）。对于显式转发连接，此代理端口为浏览器中配置的端口。对于透明连接，此代理端口与目标端口为同一端口。

选项	说明
用户代理 (User Agent)	发出请求的用户代理（客户端应用）必须包含在标识配置文件的用户代理列表中（如果列出了任何用户代理）。部分用户代理无法处理身份验证，因此，有必要创建不需要身份验证的配置文件。用户代理包括更新器和浏览器等程序，如 Internet Explorer 和 Mozilla Firefox。
URL 类别 (URL Category)	请求 URL 的 URL 类别必须包含在标识配置文件的 URL 类别列表中（如果列出了任何 URL 类别）。
身份验证要求 (Authentication requirements)	如果标识配置文件要求进行身份验证，则客户端身份验证凭证必须与标识配置文件的身份验证要求匹配。

用户和客户端软件分类

开始之前

- 创建身份验证领域。请参阅如何创建 Active Directory 身份验证领域（NTLMSSP 和基本），第 90 页或创建 LDAP 身份验证领域，第 92 页。
- 请注意，在确定对标识配置文件的更改时，最终用户必须重新进行身份验证。
- 请注意，如果您处于云连接器模式下，系统会提供其他标识配置文件选项：“计算机ID”(Machine ID)。请参阅识别用于策略应用的计算机，第 49 页。
- （可选）创建身份验证序列。请参阅创建身份验证序列，第 102 页
- （可选）如果标识配置文件包括移动用户，则启用“安全移动”(Secure Mobility)。
- （可选）了解身份验证代理。请参阅跟踪已识别用户，第 108 页。

步骤 1 依次选择**网络安全管理器 (Web Security Manager)** > **标识配置文件 (Identification Profiles)**。

步骤 2 点击**添加配置文件 (Add Profile)** 可添加配置文件。

步骤 3 使用**启用标识配置文件 (Enable Identification Profile)** 复选框启用此配置文件，或快速将其禁用（而不删除）。

步骤 4 分配一个唯一的配置文件**名称 (Name)**。

步骤 5 **说明 (Description)** 为可选项。

步骤 6 在**在上方插入 (Insert Above)** 下拉列表中，选择此配置文件要在表中的显示位置。

注释 将不要求进行身份验证的标识配置文件放在第一个要求进行身份验证的标识配置文件上方。

步骤 7 在**用户识别方法 (User Identification Method)** 部分，选择一种身份识别方法，然后提供相关参数；显示的选项因所选的方法而异。

有三类方法：免除身份验证/识别、对用户进行身份验证以及通过三种方式透明识别用户：ISE、ASA（通过 AnyConnect 安全移动）或已正确配置的身份验证领域。后者包括一个 Active Directory 领域或配置为 Novell eDirectory 的 LDAP 领域。

有三类方法：免除身份验证/识别、对用户进行身份验证以及通过三种方式透明识别用户：ISE、ASA（通过 AnyConnect 安全移动）或已正确配置的身份验证领域。后者包括一个 Active Directory 领域或配置为 Novell eDirectory 的 LDAP 领域。

a) 在**用户识别方法 (User Identification Method)** 下拉列表中，选择一种识别方法。

选项	说明
免除身份验证/识别 (Exempt from authentication/ identification)	用户主要通过 IP 地址识别。无需提供额外参数。
对用户进行身份验证 (Authenticate users)	用户通过其输入的身份验证凭证识别。
使用 ISE 透明识别用户 (Transparently identify users with ISE)	在启用 ISE 服务（“网络”(Network)>“身份服务引擎”(Identity Services Engine)）时可用。对于这些事务，将从身份服务引擎获取用户名和关联的安全组标记。有关详细信息，请参阅认证和集成 ISE 服务任务，第 131 页。
使用 ASA 透明识别用户 (Transparently identify users with ASA)	用户按从思科自适应安全设备收到的当前 IP 地址到用户名的映射进行识别（仅适用于远程用户）。当安全移动启用并与 ASA 集成时，将会出现此选项。将从 ASA 获取用户名，并且将从所选身份验证领域或序列获取关联的目录组。
使用身份验证领域透明识别用户 (Transparently identify users with authentication realm)	当一个或多个身份验证领域配置为支持透明识别时，此选项可用。

注释 当至少配置了一个具有身份验证或透明识别的标识配置文件时，策略表将支持使用用户名、目录组和安全组标记来定义策略成员。

b) 为所选的方法提供适合的参数。并非每个所选的方法都会出现此表中介绍的所有选项。

回退到身份验证领域或访客权限	如果 ISE 无法提供用户身份验证，则可以选择以下选项： • **支持访客权限 (Support Guest Privileges)** - 允许继续进行事务，并且事务将匹配所有标识配置文件中的访客用户的后续策略。 • **阻止事务 (Block Transactions)** - 不允许 ISE 无法识别的用户访问互联网。 • **支持访客权限 (Support Guest Privileges)** - 选中此框可授予访客对由于凭证无效而身份验证失败的用户的访问权限。

身份验证领域 (Authentication Realm)	**选择领域或序列 (Select a Realm or Sequence)** - 选择已定义的身份验证领域或序列。 **选择方案 (Select a Scheme)** - 选择身份验证方案： • **Kerberos** - 客户端通过 Kerberos 票证进行透明身份验证。 • **基础 (Basic)** - 客户端始终会提示用户提供凭证。在用户输入凭证后，浏览器通常会提供一个复选框，用于记住所提供的凭证。当用户打开浏览器时，客户端会提示输入凭证或重新发送之前保存的凭证。 凭证以明文 (Base64) 形式发送并不安全。客户端与网络安全设备之间的数据包捕获可能会泄露用户名和密码。 • **NTLMSSP** - 客户端使用其 Windows 登录凭证进行透明身份验证。客户端不会提示用户提供凭证。 但是，在以下情况下，客户端会提示用户提供凭证： • Windows 凭证失败。 • 由于浏览器安全设置，客户端不信任网络安全设备。 使用三次握手（摘要式身份验证）安全地发送凭证。从不跨连接发送密码。 • **支持访客权限 (Support Guest Privileges)** - 选中此框可授予访客对由于凭证无效而身份验证失败的用户的访问权限。
组身份验证的领域 (Realm for Group Authentication)	• **选择领域或序列 (Select a Realm or Sequence)** - 选择已定义的身份验证领域或序列。
身份验证代理 (Authentication Surrogates)	指定在身份验证成功后事务如何与用户关联（选项因 Web 代理部署模式而异）： • **IP 地址 (IP Address)** - Web 代理跟踪特定 IP 地址上经过身份验证的用户。对于透明用户识别，请选择此选项。 • **永久性 Cookie (Persistent Cookie)** - Web 代理通过为每个应用的每位用户生成一个永久性 Cookie，跟踪特定应用上经过身份验证的用户。关闭应用并不会清除此 Cookie。 • **会话 Cookie (Session Cookie)** - Web 代理通过为每个域内每个应用的每位用户生成一个会话 Cookie，跟踪特定应用上经过身份验证的用户。（但是，当用户从同一应用为相同的域提供不同的凭证时，此 Cookie 会被覆盖。）关闭应用会清除此 Cookie。 • **无代理 (No Surrogate)** - Web 代理不使用代理缓存凭证，但会跟踪每个新 TCP 连接的经过身份验证的用户。选择此选项时，Web 界面禁用不再适用的其他设置。仅当在显式转发模式下，以及当您在“网络”(Network) >“身份验证”(Authentication) 页面中禁用凭证加密后，此选项才可用。 • **将相同的代理设置应用于显式转发请求 (Apply same surrogate settings to explicit forward requests)** - 确保将用于透明请求的代理应用于显式请求；自动启用凭证加密。仅当 Web 代理在透明模式下部署时，系统才会显示此选项。 **注释** 可以在全局身份验证设置 (Global Authentication Settings) 中为所有请求的身份验证代理定义一个超时值。

步骤 8 在**成员定义 (Membership Definition)** 部分，为所选的方法提供恰当的成员参数。请注意，并非每种用户识别方法都会出现此表中介绍的所有选项。

成员身份定义	
按用户位置定义成员 (Define Members by User Location)	将此标识配置文件配置为应用于以下用户：**仅本地用户 (Local Users Only)**、**仅远程用户 (Remote Users Only)** 或**两者 (Both)**。此选项会影响相应标识配置文件的可用身份验证设置。
按子网定义成员 (Define Members by Subnet)	输入需要应用此标识配置文件的地址。可以使用 IP 地址、CIDR 块和子网。 **注释** 如果未输入任何内容，标识配置文件将应用于所有 IP 地址。
按协议定义成员 (Define Members by Protocol)	选择需要应用此标识配置文件的协议；选择所有适用协议： • **HTTP/HTTPS** - 适用于将 HTTP 或 HTTPS 用作基础协议的所有请求，包括 FTP over HTTP 以及使用 HTTP CONNECT 建立隧道的任何其他协议。 • **本地 FTP (Native FTP)** - 仅应用于本地 FTP 请求。 • **SOCKS** - 仅应用于 SOCKS 策略。
按计算机 ID 定义成员 (Define Members by Machine ID)	• **不在此策略中使用计算机 ID (Do Not Use Machine ID in This Policy)** - 不通过计算机 ID 识别用户。 • **定义基于计算机 ID 的用户身份验证策略 (Define User Authentication Policy Based on Machine ID)** - 用户主要通过计算机 ID 识别。 点击“计算机组”(Machine Groups) 区域以显示“授权计算机组”(Authorized Machine Groups) 页面。 对于每个要添加的组，在“目录搜索”(Directory Search) 字段，开始键入要添加的组的名称，然后点击“添加”(Add)。可以选择一个组，然后点击“删除”(Remove) 以从列表中将其删除。 点击“完成”(Done) 以返回之前的页面。 点击“计算机 ID”(Machine IDs) 区域以显示“授权计算机”(Authorized Machines) 页面。 在“授权计算机”(Authorized Machines) 字段，输入要与策略关联的计算机 ID，然后点击“完成”(Done)。 **注释** “连接器”(Connector) 模式仅支持使用计算机 ID 的身份验证且需要 Active Directory。

高级	展开此部分，定义其他成员要求。 • **代理端口 (Proxy Ports)** - 指定一个或多个用于访问 Web 代理的代理端口。输入以逗号分隔的端口号。对于显式转发连接，此代理端口为浏览器中配置的端口。 对于透明连接，此代理端口与目标端口为同一端口。 当在显式转发模式下部署设备时，或者当客户端将请求显式转发到设备时，按端口定义身份最适用。在客户端请求透明地重定向到设备时按端口定义身份可能导致一些请求遭到拒绝。 • **URL 类别 (URL Categories)** - 选择用户定义的或预定义的 URL 类别。默认情况下系统会排除这两种类别的成员身份，这意味着 Web 代理会忽略所有类别，除非在“添加”(Add) 列中选择它们。 如果需要按 URL 类别定义成员身份，只需在需要免于身份验证请求时在身份组中定义该类别即可。 • **用户代理** - 按照在客户端请求中找到的用户代理来定义策略组成员身份。可以选择某些通常定义的代理，或者使用正则表达式定义您自己的用户代理。 此外指定这些用户代理规范是包含还是不包含的。换言之，成员身份定义是仅包括选定的用户代理，还是专门排除了选定的用户代理。

步骤 9 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

- 获取最终用户凭证概述， 第 77 页
- 通过策略管理 Web 请求的任务概述， 第 176 页

启用/禁用身份

开始之前

- 请注意，禁用一个标识配置文件会从关联策略中将其删除。
- 请注意，重新启用标识配置文件不会将其与任何策略重新关联。

步骤 1 依次选择**网络安全管理器 (Web Security Manager)** > **标识配置文件 (Identification Profiles)**。

步骤 2 点击标识配置文件表中的某个配置文件，可打开该配置文件对应的标识配置文件页面。

步骤 3 随即在“客户端/用户标识配置文件设置”(Client/User Identification Profile Settings) 下选中或清除**启用标识配置文件 (Enable Identification Profile)**。

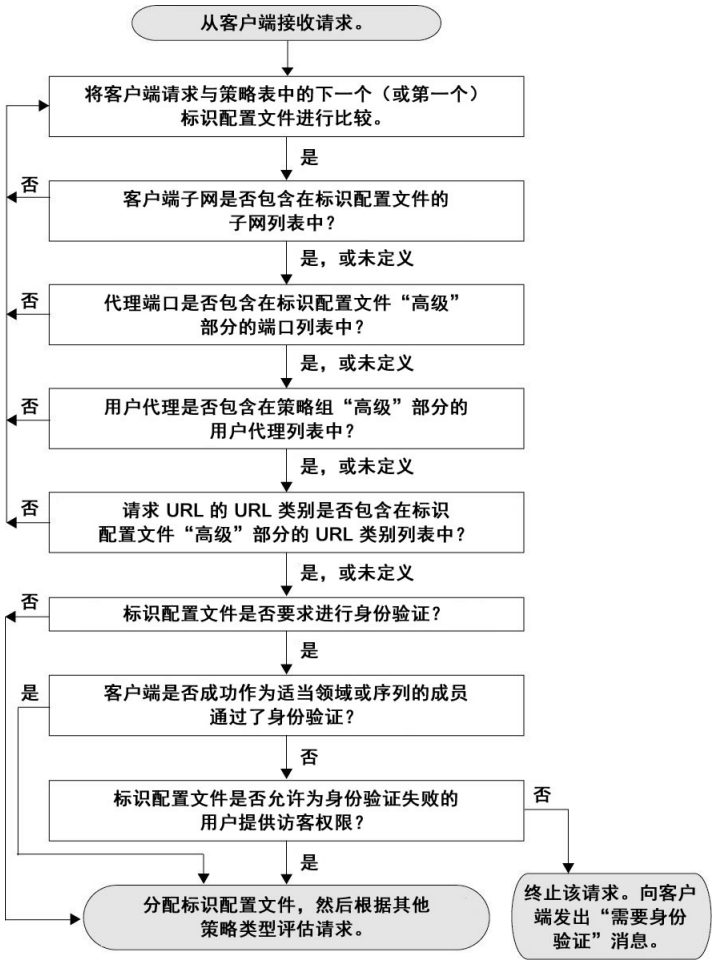
步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

标识配置文件和身份验证

下图显示在标识配置文件配置使用以下各项时，Web代理如何根据此标识配置文件评估客户端请求：

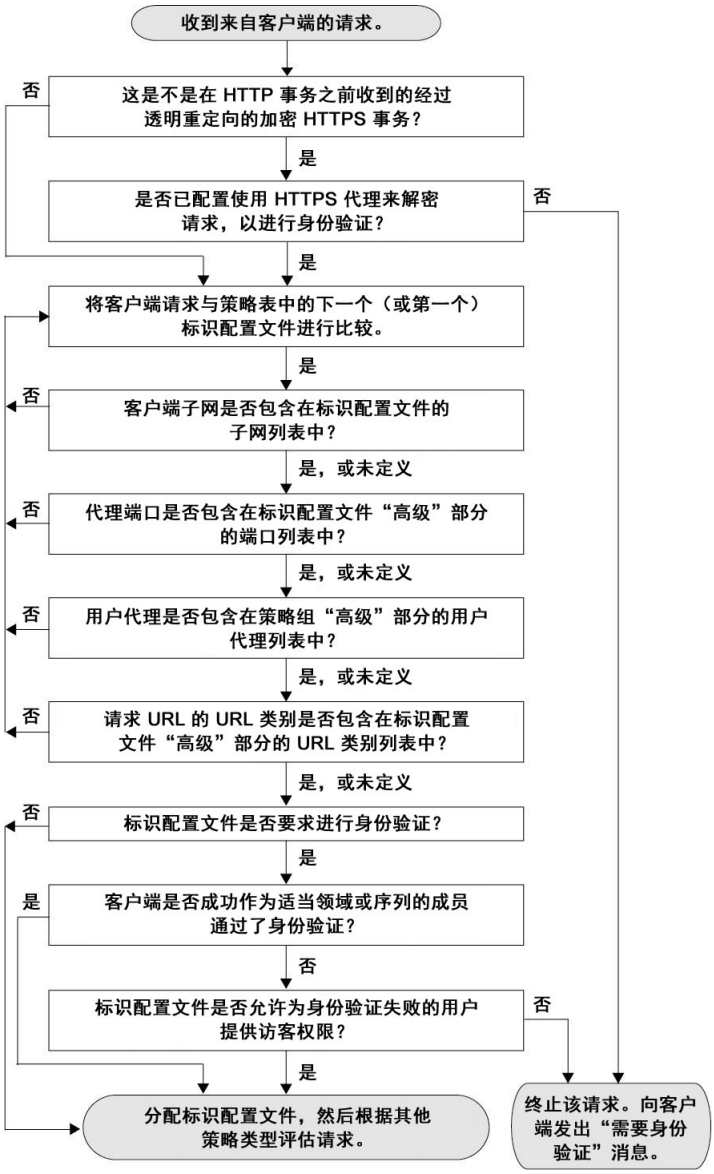
- 无身份验证代理
- IP 地址作为身份验证代理
- Cookie 作为透明请求的身份验证代理
- Cookie 作为显式请求的身份验证代理，并且启用凭证加密

图 *1:* 标识配置文件和身份验证处理 - 无代理和基于 *IP* 的代理

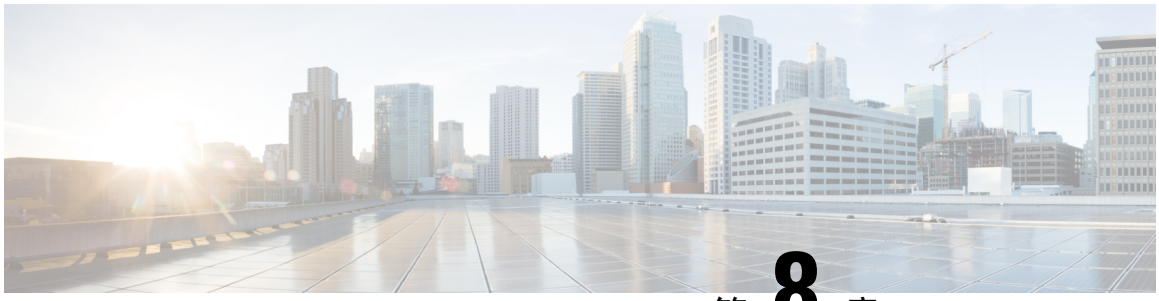


下图显示了在将标识配置文件配置为使用Cookie作为身份验证代理、已启用凭证并且将显示转发请求时，Web 代理如何根据此标识配置文件评估客户端请求。

图 *2:* 标识配置文件和身份验证处理 - 基于 ***Cookie*** 的代理



标识配置文件故障排除



第 8 章

SaaS 访问控制

本章包含以下部分：

SaaS 访问控制概述

网络安全设备使用安全声明标记语言 (SAML) 来授权对 SaaS 应用的访问权限。它与完全兼容于 SAML 2.0 版的 SaaS 应用配合使用。

思科 SaaS 访问控制允许您：

- 控制哪些用户可以访问 SaaS 应用以及从哪里访问该应用。
- 当用户不再受雇于组织时，迅速禁用其对所有 SaaS 应用的访问权限。
- 降低要求用户输入 SaaS 用户凭证的网络钓鱼攻击风险。
- 选择用户是透明登录（单点登录功能）还是按提示输入其身份验证用户名和密码。

SaaS 访问控制仅可与需要网络安全设备支持的身份验证机制的 SaaS 应用配合使用。目前，Web 代理使用“PasswordProtectedTransport”身份验证机制。

要启用 SaaS 访问控制，必须同时在网络安全设备和 SaaS 应用上配置设置。

过程

	命令或操作	目的
步骤 1	将网络安全设备配置为身份提供程序。	将设备配置为身份提供程序， 第 124 页
步骤 2	创建 SaaS 应用的身份验证策略。	创建 SaaS 应用身份验证策略， 第 126 页
步骤 3	配置 SaaS 应用的单点登录。	配置最终用户访问单点登录 URL， 第 128 页

	命令或操作	目的
步骤 4	（可选）配置多个网络安全设备。	使用 SaaS 访问控制和多个设备，第 125 页

将设备配置为身份提供程序

当您将网络安全设备配置为身份提供程序时，您定义的设置适用于与设备通信的所有SaaS应用。网络安全设备使用证书和密钥来签署其创建的每个 SAML 声明。

开始之前

- （可选）找到签署 SAML 声明的证书（PEM 格式）和密钥。
- 将证书上传至各 SaaS 应用。

步骤 1 依次选择**网络 (Network) > SaaS 标识提供程序 (Identity Provider for SaaS)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用 SaaS 单点登录服务 (Enable SaaS Single Sign-on Service)** 复选框。

步骤 4 在**标识提供程序域名 (Identity Provider Domain Name)** 字段中输入虚拟域名。

步骤 5 在**标识提供程序实体 ID (Identity Provider Entity ID)** 字段中输入唯一的文本标识符（推荐使用URI格式字符串）。

步骤 6 上传或生成证书和密钥：

方法	其他步骤
上传证书和密钥	1. 选择**使用上传的证书和密钥 (Use Uploaded Certificate and Key)**。 2. 在**证书 (Certificate)** 字段中，点击“浏览”(Browse)；找到要上传的文件。 注释 Web 代理使用文件中的第一个证书或密钥。证书文件必须是 PEM 格式。不支持 DER 格式。 3. 在**密钥 (Key)** 字段中，点击“浏览”(Browse)；找到要上传的文件。 如果密钥已加密，则选择**密钥已加密 (Key is Encrypted)**。 注释 密钥长度必须为 512 位、1024 位或 2048 位。私钥文件必须是 PEM 格式。不支持 DER 格式。 4. 点击**上传文件 (Upload Files)**。 5. 点击**下载证书 (Download Certificate)** 下载证书副本，以传输至网络安全设备将与其进行通信的 SaaS 应用。

方法	其他步骤
生成证书和密钥	1. 选择**使用生成的证书和密钥 (Use Generated Certificate and Key)**。 2. 点击**生成新的证书和密钥 (Generate New Certificate and Key)**。 1. 在“生成证书和密钥”(Generate Certificate and Key) 对话框中，输入要在签名证书中显示的信息。 注释 您可以在“公用名”(Common Name) 字段中输入除正斜杠 (/) 以外的任何 ASCII 字符。 2. 点击**生成 (Generate)**。 3. 点击**下载证书 (Download Certificate)** 将证书传输到将与网络安全设备通信的 SaaS 应用。 4. （可选）要使用签名证书，请点击**下载证书签名请求 (Download Certificate Signing Request)** (DCSR) 链接，将请求提交给证书颁发机构 (CA)。从 CA 收到签名的证书之后，点击**浏览 (Browse)** 并导航至签名证书位置。点击**上传文件 (Upload File)**。（漏洞 37984）

注释 如果设备既具有上传证书和密钥对又具有生成证书和密钥对，则其仅使用“签名证书”(Signing Certificate) 部分中当前选择的证书和密钥对。

步骤 7 记录将设备配置为身份提供程序时的设置。在配置 SaaS 应用单点登录时，必须使用其中一些设置。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

指定用于签署 SAML 声明的证书和密钥后，将证书上传至各 SaaS 应用。

相关主题

- 配置最终用户访问单点登录 URL，第 128 页

使用 SaaS 访问控制和多个设备

开始之前

将设备配置为身份提供程序，第 124 页

步骤 1 为每个网络安全设备配置相同的身份提供程序域名。

步骤 2 为每个网络安全设备配置相同的身份提供程序实体 ID。

步骤 3 在**网络 (Network) > SaaS 标识提供程序 (Identity Provider for SaaS)** 页面上将相同证书和私钥上传至各设备。

步骤 4 将该证书上传到您配置的每个 SaaS 应用。

创建 SaaS 应用身份验证策略

开始之前

- 创建关联身份。
- 有关配置标识提供程序，请参阅将设备配置为身份提供程序，第 124 页。
- 提供标识提供程序签名证书和密钥：“网络”(Network)>“SaaS 标识提供程序”(Identity Provider for SaaS) >“启用和编辑设置”(Enable and Edit Settings)。
- 创建身份验证领域，请参阅身份验证领域，第 86 页。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > SaaS 策略 (SaaS Policies)**。

步骤 2 点击**添加应用 (Add Application)**。

步骤 3 配置设置：

属性	说明
应用名称 (Application Name)	输入标识该策略 SaaS 应用的名称；各应用名称必须唯一。网络安全设备使用应用名称生成单点登录 URL。
说明 (Description)	（可选）输入此 SaaS 策略的说明。

属性	说明
服务提供程序的元数据 (Metadata for Service Provider)	配置用来描述此策略引用的服务提供程序的元数据。可以手动添加服务提供程序属性的说明，也可上传 SaaS 应用提供的元数据文件。 网络安全设备使用元数据确定如何使用 SAML 与 SaaS 应用（服务提供程序）通信。请联系 SaaS 应用来了解配置元数据的正确设置。 **手动配置密钥 (Configure Keys Manually)** - 如果选择该选项，则提供下列各项： • **服务提供商实体 ID (Service Provider Entity ID)**。输入 SaaS 应用用来将自身标识为服务提供程序的文本（通常采用 URI 格式）。 • **名称 ID 格式 (Name ID Format)**。从此下拉列表中选择设备用来在其发送到服务提供程序的 SAML 声明中标识用户的格式。在此处输入的值必须与 SaaS 应用配置的相应设置匹配。 • **声明使用者服务位置 URL (Assertion Consumer Service URL)**。输入网络安全设备要将所创建的 SAML 声明发送到的 URL。阅读 SaaS 应用文档，确定要使用的正确 URL（也称为登录 URL）。 **从硬盘导入文件 (Import File from Hard Disk)** - 如果选择此选项，点击“浏览”(Browse)，找到文件，然后点击**导入 (Import)**。 **注释** 此元数据文件是符合 SAML 标准的一个 XML 文档，描述服务提供商实例。并非所有的 SaaS 应用都使用元数据文件，但对于使用元数据文件的那些 SaaS 应用，请联系 SaaS 应用提供商获得该文件。
用于 SaaS SSO 的用户标识/身份验证	指定如何标识用户/对用户进行身份验证才能进行 SaaS 单点登录。 • 始终提示用户提供本地身份验证凭证。 • 如果 Web 代理透明获取用户名，则提示用户提供本地身份验证凭证。 • SaaS 用户使用其本地身份验证凭证自动登录。 选择 Web 代理应用于对用户（访问该 SaaS 应用）进行身份验证的身份验证领域或序列。用户必须是身份验证领域或身份验证序列成员，才能成功访问 SaaS 应用。如果身份服务引擎用于身份验证且选定 LDAP，则该领域将用于 SAML 用户名和属性映射。
SAML 用户名映射 (SAML User Name Mapping)	指定 Web 代理应如何向 SAML 声明中的服务提供程序呈现用户名。可以传送用户名，因为这些用户名用于网络内部（**无映射**），或可以使用以下方法之一将内部用户名更改为不同格式： • **LDAP 查询 (LDAP query)**。根据一个或多个 LDAP 查询属性将用户名发送到服务提供程序。输入包含 LDAP 属性字段和可选自定义文本的表达式。尖括号中必须包含属性名称。您可以包含任意数量的属性。例如，对于 LDAP 属性“user”和“domain”，可以输入 <user>@<domain>.com。 • **固定规则映射 (Fixed Rule mapping)**。根据前面或后面添加了固定字符串的内部用户名将用户名发送到服务提供程序。在**表达式名称 (Expression Name)** 字段中输入固定字符串，其中，%s 加在该字符串前或后以指示其在内部用户名中的位置。
SAML 属性映射	（可选）如果 SaaS 应用需要，您可以向 SaaS 应用提供来自 LDAP 身份验证服务器的有关内部用户的额外信息。将每个 LDAP 服务器属性映射为 SAML 属性。

属性	说明
身份验证上下文	选择 Web 代理用于对其内部用户进行身份验证的身份验证机制。 注释 身份验证情景可通知服务提供程序身份提供程序对内部用户进行身份验证时所使用的身份验证机制。一些服务提供程序需要特殊身份验证机制来允许用户访问 SaaS 应用。如果服务提供商需要不受标识提供程序支持的身份验证情景，则用户无法使用单点登录从标识提供程序访问服务提供商。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

使用配置应用时的相同参数，设置 SaaS 应用端的单点登录设置。

配置最终用户访问单点登录 URL

将网络安全设备配置为身份提供程序并为 SaaS 应用创建 SaaS 应用身份验证策略后，设备会创建单点登录 URL (SSO URL)。网络安全设备使用在 SaaS 应用身份验证策略中配置的应用名称生成单点登录 URL；SSO URL 格式为：

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

步骤 1 从**网络安全管理器 (Web Security Manager) > SaaS 策略 (SaaS Policies)** 页面获取单点登录 URL。

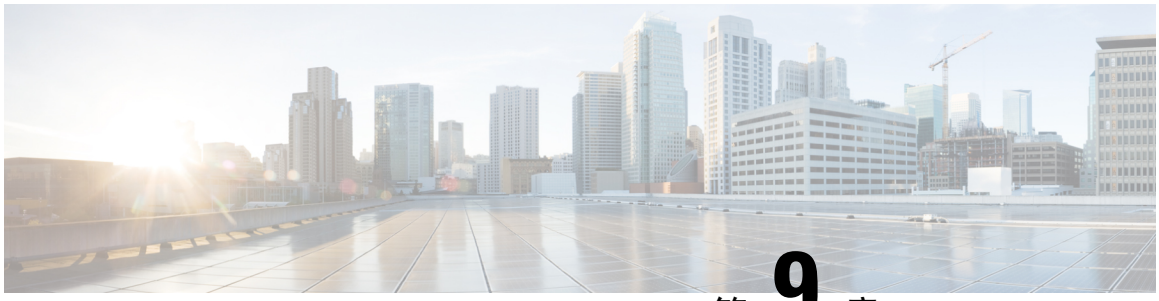
步骤 2 将 URL 提供给最终用户，这取决于流量类型。

步骤 3 如果选择身份提供程序发起的流量，设备会将用户重定向到 SaaS 应用。

步骤 4 如果选择服务提供程序发起的流量，您必须在 SaaS 应用中配置此 URL。

- 总是提示 SaaS 用户进行代理身份验证。在输入有效的凭证后，用户登录到 SaaS 应用。
- 透明登录 SaaS 用户。用户自动登录到 SaaS 应用。

  注释 在透明模式下部署设备时，要使用显式转发请求让所有通过身份验证的用户实现单点登录行为，请在配置身份组时选择“**将相同的代理设置应用于显式转发请求 (Apply same surrogate settings to explicit forward requests)**”。



第 9 章

集成思科身份服务引擎

本章包含以下部分：

身份服务引擎服务概述

思科身份服务引擎 (ISE) 是一个可在网络中的独立服务器上运行的应用，旨在提供增强的身份管理功能。AsyncOS 可通过 ISE 服务器访问用户身份信息。如果已配置 ISE，则系统会通过正确配置的标识配置文件所对应的身份服务引擎获取用户名和关联的安全组标记，以允许在配置为使用这些配置文件的策略中使用透明用户识别。

注释 ISE 服务在“连接器”(Connector) 模式下不可用。

相关主题

- 关于 pxGrid， 第 129 页
- 关于 ISE 服务器的部署和故障切换， 第 130 页

关于 pxGrid

思科平台交换架构 (pxGrid) 支持网络基础设施（包括安全监控和网络检测系统、身份和访问管理平台等）组件之间的协作。这些组件可通过发布/订用方式使用 pxGrid 来交换信息。

pxGrid 主要包括下列三个部分：pxGrid 发布方、pxGrid 客户端和 pxGrid 控制器。

- pxGrid 发布方 - 为 pxGrid 客户端提供信息。

- pxGrid 客户端 - 用于订用已发布信息的任何系统，如网络安全设备等；在本例中，是指安全组标签 (SGT) 以及用户组和分析信息。
- pxGrid 控制器 - 在本例中，是指用于控制客户端注册/管理和主题/订用过程的 ISE pxGrid 节点。

每个组件都需要提供受信任证书，并且必须在每个主机平台上安装这些证书。

关于 ISE 服务器的部署和故障切换

单个 ISE 节点设置称为“独立部署”，并且此单个节点会运行管理、策略服务和监控角色。要支持故障切换和提高性能，必须以“分布式部署”方式设置多个 ISE 节点。支持在网络安全设备上进行 ISE 故障切换所需的最低分布式 ISE 配置要求如下：

- 2 个 pxGrid 节点
- 2 个监控节点
- 2 个管理节点
- 1 个策略服务节点

有关此配置的详细信息，请参阅《思科身份服务引擎硬件安装指南》的“中型网络部署”部分。有关更多信息，请参阅《安装指南》的网络部署章节。

相关主题

- 身份服务引擎证书，第 130 页
- 认证和集成 ISE 服务任务，第 131 页
- 连接到 ISE 服务，第 134 页
- 排除身份服务引擎故障，第 136 页

身份服务引擎证书

注释 本部分介绍 ISE 连接必需的证书。认证和集成 ISE 服务任务，第 131 页 提供有关这些证书的详细信息。证书管理，第 406 页提供 AsyncOS 的通用证书管理信息。

为了在网络安全设备和各 ISE 服务器之间实现相互身份验证和安全通信，需要含三个证书的证书组：

- **WSA 客户端证书 (WSA Client Certificate)** - 供 ISE 服务器用于对网络安全设备进行身份验证。
- **ISE 管理员证书 (ISE Admin Certificate)** - 供网络安全设备用于对端口 443 上的 ISE 服务器进行身份验证，以批量下载 ISE 用户配置文件数据。
- **ISE pxGrid 证书 (ISE pxGrid Certificate)** - 供网络安全设备用于对端口 5222 上的 ISE 服务器进行身份验证，以订用 WSA-ISE 数据（对 ISE 服务器持续进行发布/订用查询）。

这三个证书可以是证书颁发机构 (CA) 签名证书或自签名证书。AsyncOS 提供此选项的目的在于生成自签名 WSA 客户端证书，或者在需要 CA 签名证书时，转而生成证书签名请求 (CSR)。同样，ISE 服务器提供此选项的目的在于生成自签名 ISE 管理员证书和 pxGrid 证书，或者在需要 CA 签名证书时，转而生成 CSR。

相关主题

- 使用自签名证书，第 131 页
- 使用 CA 签名证书，第 131 页
- 身份服务引擎服务概述，第 129 页
- 认证和集成 ISE 服务任务，第 131 页
- 连接到 ISE 服务，第 134 页

使用自签名证书

在 ISE 服务器上使用自签名证书时，所有三个证书（在 ISE 服务器上开发的 ISE pxGrid 证书和管理员证书以及在 WSA 上开发的 WSA 客户端证书）必须添加到 ISE 服务器上的受信任证书存储区（“管理”(Administration) > “证书”(Certificates) > “受信任证书”(Trusted Certificates) > “导入”(Import)）。

使用 CA 签名证书

对于 CA 签名证书：

- 在 ISE 服务器上，确保 WSA 客户端证书的适当 CA 根证书存在于受信任证书存储区（“管理”(Administration) > “证书”(Certificates) > “受信任证书”(Trusted Certificates)）。
- 在 WSA 上，确保适当 CA 根证书存在于受信任证书列表中（“网络”(Network) > “证书管理”(Certificate Management) > “管理受信任根证书” (Manage Trusted Root Certificates)）。在“身份服务引擎”(Identity Services Engine) 页上（“网络”(Network) > “身份服务引擎”(Identity Services Engine)），请务必为 ISE 管理员证书和 pxGrid 证书上传 CA 根证书。

认证和集成 ISE 服务任务

步骤	任务	相关主题和程序的链接
1a	在 WSA 上，添加 WSA 客户端证书。	• 在 WSA 上，创建或上传 CA 签名或自签名 WSA 客户端证书。 请参阅连接到 ISE 服务，第 134 页和证书管理，第 406 页。
1b	在 WSA 上，下载此 WSA 客户端证书，以将其上传到 ISE 服务器上。	• 下载 WSA 客户端证书并保存，然后将其传送至 ISE 服务器。 请参阅连接到 ISE 服务，第 134 页。

步骤	任务	相关主题和程序的链接
2	如果 WSA 客户端证书是自签名的，将此证书及其签名证书上传到 ISE 服务器。	• 导入在前一步骤中下载的 WSA 客户端证书，将其添加到 ISE 服务器的受信任证书存储区。（**管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) > 导入 (Import)**） • 请务必同时将此 WSA 客户端证书合适的签名证书添加到 ISE 服务器上的受信任证书存储区，如使用自签名证书，第 131 页中所述。

3	在 ISE 服务器上，添加 ISE 管理员证书和 pxGrid 证书。	• 导航到**管理 (Administration) > 证书 (Certificates)** 页面，并生成或上传 ISE 管理员证书和 pxGrid 证书：
		  • 对于CA签名证书，需生成两个证书签名请求，分别供管理员和 pxGrid 使用，然后对证书执行签名操作。
		  收到签名证书后，将两个证书都上传到 ISE 服务器上。
		  对两个证书执行“绑定 CA 签名证书”操作。
		  请务必将 CA 根证书添加到 ISE 服务器的受信任证书存储区。
		  重新启动 ISE 服务器。
		  • 对于自签名证书，请导航到 **管理 (Administration) > 证书 (Certificates) > 系统证书 (System Certificates)**，并生成两个自签名证书，分别用于管理员和 pxGrid。（还可以选择为这两个证书生成一个通用证书。）
		  将两个证书添加到受信任证书存储区。
		  导出自签名证书，以导入 WSA。
		注释 确保这些 ISE 管理员证书和 pxGrid 证书合适的自签名或 CA 根证书添加到受信任证书存储区，如身份服务引擎证书，第 130 页中所述。

步骤	任务	相关主题和程序的链接
4	确保正确配置ISE服务器以进行 WSA 访问。	每台 ISE 服务器必须配置为允许身份主题用户（例如 WSA）获取实时会话情景。基本步骤是： • 确保打开“启用自动注册”(Enable Auto Registration)（“管理”(Administration)>“pxGrid 服务”(pxGrid Services)>右上角）。 • 从 ISE 服务器删除所有现有 WSA 客户端（“管理”(Administration)>“pxGrid 服务”(pxGrid Services)>“客户端”(Clients)）。 • 确保 ISE 服务器页脚（“管理”(Administration)>“pxGrid 服务”(pxGrid Services)）显示“已连接到 pxGrid”(Connected to pxGrid)。 • 在 ISE 服务器上配置 SGT 组（“策略”(Policy)>“结果”(Results)>TrustSec>“安全组”(Security Groups)）。 • 配置对 SGT 组与用户进行关联操作的策略。 有关详细信息，请参阅《思科身份服务引擎文档》。
5	在 WSA 上，添加已导出的 ISE 管理员证书和 pxGrid 证书。	• 上传您要在此 WSA 上为每台 ISE 服务器配置的 ISE 管理员证书和 pxGrid 证书。请参阅连接到 ISE 服务，第 134 页。 • 如果 ISE 管理员和 pxGrid 使用单个自签名证书，请将证书文件上传两次，分别上传至“ISE 管理员证书”(ISE Admin Certificate) 和“ISE pxGrid 证书”(ISE pxGrid Certificate fields) 字段。请参阅连接到 ISE 服务，第 134 页。 • 如果使用 CA 签名证书，确保签署每对 ISE 证书的证书颁发机构在 WSA 的受信任根证书列表中列出。否则，请导入 CA 根证书。请参阅管理受信任的根证书，第 407 页。 **注释** 如果 ISE 管理员证书和 pxGrid 证书由根 CA 证书签名，请确保将其自身的根 CA 证书上传到 WSA 上的“ISE 管理员证书”(ISE Admin Certificate) 和“ISE pxGrid 证书”(ISE pxGrid Certificate fields) 字段（“网络”(Network)>“身份服务引擎”(Identity Services Engine)）。

步骤	任务	相关主题和程序的链接
6	完成 WSA 的 ISE 访问和日志记录的配置。	• 连接到 ISE 服务，第 134 页 • 将自定义字段 %m 添加至“访问日志”(Access Log)，以记录身份验证机制 - 自定义访问日志，第 361 页。 • 确认已创建“ISE 服务日志”(ISE Service Log)；否则，请创建日志 - 添加和编辑日志订用，第 338 页。 • 确保已创建“ISE 服务日志”(ISE Service Log)；否则，请添加日志 - 添加和编辑日志订用，第 338 页。 • 定义用于访问 ISE 的“标识配置文件”(Identification Profile)，以进行用户识别和身份验证 - 用户和客户端软件分类，第 115 页。 • 配置使用 ISE 识别的访问策略，以定义发出用户请求所需的条件和操作 - 策略配置，第 184 页。

注释 在 ISE 服务器上上传或更换证书时，必须重新启动 ISE 服务。此外，可能需要等待几分钟，才能恢复相关服务和连接。

相关主题

- 身份服务引擎服务概述，第 129 页
- 身份服务引擎证书，第 130 页
- 排除身份服务引擎故障，第 136 页

连接到 ISE 服务

开始之前

- 确保正确配置每台 ISE 服务器以进行 WSA 访问；请参阅认证和集成 ISE 服务任务，第 131 页。
- 获取 ISE 服务器连接信息。
- 获取有效的与 ISE 相关的证书（客户端、门户和 pxGrid）和密钥。有关其他相关信息，另请参阅身份服务引擎证书，第 130 页。

步骤 1 依次选择**网络 (Network) > 标识服务引擎 (Identification Service Engine)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用 ISE 服务 (Enable ISE Service)**。

步骤 4 使用**主 ISE pxGrid 节点 (Primary ISE pxGrid Node)** 的主机名或 IPv4 地址对其进行识别。

a) 提供 **ISE pxGrid 节点证书 (ISE pxGrid Node Certificate)**，用于订用 WSA-ISE 数据（对 ISE 服务器持续进行查询）。

浏览并选择证书文件，然后点击**上传文件 (Upload File)**。有关其他信息，请参阅上传证书和密钥，第 408 页。

步骤 5 如果使用辅助 ISE 服务器进行故障切换，请使用辅助 **ISE pxGrid 节点 (Secondary ISE pxGrid Node)** 的主机名或 IPv4 地址对其进行识别。

a) 提供辅助 **ISE pxGrid 节点证书 (ISE pxGrid Node Certificate)**。

浏览并选择证书文件，然后点击**上传文件 (Upload File)**。有关其他信息，请参阅上传证书和密钥，第 408 页。

注释 在从主 ISE 服务器故障切换到辅助 ISE 服务器期间，将要求现有 ISE SGT 缓存中未包含的任何用户都接受身份验证，或者将为其分配“访客”(Guest) 授权，具体取决于 WSA 配置。在 ISE 故障切换完成后，将恢复正常的 ISE 身份验证。

步骤 6 上传 **ISE 监控节点管理员证书 (ISE Monitoring Node Admin Certificates)**：

a) 提供**主 ISE 监控节点管理员证书 (Primary ISE Monitoring Node Admin Certificate)**，用于将 ISE 用户配置文件数据批量下载至 WSA。

浏览并选择证书文件，然后点击**上传文件 (Upload File)**。有关其他信息，请参阅上传证书和密钥，第 408 页。

b) 如果使用辅助 ISE 服务器进行故障切换，请提供**辅助 ISE 监控节点管理员证书 (Secondary ISE Monitoring Node Admin Certificate)**。

步骤 7 提供 **WSA 客户端证书 (WSA Client Certificate)**，以进行 WSA-ISE 服务器相互身份验证：

注释 这必须是 CA 受信任根证书。有关其他相关信息，请参阅身份服务引擎证书，第 130 页。

- **使用上传的证书和密钥 (Use Uploaded Certificate and Key)**

  如需查看证书和密钥，请点击“选择”(Choose)，然后浏览相应的文件。

  如果密钥已加密，请选中**密钥已加密 (Key is Encrypted)** 框。

  点击**上传文件 (Upload Files)**。（有关此选项的更多信息，请参阅上传证书和密钥，第 408 页。）

- **使用生成的证书和密钥 (Use Generated Certificate and Key)**

  点击**生成新的证书和密钥 (Generate New Certificate and Key)**。（有关此选项的更多信息，请参阅生成证书和密钥，第 408 页。）

步骤 8 下载并保存 WSA 客户端证书，然后将其上传到 ISE 服务器主机（“管理”(Administration) > “证书”(Certificates) > “受信任证书”(Trusted Certificates) > “在指定服务器上导入”(Import on the specified server)）。

步骤 9 （可选）点击**启动测试 (Start Test)**，以测试与 ISE pxGrid 节点的连接。

步骤 10 点击**提交 (Submit)**。

下一步做什么

- 用户和客户端软件分类，第 115 页
- 创建策略以控制互联网请求，第 175 页

相关信息

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html，具体而言是“如何通过 pxGrid 使用 ISE 和 TrustSec 集成思科 WSA”。

排除身份服务引擎故障

第 10 章

对策略应用的 URL 进行分类

本章包含以下部分：

URL 事务分类概述

使用策略组，您可以创建安全策略，控制对包含可疑内容的网站的访问。将要阻止、允许或解密的站点取决于您在为每个策略组设置类别阻止时所选的类别。要根据URL类别控制用户访问，您必须启用思科网络使用控件。这是使用域前缀和关键字分析进行 URL 分类的多层 URL 过滤引擎。

您可以在执行以下任务时使用 URL 类别：

选项	方法
定义策略组成员身份 (Define policy group membership)	将 URL 与 URL 类别相匹配， 第 139 页
控制对 HTTP、HTTPS 和 FTP 请求的访问 (Control access to HTTP, HTTPS, and FTP requests)	使用 URL 类别过滤事务， 第 145 页

选项	方法
创建指定特定主机名和 IP 地址的用户定义的自定义 URL 类别 (Create user defined custom URL categories that specify specific hostnames and IP addresses)	创建和编辑自定义 URL 类别，第 151 页

失败 URL 事务的分类

在仅控制对访问策略中的网站的访问时，动态内容分析引擎会对URL进行分类。在确定策略组成员身份或者使用解密或思科数据安全策略控制对网站的访问时，其不会对URL进行分类。这是因为引擎通过分析来自目标服务器的响应内容来工作，因此不能用于必须在从服务器下载任何响应前的请求时间做出的决策。

如果未分类 URL 的 Web 信誉分数处于 WBRS ALLOW 范围内，则 AsyncOS 会允许请求，而不执行动态内容分析。

动态内容分析引擎对 URL 进行分类后，会在临时缓存中存储类别判定和 URL。这样，后续事务便可以从之前的响应扫描中受益，并且可以在请求时间而不是在响应时间进行分类。

启用动态内容分析引擎会影响事务性能。但是，大多数事务使用思科网络使用控件URL类别数据库分类，因此通常只会为小部分事务调用动态内容分析引擎。

启用动态内容分析引擎

注释 访问策略或访问策略中使用的身份可以按预定义URL类别定义策略成员身份，并且访问策略可以对同一URL类别执行操作。在确定身份和访问策略组成员身份时，可以不对请求中的URL进行分类，但在收到服务器响应后，必须由动态内容分析引擎进行分类。思科网络使用控件会忽略动态内容分析引擎的类别判定，并且URL会为事务的剩余部分保留“未分类”判定。后续事务仍将受益于新类别判定。

步骤 1 依次选择**安全服务 (Security Services) > 可接受的使用控制 (Acceptable Use Controls)**。

步骤 2 启用思科网络使用控件。

步骤 3 点击以启用动态内容分析引擎。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

未分类的 URL

未分类的 URL 是不匹配任何预定义 URL 类别或包含的自定义 URL 类别的 URL。

注释 在确定策略组成员身份时，仅当为策略组成员身份选择自定义 URL 类别时，才会将该自定义 URL 类别视为包含在内。

产生不匹配类别的所有事务均将在“报告”(Reporting) >“URL 类别”(URL Categories) 页面报告为“未分类的 URL”(Uncategorized URLs)。对内部网络中网站的请求会生成大量未分类 URL。思科建议使用自定义 URL 类别来分组内部 URL 并允许对内部网站的所有请求。这会减少报告为“未分类的 URL”(Uncategorized URLs) 的 Web 事务数量，而是将内部事务报告为“绕过的 URL 过滤”(URL Filtering Bypassed) 统计数据的一部分。

相关主题

- 了解未过滤和未分类的数据，第 161 页.
- 创建和编辑自定义 URL 类别，第 151 页.

将 URL 与 URL 类别相匹配

当 URL 过滤引擎将 URL 类别与客户端请求中的 URL 匹配时，其会先根据策略组中包含的自定义 URL 类别评估该 URL。如果请求中的 URL 与包含的自定义类别不匹配，则 URL 过滤引擎会将其与预定义 URL 类别进行比较。如果该 URL 与任何包含的自定义或预定义 URL 类别均不匹配，则请求未分类。

注释 在确定策略组成员身份时，仅在为策略组成员身份选择了自定义URL类别时，才视为包含该自定义 URL 类别。

要了解为特定网站分配的类别，请转到报告未分类和误分类的 URL，第 139 页中的 URL。

相关主题

- 未分类的 URL，第 138 页.

报告未分类和误分类的 URL

您可以向思科报告未分类和分类有误的 URL。思科在其网站上提供了一款 URL 提交工具，该工具允许您同时提交多个 URL：

https://securityhub.cisco.com/web/submit_urls

要检查已提交的 URL 的状态，请点击此页面上的“有关已提交 URL 的状态”选项卡。您还可以使用 URL 提交工具查找任何 URL 的已分配 URL 类别。

URL 类别数据库

URL 的分类由过滤类别数据库决定。网络安全设备收集信息并为每个 URL 过滤引擎维护一个单独的数据库。过滤类别数据库定期从思科更新服务器接收更新。

URL 类别数据库包括许多思科内部的和来自互联网的不同因素和数据源。其中一个偶尔会考虑到的、经过大量修改的因素是来自“开放目录项目”的信息。

要了解为特定网站分配的类别，请转到报告未分类和误分类的 URL，第 139 页中的 URL。

相关主题

- 手动更新安全服务组件，第 413 页.

配置 URL 过滤引擎

默认情况下，在“系统安装向导”(System Setup Wizard) 中会启用思科网络使用控件 URL 过滤引擎。

步骤 1 依次选择**安全服务 (Security Services) > 可接受的使用控制 (Acceptable Use Controls)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 验证是否启用了“启用可接受的使用控制”(Enable Acceptable Use Controls) 属性。

步骤 4 选择是否启用动态内容分析引擎。

步骤 5 选择在 URL 过滤引擎不可用时 Web 代理将采用的默认操作，即“监控”(Monitor) 或“阻止”(Block)。默认值为“监控”(Monitor)。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

管理 URL 类别集更新

预定义的 URL 类别集可能会偶尔更新，以适应新的 Web 趋势和不断发展的使用模式。URL 类别集的更新与添加新 URL 和重映射分类有误的 URL 等更改有所不同。类别集更新可能会更改现有策略的配置，因此需要采取操作。产品版本之间可能会有 URL 类别集更新；无需 AsyncOS 升级。

相关信息可以从以下位置获取：
http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html。

请采取以下操作：

何时采取操作	方法
更新前 （将这些任务作为初始设置的一部分来执行）	了解 URL 类别集更新的影响，第 141 页 控制对 URL 类别集的更新，第 143 页 新增和更改的类别的默认设置，第 144 页 接收有关类别和策略更改的警报，第 145 页
更新后	响应有关 URL 类别集更新的警报，第 145 页

了解 URL 类别集更新的影响

URL 类别集更新可能会对现有访问策略、解密策略、思科数据安全策略以及身份带来以下影响：

- URL 类别集更改对策略组成员身份的影响，第 141 页
- URL 类别集更新对策略中的过滤操作的影响，第 141 页

URL 类别集更改对策略组成员身份的影响

此部分适用于带有可按URL类别定义的成员的所有策略类型以及身份。在策略组成员身份是按URL类别定义的情况下，对类别集进行更改可能会带来以下影响：

- 如果成员身份的唯一条件是已删除的类别，则策略或身份会被禁用。

在任何策略中的成员身份是按更改的URL类别定义的情况下，如果这会导致ACL列表更改，则Web代理将重新启动。

URL 类别集更新对策略中的过滤操作的影响

URL 类别集更新可通过以下方式更改策略行为：

变化	对策略和身份的影响
可以添加新类别	对于每个策略，新添加类别的默认操作是为该策略的“未分类的URL”(Uncategorized URLs) 指定的操作。
可以删除类别	与已删除类别关联的操作会被删除。 如果策略完全取决于已删除的类别，则策略会被禁用。 如果策略取决于完全取决于已删除类别的身份，则策略将被禁用。
可以对类别进行重命名	现有策略的行为没有变化。
可以拆分类别	一个类别可以成为多个新类别。这两种新类别的操作与原始类别相关联。

变化	对策略和身份的影响
可以合并两个或多个现有类别	如果策略中的所有原始类别均分配有相同的操作，则合并的类别具有与原始类别相同的操作。如果所有原始类别均设置为“使用全局设置”(Use Global Setting)，则合并的类别也设置为“使用全局设置”(Use Global Setting)。 如果策略为原始类别分配了不同的操作，则分配到合并类别的操作取决于该策略中的“未分类的 URL”(Uncategorized URLs) 设置： • 如果“未分类的 URL”(Uncategorized URLs) 设置为“阻止”(Block)（或在全局设置为“阻止”(Block)时，其设置为“使用全局设置”(Use Global Setting)），则原始类别中限制性最高的操作会应用到合并的类别。 • 如果“未分类的 URL”(Uncategorized URLs) 设置为“阻止”(Block)之外的任何操作（或在全局设置为“阻止”(Block) 之外的任何操作时，其设置为“使用全局设置”(Use Global Setting)），则原始类别中限制性最低的操作会应用到合并的类别。 在这种情况下，用户现在可以访问之前被阻止的站点。 如果策略成员身份是按 URL 类别定义的，并且在合并或“未分类的 URL”(Uncategorized URLs) 操作中涉及的某些类别未包含在策略成员身份定义中，则全局策略中的值会用于缺失的项目。 限制的顺序如下所示（并非所有操作对所有策略类型都可用）： • 阻止 (Block) • 丢弃 (Drop) • 解密 (Decrypt) • 警告 (Warn) • 基于时间 (Time-based) • 监控 (Monitor) • 通过 (Pass Through) 注释 以合并类别为基础的基于时间的策略采用与任一原始类别关联的操作。（在基于时间的策略中，可能没有明显的限制性最高或限制性最低的操作。）

相关主题

• 合并的类别 - 示例， 第 143 页.

合并的类别 - 示例

根据策略的“URL 过滤”(URL Filtering) 页面中的设置，一些合并类别的示例如下：

原始类别 1	原始类别 2	未分类的 URL	合并的类别
监控 (Monitor)	监控 (Monitor)	（不适用）	监控 (Monitor)
阻止 (Block)	阻止 (Block)	（不适用）	阻止 (Block)
使用全局设置	使用全局设置	（不适用）	使用全局设置 (Use Global Settings)
警告 (Warn)	阻止 (Block)	监控 (Monitor) 使用原始类别中限制性最低的操作。	警告 (Warn)
监控 (Monitor)	• 阻止 (Block) 或 • 使用“全局设置” (Use Global Settings)（当“全局”(Global) 设置为“阻止”(Block)时）	• 阻止 (Block) 或 • 使用全局设置 (Use Global Setting)（当“全局”(Global) 设置为“阻止”(Block) 时） 使用原始类别中限制性最高的操作。	阻止 (Block)
阻止 (Block)	• 监控 (Monitor) 或 • 使用全局设置 (Use Global Settings)（当“全局”(Global) 设置为“监控”(Monitor)) 时）	• 监控 (Monitor) 或 • 使用全局设置 (Use Global Setting)（当“全局”(Global) 设置为“监控”(Monitor) 时） 使用在原始类别中受限最少的操作。	监控 (Monitor)
对于成员身份是按 URL 类别定义的策略： 监控 (Monitor)	此类别的操作未在此策略中指定，但此类别的“全局策略”(Global Policy) 的值为“阻止”(Block)	“未分类的 URL”(Uncategorized URLs) 的操作未在此策略中指定，但“未分类的 URL”(Uncategorized URLs) 的“全局策略”(Global Policy) 的值为“监控”(Monitor)	监控 (Monitor)

控制对 URL 类别集的更新

默认情况下，URL 类别集更新自动执行。这些更新可能会更改现有策略配置，因此您可能更愿意禁用所有自动更新。

选项	方法
如果禁用更新，则您需要手动更新“系统管理”(System Administration) > “升级和更新设置”(Upgrade and Update Settings) 页面的“更新服务器”(Update Servers)（列表）部分中列出的所有服务	手动更新 URL 类别集，第 144 页 和 手动更新安全服务组件，第 413 页
禁用所有自动更新	配置升级和服务更新设置，第416页.

注释 如果使用 CLI，将更新间隔设置为零 (0)，即可禁用更新

手动更新 URL 类别集

注释
- 请勿中断正在进行的更新。
- 如果禁用了自动更新，您可以随时手动更新 URL 类别集。

步骤 1 依次选择**安全服务 (Security Services) > 可接受的使用控制 (Acceptable Use Controls)**。

步骤 2 确定是否有更新：

查看“可接受的使用控制引擎更新”(Acceptable Use Controls Engine Updates) 表中的“思科网络使用控件 - Web 分类类别列表”(Cisco Web Usage Controls - Web Categorization Categories List) 项目。

步骤 3 要更新，请点击**立即更新 (Update Now)**。

新增和更改的类别的默认设置

URL 类别集更新可能会更改现有策略的行为。您在配置策略时应为某些更改指定默认设置，以保证它们在URL类别集更新时可供使用。当添加了新类别或现有类别合并到一个新类别中时，每个策略的这些类别的默认操作会受到该策略中“未分类的 URL”(Uncategorized URLs) 设置的影响。

验证现有设置和/或进行更改

步骤 1 选择**网络安全管理器 (Web Security Manager)**。

步骤 2 对于每个访问策略、解密策略和思科数据安全策略，点击 **URL 过滤 (URL Filtering)**链接。

步骤 3 选中“未分类的 URL”(Uncategorized URLs) 的选定设置。

下一步做什么

相关主题

- URL 类别集更新对策略中的过滤操作的影响，第 141 页.

接收有关类别和策略更改的警报

类别集更新会触发两种类型的警报：

- 关于类别更改的警报
- 关于由于类别集更改而发生变化或被禁用的策略的警报。

步骤 1 依次选择**系统管理 (System Administration) > 警报 (Alerts)**。

步骤 2 点击**添加收件人 (Add Recipient)** 并添加邮件地址（或多个邮件地址）。

步骤 3 决定要接收哪些**警报类型 (Alert Types)** 和**警报严重性级别 (Alert Severities)**。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

响应有关 URL 类别集更新的警报

当收到有关类别集更改的警报时，您应执行以下操作：

- 检查策略和身份以确定它们在类别合并、添加和删除后仍满足策略目标，以及
- 考虑修改策略和身份以从新类别和拆分类别的进一步细化中受益。

相关主题

- 了解 URL 类别集更新的影响，第 141 页

使用 URL 类别过滤事务

通过URL过滤引擎，您可以过滤访问策略、解密策略和数据安全策略中的事务。当您为策略组配置 URL 类别时，可以为自定义 URL 类别（如果已定义）和预定义 URL 类别配置操作。

您可以配置的 URL 过滤操作取决于策略组的类型：

选项	方法
访问策略 (Access Policies)	配置访问策略组的 URL 过滤器，第 146 页
解密策略 (Decryption Policies)	配置解密策略组的 URL 过滤器，第 148 页
思科数据安全策略 (Cisco Data Security Policies)	配置数据安全策略组的 URL 过滤器，第 149 页

相关主题

- 重定向访问策略中的流量，第 158 页
- 警告用户并允许用户继续操作，第 159 页
- 创建和编辑自定义 URL 类别，第 151 页
- URL 类别集更新对策略中的过滤操作的影响，第 141 页

配置访问策略组的 URL 过滤器

可以为用户定义的访问策略组和全局策略组配置 URL 过滤。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要编辑的策略组的“URL 过滤”(URL Filtering) 列下的策略表中的链接。

步骤 3 （可选）在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中，您可以添加要在此策略中采取操作的自定义 URL 类别：

a) 点击**选择自定义类别 (Select Custom Categories)**。

b) 选择要在此策略中包含的自定义 URL 类别，然后点击**应用 (Apply)**。

选择 URL 过滤引擎在比较客户端请求时所依据的自定义 URL 类别。URL 过滤引擎将根据包含的自定义 URL 类别比较客户端请求，并忽略已排除的自定义 URL 类别。URL 过滤引擎将客户端请求中的 URL 与包含的自定义 URL 类别进行比较，然后再与预定义的 URL 类别进行比较。

策略中包含的自定义 URL 类别显示在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中。

步骤 4 在自定义 URL 类别过滤 (Custom URL Category Filtering) 部分中，为每个包含的自定义 URL 类别选择一个操作。

操作	说明
使用全局设置 (Use Global Settings)	为全局策略组中的此类别使用该操作。这是用户定义的策略组的默认操作。 仅适用于用户定义的策略组。 **注释** 如果某自定义 URL 类别不包含在全局访问策略中，则用户定义的访问策略中包含的自定义URL类别的默认操作是“监控”(Monitor)而不是“使用全局设置”(Use Global Settings)。如果某自定义 URL 类别不包含在全局访问策略中，则您不能选择“使用全局设置”(Use Global Settings)。
阻止 (Block)	Web 代理拒绝匹配此设置的事务。
重定向 (Redirect)	将最初发往此类别中的URL 的流量重定向到指定的位置。选择此操作时，系统会显示“重定向到”(Redirect To) 字段。输入要将所有流量重定向到的 URL。
允许 (Allow)	始终允许此类别中网站的客户端请求。 允许的请求会绕过所有进一步过滤和恶意软件扫描。 仅限对受信任的网站使用此设置。您可能要将此设置用于内部站点。

操作	说明
监控 (Monitor)	Web 代理既不允许请求，也不阻止请求。相反，它会继续根据其他策略组控制设置（例如 Web 信誉过滤）来评估客户端请求。
警告 (Warn)	Web 代理最初会阻止请求并显示一个警告页面，但是允许用户通过点击警告页面中的超文本链接继续进行操作。
基于配额 (Quota-Based)	当个人用户接近您指定的量或时间配额时，系统会显示警告。达到配额时，会显示阻止页面。请参阅时间范围和配额，第 191 页。
基于时间 (Time-Based)	Web 代理在指定的时间范围内阻止或监控请求。请参阅时间范围和配额，第 191 页。

步骤 5 在“预定义 URL 类别过滤”(Predefined URL Category Filtering) 部分中，为每个类别选择以下操作之一：

- 使用全局设置 (Use Global Settings)
- 监控 (Monitor)
- 警告 (Warn)
- 阻止 (Block)
- 基于时间 (Time-Based)
- 基于配额 (Quota-Based)

步骤 6 在“未分类的 URL”(Uncategorized URLs) 部分中，选择要对不属于预定义或自定义 URL 类别的网站的客户端请求采取的操作。此设置还确定因 URL 类别集更新而产生的新类别和合并类别的默认操作。

步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

- 阻止嵌入内容/引用内容的例外，第 147 页

阻止嵌入内容/引用内容的例外

网站可以嵌入或引用与源页面分类不同或被视为应用的内容。默认情况下，无论源网站如何分类，嵌入/引用内容均会根据为其指定类别或应用选择的操作受到阻止或监控。例如，新闻站点可能包含分类为视频流且已识别为 YouTube 应用的内容或内容链接。根据您的策略，视频流和 YouTube 均被阻止，而新闻站点不会。

注释 请求嵌入内容通常包括发出请求站点的地址（这称为请求的 HTTP 报头中的“引用”字段）。此报头信息用于确定引用内容的分类。

您可以使用此功能定义嵌入/引用内容默认操作的例外，例如，允许在新闻网站嵌入或从其引用的所有内容，或允许在代表您内联网的自定义类别嵌入或从其引用的所有内容。

注释 基于引用的例外情况仅在访问策略中受支持。要对 HTTPS 流量使用此功能，则在访问策略中定义例外之前，必须配置您将为例外选择的 URL 类别的 HTTPS 解密。请参阅配置解密策略组的 URL 过滤器，第 148 页了解有关配置 HTTPS 解密的信息。请参阅针对阻止嵌入和引用内容的例外情况的条件和限制，第 432 页了解有关通过 HTTPS 解密使用此功能的更多信息。

步骤 1 在特定访问策略的 URL 过滤页面上（请参阅配置访问策略组的 URL 过滤器，第 146 页），点击“阻止嵌入内容/引用内容的例外”(Exceptions to Blocking for Embedded/Referred Content) 部分中的**启用异常 (Enable Exceptions)**。

步骤 2 在“按这些类别设置引用内容的例外”(Set Exception for Content Referred by These Categories) 列中，点击**点击选择类别 (Click to select categories)**链接，打开 URL 过滤类别引用例外选择页面。

步骤 3 从预定义和自定义 URL 类别列表中，选择您要为其定义此引用例外的分类，然后点击**完成 (Done)** 返回此访问策略的 URL 过滤页面。

步骤 4 从“为此引用内容设置例外”(Set Exception for this Referred Content) 的下拉列表中选择例外类型：

- **所有嵌入/引用内容 (All embedded/referred content)** - 不阻止在指定类别类型的站点嵌入的或从其引用的所有内容，而不考虑内容的分类如何。
- **选择的嵌入/引用内容 (Selected embedded/referred content)** - 选择此选项后，选择源自特定 URL 类别不会被阻止的特定类别和应用。
- **所有嵌入/引用内容除外 (All embedded/referred content except)** - 选择此选项后，不被阻止从指定类别类型的站点嵌入的或从其引用的所有内容，但此处现在指定的 URL 类别和应用除外。换言之，这些类型仍会被阻止。

步骤 5 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

可选择在以下报告页面提供的表和图表上显示“按引用允许”(Permitted by Referrer) 事务数据：URL 类别、用户和网站以及“概述”(Overview) 页面上的相关图表。请参阅选择要绘图的数据，第 302 页了解有关选择图表显示选项的更多信息。

配置解密策略组的 URL 过滤器

您可以为用户定义的解密策略组和全局解密策略组配置 URL 过滤。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 解密策略 (Decryption Policies)**。

步骤 2 点击要编辑的策略组的“URL 过滤”(URL Filtering) 列下的策略表中的链接。

步骤 3 （可选）在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中，您可以添加要在此策略中采取操作的自定义 URL 类别：

a) 点击**选择自定义类别 (Select Custom Categories)**。
b) 选择要在此策略中包含的自定义 URL 类别，然后点击**应用 (Apply)**。

选择 URL 过滤引擎在比较客户端请求时所依据的自定义 URL 类别。URL 过滤引擎将根据包含的自定义 URL 类别比较客户端请求，并忽略已排除的自定义URL类别。URL过滤引擎将客户端请求中的URL与包含的自定义 URL 类别进行比较，然后再与预定义的 URL 类别进行比较。

策略中包含的自定义 URL 类别显示在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中。

步骤 4 为每个自定义和预定义的 URL 类别选择一项操作。

操作	说明
使用全局设置 (Use Global Setting)	为全局解密策略组中的此类别使用该操作。这是用户定义的策略组的默认操作。 仅适用于用户定义的策略组。 如果某自定义 URL 类别不包含在全局解密策略中，则用户定义的解密策略中包含的自定义 URL 类别的默认操作是“监控”(Monitor) 而不是“使用全局设置”(Use Global Settings)。如果某自定义URL类别不包含在全局解密策略中，则您不能选择“使用全局设置”(Use Global Settings)。
通过 (Pass Through)	通过客户端和服务器之间的连接而不检测流量内容。
监控 (Monitor)	Web代理既不允许请求，也不阻止请求。相反，它会继续根据其他策略组控制设置（例如 Web 信誉过滤）来评估客户端请求。
解密 (Decrypt)	允许连接，但会检测流量内容。设备解密流量并将访问策略应用于已解密的流量，就如同它是明文HTTP连接一样。通过解密连接和应用访问策略，可以扫描流量来查找恶意软件。
丢弃 (Drop)	丢弃连接，并且不通过对服务器的连接请求。设备不会通知用户它已断开连接。

注释 如果要阻止 HTTPS 请求的特定 URL 类别，请选择对解密策略组中的该 URL 类别进行解密，然后选择阻止访问策略组中的同一 URL 类别。

步骤 5 在“未分类的 URL”(Uncategorized URLs) 部分中，选择要对不属于预定义或自定义 URL 类别的网站的客户端请求采取的操作。

此设置还确定因 URL 类别集更新而产生的新类别和合并类别的默认操作。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

配置数据安全策略组的 URL 过滤器

您可以为用户定义的数据安全策略组和全局策略组配置 URL 过滤。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 思科数据安全 (Cisco Data Security)**。

步骤 2 点击要编辑的策略组的“URL 过滤”(URL Filtering) 列下的策略表中的链接。

步骤 3 （可选）在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中，您可以添加要在此策略中采取操作的自定义 URL 类别：

a) 点击**选择自定义类别 (Select Custom Categories)**。

b) 选择要在此策略中包含的自定义 URL 类别，然后点击**应用 (Apply)**。

选择 URL 过滤引擎在比较客户端请求时所依据的自定义 URL 类别。URL 过滤引擎将根据包含的自定义 URL 类别比较客户端请求，并忽略已排除的自定义 URL 类别。URL 过滤引擎将客户端请求中的 URL 与包含的自定义 URL 类别进行比较，然后再与预定义的 URL 类别进行比较。

策略中包含的自定义 URL 类别显示在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中。

步骤 4 在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中，为每个自定义 URL 类别选择一个操作。

操作	说明
使用全局设置 (Use Global Setting)	为全局策略组中的此类别使用该操作。这是用户定义的策略组的默认操作。 仅适用于用户定义的策略组。 如果某自定义 URL 类别不包含在全局思科数据安全策略中，则用户定义的思科数据安全策略中包含的自定义 URL 类别的默认操作是“监控”(Monitor) 而不是“使用全局设置”(Use Global Settings)。如果某自定义 URL 类别不包含在全局思科数据安全策略中，则您不能选择“使用全局设置”(Use Global Settings)。
允许 (Allow)	始终允许此类别中网站的上传请求。仅适用于自定义 URL 类别。 允许的请求会绕过进一步数据安全扫描，并且系统会根据访问策略评估该请求。 仅限对受信任的网站使用此设置。您可能要将此设置用于内部站点。
监控 (Monitor)	Web 代理既不允许请求，也不阻止请求。相反，它会继续根据其他策略组控制设置（例如 Web 信誉过滤）来评估上传请求。
阻止 (Block)	Web 代理拒绝匹配此设置的事务。

步骤 5 在“预定义 URL 类别过滤”(Predefined URL Category Filtering) 部分中，为每个类别选择以下操作之一：

- 使用全局设置 (Use Global Settings)
- 监控 (Monitor)
- 阻止 (Block)

步骤 6 在“未分类的 URL”(Uncategorized URLs) 部分中，选择要对不属于预定义或自定义 URL 类别的网站的上传请求采取的操作。此设置还确定因 URL 类别集更新而产生的新类别和合并类别的默认操作。

步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- URL 类别集更新对策略中的过滤操作的影响，第 141 页.

创建和编辑自定义 URL 类别

可以创建用于描述特定主机名和 IP 地址的自定义和外部实时源 URL 类别。此外，还可以编辑和删除现有 URL 类别。在同一访问策略、解密策略或思科数据安全策略组中包含这些自定义 URL 类别并为每个类别分配不同的操作时，包含的更高自定义 URL 类别的操作会优先。

注释 您可以在这些 URL 类别定义中最多使用五个外部实时源文件，且每个文件包含的条目数不应超过 1000 个。增加外部源条目数会导致性能下降。

网络安全设备在访问日志中使用自定义 URL 类别名称的前四个字符，前面加上“c_”。如果使用 Sawmill 解析访问日志，请考虑自定义 URL 类别名称。如果自定义 URL 类别的前四个字符包含空格，则 Sawmill 不能正确解析访问日志条目。相反，仅在前四个字符中使用支持的字符。如果要在访问日志中包含自定义 URL 类别的全称，请将 %XF 格式说明符添加到访问日志。

开始之前

转到**安全服务 (Security Services)** > **可接受的使用控制 (Acceptable Use Controls)** 启用可接受的使用控制。

步骤 1 选择**网络安全管理器 (Web Security Manager** > **自定义和外部 URL 类别 (Custom and External URL Categories)**。

步骤 2 要创建自定义 URL 类别，请点击**添加类别 (Add Category)**。要编辑现有的自定义 URL 类别，请点击 URL 类别的名称。

步骤 3 提供以下信息。

设置	说明
类别名称 (Category Name)	输入此 URL 类别的标识符。此名称会在您为策略组配置 URL 过滤时显示。
列表顺序 (List Order)	在自定义 URL 类别列表中指定此类别的顺序。为列表中的第一个 URL 类别输入“1”。 URL 过滤引擎会针对指定顺序的自定义 URL 类别对客户端请求进行评估。
类别类型 (Category Type)	选择**本地自定义类别 (Local Custom Category)** 或**外部实时源类别 (External Live Feed Category)**。
路由表 (Routing Table)	选择**管理 (Management)** 或**数据 (Data)**。此选项仅当启用了“拆分路由”时才可用，即，它不能用于本地自定义类别。有关启用拆分路由的信息，请参阅启用或更改网络接口，第 25 页。

设置	说明
站点/源文件位置 (Sites / Feed File Location)	如果为**类别类型 (Category Type)** 选择**本地自定义类别 (Local Custom Category)**，请提供自定义**站点 (Sites)**： • 输入此自定义类别的一个或多个站点地址。您可以输入多个以换行符或逗号分隔的地址。这些地址可以为下列任何格式： • IPv4 地址，例如 10.1.1.0 • IPv6 地址，如 2001:0db8:: • IPv4 CIDR 地址，例如 10.1.1.0/24 • IPv6 CIDR 地址，例如 2001:0db8::/32 • 域名，例如 example.com • 主机名，例如 crm.example.com • 部分主机名，如 .example.com；这也将匹配 www.example.com • 可以在**高级 (Advanced)** 部分中输入正则表达式，如下所述。 **注释** 可以在多个自定义URL类别中使用相同的地址，但其中的类别列出顺序是相关的。如果在同一策略中包含这些类别，并对每个类别定义了不同的操作，则会应用为自定义 URL 类别表最上方列出的类别定义的操作。 • （可选）点击 **URL 排序 (Sort URLs)**，可对“站点”(Sites) 字段中的所有地址进行排序。 **注释** 对地址进行排序后，您无法检索其原始顺序。

设置	说明
源位置（续）	如果为**类别类型 (Category Type)** 选择**外部实时源类别 (External Live Feed Category)**，请提供**源文件位置 (Feed File Location)** 信息；即，找到并下载包含此自定义类别的地址的文件： 1. 选择**思科源格式 (Cisco Feed Format)** 或 **Office 365 源格式 (Office 365 Feed Format)**，然后提供相应的源文件信息。 • **思科源格式 (Cisco Feed Format)**： • 选择要使用的传输协议（HTTPS 或 HTTP），然后输入实时源文件的 URL。此文件必须是格式为逗号分隔值 (.csv) 的文件。有关此文件的更多信息，请参阅外部源文件格式，第 155 页。 • （可选）在**高级 (Advanced)** 部分中提供**身份验证 (Authentication)** 凭证。提供用于连接到指定源服务器的用户名和密码。 • **Office 365 源格式 (Office 365 Feed Format)**： • 输入实时源文件的 **Office 365 源位置 (Office 365 Feed Format)** (URL)。 此文件必须是 XML 格式的文件；有关此文件的详细信息，请参阅外部源文件格式，第 155 页。 2. 点击**获取文件 (Get File)** 以测试与源服务器的连接，然后从服务器解析并下载源文件。 相应进度将显示在**获取文件 (Get File)** 按钮下面的文本框中。如果发生错误，则系统会指明问题，必须予以纠正，然后才可重试。有关可能的错误的其他信息，请参阅下载外部实时源文件时遇到问题，第 436 页。 **注释** 您可以在这些 URL 类别定义中最多使用五个外部实时源文件，且每个文件包含的条目数不应超过 1000 个。增加外部源条目数会导致性能下降。 **提示** 保存对此实时源类别进行的更改后，可以在“自定义和外部 URL 类别”(Custom and External URL Categories page) 页面（**网络安全管理器 (Web Security Manager)** > **自定义和外部 URL 类别 (Custom and External URL Categories)**）中此条目对应的**源内容 (Feed Content)** 列中点击**查看 (View)**，以打开一个窗口，其中显示您在此处下载的思科源格式或 Office 365 源格式源文件中包含的地址。
高级 (Advanced)	如果为类别类型选择**本地自定义类 (Local Custom Category)**，则可以在此部分中输入正则表达式以指定其他地址集。 您可以使用正则表达式指定与所输入模式匹配的多个地址。 **注释** URL 过滤引擎先将 URL 与“站点”(Sites) 字段中输入的地址相比较。如果事务的 URL 与“站点”(Sites) 字段中的条目匹配，则不与在此处输入的任何表达式进行比较。 有关使用正则表达式的更多信息，请参阅正则表达式，第 161 页。

设置	说明
自动更新源	选择源更新选项： • 不自动更新 • 每 *n* HH:MM；例如，输入 00:05 表示五分钟。但是请注意，频繁更新可能会影响 WSA 性能。 注释 如果可用的源文件与当前下载的文件不同，则将下载较新的文件，并更新下载时间。否则，不会获取文件，并记录“304 未修改”条目。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 正则表达式，第 161 页.
- 自定义访问日志，第 361 页.
- 自定义和外部 URL 类别的问题，第 436 页

自定义和外部 URL 类别的地址格式和源文件格式

创建和编辑自定义和外部 URL 类别时，必须为**本地自定义类别 (Local Custom Category)** 或在**外部实时源类别 (External Live Feed Category)** 源文件中提供一个或多个网络地址。在各个实例中，可输入多个以换行符或逗号分隔的地址。这些地址可以为下列任何格式：

- IPv4 地址，例如 10.1.1.0
- IPv6 地址，如 2001:0db8::
- IPv4 CIDR 地址，例如 10.1.1.0/24
- IPv6 CIDR 地址，例如 2001:0db8::/32
- 域名，例如 example.com
- 主机名，例如 crm.example.com
- 部分主机名，如 .example.com；这也将匹配 www.example.com
- 指定用于匹配所提供模式的多个地址的正则表达式（请参阅正则表达式，第 161 页以了解有关使用正则表达式的更多信息)

注释 可以在多个自定义URL类别中使用相同的地址，但其中的类别列出顺序是相关的。如果在同一策略中包含这些类别，并对每个类别定义了不同的操作，则会应用为自定义URL类别表最上方列出的类别定义的操作。

外部源文件格式

如果在创建和编辑自定义和外部URL类别时，为**类别类型**选择**外部实时源类别**，则必须选择该源格式（**思科源格式**或 **Office 365 源格式**），然后提供一个指向相应源文件服务器的 URL。

每个源文件的预期格式如下：

- **思科源格式** - 必须是逗号分隔值 (.csv) 文件；即，具有.csv 扩展名的文本文件。.csv 文件中的每个条目必须位于单独的行中，并采用地址/逗号/地址类型格式（例如：`www.cisco.com,site` 或 `ad2.*\.com,regex`）。有效的地址类型为 `site` 和 `regex`。以下是思科源格式 .csv 文件摘录：

```
www.cisco.com,site

\.xyz,regex

ad2.*\.com,regex

www.trafficholder.com,site

2000:1:1:11:1:1::200,site
```

注释 在文件的任何 `site` 条目中都不要使用 `http://` 或 `https://`，否则会出错。换言之，`www.example.com` 会被正确分析，而 `http://www.example.com` 会出错。

- **Office 365 源格式** - 这是位于 Microsoft Office 365 服务器或保存该文件的本地服务器上的 XML 文件。该文件由 Office 365 服务提供，无法修改。文件中的网络地址由 XML 标记括起来，结构如下：`products` > `product` > `addresslist` > `address`。在当前的实施中，`addresslist` 类型可以是 IPv6、IPv4 或 URL（可以包含域和正则表达式模式）。以下是 Office 365 源文件的代码段：

```
<products updated="4/15/2016">
   <product name="o365">
      <addresslist type="IPv6">
         <address>2603:1040:401::d:80</address>
         <address>2603:1040:401::a</address>
         <address>2603:1040:401::9</address>
      </addresslist>
      <addresslist type="IPv4">
         <address>13.71.145.72</address>
```

```
            <address>13.71.148.74</address>
            <address>13.71.145.114</address>
         </addresslist>
         <addresslist type="URL">
            <address>*.aadrm.com</address>
            <address>*.azurerms.com</address>
            <address>*.cloudapp.net2</address>
         </addresslist>
      </product>
      <product name="LYO">
         <addresslist type="URL">
            <address>*.broadcast.skype.com</address>
            <address>*.Lync.com</address>
         </addresslist>
      </product>
   </products>
```

过滤成人内容

您可以将网络安全设备配置为过滤某些 Web 搜索和网站的成人内容。为了执行安全搜索和站点内容分级，AVC 引擎通过重写 URL 和/或 Web Cookie 强制打开安全模式，从而利用在特定网站中实施的安全模式功能。

以下功能可过滤成人内容：

选项	说明
执行安全搜索 (Enforce safe searches)	您可以配置网络安全设备，让出站搜索请求对搜索引擎显示为安全搜索请求。这可以防止用户使用搜索引擎绕过可接受的使用策略。
执行站点内容分级 (Enforce site content ratings)	某些内容共享站点允许用户通过执行自己的安全搜索功能或阻止访问成人内容（或同时通过这两种方式）来限制对这些站点上成人内容的访问。此分类功能通常称为内容分级。

注释 任何已启用安全搜索或站点内容分级功能的访问策略都被视为安全浏览访问策略。

实施安全搜索和站点内容分级

注释 启用安全搜索或站点内容分级时，AVC 引擎负责识别安全浏览的应用程序。作为条件之一，AVC 引擎会扫描响应正文以检测搜索应用。因此，设备不会转发范围报头。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击访问策略组或全局策略组的“URL 过滤”(URL Filtering) 列下的链接。

步骤 3 当编辑用户定义的访问策略时，在“内容过滤”(Content Filtering) 部分中选择“定义内容过滤自定义设置”(Define Content Filtering Custom Settings)。

步骤 4 点击**启用安全搜索 (Enable Safe Search)** 复选框可启用安全搜索功能。

步骤 5 选择是否阻止用户使用网络安全设备安全搜索功能当前不支持的搜索引擎。

步骤 6 点击**启用站点内容分级 (Enable Site Content Rating)** 复选框可启用站点内容分级功能。

步骤 7 选择阻止受支持内容分级网站中的所有成人内容还是显示最终用户 URL 过滤警告页面。

注释 当某个受支持搜索引擎或受支持内容分级网站的 URL 包含在某个应用了“允许”(Allow) 操作的自定义 URL 类别中时，系统不会阻止任何搜索结果，所有内容均可见。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 警告用户并允许用户继续操作 ， 第 159 页.

记录对成人内容的访问

默认情况下，访问日志中每个条目的尖括号中包含安全浏览扫描判定。安全浏览扫描判定指示是否将安全搜索或站点内容分级功能应用于事务。您还可以将安全浏览扫描判定变量添加到访问日志或 W3C 访问日志：

- 访问日志：%XS
- W3C 访问日志：x-request-rewrite

值	说明
ensrch	原始客户端请求不安全并且安全搜索功能已应用。
encrt	原始客户端请求不安全并且站点内容分级功能已应用。
unsupp	原始客户端请求对象是不受支持的搜索引擎。
err	原始客户端请求不安全，但是由于错误，无法应用安全搜索和站点内容分级功能。
-	安全搜索和站点内容分级功能均未应用于客户端请求，因为功能被绕过（例如，自定义 URL 类别中允许该事务）或请求来自不支持的应用。

安全搜索或站点内容分级功能导致请求被阻止，请在访问日志中使用以下 ACL 决策标记之一：

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

相关主题

- ACL 决策标记，第 349 页.

重定向访问策略中的流量

您可以配置网络安全设备，以将原先流向自定义 URL 类别中的 URL 的流量重定向到指定的位置。这样您便可以重定向设备上的流量而非目标服务器上的流量。您可以重定向自定义访问策略组或全局策略组的流量

开始之前

要重定向流量，您必须至少定义一个自定义 URL 类别。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击访问策略组或全局策略组的“URL 过滤”(URL Filtering) 列下的链接。

步骤 3 在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分，点击**选择自定义类别 (Select Custom Categories)**。

步骤 4 在**为此策略选择自定义类别 (Select Custom Categories for this Policy)** 对话框中，为要重定向的自定义 URL 类别选择**包含在策略中 (Include in policy)**。

步骤 5 点击**应用 (Apply)**。

步骤 6 点击要重定向的自定义类别的重定向 (Redirect) 列。

步骤 7 在自定义类别的**重定向到 (Redirect To)** 字段中，输入流量重定向的目标 URL。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

注释　在配置设备以重定向流量时，请注意无限循环。

下一步做什么

相关主题

- 创建和编辑自定义 URL 类别，第 151 页

日志记录和报告

当您重定向流量时，最初请求的网站的访问日志条目具有以 REDIRECT_CUSTOMCAT 开头的 ACL 标记。之后访问日志中（通常为下一行）会显示用户被重定向到的网站的条目。

“报告”(Reporting) 选项卡中显示的报告将重定向的事务显示为“已允许”(Allowed)。

警告用户并允许用户继续操作

您可以警告用户站点不符合组织的可接受使用政策。如果身份验证让用户名可用，系统会通过用户名在访问日志中跟踪用户；如果用户名不可用，则通过 IP 地址跟踪用户。

您可以使用以下方法之一警告并允许用户继续操作：

- 为访问策略组中的 URL 类别选择“警告”(Warn) 操作，或
- 启用站点内容分级功能并警告访问成人内容的用户而不是阻止用户。

配置“最终用户过滤警告”(End-User Filtering Warning) 页面的设置

注释
- 警告并继续功能仅适用于 HTTP 和解密的 HTTPS 事务。它不适用于本地 FTP 事务。
- 当 URL 过滤引擎面向特定请求警告用户时，它提供一个警告页面供 Web 代理向最终用户发送警告。但是，并非所有的网站都会向最终用户显示警告页面。如果发生这种情况，系统会阻止用户访问分配了“警告”(Warn) 选项的 URL，让用户没有机会继续访问该站点。

步骤 1　依次选择**安全服务 (Security Services) > 最终用户通知 (End-User Notification)**。

步骤 2　点击**编辑设置 (Edit Settings)**。

步骤 3　在**最终用户过滤警告 (End-User Filtering Warning)** 页面上，配置以下设置：

选项	方法
警告间隔时间 (Time Between Warning)	“警告间隔时间”(Time Between Warning) 确定 Web 代理显示每个用户的每个 URL 类别的最终用户 URL 过滤警告页面的频率。 此设置适用于按用户名跟踪的用户和按 IP 地址跟踪的用户。 指定介于 30 和 2678400 秒（一个月）之间的任一值。默认值为 1 小时（3600 秒）。
自定义消息 (Custom Message)	自定义消息是您输入的显示在每个最终用户 URL 过滤警告页面上的文本。 包含某些简单 HTML 标签，用于对文本进行格式化。

步骤 4 点击“提交”(Submit)。

下一步做什么

相关主题

- 过滤成人内容， 第 156 页
- 通知页面上的自定义消息， 第 284 页
- 配置最终用户 URL 过滤警告页面， 第 283 页

创建基于时间的 URL 过滤器

您可以配置网络安全设备如何根据时间和日期以不同方式处理特定类别中的 URL 请求。

开始之前

依次转至**网络安全管理器 (Web Security Manager) > 定义的时间范围 (Defined Time Range)** 页面，定义至少一个时间范围。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。
步骤 2 点击要编辑的策略组的“URL 过滤”(URL Filtering) 列下的策略表中的链接。
步骤 3 为要根据时间范围配置的自定义或预定义的 URL 类别选择**基于时间范围 (Time-Based)**。
步骤 4 在**时间范围内 (In Time Range)** 字段中，选择要用于 URL 类别的已定义时间范围。
步骤 5 在**操作 (Action)** 字段中，选择要在已定义的时间范围内对此 URL 类别中的事务执行的操作。
步骤 6 在**否则 (Otherwise)** 字段中，选择要在已定义的时间范围外对此 URL 类别中的事务执行的操作。
步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 时间范围和配额， 第 191 页

查看 URL 过滤活动

报告 (Reporting) > URL 类别 (URL Categories) 页面集中显示 URL 统计信息（包括有关排名靠前的匹配的 URL 类别和排名靠前的被阻止的 URL 类别的信息）。该页面显示带宽节省和 Web 事务的类别特定数据。

相关主题

- 生成报告监控最终用户活动， 第 299 页

了解未过滤和未分类的数据

在“报告”(Reporting)>“URL 类别”(URL Categories) 页面上查看 URL 统计信息时，务必了解如何理解以下数据：

数据类型	说明
绕过的 URL 过滤 (URL Filtering Bypassed)	表示在 URL 过滤前发生的策略、端口和管理用户代理阻止。
未分类的 URL (Uncategorized URL)	表示已查询 URL 过滤引擎但未与任何类别相匹配的所有事务。

访问日志中的 URL 类别记录

访问日志文件将每个事务的 URL 类别记录在每个条目的扫描判定信息部分中。

相关主题

- 通过日志监控系统活动， 第 331 页.
- URL 类别说明， 第 165 页.

正则表达式

网络安全设备使用的正则表达式语法与其他 Velocity 模式匹配引擎实施使用的正则表达式语法略有不同。此外，设备不支持使用反斜线来转义正斜线。如果需要在正则表达式中使用正斜线，只需键入正斜线，而不要键入反斜线。

注释 从技术上说，AsyncOS for Web 使用 Flex 正则表达式分析器。

您可以在以下位置使用正则表达式：

- **访问策略的自定义 URL 类别**。当您创建要与访问策略组配合使用的自定义 URL 类别时，可以使用正则表达式指定与所输入模式匹配的多个 Web 服务器。
- **要阻止的自定义用户代理**。当您编辑访问策略组要阻止的应用时，可以使用正则表达式输入要阻止的特定用户代理。

注释 执行广泛字符匹配的正则表达式会消耗资源，并会影响系统性能。因此，应谨慎应用正则表达式。

相关主题

- 创建和编辑自定义 URL 类别，第 151 页

形成正则表达式

正则表达式是通常会在表达式中使用单词“matches”的规则。它们可应用于匹配特定 URL 目标或 Web 服务器。例如，以下正则表达式匹配包含“`blocksite.com`”的所有模式：

```
\.blocksite\.com
```

请思考以下正则表达式示例：

```
server[0-9]\.example\.com
```

在本例中，`server[0-9]` 与域 `example.com` 中的 `server0`、`server1`、`server2`、...、`server9` 匹配。

在下例中，正则表达式与 downloads 目录中扩展名为 `.exe`、`.zip` 和 `.bin` 的文件匹配。

```
/downloads/.*\.(exe|zip|bin)
```

注释 您必须用 ASCII 引号将包含空格或非字母数字字符的正则表达式引起来。

有关避免验证失败的指导原则

重要提示：返回内容超过 63 个字符的正则表达式会失败并产生无效输入错误。请确保构建不会返回超过 63 个字符的正则表达式。

请遵循以下指导原则来尽量减少验证失败：

- 尽可能使用文本表达式，而不是通配符和括号表达式。文本表达式基本上就是简单的文本，例如“`It' s as easy as ABC123`”。其发生验证失败的可能性小于使用“`It' s as easy as [A-C]{3}[1-3]{3}`”。后者表达式将导致创建非确定性有限自动机 (NFA) 条目，这可能会显著增加处理时间。

- 尽可能避免使用非转义点号。点号是一个特殊的正则表达式字符，它表示匹配除换行符外的任何字符。如果希望与实际的点匹配（例如“url.com”中的点），则使用“\”字符转义点号（例如“url\.com”）。转义的点号将按文本条目处理，因此不会引起问题。
- 对于在点号后返回超过63个字符的模式中的任何非转义点，模式匹配引擎会对其禁用，并发送一个关于该模式造成影响的警报，在纠正或替换该模式前，您会在每次更新后都会收到该警报。

  同样，尽可能使用更具体的匹配项，而不是非转义点号。例如，如果希望与后跟单个数字的URL 匹配，请使用“url[0-9]”，而不是“url.”。
- 在较长的正则表达式中的非转义点号特别可能引起故障，因此应尽可能避免。例如，“Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual”可能会导致失败。用文本“equal”代替“.qual”中的点号可以解决该问题。

  此外，在点号后将返回63个以上字符的模式中的非转义点号会被模式匹配引擎禁用。修正或替换相应模式。
- 不能使用“.*”开始或结束一个正则表达式。不能在用于匹配URL的正则表达式中使用“./”，也不能以圆号结束这样的表达式。
- 组合使用通配符和括号表达式可能会引发问题。尽可能避免使用组合。例如，“id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$”可能会导致失败，而“Gecko/20100101 Firefox/9\.0\.1\$”则不会。后一表达式不包括任何通配符或括号表达式，并且两个表达式仅使用已转义的点号。

  当无法避免使用通配符和括号表达式时，尽可能缩短表达式并降低其复杂性。例如，“[0-9a-z]{64}”可能会导致失败。将其更改为长度更短的表达式或不太复杂的表达式可能会解决此问题，例如“[0-9]{64}”或“[0-9a-z]{40}”。

如果发生失败，请尝试将上述这些规则应用于通配符（例如“*”、“+”和“.”）和括号表达式来解决问题。

注释 您可以使用 CLI 选项 advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex? 来启用或禁用默认的将正则表达式转换为小写以进行大小写匹配的功能。如果遇到大小写区分问题，请使用此选项。有关此选项的更多信息，请参阅网络安全设备CLI命令，第 457 页。

正则表达式字符表

元字符	说明
.	匹配除换行符 (0x0A) 以外的任何单个字符。例如，正则表达式r.t会匹配字符串 rat、rut、r t，但不会匹配 root。 在长模式中，请谨慎使用非转义点号，尤其是在较长模式的中间部分。有关详细信息，请参阅有关避免验证失败的指导原则，第 162 页。

元字符	说明
*	零次或多次匹配前面紧邻的字符。例如，正则表达式 .* 表示匹配任何字符串，并且 [0-9]* 匹配任何数字串。 请谨慎使用此元字符，尤其是在组合使用点号字符时。任何包含非转义点号且在点号后会返回 63 个以上字符的模式会被禁用。有关详细信息，请参阅有关避免验证失败的指导原则，第 162 页。
\	转义字符；表示将以下元字符作为普通字符进行处理。例如，\^用于匹配脱字符号字符 (^)，而不是行首。同样，表达式 \. 用于匹配实际的圆点，而不是任何单个字符。
^	匹配行首。例如，正则表达式 ^When in 匹配字符串“When in the course of human events”的开头，而不匹配字符串“What and when in the”。
$	匹配行或字符串的末尾。例如，b$\. 匹配以“b”结尾的任何行或字符串。
+	零次或多次匹配前面紧邻的字符或正则表达式。例如，正则表达式 9+ 匹配 9、99 和 999。
?	零次或一次匹配前面的模式元素。例如，colou?r 匹配“colour”和“color”，因为“u”可选。
( )	将左右括号之间的表达式作为整体进行处理，限制其他元字符的范围。例如，(abc)+ 表示零次或多次匹配字符串“abc”；例如，匹配“abcabcabc”或“abc123”，但不匹配“abab”或“ab123”。
|	逻辑或：匹配前面的模式或后面的模式。例如，(him|her) 匹配行“it belongs to him”和行“it belongs to her”，但不匹配行“it belongs to them”。
[ ]	匹配括号之间的任意一个字符。例如，正则表达式 r[aou]t 匹配“rat”、“rot”和“rut”，但不匹配“ret”。 字符的范围由开头的字符、连字符和结尾的字符指定。例如，模式 [0-9] 表示匹配任何数字。还可以指定多个范围。模式[A-Za-z]表示匹配任何大写或小写字母。要匹配除范围（即补充范围）中字符以外的任何字符，请在左括号后面使用脱字符号作为第一个字符。例如，表达式 [^269A-Z] 匹配除 2、6、9 和大写字母外的任何字符。
{ }	指定匹配之前模式的次数。 例如： D{1,3} 匹配字母 D 的一次到三次出现次数 匹配特定数量 {**n**} 或最小数量 {**n**,} 的前面模式的实例。例如，表达式 A[0-9]{3} 匹配“A”以及其后的三个数字。即，它匹配“A123”，但不匹配“A1234”。表达式 [0-9]{4,} 匹配任意序列的四个或以上数字。
“...”	按字母意思解释引号中包含的任意字符。

URL 类别说明

本部分列出思科网络使用控件的 URL 类别。表格中还包括可能显示在访问日志文件条目的 Web 信誉过滤和防恶意软件扫描部分的 URL 类别名称缩写。

注释 在访问日志中，思科网络使用控件的URL 类别缩写在每个缩写之前包含前缀“IW_”，这样“art”类别即变为“IW_art”。

URL 类别	缩写	代码	说明	示例 URL
成人	adlt	1006	主要面向成年人，但不一定包含色情内容。内容可能涉及成人俱乐部（脱衣舞俱乐部、换妻俱乐部、三陪服务、脱衣舞表演等）；有关性的一般信息（非色情性质）；生殖器穿刺；成人用品或成人贺卡；不涉及性暗示的有关健康或疾病的内容。	www.adultentertainmentexpo.com www.adultnetline.com
广告	adv	1027	通常会伴随网页显示横幅广告和弹窗广告的网站；其他提供通告内容的广告网站。与广告服务和销售相关的网站属于“商业和工业网站”类别。	www.adforce.com www.doubleclick.com
酒类	alc	1077	涉及以下内容的网站：以酒类为主题的快乐活动；啤酒和葡萄酒酿造、鸡尾酒调制方法；酒商、酒庄、葡萄园、酿酒厂、酒类经销商。酒瘾分类为“健康和营养”。酒吧和餐厅分类为“餐饮”。	www.samueladams.com www.whisky.com
艺术	art	1002	涉及以下内容的网站：画廊和画展；艺术家和艺术；摄影；文献和著作；表演艺术和剧场；音乐；芭蕾；博物馆；设计；建筑。与电影院和电视相关的网站属于“娱乐网站”类别。	www.moma.org www.nga.gov
占星	astr	1074	涉及以下内容的网站：占星术；星座占卜；算命；数字占卜；通灵；塔罗牌占卜。	www.astro.com www.astrology.com
拍卖	auct	1088	涉及以下内容的网站：网络和线下竞拍、拍卖行和分类广告。	www.craigslist.com www.ebay.com

URL 类别	缩写	代码	说明	示例 URL
商业和工业	busi	1019	涉及以下内容的网站：市场营销、商务、公司、业务实践、员工、人力资源、交通运输、薪酬、安全和风险投资；办公用品；工业设备（工艺设备）、机器和机械系统；加热设备、冷却设备；材料搬运设备；包装设备；制造业相关的固体物质运输、金属加工、建筑和建造；乘客运输；商业活动；工业设计；建设施工、建筑材料；运输和货运（货运服务、卡车运输、货运代理、卡车运输公司、货运和运输代理、快递服务、空车配运、运输跟踪、铁路运输、海运、货运专线服务、搬运和储存）。	www.freightcenter.com www.staples.com
聊天和即时消息	chat	1040	提供基于 Web 的即时消息和聊天室服务的网站。	www.icq.com www.meebo.com
欺诈和剽窃	plag	1051	助长抄袭，并出于剽窃目的销售书面著作（例如学期论文）的网站。	www.bestessays.com www.superiorpapers.com
虐童内容	cprn	1064	涉及全球违法儿童性侵内容的网站。	—
计算机安全	csec	1065	为公司和家庭用户提供安全产品和服务的网站。	www.computersecurity.com www.symantec.com
计算机和互联网	comp	1003	有关计算机和软件的信息，例如硬件、软件、软件支持；软件工程师、编程和网络信息；网站设计；常用 Web 和互联网；计算机科学；计算机图形和剪贴画。“免费软件和共享软件网站”单独分为一类。	www.xml.com www.w3.org
约会	date	1055	提供约会、网上交友、婚介服务的网站。	www.eharmony.com www.match.com
数字明信片	card	1082	支持发送数字明信片和电子贺卡的网站。	www.all-yours.net www.delivr.net
餐饮	food	1061	涉及以下内容的网站：餐饮设施；餐厅、酒吧、酒馆和休闲吧；酒店指南和评价。	www.hideawaybrewpub.com www.restaurantrow.com

URL 类别	缩写	代码	说明	示例 URL
动态和住宅	dyn	1091	通常表明用户尝试访问其家庭网络的宽带连接 IP 地址（例如远程访问家用计算机）。	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
教育	edu	1001	与教育相关的网站，内容可能涉及学校、学院、大学、教材和教学资源；技术和职业培训；在线培训；教育难题和教育政策；助学金；学校基金；标准和测试。	www.education.com www.greatschools.org
娱乐	ent	1093	涉及以下内容的网站：电影情节或讨论；音乐和乐队；电视；名人和粉丝网站；娱乐新闻；明星八卦；娱乐场所。独立于“艺术网站”类别。	www.eonline.com www.ew.com
极端	extr	1075	涉及以下内容的网站：具有性暴力或性犯罪性质的材料；暴力和暴力行为；品味低下的材料（通常是血腥暴力的图片，例如尸体解剖照片）；犯罪现场、犯罪和事故受害者的照片；极度淫秽的材料；冲击性网站。	www.car-accidents.com www.crime-scene-photos.com
时尚	fash	1076	涉及以下内容的网站：服装和时尚；发廊；化妆品；饰物；珠宝；香水；与人体改造相关的图片和文字；纹身和穿刺；模特经纪公司。与护肤产品相关的网站属于“健康和营养网站”类别。	www.fashion.net www.findabeautysalon.com
文件传输服务	fts	1071	以提供下载服务和托管文件共享服务为主要目的的文件传输服务网站。	www.rapidshare.com www.yousendit.com
规避过滤	filt	1025	推动并帮助实现无法检测的网络使用和匿名网络使用（包括 cgi、php 和 glype 匿名代理服务）的网站。	www.bypassschoolfilter.com www.filterbypass.com
金融	fnnc	1015	在性质上以金融为主的网站，内容可能涉及会计实务和会计人员、税务、税收、银行、保险、投资、国家经济、个人理财（包括所有类型的保险）、信用卡、退休规划和房地产规划、贷款、抵押等。与股票和股份相关的网站属于“在线交易网站”类别。	finance.yahoo.com www.bankofamerica.com

URL 类别	缩写	代码	说明	示例 URL
免费软件和共享软件	可用	1068	提供免费软件和共享软件下载服务的网站。	www.freewarehome.com www.shareware.com
赌博	gamb	1049	涉及以下内容的网站：赌场和网上赌博；庄家和赔率；赌博建议；具有赌博性质的竞速比赛；体育博彩；体育赌博；股票和股份点差交易服务。处理赌瘾的的网站属于“健康和营养网站”类别。国有彩票属于“彩票”类别。	www.888.com www.gambling.com
游戏	game	1007	涉及以下内容的网站：各种卡片游戏、桌上游戏、文字游戏和视频游戏；对战游戏；体育游戏；可下载的游戏；游戏评论；作弊码；计算机游戏和互联网游戏（例如角色扮演游戏）。	www.games.com www.shockwave.com
政府和法律	gov	1011	涉及以下内容的网站：政府网站；对外关系；与政府和选举相关的新闻和信息；与法律领域相关的信息（例如律师、律师事务所、法律著作、法律参考资料、法院、备审案件目录和法律协会）；立法及判决；民权问题；移民；专利和版权；与执法和执法系统相关的信息；犯罪报告、执法和犯罪统计；军事（例如军队、军事基地、军事组织）；反恐怖主义。	www.usa.gov www.law.com
黑客攻击	hack	1050	讨论如何绕过网站、软件和计算机安全保护的网站。	www.hackthissite.org www.gohacking.com
仇恨言论	hate	1016	煽动以下内容的网站：基于社会团体、肤色、宗教信仰、性取向、残疾、阶级、种族、民族、年龄、性别和性身份的仇恨、蔑视和歧视；种族主义；性别歧视；种族神学；厌世音乐；新纳粹组织；种族优越主义；否认大屠杀。	www.kkk.com www.nazi.org

URL 类别	缩写	代码	说明	示例 URL
健康和营养	hlth	1009	涉及以下内容的网站：卫生保健；疾病和残疾；医疗；医院；医生；医用药物；心理健康；精神病学；药物学；锻炼和健身；身体残疾；维生素和营养品；与性相关的健康知识（疾病和医疗）；与吸烟、饮酒、吸毒和赌博相关的健康知识（疾病和医疗）；与食物相关的一般知识；食物和饮料；烹饪和菜谱；食物与营养、健康、节食；烹饪方法（包括菜谱和烹饪网站）；替代疗法。	www.health.com www.webmd.com
幽默	lol	1079	与笑话、涂鸦、漫画和其他幽默内容相关的网站。与可能具有冒犯性的成人幽默相关的网站属于“成人网站”类别。	www.humor.com www.jokes.com
非法活动	ilac	1022	煽动犯罪的网站，内容可能涉及：盗窃、欺诈、非法接入电话网络；计算机病毒；恐怖主义、炸弹和无政府主义。也包括描述谋杀和自杀以及介绍谋杀和自杀方法的网站。	www.ekran.no www.thedisease.net
非法下载	ildl	1084	提供以下下载内容的网站：软件或其他材料、序列号、密钥生成器，以及违反版权协议绕过软件保护的工具。与 Torrent 下载相关的网站属于“对等文件传输网站”类别。	www.keygenguru.com www.zcrack.com
违禁药物	drug	1047	此类网站提供有关娱乐性毒品、吸毒工具，以及毒品购买和制造的信息。	www.cocaine.org www.hightimes.com
基础设施和内容交付网络	infr	1018	内容交付基础设施和涉及动态生成内容的网站；由于安全原因而无法更具体分类的网站，或者难以分类的网站。	www.akamai.net www.webstat.net
互联网电话服务	voip	1067	提供基于互联网的电话服务的网站。	www.evaphone.com www.skype.com
求职	作业	1004	涉及以下内容的网站：职业建议；编写简历和应对面试的技巧；就业服务；职位数据库；固定职业和临时职业介绍所；招聘网站。	www.careerbuilder.com www.monster.com

URL 类别	缩写	代码	说明	示例 URL
女用内衣和泳装	ling	1031	与贴身衣物和泳衣（特别是有模特穿着）相关的网站。	www.swimsuits.com www.victoriassecret.com
彩票	lotr	1034	与奖券、竞赛和国家赞助的彩票相关的网站。	www.calottery.com www.flalottery.com
手机	cell	1070	与短信服务 (SMS) 以及铃声和手机下载相关的网站。移动运营商网站属于“商业和工业网站”类别。	www.cbfsms.com www.zedge.net
自然	natr	1013	涉及以下内容的网站：自然资源；生态学和环境保护；森林；原野；植物；花；森林保护；森林、原野和林业实践；森林管理（重新造林、森林保护、保持、砍伐、森林健康状况、抚育间伐和计划烧除）；农业实践（农学、园艺、园林、景观、绿化、除草、灌溉、修剪和收割）；污染问题（空气质量、危险废弃物、污染防治、回收利用、废弃物管理、水质和环境清理行业）；动物、宠物、家畜和动物学；生物学；植物学。	www.enature.com www.nature.org
新闻	新闻	1058	涉及以下内容的网站：新闻；头条新闻；报纸；电视台；杂志；天气；滑雪条件。	www.cnn.com news.bbc.co.uk
非政府组织	ngo	1087	非政府组织（如俱乐部、游说团、社区、非营利组织和工会）的网站。	www.panda.org www.unions.org
非色情裸体	nsn	1060	涉及以下内容的网站：裸体主义和裸体行为；自然崇拜；裸体主义者联盟；裸体艺术。	www.artenuda.com www.naturistsociety.com
在线社区	comm	1024	涉及以下内容的网站：有亲密关系的群体；有特殊爱好的群体；网络新闻组；网络论坛。不包括“职业社交网站”类别或“社交网络”类别的网站。	www.igda.org www.ieee.org
在线存储和备份	osb	1066	出于备份、共享和托管目的提供离线和对等存储的网站。	www.adrive.com www.dropbox.com

URL 类别	缩写	代码	说明	示例 URL
在线交易	trad	1028	涉及以下内容的网站：网上证券交易；与股市、股票、债券、共同资金、经纪人、股票分析和股评、股市行情、股票走势、IPO 和股票分割相关的信息。也包括支持用户在线交易股票的网站。提供股票和股份点差交易服务的网站属于“赌博”网站类别。与其他金融服务相关的网站属于“金融”网站类别。	www.tdameritrade.com www.scottrade.com
企业邮件	pem	1085	用于访问企业邮件的网站（通常通过 Outlook Web Access 访问）。	—
寄放域	park	1092	通过使用广告网络付费列表的域，对流量进行收费的网站；或者由希望出售域名以谋取利润的“投机者”拥有的网站。此类网站也包括含有付费广告链接的虚假搜索网站。	www.domainzaar.com www.parked.com
对等文件传输	p2p	1056	对等文件请求网站。此类网站不会对文件传输进行跟踪。	www.bittorrent.com www.limewire.com
个人网站	pers	1081	与个人相关或由个人运营的网站；个人主页服务器；含有个人内容的网站；没有特定主题的个人博客。	www.karymullis.com www.stallman.org
照片搜索和图像	img	1090	为存储和搜索图片、照片和剪贴画提供便利的网站。	www.flickr.com www.photobucket.com
政治	pol	1083	涉及以下内容的网站：政治家；政党；与政治、选举，民主和投票相关的新闻和信息。	www.politics.com www.thisnation.com
色情	porn	1054	含有露骨的色情文字或内容的网站。内容可能涉及露骨的动画和卡通；一般的露骨内容；其他色情材料；毫无隐晦的聊天室；情爱模拟器；脱衣扑克游戏；成人电影；猥亵的艺术；基于 Web 的露骨邮件。	www.redtube.com www.youporn.com
职业社交网络	pnet	1089	以事业或职业发展为目的的社交网络。另请参阅“社交网络”。	www.linkedin.com www.europeanpwn.net

URL 类别	缩写	代码	说明	示例 URL
房地产	rest	1045	为帮助搜索以下内容提供信息的网站：房地产；办公室和商业场所；房地产列表（如出租房屋、公寓和住宅）；住宅建筑。	www.realtor.com www.zillow.com
参考	ref	1017	涉及以下内容的网站：城市和州指南；地图、时间；参考源；词典；资料库。	www.wikipedia.org www.yellowpages.com
宗教	版本	1086	涉及宗教内容和宗教信息的网站；宗教社区。	www.religionfacts.com www.religioustolerance.org
以及 B2B	saas	1080	提供在线业务服务以及支持在线会议的网络门户。	www.netsuite.com www.salesforce.com
儿童安全	kids	1057	专门面向少年儿童（尤其是经过批准）的网站。	kids.discovery.com www.nickjr.com
科技	sci	1012	与科学技术相关的网站，内容可能涉及航空航天、电子、工程、数学和其他类似学科；太空探索；气象学；地理；环境；能源（化石能源、核能、可再生能源）；通信（电话、电信）。	www.physorg.com www.science.gov
搜索引擎和门户	srch	1020	搜索引擎以及其他访问互联网信息的入口点。	www.bing.com www.google.com
性教育	sxed	1052	如实介绍性、性健康、避孕和怀孕知识的网站。	www.avert.org www.scarleteen.com
购物	shop	1005	涉及以下内容的网站：以物换物；网络购物；优惠券和赠品；常规办公用品；在线目录；在线商城。	www.amazon.com www.shopping.com
社交网络	snet	1069	社交网络.另请参阅“专业网络网站”。	www.facebook.com www.twitter.com
社会科学	socs	1014	涉及以下内容的网站：与社会相关的科学和历史；考古学；人类学；文化研究；历史；语言学；地理学；哲学；心理学；女性研究。	www.archaeology.org www.anthropology.net

URL 类别	缩写	代码	说明	示例 URL
社会文化	scty	1010	涉及以下内容的网站：家族和关系；种族；社会组织；家谱；敬老；儿童看护。	www.childcare.gov www.familysearch.org
软件更新	swup	1053	托管软件包更新的网站。	www.softwarepatch.com www.versiontracker.com
体育和娱乐	sprt	1008	涉及以下内容的网站：各种体育运动（职业和业余）；娱乐活动；钓鱼；梦幻竞技；公园；游乐园；水上公园；主题公园；动物园和水族馆；SPA。	www.espn.com www.recreation.gov
流式音频	aud	1073	提供实时音频流内容（包括互联网电台和音频源）的网站。	www.live-radio.net www.shoutcast.com
视频流	vid	1072	提供实时流式视频（包括互联网电视、网播和共享视频）的网站。	www.hulu.com www.youtube.com
烟草	tob	1078	烟草宣传网站；烟草制造商网站；有关烟斗和吸烟产品（不是用于非法吸毒目的）的网站。与烟瘾相关的网站属于“健康和营养网站”类别。	www.bat.com www.tobacco.org
交通	trns	1044	涉及以下内容的网站：个人交通；有关汽车和摩托车的信息；全新和二手汽车与摩托车的商店；汽车俱乐部；船只、飞机、房车 (RV) 和其他类似物品。注：汽车和摩托车比赛属于“体育和娱乐网站”类别。	www.cars.com www.motorcycles.com
旅行	trvl	1046	涉及以下内容的网站：商务和个人旅行；旅游信息；旅游资源；旅行社；度假套装；游轮航线；住宿和宿泊；旅行交通；航班预订；机票；租车；度假屋。	www.expedia.com www.lonelyplanet.com
未分类	—	—	未包含在思科数据库中的网站将被分类为“未分类网站”，以便于报告。此类网站可能包括输入错误的URL。	—

URL 类别	缩写	代码	说明	示例 URL
武器	weap	1036	此类网站提供有关常规武器购买或使用的信息，例如枪支贩卖商、枪支拍卖、枪支分类广告、枪支配件、枪展和枪支培训；有关枪的一般信息。此类网站也可能包括其他武器和图片搜索网站。政府军事网站属于“政府和法律网站”类别。	www.coldsteel.com www.gunbroker.com
Web 托管	whst	1037	提供 Web 托管和带宽服务的网站。	www.bluehost.com www.godaddy.com
网页翻译	tran	1063	在不同语言之间翻译网页的网站。	babelfish.yahoo.com translate.google.com
基于 Web 的邮件	mail	1038	提供基于 Web 的公共邮件服务的网站。为个人访问其公司或组织的邮件服务提供支持的网站属于“组织邮件网站”类别。	mail.yahoo.com www.hotmail.com

相关主题

- 管理 URL 类别集更新， 第 140 页
- 报告未分类和误分类的 URL， 第 139 页

第 11 章

创建策略以控制互联网请求

本章包含以下部分：

策略概述：控制拦截的互联网请求

当用户创建 Web 请求时，配置的网络安全设备会拦截该请求并管理该请求传输到目的地的过程，即访问特定网站、邮件或甚至访问在线应用。在配置网络安全设备时，系统会创建策略以定义用户提出的请求的条件和操作。

策略是网络安全设备用来识别和控制 Web 请求的方法。当客户端向服务器发送 Web 请求时，Web 代理接收该请求，对其进行评估，然后确定其所属的策略。在策略中定义的操作之后将应用于该请求。

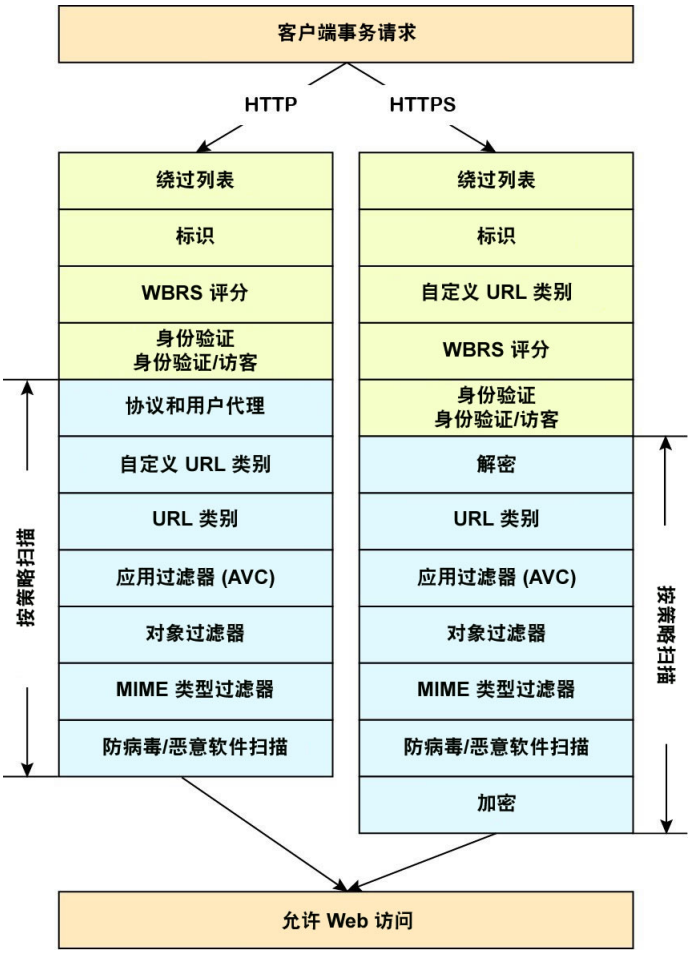
网络安全设备使用多个策略类型管理 Web 请求的不同方面。策略类型可能独自管理全部事务，也可能将事务传递到其他策略类型，以进行其他处理。策略类型可以按其执行的功能分组，例如访问、路由或安全。

AsyncOS 先根据策略评估事务，再评估外部依赖关系，以避免来自设备的不必要外部通信。例如，如果某事务因阻止未分类 URL 的策略而被阻止，则该事务不会因 DNS 错误而失败。

拦截的 HTTP/HTTPS 请求的处理

下图显示了设备处理拦截的 Web 请求的流程。

图 *3: HTTP/HTTPS* 事务流



另请参阅以下用于说明各种事务处理流的流程图：

- 图 1: 标识配置文件和身份验证处理 - 无代理和基于 IP 的代理， 第 120 页
- 图 2: 标识配置文件和身份验证处理 - 基于 Cookie 的代理， 第 121 页
- 图 4: 访问策略的策略组事务流， 第 180 页
- 图 6: 针对解密策略的策略组事务流， 第 201 页
- 图 7: 应用解密策略操作， 第 204 页

通过策略管理 Web 请求的任务概述

步骤	通过策略管理 Web 请求的任务列表	相关主题和程序的链接
1	设置身份验证领域并对其排序	身份验证领域， 第 86 页

步骤	通过策略管理 Web 请求的任务列表	相关主题和程序的链接
2	（对于上游代理）创建一个代理组	为上游代理创建代理组，第 23 页
2	（可选）创建自定义客户端应用	客户端应用，第 189 页
3	（可选）创建自定义 URL 类别	创建和编辑自定义 URL 类别，第 151 页
4	创建标识配置文件	用户和客户端软件分类，第 115 页
5	（可选）创建时间范围以按每天的时间限制访问	时间范围和配额，第 191 页
6	创建策略并对其进行排序	• 创建策略，第 181 页 • 策略顺序，第 180 页

通过策略管理 Web 请求的最佳实践

如果您要使用 Active Directory 用户对象管理 Web 请求，请勿使用主要组作为条件。Active Directory 用户对象不包含主要组。

策略

- 策略类型，第 177 页
- 策略顺序，第 180 页
- 创建策略，第 181 页

策略类型

策略类型	请求类型	说明	任务链接
访问	• HTTP • 已解密 HTTPS • FTP	阻止、允许或重定向入站 HTTP、FTP 和已解密 HTTPS 流量。 如果 HTTPS 代理处于禁用状态，访问策略还管理入站加密 HTTPS 流量。	创建策略，第 181 页
SOCKS	• SOCKS	允许或阻止 SOCKS 通信请求。	创建策略，第 181 页

策略类型	请求类型	说明	任务链接
应用身份验证	• 应用	允许或拒绝对软件即服务 (SaaS) 应用的访问。 使用单点登录对用户进行身份验证以及通过允许快速禁用对应用的访问来提高安全性。 要使用策略的单点登录功能，您必须将网络安全设备配置为身份提供程序并为 SaaS 上传或生成证书和密钥。	创建 SaaS 应用身份验证策略，第 126 页
加密 HTTPS 管理	• HTTPS	解密、通过或丢弃 HTTPS 连接。 AsyncOS 将解密流量传递到访问策略，以供进一步处理。	创建策略，第 181 页
数据安全	• HTTP • 已解密 HTTPS • FTP	管理到 Web 的数据上传。数据安全策略根据出站流量的目标和内容进行扫描，确保该流量符合公司数据上传规则。外部 DLP 策略将出站流量重定向到外部服务器以进行扫描，数据安全策略与之不同，其使用网络安全设备扫描和评估流量。	创建策略，第 181 页
外部 DLP（防数据丢失）	• HTTP • 已解密 HTTPS • FTP	将出站流量发送到运行第三方 DLP 系统的服务器，该服务器会对流量进行扫描，确保其符合公司数据上传规则。数据安全策略也管理数据上传，外部 DLP 策略与之不同，其让扫描工作在网络安全设备之外进行，从而释放了设备上的资源并利用第三方软件提供的任何附加功能。	创建策略，第 181 页
出站恶意软件扫描	• HTTP • 已解密 HTTPS • FTP	阻止、监控或允许可能包含恶意数据的数据上传请求。 防止网络上已存在的恶意软件传输到外部网络。	创建策略，第 181 页

策略类型	请求类型	说明	任务链接
路由	• HTTP • HTTPS • FTP	通过上游代理定向 Web 流量或者将其定向到目标服务器。您可能想要通过上游代理重定向流量以保留现有网络设计，减轻网络安全设备的处理负担，或利用第三方代理系统提供的附加功能。 如果多个上游代理可用，则网络安全设备可以使用负载均衡技术向它们分配数据。	创建策略，第 181 页

每个策略类型使用一个策略表来存储和管理其策略。每个策略表具有一个预定义全局策略，用于维护策略类型的默认操作。此外，系统会根据需要创建用户定义的策略并将其添加到策略表。策略按其在策略表中列出的顺序进行处理。

各个策略定义其管理的用户请求类型以及它们对这些请求执行的操作。每个策略定义有两个主要部分：

- **标识配置文件和用户** – 标识配置文件用于策略成员身份条件，并且尤为重要，因为它们包含许多用于标识 Web 事务的选项。它们还与策略共享许多属性。
- **高级 (Advanced)** - 用于识别策略适用的用户的条件。可以在策略中指定一个或多个条件，必须匹配所有条件才算满足条件。
  - **协议 (Protocols)** - 允许在各种网络设备之间传输数据，例如 http、https、ftp 等。
  - **代理端口 (Proxy Ports)** - 请求用于访问 Web 代理的编号端口。
  - **子网 (Subnets)** - 联网设备的逻辑分组（例如地理位置或局域网 [LAN]），这是请求的发出位置。
  - **时间范围 (Time Range)** - 可在策略中创建时间范围，用于根据发起请求的时间或日期识别操作或将操作应用到 Web 请求。时间范围可以作为单个单元来创建。
  - **URL 类别 (URL Categories)** - URL 类别是网站的预定义或自定义类别，例如新闻、商业、社交媒体等。这些类别可用于识别操作或将操作应用到 Web 请求。
  - **用户代理 (User Agents)** – 这些是用于发出请求的客户端应用程序（如更新程序和 Web 浏览器）。您可以根据用户代理定义策略条件，并可以根据用户代理指定控制设置。您还可以豁免用户代理进行身份验证，这对于无法提示输入凭证的应用非常有用。您可以定义自定义用户代理，但无法将这些定义重新用于其他策略。

注释 定义多个成员身份条件时，客户端请求必须满足所有条件才能与策略相匹配。

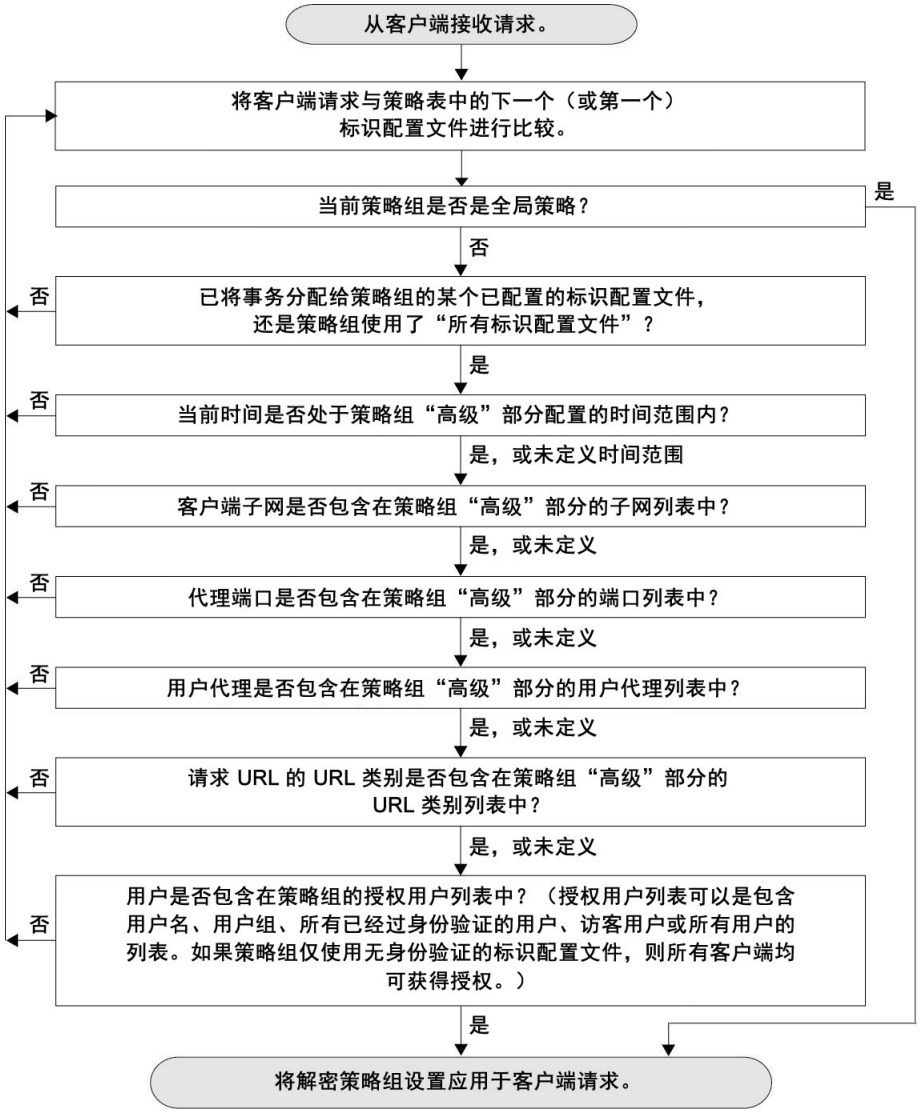
策略顺序

策略在策略表中列出的顺序决定了它们应用到 Web 请求的优先级。系统将会针对策略（从表最上面的策略开始，到第一个匹配的策略结束）对 Web 请求进行检查。在表格中找到匹配策略后，不会处理之后的任何策略。

如果没有用户定义的策略与 Web 请求匹配，则会应用该策略类型的全局策略。全局策略通常位于策略表最后面的位置，并且无法重新排序。

下图描述了通过访问策略表的客户端请求流。

图 *4:* 访问策略的策略组事务流



创建策略

开始之前

- 启用相应的代理：
  - Web 代理（针对 HTTP、已解密 HTTPS 和 FTP）
  - HTTPS 代理
  - SOCKS 代理
- 创建关联的标识配置文件。
- 了解策略顺序，第 180 页。
- （仅限加密 HTTPS）上传或生成证书和密钥。
- （仅限数据安全）启用思科数据安全过滤器设置。
- （仅限外部 DLP）定义外部 DLP 服务器。
- （仅限路由）定义网络安全设备上的关联上游代理。
- （可选）创建关联的客户端应用。
- （可选）创建关联的时间范围。请参阅时间范围和配额，第 191 页。
- （可选）创建关联的 URL 类别。请参阅创建和编辑自定义 URL 类别，第 151 页。

步骤 1 在**策略设置 (Policy Settings)** 部分中，使用**启用身份 (Enable Identity)** 复选框启用此策略，或者快速禁用而不将其删除。

步骤 2 指定唯一的策略**名称 (Name)**。

步骤 3 **说明 (Description)** 为可选项。

步骤 4 从“在上方插入”(Insert Above) 下拉列表中，选择此策略要在表中显示的位置。

注释 对策略进行排列，从表的顶部到底端按最严格到最不严格的顺序排列。有关详细信息，请参阅策略顺序，第 180 页。

步骤 5 在**策略成员定义 (Policy Member Definition)** 部分中，指定用户和组成员身份的定义方式：从标识配置文件和用户列表中，选择以下项之一：

- **所有标识配置文件 (All Identification Profiles)** – 此策略将应用于所有现有配置文件。您还必须至少定义一个**高级 (Advanced)** 选项。
- **选择一个或多个标识配置文件 (Select One or More Identification Profiles)** – 用于指定显示的各个标识配置文件的表，每行一个配置文件成员身份定义。

步骤 6 如果选择**所有标识配置文件 (All Identification Profile)**：

a) 通过选择以下选项之一指定此策略要应用到的授权用户和组：

- **所有经过身份验证的用户 (All Authenticated Users)** - 通过身份验证或透明标识识别的所有用户。
- **选定的组和用户** - 使用指定的用户和组。

  要添加或编辑指定的 ISE 安全组标签 (SGT) 和指定的用户，请点击相应标签后面的链接。例如，点击当前指定的用户的列表以编辑该列表。有关详细信息，请参阅添加和编辑策略的安全组标记，第 183 页。

- **访客 (Guests)** - 以访客身份连接的用户和那些身份验证失败的用户。
- **所有用户 (All Users)** - 所有客户，不论是否经过身份验证。如果选择此选项，还必须至少提供一个**高级 (Advanced)** 选项。

步骤 7 如果您选择**选择一个或多个标识配置文件 (Select One or More Identification Profiles)**，则系统会显示配置文件选择表。

a) 从“标识配置文件”(Identification Profiles) 列的“选择标识配置文件”(Select Identification Profile) 下拉列表中选择一个标识配置文件。

b) 指定此策略应用到的授权用户和组：

- **所有经过身份验证的用户 (All Authenticated Users)** - 通过身份验证或透明标识识别的所有用户。
- **选定的组和用户** - 使用指定的用户和组。

  要添加或编辑指定的 ISE 安全组标签 (SGT) 和指定的用户，请点击相应标签后面的链接。例如，点击当前指定的用户的列表以编辑该列表。有关详细信息，请参阅添加和编辑策略的安全组标记，第 183 页。

- **访客 (Guests)** - 以访客身份连接的用户和那些身份验证失败的用户。

c) 要向配置文件选择表中添加一行，请点击**添加标识配置文件 (Add Identification Profile)**。要删除行，请点击该行中的垃圾桶图标。

根据需要重复步骤 (a) 至 (c)，添加所有所需的标识配置文件。

步骤 8 展开**高级 (Advanced)** 部分定义其他组成员身份条件。（根据**策略成员定义 (Policy Member Definition)** 部分中的选择，该步骤可能为可选。此外，根据您配置的策略类型，以下某些选项将不可用。）.

高级选项	说明
协议 (Protocols)	选择此策略将应用到的协议。**所有其他 (All others)** 表示未选择的任何协议。如果相关联的标识配置文件应用于特定协议，此策略将应用于这些相同的协议
代理端口 (Proxy Ports)	将此策略仅应用于使用特定端口的流量以访问 Web 代理。输入一个或多个端口号，用逗号分隔多个端口。 对于显式转发连接，此代理端口为浏览器中配置的端口。 对于透明连接，此代理端口与目标端口为同一端口。 **注释** 如果关联的标识配置文件仅应用于特定的代理端口，则不能在此输入代理端口。
子网 (Subnets)	仅将此策略应用于特定子网上的流量。选择**指定子网 (Specify subnets)** 并输入特定子网，用逗号分隔。 如果不想要按子网进行其他过滤，请保持选中**使用选定身份的子网 (Use subnets from selected Identities)**。 **注释** 如果关联身份应用于特定子网，则您可以进一步限制将此策略应用至身份应用到的地址子网。

高级选项	说明
时间范围（Time Range）	您可以对策略成员身份应用时间范围： • 时间范围 (Time Range) - 选择先前定义的时间范围（时间范围和配额，第 191 页）。 • 匹配时间范围 (Match Time Range) - 使用此选项可指示包含还是排除此时间范围。换言之，无论是仅在指定范围内匹配，还是在除了指定范围中的时间以外的所有时间匹配。
URL 类别 (URL Categories)	您可以按特定目标 (URL) 以及 URL 类别来限制策略成员身份。选择所需的所有自定义和预定义类别。有关自定义类别的信息，请参阅创建和编辑自定义 URL 类别，第 151 页。

用户代理 (User Agents)	作为此策略成员身份定义的一部分，您可以选择特定用户代理，并使用正则表达式定义自定义代理。
	• **通用用户代理 (Common User Agents)**
	  • **浏览器 (Browsers)** - 展开此部分以选择各种网络浏览器。
	  • **其他 (Others)** - 展开此部分以选择特定的非浏览器代理，如应用更新程序。
	• **自定义用户代理 (Custom User Agents)** - 您可以输入一个或多个正则表达式（每行一个），以定义自定义用户代理。
	• **匹配用户代理 (Match User Agents)** - 使用此选项表示这些用户代理规范是包含还是不包含的。换言之，成员资格定义仅包括选定的用户代理，还是专门排除了选定的用户代理。

添加和编辑策略的安全组标记

要更改分配给策略中特定标识配置文件的安全组标记 (SGT) 列表，请点击“添加/编辑策略”(Add/Edit Policy) 页面上“选定组和用户”(Selected Groups and Users) 列表中 ISE 安全组标记标签后面的链接。（请参阅创建策略，第 181 页。）此链接是“没有输入任何标记”或者是当前已分配标记的列表。此链接将打开“添加/编辑安全组标记”(Add/Edit Secure Group Tags) 页面。

当前分配给此策略的所有 SGT 均会在“授权安全组标记”(Authorized Secure Group Tags) 部分中列出。互联 ISE 服务器中可用的所有 SGT 均在“安全组标记搜索”(Secure Group Tag Search) 部分中列出。

步骤 1 要将一个或多个 SGT 添加到“授权安全组标记”(Authorized Secure Group Tags) 列表，请在“安全组标记搜索”(Secure Group Tag Search) 部分中选择所需的条目，然后点击**添加 (Add)**。

SGT 已添加，以绿色突出显示。要在可用安全组标记列表中快速找到特定标记，请在**搜索 (Search)** 字段中输入文本字符串。

步骤 2 要从“授权安全组标记”(Authorized Secure Group Tags) 列表中删除一个或多个 SGT，请选择那些条目，然后点击**删除 (Delete)**。

步骤 3 点击“完成”(Done) 返回“添加/编辑组”(Add/Edit Group) 页面。

下一步做什么

相关主题

- 时间范围和配额，第 191 页
- 在策略中使用客户端应用，第 190 页

策略配置

策略表中的每一行表示一个策略定义，每一列显示当前包含转到策略元素配置页的链接。

注释 对于以下策略配置组件，您只能指定采用“URL 过滤”(URL Filtering) 的“警告”(Warn) 选项。

选项	说明
协议和用户代理 (Protocols and User Agents)	用于控制对协议的访问策略并配置对特定客户端应用（如即时消息客户端、Web 浏览器和网络电话服务）的阻止。您还可以将设备配置为在特定端口上传递 HTTP CONNECT 请求。当隧道传输启用后，设备将通过指定端口传递 HTTP 流量，不对其进行评估。
URL 过滤 (URL Filtering)	通过 AsyncOS for Web，您可以配置设备如何基于特定 HTTP 或 HTTPS 请求的 URL 类别来处理事务。通过预定义的类别列表，您可以选择阻止、监控、警告或设置基于配额或基于时间的过滤器。 您可以创建自定义 URL 类别，然后选择阻止、重定向、允许、监控、警告或应用自定义类别中面向网站的基于配额或时间的过滤器。有关创建自定义 URL 类别的信息，请参阅创建和编辑自定义 URL 类别，第 151 页。 此外，您可以添加对于阻止嵌入或引用内容的行为的例外情况。
应用 (Applications)	应用可视性与可控性引擎（AVC 引擎）是一个检查 Web 流量以更深入了解和控制用于应用的 Web 流量的可接受使用策略组件。设备允许将 Web 代理配置为按应用类型以及各个应用来阻止或允许应用。您还可以将控制应用于特定应用行为，例如特定应用内的文件传输。有关配置信息，请参阅管理对 Web 应用的访问，第 253 页。
对象 (Objects)	通过这些选项，您可以将 Web 代理配置为基于文件特征（例如文件大小、文件类型以及 MIME 类型）阻止文件。通常，对象是可以单独选择、上传、下载和操作的任意项目。请参阅访问策略：阻止对象，第 185 页了解有关指定受阻对象的信息，

选项	说明
防恶意软件和信誉 (Anti-Malware and Reputation)	Web 信誉过滤器允许向 URL 分配基于 Web 的信誉分数，以确定其包含基于 URL 的恶意软件的可能性。防恶意软件扫描可识别并阻止基于 Web 的恶意软件威胁。高级恶意软件防护可识别已下载文件中的恶意软件。 防恶意软件和信誉策略继承每个组件对应的全局设置。在**安全服务 (Security Services)** > **防恶意软件和信誉 (Anti-Malware and Reputation)** 内，可以自定义恶意软件类别以基于恶意软件扫描判定进行监控或阻止，并且可以自定义 Web 信誉分数阈值。可以进一步在策略中自定义恶意软件类别。此外，还有文件信誉和分析服务的全局设置。 有关详细信息，请参阅访问策略中的防恶意软件和信誉设置，第 227 页和配置文件信誉和分析功能，第 237 页。

访问策略：阻止对象

可以使用“访问策略: 对象”(Access Policies: Objects) 页面上的选项来基于文件特征（如文件大小、文件类型和 MIME 类型）阻止文件下载。通常，对象是可以单独选择、上传、下载和操作的任意项目。

可以指定由每个访问策略和全局策略阻止的对象类型数。这些对象类型包括存档、文档类型、可执行代码、网页内容等。

步骤 1 在“访问策略”(Access Policies) 页面（**网络安全管理器 (Web Security Manager)** > **访问策略 (Access Policies)**）中，代表要编辑的策略的行的**对象 (Objects)** 列中点击相应链接。

步骤 2 为此访问策略选择所需的对象阻止类型：

- **使用全局策略对象阻止设置 (Use Global Policy Objects Blocking Settings)** – 此策略使用为全局策略定义的对象阻止设置；这些设置以只读模式显示。编辑全局策略的设置以更改它们。
- **定义自定义对象阻止设置 (Define Custom Objects Blocking Settings)** – 您可以编辑此策略的所有对象阻止设置。
- **禁用此策略的对象阻止 (Disable Object Blocking for this Policy)** – 为此策略禁用对象阻止；不显示对象阻止选项。

步骤 3 如果在上一步中选择了**定义自定义对象阻止设置 (Define Custom Objects Blocking Settings)**，请根据需要在“访问策略: 对象”(Access Policies: Objects) 页面中选择和取消选择对象阻止选项。

对象大小	可以基于阻止对象的下载大小来阻止它们： • **HTTP/HTTPS 最大下载大小 (HTTP/HTTPS Max Download Size)** – 提供 HTTP/HTTPS 下载的最大对象大小（大于此大小的对象将被阻止），或者指示对于通过 HTTP/HTTPS 下载的对象没有最大大小。 • **FTP 最大下载大小 (FTP Max Download Size)** – 提供 FTP 下载的最大对象大小（大于此大小的对象将被阻止），或者指示对于通过 FTP下载的对象没有最大大小。
阻止对象类型	
存档 (Archives)	展开此部分可选择要阻止的存档文件的类型。此列表包括诸如 ARC、BinHex 和 StuffIt 等存档类型。
可检查的存档 (Inspectable Archives)	展开此部分可选择是**允许 (Allow)**、**阻止 (Block)** 还是**检查 (Inspect)** 特定类型的可检查存档文件。可检查存档是存档或压缩文件，WSA 可以解压这些文件以检查包含的每个文件，以便应用文件类型阻止策略。可检查存档列表包括诸如 7zip、Microsoft CAB、RAR 和 TAR 等存档类型。 存档检测有以下要点： • 只有标记为**检查 (Inspect)** 的存档类型才可解压和检查。 • 一次只能检查一个存档，不可检查其他并发可检查存档。 • 如果已检查的存档包含由当前策略分配了阻止操作的文件类型，则整个存档都将被阻止，而不管它是否包含任何允许的文件类型。 • 包含不受支持的存档类型的已检查存档将被标记为“不可扫描”(unscannable)。如果它包含被阻止的存档类型，则将被阻止。 • 受密码保护和加密的存档不受支持，并将被标记为“不可扫描”(unscannable)。 • 不完整或损坏的可检查存档将标记为“不可扫描”(unscannable)。 • 为**防恶意软件和信誉 (Anti-Malware and Reputation)** 指定的 **DSV 引擎对象扫描限制 (DVS Engine Object Scanning Limits)** 值还适用于可检查存档的大小；超过此大小的对象将被标记为“不可扫描”(unscannable)。有关此对象大小限制的信息，请参阅启用防恶意软件和信誉过滤器，第 225 页。 • 标记为“不可扫描”(unscannable) 的可检查存档可以被全部“阻止”(Blocked) 或全部“允许”(Allowed)。 有关配置存档检测的信息，请参阅存档检查设置，第 187 页。
文档类型 (Document Types)	展开此部分可选择要阻止的文本文档的类型。此列表包括文档类型，如 FrameMaker、Microsoft Office 和 PDF。
可执行代码 (Executable Code)	展开此部分可选择要阻止的可执行代码的类型。该列表包括 Java 小程序、UNIX 可执行文件和 Windows 可执行文件。

安装程序 (Installers)	要阻止的安装程序的类型；该列表包括 UNIX/LINUX 包。
媒体 (Media)	要阻止的媒体文件的类型。该列表包括音频、视频和照片图像处理格式(TIFF/PSD)。
P2P 元文件 (P2P Metafiles)	此列表包括 BitTorrent 链接 (`.torrent`)。
网页内容 (Web Page Content)	此列表包括 Flash 和图像。
其他 (Miscellaneous)	此列表包含日历数据。
自定义 MIME 类型	您可以根据 MIME 类型定义要阻止的其他对象/文件。 在**阻止自定义 MIME 类型 (Block Custom MIME Types)** 字段中输入一个或多个 MIME 类型，每行一个。

步骤 4 点击**提交 (Submit)**。

存档检查设置

您可以允许、阻止或检查单个访问策略的特定类型的可检查存档。可检查存档是 WSA 可以增加以检查每个所包含文件的存档或压缩文件，用以应用文件类型阻止策略。有关为单个访问策略配置存档检查的详细信息，请参阅访问策略：阻止对象 ，第 185 页。

注释 在存档检查期间，嵌套的对象被写入磁盘以进行检查。文件检查期间在任何给定时间可以占用的磁盘空间量为 1 GB。超过此最大磁盘使用大小的任何存档文件都将被标记为不可扫描。

“WSA 的可接受使用控制”(WSA’s Acceptable Use Controls) 页面提供系统范围的可检查存档设置；即，每当在访问策略中启用这些设置后，都将应用这些设置以将提取和检查存档。

步骤 1 选择**安全服务 (Security Services)** > **可接受的使用控制 (Acceptable Use Controls)**。

步骤 2 点击**编辑存档设置 (Edit Archives Settings)** 按钮。

步骤 3 根据需要编辑可检查存档设置。

- **最大封装的存档提取 (Maximum Encapsulated Archive Extractions)** - 要提取和检查的“封装”存档的最大数。即，要检查一个包含其他可检查存档的存档的最大深度。封装存档是指包含在另一存档文件中的存档。此值可以为零到五；深度计数从具有第一个嵌套文件的文件开始。

  外部存档视为文件零。如果存档嵌套的文件超出了此最大嵌套值，则存档标记为不可扫描。请注意，这会影响性能。

- **阻止不可检查的存档 (Block Uninspectable Archives)** - 如果选中此项，则 WSA 将会阻止无法增加和检查的存档。

步骤 4 提交 **(Submit)** 并确认更改 **(Commit Changes)**。

阻止、允许或重定向事务请求

Web 代理基于您为事务请求组创建的策略控制 Web 流量。

- **允许**。Web 代理允许连接，无需中断。允许的连接可能尚未由 DVS 引擎进行扫描。
- **阻止**。Web 代理不允许连接，而是显示最终用户通知页面，以说明阻止的原因。
- **重定向**。Web 代理不允许与最初请求的目标服务器进行连接，而是连接到其他指定的 URL，请参阅重定向访问策略中的流量，第 158 页。

注释 之前的操作是 Web 代理对客户端请求采取的最终操作。您可以为访问策略配置的监控操作不是最终操作。

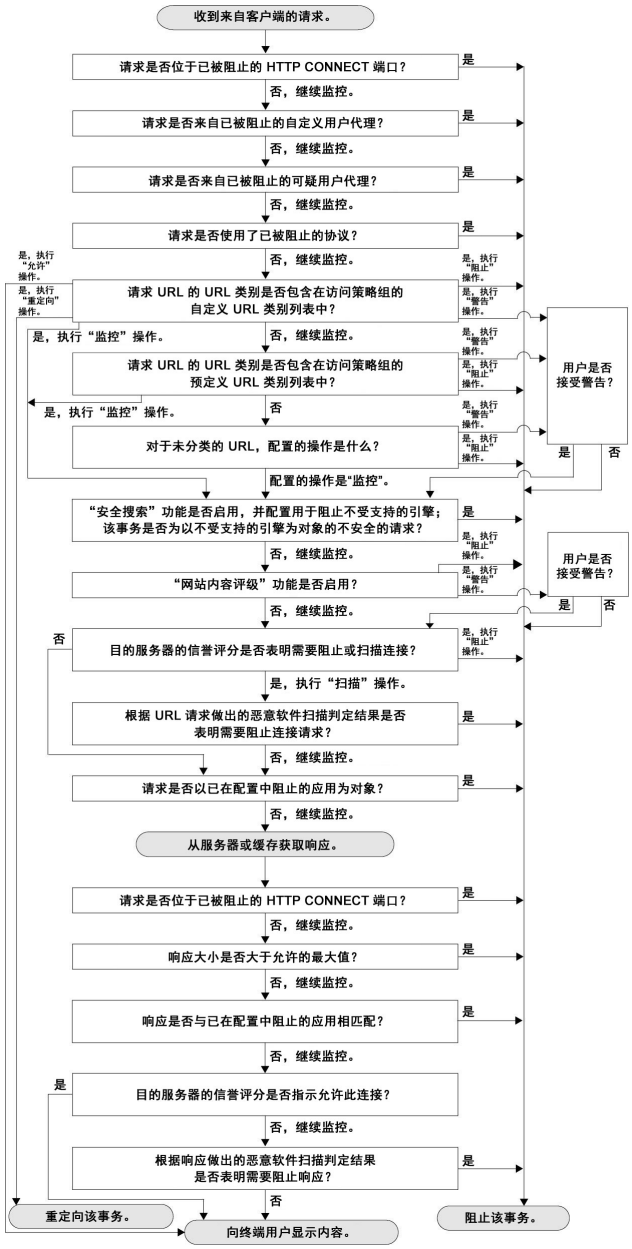
通常，不同的策略类型基于传输协议控制流量。

策略类型	协议				支持的操作			
	HTTP	HTTPS	FTP	SOCKS	阻止	允许	重定向	监控
访问	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
解密	x	x						x
数据安全	x	x	x		x			x
外部 DLP	x	x	x				x	
出站恶意软件扫描	x	x	x		x			x
路由	x	x	x				x	

注释 解密策略优先于访问策略。

下图显示 Web 代理如何在向请求分配特定访问策略后决定对请求执行的操作。目标服务器的 Web 信誉评分只评估一次，但结果会应用到决策流中两个不同的点上。

图 *5:* 应用访问策略操作



客户端应用

关于客户端应用

客户端应用（如 Web 浏览器）用于创建请求。您可以根据客户端应用定义策略成员身份，并可以指定控制设置并豁免客户端应用进行身份验证，这对于无法提示输入凭证的应用非常有用。

在策略中使用客户端应用

使用客户端应用定义策略成员身份

步骤 1 从“网络安全管理器”(Web Security Manager) 菜单中选择策略类型。

步骤 2 点击策略表中的策略名称。

步骤 3 展开“高级”(Advanced) 部分并点击“客户端应用”(Client Applications) 字段中的链接。

步骤 4 定义一个或多个客户端应用：

选项	方法
选择预定义客户端应用 (Choose a predefined client application)	展开“浏览器”(Browser) 和“其他”(Other) 部分，选中所需的客户端应用复选框。 **提示** 如果可能，请仅选择任意版本选项，因为相对于多个选择，这样可以提供更出色的性能。
定义自定义客户端应用 (Define a custom client application)	在“自定义客户端应用”(Custom Client Applications) 字段中输入适当的正则表达式。根据需要，在新行上输入其他正则表达式。 **提示** 点击**客户端应用模式示例 (Example Client Applications Patterns)** 获取正则表达式示例。

步骤 5 （可选）点击**匹配除所选客户端应用定义之外的所有定义 (Match All Except The Selected Client Applications Definitions)** 单选按钮，使策略成员身份基于**除**您定义的客户端应用之外的所有客户端应用。

步骤 6 点击**完成 (Done)**。

使用客户端应用定义策略控制设置

步骤 1 从“网络安全管理器”(Web Security Manager) 菜单中选择策略类型。

步骤 2 在策略表中查找所需的策略名称。

步骤 3 点击同一行上“协议和客户端应用”(Protocols and Client Applications) 列中的单元格链接。

步骤 4 从“编辑协议和客户端应用设置”(Edit Protocols and Client Applications Settings) 窗格的下拉列表中选择**定义自定义设置 (Define Custom Settings)**（如果尚未设置）。

步骤 5 在“自定义客户端应用”(Custom Client Applications) 字段中输入与要定义的客户端应用匹配的正则表达式。根据需要，在新行上输入其他正则表达式。

提示 点击**客户端应用模式示例 (Example Client Applications Patterns)** 可获取正则表达式示例。

步骤 6 提交并确认更改。

豁免客户端应用进行身份验证

过程

	命令或操作	目的
步骤 1	创建不需要进行身份验证的标识配置文件。	用户和客户端软件分类，第 115 页
步骤 2	设置标识配置文件成员身份作为要豁免的客户端应用。	在策略中使用客户端应用，第 190 页
步骤 3	将标识配置文件置于策略表中需要进行身份验证的所有其他标识配置文件之上。	策略顺序，第 180 页

时间范围和配额

您可以为访问策略和解密策略应用时间范围以及时间和量的配额，以限制用户何时具有访问权限及其最长连接时间或最大数据量（也称为“带宽配额”）。

- 针对策略和可接受使用控制的时间范围，第 191 页
- 时间和数量配额，第 192 页

针对策略和可接受使用控制的时间范围

时间范围是指在期间应用策略和可接受使用控制的定义时间段。

注释 您无法使用时间范围来定义用户必须进行身份验证的时间。身份验证要求在身份配置文件中定义，身份配置文件不支持时间范围。

- 创建时间范围，第 191 页

创建时间范围

步骤 1 选择**网络安全管理器 (Web Security Manager)** > **定义时间范围和配额 (Define Time Ranges and Quotas)**。

步骤 2 点击**添加时间范围 (Add Time Range)**。

步骤 3 输入时间范围的名称。

步骤 4 选择**时区 (Time Zone)**选项：

- 使用**设备中的时区设置 (Time Zone Setting From Appliance)** - 使用与网络安全设备相同的时区。
- **为此时间范围指定时区 (Specify Time Zone for this Time Range)** - 定义一个不同的时区，可以定义为 GMT 偏移，或是一个地区、国家/地区或该国家/地区中的特定时区。

步骤 5 选中一个或多个**星期几 (Day of Week)**复选框。

步骤 6 选择**时间 (Time of Day)**选项：

- **全天 (All Day)** - 采用完整的 24 小时期限。
- **开始时间 (From)** 和**结束时间 (To)** - 定义特定范围的小时数：以 HH: MM（24 小时制格式）格式输入开始时间和结束时间。

提示 每个时间范围定义一个开始时间和结束时间边界。例如，输入 8:00 至 17:00 匹配 8:00:00 至 16:59:59，但不匹配 17:00:00。对于午夜，必须指定 00:00 作为开始时间，指定 24:00 作为结束时间。

步骤 7 提交并确认更改。

时间和数量配额

在各个用户达到已应用的数据量或时间限制前，配额允许他们持续访问某个互联网资源（或某类互联网资源）。AsyncOS 对 HTTP、HTTPS 和 FTP 流量强制执行定义的配额。

当用户接近其时间或数量配额时，AsyncOS 首先显示警告，然后显示阻止页面。

请注意以下有关时间和数量配额的使用情况：

- 如果 AsyncOS 在透明模式下部署，并且 HTTPS 代理已禁用，则端口 443 上没有侦听，并且会丢弃请求。这是标准行为。如果 AsyncOS 在显示模式下部署，则可以在您的访问策略中设置配额。

  启用HTTPS代理时，对请求可能执行的操作为传递、解密、丢弃或监控。总体而言，解密策略中的配额仅适用于传递类别。

  对于传递操作，您还可以选择为隧道流量设置配额。对于解密操作，此选项不可用，因为访问策略中配置的配额将应用至解密的流量。

- 如果“URL 过滤”已禁用或者其功能密钥不可用，AsyncOS 将无法识别 URL 的类别，并且**访问策略 (Access Policy)** > **URL 过滤 (URL Filtering)** 页面处于禁用状态。因此，必须存在功能密钥并且启用“可接受使用策略”(Acceptable Use Policies)，才能配置配额。
- 许多网站（例如 Facebook 和 Gmail）会定期自动更新。如果此类网站在一个未使用的浏览器窗口或选项卡中处于打开状态，它将继续使用用户的时间和数量配额。
- 代理重启将导致配额重置，可能允许进行比计划更多的访问。发生代理重启可能是由于配置更改、崩溃、计算机重启等原因所致。因为管理员没有被明确告知代理重启，因此可能出现一些混淆。
- 即使已启用“为 EUN 解密”(decrypt-for-EUN) 选项，也可能无法对 HTTPS 显示您的 EUN 页面（警告和阻止）。

注释 当多个配额应用于任意给定用户时，将始终应用限制最严格的配额。

- 数量配额计算， 第 193 页
- 时间配额计算， 第 193 页
- 定义时间和数量配额， 第 193 页

数量配额计算

数量配额的计算如下所示：

- HTTP 和解密的 HTTPS 流量 - HTTP 请求和响应正文计入配额限制。请求头和响应头将不会计入限制。
- 隧道流量（包括隧道 HTTPS）- AsyncOS 将隧道流量从客户端传输到服务器，反之亦然。隧道流量的整个数据量会计入配额限制。
- FTP - 不会计入控制连接流量。上传和下载的文件的大小会计入配额限制。

注释 仅客户端流量会计入配额限制。缓存的内容也会计入限制，因为即使从缓存提供响应，也会生成客户端流量。

时间配额计算

时间配额的计算如下所示：

- HTTP 和解密的 HTTPS 流量 - 每个与相同 URL 类别的连接的持续时间（从形成到断开连接），加上一分钟计入时间配额限制。如果一分钟内向同一URL类别发起多个请求，它们会计为一个连续会话并且仅在此会话结束时加一分钟（即至少一分钟“静默”之后）。
- 隧道流量（包括隧道 HTTPS）- 隧道的实际持续时间（从形成到断开）计入配额限制。上述针对多个请求的计算也适用于隧道流量。
- FTP - FTP 控制会话的实际持续时间（从形成到断开）计入配额限制。上述针对多个请求的计算也适用于 FTP 流量。

定义时间和数量配额

开始之前

- 转到**安全服务 (Security Services)** > **可接受的使用控制 (Acceptable Use Controls)** 启用可接受的使用控制。
- 除非您想要配额限制为每日应用，否则请定义时间范围。

步骤 1 导航到**网络安全管理器 (Web Security Manager)** > **定义时间范围和配额 (Define Time Ranges and Quotas)**。

步骤 2 点击**添加配额 (Add Quota)**。

步骤 3 在字段中输入唯一的**配额名称 (Quota Name)**。

步骤 4 要每天重置配额，请选择**每天于以下时间重置此配额 (Reset this quota daily at)** 并在字段中输入 12 小时制的时间，然后从菜单中选择 **AM** 或 **PM**。或者，选择**选择预定义的时间范围配置文件 (Select a predefined time range profile)**。

步骤 5 要设置时间配额，请选中**时间配额 (Time Quota)** 复选框并从**小时 (hrs)** 菜单中选择小时数，从**分钟 (mins)** 菜单中选择分钟数，从零（始终阻止）到 23 小时 59 分钟。

步骤 6 要设置数量配额，请在字段中输入一个数字并从菜单中选择 **KB**（千字节）、MB（兆字节），或 **GB**（千兆字节）。

步骤 7 点击**提交 (Submit)**，然后点击**确认更改 (Commit Changes)** 以应用更改。或者，点击**取消 (Cancel)** 放弃更改。

下一步做什么

（可选）导航到**安全服务 (Security Services) > 最终用户通知 (End-User Notification)** 以针对配额配置最终用户通知。

按 URL 类别划分的访问控制

您可以根据 Web 请求寻址的网站的类别来识别和处理这些请求。网络安全设备附带许多预定义 URL 类别，例如基于网络的邮件及其他类别。

预定义的类别以及与其关联的网站是在网络安全设备上的过滤数据库中定义。这些数据库由思科自动保持更新。您也可以为指定的主机名和 IP 地址创建自定义 URL 类别。

URL 类别可供所有策略使用，但用于识别请求的策略除外。它们还可供访问、加密 HTTPS 管理和数据安全策略用于将操作应用到请求。

有关创建自定义 URL 类别的信息，请参阅创建和编辑自定义 URL 类别，第 151 页。

使用 URL 类别识别 Web 请求

开始之前

- 启用“可接受的使用控制”(Acceptable Use Control)，请参阅配置 URL 过滤引擎，第 140 页。
- （可选）创建自定义 URL 类别，请参阅创建和编辑自定义 URL 类别，第 151 页。

步骤 1 从“网络安全管理器”(Web Security Manager) 菜单中选择策略类型（SaaS 除外）。

步骤 2 点击策略表中的策略名称（或添加新策略）。

步骤 3 展开**高级 (Advanced)** 部分部分并点击“URL 类别”(URL Categories) 字段中的链接。

步骤 4 点击与要将其作为识别 Web 请求依据的 URL 类别对应的“添加”(Add) 列单元格。根据需要对自定义 URL 类别和预定义 URL 类别列表执行此操作。

步骤 5 点击**完成 (Done)**。

步骤 6 提交并确认更改。

使用 URL 类别处理 Web 请求

开始之前

- 启用“可接受的使用控制”(Acceptable Use Control)，请参阅配置 URL 过滤引擎，第 140 页。
- （可选）创建自定义 URL 类别，请参阅创建和编辑自定义 URL 类别，第 151 页。

注释 如果您使用 URL 类别作为某策略中的条件，则可以在同一策略内针对这些类别本身指定操作。因此，下述某些选项可能会有所不同或因此不可用。

步骤 1 从“网络安全管理器”(Web Security Manager) 菜单中选择**访问策略 (Access Policies)**、**思科数据安全策略 (Cisco Data Security Policies)** 或 **加密 HTTPS 管理 (Encrypted HTTPS Management)** 中的一项。

步骤 2 在策略表中查找所需的策略名称。

步骤 3 点击同一行上“URL 过滤”(URL Filtering) 列中的单元格链接。

步骤 4 （可选）添加自定义 URL 类别：

a) 点击**选择自定义类别 (Select Custom Categories)**。

b) 选择要在此策略中包含的自定义 URL 类别，然后点击**应用 (Apply)**。

选择 URL 过滤引擎在比较客户端请求时所依据的自定义 URL 类别。URL 过滤引擎将根据包含的自定义 URL 类别比较客户端请求，并忽略已排除的自定义 URL 类别。URL 过滤引擎将客户端请求中的 URL 与包含的自定义 URL 类别进行比较，然后再与预定义的 URL 类别进行比较。

策略中包含的自定义 URL 类别显示在“自定义 URL 类别过滤”(Custom URL Category Filtering) 部分中。

步骤 5 为每个自定义和预定义的 URL 类别选择一项操作。

注释 可用的操作可能因自定义和预定义类别以及策略类型而异。

步骤 6 在“未分类的 URL”(Uncategorized URLs) 部分中，选择要对不属于预定义或自定义 URL 类别的网站的客户端请求采取的操作。

步骤 7 提交并确认更改。

远程用户

关于远程用户

思科 AnyConnect Secure Mobility 将网络边界扩展到远程终端，支持集成网络安全设备所提供的网络过滤服务。

远程和移动用户使用思科 AnyConnect Secure VPN（虚拟专用网）客户端建立与自适应安全设备 (ASA) 的 VPN 会话。ASA 将 Web 流量连同按 IP 地址和用户名标识用户的信息一起发送到网络安全设备。网络安全设备扫描流量，执行可接受的使用策略，并保护用户免受安全威胁。安全设备将视为安全且可接受的所有流量返回到用户。

在启用了 Secure Mobility 的情况下，您可以配置通过用户位置应用到用户的身份和策略：

- **远程用户**。这些用户使用 VPN 从远程位置连接到网络。当思科 ASA 和 Cisco AnyConnect 客户端均用于VPN访问时，网络安全设备会自动识别远程用户。否则，网络安全设备管理员必须通过配置 IP 地址范围指定远程用户。
- **本地用户**。这些用户以物理方式或无线方式连接到网络。

当网络安全设备与思科ASA集成时，您可以将其配置为通过已经过身份验证的用户名透明地识别用户，来实现远程用户的单点登录。

如何配置远程用户的标识

任务	详细信息
1.配置远程用户的标识。	配置远程用户的标识，第 196 页
2.创建远程用户的身份。	用户和客户端软件分类，第 115 页 **1.** 在“按用户位置定义成员”(Define Members by User Location)部分中，选择“仅限远程用户”(Remote Users Only)。 **2.** 在“按身份验证定义成员”(Define Members by Authentication)部分中，选择“通过思科 ASA 集成以透明方式识别用户”(Identify Users Transparently through Cisco ASA Integration)。
3.为远程用户创建策略。	创建策略，第 181 页

配置远程用户的标识

步骤 1 依次选择“安全服务”(Security Services) > “AnyConnect 安全移动”(AnyConnect Secure Mobility)，然后点击**启用 (Enable)**。

步骤 2 阅读 AnyConnect 安全移动许可证协议的条款，然后点击**接受 (Accept)**。

步骤 3 配置识别远程用户的方式。

选项	说明	其他步骤
IP 地址 (IP Address)	指定设备向远程设备分配 IP 地址时应考虑的 IP 地址范围。	**1.** 在“IP 范围”(IP Range) 字段中输入 IP 地址范围。 **2.** 转到步骤 4

选项	说明	其他步骤
思科 ASA 集成 (Cisco ASA Integration)	指定与网络安全设备通信的一个或多个思科 ASA。思科 ASA 维护 IP 地址到用户的映射，并与网络安全设备交流该信息。当 Web 代理接收事务时，它获取 IP 地址并通过检查 IP 地址到用户的映射确定用户。当通过与思科 ASA 集成来确定用户时，您可以启用远程用户的单点登录。	1. 输入思科 ASA 主机名或 IP 地址。 2. 输入用于访问 ASA 的端口号。思科 ASA 的默认端口号为 11999。 3. 如果在集群中配置了多个思科 ASA，请点击**添加行 (Add Row)**，配置集群中的每个 ASA。 注释 如果出于高可用性配置了两个思科 ASA，请只为活动的思科 ASA 输入一个主机名或 IP 地址。 4. 输入思科 ASA 的访问密码。 注释 在此处输入的密码必须与为指定思科 ASA 配置的访问密码匹配。 5. （可选）点击**开始测试 (Start Test)** 以验证网络安全设备是否可以连接到所配置的思科 ASA。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

显示 ASA 的远程用户状态和统计信息

当网络安全设备与 ASA 集成时，使用此命令可显示与 Secure Mobility 相关的信息。

命令	说明
`musstatus`	此命令会显示以下信息： • 网络安全设备与每个 ASA 连接的状态。 • 网络安全设备与每个 ASA 连接的持续时间（分钟）。 • 来自每个 ASA 的远程客户端的数量。 • 服务的远程客户端数量，其定义为通过网络安全设备传递流量的远程客户端的数量。 • 远程客户端的总数。

对策略进行故障排除

• 无法配置 HTTPS 的访问策略， 第 439 页
• 未阻止某些 Microsoft Office 文件， 第 427 页
• 阻止 DOS 可执行对象类型会阻止 Windows OneCare 的更新， 第 427 页
• 标识配置文件从策略中消失， 第 439 页

第 12 章

创建解密策略以控制 HTTPS 流量

本章包含以下部分：

创建解密策略以控制 HTTPS 流量概述

解密策略定义 HTTPS 流量在 Web 代理中的处理：

- 何时解密 HTTPS 流量。
- 如何处理使用无效或已吊销的安全证书的请求。

可以创建解密策略来通过以下方式处理 HTTPS 流量：

- 通过加密流量。
- 解密流量并应用为 HTTP 流量定义的基于内容的访问策略。借此也可以进行恶意软件扫描。
- 丢弃 HTTPS 连接。
- 在 Web 代理继续根据可能导致最终丢弃、通过或解密操作的策略来评估请求时监控请求（不采取最终操作）。

注意 **谨慎处理个人可识别信息：**如果您选择解密最终用户的HTTPS会话，则网络安全设备访问日志和报告可能包含个人可识别信息。管理员可以使用 `advancedproxyconfig` CLI 命令和 `HTTPS` 子命令配置日志中存储的 URI 文本量。您可以记录整个 URI，也可以记录删除了查询部分的部分形式的 URI。但是，即使选择从 URI 中删除查询，也仍然可能保留个人可识别信息。

通过解密策略管理 HTTPS 流量的任务概述

步骤	通过解密策略管理 HTTPS 流量的任务列表	相关主题和程序的链接
1	启用 HTTPS 代理	启用 HTTPS 代理，第 202 页
2	上传或生成证书和密钥	• 上传根证书和密钥，第 207 页 • 生成 HTTPS 代理的证书和密钥，第 208 页
3	配置解密选项	配置解密选项，第 204 页
5	（可选）配置无效证书处理	配置无效证书处理，第 208 页
6	（可选）启用实时吊销状态检查	启用实时吊销状态检查，第 209 页
7	（可选）管理受信任和受阻证书	受信任根证书，第 210 页

通过解密策略管理 HTTPS 流量的最佳实践

创建适用于网络上的所有用户或更少用户，或更大的用户组的更少、更通用的解密策略组。然后，如果需要对已解密的 HTTPS 流量应用更精细的控制，请使用更具体的访问策略组。

解密策略

设备可以对 HTTPS 连接请求执行以下任何操作：

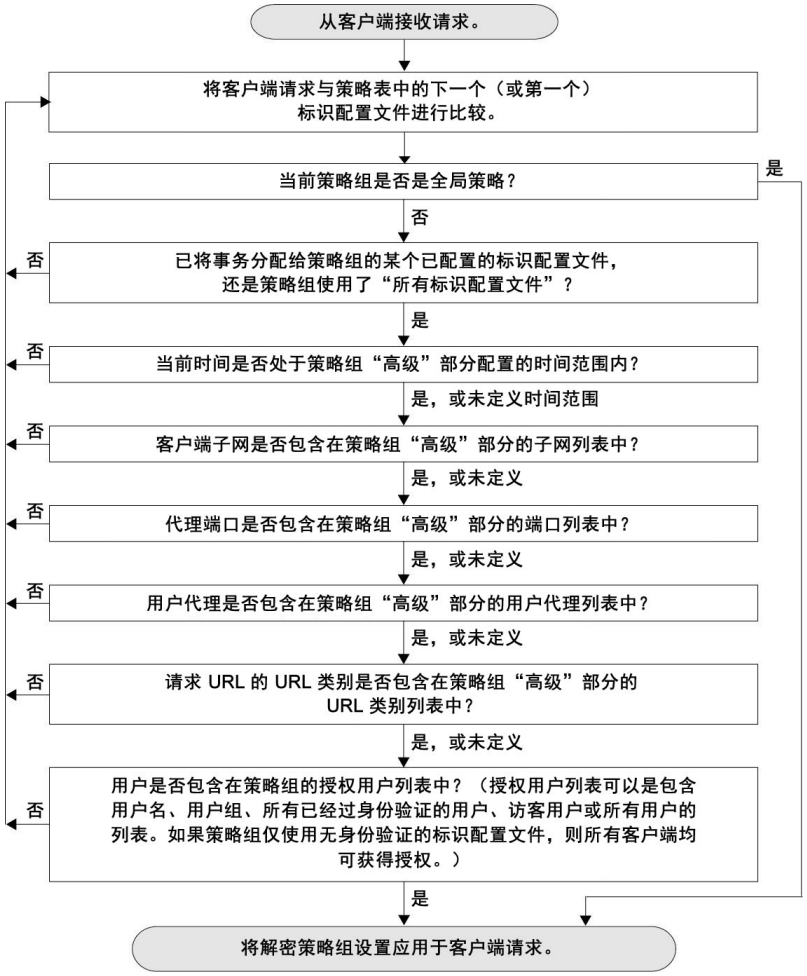
选项	说明
监控 (Monitor)	监控是一项中间操作，用于表明 Web 代理应根据其他控制设置继续评估事务以确定最终应用哪个最终操作。
丢弃 (Drop)	设备丢弃连接，并且不将连接请求传递到服务器。设备不会通知用户它已断开连接。
通过 (Pass Through)	设备通过客户端和服务器之间的连接，而不检测流量内容。 但是，在使用标准通过策略的情况下，WSA 会通过发起与服务器的 HTTPS 握手来检查被请求服务器的有效性。此有效性检查包括服务器证书验证。如果服务器未通过此检查，则事务会被阻止。 您可以跳过对某些特定站点的验证检查，方法是配置涵盖这些站点的自定义类别的策略，指示这些站点是可信站点，可通过而无需进行有效性检查。配置用以允许跳过有效性检查的策略时请格外小心。

选项	说明
解密 (Decrypt)	设备允许连接，但会检测流量内容。它解密流量并将访问策略应用于已解密的流量，就如同它是明文 HTTP 连接一样。通过解密连接和应用访问策略，可以扫描流量来查找恶意软件。

除“监控”外的所有操作都是 Web 代理应用于事务的“最终操作”。最终操作是导致 Web 代理停止根据其他控制设置评估事务的操作。例如，如果将“解密策略”配置为监控无效服务器证书，则 Web代理不会针对服务器证书无效时如何处理HTTPS事务做出最终决策。如果将“解密策略”配置为阻止 Web 信誉分数较低的服务器，那么发往信誉分数低的服务器的任何请求都将被丢弃，而不考虑 URL 类别操作。

下图显示 Web 代理如何根据“解密策略”组评估客户端请求。 图 7: 应用解密策略操作，第 204 页显示 Web 代理在评估解密策略控制设置时使用的顺序。 图 5: 应用访问策略操作，第 189 页显示 Web 代理在评估访问策略控制设置时使用的顺序。

图 *6:* 针对解密策略的策略组事务流



启用 HTTPS 代理

要监控和解密 HTTPS 流量，必须启用 HTTPS 代理。当启用 HTTPS 代理时，必须配置在设备将自签名服务器证书发送到网络上的客户端应用时该设备对根证书使用的设置。可以上传贵组织已有的根证书和密钥，也可以将设备配置为使用输入的信息生成证书和密钥。

启用 HTTPS 代理之后，所有 HTTPS 策略决策都由解密策略进行处理。另外在此页面上，还可以配置当服务器证书无效时设备如何处理 HTTPS 流量。

开始之前

当启用 HTTPS 代理时，将会禁用访问策略中的 HTTPS 特定规则，并且 Web 代理使用用于 HTTP 的规则来处理已解密的 HTTPS 流量。

步骤 1 **安全服务 (Security Services)** > **HTTPS 代理 (HTTPS Proxy)**，点击**启用和编辑设置 (Enable and Edit Settings)**。

系统将显示 HTTPS 代理许可协议。

步骤 2 阅读 HTTPS 代理许可协议的条款，然后点击**接受 (Accept)**。

步骤 3 验证“启用 HTTPS 代理”(Enable HTTPS Proxy) 字段是否已启用。

步骤 4 在 **HTTPS 代理端口 (HTTPS Ports to Proxy)** 字段中，输入设备应检查以获取 HTTPS 流量的端口。默认端口为端口 443。

注释 网络安全设备可为其充当代理的最大端口数为 30，其中包括 HTTP 和 HTTPS。

步骤 5 上传或生成要用于解密的根证书/签名证书。

注释 如果设备具有已上传的证书/密钥对和已生成的证书/密钥对，则其仅使用“用于签名的根证书”(Root Certificate for Signing) 部分中当前选择的证书/密钥对。

步骤 6 在“HTTPS 透明请求”(HTTPS Transparent Request) 部分中，选择以下选项之一：

- 解密 HTTPS 请求并重定向以进行身份验证 (Decrypt the HTTPS request and redirect for authentication)
- 拒绝 HTTPS 请求 (Deny the HTTPS request)

此设置仅适用于使用 IP 地址作为身份验证代理的事务，并且仅在用户尚未进行身份验证时适用。

注释 仅当在透明模式下部署设备时，才会显示此字段。

步骤 7 在“使用 HTTPS 的应用”(Applications that Use HTTPS) 部分中，选择是否启用解密以获得增强的应用可视性与可控性。

注释 除非在客户端上安装用于签名的根证书，否则解密可能会导致某些应用失败。有关设备根证书的详细信息，请参阅管理 HTTPS 的证书验证和解密，第 206 页。

步骤 8 提交并确认更改。

下一步做什么

相关主题

- 管理 HTTPS 的证书验证和解密，第 206 页

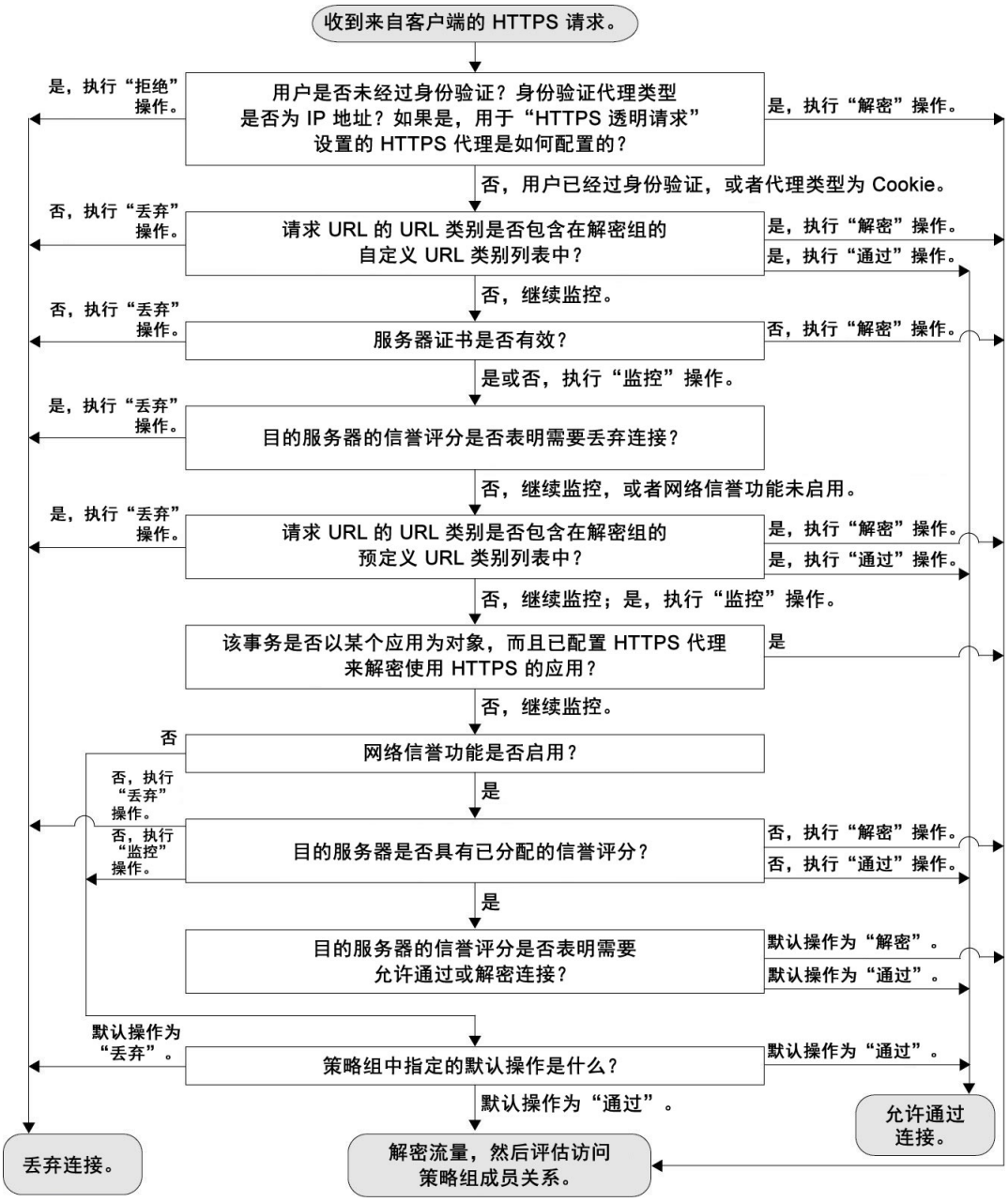
控制 HTTPS 流量

在网络安全设备将HTTPS连接请求分配到解密策略组后，连接请求继承该策略组的控制设置。“解密策略”组的控制设置决定了设备是解密、丢弃还是通过连接：

选项	说明
URL 类别 (URL Categories)	可以面向每个预定义和自定义URL类别配置要对HTTPS请求采取的操作。点击要配置的策略组的“URL 过滤”(URL Filtering) 列下的链接。 **注释** 如果要阻止（带有最终用户通知）HTTPS请求的特定URL类别而不是丢弃（不带最终用户通知），请选择在解密策略组中解密该 URL 类别，然后选择在访问策略组中阻止同一 URL 类别。
Web 信誉 (Web Reputation)	可以基于所请求的服务器的 Web 信誉分数来配置要对 HTTPS 请求采取的操作。点击要配置的策略组的“Web 信誉”(Web Reputation) 列下的链接。
默认操作 (Default Action)	可以配置在无任何其他设置适用时设备应采取的操作。点击要配置的策略组的“默认操作”(Default Action) 列下的链接。 **注释** 仅当未基于 URL 类别或 Web 信誉分数制定决策时，所配置的默认操作才会影响事务。如果禁用 Web 信誉过滤，则默认操作适用于与 URL 类别中的“监控”(Monitor) 操作相匹配的所有事务。如果启用 Web 信誉过滤，则仅在为没有评分的站点选择“监控”(Monitor) 操作时，才会使用默认操作。

下图显示设备如何在为HTTPS请求分配特定解密策略后决定对请求执行的操作。目标服务器的Web信誉评分只评估一次，但结果会应用到决策流中两个不同的点上。例如，请注意 Web 信誉分数的“丢弃”(Drop) 操作会覆盖为预定义 URL 类别指定的任何操作。

图 7: 应用解密策略操作



配置解密选项

开始之前

验证是否启用了 HTTPS 代理，如启用 HTTPS 代理，第 202 页中所述。

步骤 1 安全服务 **(Security Services)** > **HTTPS 代理 (HTTPS Proxy)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 启用解密选项。

解密选项	说明
为身份验证解密 (Decrypt for Authentication)	对于在此 HTTPS 事务之前尚未进行身份验证的用户，允许解密以进行身份验证。
为最终用户通知解密 (Decrypt for End-User Notification)	允许解密，以便 AsyncOS 可以显示最终用户通知。 **注释** 如果证书无效，并且无效证书即将丢弃，则在运行策略跟踪时，事务的第一个记录的操作将是“解密”(decrypt)。
为最终用户确认解密 (Decrypt for End-User Acknowledgement)	对于在此 HTTPS 事务之前尚未确认 Web 代理的用户，允许解密，以便 AsyncOS 可以显示最终用户确认。
为应用检测解密 (Decrypt for Application Detection)	增强 AsyncOS 检测 HTTPS 应用的能力。

身份验证和 HTTPS 连接

在 HTTPS 连接层进行身份验证适用于以下类型的请求：

选项	说明
显式请求 (Explicit requests)	• 已禁用安全客户端身份验证或 • 已启用安全客户端身份验证，并且基于 IP 的代理
透明请求 (Transparent requests)	• 基于 IP 的代理，已启用适用于身份验证的解密 • 基于 IP 的代理，客户端先前使用 HTTP 请求进行了身份验证

根证书

HTTPS 代理使用上传到设备的根证书和私钥文件来解密流量。上传到设备的根证书和私钥文件必须是 PEM 格式；不支持 DER 格式。

可以通过以下方式输入根证书信息：

- **生成**。可以输入某些基本组织信息，然后点击一个按钮，以使设备生成证书的其余内容和私钥。
- **上传**。可以上传证书文件及其在设备外创建的匹配私钥文件。

注释 还可以上传已由根证书颁发机构签署的中间证书。当 Web 代理模仿服务器证书时，它将上传的证书以及模仿的证书发送到客户端应用。这样，只要中间证书由客户端应用信任的根证书颁发机构签署，应用也会信任模仿的服务器证书。有关详细信息，请参阅证书和密钥简介，第 406 页。

可以选择网络安全设备如何处理发放的根证书：

- **通知用户接受根证书**。可以通知贵组织中的用户，告知其公司的新策略并指示其接受组织提供的根证书作为受信任来源。
- **将根证书添加到客户端计算机**。能够以受信任根证书颁发机构身份将根证书添加到网络上的所有客户端计算机。这样，客户端应用将自动接受包含根证书的事务。

步骤 1 安全服务 (Security Services) > HTTPS 代理 (HTTPS Proxy)。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 点击已生成或已上传的证书的“下载证书”(Download Certificate) 链接。

注释 要降低客户端计算机发生证书错误的可能性，请在生成根证书或将其上传到网络安全设备后提交更改，然后将证书分发到客户端计算机，再提交对设备的更改。

管理 HTTPS 的证书验证和解密

网络安全设备在检测和解密内容之前会验证证书。

有效证书

有效证书的质量：

- **没有过期**。证书的有效期包括当前日期。
- **证书颁发机构可识别**。证书颁发机构包含在网络安全设备上存储的受信任证书颁发机构列表中。
- **签名有效**。已根据密码标准正确实施数字签名。
- **命名一致**。公用名与 HTTP 报头中指定的主机名相匹配。
- **未吊销**。证书颁发机构尚未吊销证书。

相关主题

- 启用实时吊销状态检查，第 209 页
- 配置无效证书处理，第 208 页
- 证书吊销状态检查选项，第 209 页

无效证书处理

设备可以对无效服务器证书执行以下操作之一：

- 丢弃。
- 解密。
- 监控。

由于各种原因而无效的证书

对于由于无法识别的根证书颁发机构和已过期证书而无效的服务器证书，HTTPS 代理执行适用于无法识别的根证书颁发机构的操作。

在所有其他情况下，对于由于多个原因而同时无效的服务器证书，HTTPS 代理按操作限制性从高到低的顺序执行操作。

面向已解密连接的不受信任的证书警告

当网络安全设备遇到无效证书并配置为解密连接时，AsyncOS 会创建要求最终用户接受或拒绝连接的不受信任证书。证书的公用名是“不受信任的证书警告”(Untrusted Certificate Warning)。

将此不受信任证书添加到受信任证书列表将会删除最终用户的用于接受或拒绝连接的选项。

当 AsyncOS 生成这些证书之一时，它创建包含文本“签署不受信任的密钥”(Signing untrusted key) 或“签署不受信任的证书”(Signing untrusted cert) 的代理日志条目。

上传根证书和密钥

开始之前

启用 HTTPS 代理。启用 HTTPS 代理 ， 第 202 页。

步骤 1 **安全服务 (Security Services)** > **HTTPS 代理 (HTTPS Proxy)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择**使用上传的证书和密钥 (Use Uploaded Certificate and Key)**。

步骤 4 点击“证书”(Certificate) 字段的**浏览 (Browse)** 以导航到本地计算机上存储的证书文件。

如果上传的文件包含多个证书或密钥，则 Web 代理使用文件中的第一个证书或密钥。

步骤 5 点击“密钥”(Key) 字段的**浏览 (Browse)** 可导航到私钥文件。

注释 密钥长度必须为 512 位、1024 位或 2048 位。

步骤 6 如果密钥已加密，请选择**密钥已加密 (Key is Encrypted)**。

步骤 7 点击**上传文件 (Upload Files)** 将证书和密钥文件传输到网络安全设备。

上传的证书信息显示在“编辑 HTTPS 代理设置”(Edit HTTPS Proxy Settings) 页面上。

步骤 8 （可选）点击**下载证书 (Download Certificate)**，以便将该证书传输到网络上的客户端应用。

生成 HTTPS 代理的证书和密钥

开始之前

启用 HTTPS 代理。启用 HTTPS 代理，第 202 页。

步骤 1 安全服务 (Security Services) > HTTPS 代理 (HTTPS Proxy)。

步骤 2 点击编辑设置 (Edit Settings)。

步骤 3 选择使用生成的证书和密钥 (Use Generated Certificate and Key)。

步骤 4 点击生成新的证书和密钥 (Generate New Certificate and Key)。

步骤 5 在“生成证书和密钥”(Generate Certificate and Key) 对话框中，输入要在根证书中显示的信息。

可以在公用名 (Common Name) 字段中输入除正斜杠 (/) 以外的任何 ASCII 字符。

步骤 6 点击生成 (Generate)。

步骤 7 生成的证书信息显示在“编辑 HTTPS 代理设置”(Edit HTTPS Proxy Settings) 页面上。

步骤 8 （可选）点击下载证书 (Download Certificate)，以便将该证书传输到网络上的客户端应用。

步骤 9 （可选）点击下载证书签名请求 (Download Certificate Signing Request) 链接，可将证书签名请求 (CSR) 提交到证书颁发机构 (CA)。

步骤 10 （可选）在从 CA 收回签名证书后将该证书上传到网络安全设备。可以在设备上生成证书后随时上传。

步骤 11 “提交”(Submit) 并“确认更改”(Commit Changes)。

配置无效证书处理

开始之前

验证是否启用了 HTTPS 代理，如启用 HTTPS 代理，第 202 页中所述。

步骤 1 安全服务 (Security Services) > HTTPS 代理 (HTTPS Proxy)。

步骤 2 点击编辑设置 (Edit Settings)。

步骤 3 对于每个类型的证书错误，定义代理响应：丢弃 (Drop)、解密 (Decrypt) 或监控 (Monitor)。

证书错误类型	说明
到期 (Expired)	当前日期超出证书的有效性范围。
主机名不匹配 (Mismatched hostname)	证书中的主机名与客户端尝试访问的主机名不匹配。 注释 仅当 Web 代理在显式转发模式下部署时，才能执行主机名匹配。在透明模式下部署该代理时，它不知道目标服务器的主机名（它仅知道 IP 地址），因此其不能与服务器证书中的主机名进行比较。

证书错误类型	说明
根证书颁发机构/颁发者无法识别 (Unrecognized root authority/issuer)	无法识别根证书颁发机构或中间证书颁发机构。
签名证书无效 (Invalid signing certificate)	签名证书存在问题。
叶证书无效 (Invalid leaf certificate)	叶证书存在问题，例如，拒绝、解码或不匹配问题。
其他所有错误类型	大多数其他错误类型都是由于设备无法与 HTTPS 服务器完成 SSL 握手。有关服务器证书的其他错误场景的详细信息，请参阅 http://www.openssl.org/docs/apps/verify.html。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

证书吊销状态检查选项

要确定证书颁发机构是否已吊销证书，网络安全设备可以通过以下方式向证书颁发机构核查：

- **证书吊销列表（仅限 Comodo 证书）**。网络安全设备会检查 Comodo 的证书吊销列表。Comodo 维护此列表，根据各自的策略对其进行更新。根据其上次更新时间，在网络安全设备检查证书吊销列表时，该列表可能已过期。
- **在线证书状态协议 (OCSP)**。网络安全设备实时向证书颁发机构核查吊销状态。如果证书颁发机构支持 OCSP，则证书将包含用于实时状态检查的 URL。默认情况下，进行全新安装会启用此功能，而进行更新则会禁用此功能。

注释 网络安全设备仅对确定为在所有其他方面都有效并包含 OCSP URL 的证书执行 OCSP 查询。

相关主题

- 启用实时吊销状态检查， 第 209 页
- 配置无效证书处理， 第 208 页

启用实时吊销状态检查

开始之前

确保 HTTPS 代理已启用。请参阅启用 HTTPS 代理， 第 202 页。

步骤 1 **安全服务 (Security Services) > HTTPS 代理 (HTTPS Proxy)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择“启用在线证书状态协议 (OCSP)”**(Enable Online Certificate Status Protocol (OCSP))**。

步骤 4 配置 **OCSP 结果处理 (OCSP Result Handling)** 属性。

思科建议将“OCSP 结果处理”(OCSP Result Handling) 选项配置为与“无效证书处理”(Invalid Certificate Handling) 选项相同的操作。例如，如果将“已到期证书”(Expired Certificate) 设置为“监控”(Monitor)，请将“已吊销证书”(Revoked Certificate) 配置为“监控”(Monitor)。

步骤 5 （可选）展开“高级”(Advanced) 配置部分并配置下述设置。

字段名称	说明
OCSP 有效响应缓存超时 (OCSP Valid Response Cache Timeout)	在重新检查有效的 OCSP 响应之前要等待的时间，以秒 (s)、分钟 (m)、小时 (h) 或天 (d) 为单位。默认单位为秒。有效范围介于 1 秒到 7 天之间。
OCSP 无效响应缓存超时 (OCSP Invalid Response Cache Timeout)	在重新检查无效的 OCSP 响应之前要等待的时间，以秒 (s)、分钟 (m)、小时 (h) 或天 (d) 为单位。默认单位为秒。有效范围介于 1 秒到 7 天之间。
OCSP 网络错误缓存超时 (OCSP Network Error Cache Timeout)	在获取响应失败后再次尝试联系 OCSP 响应方之前要等待的时间，以秒 (s)、分钟 (m)、小时 (h) 或天 (d) 为单位。有效范围介于 1 秒到 24 小时之间。
允许的时钟偏差 (Allowed Clock Skew)	网络安全设备和 OCSP 响应方之间的时间设置中允许的最大差异，以秒 (s) 或分钟 (m) 为单位。有效范围介于 1 秒到 60 分钟之间。
等待 OCSP 响应的最长时间 (Maximum Time to Wait for OCSP Response)	等待来自 OCSP 响应方的响应的最长时间。有效范围介于 1 秒到 10 分钟之间。指定更短的持续时间可减少在 OCSP 响应方不可用的情况下最终用户访问 HTTPS 请求的延迟。
对 OCSP 检查使用上游代理 (Use upstream proxy for OCSP checking)	上游代理的组名。
免除上游代理的服务器 (Servers exempt from upstream proxy)	要免除的服务器的 IP 地址或主机名。可以留空。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

受信任根证书

网络安全设备随附并维护受信任根证书列表。具有受信任证书的网站无需解密。

您可以管理受信任证书列表、向其中添加证书以及在功能上将证书从列表中删除。虽然网络安全设备不会从主列表中删除证书，但它允许在证书中覆盖信任，这可在功能上从受信任列表中删除该证书。

向受信任列表中添加证书

开始之前

验证 HTTPS 代理是否已启用。请参阅启用 HTTPS 代理，第 202 页。

步骤 1 安全服务 **(Security Services)** > **HTTPS 代理 (HTTPS Proxy)**。

步骤 2 点击管理受信任根证书 **(Manage Trusted Root Certificates)**。

步骤 3 点击导入 **(Import)**。

步骤 4 点击浏览 **(Browse)** 并导航到证书文件。

步骤 5 提交 **(Submit)** 并确认更改 **(Commit Changes)**。

在自定义受信任根证书 **(Custom Trusted Root Certificates)** 列表中查找已上传的证书。

从受信任列表中删除证书

步骤 1 依次选择安全服务 **(Security Services)** > **HTTPS 代理 (HTTPS Proxy)**。

步骤 2 点击管理受信任根证书 **(Manage Trusted Root Certificates)**。

步骤 3 选中与要从列表中删除的证书对应的覆盖信任 **(Override Trust)** 复选框。

步骤 4 提交 **(Submit)** 并确认更改 **(Commit Changes)**。

路由 HTTPS 流量

AsyncOS 根据客户端报头中存储的信息来路由 HTTPS 事务的能力有限，并且对于透明和显式 HTTPS 不同。

选项	说明
透明 HTTPS (Transparent HTTPS)	如果是透明 HTTPS，则 AsyncOS 无权访问客户端报头中的信息。因此，AsyncOS 无法实施依赖于客户端报头中的信息的路由策略。
显式 HTTPS (Explicit HTTPS)	如果是显式 HTTPS，则 AsyncOS 有权访问客户端报头中的以下信息： • URL • 目标端口号 因此，对于显式 HTTPS 事务，可以基于 URL 或端口号与路由策略相匹配。

解密/HTTPS/证书故障排除

第 13 章

扫描出站流量以查找现有感染

本章包含以下部分：

扫描出站流量概述

为防止恶意数据从网络中泄露出去，网络安全设备提供出站恶意软件扫描功能。使用策略组，您可以定义扫描了哪些上传内容以查找恶意软件，哪些防恶意软件扫描引擎将用于扫描，以及将阻止哪些恶意软件类型。

Cisco 动态矢量和流 (DVS) 引擎在事务请求从网络中泄露出去时对其进行扫描。通过与 Cisco DVS 引擎配合使用，网络安全设备使您能够阻止用户故意上传恶意数据。

您可以执行以下任务：

任务	任务链接
创建用于阻止恶意软件的策略	创建出站恶意软件扫描策略， 第 215 页
将上传请求分配到出站恶意软件策略组	控制上传请求， 第 216 页

DVS 引擎阻止请求时的用户体验

当思科DVS引擎阻止上传请求时，Web代理会向最终用户发送一个阻止页面。但是，并非所有网站都向最终用户显示该阻止页面。某些 Web 2.0 网站使用 JavaScript 显示动态内容而不是静态网页，因此不可能显示阻止页面。系统仍然会适当阻止用户上传恶意数据，但网站并不会始终将此情况通知给用户。

了解上传请求

出站恶意软件扫描策略定义 Web 代理是否阻止将数据上传到服务器的事务（上传请求）的 HTTP 请求和已解密 HTTPS 连接。上传请求是在请求正文中具有内容的 HTTP 请求或已解密 HTTPS 请求。

当 Web 代理收到上传请求时，它将该请求与出站恶意软件扫描策略组进行比较，确定要应用的策略组。在它将请求分配到策略组之后，它将该请求与策略组的已配置控制设置进行比较，确定是阻止请求还是监控请求。当出站恶意软件扫描策略确定要监控请求时，将根据访问策略评估该请求，并且 Web 代理对该请求采取的最终操作由适用的访问策略确定。

注释 尝试上传大小为零 (0) 字节的文件的上传请求不会根据出站恶意软件扫描策略进行评估。

组成员的条件

每个客户端请求都会分配到一个身份，然后根据其他策略类型进行评估，以确定其针对每个类型属于哪个策略组。Web代理根据请求的策略组成员身份将已配置的策略控制设置应用于此客户端请求。

Web 代理遵循特定过程来匹配组成员身份条件。Web 代理对组成员身份考虑以下因素：

条件	说明
标识配置文件	每个客户端请求要么与**标识配置文件**相匹配，要么未通过身份验证并被授予访客访问权限，要么未通过身份验证并被终止。
授权用户	如果所分配的**标识配置文件**要求执行身份验证，则用户必须包含在出站恶意软件扫描策略组中的授权用户列表中才能与策略组进行匹配。授权用户列表可以是任何指定的组或用户，如果**标识配置文件**允许访客访问，则也可以是访客用户。
高级选项	您可以配置出站恶意软件扫描策略组成员身份的多个高级选项。某些选项（例如，代理端口和URL类别）也可在**标识配置文件**内定义。在**标识配置文件**中配置高级选项后，该高级选项在出站恶意软件扫描策略组级别中不可配置。

将客户端请求与出站恶意软件扫描策略组相匹配

Web 代理将上传请求状态与第一个策略组的成员身份条件进行比较。如果匹配，Web 代理应用该策略组的策略设置。

如果不匹配，Web 代理将上传请求与下一个策略组进行比较。Web 代理会继续此过程，直到它将上传请求与用户定义的策略组匹配。如果 Web 代理与用户定义的策略组不匹配，则与全局策略组匹配。当 Web 代理将上传请求与策略组或全局策略组相匹配时，它将应用该策略组的策略设置。

创建出站恶意软件扫描策略

您可以根据多个条件的组合（例如，一个或多个身份或目标站点的URL类别）创建出站恶意软件扫描策略组。必须至少为策略组成员身份定义一个条件。当您定义多个条件时，上传请求必须满足所有条件才能匹配策略组。但是，上传请求只需与一个已配置身份匹配。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 出站恶意软件扫描 (Outbound Malware Scanning)**。

步骤 2 点击**添加策略 (Add Policy)**。

步骤 3 输入策略组的名称和可选说明。

注释 每个策略组名称都必须唯一，并且仅包含字母数字字符或空格字符。

步骤 4 在“插入到策略上面”(Insert Above Policy) 字段中，选择需要将策略组放入到策略表中的哪个位置。

当配置多个策略组时，必须为每个组指定逻辑顺序。

步骤 5 在**身份和用户 (Identities and Users)** 部分中，选择要应用到此策略组的一个或多个身份组。

步骤 6 （可选）展开“高级”(Advanced) 部分，定义其他成员身份要求。

步骤 7 要通过任何高级选项来定义策略组成员身份，请点击高级选项的链接并在显示的页面上配置选项。

高级选项	说明
协议 (Protocols)	选择是否按照客户端请求中使用的协议来定义策略组成员身份。选择要包括的协议。 “所有其他”(All others) 表示此选项上未列出的任何协议。 注释 当 HTTPS 代理启用时，只有解密策略应用于 HTTPS 事务。您无法通过 HTTPS 协议为访问、路由、出站恶意软件扫描、数据安全或外部 DLP 策略定义策略成员身份。
代理端口 (Proxy Ports)	选择是否按照用于访问Web代理的代理端口来定义策略组成员身份。在“代理端口”(Proxy Ports) 字段中输入一个或多个端口号。使用逗号分隔多个端口。 对于显式转发连接，此代理端口为浏览器中配置的端口。对于透明连接，此代理端口与目标端口为同一端口。 当客户端请求透明地重定向到设备时，如果您通过代理端口定义策略组成员身份，则某些请求会被拒绝。 注释 如果与此策略组关联的身份按此高级设置定义身份成员身份，不会在非身份策略组级别配置此设置。
子网 (Subnets)	选择是否按子网或其他地址定义策略组成员身份。 您可以选择使用能够借助相关身份定义的地址，或者可以在此处输入特定地址。 注释 如果与此策略组关联的身份按地址定义其成员身份，则在此策略组中，您输入的地址必须是身份中定义的地址的子集。在策略组中添加地址会进一步缩小与此策略组匹配的事务列表的范围。

高级选项	说明
URL 类别 (URL Categories)	选择是否按 URL 类别定义策略组成员身份。选择用户定义的或预定义的 URL 类别。 **注释** 如果与此策略组关联的身份按此高级设置定义身份成员身份，不会在非身份策略组级别配置此设置。
用户代理 (User Agents)	选择是否要按在客户端请求中使用的用户代理（诸如更新程序和 Web 浏览器等客户端应用）来定义策略组成员身份。可以选择某些通常定义的用户代理，或者使用正则表达式定义自己的用户代理。指定成员身份定义仅包括选定的用户代理，还是专门排除了选定的用户代理。 **注释** 如果与此策略组关联的**标识配置文件 (Identification Profile)** 通过此高级设置定义了**标识配置文件 (Identification Profile)** 成员身份，则不会在非**标识配置文件 (Identification Profile)** 策略组级别配置此设置。
用户位置 (User Location)	选择是否按照用户位置（不管是远程还是本地）来定义策略组成员身份。

步骤 8 提交更改。

步骤 9 配置出站恶意软件扫描策略组控制设置以定义 Web 代理如何处理事务。

新的出站恶意软件扫描策略组自动继承全局策略组设置，直到您为每个控制设置配置选项。

步骤 10 “提交”(Submit) 并“确认更改”(Commit Changes)。

控制上传请求

每个上传请求均分配到出站恶意软件扫描策略组并继承该策略组的控制设置。Web 代理收到上传请求报头后，Web 代理即具有必要的信息，可决定其是否应扫描请求正文。DVS 引擎扫描请求并将判定返回到 Web 代理。如果适用，将向最终用户显示阻止页面。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 出站恶意软件扫描 (Outbound Malware Scanning)**。

步骤 2 在**目标 (Destinations)** 列中，点击要配置的策略组的链接。

步骤 3 在**编辑目标设置 (Edit Destination Settings)** 部分中，从下拉菜单中选择**定义目标扫描自定义设置 (Define Destinations Scanning Custom Settings)**。

步骤 4 在**要扫描的目标 (Destinations to Scan)** 部分中，选择以下选项之一：

选项	说明
不扫描任何上传 (Do not scan any uploads)	DVS 引擎不扫描任何上传请求。所有上传请求都根据访问策略进行评估
扫描所有上传内容 (Scan all uploads)	DVS 引擎扫描所有上传请求。根据访问策略阻止或评估上传请求，具体取决于 DVS 引擎扫描判定。

选项	说明
扫描属于指定的自定义 URL 类别的上传内容 (Scan uploads to specified custom URL categories)	DVS 引擎扫描属于特定自定义 URL 类别的上传请求。根据访问策略阻止或评估上传请求，具体取决于 DVS 引擎扫描判定。 点击**编辑自定义类别列表 (Edit custom categories list)** 以选择要扫描的 URL 类别

步骤 5 提交更改。

步骤 6 在**防恶意软件过滤 (Anti-Malware Filtering)** 列中，点击策略组的链接。

步骤 7 在**防恶意软件设置 (Anti-Malware Settings)** 部分中，选择**定义防恶意软件自定义设置 (Define Anti-Malware Custom Settings)**。

步骤 8 在**思科 DVS 防恶意软件设置 (Cisco DVS Anti-Malware Settings)** 部分中，选择要为此策略组启用的防恶意软件扫描引擎。

步骤 9 在**恶意软件类别 (Malware Categories)** 部分中，选择是监控还是阻止各种恶意软件类别。

此部分中列出的类别取决于启用哪些扫描引擎。

注释 当达到配置的最大时间设置或者当系统遇到暂时性错误状况时，URL 事务分类为不可扫描。例如，事务可能在扫描引擎更新或 AsyncOS 升级期间分类为不可扫描。恶意软件扫描判定 SV_TIMEOUT 和 SV_ERROR 被视为不可扫描的事务。

步骤 10 “提交”(Submit) 并“确认更改”(Commit Changes)。

DVS 扫描的日志记录

访问日志表明DVS引擎是否扫描了恶意软件的上传请求。每个访问日志条目的扫描判定信息部分都包含已扫描的上传内容的 DVS 引擎活动的值。您还可以将其中一个字段添加到 W3C 或访问日志，以更轻松地查找此 DVS 引擎活动：

表 *1: W3C* 日志中的日志字段和访问日志中的格式说明符

W3C 日志字段	访问日志中的格式说明符
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

当 DVS 引擎将上传请求标记为恶意软件，并且其配置为阻止恶意软件上传时，访问日志中的 ACL 决策标记为 BLOCK_AMW_REQ。

但是，当DVS引擎将上传请求标记为恶意软件，并且其配置为监控恶意软件上传时，访问日志中的 ACL 决策标记实际由应用于事务的访问策略确定。

要确定DVS引擎是否扫描了恶意软件的上传请求，请在每个访问日志条目的扫描判定信息部分中查看 DVS 引擎活动的结果。

第 14 章

配置安全服务

本章包含以下部分：

配置安全服务概述

网络安全设备使用安全组件保护最终用户免遭各种恶意软件威胁。可以配置各策略组的防恶意软件和 Web 信誉设置。配置访问策略时，也可以让 AsyncOS for Web 选择确定阻止内容时要用的防恶意软件扫描和 Web 信誉分数组合。

为保护最终用户免受恶意软件威胁，启用设备上的这些功能，然后按照策略配置防恶意软件和 Web 信誉设置。

选项	说明	链接
防恶意软件扫描 (Anti-malware scanning)	与集成于设备上的多个防恶意软件扫描引擎配合工作来阻止恶意软件威胁	防恶意软件扫描概述， 第 222 页
Web 信誉过滤器 (Web Reputation Filters)	分析 Web 服务器行为并确定 URL 是否包含基于 URL 的恶意软件	Web 信誉过滤器概述， 第 220 页
高级恶意软件防护 (Advanced Malware Protection)	通过评估文件信誉和分析文件特性防范已下载文件中的威胁。	文件信誉过滤和文件分析概述， 第 233 页

相关主题

- 启用防恶意软件和信誉过滤器， 第 225 页
- 了解自适应扫描， 第 225 页

Web 信誉过滤器概述

Web 信誉过滤器将基于 Web 的信誉分数 (WBRS) 分配至 URL，确定其包含基于 URL 的恶意软件的可能性。网络安全设备使用 Web 信誉分数在恶意软件攻击发生前进行识别和停止。可以将 Web 信誉过滤器与访问策略、解密策略和思科数据安全策略结合使用。

Web 信誉分数

Web 信誉过滤器使用数据评估互联网域可靠性并对 URL 信誉进行评分。Web 信誉计算会将 URL 与网络参数相关联，以确定存在恶意软件的可能性。然后得出的恶意软件存在的综合可能性会映射为一个 -10 到 +10 之间的网络信誉分数，+10 为最不可能包含恶意软件。

示例参数包括：

- URL 类别数据
- 存在的可下载代码
- 存在的冗长且含混的最终用户许可协议 (EULA)
- 全局量和量的变化
- 网络所有者信息
- URL 的历史记录
- URL 的时长
- 存在于任何阻止列表上
- 存在于任何允许列表上
- 常用域的 URL 拼写错误
- 域注册商信息
- IP 地址信息

注释 思科不会收集用户名、密码或客户端 IP 地址等身份信息。

了解 Web 信誉过滤工作方式

Web 信誉分数与处理 URL 请求的操作相关联。可以配置各策略组将操作与特定 Web 信誉分数相关联。可用操作取决于分配至 URL 请求的策略组类型：

策略类型	操作
访问策略	可以选择阻止、扫描或允许
解密策略	可以选择丢弃、解密或通过
思科数据安全策略	可以选择阻止或监控

访问策略中的 Web 信誉

在访问策略中配置 Web 信誉设置时，可以选择手动配置设置，或者使用自适应扫描使 AsyncOS for Web 选择最佳选项。启用自适应扫描后，可以启用或禁用各访问策略中的 Web 信誉过滤，但无法编辑 Web 信誉分数。

分数	操作	说明	示例
-10 到 -6.0	阻止	恶意站点。请求被阻止，未发生进一步的恶意软件扫描。	• URL 下载信息，但未经用户许可。 • URL 容量突然达到峰值。 • URL 为常见域拼写错误。
-5.9 到 5.9	扫描	未确定站点。请求被传递至 DVS 引擎，进行进一步恶意软件扫描。DVS 引擎扫描请求和服务器响应内容。	• 具有动态 IP 地址并且包含可下载内容的最近创建的 URL。 • 具有正 Web 信誉分数的网络所有者 IP 地址。
6.0 到 10.0	允许	良好站点。允许请求。无需恶意软件扫描。	• URL 不包含可下载的内容。 • 具有悠久历史的信誉良好、高容量域。 • 域存在于若干允许列表上。 • 没有转至信誉不佳 URL 的链接。

默认情况下，允许 HTTP 请求中被分配 +7 Web 信誉分数且无需进一步扫描的 URL。然而，较弱的 HTTP 请求分数（如 +3）会被自动转发至 Cisco DVS 引擎，在此进行恶意软件扫描。阻止信誉较差的 HTTP 请求中的任何 URL。

相关主题

- 了解自适应扫描，第 225 页

解密策略中的 Web 信誉

分数	操作	描述
-10 到 -9.0	丢弃	恶意站点。删除请求，但未向最终用户发送通知。慎用此设置。

分数	操作	描述
-8.9 到 5.9	解密	未确定站点。允许请求，但解密连接，并将访问策略应用于解密流量。
6.0 到 10.0	通过	良好站点。请求通过，但未检查或解密。

思科数据安全策略中的 Web 信誉

分数	操作	说明
-10 到 -6.0	阻止	恶意站点。事务被阻止，未发生进一步扫描。
-5.9 到 0.0	监控	将不会基于 Web 信誉对事务进行阻止，并将进行内容检查（文件类型和大小）。 **注释** 监控无分数站点。

防恶意软件扫描概述

网络安全设备防恶意软件功能将 Cisco DVS™ 引擎与防恶意软件扫描引擎结合使用，停止基于 Web 的恶意软件威胁。DVS 引擎与 Webroot™、McAfee 和 Sophos 防恶意软件扫描引擎配合使用。

扫描引擎检查事务，确定恶意软件扫描判定并将其传递到 DVS 引擎。DVS 引擎根据恶意软件扫描判定确定是否监控或阻止请求。要使用设备的防恶意软件组件，必须启用防恶意软件扫描和配置全局设置，然后将特定设置应用于不同策略。

相关主题

- 启用防恶意软件和信誉过滤器，第 225 页
- 了解自适应扫描，第 225 页
- McAfee 扫描，第 223 页

了解 DVS 引擎工作方式

DVS 引擎对从 Web 信誉过滤器转发的 URL 事务进行防恶意软件扫描。Web 信誉过滤器计算特定 URL 包含恶意软件的可能性，并分配与操作相关联的 URL 分数以阻止、扫描或允许事务。

如果分配的 Web 信誉分数指示扫描事务，则 DVS 引擎接收 URL 请求和服务器响应内容。与 Webroot 和/或 Sophos 或 McAfee DVS 引擎结合使用的 DVS 引擎返回恶意软件扫描判定。DVS 引擎使用恶意软件扫描判定和“访问策略”(Access Policy) 设置中的信息确定是否阻止内容或将内容传递给客户端。

使用多个恶意软件判定

DVS 引擎可以确定单一 URL 的多个恶意软件判定。多个判定可以来自一台或两台已启用的扫描引擎：

- **来自不同扫描引擎的不同判定**。启用 Webroot 和 Sophos/McAfee 后，对于同一对象，各扫描引擎可能返回不同的恶意软件判定。如果对于一个 URL，两台已启用扫描引擎返回多个判定，则设备执行最受限制的操作。例如，如果一台扫描引擎返回阻止判定，而另一台返回监控判定，则 DVS 引擎总是阻止请求。
- **来自同一扫描引擎的不同判定**。如果某单个对象包含多重感染，则用于该对象的扫描引擎可能返回多个判定。如果对于一个 URL，同一扫描引擎返回多个判定，则设备按照优先级最高的判定操作。下文按照最高到最低优先级列出可能的恶意软件扫描判定。
- 病毒
- 特洛伊木马下载程序
- 特洛伊木马
- 特洛伊木马钓鱼程序
- 劫持程序
- 系统监视程序
- 商业系统监视程序
- 拨号程序
- 蠕虫
- 浏览器助手对象
- 网络钓鱼 URL
- 广告软件
- 加密文件
- 不可扫描
- 其他恶意软件

Webroot 扫描

Webroot 扫描引擎检查对象，确定要发送至 DVS 引擎的恶意软件扫描判定。Webroot 扫描引擎检查以下对象：

- **URL 请求**。Webroot 评估 URL 请求，确定 URL 是否为疑似恶意软件。如果 Webroot 怀疑该 URL 响应可能包含恶意软件，则设备监控或阻止请求，这取决于如何配置设备。如果 Webroot 评估清除请求，则设备会提取 URL 并且扫描服务器响应。
- **服务器响应**。设备提取 URL 时，Webroot 扫描服务器响应并将其与 Webroot 签名数据库比较。

McAfee 扫描

McAfee 扫描引擎检查从 HTTP 响应中的 Web 服务器中所下载的对象。检查对象后，将恶意软件扫描判定传递至 DVS 引擎，使 DVS 引擎能够确定是监控还是阻止请求。

McAfee 扫描引擎使用以下方法确定恶意软件扫描判定：

- 匹配病毒特征模式
- 启发式分析

匹配病毒特征模式

McAfee将其数据库中的病毒定义与扫描引擎配合使用，检测特定病毒、病毒类型或其他可能不需要的软件。其搜索文件中的病毒特征。启用 McAfee 后，McAfee 扫描引擎使用该方法扫描服务器响应内容。

启发式分析

启发式分析是使用一般规则而不是特定规则检测新病毒和恶意软件的一种技术。当 McAfee 扫描引擎使用启发式分析时，它着眼于对象代码、应用通用规则并确定对象类似于病毒的可能性。

使用启发式分析会增加误报的可能性（干净内容被指定为病毒）并且可能影响设备性能。当启用 McAfee 时，可以选择是否在扫描对象时也启用启发式分析。

McAfee 类别

McAfee 判定	恶意软件扫描判定类别
已知病毒	病毒
特洛伊木马	特洛伊木马
笑话文件	广告软件
测试文件	病毒
自封为病毒	病毒
灭活	病毒
商业应用	商业系统监视程序
可能不需要的对象	广告软件
可能不需要的软件数据包	广告软件
加密文件	加密文件

Sophos 扫描

Sophos 扫描引擎检查 HTTP 响应中从 Web 服务器下载的对象。检查对象后，将恶意软件扫描判定传递至 DVS 引擎，使 DVS 引擎能够确定是监控还是阻止请求。如果已安装 McAfee 防恶意软件，则您可能想要启用 Sophos 扫描引擎而不是 McAfee 扫描引擎。

了解自适应扫描

自适应扫描决定哪台防恶意软件扫描引擎（包括用于下载文件的高级恶意软件保护扫描）将处理网络请求。

运行任何扫描引擎前，自适应扫描将“启发式爆发”防恶意软件类别应用至其识别为恶意软件的事务。当设备上配置防恶意软件设置时，您可以选择是否阻止这些事务。

自适应扫描和访问策略

启用自适应扫描后，可以在访问策略中配置的某些防恶意软件和信誉设置略有不同：

- 可以启用或禁用各访问策略中的 Web 信誉过滤，但无法编辑 Web 信誉分数。
- 可以启用各访问策略中的防恶意软件扫描，但无法选择要启用的防恶意软件扫描引擎。自适应扫描为各 Web 请求选择最适用的引擎。

注释 如果未启用自适应扫描且访问策略已配置特定 Web 信誉和防恶意软件设置，那么启用自适应扫描后，会覆盖所有现有 Web 信誉和防恶意软件设置。

逐个策略的高级恶意软件防护设置相同，而不论是否启用自适应扫描。

启用防恶意软件和信誉过滤器

开始之前

检查 Web 信誉过滤器、DVS 引擎以及 Webroot、McAfee 和 Sophos 扫描引擎是否已启用。默认情况下，应在系统设置期间启用这些项目。

步骤 1 依次选择**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 根据需要配置设置。

设置	说明
Web 信誉过滤 (Web Reputation Filtering)	选择是否启用 Web 信誉过滤。
自适应扫描	选择是否启用自适应扫描。仅在启用“Web 信誉过滤”(Web Reputation Filtering) 后，才可以启用“自适应扫描”(Adaptive Scanning)。
文件信誉过滤和文件分析：	请参阅启用和配置文件信誉和分析服务，第 240 页。

设置	说明
DVS 引擎对象扫描限制 (DVS Engine Object Scanning Limits)	指定扫描的最大/对象大小。 您指定的最大对象大小适用于可能由所有防恶意软件和防病毒扫描引擎以及高级恶意软件防护功能扫描的整个请求和响应大小。它还指定用于存档检查的可视察存档的最大大小。有关存档检查的详细信息，请参阅访问策略：阻止对象，第 185 页。 上传或下载大小超过该值时，安全组件可能中止正在进行的扫描，并可能不向 Web 代理提供扫描判定。如果可视察存档超过此大小，则标记为“扫描”。
Sophos	选择是否启用 Sophos 扫描引擎。
McAfee	选择是否启用 McAfee 扫描引擎。 启用 McAfee 扫描引擎时，可以选择是否启用启发式扫描。 **注释** 启发式分析可以增强安全防护，但会导致误报和降低性能。
Webroot	选择是否启用 Webroot 扫描引擎。 启用 Webroot 扫描引擎后，可以配置威胁风险阈值 (TRT)。TRT 指定恶意软件存在可能性的数值。 专有算法评估匹配序列的URL结果并指定威胁风险分级(TRR)。该值与威胁风险阈值设置相关联。如果 TRR 值大于或等于 TRT，则将该 URL 视为恶意软件并进行传递以供进一步处理。 **注释** 将威胁风险阈值设定为低于 90 的值会显著增加 URL 阻止率和拒绝合法请求。思科强烈建议保留 TRT 默认值 90。TRT 设置的最小值为 51。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

- 了解自适应扫描，第 225 页
- McAfee 扫描，第 223 页

在策略中配置防恶意软件和信誉

启用设备上的防恶意软件和信誉过滤器后，可以在策略组中配置不同的设置。可以根据恶意软件扫描判定启用对恶意软件类别的监控或阻止。

可以在以下策略组中配置防恶意软件设置：

策略类型	任务链接
访问策略	访问策略中的防恶意软件和信誉设置，第 227 页
出站恶意软件扫描策略	使用出站恶意软件扫描策略控制上传请求

可以在以下策略组中配置 Web 信誉设置：

策略类型	任务链接
访问策略	访问策略中的防恶意软件和信誉设置，第 227 页
解密策略	为解密策略组配置 Web 信誉过滤器设置，第 230 页
思科数据安全策略	为解密策略组配置 Web 信誉过滤器设置，第 230 页

仅可以在访问策略中配置“高级恶意软件防护”(Advanced Malware Protection) 设置。请参阅 配置文件信誉和分析功能，第 237 页

访问策略中的防恶意软件和信誉设置

启用自适应扫描时，可以为访问策略配置的 Web 信誉和防恶意软件设置与关闭自适应扫描时的设置略有不同。

注释 如果部署包括安全管理设备并且在主配置中配置了该功能时，此页面上的选项取决于是否为相关主配置启用自适应安全。在“**网络**”**(Web)**>“**实用程序**”**(Utilities)**>“**安全服务显示**”**(Security Services Display)** 页面上检查安全管理设备相关设置。

- 了解自适应扫描，第 225 页

启用自适应扫描后配置防恶意软件和信誉设置

步骤 1 依次选择**网络安全管理器 (Web Security Manager)** > **访问策略 (Access Policies)**。

步骤 2 点击要配置的访问策略**防恶意软件和信誉 (Anti-Malware and Reputation)**链接。

步骤 3 在 **Web 信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)** 部分下，选择**定义 Web 信誉和防恶意软件自定义设置 (Define Web Reputation and Anti-Malware Custom Settings)**。

这让您能够为不同于全局策略的该访问策略配置 Web 信誉和防恶意软件设置。

步骤 4 在**Web 信誉设置 (Web Reputation Settings)** 部分中，选择是否启用 Web 信誉过滤。自适应扫描为各 Web 请求选择最适用的 Web 信誉分数。

步骤 5 在**高级恶意软件防护设置 (Advanced Malware Protection Settings)** 部分中配置设置。

步骤 6 向下滚动至“思科 DVS 防恶意软件设置”(Cisco DVS Anti-Malware Settings section) 部分。

步骤 7 根据需要配置策略的防恶意软件设置。

启用可疑用户代理扫描 (Enable Suspect User Agent Scanning)	选择是否基于 HTTP 请求头中指定的用户代理字段扫描流量。 选择该复选框后，可以选择监控或阻止页面底部“其他扫描”(Additional Scanning) 部分中的可疑用户代理。 **注释** Chrome 浏览器在 FTP-over-HTTP 请求中不包括用户代理字符串，因而，在这些请求中 Chrome 浏览器不会检测为用户代理。
启用防恶意软件扫描 (Enable Anti-Malware Scanning)	选择是否使用 DVS 引擎扫描恶意软件流量。自适应扫描为各网络请求选择最适用的引擎。
恶意软件类别数 (Malware Categories)	选择是否基于恶意软件扫描判定监控或阻止各种恶意软件类别。
其他类别 (Other Categories)	选择是监控还是阻止本部分中所列的对象和响应类型。 **注释** “病毒爆发启发式扫描”(Outbreak Heuristics) 类别适用于运行任何扫描引擎前由自适应扫描标识为恶意软件的事务。 **注释** 当达到配置的最大时间设置或者当系统遇到暂时性错误状况时，URL 事务分类为不可扫描。例如，事务可能在扫描引擎更新或 AsyncOS 升级期间分类为不可扫描。恶意软件扫描判定 SV_TIMEOUT 和 SV_ERROR 被视为不可扫描的事务。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

- 了解自适应扫描，第 225 页

禁用自适应扫描后配置防恶意软件和信誉设置

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要配置的访问策略**防恶意软件和信誉 (Anti-Malware and Reputation)**链接。

步骤 3 在 **Web 信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)** 部分下，选择**定义 Web 信誉和防恶意软件自定义设置 (Define Web Reputation and Anti-Malware Custom Settings)**。

这让您能够为不同于全局策略的该访问策略配置 Web 信誉和防恶意软件设置。

步骤 4 在 **Web 信誉设置 (Web Reputation Settings)** 部分中配置设置。

步骤 5 在**高级恶意软件防护设置 (Advanced Malware Protection Settings)** 部分中配置设置。

步骤 6 向下滚动至“思科 DVS 防恶意软件设置”(Cisco DVS Anti-Malware Settings section) 部分。

步骤 7 根据需要配置策略的防恶意软件设置。

注释 启用 Webroot、Sophos 或 McAfee 扫描后，可以选择监控或阻止此页面上的“恶意软件”(Malware) 类别中的某些其他类别。

设置	说明
启用可疑用户代理扫描 (Enable Suspect User Agent Scanning)	选择是否基于 HTTP 请求头中指定的用户代理字段来启用设备扫描流量。 选择该复选框后，可以选择监控或阻止页面底部“其他扫描”(Additional Scanning) 部分中的可疑用户代理。 注释 Chrome 浏览器在 FTP-over-HTTP 请求中不包括用户代理字符串，因而，在这些请求中 Chrome 浏览器不会检测为用户代理。
启用 Webroot (Enable Webroot)	选择扫描流量时是否启用设备使用 Webroot 扫描引擎。
启用 Sophos 或 McAfee (Enable Sophos or McAfee)	选择扫描流量时是否启用设备使用 Sophos 或 McAfee 扫描引擎。
恶意软件类别数 (Malware Categories)	选择是否基于恶意软件扫描判定监控或阻止各种恶意软件类别。此部分中列出的类别取决于上文中所启用的扫描引擎。
其他类别 (Other Categories)	选择是监控还是阻止本部分中所列的对象和响应类型。 注释 当达到配置的最大时间设置或者当系统遇到暂时性错误状况时，URL 事务分类为不可扫描。例如，事务可能在扫描引擎更新或 AsyncOS 升级期间分类为不可扫描。恶意软件扫描判定 SV_TIMEOUT 和 SV_ERROR 被视为不可扫描的事务。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

- 为访问策略配置 Web 信誉分数阈值， 第 229 页
- 恶意软件类别说明， 第 231 页

配置 Web 信誉分数

安装和设置网络安全设备后，其具有 Web 信誉分数的默认设置。但是可以根据贵组织需求修改 Web 信誉分数阈值设置。可以为各策略组配置 Web 信誉过滤器设置。

为访问策略配置 Web 信誉分数阈值

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要编辑的访问策略组的**防恶意软件和信誉 (Anti-Malware and Reputation)** 列下的链接。

步骤 3 在 **Web 信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)** 部分下，选择**定义 Web 信誉和防恶意软件自定义设置 (Define Web Reputation and Anti-Malware Custom Settings)**。

这让您能够为不同于全局策略的该访问策略配置 Web 信誉和防恶意软件设置。

步骤 4 验证是否启用了**启用 Web 信誉过滤 (Enable Web Reputation Filtering)** 字段。

步骤 5 移动标记更改 URL 阻止、扫描和允许操作的范围。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

注释 禁用自适应扫描后，可以编辑访问策略中的 Web 信誉分数阈值。

为解密策略组配置 Web 信誉过滤器设置

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 解密策略 (Decryption Policies)**。

步骤 2 点击要编辑的解密策略组的“Web 信誉”(Web Reputation) 列下的链接。

步骤 3 在**Web 信誉设置 (Web Reputation Settings)** 部分下，选择**定义 Web 信誉自定义设置 (Define Web Reputation Custom Settings)**。这让您能够覆盖全局策略组的 Web 信誉设置。

步骤 4 验证是否选择**启用 Web 信誉过滤 (Enable Web Reputation Filtering)** 字段。

步骤 5 移动标记更改 URL 丢弃、解密和通过操作的范围。

步骤 6 在**无分数站点 (Sites with No Score)** 字段中，选择要对未指定 Web 信誉分数的站点处理请求的操作。

步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

为数据安全策略组配置 Web 信誉过滤器设置

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 思科数据安全 (Cisco Data Security)**。

步骤 2 点击要编辑的数据安全策略组的“Web 信誉”(Web Reputation) 列下的链接。

步骤 3 在**Web 信誉设置 (Web Reputation Settings)** 部分下，选择**定义 Web 信誉自定义设置 (Define Web Reputation Custom Settings)**。

这让您能够覆盖全局策略组的 Web 信誉设置。

步骤 4 移动标记更改 URL 阻止和监控操作的范围。

步骤 5 “提交”(Submit) 并“确认更改”(Commit Changes)。

注释 仅可为思科数据安全策略的 Web 信誉阈值设置配置负值和零值。根据定义，所有正值分数都会进行监控

维护数据库表

Web 信誉、Webroot、Sophos 和 McAfee 数据库定期从思科更新服务器接收更新。服务器更新自动完成且更新间隔由服务器设置。

Web 信誉服务器

网络安全设备维护过滤数据库，其中包含统计信息以及如何处理不同类型请求的相关信息。也可以将设备配置为发送 Web 信誉统计信息至 Cisco SensorBase 网络服务器。通过 SensorBase 网络的数据馈送可以利用 SensorBase 服务器信息，并且该信息用于生成 Web 信誉分数。

对 Web 信誉过滤活动和 DVS 扫描的日志记录

访问日志文件记录 Web 信誉过滤器和 DVS 引擎返回的各事务信息。访问日志中的扫描判定信息部分包括许多字段，有助于了解应用于事务的操作的原因。例如，某些字段显示传送至 DVS 引擎的 Web 信誉分数和恶意软件扫描判定 Sophos。

日志记录自适应扫描

访问日志中的自定义字段	W3C 日志中的自定义字段	说明
%X6	x-as-malware-threat-name	自适应扫描返回的防恶意软件名称。如果未阻止事务，则该字段返回连字符（“-”）。此变量包含在扫描判定信息中（在每个访问日志条目末尾的尖括号内）。

自适应扫描引擎阻止和监控的事务使用 ACL 决策标签：

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

缓存

以下准则介绍 AsyncOS 扫描恶意软件时如何使用缓存：

- 如果整个对象下载完成，则 AsyncOS 仅缓存对象。如果扫描期间阻止恶意软件，则不会下载整个对象，因此不被缓存。
- AsyncOS 扫描是否从服务器或网络缓存检索内容。
- 内容缓存时间长短因许多因素而异 - 无默认值。
- 特征更新后，AsyncOS 重新扫描内容。

恶意软件类别说明

恶意软件类型	说明
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。这些程序也可能更改安全设置，使得用户无法对其系统设置进行更改。

恶意软件类型	说明
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供完全许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未同意的情况下，将用户引导至一个网站或运行一个程序。
已知的恶意文件和高风险文件	这些文件是被高级恶意软件防护文件信誉服务标识为威胁的文件。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
网络钓鱼 URL	网络钓鱼URL显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。
PUA	可能不需要的应用。PUA是非恶意应用，但可能被视为不想要的应用。
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： • 公开地或隐蔽地记录系统进程和/或用户操作。 • 使这些记录可用于以后检索和审核。
特洛伊木马下载程序	特洛伊木马下载程序是一种木马程序，在安装后，会与远程主机/站点联系，并安装来自远程主机的程序包或附属程序。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可以扫描受感染的计算机来查找用户名和密码。
病毒	病毒是未经您确认就加载到您的计算机上的程序或代码段。
蠕虫	蠕虫是通过计算机网络自我复制的程序或算法，而且执行恶意操作。

第 15 章

文件信誉过滤和文件分析：

本章包含以下部分：

文件信誉过滤和文件分析概述

高级恶意软件防护通过如下方式防范中的零日威胁和基于文件的针对性威胁：

- 获取已知文件的信誉。
- 分析尚不为信誉服务所知的某些文件行为。
- 在获得新信息时持续评估新出现的威胁，并在确定为威胁的文件进入您的网络后通知您。

此功能可用于文件下载。上传的文件。

文件信誉服务在云中。文件分析服务提供适用于公共云或私有云（本地）的选项。

- 私有云文件信誉服务由思科 AMP 虚拟私有云设备提供，在“proxy”或“air-gap”（本地）模式下运行。请参阅配置本地文件信誉服务器，第 239 页。
- 私有云文件分析服务由本地思科 AMP Threat Grid 设备提供。请参阅配置本地文件分析服务器，第 240 页。

文件威胁判定更新

威胁判定可以随着新信息的出现而更改。文件最初可能会被评定为未知或正常，然后，可能允许用户访问文件。。如果获得新信息时威胁判定更改，您会收到警报，且文件及其新判定将出现在 AMP 判定更新报告中。可以调查进入点消息事务，作为补救任何威胁影响的起点。

判定还可能从恶意更改为干净。

当设备处理同一文件的后续实例时，系统将立即应用已更新的判定。

有关判定更新的定时信息包括在文件信誉和分析服务所支持的文件，第 235 页中引用的文件条件文档中。

相关主题

- 文件信誉和文件分析报告与跟踪，第 246 页
- 在文件威胁判定更改时采取操作，第 249 页

文件处理概述

首先，根据基于 Web 的信誉服务 (WBRS) 评估文件下载网站。

如果该站点的 Web 信誉分数处于配置为“扫描”(Scan) 的范围内，设备会同时扫描事务是否存在恶意软件并向基于云的服务查询文件的信誉。（如果该站点的信誉分数处于“阻止”[Block] 范围内，设备会相应地处理事务，无需进一步处理文件。）如果在扫描过程中发现恶意软件，则无论文件的信誉如何，都将阻止事务。

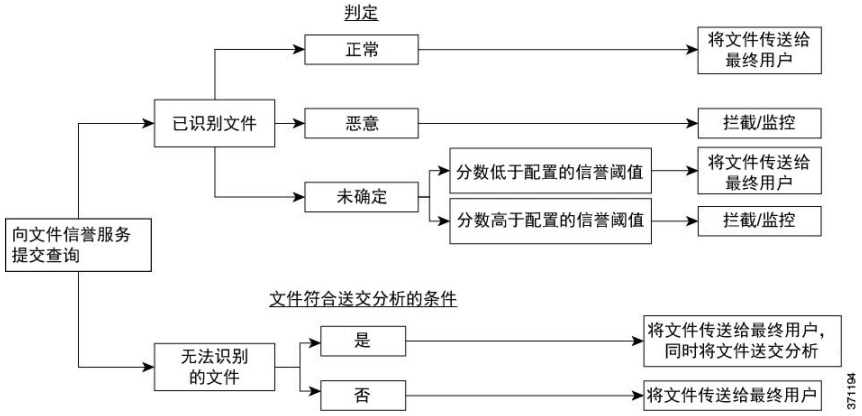
如果还启用了自适应扫描，则会在自适应扫描中包含文件信誉评估和文件分析。

设备和文件信誉服务之间的通信已加密并已防止篡改。

评估文件的信誉后：

- 如果文件为文件信誉服务所熟知且被确定为正常，则将文件发送至最终用户 。
- 对于，如果文件信誉服务返回恶意判定，则设备应用您为此类文件指定的操作。
- 如果文件为信誉服务所知但信息不足以作出最后判定，则信誉服务基于文件特征（例如威胁指纹和行为分析）返回威胁得分。如果此分数达到或超过所配置的信誉阈值，则设备将应用您在访问策略中为恶意或高危文件所配置的操作。
- 如果信誉服务没有文件相关信息，且文件不符合分析标准（请参阅文件信誉和分析服务所支持的文件，第 235 页），则将文件视为正常并且文件释放给最终用户。
- 如果已启用基于云的文件分析服务，信誉服务没有文件相关信息且文件符合可以分析的文件的标准（请参阅文件信誉和分析服务所支持的文件，第 235 页），则将文件视为正常并将文件送交分析。
- 对于具备本地文件分析的部署，信誉评估和文件分析同时进行。如果信誉服务返回判定结果，则使用该判定结果，这是因为信誉服务包含的信息具有更为广泛的来源。如果文件对于信誉服务来说是未知的，则会将该文件释放给用户，但会在本地缓存中更新文件分析结果，并使用该结果来评估该文件的未来实例。
- 如果因为与服务器的连接超时而导致文件信誉判定信息不可用，则将该文件视为“不可扫描”，并应用配置的操作。

图 *8:* 面向云文件分析部署的高级恶意软件防护工作流程



如果将文件送交分析：

- 如果将文件发送到云进行分析：文件将通过 HTTPS 发送。
- 分析通常需要数分钟，但可能更长。
- 在文件分析后标记为恶意的文件可能不会被信誉服务识别为恶意文件。文件信誉由一段时间内的多种因素确定，而不一定由单一的文件分析判定来确定。
- 使用本地 Cisco AMP Threat Grid 设备分析文件的结果将缓存在本地。

有关判定更新的信息，请参阅文件威胁判定更新，第 233 页。

文件信誉和分析服务所支持的文件

信誉服务会评估大多数文件类型。文件类型识别由文件内容确定，并且不取决于文件扩展名。

可以分析某些信誉未知的文件来查找威胁特征。在配置文件分析功能时，选择要分析的文件类型。可以动态添加新类型；当可上传的文件类型列表变化时，则会收到警报，并可以选择添加的文件类型进行上传。

有关信誉及分析服务支持哪些文件的详细信息只向注册思科客户提供。有关评估和分析哪些文件的信息，请参阅可从以下网址获取的《思科内容安全产品高级恶意软件保护服务的文件条件：http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html。评估文件信誉和文件送交分析的标准可能随时变更。

要访问此文档，您必须拥有一个含有支持合同的思科客户帐户。要注册帐户，请访问 https://tools.cisco.com/RPF/register/register.do。

安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation) 页面上 **DVS 引擎对象扫描限制 (DVS Engine Object Scanning Limits)** 的设置还可确定文件信誉和分析的最大文件大小。

您应将策略配置为阻止下载不是由高级恶意软件保护处理的文件。

注释 已从源上传以进行分析的文件（传入邮件或传出邮件中的文件）不会再次上传。要查看此类文件的分析结果，请在“文件分析”(File Analysis) 报告页面中搜索 SHA-256。

相关主题

- 启用和配置文件信誉和分析服务，第 240 页
- 确保接收有关高级恶意软件防护问题的警报，第 245 页
- 存档或压缩文件处理，第 236 页

存档或压缩文件处理

如果文件已压缩或存档，

- 则系统会评估压缩或存档文件的信誉。

有关检查哪些存档和压缩文件的信息（包括文件格式），请参阅文件信誉和分析服务所支持的文件，第 235 页链接的信息。

在此情景中，

- 如果提取的其中一个文件是恶意的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。
- 如果压缩或存档文件是恶意的，并且所有已提取文件都是干净的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。
- 如果判定任何提取的文件为未知文件，则可以选择将提取的文件送交分析（如果已配置该功能且文件分析支持该文件类型）。
- 如果在对压缩或存档文件解压缩时文件提取失败，则文件信誉服务会针对压缩或存档文件返回“不可扫描”判定。请记住，在此情景中，如果提取的其中一个文件是恶意的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定（“恶意”判定优先于“不可扫描”判定）。

注释 系统不会评估具有安全 MIME 类型（例如文本/纯文本）的已提取文件的信誉。

发送到云端的信息的隐私性

- 只有唯一标识文件的 SHA 才会发送到云端的信誉服务。不会发送文件本身。
- 如果使用云端的文件分析服务，并且文件符合分析条件，则该文件本身将发送到云端。
- 有关每个发送到云端进行分析并且判定为“恶意”的文件的信息将添加到信誉数据库中。此信息与其他数据共同用于确定信誉分数。

  有关现场 Cisco AMP Threat Grid 设备所分析文件的信息不会与信誉服务共享。

配置文件信誉和分析功能

与文件信誉和分析服务通信的要求

- 所有使用这些服务的网络安全设备都必须能通过互联网直接与其连接（不包括配置为使用现场思科 AMP Threat Grid 设备的文件分析服务）。
- 默认情况下，与文件信誉和分析服务的通信通过设备上的管理端口 (M1) 进行路由。如果设备并未通过管理端口路由数据，请参阅通过数据接口将流量路由至文件信誉和文件分析服务器， 第 238 页。
- 默认情况下，通过与默认网关相关联的接口来路由与文件信誉分析服务和基于云的分析服务的通信。要通过其他接口路由此流量，请在“安全服务”(Security Services) > “文件信誉和分析”(File Reputation and Analysis) 页面的“高级”(Advanced) 部分中为每个地址创建静态路由。
- 必须打开以下防火墙端口：

防火墙端口	说明	协议	输入/输出	主机名	设备接口
32137（默认）或 443	访问云服务获取文件信誉。	TCP	输出	如在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分：文件信誉高级设置的云服务器池参数中所配置的一样。	管理，除非将静态路由配置为通过数据端口路由该流量。
443	访问云服务以进行文件分析。	TCP	输出	如在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分：文件分析高级设置中所配置的一样。	

- 配置文件信誉功能时，选择是否通过端口 443 使用 SSL。

相关主题

- 启用和配置文件信誉和分析服务，第 240 页

通过数据接口将流量路由至文件信誉和文件分析服务器

如果设备配置为仅限通过管理端口处理设备管理服务（位于**网络 (Network) > 接口 (Interfaces)** 页面），请配置设备，改为通过数据端口路由文件信誉和分析流量。

在“网络”(Network)>“路由”(Routes) 页面上添加数据流量的路由。有关一般要求和说明，请参阅配置 TCP/IP 通信路由，第 29 页

连接对象	目标网络	Gateway
文件信誉服务	在“安全服务”(Security Services) >“防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分 >“文件信誉的高级设置”(Advanced Settings for File Reputation) 部分中，提供 **文件信誉服务器 (File Reputation Server)** 的名称 (URL) 和云服务器池的**云域 (Cloud Domain)** 名称。 如果选择“私有云”作为文件信誉服务器，请输入服务器的主机名或 IP 地址，并提供有效的公钥。此密钥必须与私有云设备使用的密钥相同。 云服务器池的主机名，如在“安全服务”(Security Services) >“防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分 >“文件信誉的高级设置”(Advanced Settings for File Reputation) 部分中所配置的那样。	数据端口网关 IP 地址

连接对象	目标网络	Gateway
文件分析服务	• 在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分 > “文件分析的高级设置”(Advanced Settings for File Analysis) 部分，提供 **文件信誉服务器 (File Analysis Server)** 的名称 (URL)。 如果选择“私有云”作为文件分析服务器，请输入服务器 URL，并提供有效的证书颁发机构。 • 文件分析客户端 ID 是文件分析服务器上此设备的客户端 ID（只读）。 文件分析服务器主机名，如在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分 > “文件分析的高级设置”(Advanced Settings for File Analysis) 中所配置的那样。	数据端口网关 IP 地址

相关主题

- 配置 TCP/IP 通信路由， 第 29 页

配置本地文件信誉服务器

如果您将思科 AMP 虚拟私有云设备用作私有云文件分析服务器：

- 您可以从以下位置获得思科高级恶意软件保护虚拟私有云设备文档，包括安装和配置 FireAMP 私有云指南：
  http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html
  使用此文档执行本主题中介绍的任务。
  其他文件可从 AMP 虚拟私有云设备的“帮助”链接获取。
- 在“代理”或“空隙”（本地部署）模式中设置和配置思科 AMP 虚拟私有云设备。
- 确保思科 AMP 虚拟私有云设备软件版本为 2.2，该版本可与思科网络安全设备集成。
- 在该设备上下载 AMP 虚拟私有云证书和密钥，以便上传到此网络安全设备

注释 设置本地文件信誉服务器之后，您将从此网络安全设备配置与该服务器的连接；请参阅步骤 6 启用和配置文件信誉和分析服务， 第 240 页

配置本地文件分析服务器

如果您将 Cisco AMP Threat Grid 设备用作私有云文件分析服务器：

- 获取《思科 AMP Threat Grid 设备设置和配置指南》以及《思科 AMP Threat Grid 设备管理指南》。思科 AMP Threat Grid 设备文档可从 http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides%20-list.html 获取。

  使用此文档可执行本主题中描述的任务。

  使用 AMP Threat Grid 设备中的“帮助”(Help) 链接可获取其他文档。

  在《管理指南》中，请搜索有关下列所有各项的信息：与其他思科设备、CSA、思科沙盒APIWSA和网络安全设备的集成。

- 设置和配置思科 AMP Threat Grid 设备。
- 如果需要，请将思科 AMP Threat Grid 设备软件更新为版本 1.2.1，该版本支持与思科网络安全设备的集成。

  有关确定版本号和执行更新的说明，请参阅 AMP Thread Grid 文件。

- 确保您的设备能够通过您的网络彼此通信。思科网络安全设备必须能够连接到 AMP Threat Grid 设备的正常接口。
- 如果您要部署自签名证书：从思科 AMP Threat Grid 设备生成要在您的网络安全设备上使用的自签名 SSL 证书。请参阅 AMP Threat Grid 设备管理员指南中有关下载 SSL 证书和密钥的说明。请务必生成一个将 AMP Threat Grid 设备主机名作为 CN 的证书。来自 AMP Threat Grid 设备的默认证书不起作用。
- 当您提交用于文件分析的配置时，系统将自动向 Threat Grid 设备注册您的网络安全设备，如启用和配置文件信誉和分析服务，第 240 页中所述。但是，您必须按照同一程序中所述激活注册。

注释 在设置了内部部署分析服务器之后，您将从该网络安全设备配置与该服务器的连接；请参阅步骤 7 启用和配置文件信誉和分析服务，第 240 页

启用和配置文件信誉和分析服务

开始之前

- 获取文件信誉服务和文件分析服务的功能密钥，并将其传输到此设备。有关向设备中添加功能密钥的详细信息，请参阅使用功能密钥，第 382 页。
- 符合与文件信誉和分析服务通信的要求，第 237 页。
- 如果需要将“数据”(Data) 网络接口用于“文件信誉和分析”(File Reputation and Analysis) 服务，则应确保“数据”(Data) 网络接口已在设备上启用。请参阅 启用或更改网络接口，第 25 页
- 验证与配置升级和服务更新设置，第 416 页中配置的更新服务器的连接。

- 如果您将思科 AMP Threat Grid 设备用作私有云文件信誉服务器，请参阅配置本地文件信誉服务器，第 239 页。
- 如果您将 Cisco AMP Threat Grid 设备用作私有云文件分析服务器，请参阅配置本地文件分析服务器，第 240 页。

步骤 1 选择**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 点击**启用文件信誉过滤 (Enable File Reputation Filtering)**和可选的**启用文件分析 (Enable File Analysis)**。

- 如果选中**启用文件信誉过滤 (Enable File Reputation Filtering)**，则必须配置**文件信誉服务器 (File Reputation Server)** 部分（在**步骤 6** 中），方法如下：选择外部公共信誉云服务器的 URL，或提供私有信誉云服务器连接信息。
- 同样，如果选中**启用文件分析 (Enable File Analysis)**，则必须配置**文件分析服务器 URL (File Analysis Server URL)** 部分（在**步骤 7** 中），方法如下：提供外部云服务器的 URL，或提供私有分析云连接信息。

步骤 4 接受许可协议（如果存在）。

步骤 5 展开**文件信誉的高级设置 (Advanced Settings for File Reputation)** 面板，并根据需要调整下列选项：

选项	说明
云域 (Cloud Domain)	用于文件信誉查询的域的名称。
文件信誉服务器 (File Reputation Server)	选择公共信誉云服务器的主机名，或私有信誉云。 如果选择私有信誉云，请提供以下内容： • **服务器 (Server)** - 思科 AMP 虚拟私有云设备的主机名或 IP 地址。 • **公钥 (Public Key)** - 为此设备与您的私有云设备之间的加密通信提供有效的公钥。此公钥必须与私有云服务器使用的密钥相同：找到此设备上的密钥文件，然后点击**上传文件 (Upload File)**。 **注释** 您必须已将此密钥文件从服务器下载到此设备。
路由表 (Routing Table)	要用于高级恶意软件防护服务的路由表（与设备网络接口类型[管理或数据]关联）。如果设备已启用管理接口和一个或多个数据接口，则可选择“管理”(Management)或“数据”(Data)。

选项	说明
文件信誉的 SSL 通信 (SSL Communication for File Reputation)	选中**使用 SSL (端口 443）(Use SSL [Port 443])** 以在端口 443 而不是默认端口 32137 上进行通信。有关启用对服务器的 SSH 访问的信息，请参阅《思科 AMP 虚拟私有云设备用户指南》。 **注释** 通过端口 32137 的 SSL 通信可能需要您在防火墙中打开该端口。 通过此选项，您还可配置上游代理来与文件信誉服务进行通信。如果选中此选项，请提供相应的**服务器 (Server)**、**用户名 (Username)** 和**密码 (Passphrase)** 信息。 选中**使用 SSL (端口 443) (Use SSL (Port 443))** 时，如果隧道代理服务器的证书未由受信任的根颁发机构签名，还可以选中**放宽证书验证 (Relax Certificate Validation)** 以跳过标准证书验证。例如，如果在受信任的内部隧道代理服务器上使用自签名证书，则选择此选项。 **注释** 如果在“文件信誉的高级设置”的“文件信誉的 SSL 通信”部分选中**使用 SSL (端口 443) (Use SSL (Port 443))**，则必须使用 Web 界面中的“网络”>“证书”（自定义证书颁发机构）将内部部署信誉服务器 CA 证书上的 AMP 添加到此设备上的证书存储库。从服务器获得此证书（“配置”(Configuration) >“SSL”>“云服务器”(Cloud server) >“下载”(download)）。
心跳间隔 (Heartbeat Interval)	以分钟为单位的 ping 追溯事件频率。
信誉阈值 (Reputation Threshold)	可接受的文件信誉分数的上限。高于此阈值的分数表示文件被感染。 • **使用来自云服务的值 (60)** • **输入自定义值 (Enter Custom Value)** - 默认值为 60。
查询超时 (Query Timeout)	信誉查询超时前经过的秒数。
处理超时 (Processing Timeout)	文件处理超时前经过的秒数。
文件信誉客户端 ID (File Reputation Client ID)	文件信誉服务器上此设备的客户端 ID（只读）。

注释 在无思科支持指导的情况下，请勿更改本部分中的任何其他设置。

步骤 6 如果要使用云服务进行文件分析，请展开“文件分析的高级设置”面板并根据需要调整以下选项：

选项	说明
文件分析服务器 URL (File Analysis Server URL)	选择外部云服务器的名称 (URL) 或**私有分析云 (Private analysis cloud)**。 如果指定外部云服务器，请选择与您的设备物理距离最近的服务器。系统将使用标准更新流程定期将新的可用服务器添加到该列表中。 选择私有分析云以使用内部部署的思科 AMP Threat Grid 设备进行文件分析，并提供以下内容： • **服务器 (Server)** - 内部部署的私有分析云服务器的 URL。 • **证书颁发机构 (Certificate Authority)** - 选择**使用思科默认的证书颁发机构 (Use Cisco Default Certificate Authority)** 或**使用上传的证书颁发机构 (Use Uploaded Certificate Authority)**。 如果选择**使用上传的证书颁发机构 (Uploaded Certificate Authority)**，请点击**浏览 (Browse)** 来为此设备与私有云设备间的加密通信上传有效证书文件。此证书必须与私有云服务器使用的证书相同。
文件分析客户端 ID (File Analysis Client ID)	文件分析服务器上此设备的客户端 ID（只读）。

步骤 7 （可选）如果要为文件信誉处置值配置缓存到期期限，请展开“缓存设置”(Cache Settings) 面板。

步骤 8 提交并确认更改。

步骤 9 如果您使用现场 Cisco AMP Threat Grid 设备，请在 AMP Threat Grid 设备上激活此设备的帐户。

激活“用户”帐户的完整说明在 AMP Threat Grid 文档中提供。

a) 请记下页面部分底部显示的文件分析客户端 ID。此 ID 标识您将要激活的“用户”。
b) 登录 AMP Threat Grid 设备。
c) 选择**欢迎...(Welcome...)> 管理用户 (Manage Users)**，并浏览到“用户详细信息”(User Details)。
d) 根据 Web 安全设备的文件分析客户端 ID 找到“user”帐户。
e) 为设备激活该“user”帐户。

重要提示！文件分析设置中所需的更改

如果计划使用新的公共云文件分析服务，请务必阅读以下说明以保持数据中心隔离：

- 新文件分析服务器中不保留现有的设备分组信息。您必须在新文件分析服务器上对设备重新分组。
- 隔离到文件分析隔离区的邮件将会被保留到保留期。隔离区保留期过后，邮件将从文件分析隔离区中删除，并由 AMP 引擎重新扫描。然后，将该文件上传到新的文件分析服务器以进行分析，但不会再次将该邮件发送到文件分析隔离区。

有关详细信息，请参阅 http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html 中的思科 AMP Thread Grid 文档。

（仅公共云文件分析服务）配置设备组

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

注释 可以在计算机级别配置设备组。无法在集群级别配置设备组。

步骤 1 选择**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)**。

步骤 2 在“用于文件分析云报告的设备分组”(Appliance Grouping for File Analysis Cloud Reporting) 部分中，输入文件分析云报告组 ID。

- 如果这是要添加到组中的第一个设备，请为该组提供有用的标识符。
- 此 ID 区分大小写，并且不能包含空格。
- 提供的 ID 在将要共享有关上传以供分析的文件的数据的所有设备上必须相同。但在后续组设备上，不会验证该 ID。
- 如果未正确输入组 ID 或出于任何其他原因需要对其进行更改，则必须向思科 TAC 提交请求。
- 此更改会立即生效；它不需要“确认”(Commit)。
- 该组中的所有设备都必须配置为在云中使用相同的文件分析服务器。
- 一个设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。

步骤 3 点击 **将设备添加到组 (Add Appliance to Group)**。

哪些设备在分析组中？

步骤 1 选择**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)** 。

步骤 2 在“用于文件分析云报告的设备分组”部分中，点击**查看组中的设备 (View Appliances in Group)**。

步骤 3 要查看特定设备的**文件分析客户端 ID (File Analysis Client ID)**，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)** 页面上的“文件分析的高级设置”(Advanced Settings for File Analysis) 部分。
网络安全设备	**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)** 页面上的“文件分析高级设置”(Advanced Settings for File Analysis) 部分。
安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

根据访问策略配置文件信誉和分析服务操作

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击**防恶意软件和信誉 (Anti-Malware and Reputation)** 列中的链接，以查看表中的策略。

步骤 3 在**高级恶意软件防护设置 (Advanced Malware Protection Settings)** 部分中，选择**启用文件信誉过滤和文件分析 (Enable File Reputation Filtering and File Analysis)**。

如果未全局启用“文件分析”(File Analysis)，则仅提供“文件信誉过滤”(File Reputation Filtering)。

步骤 4 选择**已知恶意和高危文件 (Known Malicious and High-Risk Files)** 操作：**监控 (Monitor)** 或**阻止 (Block)**。

默认设置为“监控”(Monitor)。

步骤 5 提交并确认更改。

确保接收有关高级恶意软件防护问题的警报

确保设备配置为向您发送与高级恶意软包含相关的警报。

当出现以下情况时，您将收到警报：

警报说明	类型	严重性
您正在建立与现场（私有云）思科 AMP Threat Grid 设备的连接，并且需要激活帐户，如中所述。启用和配置文件信誉和分析服务，第240页	防恶意软件	警告
功能密钥过期	（作为所有功能的标准）	
不可访问文件信誉或文件分析服务。	防恶意软件	Warning
与云服务建立通信。	防恶意软件	信息

警报说明	类型	严重性
		信息
文件信誉判定更改。	防恶意软件	信息
可以发送进行分析的文件类型已更改。您可能需要启用上传新文件类型。	防恶意软件	信息
暂时无法分析某些文件类型。	防恶意软件	Warning
临时性中断后恢复分析所有受支持文件类型。	防恶意软件	信息

相关主题

- 有关无法连接至文件信誉或文件分析服务器的若干警报，第 250 页
- 在文件威胁判定更改时采取操作，第 249 页

配置高级恶意软件防护功能的集中报告

如果您将在安全管理设备上集中报告，请参阅管理设备的联机帮助或用户指南的网络报告章节中“高级恶意软件防护”部分中的重要配置要求。

文件信誉和文件分析报告与跟踪

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，所有实例被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，文件按其 SHA-256 值列出（以缩写格式）。为了标识您的组织中与恶意软件实例相关联的文件名，请选择“报告”(Reporting) > “高级恶意软件防护”(Advanced Malware Protection)，并点击表中的 SHA-256 链接。详细信息页面会显示关联文件名。

文件信誉和文件分析报告页面

报告	说明
高级恶意软件防护	显示由文件信誉服务识别的基于文件的威胁。 要查看尝试访问每个 SHA 的用户以及与该 SHA-256 关联的文件名，请点击表格中的 SHA-256。 点击“恶意软件威胁文件详细信息”(Malware Threat File Details) 报告页面底部的链接，会在网络跟踪中显示在最大可用时间范围内遇到的该文件的所有实例，不管为该报告选择什么时间范围都是如此。 对于那些具有已更改判定的文件，请参阅 AMP 判定更新报告。这些判定不会反映在“高级恶意软件防护”(Advanced Malware Protection) 报告中。 **注释** 如果从压缩或存档文件中提取的某个文件是恶意文件，则高级恶意软件防护报告中仅包含压缩或存档文件的 SHA 值。
高级恶意软件防护文件分析	显示送交分析的每个文件的时间和判定（或临时判定）。 在思科 AMP Threat Grid 设备上已列入白名单的文件显示为“正常”。有关白名单的信息，请参阅 AMP Threat Grid 联机帮助。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 深入查看详细分析结果，包括每个文件的威胁特征和得分。 您还可以直接在执行分析的 AMP Threat Grid 设备或云服务器上查看有关 SHA 的其他详细信息，方法是搜索 SHA 或点击文件分析详细信息页面底部的思科 AMP Threat Grid 链接。 **注释** 如果从某个压缩文件或存档文件中提取的文件送交文件分析，则只有这些已提取文件的 SHA 值包括在“文件分析”(File Analysis) 报告中。
高级恶意软件防护判定更新	列出由该设备处理且在事务处理后判定已更改的文件。有关这种情况的信息，请参阅文件威胁判定更新，第 233 页。 要查看超过 1000 个判定更新，请将数据导出为 .csv 文件。 如果单个 SHA-256 的判定多次发生变化，则此报告仅显示最新判定，而不显示判定历史记录。 点击 SHA-256 链接会显示在最大可用时间范围内包括此 SHA-256 的所有事务的网络跟踪结果，不论为报告选择的是哪种时间范围。 要查看在最大可用时间范围内（不管为该报告选择的时间范围）特定 SHA-256 的所有受影响的事务，请点击，此链接位于“恶意软件威胁文件”页面的底部。

查看其他报告中的文件信誉过滤数据

在相关的情况下，其他报告中会提供文件信誉和分析的数据。默认情况下，“被高级恶意软件防护阻止”(Blocked by Detected by Advanced Malware Protection) 列在适用报告中可能被隐藏。要显示其他列，请点击表格下方的“列”(Columns) 链接。

“按用户地点分类的报告”(Report by User Location) 包括一个“高级恶意软件保护”(Advanced Malware Protection) 选项卡。

关于网络跟踪和高级恶意软件保护功能

在“网络跟踪”(Web Message Tracking) 中搜索文件威胁信息时，请注意以下几点：

- 要搜索文件信誉服务找到的恶意文件，请在“恶意软件威胁”(Advanced Malware Protection Positive) 区域中，对**按恶意软件类别过滤 (Filter by Malware Category)** 选项选择**已知恶意和高危文件 (Known Malicious and High-Risk Files)**，在“网络邮件跟踪”(Web Message Tracking) 的“高级”(Advanced) 部分，对“邮件事件”(Message Event) 选项选择。
- “网络跟踪”(Web Message Tracking) 仅包括处理事务邮件时返回的文件信誉处理和原始文件信誉判定的相关信息。例如，如果最初发现文件是干净的，然后判定更新发现文件是恶意的，则在跟踪结果中仅显示干净判定。

  对于干净或不可扫描的附件，不提供任何信息。

  搜索结果中的“阻止 - AMP”意味着事务因文件的信誉判定而被阻止。

  在跟踪详细信息中，“AMP 威胁得分”是云信誉服务无法判定某个文件是否正常时所能提供的最佳得分。在这种情况下，得分介于 1 和 100 之间。（如果返回了 AMP 判定，或者分数为零，请忽略 AMP 威胁得分。）设备会将此得分与阈值得分（在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation) 页面上配置）进行比较，以确定需要采取的措施。默认情况下，得分介于 60 到 100 之间的文件会被视为恶意文件。思科不建议更改默认阈值得分。WBRS 得分是从中下载文件的站点的信誉；此得分与文件信誉无关。

- 判定更新仅在 AMP 判定更新报告中可用。“网络跟踪”(Web Message Tracking) 中的原始事务详细信息不会随着判定变化而更新。要查看事务，请点击判定更新报告中的 SHA-256。
- 有关文件分析的信息（包括分析结果以及是否发送文件进行分析）仅在文件分析报告中可用。

  有关所分析的文件的其他信息，可从云端或现场文件分析服务器获取。要查看文件的任何可用文件分析信息，请依次选择**报告 (Reporting) > 文件分析 (File Analysis)**，然后输入 SHA-256 搜索文件或点击“网络跟踪”(Web Tracking) 详细信息中的 SHA-256 链接。如果文件分析服务已从任意来源分析了该文件，您可以查看该详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了送交分析的某个文件的后续实例，这些实例将显示在“网络跟踪”(Web Message Tracking) 搜索结果中。

在文件威胁判定更改时采取操作

步骤 1 查看“AMP 判定更新”(AMP Verdict Updates) 报告。

步骤 2 点击相关的 SHA-256 链接查看跟踪数据，允许终端用户访问并可发送至。

步骤 3 使用跟踪数据标识可能已危及用户、违规中所涉及的文件名等信息以及文件下载网站和。

步骤 4 检查“文件分析”(File Analysis) 报告查看是否将该 SHA-256 送交分析，以更详细地了解文件威胁行为。

下一步做什么

相关主题

文件威胁判定更新，第 233 页

故障排除文件信誉和分析

日志文件

在日志中：

- `AMP` 和 `amp` 是指文件信誉服务或引擎。
- `Retrospective` 是指判定更新。
- `VRT` 和 `sandboxing` 是指文件分析服务。

将有关高级恶意软件保护（包括文件分析）的信息记录在访问日志或AMP引擎日志中。有关详细信息，请参阅通过日志监控系统活动的章节。

在日志消息“文件信誉查询收到的响应”中，“上传操作”的可能值为：

- 0：文件不为信誉服务所知；不送交分析。
- 1：发送
- 2：文件不为信誉服务所知；不送交分析。

有关无法连接至文件信誉或文件分析服务器的若干警报

问题

您收到有关无法连接到云中的文件信誉或分析服务的若干警报。（单个警报可能仅表示瞬态问题。）

解决方案

- 确保符合与文件信誉和分析服务通信的要求，第 237 页中的要求。
- 检查可能阻止设备与云服务进行通信的网络问题。
- 增加查询超时值：

  选择**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)**。“查询超时”值出现在**高级恶意软件保护服务 (Advanced Malware Protection Services)** 部分的“高级”(Advanced) 设置区域中。

API 密钥错误（本地文件分析）

问题

您在尝试查看“文件分析”报告详细信息时收到 API 密钥警告，或者网络安全设备无法连接到 AMP Threat Grid 服务器以上传要分析的文件。

解决方案

如果更改 AMP Threat Grid 服务器的主机名并且使用来自 AMP Threat Grid 服务器的自签名证书，则会出现该错误。此外，在其他情况下也有可能出现。解决问题：

- 从拥有新主机名的 AMP Threat Grid 设备生成新证书。
- 将新证书上传到网络安全设备。
- 在 AMP Threat Grid 设备上重置 API 密钥。有关说明，请参阅 AMP Threat Grid 设备的在线帮助。

相关主题

- 启用和配置文件信誉和分析服务，第 240 页

未按预期上传文件

问题

未按预期评估或分析文件。无警报或明显错误。

解决方案

请考虑以下方面：

- 该文件可能已由另一设备送交分析，因此已存在于文件分析服务器上，或存在于正在处理该文件的设备的缓存中。

- 在**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)**页面上，检查为 **DVS 引擎对象扫描限值 (DVS Engine Object Scanning Limits)** 配置的最大文件大小限值。该限值适用于高级恶意软件防护功能。

云端的文件分析详细信息不完整

问题

对于从组织中其他网络安全设备上传的文件，无法在公共云中获取完整的文件分析结果。

解决方案

务必将所有要共享文件分析结果数据的设备分组到一起。请参阅（仅公共云文件分析服务）配置设备组，第 244 页。必须在该组中的每台设备上完成此配置。

有关可送交分析的文件类型警报

问题

您会收到有关可送交文件分析的文件类型严重性信息警报。

解决方案

受支持文件类型更改或检查设备以查看受支持的文件类型时，发送该警报。这可能会出现于：

- 您或其他管理员更改选作分析的文件类型时。
- 基于云服务可用性受支持文件类型暂时改变。在这种情况下，将尽快恢复设备上选定的文件类型支持。两个过程均是动态的，您无需进行任何操作。
- 设备重新启动，例如作为 AsyncOS 升级的一部分。

第 16 章

管理对 Web 应用的访问

本章包含以下部分：

管理对 Web 应用的访问概述

通过应用可视性与可控性 (AVC) 引擎，您可以创建策略来控制网络上的应用活动，而不必完全了解每种应用的基础技术。您可以在访问策略组中配置应用控制设置。您可以单独或根据应用类型阻止或允许应用。您还可以将控制应用于特定应用类型。

使用访问策略可以：

- 控制应用行为
- 控制用于特定应用类型的带宽量
- 当最终用户受阻时通知最终用户
- 向即时消息、博客和社交媒体应用分配控制
- 指定范围请求设置

要使用 AVC 引擎来控制应用，请执行以下任务：

任务	任务链接
启用 AVC 引擎	启用 AVC 引擎， 第 254 页
在访问策略组中设置控制	在访问策略组中配置应用控制设置， 第 257 页
限制某些应用类型消耗的带宽以控制拥塞	控制带宽， 第 258 页

任务	任务链接
允许即时消息流量，但是不允许通过即时消息功能进行文件共享	控制即时消息流量，第 260 页

启用 AVC 引擎

当启用可接受的使用控制 (Acceptable Use Controls) 时，启用 AVC 引擎。

注释 您可以查看报告 (Reporting) > 应用可视性 (Application Visibility) 页面上“应用可视性”(Application Visibility) 报告中的 AVC 引擎扫描活动。

步骤 1 依次选择**安全服务 (Security Services) > 可接受的使用控制 (Acceptable Use Controls)**。

步骤 2 点击**启用 (Enable)** 或**编辑全局设置 (Edit Global Settings)**，具体取决于可接受的使用控制的当前状态。

步骤 3 请务必选中“启用思科网络使用控制”(Enable Cisco Web Usage Controls)。

步骤 4 在“可接受的使用控制服务”(Acceptable Use Controls Service) 面板中，选择**思科网络使用控制 (Cisco Web Usage Controls)**，然后选择**启用应用可视性与可控性 (Enable Application Visibility and Control)**。

步骤 5 选择**不可访问服务的默认操作 (Default Action for Unreachable Service)**：**监控 (Monitor)** 或**阻止 (Block)**。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- AVC 引擎更新和默认操作，第 254 页
- AVC 引擎阻止请求时的用户体验，第 255 页

AVC 引擎更新和默认操作

AsyncOS 会定期查询更新服务器是否存在对所有安全服务组件（包括 AVC 引擎）的新更新。AVC 引擎更新可以包括对新应用类型和应用的支持，以及对现有应用的更新支持（如果存在任何应用行为更改）。通过在 AsyncOS 版本更新之间更新 AVC 引擎，可以保持网络安全设备的灵活性，而无需服务器升级。

AsyncOS for Web 为全局访问策略分配以下默认操作：

- 新的应用类型默认为**监控 (Monitor)**。
- 新的应用行为（例如阻止特定应用内的文件传输）默认为**监控 (Monitor)**。
- 现有应用类型对应的新应用默认设置为应用类型的默认值。

注释 在全局访问策略中，您可以设置每个应用类型的默认操作，因此，AVC 引擎更新中介绍的新应用将自动继承指定的默认操作。请参阅在访问策略组中配置应用控制设置，第 257 页。

AVC 引擎阻止请求时的用户体验

当 AVC 引擎阻止事务时，Web 代理会向最终用户发送阻止页面。但是，并非所有网站都会向最终用户显示该阻止页面；许多网站使用 JavaScript 显示动态内容，而不是静态网页，因此不可能显示该阻止页面。系统仍然会适当阻止用户下载恶意数据，但网站并非始终会就此情况通知用户。

策略应用控制设置

控制应用涉及配置以下元素：

选项	说明
应用类型 (Application Types)	包含一个或多个应用的类别。
应用 (Applications)	应用类型内的特定应用。
应用行为 (Application behaviors)	用户在管理员可以控制的应用内能够执行的特定操作或行为。并非所有应用都包含您可以配置的行为。

您可以在访问策略组中配置应用控制设置。在**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)** 页面上，点击要配置的策略组的**应用 (Applications)** 链接。配置应用时，您可以选择以下操作：

选项	说明
阻止 (Block)	此操作为最终操作。系统将阻止用户查看网页，并改为显示最终用户通知页面。
监控 (Monitor)	此操作为中间操作。Web 代理继续将事务与其他控制设置进行比较，以确定要应用的最终操作。
限制 (Restrict)	此操作表示应用行为受阻。例如，当您阻止特定即时消息应用的文件传输时，该应用的操作为“限制”(Restrict)。
带宽限制 (Bandwidth Limit)	对于某些应用（例如 Media 和 Facebook），您可以限制网络流量的可用带宽。您可以限制应用本身及其用户的带宽。

相关主题

- 范围请求设置，第 256 页

• 关于配置应用控制的规则和准则，第 256 页

范围请求设置

当禁用 HTTP 范围请求并通过多个流下载大型文件时，会扫描合并后的数据包。这会使用于下载大型对象的下载管理工具和应用失去性能上的优势。

或者，在启用“范围请求转发”(Range Request Forwarding) 后（请参阅配置 Web 代理设置，第 61 页），您可以控制如何逐个策略处理传入范围请求。当请求大文件时，此过程称为“字节服务”，是一种带宽优化方式。

但是，启用“范围请求转发”会影响基于策略的应用可视性与可控性 (AVC) 效率，并可能危及安全性。请小心谨慎，并且仅在对性能优势的需求高于安全隐患时才启用 HTTP 范围请求转发。

注释 当“范围请求转发”(Range Request Forwarding) 未启用时，范围请求设置为只读。当将其启用时也是如此，但所有应用均设置为“监控”(Monitor)。这些设置在至少一个应用设置为“阻止”(Block)、“限制”(Restrict) 或者“节流”(Throttle) 时可用。

策略的范围请求设置	
范围请求设置	• **不转发范围请求 (Do not forward range requests)** - 不转发部分文件的任何请求，返回整个文件。 • **转发范围请求 (Forward range requests)** - 如果请求的范围有效，则将转发，并且目标服务器将只返回所需文件的请求部分。
例外列表	您可以指定免于进行当前转发选择的流量目标。例如，当选择**不转发范围请求 (Do not forward range requests)** 时，您可以指定要为其转发请求的目标。同样，当选择**转发范围请求 (Forward range requests)** 时，您可以指定不为其转发请求的目标。

关于配置应用控制的规则和准则

当配置应用控制设置时，请考虑以下规则和准则：

- AsyncOS for Web 升级之间或者 AVC 引擎更新之后，支持的应用类型、应用和应用行为可能会有变化。
- 如果启用“安全搜索”或“站点内容分级”，AVC 引擎将需要识别安全浏览的应用程序。作为条件之一，AVC 引擎会扫描响应正文以检测搜索应用。因此，设备不会转发范围报头。
- 在应用类型列表中，每个应用类型的摘要都列出其应用的最终操作，但不指示这些操作是继承自全局策略还是在当前访问策略中进行配置。要了解有关特定应用的操作的详细信息，请展开应用类型。
- 在全局访问策略中，您可以设置每个应用类型的默认操作，以使AVC引擎更新中引入的新应用自动继承默认操作。

- 您可以通过点击“浏览”(Browse) 视图中应用类型对应的“编辑全部”(edit all) 链接，快速为应用类型中的所有应用配置相同操作。但是，您只能配置应用操作，无法配置应用行为操作。要配置应用行为，必须单独编辑应用。
- 在“搜索”(Search) 视图中，当您按操作列对表进行排序时，排序顺序由最终操作决定。例如，“使用全局（阻止）”(Use Global [Block]) 在排序顺序中位于“阻止”(Block) 之后。
- 除非在客户端上安装用于签名的根证书，否则解密可能会导致某些应用失败。

相关主题

- 在访问策略组中配置应用控制设置，第 257 页
- 配置整体带宽限制，第 258 页
- 查看 AVC 活动，第 260 页

在访问策略组中配置应用控制设置

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要编辑的策略组的“应用”(Applications) 列下的策略表中的链接。

步骤 3 配置全局访问策略时：

a) 在**应用类型的默认操作 (Default Actions for Application Types)** 部分中定义每个应用类型的默认操作。

b) 您可以在页面的 **编辑应用设置 (Edit Applications Settings)** 部分中，将每个应用类型的个别成员的默认操作作为组进行编辑或逐个编辑。以下步骤中介绍编辑单独应用的默认操作。

步骤 4 配置用户定义的访问策略时，请在**编辑应用设置 (Edit Applications Settings)** 部分中选择**定义应用自定义设置 (Define Applications Custom Settings)**。

步骤 5 在“应用设置”(Application Settings) 区域中，从下拉菜单中选择**浏览视图 (Browse view)** 或 **搜索视图 (Search view)**：

- **浏览视图 (Browse view)**。您可以浏览“应用类型”(Application Types)。可以使用“浏览视图”(Browse view) 同时配置特定类型的所有应用。当应用类型在“浏览视图”(Browse view) 中处于折叠状态时，应用类型的摘要会列出其应用的最终操作，但不会指示操作是继承自全局策略还是在当前访问策略中进行配置。
- **搜索视图 (Search view)**。您可以按名称搜索应用。当应用的总列表较长，并且需要快速查找并配置特定应用时，可能会使用“搜索视图”(Search view)。

步骤 6 为每个应用和应用行为配置操作。

步骤 7 为每个适用的应用配置带宽控制。

步骤 8 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 控制带宽，第 258 页

控制带宽

在对事务同时应用整体限制和用户限制时，将应用最严格的选项。您可以通过定义URL类别的身份组并在限制带宽的访问策略中使用该身份组，来定义特定 URL 类别的带宽限制。

可以定义以下带宽限制：

带宽限制	说明	任务链接
整体	对受支持的应用类型定义网络上所有用户的整体限制。整体带宽限制会影响网络安全设备和 Web 服务器之间的流量。它不限制从网络缓存提供的流量。	配置整体带宽限制，第 258 页
用户	根据应用类型定义网络上特定用户的限制。用户带宽限制来自 Web 服务器的流量以及从网络缓存提供的流量。	配置用户带宽限制，第 258 页

注释 定义带宽限制仅限制流向用户的数据。它不会根据是否达到配额来阻止数据。Web 代理会在每个应用事务中引入延迟，以模仿速度较慢的服务器链接。

配置整体带宽限制

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 整体带宽限制 (Overall Bandwidth Limits)**

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择**限制为 (Limit to)** 选项。

步骤 4 以兆位/秒 (Mbps) 或千位/秒 (kbps) 为单位输入要限制的流量。

步骤 5 “提交”(Submit) 并“确认更改”(Commit Changes)。

配置用户带宽限制

可以通过在“访问策略”(Access Policies) 的“应用可视性与可控性”(Applications Visibility and Control) 页面上配置带宽控制限制来定义用户带宽限制。可以在“访问策略”(Access Policies) 中为用户定义以下类型的带宽控制：

选项	说明	任务链接
应用类型的默认带宽限制 (Default bandwidth limit for an application type)	在全局访问策略中，可以为某个应用类型的所有应用定义默认带宽限制。	配置应用类型的默认带宽限制，第 259 页

选项	说明	任务链接
应用类型的带宽限制 (Bandwidth limit for an application type)	在用户定义的访问策略中，可以为全局访问策略中定义的应用类型覆盖默认带宽限制。	覆盖应用类型的默认带宽限制，第 259 页
应用的带宽限制 (Bandwidth limit for an application)	在用户定义的访问策略或全局访问策略中，可以选择应用应用类型带宽限制或不应用任何限制（免除应用类型限制）。	配置应用的带宽控制，第 259 页

配置应用类型的默认带宽限制

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击全局访问策略的“应用”(Applications) 列下的策略表中的链接。

步骤 3 在**应用类型的默认操作 (Default Actions for Application Types)** 部分中，点击要编辑的应用类型的“带宽限制”(Bandwidth Limit) 旁边的链接。

步骤 4 选择**设置带宽限制 (Set Bandwidth Limit)**，并以兆位/秒 (Mbps) 或千位/秒 (kbps) 为单位输入要限制的流量。

步骤 5 点击**应用 (Apply)**。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

覆盖应用类型的默认带宽限制

您可以覆盖在用户定义的访问策略中的全局访问策略组处定义的默认带宽限制。您只能在“浏览”(Browse) 视图中执行此操作。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要编辑的用户定义的策略组的“应用”(Applications) 列下的策略表中的链接。

步骤 3 选择**编辑应用设置 (Edit Applications Settings)** 部分中的**定义应用自定义设置 (Define Applications Custom Settings)**。

步骤 4 点击要编辑的应用类型的“带宽限制”(Bandwidth Limit) 旁边的链接。

步骤 5 要选择其他带宽限制值，请选择**设置带宽限制 (Set Bandwidth Limit)** 并以兆位/秒 (Mbps) 或千位/秒 (kbps) 为单位输入要限制的流量。要指定无带宽限制，请选择**应用类型无带宽限制 (No Bandwidth Limit for Application Type)**。

步骤 6 点击**应用 (Apply)**。

步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

配置应用的带宽控制

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要编辑的策略组的“应用”(Applications) 列下的策略表中的链接。

步骤 3 展开包含要定义的应用的应用类型。

步骤 4 点击要配置的应用的链接。

步骤 5 选择**监控 (Monitor)**，然后选择使用为应用类型定义的带宽限制或不使用任何限制。

注释 当应用被阻止或者没有为应用类型定义带宽限制时，带宽限制设置不适用。

步骤 6 点击**完成 (Done)**。

步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

控制即时消息流量

您可以阻止或监控 IM 流量，并且根据 IM 服务，可以阻止 IM 会话中的特定活动（也称为应用行为）。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 访问策略 (Access Policies)**。

步骤 2 点击要编辑的策略组的“应用”(Applications) 列下的策略表中的链接。

步骤 3 点击**定义应用自定义设置 (Define Applications Custom Setting)**。

步骤 4 展开“即时消息”(Instant Messaging) 应用类型。

步骤 5 点击要配置的 IM 应用旁边的链接。

步骤 6 要阻止此 IM 应用的所有流量，请选择**阻止 (Block)**。

步骤 7 要监控 IM 应用，但是阻止该应用内的特定活动，请选择**监控 (Monitor)**，然后选择要**阻止 (Block)** 的应用行为。

步骤 8 点击**完成 (Done)**。

步骤 9 “提交”(Submit) 并“确认更改”(Commit Changes)。

查看 AVC 活动

报告 (Reporting) > 应用可视性 (Application Visibility) 页面显示有关所使用的排名靠前的应用和应用类型的信息。此外，它还显示阻止的排名靠前的应用和应用类型。

访问日志文件中的 AVC 信息

访问日志文件记录应用可视性与可控性引擎返回的各事务信息。访问日志中的扫描判定信息部分包含下列字段：

说明	访问日志中的自定义字段	W3C 日志中的自定义字段
应用名称	%XO	x-avc-app
应用类型	%Xu	x-avc-type

应用行为	%Xb	x-avc-behavior

第 17 章

防止敏感数据丢失

本章包含以下部分：

防止敏感数据丢失概述

网络安全设备通过提供以下功能来保护您的数据：

选项	说明
思科数据安全过滤器 (Cisco Data Security filters)	网络安全设备上的思科数据安全过滤器评估数据通过 HTTP、HTTPS 和 FTP 从网络中泄露的情况。
第三方防数据丢失 (Third-party data loss prevention (DLP)) 集成	网络安全设备与可识别和保护敏感数据的领先第三方内容感知DLP系统集成。Web 代理使用互联网内容适配协议 (ICAP) 以允许代理服务器将内容扫描卸载到外部系统。

当 Web 代理收到上传请求时，Web 代理将请求与数据安全和外部 DLP 策略组进行比较以确定哪个策略组适用。如果配置了两种类型的策略，Web 代理会将请求先与思科数据安全策略进行比较，然后再与外部 DLP 策略比较。在 Web 代理将请求分配到策略组之后，Web 代理会将请求与策略组的已配置控制设置进行比较，以便确定如何处理请求。如何配置设备处理上传请求取决于策略组类型。

注释 不会根据思科数据安全或外部 DLP 策略对尝试上传零 (0) 字节文件的上传请求进行评估。

要限制和控制从网络泄露的数据，您可执行以下任务：

任务	任务链接
创建思科数据安全策略	管理上传请求，第 265 页
创建外部 DLP 策略	在外部 DLP 系统上管理上传请求，第 265 页
创建数据安全和外部 DLP 策略	创建数据安全和外部 DLP 策略，第 267 页
使用思科数据安全策略控制上传请求	管理上传请求的设置，第 269 页
使用外部 DLP 策略控制上传请求	使用外部 DLP 策略控制上传请求，第 272 页

绕过低于最小大小的上传请求

为了帮助减少日志文件中记录的上传请求数，您可以定义最小请求正文大小，让思科数据安全过滤器或外部 DLP 服务器不扫描低于最低大小的上传请求。

为此，请使用以下 CLI 命令：

- **datasecurityconfig**。适用于思科数据安全过滤器。
- **externaldlpconfig**。适用于已配置的外部 DLP 服务器。

两个 CLI 命令的默认最小请求正文大小为 4 KB（4096 个字节）。有效值为 1 至 64 KB。您指定的大小适用于上传请求正文的整个大小。

注释 当启用时，思科数据安全过滤器或外部 DLP 服务器会扫描所有数据块编码的上传和所有本地 FTP 事务。但是，它们仍然可以基于自定义 URL 类别来绕过某些项。

请求作为敏感数据被阻止时的用户体验

当思科数据安全过滤器或外部 DLP 服务器阻止上传请求时，会提供一个阻止页面，由 Web 代理发送给最终用户。并非所有网站均向最终用户显示阻止页面。某些 Web 2.0 网站使用 JavaScript 显示动态内容而不是静态网页，因此不可能显示阻止页面。用户因违反数据安全而仍受到阻止，但网站并不会始终向用户通报此情况。

管理上传请求

开始之前

转到**安全服务 (Security Services) > 数据安全过滤器 (Data Security Filters)** 以启用思科数据安全过滤器。

创建和配置数据安全策略组。

在评估上传请求时，思科数据安全策略会使用 URL 过滤、Web 信誉和上传内容信息.您配置每个安全组件以确定是否阻止上传请求。

当 Web 代理将上传请求与控制设置进行比较时，Web 代理会按顺序评估设置。每个控制设置可配置为执行思科数据安全策略的以下操作之一：

操作	说明
阻止	Web 代理不允许连接，而是显示最终用户通知页面，以说明阻止的原因。
允许	Web代理绕过数据安全策略安全服务扫描的剩余部分，然后在采取最终操作之前根据访问策略评估请求。 对于思科数据安全策略，请允许绕过数据安全扫描的剩余部分，但不绕过外部 DLP 或访问策略扫描。Web 代理对请求采取的最终操作由适用的访问策略（或可能阻止请求的适用外部 DLP 策略）来确定。
监控	Web代理继续将事务与其他数据安全策略组控制设置进行比较以确定是阻止该事务还是根据访问策略对事务进行评估。

对于思科数据安全策略，只有阻止操作是 Web 代理对客户端请求采取的最终操作。监控和允许操作是中间操作。在这两种情况下，Web 代理均会根据外部 DLP 策略（如果已配置）和访问策略来评估事务。Web 代理基于访问策略组控制设置（或可能阻止请求的适用外部 DLP 策略）来确定应采取哪个最终操作。

下一步做什么

相关主题

- 在外部 DLP 系统上管理上传请求 ， 第 265 页
- 管理上传请求的设置 ， 第 269 页

在外部 DLP 系统上管理上传请求

要将网络安全设备配置为处理外部 DLP 系统中的上传请求，请执行以下任务：

步骤 1 依次选择**网络 (Network) > 外部 DLP 服务器 (External DLP Servers)**。定义外部 DLP 系统。要将上传请求传递到外部 DLP 系统进行扫描，您必须在安全管理设备上定义至少一个兼容 ICAP 的 DLP 系统。

步骤 2 **创建和配置外部 DLP 策略组**。在定义外部 DLP 系统之后，创建和配置外部 DLP 策略组以确定将哪个上传请求发送到 DLP 系统进行扫描。

步骤 3 当上传请求匹配外部 DLP 策略时，Web 代理使用互联网内容适配协议 (ICAP) 将上传请求发送到 DLP 系统进行扫描。DLP 系统扫描请求正文内容并向 Web 代理返回阻止或允许判定。允许判定类似于思科数据安全策略的允许操作，上传请求将与访问策略进行比较。Web 代理对请求采取的最终操作由适用的访问策略来确定。

下一步做什么

相关主题

- 使用外部 DLP 策略控制上传请求，第 272 页
- 定义外部 DLP 系统，第 270 页

评估数据安全和外部 DLP 策略组成员身份

每个客户端请求均分配一个身份，然后根据其他策略类型进行评估以确定每种类型属于哪个策略组。Web 代理根据数据安全和外部 DLP 策略来评估上传请求。Web 代理根据客户端请求的策略组成员身份将已配置的策略控制设置应用于客户端请求。

将客户端请求与数据安全和外部 DLP 策略组匹配

为确定与客户端请求匹配的策略组，Web 代理遵循匹配组成员身份条件的特定流程。Web 代理对组成员身份考虑以下因素：

- **身份**。每个客户端请求要么与标识配置文件相匹配，要么未通过身份验证并被授予访客访问权限，要么未通过身份验证并被终止。
- **授权用户**。如果分配的标识配置文件需要身份验证，用户必须处于数据安全或外部 DLP 策略组中的已授权用户列表中，然后才能匹配策略组。授权用户列表可以是任何指定的组或用户，如果标识配置文件允许访客访问，则也可以是访客用户。
- **高级选项**。您可为数据安全和外部 DLP 策略组成员身份配置几个高级选项。某些选项（例如，代理端口和 URL 类别）也可在身份内定义。在身份中配置了高级选项时，在数据安全或外部 DLP 策略组级别不可配置该选项。

此部分的信息概述了 Web 代理如何将上传请求与数据安全和外部 DLP 策略组匹配。

Web 代理按顺序读取策略表中的每个策略组。Web 代理将上传请求状态与第一个策略组的成员身份条件进行比较。如果匹配，Web 代理应用该策略组的策略设置。

如果不匹配，Web 代理将上传请求与下一个策略组进行比较。Web 代理会继续此过程，直到它将上传请求与用户定义的策略组匹配。如果 Web 代理与用户定义的策略组不匹配，则与全局策略组匹配。当 Web 代理将上传请求与策略组或全局策略组相匹配时，它将应用该策略组的策略设置。

创建数据安全和外部 DLP 策略

您可以基于若干条件（例如，一个或多个标识配置文件或目标站点的URL类别）的组合来创建数据安全和外部DLP策略组。必须至少为策略组成员身份定义一个条件。当您定义多个条件时，上传请求必须满足所有条件才能匹配策略组。但是，上传请求只需与一个已配的标识配置文件匹配。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > Cisco 数据安全 (Cisco IronPort Data Security)**（定义数据安全策略组成员）或**网络安全管理器 (Web Security Manager) > 外部防数据丢失 (External Data Loss Prevention)**（定义外部 DLP 策略组成员）。

步骤 2 点击**添加策略 (Add Policy)**。

步骤 3 在**策略名称 (Policy Name)** 字段中输入策略组的名称，在可选的“说明”(Description) 字段中添加说明信息。

注释 每个策略组名称都必须唯一，并且仅包含字母数字字符或空格字符。

步骤 4 在**插入到策略上面 (Insert Above Policy)** 字段中，选择需要将策略组放入到策略表中的哪个位置。

当配置多个策略组时，必须为每个组指定逻辑顺序。为策略组排序，确保发生正确的匹配。

步骤 5 在**身份和用户 (Identities and Users)** 部分中，选择一个或多个要应用到此策略组的标识配置文件。

步骤 6 （可选）展开**高级 (Advanced)** 部分，定义其他成员身份要求。

步骤 7 要通过任何高级选项来定义策略组成员身份，请点击高级选项的链接并在显示的页面上配置选项。

高级选项	说明
协议 (Protocols)	选择是否按照客户端请求中使用的协议来定义策略组成员身份。选择要包括的协议。 “所有其他”(All others) 表示此选项上未列出的任何协议。 **注释** 当HTTPS代理启用时，只有解密策略应用于HTTPS事务。您无法通过HTTPS协议为访问、路由、出站恶意软件扫描、数据安全或外部DLP策略定义策略成员身份。
代理端口 (Proxy Ports)	选择是否按照用于访问Web代理的代理端口来定义策略组成员身份。在“代理端口”(Proxy Ports) 字段中输入一个或多个端口号。使用逗号分隔多个端口。 对于显式转发连接，此代理端口为浏览器中配置的端口。对于透明连接，此代理端口与目标端口为同一端口。如果您将一组客户端配置为在某个端口上显式转发请求，并将另一组客户端配置为在另一个端口上显式转发请求，则您可能要在代理端口上定义策略组成员身份。 当设备采用显式转发模式进行部署，或者当客户端明确地将请求转发给设备时，思科建议仅通过代理端口定义策略组成员身份。当客户端请求透明地重定向到设备时，如果您通过代理端口定义策略组成员身份，则某些请求会被拒绝。 **注释** 如果与此策略组关联的身份按此高级设置定义身份成员身份，不会在非身份策略组级别配置此设置。

高级选项	说明
子网 (Subnets)	选择是否按子网或其他地址定义策略组成员身份。 您可以选择使用可通过关联标识配置文件定义的地址，也可以在此处输入具体地址。 **注释** 如果与此策略组关联的标识配置文件按地址定义其成员身份，则在此策略组中，您输入的地址必须是标识配置文件中定义的地址的子集。在策略组中添加地址会进一步缩小与此策略组匹配的事务列表的范围。
URL 类别 (URL Categories)	选择是否按 URL 类别定义策略组成员身份。选择用户定义的或预定义的 URL 类别。 **注释** 如果与此策略组关联的身份按此高级设置定义身份成员身份，不会在非身份策略组级别配置此设置。
用户代理 (User Agents)	选择是否要按在客户端请求中使用的用户代理（诸如更新程序和 Web 浏览器等客户端应用）来定义策略组成员身份。可以选择某些通常定义的用户代理，或者使用正则表达式定义自己的用户代理。指定成员身份定义仅包括选定的用户代理，还是专门排除了选定的用户代理。 **注释** 如果与此策略组关联的标识配置文件 (Identification Profile) 通过此高级设置定义了标识配置文件 (Identification Profile) 成员身份，则不会在非标识配置文件 (Identification Profile) 策略组级别配置此设置。
用户位置 (User Location)	选择是否按照用户位置（不管是远程还是本地）来定义策略组成员身份。 仅当 Secure Mobility 已启用时，此选项才会显示。

步骤 8 提交更改。

步骤 9 如果您正在创建数据安全策略组，请配置其控制设置以定义 Web 代理如何处理上传请求。

新的数据安全策略组自动继承全局策略组设置，直到您为每个控制设置配置选项。

如果您正在创建外部 DLP 策略组，请配置其控制设置以定义 Web 代理如何处理上传请求。

新的外部 DLP 策略自动继承全局策略组设置，直到您配置自定义设置。

步骤 10 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 评估数据安全和外部 DLP 策略组成员身份， 第 266 页
- 将客户端请求与数据安全和外部 DLP 策略组匹配， 第 266 页
- 管理上传请求的设置， 第 269 页
- 使用外部 DLP 策略控制上传请求， 第 272 页

管理上传请求的设置

每个上传请求均分配到数据安全策略组并继承该策略组的控制设置。数据安全策略组的控制设置确定设备是否阻止连接或根据访问策略对其进行评估。

在“网络安全管理器”(Web Security Manager) >“思科数据安全”(Cisco IronPort Data Security) 页面上配置适用于数据安全策略组的控制设置。

您可以配置以下设置以确定对上传请求采取何种操作：

选项	链接
URL 类别	URL 类别， 第 269 页
Web 信誉	Web 信誉， 第 269 页
内容	内容阻止，第269 页

在数据安全策略组分配到上传请求后，对策略组的控制设置进行评估以确定是否阻止请求或根据访问策略对其进行评估。

URL 类别

AsyncOS for Web 允许您配置设备如何基于特定请求的URL 类别处理事务。使用预定义的类别列表，您可以选择按类别监控或阻止内容。您还可以创建自定义URL类别并选择允许、监控或阻止自定义类别中的网站的流量。

Web 信誉

Web信誉设置继承全局设置。要为特定策略组自定义Web信誉过滤，您可使用“Web信誉设置”(Web Reputation Setting) 下拉菜单自定义 Web 信誉分数阈值。

仅可为思科数据安全策略的 Web 信誉阈值设置配置负值和零值。根据定义，系统会监控所有正值分数。

内容阻止

您可以基于以下文件特性，使用“思科数据安全”(Cisco Data Security)>“内容”(Content) 页面上的设置将 Web 代理配置为阻止数据上传：

- **文件大小**。您可以指定允许的最大上传大小。大小等于或大于指定的最大值的所有上传均被阻止。您可为 HTTP/HTTPS 和本机 FTP 请求指定不同的最大文件大小。

  当上传请求大小大于最大上传大小和最大扫描大小（在“安全服务”(Security Services)>“防恶意软件”(Anti-Malware) 页面上的“DVS 引擎对象扫描限制”(DVS Engine Object Scanning Limits)

字段中配置）时，上传请求仍被阻止，但数据安全日志中的条目不记录文件名和内容类型。访问日志中的条目不变。

- **文件类型**。您可以阻止预定义文件类型或您输入的自定义 MIME 类型。当您阻止预定义文件类型时，您可以阻止该类型的所有文件或大于指定大小的文件。当您按大小阻止文件类型时，可以指定的最大文件大小与“安全服务”(Security Services) > “防恶意软件”(Anti-Malware) 页面上的“DVS 引擎对象扫描限制”(DVS Engine Object Scanning Limits) 字段的值相同。默认情况下，该值为 32 MB。

  按文件类型阻止时，思科数据安全过滤器不检查存档文件的内容。存档文件可按其文件类型或文件名而不根据其内容来阻止。

  注释 对于某些 MIME 类型组，阻止一个类型即会阻止该组中的所有 MIME 类型。例如，阻止 application/x-java-applet 即会阻止所有 Java MIME 类型，例如 application/java 和 application/javascript。

- **文件名**。您可以阻止使用指定名称的文件。您可以将文本用作文字字符串或正则表达式，用于指定要阻止的文件名。

  注释 请只输入使用 8 位 ASCII 字符的文件名。Web 代理仅匹配使用 8 位 ASCII 字符的文件名。

定义外部 DLP 系统

通过在设备中定义多台DLP服务器，网络安全设备可与同一个供应商的多台外部DLP服务器集成。您可以定义在与DLP系统联系时Web代理使用的负载均衡技术。定义多个DLP系统时，这很有用。请参阅SSL 配置，第 404 页，了解如何指定用于保护与外部 DLP 服务器的通信的协议。

注释 验证外部 DLP 服务器不发送 Web 代理修改的内容。AsyncOS for Web 仅支持阻止或允许上传请求的能力。它不支持上传由外部 DLP 服务器修改的内容。

配置外部 DLP 服务器

步骤 1 依次选择**网络 (Network) > 外部 DLP 服务器 (External DLP Servers)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

设置	说明
用于外部DLP服务器的协议 (Protocol for External DLP Servers)	选择以下任一协议： • **ICAP** – 对 DLP 客户端/服务器 ICAP 通信不进行加密。 • **安全 ICAP (Secure ICAP)** – 通过加密隧道进行 DLP 客户端/服务器 ICAP 通信。系统会显示其他选项。

外部 DLP 服务器 (External DLP Servers)	输入以下信息以访问 ICAP 兼容 DLP 系统：
	• **服务器地址 (Server address)** 和**端口 (Port)** - 用于访问 DLP 系统的主机名或 IP 地址和 TCP 端口。
	• **重新连接尝试次数 (Reconnection attempts)** - Web 代理在连接 DLP 系统失败之前的连接尝试次数。
	• **服务 URL (Service URL)** - 针对特定 DLP 服务器的 ICAP 查询 URL。Web 代理将您在此处输入的内容包括在它发送到外部 DLP 服务器的 ICAP 请求中。URL 必须以 ICAP 协议开头：icap://
	• 证书 (Certificate)（可选）- 所提供的用于保护外部 DLP 服务器连接安全的证书可以是证书颁发机构 (CA) 签名证书或自签名证书。从指定服务器获取证书，然后将其上传到设备：
	  • 浏览并选择证书文件，然后点击**上传文件 (Upload File)**。
	  注释 此单个文件必须包含客户端证书和未加密形式的私钥。
	  • **将此证书用于所有采用安全 ICAP 的 DLP 服务 (Use this certificate for all DLP servers using Secure ICAP)** - 选中此复选框可将同一证书用于您在此处定义的所有外部 DLP 服务器。取消选中此选项，可为每台服务器输入不同的证书。
	• 开始测试 – 您可以点击**开始测试 (Start Test)** 以测试网络安全设备与已定义的外部 DLP 服务器之间的连接。

负载均衡 (Load Balancing)	如果定义了多台 DLP 服务器，可选择 Web 代理使用哪种负载均衡技术将上传请求分配到不同 DLP 服务器。您可以选择以下负载均衡技术： • **无（故障切换）(None [failover])**。Web 代理将上传请求定向到一台 DLP 服务器。它会尝试按照它们列出的顺序连接到 DLP 服务器。如果一台 DLP 服务器无法接通，Web 代理尝试连接到列表中的下一台服务器。 • **最小连接数 (Fewest connections)**。Web 代理记录不同的 DLP 服务器有多少个有效请求，然后将上传请求定向到当前处理最少连接数的 DLP 服务器。 • **基于散列 (Hash based)**。Web 代理使用散列函数将请求分配到 DLP 服务器。散列函数使用代理 ID 和 URL 作为输入，以便相同 URL 的请求总是定向到同一台 DLP 服务器。 • **轮询 (Round robin)**。Web 代理按列出的顺序在所有 DLP 服务器之间均衡地循环上传请求。
服务请求超时 (Service Request Timeout)	输入 Web 代理等待 DLP 服务器响应的时间。当超过此时间时，ICAP 请求失败，上传请求被阻止或允许，具体取决于故障处理设置。 默认值为 60 秒。

设置	说明
最大同时连接数 (Maximum Simultaneous Connections)	指定从网络安全设备发送至每台已配置外部 DLP 服务器的最大同时 ICAP 请求连接数。此页面上的“故障处理”(Failure Handling) 设置适用于超过此限制的任何请求。 默认值为 25。
故障处理 (Failure Handling)	选择在DLP服务器无法提供及时响应时上传请求是被阻止还是允许（传递到访问策略进行评估）。 默认为允许（“允许在不扫描的情况下继续传输所有数据”(Permit all data transfers to proceed without scanning)）。
受信任的根证书 (Trusted Root Certificate)	浏览并为外部DLP服务器提供的证书选择受信任的根证书，然后点击“上传文件”(Upload Files)。有关其他信息，请参阅证书管理，第 406 页。
无效证书选项 (Invalid Certificate Options)	指定对各种无效证书的处理方式：**丢弃 (Drop)** 或**监控 (Monitor)**。
服务器证书 (Server Certificates)	此部分显示当前设备上可用的所有 DLP 服务器证书。

步骤 3 （可选）可以通过点击**添加行 (Add Row)** 并在提供的新字段中输入 DLP 服务器信息，添加另一台 DLP 服务器。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

使用外部 DLP 策略控制上传请求

Web 代理收到上传请求报头之后，Web 代理即拥有了必要的信息，可决定请求是否应转到外部 DLP 系统进行扫描。DLP 系统扫描请求并将判定返回给 Web 代理，然后阻止或监控（根据访问策略评估请求）。

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > 外部防数据丢失 (External Data Loss Prevention)**。

步骤 2 点击您要配置的策略组的“目标”(Destinations) 列下面的链接。

步骤 3 在**编辑目标设置 (Edit Destination Settings)** 部分下，选择**定义目标扫描自定义设置 (Define Destinations Scanning Custom Settings)**。

步骤 4 在**待扫描目标 (Destination to scan)** 部分中，选择以下选项之一：

- **不扫描任何上传 (Do not scan any uploads)**。不将上传请求发送到已配置的 DLP 系统进行扫描。所有上传请求均根据访问策略进行评估。
- **扫描所有上传 (Scan all uploads)**。所有上传请求均发送到已配置的 DLP 系统进行扫描。上传请求被阻止或根据访问策略进行评估，具体取决于 DLP 系统扫描判定。
- **扫描指定自定义和外部 URL 类别以外的上传内容 (Scan uploads except to specified custom and external URL categories)**。归属于特定自定义 URL 类别的上传请求发送到已配置的 DLP 系统进行扫描。上传请求被阻止或

根据访问策略进行评估，具体取决于 DLP 系统扫描判定。点击**编辑自定义类别列表 (Edit custom categories list)** 以选择要扫描的 URL 类别。

步骤 5 “提交”(Submit) 并“确认更改”(Commit Changes)。

对防数据丢失扫描的日志记录

访问日志指示上传请求是否由思科数据安全过滤器或外部DLP服务器扫描。访问日志条目包括一个思科数据安全扫描判定字段和另一个基于外部 DLP 扫描判定的字段。

除了访问日志以外，网络安全设备还提供以下日志文件类型，以便排除 Cisco 数据安全和外部 DLP 策略的故障：

- **数据安全日志 (Data Security Logs)**。记录由思科数据安全过滤器评估的上传请求的客户端历史记录。
- **数据安全模块日志 (Data Security Module Logs)**。记录与思科数据安全过滤器相关的消息。
- **默认代理日志 (Default Proxy Logs)**。除了记录与 Web 代理相关的错误，默认代理日志还包含与连接到外部DLP服务器相关的消息。这样就让您可以解决外部DLP服务器的连接或集成问题。

以下文本说明了一个示例数据安全日志条目：

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

字段值	说明
`Mon Mar 30 03:02:13 2009 Info:`	时间戳和跟踪级别
`303`	事务 ID
`10.1.1.1`	源 IP 地址
`-`	用户名
`-`	授权组名称
`<<bar,text/plain,5120><foo,text/plain,5120>>`	立刻上传的每个文件的文件名、文件类型、文件大小 **注释** 此字段不包括小于已配置最小请求正文大小（默认为 4096 字节）的文本/明文文件。
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	思科数据安全策略和操作

字段值	说明
`ns`	Web 信誉分数
`server.com`	传出 URL
`nc`	URL 类别

注释 要了解向站点发送的数据传输（例如 POST 请求）何时被外部 DLP 服务器阻止，可在访问日志中搜索 DLP 服务器的 IP 地址或主机名。

第 18 章

通知最终用户代理操作

本章包含以下部分：

最终用户通知概述

您可以为最终用户配置以下类型的通知：

选项	说明	详细信息
最终用户确认页面 (End-user acknowledgement page)	通知最终用户其 Web 活动正在接受过滤和监控。用户在一定时间段后初次访问浏览器时，系统显示最终用户确认页面。	最终用户确认页面， 第 277 页
最终用户通知页面 (End-user notification pages)	访问特定页面受阻时向最终用户显示阻止的原因。	最终用户通知页面， 第 279 页
最终用户 URL 过滤警告页面 (End-user URL filtering warning page)	警告最终用户他们正在访问的网站不符合贵组织可接受的使用策略，并且如果他们选择访问则允许他们继续。	配置最终用户 URL 过滤警告页面， 第 283 页

选项	说明	详细信息
FTP 通知消息 (FTP notification messages)	向最终用户提供本地FTP事务被阻止的原因。	配置FTP通知消息，第284页。
时间和数量配额到期警告页面 (Time and Volume Quotas Expiry Warning Page)	当最终用户由于其已达到配置的数据量或时间限制而被阻止访问时，通知最终用户。	可在“安全服务”(Security Services) > “最终用户通知”(End User Notification) 页面的“时间和数量配额到期警告页面”(Time and Volume Quotas Expiry Warning Page) 部分配置这些设置。 另请参阅时间范围和配额，第191页。

配置通知页面的一般设置

指定通知页面的显示语言和徽标。此过程中会说明限制信息。

步骤 1 依次选择**安全服务 (Security Services) > 最终用户通知 (End-User Notification)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在“一般设置”(General Settings) 部分中，选择显示通知页面时 Web 代理应使用的语言。

- HTTP 语言设置适用于所有 HTTP 通知页面（确认、机上最终用户、自定义最终用户和最终用户 URL 过滤警告页面）。
- FTP 语言适用于所有 FTP 通知消息。

步骤 4 选择在各通知页面上是否使用徽标。可以指定在“使用自定义徽标”(Use Custom Logo) 字段中所输入的 URL 上引用的思科徽标或任何图形文件。

此设置适用于 IPv4 上服务的所有 HTTP 通知页面。AsyncOS 不支持 IPv6 上的图像。

步骤 5 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 针对通知页面上的 URL 和徽标的警告，第285页

最终用户确认页面

您可以将网络安全设备配置为通知用户其正在过滤和监控 Web 活动。配置后，设备将为使用 HTTP 或HTTPS 访问网络的每个用户显示一个最终用户确认页面。用户尝试初次访问网站时或在配置的时间间隔后，设备将显示最终用户确认页面。

如果身份验证后用户名可用，则 Web 代理按用户名跟踪用户。如果无可用的用户名，则可以选择用户跟踪方式，即通过 IP 地址或网络浏览器会话 Cookie。

注释 最终用户确认页面中无本地 FTP 事务。

- 利用最终用户确认页面访问 HTTPS 和 FTP 站点，第 277 页
- 关于最终用户确认页面，第 277 页
- 配置最终用户确认页面，第 278 页

利用最终用户确认页面访问 HTTPS 和 FTP 站点

最终用户确认页面工作，因为其向最终用户显示迫使其点击可接受使用策略协议的 HTML 页面。用户点击链接后，Web 代理将客户端重定向至最初请求的网站。如果没有可用于用户的用户名，则使用代理持续跟踪用户何时接受最终用户确认页面（通过 IP 地址或网络浏览器会话 Cookie）。

- **HTTPS**。Web 代理使用 Cookie 跟踪用户是否已确认最终用户确认页面，但无法获取该 Cookie，除非其解密事务。当最终用户确认页面已启用并使用会话 Cookie 跟踪用户时，您可以选择绕过（通过）或丢弃 HTTPS 请求。使用 advancedproxyconfig > EUN CLI 命令完成此操作，并且对“要使用基于会话的 EUA 对 HTTPS 请求采取的操作（“绕过”或“丢弃”）”（Action to be taken for HTTPS requests with Session based EUA ["bypass" or "drop"]）命令选择旁路。
- **FTP over HTTP**。网络浏览器从不发送 FTP over HTTP 事务的 Cookie，因此 Web 代理无法获取 Cookie。要解决该问题，可以免除 FTP over HTTP 事务需要最终用户确认页面。执行此操作的方法为将“ftp://”作为正则表达式（不带引号）创建自定义 URL 类别，并定义身份策略，即免除用户接收用于该自定义 URL 类别的最终用户确认页面。

关于最终用户确认页面

- 按 IP 地址跟踪用户时，设备使用最大时间间隔和最大 IP 地址闲置超时中的最短值，来确定再次显示最终用户确认页面的时间。
- 使用会话 Cookie 跟踪用户时，如果用户关闭然后重新打开其网络浏览器或打开第二个网络浏览器应用，则 Web 代理将再次显示最终用户确认页面。
- 客户端访问 HTTPS 站点或使用 FTP over HTTP 访问 FTP 服务器时，无法使用会话 Cookie 跟踪用户。
- 以显式转发模式部署设备并且用户转至 HTTPS 站点时，最终用户确认页面仅在将用户重定向至最初请求 URL 的链接中包含该域名。如果最初请求 URL 在域名后包含文本，则该文本被截断。

- 向用户显示最终用户确认页面时，该事务的访问日志条目将 OTHER 显示为 ACL 决策标签。这是由于最初请求 URL 受阻，而且取而代之的是向用户显示最终用户确认页面。

配置最终用户确认页面

开始之前

- 要配置显示语言和自定义显示的徽标，请参阅配置通知页面的一般设置，第 276 页。
- 如果要自定义向最终用户显示的消息，请参阅通知页面上的自定义消息，第 284 页。如果您需要比“自定义消息”(Custom Message) 框允许的更多的自定义，请参阅直接编辑通知页面 HTML 文件，第 286 页。

可以在 Web 界面或命令行界面中启用和配置最终用户确认页面。在 Web 界面中配置最终用户确认页面时，可以包括出现在各页面上的自定义消息。

在 CLI 中，使用 `advancedproxyconfig > eun`。

步骤 1 依次选择**安全服务 (Security Services) > 最终用户通知 (End-User Notification)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 启用**要求最终用户在确认页面中点击 (Require end-user to click through acknowledgment page)** 字段。

步骤 4 输入选项：

设置	说明
确认间隔时间 (Time Between Acknowledgements)	“确认间隔时间”(Time Between Acknowledgments) 确定 Web 代理显示各用户最终用户确认页面的频率。该设置适用于按用户名跟踪的用户以及按 IP 地址或会话 Cookie 跟踪的用户。可以指定 30 至 2678400 秒（一个月）之间的任何值。默认值为一天（86400 秒）。 “确认间隔时间”(Time Between Acknowledgments) 更改并应用后，即使对于已确认 Web 代理的用户，Web 代理也使用新值。
不活动超时 (Inactivity Timeout)	“不活动超时”(Inactivity Timeout) 将确定按 IP 地址或会话 Cookie（仅未进行身份验证的用户）跟踪和确认的用户在不再被视为同意可接受的使用策略认前可空闲多久。可以指定 30 至 2678400 秒（一个月）之间的任何值。默认值为四小时（14400 秒）。

设置	说明
代理类型 (Surrogate Type)	确定 Web 代理使用哪种方法跟踪用户： • **IP 地址 (IP Address)**。Web 代理允许该 IP 地址上的用户使用任何网络浏览器或非浏览器 HTTP 进程访问网络，但条件是用户点击最终用户确认页面上的链接。按 IP 地址跟踪用户允许用户访问网络，直至由于不活动或配置的新确认时间间隔，Web 代理显示新的最终用户确认页面。不同于按会话 Cookie 跟踪，按 IP 地址跟踪允许用户打开多个网络浏览器应用，而不必同意最终用户确认，除非配置的时间时间已到期。 注释 配置 IP 地址且对用户进行身份验证后，Web 代理按用户名而不是 IP 地址跟踪用户。 • **会话 Cookie (Session Cookie)**。用户点击最终确认页面上的链接并使用 Cookie 跟踪会话时，Web 代理向用户的网络浏览器发送 Cookie。用户可以使用网络浏览器继续访问网络直至“确认间隔时间”(Time Between Acknowledgments) 值过期、不活动时间长于分配时间或关闭网络浏览器。 如果用户使用非浏览器 HTTP 客户端应用，则必须能够点击最终用户确认页面上的链接以访问网络。如果用户打开第二个网络浏览器应用，则必须再次通过最终用户确认过程以便 Web 代理将会话 Cookie 发送至第二个网络浏览器。 注释 客户端访问 HTTPS 站点或使用 FTP over HTTP 访问 FTP 服务器时，不支持使用会话 Cookie 跟踪用户。
自定义消息 (Custom message)	自定义出现在各最终用户确认页面上的文本。可以包括某些简单的 HTML 标签以格式化文本。 注释 相对于 CLI，在网络界面中配置最终用户确认页面时，仅可以包括自定义消息。 另请参阅通知页面上的自定义消息，第 284 页。

步骤 5 （可选）点击**预览确认页面自定义 (Preview Acknowledgment Page Customization)**，在单独浏览器窗口中查看当前最终用户通知页面。

注释 如果已编辑通知 HTML 文件，则该预览功能不可用。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

最终用户通知页面

策略阻止用户浏览网站时，可配置设备通知用户 URL 请求阻止原因。共有几种方法：

目标	请参阅
显示托管在网络安全设备上的可自定义的预定义页面。	配置机上最终用户通知页面，第 280 页

目标	请参阅
将用户重定向到位于特定URL的HTTP最终用户通知页面。	机下最终用户通知页面，第 280 页

配置机上最终用户通知页面

开始之前

- 要配置显示语言和自定义显示的徽标，请参阅配置通知页面的一般设置，第 276 页。
- 如果您使用机上通知自定义显示的消息，请查看通知页面上的自定义消息，第284页下的主题。如果您需要比“自定义消息”(Custom Message) 框允许的更多的自定义，请参阅直接编辑通知页面 HTML 文件，第 286 页。

机上页面是设备上预定义的、可自定义的通知页面。

步骤 1 **安全服务 (Security Services) > 最终用户通知 (End-User Notification)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 从“通知类型”(Notification Type) 字段中，选择**使用机上最终用户通知 (Use On Box End User Notification)**。

步骤 4 配置机上最终用户通知页面设置。

设置	说明
自定义消息 (Custom Message)	包括各通知页面上所需的任何其他文本。输入自定义消息后，AsyncOS 将该消息置于包含联系信息的通知页面上的最后语句前面。
联系信息 (Contact Information)	自定义列于各通知页面上的联系信息。 提供用户可提供给网络管理员的通知代码前，AsyncOS 将联系信息语句显示为一页上的最后语句。
最终用户误分类报告 (End-User Misclassification Reporting)	启用后，用户可向思科报告误分类的 URL。附加按钮出现在由于可疑恶意软件或 URL 过滤器而受阻站点的机上最终用户通知页面上。通过该按钮，用户能够报告其认为页面被误分类的时间。但对于由于其他策略设置而受阻的页面，则不显示该按钮。

步骤 5 （可选）点击**预览通知页面自定义 (Preview Notification Page Customization)** 链接，可在单独浏览器窗口中查看当前最终用户通知页面。

注释 如果已编辑通知 HTML 文件，则该预览功能不可用。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

机下最终用户通知页面

可以将 Web 代理配置为将所有 HTTP 最终用户通知页面重定向至您指定的特定 URL。

根据阻止访问的原因显示正确的机下页面

默认情况下，AsyncOS 将所有受阻网站重定向至 URL，而不考虑为何其阻止原始页面的原因。但是，AsyncOS 还将作为查询字符串的参数附加至重定向 URL，因此，可以确保用户看到说明受阻原因的唯一页面。有关所包含参数的详细信息，请参阅机下最终用户通知页面参数，第 281 页。

如果您希望用户查看出于各种原因的不同受阻网站页面，则在可以解析重定向 URL 中查询字符串的 Web 服务器上构建 CGI 脚本。然后，服务器可以执行至适当页面的第二次重定向。

机下通知页面的 URL 条件

- 可以使用任何 HTTP 或 HTTPS URL。
- URL 可以指定特定端口号。
- URL 在问号后不得有任何参数。
- URL 必须包含正确格式的主机名。

例如，如果在“重定向至自定义 URL”(Redirect to Custom URL) 字段中输入以下 URL：

```
http://www.example.com/eun.policy.html
```

并且具有以下访问日志条目：

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html HTTP/1.1
 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

AsyncOS 创建以下重定向 URL：

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

机下最终用户通知页面参数

AsyncOS 将参数用作 HTTP GET 请求中的标准 URL 参数传递至 Web 服务器。其使用以下格式：

```
<notification_page_url>?param1=value1&param2=value2
```

该表介绍 AsyncOS 的查询字符串中的参数。

参数名	说明
Time	事务日期和时间。

参数名	说明
ID	事务 ID。
Client_IP	客户端的 IP 地址。
User	发出请求的客户端的用户名（如果可用）。
Site	HTTP 请求中的目标的主机名。
URI	HTTP 请求中指定的 URL 路径。
Status_Code	请求的 HTTP 状态代码。
Decision_Tag	如访问日志条目中定义的 ACL 决策标记，指示 DVS 引擎如何处理事务。
URL_Cat	URL 过滤引擎分配给事务请求的 URL 类别。 **注：**AsyncOS for Web 发送预定义和用户定义 URL 类别的整个 URL 类别名称。其对类别名称执行 URL 编码，因此空间被写为“%20”。
WBRS	Web 信誉过滤器分配给请求中的 URL 的 WBRS 分数。
DVS_Verdict	DVS 引擎分配给事务的恶意软件类别。
DVS_ThreatName	DVS 引擎发现的恶意软件的名称。
Reauth_URL	用户可以点击以再次进行身份验证的 URL，但条件是用户由于限制性 URL 过滤策略而受阻止访问某网站。在“如果按URL类别或用户会话限制阻止最终用户，则启用重新验证提示”(Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction) 全局身份验证设置启用后，并且用户由于受阻的 URL 类别而被阻止访问某网站时，使用该参数。 要使用该参数，确保 CGI 脚本执行以下步骤： 1.获取 `Reauth_Url` 参数值。 2.URL-解码该值。 3.Base64 解码该值并获取实际重新验证 URL。 4.以某种方式（作为链接或按钮）在最终用户通知页面上包含解码URL，加上告知用户其可点击该链接并输入可进一步访问的新身份验证凭证的用户说明。

注释 AsyncOS 始终将所有参数包含在各重定向 URL 中。如果不存在适用于特定参数的值，则 AsyncOS 传递一个连字符 (-)。

将最终用户通知页面重定向至自定义 URL（机下）

步骤 1 安全服务 (Security Services) > 最终用户通知 (End-User Notification)。
步骤 2 点击编辑设置 (Edit Settings)。
步骤 3 在最终用户通知页面 (End-User Notification Pages) 部分中，选择重定向至自定义 URL (Redirect to Custom URL)。
步骤 4 在通知页面 URL (Notification Page URL) 字段中，输入要将受阻网站重定向到的 URL。
步骤 5 （可选）点击预览自定义 URL (Preview Custom URL) 链接。
步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

配置最终用户 URL 过滤警告页面

开始之前

- 如果您使用机上通知自定义显示的消息，请查看通知页面上的自定义消息，第 284 页下的主题。如果您需要比“自定义消息”(Custom Message) 框允许的更多的自定义，请参阅直接编辑通知页面 HTML 文件，第 286 页。

用户在一定时间段后初次访问特定 URL 类中的网站时，系统显示最终用户 URL 过滤警告页面。启用网站内容分级功能后，用户访问成人内容时，您也可以配置警告页面。

步骤 1 安全服务 (Security Services) > 最终用户通知 (End-User Notification)。
步骤 2 点击编辑设置 (Edit Settings)。
步骤 3 向下滚动至“最终用户 URL 过滤警告页面”(End-User URL Filtering Warning Page) 部分。
步骤 4 在“警告间隔时间”(Time Between Warning) 字段中，输入 Web 代理根据用户显示各 URL 类别的最终用户 URL 过滤警告页面所用的时间间隔。

可以指定 30 至 2678400 秒（一个月）之间的任何值。默认值为 1 小时（3600 秒）。可以输入以秒、分钟或天为单位的值。用“s”代表秒，“m”代表分钟，“d”代表天。

步骤 5 在“自定义消息”(Custom Message) 字段中，输入要显示在各最终用户 URL 过滤警告页面上的文本。
步骤 6 （可选）点击预览 URL 类别警告页面自定义 (Preview URL Category Warning Page Customization)，可在单独浏览器窗口中查看当前最终用户 URL 过滤警告页面。

注释 如果已编辑通知 HTML 文件，则该预览功能不可用。

步骤 7 “提交”(Submit) 并“确认更改”(Commit Changes)。

配置 FTP 通知消息

开始之前

如果您使用机上通知自定义显示的消息，请查看通知页面上的自定义消息，第 284 页下的主题。如果您需要比“自定义消息”(Custom Message) 框允许的更多的自定义，请参阅直接编辑通知页面 HTML 文件，第 286 页。

如果 FTP 代理出于任何原因（例如 FTP 代理身份验证错误或者服务器域名信誉不良）无法与 FTP 服务器建立连接，则 FTP 代理向本地 FTP 客户端显示预定义、可定制的通知消息。通知是针对连接被阻的原因。

步骤 1 **安全服务 (Security Services) > 最终用户通知 (End-User Notification)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 向下滚动至“本地 FTP”(Native FTP) 部分。

步骤 4 在**语言(Language)** 字段中，选择显示本地 FTP 通知消息时所用的语言。

步骤 5 在**自定义消息 (Custom Message)** 字段中，输入在各条本地 FTP 通知消息中要显示的文本。

步骤 6 “提交”(Submit) 并“确认更改”(Commit Changes)。

通知页面上的自定义消息

以下章节适用于在“编辑最终用户通知”(Edit End User Notification) 页面上配置的任何通知类型的“自定义消息”(Custom Message) 框中输入的文本。

- 通知页面上自定义消息中支持的 HTML 标签，第 284 页
- 针对通知页面上的 URL 和徽标的警告，第 285 页

通知页面上自定义消息中支持的 HTML 标签

您可以使用 HTML 标签来设置用于提供“自定义消息”(Custom Message) 框的“编辑最终用户通知”(Edit End User Notification) 页面上任何通知文本的格式。标签必须为小写，并遵循标准 HTML 语法（结束标签等）。

可以使用以下 HTML 标签。

- <a>
-
-
- <big></big>
-
- <code></code>

-
-
- <small></small>
-

例如，可以倾斜某些文本：

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

如果带有 标签，可以使用任何 CSS 样式格式化文本。例如，可以让某些 文本以红色显示：

```
 <span style=”color: red”>Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

注释 如果您需要更高的灵活性，或者要添加 JavaScript 到通知页面，则必须直接编辑 HTML 通知文件。在 Web 用户界面上用于通知的“自定义消息”(Custom Message) 框输入的 JavaScript 会被删掉。请参阅直接编辑通知页面 HTML 文件 ， 第 286 页。

针对通知页面上的 URL 和徽标的警告

此部分适用于您将进行以下任何自定义的情况：

- 在“编辑最终用户通知”(End User Notification) 页面上，在“自定义消息”(Custom Message) 框中为任何通知输入文本。
- 直接编辑对应于机上通知的 HTML 文件。
- 使用自定义徽标。

对于URL路径与自定义文本内嵌入链接中域名的所有组合以及自定义徽标，不受针对机上通知的以下情况的影响：

- 用户身份验证
- 最终用户确认
- 所有扫描，例如恶意软件扫描和 Web 信誉分数

例如，如果自定义文本中嵌入以下 URL：

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

然后，也将以下所有 URL 处理为无需任何扫描：

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

```
http://www.example.com/logo.jpg
```

```
http://www.mycompany.com/index.html
```

此外，如果嵌入式 URL 采用以下形式：`<protocol>://<domain-name>/<directory path>/`，则主机上该目录路径下的所有子文件和子目录也将无需所有扫描。

例如，如果嵌入以下 URL：`http://www.example.com/gallery2/`，诸如 `http://www.example.com/gallery2/main.php` 的 URL 也被视为无需任何扫描。

因此，您可以利用嵌入式内容创建更复杂的页面，但前提是该嵌入式内容与初始URL相关。但是，您在决定包括哪些作为链接和自定义徽标的路径时也应注意。

直接编辑通知页面 HTML 文件

各通知页面在网络安全设备上存储为 HTML 文件。如果需要比 Web 界面的“自定义消息”(Custom Message) 框中所允许自定义更多的自定义，您可以直接编辑这些 HTML 文件。例如，您可以包括标准 JavaScript，或编辑每个页面的整体外观和风格。

以下各节中的信息适用于设备上任何类型的最终用户通知 HTML 文件，包括最终用户确认页面。

- 对直接编辑通知 HTML 文件的要求，第 286 页
- 直接编辑通知页面 HTML 文件，第 286 页
- 在通知 HTML 文件中使用变量，第 287 页
- 用于自定义通知 HTML 文件的变量，第 288 页

对直接编辑通知 HTML 文件的要求

- 各通知页面文件必须是有效的HTML文件。有关可以包括的HTML标签列表，请参阅通知页面上自定义消息中支持的 HTML 标签，第 284 页。
- 自定义通知页面文件名必须完全匹配网络安全设备随附的文件名。

  如果 `configuration\eun` 目录不含带有所需名称的特定文件，则设备显示标准机上最终用户通知页面。

- 不要在 HTML 文件中含有任何 URL 链接。通知页面中所含的任何链接均受约束于访问策略中定义的访问控制规则，并且用户可能会以递归循环结束。
- 在支持的客户端浏览器上测试您的 HTML 文件（尤其是如果包含 JavaScript 的 HTML 文件），以确保它们的行为符合预期。
- 要使您自定义的页面生效，您必须使用 `advancedproxyconfig > EUN > Refresh EUN Pages` CLI 命令启用自定义文件。

直接编辑通知 HTML 文件

开始之前

- 了解对直接编辑通知 HTML 文件的要求，第 286 页中的要求。
- 请参阅用于自定义通知 HTML 文件的变量，第 288 页 和 在通知 HTML 文件中使用变量，第 287 页。

步骤 1 使用 FTP 客户端连接网络安全设备。

步骤 2 导航至 `configuration\eun` 目录。

步骤 3 下载要编辑的通知页面的语言目录文件。

步骤 4 在本地计算机上，使用文本编辑器或 HTML 编辑器编辑 HTML 文件。

步骤 5 使用 FTP 客户端将自定义 HTML 文件上传至在第 3 步期间从中下载这些文件的同一目录。

步骤 6 打开 SSH 客户端并连接到网络安全设备。

步骤 7 运行 `advancedproxyconfig > EUN` CLI 命令。

步骤 8 键入 **2** 以使用自定义最终用户通知页面。

步骤 9 如果在更新 HTML 文件时，当前已启用自定义最终用户通知页面选项，则必须键入 **1** 以刷新自定义最终用户通知页面。

如果不执行此操作，则 Web 代理重启后，新文件才生效。

步骤 10 确认您的更改。

步骤 11 关闭 SSH 客户端。

在通知 HTML 文件中使用变量

编辑通知HTML文件时，可以包含条件变量以创建如果-那么语句，从而进行不同的操作，这取决于当前状态。

该表介绍不同条件变量格式。

条件变量格式	说明
%?*V*	如果变量 %*V* 输出不为空，则该条件变量的求值结果为“真”(TRUE)。
%!*V*	表示以下条件： `else` 将其与 %?*V* 条件变量结合使用。
%#*V*	表示以下条件： `endif` 将其与 %?*V* 条件变量结合使用。

例如，以下文本显示的是将%R用作条件变量以检查是否提供重新验证，并将%r用作常规变量以提供重新验证 URL 的某一 HTML 代码。

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'"
id="Reauth" value="Login as different user...">
```

```
  </form>
</div>
%#R
```

用于自定义通知HTML 文件的变量，第 288 页中所含的任何变量均可用作条件变量。但是，条件语句中所使用的最佳变量为与客户端请求而不是与服务器响应相关，以及求值结果或为“真”(TRUE) 而不是始终为“真”(TRUE) 的那些变量。

用于自定义通知 HTML 文件的变量

可以在通知 HTML 文件中使用变量来向用户显示具体信息。还可以将各变量转换为条件变量，以创建 if-then 语句。有关详细信息，请参阅在通知 HTML 文件中使用变量，第 287 页。

变量	说明	如果用作条件变量，则求值结果始终为“真”(TRUE)
%a	FTP 身份验证领域	否
%A	ARP 地址	是
%b	用户代理名称	否
%B	阻止原因，例如 BLOCK-SRC 或 BLOCK-TYPE	否
%c	错误页面联系人	是
%C	整个 Set-Cookie：标题行或空字符串	否
%d	客户端 IP 地址	是
%D	用户名	否
%e	错误页面邮件地址	是
%E	错误页面徽标 URL	否
%f	用户反馈部分	否
%F	用户反馈 URL	否
%g	Web 类别名称（如果可用）	是
%G	允许的最大文件大小（单位：MB）	否
%h	代理主机名	是
%H	URL 服务器名称	是
%i	以十六进制数表示的事务 ID	是
%I	管理 IP 地址	是

变量	说明	如果用作条件变量，则求值结果始终为“真”(TRUE)
%j	URL 类别警告页面自定义文本	否
%k	最终用户确认页面和最终用户 URL 过滤警告页面重定向链接	否
%K	响应文件类型	否
%l	WWW-身份验证：标题行	否
%L	代理-身份验证：标题行	否
%M	请求方法，例如“GET”或“POST”	是
%n	恶意软件类别名称（如果可用）	否
%N	恶意软件威胁名称（如果可用）	否
%o	Web 信誉威胁类型（如果可用）	否
%O	Web 信誉威胁原因（如果可用）	否
%p	代理-连接 HTTP 报头字符串	是
%P	协议	是
%q	身份策略组名	是
%Q	非身份策略的策略组名	是
%r	重定向 URL	否
%R	提供重新验证。值为假时，该变量输出空字符串，为真时输出空格，因此单独使用时无用。相反，应该将其用作条件变量。	否
%S	代理签名	否，求值结果始终为“假”(FALSE)
%t	以 Unix 秒 + 毫秒表示的时间戳	是
%T	日期	是
%u	URL 的 URI 部分（URL，不包括服务器名称）	是
%U	请求的完整 URL	是
%v	HTTP 协议版本	是
%W	管理 WebUI 端口	是

变量	说明	如果用作条件变量，则求值结果始终为“真”(TRUE)
%X	扩展阻止代码。这是编码大多数 Web 信誉和记录在访问日志中防恶意软件信息（例如 ACL 决策标记和 WBRS 分数）的一个 16 字节 base64 值。	是
%Y	管理员自定义文本字符串（如已设置；否则为空）	否
%y	最终用户确认页面自定义文本	是
%z	Web 信誉分数	是
%Z	DLP 元数据	是
%%	在通知页面上显示百分比符号 (%)	不适用

通知页面类型

默认情况下，Web 代理显示通知页面，告知用户受阻及受阻原因。

大多数通知页面显示不同的代码集，可帮助管理员或思科客户支持诊断任何问题。某些代码仅供思科内部使用。可能出现在通知页面中的不同代码与可以包括在自定义通知页面中的变量相同，如用于自定义通知 HTML 文件的变量，第 288 页中所示。

该表介绍用户可能遇到的不同通知页面。

文件名和 通知标题	通知说明	通知文本
ERR_ACCEPTED 反馈已接受，谢谢 (Feedback Accepted, Thank You)	用户使用“报告误分类”(Report Misclassification) 选项后显示的通知页面。	分类错误报告已发送。感谢您的反馈。
ERR_ADAPTIVE_SECURITY 策略：通用 (Policy: General)	由于自适应扫描功能而阻止用户时显示的阻止页面。	根据贵组织的安全策略，此网站 <*URL*> 已被阻止，因为已确定其内容是一个安全风险。
ERR_ADULT_CONTENT 策略确认 (Policy Acknowledgment)	最终用户访问归为成人内容的页面时显示的警告页面。用户可以点击确认链接继续访问最初请求的站点。	您尝试访问的网页被评级为“色情或成人”内容。点击下面的链接即表示您确认已经阅读并同意该组织管制使用互联网阅读此类内容的规定。您的浏览行为的数据可能受到监控和记录。如果您继续访问此类网页，您将定期被要求确认此声明。 点击此处接受此声明并访问互联网。

文件名和 通知标题	通知说明	通知文本
ERR_AVC 策略：应用控制 (Policy: Application Controls)	由于应用可视性与可控性引擎而阻止用户时显示的阻止页面。	根据贵组织访问策略，已阻止访问类型为 %2 的应用 %1。
ERR_BAD_REQUEST 错误请求 (Bad Request)	由于事务请求无效而产生的错误页面。	系统无法处理此请求。非标准浏览器可能生成了无效的 HTTP 请求。 如果您正在使用标准浏览器，请重试请求。
ERR_BLOCK_DEST 策略：目标 (Policy: Destination)	用户尝试访问受阻网站地址时显示的阻止页面。	根据贵组织访问策略，已阻止访问此网站 <*URL*>。
ERR_BROWSER 安全：浏览器 (Security: Browser)	事务请求来自已被标识为受恶意软件或间谍软件入侵的应用时显示的阻止页面。	根据贵组织访问策略，已阻止计算机发出的请求，因为已确定该请求对组织网络构成安全威胁。浏览器可能已被标识为“<恶意软件名称>”的恶意软件/间谍软件代理入侵。 请联系<联系人姓名><邮件地址>并提供如下所示的代码。 如果您正在使用非标准浏览器并且认为其分类有误，请使用以下按钮报告此分类错误。
ERR_BROWSER_CUSTOM 策略：浏览器 (Policy: Browser)	事务请求来自受阻用户代理时显示的阻止页面。	根据贵组织访问策略，已阻止来自浏览器的请求。由于该浏览器“<浏览器类型>”可能存在安全风险而不被允许。
ERR_CERT_INVALID 证书无效 (Invalid Certificate)	请求的 HTTPS 站点使用无效证书时显示的阻止页面。	无法建立安全会话，因为站点<主机名> 提供的证书无效。
ERR_CONTINUE_UNACKNOWLEDGED 策略确认 (Policy Acknowledgment)	当用户请求已分配“警告”操作的自定义 URL 类别中的站点时显示的警告页面。用户可以点击确认链接继续访问最初请求的站点。	您正在尝试访问 URL 类别 <*URL* 类别>下的网页。点击下面链接即表示您确认已经阅读并同意该组织管制使用互联网阅读此类内容的规定。您的浏览行为的数据可能受到监控和记录。如果您继续访问此类网页，您将定期被要求确认此声明。 点击此处接受此声明并访问互联网。

文件名和 通知标题	通知说明	通知文本
ERR_DNS_FAIL DNS 故障 (DNS Failure)	请求的 URL 含无效域名时显示的错误页面。	对此主机名 <主机名> 的主机名解析（DNS 查找）已失败。互联网地址可能拼写错误或已过期，主机<主机名> 可能暂时不可用，或者 DNS 服务器可能无响应。 请检查输入的互联网地址拼写是否正确。如果地址正确，请稍后尝试此请求。
ERR_EXPECTATION_FAILED 期望无法满足 (Expectation Failed)	事务请求触发 HTTP 417“期望无法满足”响应时显示的错误页面。	系统无法处理此站点 <*URL*> 的请求。非标准浏览器可能生成了无效的 HTTP 请求。 如果正在使用标准浏览器，请重试请求。
ERR_FILE_SIZE 策略：文件大小 (Policy: File Size)	请求文件超过允许的最大文件大小时显示的阻止页面。	根据贵组织的访问策略，已阻止访问此网站或下载 <*URL*>，因为下载大小超过允许限制。
ERR_FILE_TYPE 策略：文件类型 (Policy: File Type)	请求文件为受阻文件类型时显示的阻止页面。	根据贵组织的访问策略，已阻止访问此网站或下载 <*URL*>，因为不允许使用该文件类型“<文件类型>”。
ERR_FILTER_FAILURE 过滤器故障 (Filter Failure)	URL 过滤引擎暂时无法提供 URL 过滤响应且将“默认无法访问服务操作”(Default Action for Unreachable Service) 选项设为“阻止”(Block) 时显示的错误页面。	对页面 <*URL*> 的请求受拒，因为内部服务器当前无法访问或超载。 请稍后重试请求。
ERR_FOUND 找到 (Found)	内部重定向页面存在一些错误。	页面 <*URL*> 正被重定向至 <重定向 *URL*>。
ERR_FTP_ABORTED FTP 中止 (FTP Aborted)	FTP over HTTP 事务请求触发 HTTP 416“请求范围无效”(Requested Range Not Satisfiable) 响应时显示的错误页面。	对文件 <*URL*> 的请求未成功。FTP 服务器 <主机名> 意外终止连接。 请稍后重试请求。

文件名和 通知标题	通知说明	通知文本
ERR_FTP_AUTH_REQUIRED 需 FTP 授权 (FTP Authorization Required)	FTP over HTTP 事务请求触发 FTP 530“未登录”(Not Logged In) 响应时显示的错误页面。	FTP 服务器 <主机名> 需要身份验证。当系统提示时，必须输入有效的用户 ID 和密码。 在某些情况下，FTP 服务器可能限制匿名连接数。如果您通常以匿名用户身份连接此服务器，请稍后再试。
ERR_FTP_CONNECTION_FAILED FTP 连接失败 (FTP Connection Failed)	FTP over HTTP 事务请求触发 FTP 425“无法打开数据连接”(Can’t open data connection) 响应时显示的错误页面。	系统无法与 FTP 服务器 <主机名> 通信。FTP 服务器可能暂时或永久停机，也可能由于网络问题而无法访问。 请检查输入的地址拼写是否正确。如果地址正确，请稍后尝试此请求。
ERR_FTP_FORBIDDEN FTP 禁止 (FTP Forbidden)	FTP over HTTP 事务请求针对不允许用户访问的对象时显示的错误页面。	FTP 服务器 <主机名> 拒绝访问。您的用户 ID 无权访问此文档。
ERR_FTP_NOT_FOUND FTP 未找到 (FTP Not Found)	FTP over HTTP 事务请求针对服务器上不存在的对象时显示的错误页面。	找不到文件 <*URL*>。地址不正确或已过期。
ERR_FTP_SERVER_ERR FTP 服务器错误 (FTP Server Error)	FTP over HTTP 事务尝试访问确实支持FTP的服务器时显示的错误页面。服务器通常返回 HTTP 501“未执行”(Not Implemented) 响应。	系统无法与 FTP 服务器 <主机名> 通信。FTP 服务器可能暂时或永久停机，也可能不提供此服务。 请确认此地址是否有效。如果地址正确，请稍后尝试此请求。
ERR_FTP_SERVICE_UNAVAIL FTP 服务不可用 (FTP Service Unavailable)	FTP over HTTP 事务尝试访问不可用的 FTP 服务器时显示的错误页面。	系统无法与 FTP 服务器 <主机名> 通信。FTP 服务器可能正忙或永久停机，也可能不提供此服务。 请确认此地址是否有效。如果地址正确，请稍后尝试此请求。
ERR_GATEWAY_TIMEOUT 网关超时 (Gateway Timeout)	请求服务器未及时响应时显示的错误页面。	系统无法与外部服务器 <主机名> 通信。互联网服务器可能正忙或永久停机，也可能由于网络问题而无法访问。 请检查输入的互联网地址拼写是否正确。如果地址正确，请稍后尝试此请求。

文件名和 通知标题	通知说明	通知文本
ERR_IDS_ACCESS_FORBIDDEN IDS 访问被禁止 (IDS Access Forbidden)	用户尝试上传由于配置的“思科数据安全策略”而受阻的文件时显示的阻止页面。	根据贵组织数据传输策略，已阻止上传请求。文件详情： <文件详情 >
ERR_INTERNAL_ERROR 内部错误 (Internal Error)	出现内部错误时显示的错误页面。	处理页面 <*URL*> 请求时出现内部系统错误。 请重试此请求。 如果此情况持续存在，请联系<联系人姓名> <邮件地址> 并提供如下所示的代码。
ERR_MALWARE_SPECIFIC 安全：检测到恶意软件 (Security: Malware Detected)	下载文件时检测到恶意软件后显示的阻止页面。	根据贵组织的访问策略，此网站 <*URL*> 已被阻止，因为已确定该网站对您的计算机或组织的网络构成安全威胁。 在此站点中发现类别<恶意软件类别> 中的恶意软件 <恶意软件名称>。
ERR_MALWARE_SPECIFIC_OUTGOING 安全：检测到恶意软件 (Security: Malware Detected)	上传文件时检测到恶意软件后显示的阻止页面。	根据贵组织的策略，上传到 URL (<*URL*>) 的文件已被阻止，因为检测到该文件所含的恶意文件会对接收端的网络安全带来危害。 恶意软件名称：<恶意软件名称> 恶意软件类别：<恶意软件类别>
ERR_NATIVE_FTP_DENIED	本地 FTP 事务受阻时显示在本地 FTP 客户端中的阻止消息。	530 登录遭拒
ERR_NO_MORE_FORWARDS 无更多转发 (No More Forwards)	设备检测到网络上 Web 代理和另一代理服务器之间的转发环路时显示的错误页面。Web 代理打破环路，并向客户端显示该消息。	对此页面 <*URL*> 的请求失败。 服务器地址 <主机名> 可能无效，或者您可能需要指定一个端口号才能访问此服务器。
ERR_POLICY 策略：通用 (Policy: General)	为任何策略设置阻止请求时显示的阻止页面。	根据贵组织访问策略，已阻止访问此网站 <*URL*>。
ERR_PROTOCOL 策略：协议 (Policy: Protocol)	根据所用协议阻止请求时显示的阻止页面。	根据贵组织的访问策略，已阻止该请求，因为不允许使用数据传输协议“<协议类型>”。

文件名和 通知标题	通知说明	通知文本
ERR_PROXY_AUTH_REQUIRED 需代理授权 (Proxy Authorization Required)	用户必须输入身份验证凭证以继续操作时显示的通知页面。这用于显式事务请求。	使用此系统访问互联网需要身份验证。当系统提示时，必须输入有效的用户 ID 和密码。
ERR_PROXY_PREVENT_MULTIPLE_LOGIN 已从另一台计算机登录 (Already Logged In From Another Machine)	当某人使用已经过不同的计算机上的 Web 代理进行身份验证的同一用户名尝试访问网络时显示的阻止页面。这在启用“用户会话限制”(User Session Restrictions) 全局身份验证选项后使用。	根据贵组织的策略，访问互联网的请求被拒绝，因为此用户 ID 已在另一个 IP 地址进行会话。 如果您想以另一用户身份登录，请点击以下按钮并输入不同的用户名和密码。
ERR_PROXY_REDIRECT 重定向 (Redirect)	重定向页面。	此请求正在重定向。如果此页面未自动重定向，请点击此处继续。
ERR_PROXY_UNACKNOWLEDGED 策略确认 (Policy Acknowledgment)	最终用户确认页面。 有关详细信息，请参阅最终用户通知页面，第 279 页。	在访问互联网之前，请确认以下声明。 系统将自动监控和处理 Web 事务，且同时检测危险内容和实施贵组织的策略。点击以下链接，您将确认此监控，并认可系统可能记录您访问的站点的数据。您将被定期要求确认监控系统的存在。您有义务遵守组织的互联网访问策略。 点击此处接受此声明并访问互联网。
ERR_PROXY_UNLICENSED 代理未获许可 (Proxy Not Licensed)	网络安全设备 Web 代理无有效许可密钥时显示的阻止页面。	如果安全设备未经正确许可，则无法访问互联网。 请联系<联系人姓名><邮件地址>并提供如下所示的代码。 **注释** 要访问安全设备的管理界面，请输入配置的 IP 地址与端口。
ERR_RANGE_NOT_SATISFIABLE 范围无效 (Range Not Satisfiable)	Web 服务器无法满足请求的字节范围时显示的错误页面。	系统无法处理此请求。非标准浏览器可能生成了无效的 HTTP 请求。 如果您正在使用标准浏览器，请重试请求。

文件名和 通知标题	通知说明	通知文本
ERR_REDIRECT_ PERMANENT 永久重定向 (Redirect Permanent)	内部重定向页面。	页面 <*URL*> 正被重定向至 <重定向 *URL*>。
ERR_REDIRECT_REPEAT_ REQUEST 重定向 (Redirect)	内部重定向页面。	请重复您的请求。
ERR_SAAS_AUTHEN TICATION 策略：访问被拒绝 (Policy: Access Denied)	用户必须输入身份验证凭证以继续操作时显示的通知页面。这用于访问应用。	根据贵组织的策略，<*URL*> 访问请求被重定向至您必须输入登录凭证的页面。一旦验证成功并获得适当权限，您即可访问此程序。
ERR_SAAS_AUTHORI ZATION 策略：访问被拒绝 (Policy: Access Denied)	用户尝试访问其无访问权限的应用时显示的阻止页面。	根据贵组织的策略，<*URL*> 应用访问被阻止，因为您不是授权用户。如果您想以另一用户登录，请输入另一个有权访问该应用的用户名和密码。
ERR_SAML_PROCESSING 策略：访问被拒绝 (Policy: Access Denied)	内部流程无法处理用于访问应用的单点登录 URL 时显示的错误页面。	由于根据请求处理单一登录的过程中出现错误，对 <用户名> 的访问请求未获通过。
ERR_SERVER_NAME_ EXPANSION 服务器名称扩展 (Server Name Expansion)	自动扩展 URL 并将用户重定向至更新的 URL 的内部重定向页面。	服务器名称 <主机名> 显示为缩写，正在重定向至 <重定向 *URL*>。
ERR_URI_TOO_LONG URI 过长 (URI Too Long)	URL 过长时显示的阻止页面。	请求的 URL 过长，无法处理。这可能表示您的网络受到攻击。 请联系 <联系人姓名><邮件地址> 并提供如下所示的代码。
ERR_WBRS 安全：恶意软件风险 (Security: Malware Risk)	Web 信誉过滤器由于低 Web 信誉分数阻止站点时显示的阻止页面。	根据贵组织的访问策略，此网站 <*URL*> 已被阻止，因为 Web 信誉过滤器已确定该网站对您的计算机或公司网络构成安全威胁。此网站已经与恶意软件/间谍软件相关联。 威胁类型：%o 威胁原因：%O

文件名和 通知标题	通知说明	通知文本
ERR_WEBCAT 策略：URL 过滤 (Policy: URL Filtering)	用户尝试访问受阻 URL 类别中的网站时显示的阻止页面。	根据贵组织的访问策略，已阻止访问此网站 <*URL*>，因为不允许使用 Web 类别“<类别类型>”。
ERR_WWW_AUTH_REQUIRED 需要 WWW 授权 (WWW Authorization Required)	请求服务器要求用户输入凭证以继续时显示的通知页面。	访问请求的网站 <主机名> 需要身份验证。当系统提示时，必须输入有效的用户 ID 和密码。

第 19 章

生成报告监控最终用户活动

本章包含以下部分：

报告概述

网络安全设备生成高级报告，让您既可以了解网络上的状况，还可以查看特定域、用户或类别的流量详细信息。您可以运行报告来查看特定时间段内系统活动的交互显示，也可以安排并定期运行报告。

相关主题

- 从报告页面打印和导出报告，第 304 页

使用报告中的用户名

当您启用身份验证时，报告通过 Web 代理进行身份验证时，会按用户名列出用户。默认情况下，用户名一出现即被写入验证服务器。但是，您可以选择使用用户名在所有报告中都不可识别。

注释 管理员始终可以看到报告中的用户名。

步骤 1 依次选择**安全服务 (Security Services) > 报告 (Reporting)**，然后点击**编辑设置 (Edit Settings)**。

步骤 2 在“本地报告”(Local Reporting) 下，选择**匿名化报告中的用户名 (Anonymize usernames in reports)**。

步骤 3 “提交”(Submit) 并“确认更改”(Commit Changes)。

报告页面

网络安全设备提供以下报告：

- 我的控制面板（报告“主页”；也可以通过点击菜单栏左边的主页图标来访问）
- 概述
- 用户
- 网站
- URL 类别
- 应用可视性
- 防恶意软件
- 高级恶意软件防护
- 文件分析
- AMP 判定更新
- 客户端恶意软件风险
- Web 信誉过滤器
- L4 流量监控器
- SOCKS 代理
- 按用户位置分类的报告
- 网络跟踪
- 系统容量
- 系统状态
- 计划的报告
- 存档的报告

使用“报告”(Reporting) 页面

多个报告页面提供系统活动概述，并支持多个用于查看系统数据的选项。也可以搜索各页面了解网站和客户端特定数据。

可以在大多数报告页面上执行下列任务：

选项	任务链接
更改报告中显示的时间范围	更改时间范围， 第 301 页
搜索特定客户端和域	搜索数据， 第 301 页
选择要显示在图表中的数据	选择要绘图的数据， 第 302 页

选项	任务链接
将报告导出至外部文件	从报告页面打印和导出报告，第 304 页

更改时间范围

您可以使用“时间范围”(Time Range) 字段，更新每个安全组件显示的数据。通过此选项，您可以生成预定义时间范围的更新，可以定义从某个特定开始时间到某个特定结束时间的自定义时间范围。

注释 所选择的时间范围用于所有报告页面，直到在“时间范围”(Time Ranges) 菜单中选择其他值。

时间范围	过多长时间才返回数据...
小时	完整的六十分钟，外加最多 5 分钟的额外时间。
天	过去 24 小时，以一小时为间隔，并包括当前小时部分。
星期	过去 7 天，以一天为间隔，加上当前天的部分。
月 (30 天)	过去 30 天，以一天为间隔，加上当前天的部分。
过去	过去 24 小时 (00:00 到 23:59)（使用在网络安全设备上定义的时区）。
自定义范围	您已定义的自定义时间范围。 选择“自定义范围”(Custom Range) 后，系统会显示一个对话框，可在此输入开始和结束时间。

注释 所有报告均基于系统配置的时区显示日期和时间信息，并且以格林威治标准时间 (GMT) 时差显示。但是，数据导出会仅显示 GMT 的时间，以适应全球多个时区的多个系统。

搜索数据

某些报告中包括一个可用于搜索特定数据点的字段。当您搜索数据时，报告会优化您正在搜索的特定数据集的报告数据。您可以搜索与所输入字符串完全匹配的值，也可以搜索以所输入字符串开头的值。以下报告页面包括搜索字段：

搜索字段	说明
用户	按用户名或客户端 IP 地址搜索用户。
网站	按域或服务器 IP 地址搜索服务器。

搜索字段	说明
URL 类别	搜索 URL 类别。
应用可视性	搜索 AVC 引擎监控和阻止的应用名称。
客户端恶意软件风险	按用户名或客户端 IP 地址搜索用户。

注释 需要配置身份验证以查看客户端用户 ID 和客户端 IP 地址。

选择要绘图的数据

每个网络报告页面上的默认图表会显示通常引用的数据，但是，您可以选择用其他数据绘制图表。如果页面有多个图表，则可以更改每个图表。图表选项与报告中表的列标题相同。

步骤 1 点击图表下的**图表选项 (Chart Options)** 链接。

步骤 2 选择要显示的数据。

步骤 3 点击**完成 (Done)**。

自定义报告

可以通过组合现有报告页中的图表（图形）和表格，来创建自定义报告页。

目标	请
将模块添加到自定义报告页面	请参阅： • 无法添加到自定义报告的模块，第 303 页. • 创建自定义报告页面，第 303 页
查看自定义报告页面	1. 依次选择**监控 (Monitor) > 邮件或网络 (Email or Web) > 报告 (Reporting) > 报告 (Reporting) > 我的报告 (My Reports)**。 2. 选择要查看的时间范围。所选时间范围会应用到所有报告，包括“我的报告”(My Reports) 页面中的所有模块。 新添加的模块显示在相关部分的的顶部。
在自定义报告页面上重新排列模块	将模块拖放到所需的位置。
从自定义报告页面中删除模块	点击模块右上角的 [X]。

目标	请
生成自定义报告的 PDF 或 CSV 版本	依次选择**报告 (Reporting) > 存档的报告 (Archived Reports)**，然后点击**立即生成报告 (Generate Report Now)**。
定期生成自定义报告的 PDF 或 CSV 版本	依次选择**报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

无法添加到自定义报告的模块

- 搜索结果，包括网络跟踪搜索结果

创建自定义报告页面

开始之前

- 确保要添加的模块可以添加。请参阅无法添加到自定义报告的模块，第 303 页。
- 通过点击模块右上角的 **[X]** 删除任何不需要的默认模块。

步骤 1 使用以下方法之一将模块添加到自定义报告页面：

注释 某些模块仅在使用这些方法中的一种时可用。如果无法使用一种方法添加模块，请尝试另一种方法。

- 导航至具有要添加的模块的 选项卡下的报告页面，然后点击模块顶部 [+] 按钮。
- 转到**报告 (Reporting) > 我的报告 (My Reports)**，点击其中一个部分顶部的 按钮，，然后选择需要添加的报告模块。您可能需要点击“我的报告”(My Reports) 页面中每个部分的 按钮，以找到您要查找的模块。

  每个模块只能添加一次；如果您已向报告中添加特定模块，则用于添加该模块的选项将不可用。

步骤 2 如果添加已自定义的模块（例如，通过添加、删除或重新排序列，或者通过在图表中显示非默认数据），则在“我的报告”(My Reports) 页面上自定义模块。

添加的模块使用默认设置。原始模块的时间范围无法保留。

步骤 3 如果添加包含单独图例的图表（例如，“概述”(Overview) 页面中的图形），请单独添加图例。如果需要，请将其拖放到其描述的数据的旁边。

报告和跟踪中的子域与二级域

在报告和跟踪搜索中，对二级域（在http://george.surbl.org/two-level-tlds中列出的地区域）的处理方式与子域不同，即使两种域类型可能看起来相同。例如：

- 报告不会包含两级域（例如 `co.uk`）的结果，但是会包含 `foo.co.uk` 的结果。报告包含主公司域下的子域，例如 `cisco.com`。

- 对应于地区域 co.uk 的跟踪搜索结果不会包含诸如 foo.co.uk 等域，而对应于 cisco.com 的搜索结果将包含子域，例如 subdomain.cisco.com。

从报告页面打印和导出报告

对于任何报告页面，您均可通过点击页面右上角的**可打印 (PDF)** 链接生成打印格式的 PDF 版本。也可以点击 **导出(Export)** 链接，将原始数据导出为逗号分隔值 (CSV) 文件。

由于 CSV 导出仅包括原始数据，因此从一个基于 Web 的报告页面导出的数据可能不包括计算的数据，例如百分比，即使这些数据显示在基于 Web 的报告中也是如此。

导出报告数据

大多数报告包括允许您将原始数据导出为逗号分隔值 (CSV) 文件的**导出 (Export)** 链接。将数据导出为 CSV 文件后，可使用 Microsoft Excel 等应用访问和操作其中的数据。

无论网络安全设备使用哪种时区，导出的 CSV 数据都以格林威治标准时间 (GMT) 显示所有消息跟踪和报告数据。GMT 时间转换是为了允许独立于设备使用数据，或从分布于多个时区的设备中引用数据的情况。

以下示例是从防恶意软件类别报告导出的原始数据中的一个条目，其中太平洋夏令时 (PDT) 显示为 GMT 07:00 小时：

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
 Transactions Monitored, Transactions Blocked, Transactions Detected
 1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100,
2625
```

类别标题	值	说明
开始时间戳	1159772400.0	以系统纪元以来的秒数表示的查询开始时间。
结束时间戳	1159858799.0	以系统纪元以来的秒数表示的查询结束时间。
开始日期	2006-10-02 07:00 GMT	查询开始的日期。
结束日期	2006-10-03 06:59 GMT	查询结束的日期。
名称	广告软件	恶意软件类别的名称。
受控事务数	525	监控的事务数。
受阻事务数	2100	阻止的事务数。
检测到的事务数	2625	总事务数 =（检测到的事务数）+（阻止的事务数）。

注释 - 每种类型的报告具有不同的类别标题。

- 如果导出本地化的 CSV 数据，某些浏览器可能无法正确显示标题。出现该情况是因为某些浏览器可能没有为本地化文本使用正确的字符集。要解决该问题，可以将文件保存到本地计算机，然后在任何 Web 浏览器中使用**文件 (File) > 打开 (Open)** 打开该文件。打开文件时，请选择字符集以显示本地化文本。

启用报告

如果贵组织有多个网络安全设备，并使用思科内容安全管理设备来管理和查看报告数据汇总，必须在每个网络安全设备上启用集中报告。

您可以根据设备设置选择报告类型。可以选择在本地保留所有报告，或者（如果设备已装载到思科防御协调器上）通过思科防御协调器来访问这些报告。如果贵组织有多个网络安全设备，并使用思科内容安全管理设备，您可以选择集中报告来管理和查看报告数据汇总。如果选择集中报告或通过思科防御协调器选择本地报告，必须在每个网络安全设备上应用这些选择。

步骤 1 依次选择**安全服务 (Security Services) > 报告 (Reporting)**，并点击**编辑设置 (Edit Settings)**。

a) 选择**本地报告 (Local Reporting)** 以在设备上启用报告。报告在登录到设备门户后便可访问。

b) 选择**本地报告 (Local Reporting)** 和**思科防御协调器 (Cisco Defense Orchestrator Reporting)**，以通过思科防御协调器启用报告。

c) 选择**集中报告 (Centralized Reporting)** 以通过思科内容安全管理设备启用报告。

网络安全设备仅会存储其收集的所有数据以用于本地报告。如果在设备上启用了集中报告，则网络安全设备仅会保留系统容量和系统状态数据，并且这些数据是在本地网络安全设备上唯一可用的报告。

请参阅《思科内容安全管理设备用户指南》中的“使用集中 Web 报告和跟踪"章节，以了解有关在管理设备上配置此功能的信息。

步骤 2 **提交 (Submit)** 并确认更改 (Commit Changes)。

安排报告

您可以安排报告每日、每周或每月运行。可以配置计划报告以包括前一天、前七天或上个月的数据。

可以计划报告类型如下的报告：

- 概述
- 用户
- 网站
- URL 类别
- 应用可视性

- 防恶意软件
- 高级恶意软件防护
- 高级恶意软件防护判定更新
- 客户端恶意软件风险
- Web 信誉过滤器
- L4 流量监控器
- SOCKS 代理
- 按用户位置分类的报告
- 系统容量
- 我的控制面板

添加计划报告

步骤 1 依次选择**报告 (Reporting) > 计划报告 (Scheduled Reports)**，然后点击**添加计划报告 (Add Scheduled Report)**。

步骤 2 选择报告**类型 (Type)**。

步骤 3 为报告输入描述性**标题 (Title)**。

避免创建具有相同名称的多个报告。

步骤 4 选择报告中所含的数据时间范围。

步骤 5 选择所生成报告的**格式 (Format)**。

默认格式为 PDF。大多数报告还允许将原始数据另存为 CSV 文件。

步骤 6 根据所配置的报告类型，可以指定不同的报告选项，例如要包括的行数以及按哪一列排序数据。根据需要配置这些选项。

步骤 7 在**计划 (Schedule)** 部分中，选择是否每天、每周或每月以及其他什么时间运行报告。

步骤 8 在 **电子邮件发送至 (Email to)** 字段，输入生成的报告要发送至的电子邮件地址。

如果不指定邮件地址，将只会存档该报告。

步骤 9 选择数据的**报告语言 (Report Language)**。

步骤 10 “提交”(Submit) 并“确认更改”(Commit Changes)。

编辑计划的报告

步骤 1 依次选择**报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2 从列表中选择报告标题。

步骤 3 修改设置。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

删除计划报告

步骤 1 依次选择**报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2 选中与要删除的报告对应的复选框。

步骤 3 要删除所有计划的报告，请选中**全部 (All)** 复选框。

步骤 4 **删除 (Delete)** 并**确认更改 (Commit Changes)**。

注释 已删除报告的存档版本不会被删除。

按需生成报告

步骤 1 依次选择**报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2 点击**立即生成报告 (Generate Report Now)**。

步骤 3 选择报告**类型 (Type)**。

步骤 4 为报告输入描述性**标题 (Title)**。

避免创建具有相同名称的多个报告。

步骤 5 选择报告中所含的数据时间范围。

步骤 6 选择所生成报告的**格式 (Format)**。

默认格式为 PDF。大多数报告还允许将原始数据另存为 CSV 文件。

步骤 7 根据所配置的报告类型，可以指定不同的报告选项，例如要包括的行数以及按哪一列排序数据。根据需要配置这些选项。

步骤 8 选择一个**交付选项**：

- **存档 (Archive)** 报告（报告出现在“存档的报告”(Archived Reports) 页）。
- **现在给收件人发送邮件 (Email now to recipients)**；提供一个或多个电子邮件地址。

步骤 9 选择数据的**报告语言 (Report Language)**。

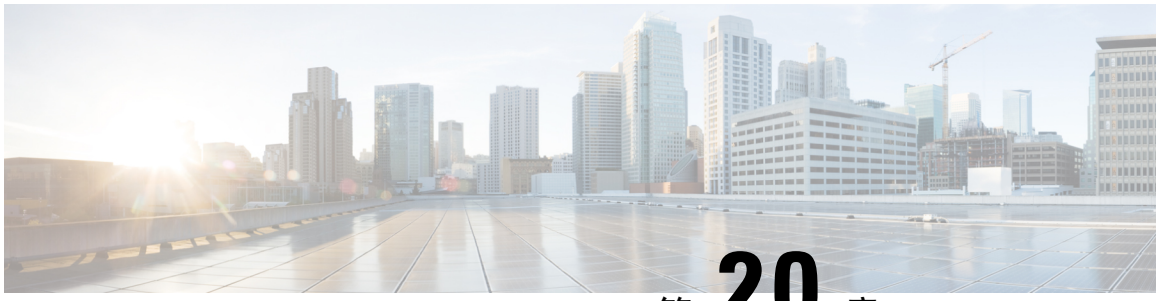
步骤 10 点击**发送此报告 (Deliver This Report)** 生成报告。

步骤 11 确认更改。

存档的报告

报告 (Reporting) > 存档的报告 (Archived Reports) 页面列出可用的存档报告。“报告标题”(Report Title) 列中的各个名称提供了用于查看此报告的链接。**显示 (Show)** 菜单可过滤将列出的报告类型。可以点击列标题对各列中的数据进行排序。

设备可为每个计划报告（共计达 1000 个报告）最多存储 12 个实例。已存档的报告存储在设备上的 `/periodic_reports` 目录。存档的报告会自动删除。在添加新报告时，会删除较旧的报告以使数量保持在 1000。最多可将 12 个实例应用到具有相同名称和时间范围的计划报告。



第 20 章

网络安全设备报告

本章包含以下部分：

“概述”(Overview) 页面

报告 (Reporting) > 概述 (Overview) 页面提供网络安全设备上的活动摘要。它包括网络安全设备处理的 Web 流量的图形和摘要表。

表 2: 系统概况

部分	说明
Web 代理流量特征 (Web Proxy Traffic Characteristics)	列出在过去一分钟内平均每秒事务数、在过去一分钟内的平均带宽 (bps)、在过去一分钟内的平均响应时间 (ms) 和当前连接总数。

部分	说明
系统资源利用率 (System Resource Utilization)	列出当前总 CPU 负载、RAM 和报告/日志记录磁盘使用率。点击 **系统状态详细信息 (System Status Details)** 切换到“系统状态”(System Status) 页面（请参阅“系统状态”(System Status) 页面，第 322 页了解更多详细信息)。 **注释** 此页面上显示的 CPU 使用率值和“系统状态”(System Status) 页面上显示的 CPU 值可能会略有不同，原因是它们是在不同时间分别读取的。

表 *3:* 基于时间范围的类别和摘要

部分	说明
时间范围：选择在以下各部分显示的数据的时间范围。选项包括“小时”(Hour)、“天”(Day)、“周”(Week)、“30 天”(30 Days)、“昨天”(Yesterday) 或“自定义范围”(Custom Range)。	
Web 代理活动总数 (Total Web Proxy Activity)	显示实际事务数（纵坐标）以及发生（Web 代理）活动的大约日期（水平时间轴）。
Web 代理摘要 (Web Proxy Summary)	可用于查看可疑 Web 代理活动或干净 Web 代理活动的百分比。
L4 流量监控器摘要 (L4 Traffic Monitor Summary)	有关 L4 流量监控器监控和阻止流量的报告。
可疑事务数 (Suspect Transactions)	可用于查看各个安全组件标记为可疑的 Web 事务。 显示实际事务数以及发生活动的大约日期。
可疑事务摘要 (Suspect Transactions Summary)	可用于查看阻止或警告的可疑事务的百分比。
排名靠前的 URL 类别：按事务总数排列 (Top URL Categories: Total Transactions)	显示被阻止的前 10 个 URL 类别。
排名靠前的应用类型：按事务总数排列 (Top Application Types: Total Transactions)	显示 AVC 引擎阻止的前几个应用类型。
排名靠前的恶意软件类别：受监控或受阻止 (Top Malware Categories: Monitored or Blocked)	显示检测到的所有恶意软件类别。
排名靠前的用户：按受阻或警告的事务数排列 (Top Users: Blocked or Warned Transactions)	显示生成阻止或警告的事务的用户。以用户名显示通过验证的用户，以 IP 地址显示未通过身份验证的用户。

“用户”(User) 页面

报告 (Reporting) > 用户 (Users) 页面提供能够查看各用户网络流量信息的若干链接。您可查看网络中用户花在互联网或者特定网站或 URL 上的时间有多少，以及用户使用了多少带宽。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
按受阻事务数排名靠前的用户 (Top Users by Transactions Blocked)	列出受阻事务数最多（水平时间轴）的排名靠前的用户（纵坐标）。
按使用的带宽排名靠前的用户 (Top Users by Bandwidth Used)	显示在系统上使用最多带宽（以使用的 GB 数表示横坐标）的排名靠前的用户（纵坐标）。
用户表 (Users Table)	列出各个用户并显示每个用户的多项统计信息。

“用户详细信息”(User Details) 页面

用户详细信息 (User Details) 页面显示有关在**报告 (Reporting) > 用户 (Users)** 页面的“用户表”(Users Table) 中选择的特定用户的信息。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
按事务总数的URL类别 (URL Categories by Total Transactions)	列出特定用户使用的特定 URL 类别。
按事务总数的趋势 (Trend by Total Transaction)	显示用户访问 Web 的时间。
匹配的 URL 类别 (URL Categories Matched)	显示在指定时间范围内与已完成和已阻止的事务均匹配的所有URL类别。
匹配的域 (Domains Matched)	显示有关此用户访问的特定域或 IP 地址的信息。 **注释** 如果将该域数据导出至 CSV 文件，请注意，仅会将最初的 300,000 条导出至文件。
匹配的应用 (Applications Matched)	显示 AVC 引擎检测到的特定用户正在使用的特定应用。

部分	说明
检测到的恶意软件威胁 (Malware Threats Detected)	显示特定用户触发的排名靠前的恶意软件威胁。
匹配的策略 (Policies Matched)	显示正在对此特定用户执行的特定策略。

“网站”(Web Sites) 页面

报告 (Reporting) > 网站 (Web Sites) 页面是对网络安全设备上所发生活动的整体汇总。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
按事务总数排名靠前的域 (Top Domains by Total Transactions)	以图形格式列出在站点上访问的排名靠前的域。
按受阻事务数排名靠前的域 (Top Domains by Transactions Blocked)	以图形格式列出根据事务触发阻止操作的排名靠前的域。
匹配的域 (Domains Matched)	以交互式表格的形式列出在站点上访问的域。 **注释** 如果将该域数据导出至 CSV 文件，请注意，仅会将最初的 300,000 条导出至文件。

“URL 类别”(URL Categories) 页面

报告 (Reporting) > URL 类别 (URL Categories) 页面可用于查看网络上的用户正在访问的 URL 类别。“URL 类别”(URL Categories) 页面可与应用可视性 (Application Visibility) 页面和用户 (Users) 页面结合使用以调查特定用户，以及特定用户尝试访问的应用或网站类型。

注释 预定义的 URL 类别集合不定期更新。

部分	说明
时间范围 (Time Range)（下拉列表）	选择报告的时间范围。

部分	说明
按事务总数排名靠前的 URL 类别 (Top URL Categories by Total Transactions)	以图形格式列出在站点上访问的排名靠前的 URL 类别。
按阻止和警告的事务数排名靠前的 URL 类别 (Top URL Categories by Blocked and Warned Transactions)	以图形格式列出按事务触发阻止或警告操作的排名靠前的 URL。
匹配的 URL 类别 (URL Categories Matched)	按URL类别显示指定时间范围内的事务处理结果，以及每个类别中使用的带宽量以及花费的时间。 如果未分类的 URL 的百分比高于 15-20%，请考虑以下选项： • 对于特定的本地化 URL，您可以创建自定义 URL 类别，并将其应用到特定用户或组策略。 • 您可以向思科报告未分类和分类有误的 URL，用于评估和数据库更新。 • 验证 Web 信誉过滤和防恶意软件过滤是否已启用。

URL 类别集更新和报告

预定义的 URL 类别集可能会自动在网络安全设备上定期更新。

当发生这些更新时，旧类别名称将继续显示在报告中，直到与较旧类别关联的数据因太旧而无法包括在报告中。在URL类别集更新后生成的报告数据将使用新的类别，因此，可能会在同一报告中显示新类别和旧类别。

“应用可视性”(Application Visibility) 页面

报告 (Reporting) > 应用可视性 (Application Visibility) 页面显示应用可视性与可控性引擎检测到的被使用和阻止的应用和应用类型。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)	此部分以图形格式列出在站点上访问的排名靠前的应用类别。
按受阻事务数排名靠前的应用 (Top Applications by Blocked Transactions)	以图形格式列出根据事务触发阻止操作的排名靠前的应用类型。

部分	说明
匹配的应用类型 (Application Types Matched)	可用于查看有关“按事务总数排名靠前的应用类型”(Top Application Types by Total Transactions) 图表中列出的应用类型的精细详细信息。
匹配的应用 (Applications Matched)	显示指定时间范围内的所有应用。

“防恶意软件”(Anti-Malware) 页面

可通过“报告”(Reporting) > “防恶意软件”(Anti-Malware) 页面监控和识别思科 DVS 引擎所检测的恶意软件。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
检测到的排名靠前的恶意软件类别 (Top Malware Categories Detected)	显示 DVS 引擎检测到的排名靠前的恶意软件类别。
检测到的排名靠前的恶意软件威胁 (Top Malware Threats Detected)	显示 DVS 引擎检测到的排名靠前的恶意软件威胁。
恶意软件类别数 (Malware Categories)	显示有关在“检测到的排名靠前的恶意软件类别”(Top Malware Categories Detected) 部分中显示的特定恶意软件类别的信息。
恶意软件威胁 (Malware Threats)	显示有关在“排名靠前的恶意软件威胁”(Top Malware Threats) 部分中显示的特定恶意软件威胁的信息。

“恶意软件类别”(Malware Category) 报告页面

步骤 1 依次选择报告 (Reporting) > 防恶意软件 (Anti-Malware)。

步骤 2 在“恶意软件类别”(Malware Categories) 交互式表格中，点击“恶意软件类别”(Malware Category) 列中的一个类别。

“恶意软件威胁”(Malware Threat) 报告页面

步骤 1 依次选择报告 (Reporting) > 防恶意软件 (Anti-Malware)。

步骤 2 在“恶意软件威胁”(Malware Threat) 表格中，点击“恶意软件类别”(Malware Category) 列中的一个类别。

“高级恶意软件保护”(Advanced Malware Protection) 页面

请参阅文件信誉过滤和文件分析：，第 233 页。

“文件分析”(File Analysis) 页面

请参阅文件信誉和文件分析报告与跟踪，第 246 页。

“AMP 判定更新”(AMP Verdict Updates) 页面

请参阅文件信誉过滤和文件分析：，第 233 页。

“客户端恶意软件风险”(Client Malware Risk) 页面

报告 (Reporting) > 客户端恶意软件风险 (Client Malware Risk) 页面是可用于监控客户端恶意软件风险活动的安全相关报告页面。“客户端恶意软件风险”(Client Malware Risk) 页面还会列出常见恶意软件连接中涉及的客户端 IP 地址，如 L4 流量监控器 (L4TM) 确定的 IP 地址。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
Web 代理：按恶意软件风险排名靠前的客户端 (Web Proxy: Top Clients by Malware Risk)	此图表显示遇到恶意软件风险的前十个用户。
L4 流量监控器：检测到的恶意软件连接 (L4 Traffic Monitor: Malware Connections Detected)	此图表显示贵组织中最频繁地连接到恶意软件站点的计算机的 IP 地址。
Web 代理：按恶意软件风险排名的客户端 (Web Proxy: Clients by Malware Risk)	“Web 代理：按恶意软件风险排名的客户端”(Web Proxy: Clients by Malware Risk) 表格显示有关“Web 代理：按恶意软件风险排名靠前的客户端”(Web Proxy: Top Clients by Malware Risk) 部分中显示的特定客户端的详细信息。
L4 流量监控器：按恶意软件风险排名的客户端 (L4 Traffic Monitor: Clients by Malware Risk)	此表显示您的组织中最常连接到恶意站点的计算机的 IP 地址。

“Web 代理 - 按恶意软件风险排名的客户端”(Web Proxy - Clients by Malware Risk) 的“客户端详细信息”(Client Detail) 页面

客户端详细信息 (Client Details) 页面显示指定时间范围内特定客户端的所有 Web 活动和恶意软件风险数据。

步骤 1 依次选择**报告 (Reporting) > 客户端恶意软件风险 (Client Malware Risk)**。

步骤 2 在 **Web 代理 - 客户端恶意软件风险 (Web Proxy - Client Malware Risk)** 部分中，点击“用户 ID/客户端 IP 地址”(User ID / Client IP Address) 列中的用户名。

下一步做什么

“用户详细信息”(User Details) 页面，第 311 页

“Web 信誉过滤器”(Web Reputation Filters) 页面

报告 (Reporting) > Web 信誉过滤器 (Web Reputation Filters) 页面是可用于查看指定时间范围内设置的事务 Web 信誉过滤器 (Web Reputation Filters) 结果的安全相关报告页面。

部分	说明
时间范围 (Time Range)（下拉列表）	可以选择本报告中所含数据时间范围的菜单。
Web 信誉操作（趋势）(Web Reputation Actions [Trend])	根据指定的时间（水平时间线）显示 Web 信誉操作（垂直时间线）总数。
Web 信誉操作（数量）(Web Reputation Actions [Volume])	按事务以百分比的形式显示 Web 信誉操作数量。
按受阻事务数排名的 Web 信誉威胁类型 (Web Reputation Threat Types by Blocked Transactions)	显示因低信誉分数而受阻的威胁类型。
按进一步扫描的事务数排名的 Web 信誉威胁类型 (Web Reputation Threat Types by Scanned Further Transactions)	显示导致指示扫描事务的信誉分数的威胁类型。
Web 信誉操作（按分数细分）(Web Reputation Actions [Breakdown by Score])	显示为每个操作细分的 Web 信誉分数。

“L4 流量监控器”(L4 Traffic Monitor) 页面

报告 (Reporting) > L4 流量监控器 (L4 Traffic Monitor) 页面是与安全相关的报告页面，显示有关 L4 流量监控器在指定的时间范围内检测到的恶意软件端口和恶意软件站点的信息。它还会显示经常遇到恶意软件站点的客户端的 IP 地址。

L4 流量监控器会监听通过设备上的所有端口传入的网络流量，并且将域名称和 IP 地址与其自有数据库表中的条目进行匹配，以确定是否允许传入和传出流量。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择要报告的时间范围的菜单。
排名靠前的客户端 IP (Top Client IPs)	以图形格式显示贵组织中最频繁连接到恶意软件站点的计算机的 IP 地址。
恶意软件最多的网站 (Top Malware Sites)	以图形格式显示 L4 流量监控器检测到的排名靠前的恶意软件域。
客户端源 IP (Client Source IPs)	显示贵组织中经常连接到恶意软件站点的计算机的 IP 地址。
恶意软件端口 (Malware Ports)	显示 L4 流量监控器在其上最常检测到恶意软件的端口。
检测到的恶意软件站点数 (Malware Sites Detected)	显示 L4 流量监控器在其上最常检测到恶意软件的域。

“SOCKS 代理”(SOCKS Proxy) 页面

通过**报告 (Reporting) > SOCKS 代理 (SOCKS Proxy)** 页面可以查看通过 SOCKS 代理处理的事务数据和趋势，其中包括排名靠前的目标和用户的相关信息。

“按用户位置分类的报告”(Reports by User Location) 页面

通过**报告 (Reporting) > 按用户位置分类的报告 (Reports by User Location)** 页面能够找出本地和远程用户所进行的活动。

具体活动包括：

- 本地和远程用户正在访问的 URL 类别。
- 本地和远程用户访问的站点所触发的防恶意软件活动。
- 本地和远程用户正访问的站点的网络信誉。
- 本地和远程用户正访问的应用。
- 用户（本地和远程）。
- 本地和远程用户访问的域。

部分	说明
时间范围 (Time Range)（下拉列表）	可用于选择报告中所含数据的时间范围的菜单。
Web 代理活动总数：远程用户 (Total Web Proxy Activity: Remote Users)	显示远程用户在指定时间（水平坐标）内的活动（纵坐标）。
Web 代理摘要 (Web Proxy Summary)	显示网络上的本地用户和远程用户活动摘要。
Web 代理活动总数：本地用户 (Total Web Proxy Activity: Local Users)	显示远程用户在指定时间（水平坐标）内的活动（纵坐标）。
检测到的可疑事务数：远程用户 (Suspect Transactions Detected: Remote Users)	显示由于为远程用户定义的访问策略，已在指定时间内（水平坐标）检测到的可疑事务数（纵坐标）。
可疑事务摘要 (Suspect Transactions Summary)	显示网络上远程用户的可疑事务摘要。
检测到的可疑事务数：本地用户 (Suspect Transactions Detected: Local Users)	显示由于为远程用户定义的访问策略，已在指定时间内（水平坐标）检测到的可疑事务数（纵坐标）。
可疑事务摘要 (Suspect Transactions Summary)	显示网络上本地用户的可疑事务摘要。

“Web 跟踪”(Web Tracking) 页面

使用“Web跟踪”(Web Tracking)页面搜索和获取有关各事务或可能需关注的事务模式的详细信息。按需以下列选项卡之一进行搜索：

“Web 跟踪”(Web Tracking) 页面	任务链接
Web 代理处理的事务	搜索 Web 代理处理的事务， 第 318 页
L4 流量监控器处理的事务	搜索 L4 流量监控器处理的事务， 第 321 页
SOCKS 代理处理的事务	搜索 SOCKS 代理处理的事务， 第 321 页

搜索 Web 代理处理的事务

您可以使用**报告 (Reporting) > Web 跟踪 (Web Tracking)** 页面的**代理服务 (Proxy Services)** 选项卡跟踪和报告特定用户或所有用户的 Web 使用情况。

您可以查看搜索结果以了解在特定时段记录的事务类型（已阻止、监控、警告和完成的事务），还可以使用多个条件过滤数据结果，例如 URL 类别、恶意软件威胁和应用。

注释 Web 代理仅报告包括 ACL 决策标记（而非“OTHER-NONE”）的事务。

步骤 1 依次选择**报告 (Reporting) > Web 跟踪 (Web Tracking)**。

步骤 2 点击**代理服务 (Proxy Services)** 选项卡。

步骤 3 配置设置。

设置	说明
时间范围（Time Range）	选择要报告的时间范围。
用户/客户端 IP (User/Client IP)	（可选）输入报告中显示的身份验证用户名，或者输入要跟踪的客户端 IP 地址。也可以输入 CIDR 格式的 IP 范围。 如果将此字段留空，则搜索将返回所有用户的结果。
网站 (Website)	（可选）输入要跟踪的网站。如果将此字段留空，则搜索将返回所有网站的结果。
交易类型	选择要跟踪的事务类型，可以是“所有事务”(All Transactions)、“已完成”(Completed)、“已阻止”(Blocked)、“已监控”(Monitored) 或“已警告”(Warned)。

步骤 4 （可选）展开“高级”(Advanced) 部分，配置字段，以通过更高级的条件过滤 Web 跟踪的结果。

设置	说明
URL 类别 (URL Category)	要按 URL 类别进行过滤，请选择**按 URL 类别过滤 (Filter by URL Category)** 并键入要依据其进行过滤的 URL 类别的首个字母。从显示的列表中选择类别。
应用 (Application)	要按应用过滤，选择**按应用过滤 (Filter by Application)** 并选择按其过滤的应用。 要按应用类型过滤，选择**按应用类型过滤 (Filter by Application Type)** 并选择按其过滤的应用类型。
策略 (Policy)	要按负责该事务最终决定的策略名称进行过滤，选择**按操作策略过滤 (Filter by Action Policy)** 并输入要依据其进行过滤的策略组名称（访问策略、解密策略或数据安全策略）。有关详细信息，请参阅访问日志文件中的 Web 代理信息，第 345 页部分的 PolicyGroupName 说明。
高级恶意软件防护 (Advanced Malware Protection)	请参阅关于网络跟踪和高级恶意软件保护功能，第 248 页。

设置	说明
恶意软件威胁 (Malware Threat)	要按特定恶意软件威胁过滤，选择**按恶意软件威胁过滤 (Filter by Malware Threat)** 并输入按其过滤的恶意软件威胁名称。 要按恶意软件类别进行过滤，请选择**按恶意软件类别过滤 (Filter by Malware Category)** 并选择要依据其进行过滤的恶意软件类别。
WBRS	在 WBRS 部分中，可以按 Web 信誉分数和特定 Web 信誉威胁进行过滤。 • 要按 Web 信誉分数进行过滤，请选择**分数范围 (Score Range)**，然后选择要依据其进行过滤的上限值和下限值。或者，您可以选择**无得分 (No Score)** 来过滤出那些没有得分的网站。 • 要按 Web 信誉威胁进行过滤，请选择**按信誉威胁过滤 (Filter by Reputation Threat)** 并选择要依据其进行过滤的 Web 信誉威胁。
AnyConnect 安全移动 (AnyConnect Secure Mobility)	要按用户位置（远程或本地）进行过滤，请选择**按用户位置过滤 (Filter by User Location)** 并选择要依据其进行过滤的用户类型。
用户请求 (User Request)	要按照用户启动的事务进行过滤，请选择**按用户请求的事务过滤 (Filter by User-Requested Transactions)**。 **注释** 启用此过滤器后，搜索结果将包括一些“最佳猜测”事务。

步骤 5 点击**搜索 (Search)**。

结果按时间戳排序，最新的结果会显示在顶部。

“显示详细信息”(Display Details) 列下方的括号中的数字是用户发起的事务所衍生的相关事务数，例如加载的映像数、运行的 JavaScript 数和访问的辅助站点数。

步骤 6 （可选）点击“事务”(Transactions) 列中的**显示详细信息 (Display Details)** 查看各事务的详细信息。

注释 如果需要查看超过 1000 个结果，请点击**可打印的下载 (Printable Download)** 链接获取 CSV 文件，该文件包括完整的原始数据集，不包括相关事务的详细信息。

提示 如果结果中的 URL 被截断，您可以在访问日志中找到完整 URL。

要查看超过 500 个相关事务的详细信息，请点击**相关事务 (Related Transactions)** 链接。

下一步做什么

- URL 类别集更新和报告，第 313 页
- 恶意软件类别说明，第 231 页
- 关于网络跟踪和高级恶意软件保护功能，第 248 页

搜索 L4 流量监控器处理的事务

报告 (Reporting) > Web 跟踪 (Web Tracking) 页面上的“L4 流量监控器”(L4 Traffic Monitor) 选项卡提供有关与恶意软件站点和端口连接的详细信息。您可以通过以下信息类型搜索至恶意软件站点的连接：

- 时间范围
- 站点，使用 IP 地址或域
- 端口
- 与组织中的计算机相关联的 IP 地址
- 连接类型

将会显示前 1000 个匹配的搜索结果。

搜索 SOCKS 代理处理的事务

您可以搜索符合各种条件的事务（包括已阻止或完成的事务）；用户；以及目标域、IP地址或端口。

步骤 1 依次选择**网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking)**。

步骤 2 点击 **SOCKS 代理 (SOCKS Proxy)** 选项卡。

步骤 3 要过滤结果，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件。

步骤 5 点击**搜索 (Search)**。

下一步做什么

“SOCKS 代理”(SOCKS Proxy) 页面 ， 第 317 页

“系统容量”(System Capacity) 页面

报告 (Reporting) > 系统容量 (System Capacity) 页面显示有关网络安全设备上资源使用情况的当前和历史信息。

在“系统容量”(System Capacity) 页面上选择查看数据的时间范围时，务必记住以下内容：

- **每小时报告 (Hour Report)**。每小时报告会查询每分钟表格，并显示设备在过去 60 分钟内每分钟记录的确切项目数，例如字节和连接。
- **每日报告 (Day Report)**。每日报告会查询每小时表格，并显示设备在过去 24 小时内每小时记录的确切项目数，例如字节和连接。此信息是从小时表收集。

每周报告和每 30 天报告与每小时报告和每日报告的工作方式类似。

“系统状态”(System Status) 页面

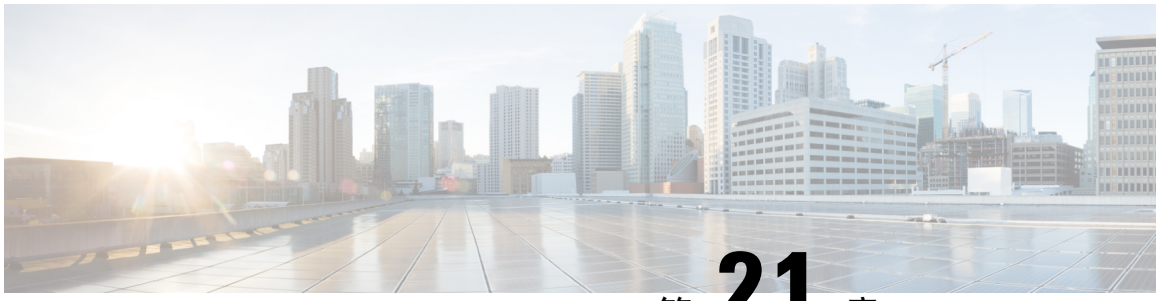
使用**报告 (Reporting) > 系统状态 (System Status)** 页面监控系统状态。该页面显示网络安全设备的当前状态和配置。

此部分...	显示
网络安全设备状态	• 系统运行时间 • 系统资源利用率 - CPU 使用情况、RAM 使用情况以及报告和日志记录所占用的磁盘空间百分比。 此页面上显示的 CPU 使用率值和系统“概述”(Overview) 页面 (“概述”(Overview) 页面，第 309 页) 上显示的 CPU 值可能略有不同，因为它们是在不同时间分别读取的。 对于高效工作的系统，RAM 使用率可能在 90% 以上，因为系统未使用的 RAM 被 Web 对象缓存使用。如果系统没有遇到严重的性能问题，并且此值没有卡在 100%，则系统运行正常。 **注释** 代理缓冲内存是使用此 RAM 的一个组件。
代理流量特征	• 每秒事务数 • 带宽 • 响应时间 • 缓存命中率 • 连接
高可用性	高可用性服务的状态。
外部服务	• 身份服务引擎

此部分...	显示
当前配置	Web 代理设置： • Web 代理状态 - 启用或禁用。 • 部署拓扑。 • Web 代理模式 - 转发或透明。 • IP 欺骗 - 启用或禁用。 L4 流量监控器设置： • L4 流量监控器状态 - 启用或禁用。 • L4 流量监控器接线。 • L4 流量监控器操作 - 监控或阻止。 网络安全设备版本信息 硬件信息

相关主题

“系统容量”(System Capacity) 页面，第 321 页



第 21 章

检测非标准端口上的恶意流量

本章包含以下部分：

检测恶意流量概述

网络安全设备具有集成式 L4 流量监控器，可检测所有网络端口的非法流量并阻止试图绕过端口 80 的恶意软件。当内部客户端感染恶意软件并尝试通过非标准端口和协议回拨时，L4 流量监控器会阻止回拨活动超出公司网络。默认情况下，L4 流量监控器处于启用状态并设置为监控所有端口上的流量。这包括 DNS 及其他服务。

L4 流量监控器使用并维护自己的内部数据库。此数据库使用 IP 地址和域名的匹配结果不断更新。

配置 L4 流量监控器

步骤 1 在防火墙内部配置 L4 流量监控器。

步骤 2 确保 L4 流量监控器在代理端口后并在对客户端 IP 地址执行网络地址转换 (NAT) 的任何设备前以“逻辑”方式进行连接。

步骤 3 配置全局设置

请参阅配置 L4 流量监控器全局设置， 第 326 页。

步骤 4 创建 L4 流量监控器策略

请参阅创建策略以检测恶意流量，第 327 页。

已知站点列表

地址	说明
已知允许	在“允许列表”(Allow List) 属性中列出的任何 IP 地址或主机名。这些地址作为“白名单”地址显示在日志文件中。
未列出	既不是已知的恶意软件站点也不是已知的允许地址的任何 IP 地址。它们未列示在“允许列表”(Allow List)、“其他可疑恶意软件地址”(Additional Suspected Malware Addresses) 属性或 L4 流量监控器数据库中。这些地址不会显示在日志文件中。
不明确	这些地址作为“灰名单”地址显示在日志文件中，包括： • 任何同时与未列出的主机名以及已知恶意软件主机名关联的 *IP* 地址。 • 同时与未列出的主机名以及“其他可疑恶意软件地址”(Additional Suspected Malware Addresses) 属性中的主机名关联的任何 *IP* 地址。
已知恶意软件	这些地址作为“黑名单”地址显示在日志文件中，包括： • 由 L4 流量监控器数据库确定为已知恶意软件站点且在“允许列表”(Allow List) 中未列出的任何 IP 地址或主机名。 • 任何在“其他可疑恶意软件地址”(Additional Suspected Malware Addresses) 属性中列出、未在“允许列表”(Allow List) 中列出且不属于不明确地址的 *IP* 地址。

配置 L4 流量监控器全局设置

步骤 1 依次选择**安全服务 (Security Services) > L4 流量监控器 (L4 Traffic Monitor)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 选择是否启用 L4 流量监控器。

步骤 4 如果启用 L4 流量监控器，请选择应监控的端口：

- **所有端口 (All ports)**。监控所有 65535 TCP 端口的非法活动。
- **除代理端口之外的所有端口 (All ports except proxy ports)**。监控除以下端口外所有 TCP 端口的非法活动。
  - 在“安全服务”(Security Services) >“Web 代理”(Web Proxy) 页面的“代理的 HTTP 端口”(HTTP Ports to Proxy) 属性中配置的端口（通常为端口 80）。
  - 在“安全服务”(Security Services) >“HTTPS 代理”(HTTPS Proxy) 页面的“代理的透明 HTTP 端口”(Transparent HTTPS Ports to Proxy) 属性中配置的端口（通常为端口 443）。

步骤 5 “提交”(Submit) 并“确认更改”(Commit Changes)。

更新 L4 流量监控器防恶意软件规则

步骤 1 依次选择**安全服务 (Security Services) > L4 流量监控器 (L4 Traffic Monitor)**。

步骤 2 点击**立即更新 (Update Now)**。

创建策略以检测恶意流量

L4 流量监控器采取的操作取决于您配置的 L4 流量监控器策略：

步骤 1 依次选择**网络安全管理器 (Web Security Manager) > L4 流量监控器 (L4 Traffic Monitor)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在**编辑 L4 流量监控器策略 (Edit L4 Traffic Monitor Policies)** 页面上，配置 L4 流量监控器策略：

a) **定义允许列表 (Allow List)**

b) 将已知良好的站点添加到**允许列表 (Allow List)**

注释 请勿在允许列表 (Allow List) 中包括网络安全设备 IP 地址或主机名，否则 L4 流量监控器不会阻止任何流量。

c) 确定要对**可疑恶意软件地址 (Suspected Malware Addresses)** 执行的操作：

操作	说明
允许	始终允许往来于已知允许地址和未列出地址的流量。
监控	在以下情况下监控流量： • 当“用于可疑恶意软件地址的操作”(Action for Suspected Malware Addresses) 选项设置为“监控”(Monitor) 时，始终监控并非往来于已知允许地址的所有流量。 • 当“用于可疑恶意软件地址的操作”(Action for Suspected Malware Addresses) 选项设置为“阻止”(Block) 时，监控往来于不明确的地址的流量。
阻止	当“用于可疑恶意软件地址的操作”(Action for Suspected Malware Addresses) 选项设置为“阻止”(Block) 时，阻止往来于已知恶意软件地址的流量。

注释 - 如果选择阻止可疑恶意软件流量，还可以选择是否始终阻止不明确的地址。默认情况下，监控不明确的地址。

- 如果 L4 流量监控器已配置为阻止，则必须在同一网络上配置 L4 流量监控器和 Web 代理。使用**网络 (Network) > 路由 (Routes)** 页面可确认在为数据流量配置的路由上可访问所有客户端。

d) 定义**其他可疑恶意软件地址 (Additional Suspected Malware Addresses)** 属性

注释 将内部 IP 地址添加到“其他可疑恶意软件地址”(Additional Suspected Malware Addresses) 列表会导致合法目标 URL 在 L4 流量监控器报告中显示为恶意软件。要避免这种情况，请不要在**网络安全管理器 (Web Security Manager) > L4 流量监控器策略 (L4 Traffic Monitor Policies)** 页面上的**其他可疑恶意软件地址 (Additional Suspected Malware Addresses)** 字段中输入内部 IP 地址。

步骤 4 “提交”(Submit) 并“确认更改”(Commit Changes)。

下一步做什么

相关主题

- 检测恶意流量概述， 第 325 页
- 有效格式， 第 328 页.

有效格式

向“允许列表”(Allow List) 或“其他可疑恶意软件地址”(Additional Suspected Malware Addresses) 属性添加地址时，用空格或逗号分隔多个条目。您可以输入以下任何格式的地址：

- **IPv4 IP 地址**。示例：IPv4 格式：10.1.1.0。IPv6 格式：2002:4559:1FE2::4559:1FE2
- **CIDR 地址**。示例：10.1.1.0/24。
- **域名**。示例：example.com。
- **主机名**。示例：crm.example.com。

查看 L4 流量监控器活动

S 系列设备支持多个用于生成功能特定报告和交互显示摘要统计信息的选项。

监控活动和查看摘要统计信息

报告 (Reporting) > L4 流量监控器 (L4 Traffic Monitor) 页面提供监控活动的统计摘要。您可以使用以下显示和查看工具查看 L4 流量监控器活动的结果：

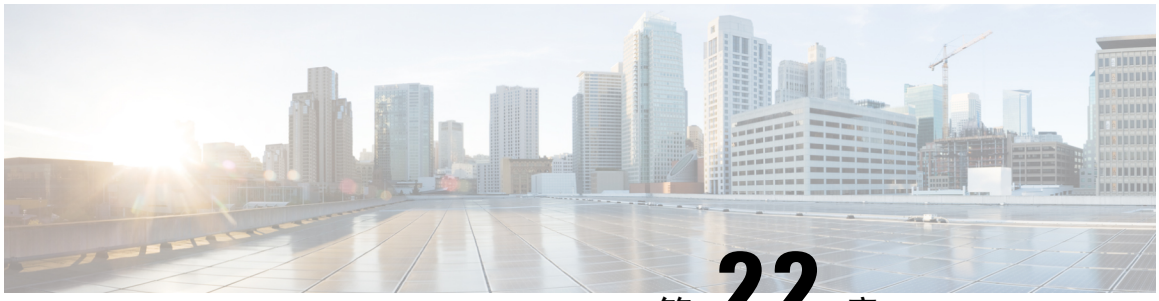
要查看.....	请参阅……
客户端统计信息	报告 (Reporting) > 客户端活动 (Client Activity)
恶意软件统计信息 端口统计信息	报告 (Reporting) > L4 流量监控器 (L4 Traffic Monitor)

要查看.....	请参阅……
L4 流量监控器日志文件	系统管理 (System Administration) > 日志订用 (Log Subscriptions) • trafmon_errlogs • trafmonlogs

注释 如果 Web 代理配置为转发代理，并且 L4 流量监控器设置为监控所有端口，则代理数据端口的 IP 地址会在**报告 (Reporting) > 客户端活动 (Client Activity)** 页面的客户活动报告中记录并显示为客户端 IP 地址。如果 Web 代理配置为透明代理，请启用 IP 欺骗以正确记录和显示客户端 IP 地址。

L4 流量监控器日志文件条目

L4 流量监控器日志文件提供监控活动的详细记录。



第 22 章

通过日志监控系统活动

本章包含以下部分：

日志记录概述

网络安全设备通过将自己的系统和流量管理活动写入日志文件来记录这些活动。管理员可以查阅这些日志文件，以监控设备和排除设备故障。

设备将不同类型的活动划分为不同的日志记录类型，以简化查找具体活动相关信息的任务。其中大部分类型在默认情况下自动启用，但有些类型必须根据需要手动启用。

您通过日志文件订用启用和管理日志文件。您可利用订用来定义用于创建、自定义和管理日志文件的设置。

管理员通常使用的两个主要日志文件类型如下：

- **访问日志**。这记录所有 Web 代理过滤和扫描活动。

- **流量监控器日志**。这记录所有 L4 流量监控器活动。

可使用这些及其他日志类型，查看当前和过去的设备活动。参考表可帮助您说明日志文件条目。

相关主题

- 常见的日志记录任务，第 332 页
- 日志文件类型，第 333 页

常见的日志记录任务

任务	相关主题和程序的链接
添加和编辑日志订用	添加和编辑日志订用，第 338 页
查看日志文件	查看日志文件，第 344 页
解释日志文件	解释访问日志扫描判定条目，第 354 页
自定义日志文件	自定义访问日志，第 361 页
推送日志文件到另一台服务器	将日志文件推送到另一台服务器，第 342 页
存档日志文件	存档日志文件，第 343 页

日志记录的最佳实践

- 最大限度减少日志订用数量将有益于提高系统性能。
- 记录较少详细信息将有益于提高系统性能。

使用日志排除 Web 代理问题

默认情况下，网络安全设备有一个为 Web 代理日志记录消息创建的日志订用，称为“默认代理日志”。其用于捕获有关所有 Web 代理模块的基本信息。设备还有用于每个 Web 代理模块的日志文件类型，因此您可以阅读有关每个模块的更具体的调试信息，而不扰乱默认代理日志。

使用各种可用日志，按照以下步骤对 Web 代理问题进行故障排除。

步骤 1 阅读默认代理日志。

步骤 2 如果您看到可能与问题相关的条目，但没有足够的信息来解决问题，则为相关的具体 Web 代理模块创建日志订用。以下 Web 代理模块日志类型可用：

访问控制引擎日志 AVC 引擎框架日志 配置日志 连接管理日志 数据安全模块日志 DCA 引擎框架日志 磁盘管理器日志 FireAMP FTP 代理日志 HTTPS 日志 许可模块日志	日志记录框架日志 McAfee 集成框架日志 内存管理器日志 杂项代理模块日志 请求调试日志 SNMP 模块日志 Sophos 集成框架日志 WBRS 框架日志 WCCP 模块日志 Webcat 集成框架日志 Webroot 集成框架日志

步骤 3 重新创建问题，并阅读新 Web 代理模块日志，了解相关条目。

步骤 4 根据需要对其他 Web 代理模块日志重复此过程。

步骤 5 删除不再需要的订用。

下一步做什么

相关主题

- 日志文件类型， 第 333 页
- 添加和编辑日志订用， 第 338 页

日志文件类型

与 Web 代理组件相关的某些日志类型未启用。默认情况下启用主要 Web 代理日志类型（称为“默认代理日志”），并捕获有关所有 Web 代理模块的基本信息。每个 Web 代理模块还有其自己日志类型，您可以根据需要手动启用这些日志类型。

下表介绍了网络安全设备日志文件类型。

日志文件类型	说明	支持系统日志推送？	默认情况下启用？
访问控制引擎日志	记录与 Web 代理 ACL（访问控制列表）评估引擎相关的消息。	否	否

日志文件类型	说明	支持系统日志推送？	默认情况下启用？
AMP 引擎日志	记录有关文件信誉扫描和文件分析（高级恶意软件保护）的信息。 另请参阅日志文件，第 249 页。	是	是
审核日志	记录AAA（身份验证、授权和记帐）事件。记录与应用和命令行界面进行的所有用户交互，并捕获已提交的更改。 某些审核日志详细信息如下： • 用户 - 登录 • 用户 - 登录失败，密码不正确 • 用户 - 登录失败，用户名未知 • 用户 - 登录失败，帐户到期 • 用户 - 注销 • 用户 - 锁定 • 用户 - 已激活 • 用户 - 密码更改 • 用户 - 密码重置 • 用户 - 安全设置/配置文件更改 • 用户 - 已创建 • 用户 - 已删除/修改 • 组/角色 - 删除/已修改 • 组/角色 - 权限更改	是	是
访问日志	记录 Web 代理客户端历史记录。	是	是
身份验证框架日志	记录身份验证历史记录和消息。	否	是
AVC 引擎框架日志	记录与 Web 代理和 AVC 引擎之间的通信相关的消息。	否	否
AVC 引擎日志	记录来自 AVC 引擎的调试消息。	是	是
CLI审核日志	记录命令行界面活动的历史审核。	是	是
配置日志	记录与 Web 代理配置管理系统相关的消息。	否	否

日志文件类型	说明	支持系统日志推送？	默认情况下启用？
连接管理日志	记录与 Web 代理连接管理系统相关的消息。	否	否
数据安全日志	记录由思科数据安全过滤器评估的上传请求客户端历史记录。	是	是
数据安全模块日志	记录与思科数据安全过滤器相关的消息。	否	否
DCA 引擎框架日志（动态内容分析）	记录与Web代理和思科网络使用控件动态内容分析引擎之间的通信相关的消息。	否	否
DCA 引擎日志（动态内容分析）	记录与思科网络使用控件动态内容分析引擎相关的消息。	是	是
默认代理日志	记录与 Web 代理相关的错误。 这是所有与Web代理相关的日志中最基本的功能。要对与Web代理相关的更多具体方面进行故障排除，请为适用的Web代理模块创建一个日志订用。	是	是
磁盘管理器日志	记录与写入磁盘缓存相关的 Web 代理消息。	否	否
外部身份验证日志	记录与使用外部身份验证功能相关的消息，例如与外部身份验证服务器通信成功还是失败。 即使外部身份验证已禁用，此日志仍会包含有关本地用户登录成功或失败的消息。	否	是
反馈日志	记录报告页面分类错误的 Web 用户。	是	是
FTP 代理日志	记录与 FTP 代理相关的错误和警告消息。	否	否
FTP服务器日志	记录使用FTP上传到网络安全设备或从该设备下载的所有文件。	是	是
GUI 日志（图形用户界面）	记录Web界面中的页面刷新历史记录。GUI日志还包括有关 SMTP 事务的信息，例如有关通过邮件从设备发送的计划报告的信息。	是	是
Haystack 日志	Haystack 日志会记录跟踪数据处理的 Web 事务。	是	是
HTTPS 日志	记录特定于 HTTPS 代理的 Web 代理消息（当启用 HTTPS 代理时）。	否	否
ISE 服务器日志	记录 ISE 服务器连接和运行信息。	是	是

日志文件类型	说明	支持系统日志推送？	默认情况下启用？
许可模块日志	记录与Web代理的许可证和功能密钥处理系统相关的消息。	否	否
记录框架日志	记录与Web代理的日志记录系统相关的消息。	否	否
记录日志	记录与日志管理相关的错误。	是	是
McAfee 集成框架日志	记录与 Web 代理和 McAfee 扫描引擎之间的通信相关的消息。	否	否
McAfee 日志	记录来自 McAfee 扫描引擎的防恶意软件扫描活动的状态。	是	是
内存管理器日志	记录与管理所有内存相关的Web代理消息，包括 Web 代理进程的内存缓存消息。	否	否
杂项代理模块日志	记录主要被开发人员或客户支持使用的Web代理消息。	否	否
AnyConnect安全移动守护程序日志	记录网络安全设备和 AnyConnect 客户端之间的交互，包括状态检查。	是	是
NTP 日志 （网络时间协议）	记录网络时间协议进行的系统时间更改。	是	是
PAC 文件托管后台守护程序日志	记录由客户端使用的代理自动配置 (PAC) 文件。	是	是
代理旁路日志	记录绕过 Web 代理的事务。	否	是
报告日志	记录报告生成历史记录。	是	是
路由查询日志	记录与报告生成相关的错误。	是	是
请求调试日志	记录所有 Web 代理模块日志类型中有关特定 HTTP 事务的详细调试信息。您可能要创建此日志订用，以对特定事务的代理问题进行故障排除，无需创建所有其他代理日志订用。 **注：**您只能在 CLI 中创建此日志订用。	否	否
身份验证日志	记录与访问控制功能相关的消息。	是	是
SHD 日志 （系统运行状况后台守护程序）	记录系统服务运行状况的历史记录以及后台守护程序意外重启的历史记录。	是	是

日志文件类型	说明	支持系统日志推送？	默认情况下启用？
SNMP 日志	记录与 SNMP 网络管理引擎相关的调试消息。	是	是
SNMP 模块日志	记录有关与 SNMP 监控系统交互的 Web 代理消息。	否	否
Sophos 集成框架日志	记录与 Web 代理和 Sophos 扫描引擎之间的通信相关的消息。	否	否
Sophos 日志	记录来自 Sophos 扫描引擎的防恶意软件扫描活动的状态。	是	是
状态日志	记录与系统相关的信息，例如功能密钥下载。	是	是
系统日志	记录 DNS、错误并确认活动。	是	是
通信监控错误日志	记录 L4TM 接口并捕获错误。	是	是
通信监控日志	记录添加到 L4TM 块的站点并允许列表。	否	是
UDS 日志 （用户发现服务）	记录有关 Web 代理如何不执行实际身份验证即发现用户名的数据。其包括有关与 Secure Mobility 的思科自适应安全设备交互以及与透明用户标识的 Novell eDirectory 服务器集成的信息。	是	是
更新程序日志	记录 WBRS 及其他更新的历史记录。	是	是
W3C 日志	以符合 W3C 的格式记录 Web 代理客户端历史记录。 有关详细信息，请参阅符合 W3C 标准的访问日志文件，第 359 页。	是	否
WBNP 日志 （SensorBase 网络参与）	记录 Cisco SensorBase 网络参与上传到 SensorBase 网络的历史记录。	否	是
WBRS 框架日志 （Web 信誉分数）	记录与 Web 代理和 Web 信誉过滤器之间的通信相关的消息。	否	否
WCCP 模块日志	记录与实施 WCCP 相关的 Web 代理消息。	否	否
Webcat 集成框架日志	记录与 Web 代理和思科网络使用控件关联 URL 过滤引擎之间的通信相关的消息。	否	否

日志文件类型	说明	支持系统日志推送？	默认情况下启用？
Webroot 集成框架日志	记录与 Web 代理和 Webroot 扫描引擎之间的通信相关的消息。	否	否
Webroot 日志	记录来自 Webroot 扫描引擎的防恶意软件扫描活动的状态。	是	是
欢迎页面确认日志	记录在最终用户确认页面点击“接受”(Accept) 按钮的 Web 客户端的历史记录。	是	是

添加和编辑日志订用

您可为每种类型的日志文件创建多个日志订用。订用包括存档和存储的详细配置信息，其中包括：

- 滚动设置，确定什么时候存档日志文件。
- 已存档日志的压缩设置。
- 已存档日志的检索设置，指定日志是存档到远程服务器还是存储在设备中。

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**。

步骤 2 要添加日志订用，点击**添加日志订用 (Add Log Subscription)**。或者，要编辑日志订用，请点击“日志名称”(Log Name) 字段中的日志文件名。

步骤 3 配置订用：

选项	说明
日志类型 (Log Type)	您可以订用的可用日志文件类型列表。页面上的其他选项可能会因您选择的日志文件类型而有所不同。 **注释** “请求调试日志”日志类型只能使用 CLI 进行订用，并且不会显示在此列表中。
日志名称 (Log Name)	用于描述网络安全设备上的订用的名称。此名称也用于将存储订用日志文件的日志目录。
按文件大小滚动 (Rollover by File Size)	在存档当前日志文件并启动新日志文件之前，当前日志文件可增长到的最大文件大小。输入 100 KB 至 10 GB 之间的数字。

选项	说明
按时间滚动 (Rollover by Time)	系统存档当前日志文件并且开始新日志文件前允许的最大时间间隔。以下间隔类型可用： • **无**。AsyncOS 仅在日志文件达到最大文件大小时执行回滚。 • **自定义时间间隔**。AsyncOS 将在上次回滚后经过指定的一段时间再执行回滚。用 d、h、m 和 s 作为后缀指定滚动之间的天数、小时数、分钟数和秒数。 • **每日回滚**。AsyncOS 每天在指定的时间执行滚动。使用逗号分隔一天内的多个时间。使用星号 (*) 指定在一天内的每一小时执行一次滚动。您还可以使用星号指定在一小时内的每一分钟执行一次滚动。 • **每周滚动 (Weekly Rollover)**。AsyncOS 在一周中的一天或多天在指定的时间执行滚动。
日志样式 (Log Style) （访问日志）	指定要使用的日志格式，Squid、Apache 或 Squid Details。

自定义字段 (Custom Fields)
（访问日志）
	允许您在每个访问日志条目中包括自定义信息。
	“自定义字段”(Custom Field) 中输入格式说明符的语法如下：
	`<format_specifier_1> <format_specifier_2> ...`
	例如：`%a %b %E`
	可以在格式说明符之前添加令牌，以在访问日志文件中显示描述性文本。例如：
	`client_IP %a body_bytes %b error_type %E`
	其中，`client_IP` 是日志格式说明符 `%a` 的说明令牌，以此类推。

文件名 (File Name)	日志文件的名称。当前日志文件附加 `.c` 扩展名，而滚动日志文件附加文件创建时间戳和 `.s` 扩展名。
日志字段 (Log Fields) （W3C 访问日志）	允许您选择想要包含在 W3C 访问日志中的字段。 选择“可用字段”(Available Fields) 列表中的字段，或在“自定义字段”(Custom Field) 框中键入字段，然后点击“添加”(Add)。 字段在“选定日志字段”(Selected Log Fields) 列表中的显示顺序决定了 W3C 访问日志文件中字段的顺序。您也可以使用**上移 (Move Up)** 和**下移 (Move Down)** 按钮来更改字段的顺序。您可以通过在“所选日志字段”(Selected Log Fields) 列表中选择待删除的字段，然后点击**删除 (Remove)** 来删除它。 您可在“自定义字段”(Custom Fields) 框中输入多个用户定义的字段并同时添加它们，只要在点击**添加 (Add)** 之前将每个条目用新行（点击 Enter 键）来分隔。 当您更改 W3C 日志订用中包括的日志字段时，日志订用会自动转换。这样，最新版本的日志文件便会包含正确的新字段信头 在创建日志后，如果需要，可以取消已匿名化字段的匿名化。请参阅 对 W3C 日志字段取消匿名，第 341 页

选项	说明
日志压缩 (Log Compression)	指定是否压缩滚动后的文件。AsyncOS 使用 gzip 压缩格式压缩日志文件。
日志排外 (Log Exclusions)（可选）： （访问日志）	允许您指定 HTTP 状态代码（仅 4xx 或 5xx）来从访问日志或 W3C 访问日志排除关联事务。 例如，输入 401 将过滤出具有该事务号的身份验证失败请求。
日志级别 (Log Level)	指定日志条目的详细程度。选项包括： • **严重 (Critical)**。仅包含错误。这是详细程度最低的设置，等同于系统日志级别“警报”(Alert)。 • **警告 (Warning)**。包括错误和警告。此日志级别相当于系统日志级别“警告”(Warning)。 • **信息 (Information)**。包括错误、警告及其他系统操作。这是默认的详细级别，等同于系统日志级别“信息”(Info)。 • **调试 (Debug)**。包括可用于调试系统问题的数据。尝试发现错误原因时，使用“调试”(Debug) 日志级别。可临时使用该设置，然后返回默认级别。此日志级别相当于系统日志级别“调试”(Debug)。 • **跟踪 (Trace)**。这是最详细的设置。此级别包括系统操作和活动的完整记录。仅建议开发人员使用“跟踪”(Trace) 日志级别。使用此级别会造成严重的系统性能下降，建议不要使用。此日志级别相当于系统日志级别“调试”(Debug)。 **注释** 更详细的设置会生成更大的日志文件，并对系统性能造成更大的影响。
检索方法	指定存储滚动日志文件的位置以及检索这些文件以读取它们的方式。有关可用方法的说明，请参阅下文。
检索方法： FTP 到设备 (FTP on Appliance)	“FTP 到设备”方法（等同于 FTP 轮询）需要远程 FTP 客户端使用管理或操作用户的用户名和密码访问设备，以检索日志文件。 如果选择此方法，必须输入在设备上存储日志文件的最大数量。当达到最大数量时，系统将删除最早的文件。 这是默认检索方法。
检索方法： FTP 到其他服务器 (FTP on Remote Server)	“FTP 到远程服务器”(FTP on Remote Server) 方法（等同于 FTP 推送）定期将日志文件推送到远程计算机上的 FTP 服务器。 如果选择此方法，必须输入以下信息： • FTP 服务器主机名 • FTP 服务器上用于存储日志文件的目录 • 拥有 FTP 服务器连接权限的用户的用户名和密码 **注释** AsyncOS for Web 仅支持被动模式的远程 FTP 服务器。它无法将日志文件推送到处于主动模式的 FTP 服务器。

选项	说明
检索方法： SCP 到其他服务器 (SCP on Remote Server)	“SCP 到远程服务器”(SCP on Remote Server) 方法（等同于 SCP 推送）定期使用安全复制协议将日志文件推送到远程 SCP 服务器。此方法要求远程计算机上的 SSH SCP 服务器使用 SSH2 协议。这种订用需要提供远程计算机上的用户名、SSL 密钥和目标目录。日志文件根据您设置的滚动计划传输。 如果选择此方法，必须输入以下信息： • SCP 服务器主机名 • SCP 服务器上用于存储日志文件的目录 • 拥有 SCP 服务器连接权限的用户的用户名
检索方法： Syslog Push	只能选择基于文本的日志的系统日志。 “系统日志推送”(Syslog Push) 方法将日志消息发送到端口 514 上的远程系统日志服务器。此方法符合 RFC 3164 标准。 如果选择此方法，必须输入以下信息： • 系统日志服务器主机名 • 传输使用的协议，UDP 或 TCP • 最大邮件大小 UDP 的有效值为 1024 至 9216。 TCP 的有效值为 1024 至 65535。 最大消息大小取决于系统日志服务器配置。 • 与日志结合使用的设备

步骤 4 提交并确认更改。

下一步做什么

如果您选择了 SCP 作为检索方法，请注意，设备会显示 SSH 密钥，您需要将它添加到 SCP 服务器主机。请参阅将日志文件推送到另一台服务器，第 342 页。

相关主题

- 日志文件类型，第 333 页
- 日志文件名称和设备目录结构，第 343 页

对 W3C 日志字段取消匿名

如果在日志订用期间启用了字段值（*c-ip*、*cs-username* 和 *cs-auth-group*）的匿名功能，目标日志服务器将收到这些日志字段的匿名值（*c-a-ip*、*cs-a-username* 和 *cs-a-auth-group*），而不是实际值。如果要查看实际值，必须对日志字段取消匿名。

在添加 W3C 日志订用过程中，您可以对匿名化的 *c-a-ip*、*cs-a-username* 和 *cs-a-auth-group* 日志字段值取消匿名。

步骤 1 依次选择**系统管理 (System Administration)** > **日志订用 (Log Subscriptions)**。

步骤 2 对要取消匿名的匿名字段的日志，请点击与其对应的“取消匿名”(Denonymization) 列中的**取消匿名 (Deanonymization)**。

步骤 3 在**方法 (Method)** 部分中，选择下列任一方法以输入要取消匿名的加密文本。

- 粘贴已加密文本，将其粘贴到“匿名文本”(Anonymized Text) 字段中。在此字段中最多可以输入 500 个条目。必须用逗号分隔多个条目。
- 上传文件，选择包含加密文本的文件。文件最多可以存储 1000 个条目。文件格式应为 CSV。系统支持空格、新行、制表符和分号作为字段分隔符。

注释 如果更改了密码，则必须输入旧密码，以对旧数据取消匿名。

步骤 4 点击**取消匿名 (Deanonymize)**，“取消匿名结果”(Deanonymization Result) 表将显示已取消匿名的日志字段值。

将日志文件推送到另一台服务器

开始之前

创建或编辑所需的日志订用，选择 SCP 作为检索方法。添加和编辑日志订用，第 338 页

步骤 1 将密钥添加到远程系统：

a) 访问 CLI。

b) 输入 `logconfig -> hostkeyconfig` 命令。

c) 使用以下命令来显示密钥：

命令	描述
Host	显示系统主机密钥。这是放置在远程系统上“known_hosts”文件中的值。
用户	显示将日志推送到远程计算机的系统帐户的公钥。这与设置 SCP 推送订用时显示的密钥相同。这是放置在远程系统上“authorized_keys”文件中的值。

d) 将这些密钥添加到远程系统。

步骤 2 仍在 CLI 中，将远程服务器的 SSH 公共主机密钥添加到设备：

命令	描述
新	添加新密钥。

命令	描述
指纹	显示系统主机密钥指纹。

步骤 3 确认您的更改。

存档日志文件

当前日志文件达到用户指定的最大文件大小限制或自从上次滚动之后达到最长时间时，AsyncOS 会存档（滚动）日志订用。

这些存档设置包括在日志订用中：

- 按文件大小滚动 (Rollover by File Size)
- 按时间滚动 (Rollover by Time)
- 日志压缩 (Log Compression)
- 检索方法 (Retrieval Method)

您也可以手动存档（滚动）日志文件。

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**。

步骤 2 选中您要存档的日志订用的“滚动”(Rollover) 栏中的复选框，或选中**所有 (All)** 复选框以选择所有订用。

步骤 3 点击**立即滚动 (Rollover Now)** 以存档选定的日志。

下一步做什么

相关主题

- 添加和编辑日志订用，第 338 页
- 日志文件名称和设备目录结构，第 343 页

日志文件名称和设备目录结构

设备基于日志订用名称为每个日志订用创建目录。目录中的日志文件名包含以下信息：

- 在日志订用中指定的日志文件名
- 日志文件开始时的时间戳
- 单字符状态代码，.c（表示当前）或 .s（表示已保存）

日志的文件名使用以下公式生成：

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

注释 仅限传输处于已保存状态的日志文件。

读取和解释日志文件

您可以读取当前日志文件活动，作为监控和排除网络安全设备故障的一种方法。使用设备界面即可完成读取。

您还可以阅读存档文件，查看过去活动的记录。如果存档文件存储在设备上，使用设备界面即可完成读取；否则必须使用适当的方法从其外部存储位置读取。

日志文件中的每项信息都用字段变量来表示。通过确定哪个字段代表哪项信息，您可以查询字段功能和解释日志文件内容。对于W3C兼容访问日志，文件标题按照字段名称在日志条目中显示的顺序列出字段名称。然而，对于标准访问日志，您必须查阅有关此日志类型的文档，了解有关其字段顺序的信息。

相关主题

- 查看日志文件，第 344 页.
- 访问日志文件中的 Web 代理信息，第 345 页.
- 解释 W3C 访问日志，第 359 页.
- 流量监控器日志说明，第 364 页.
- 日志文件字段和标签，第 365 页.

查看日志文件

开始之前

请注意，此查看方法适用于在设备上存储的日志文件。查看外部存储的文件的过程不在本文档的讨论范围内。

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**。

步骤 2 点击日志订用列表的“日志文件”(Log Files) 列中的日志订用名称。

步骤 3 出现提示时，输入用于访问设备的管理员用户名和密码。

步骤 4 登录后，点击其中一个日志文件，在浏览器中查看它，或将其保存到磁盘。

步骤 5 刷新浏览器获得更新的结果。

注释 如果日志订用已压缩，请下载并解压，然后打开它。

下一步做什么

相关主题

- 访问日志文件中的 Web 代理信息， 第 345 页.
- 解释 W3C 访问日志， 第 359 页.
- 流量监控器日志说明， 第 364 页.

访问日志文件中的 Web 代理信息

访问日志文件提供所有 Web 代理过滤和扫描活动的描述性记录。访问日志文件条目显示设备如何处理每个事务的记录。

访问日志以两种格式提供：标准和 W3C 兼容格式。W3C 兼容日志文件在内容和布局方面比标准访问日志更加可自定义。

以下文本是一个事务的示例访问日志文件条目：

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e" >
 -
```

格式说明符	字段值	字段描述
%t	1278096903.150	自 UNIX 时期以来的时间戳。
%e	97	经过时间（延迟），以毫秒为单位。
%a	172.xx.xx.xx	客户端 IP 地址。 **注：**您可选择使用 advancedproxyconfig > authentication CLI 命令屏蔽访问日志中的 IP 地址。
%w	TCP_MISS	事务结果代码。 有关详细信息，请参阅符合 W3C 标准的访问日志文件，第 359 页。
%h	200	HTTP 响应代码。
%s	8187	响应大小（报头 + 正文）。

格式说明符	字段值	字段描述
%1r %2r	`GET http://my.site.com/`	请求的第一行。 注：当请求的第一行针对本地FTP事务时，文件名中的某些特殊字符在访问日志中采用 URL 编码。例如，“@”符号在访问日志中写为“%40”。 以下字符采用 URL 编码： & # % + , : ; = @ ^ { } [ ]
%A	-	经过身份验证的用户名。 **注：**您可选择使用 `advancedproxyconfig > authentication` CLI 命令屏蔽访问日志中的用户名。
%H	`DIRECT`	用于说明与哪台服务器联系以检索请求内容的代码。 最常用的值包括： • **NONE**。Web代理具有内容，因此它不与任何其他服务器联系以检索内容。 • **DIRECT**。Web 代理转向请求中命名的服务器以获取内容。 • **DEFAULT_PARENT**。Web 代理转向其主要父代理或外部 DLP 服务器以获取内容。
%d	`my.site.com`	数据源或服务器 IP 地址。
%c	`text/plain`	响应正文 MIME 类型。
%D	`DEFAULT_CASE_11`	ACL 决策标记。 **注：**ACL 决策标记的末尾包括 Web 代理在内部使用的动态生成的编号。您可以忽略此编号。 有关详细信息，请参阅ACL 决策标记，第 349 页。

格式说明符	字段值	字段描述
不适用（ACL 决策标记的一部分）	`PolicyGroupName`	负责对此事务（访问策略、解密策略或数据安全策略）作出最终决策的策略组的名称。当事务与全局策略匹配时，该值为“DefaultGroup”。 策略组名称中包含的任何空格均使用下划线 (_) 来替换。
不适用（ACL 决策标签的一部分）	`Identity`	身份策略组名称。 策略组名称中包含的任何空格均使用下划线 (_) 来替换。
不适用（ACL 决策标签的一部分）	`OutboundMalwareScanningPolicy`	出站恶意软件扫描策略组名称。 策略组名称中包含的任何空格均使用下划线 (_) 来替换。
不适用（ACL 决策标签的一部分）	`DataSecurityPolicy`	思科数据安全策略组名称。当事务符合全局思科数据安全策略时，该值是“DefaultGroup”。仅当思科数据安全过滤器已启用时，此策略组名称才会显示。当没有适用的数据安全策略时，显示“NONE”。 策略组名称中包含的任何空格均使用下划线 (_) 来替换。
不适用（ACL 决策标签的一部分）	`ExternalDLPPolicy`	外部 DLP 策略组名称。当事务符合全局外部 DLP 策略时，该值为“DefaultGroup”。当没有适用的外部 DLP 策略时，显示“无”(None)。 策略组名称中包含的任何空格均使用下划线 (_) 来替换。
不适用（ACL 决策标签的一部分）	`RoutingPolicy`	路由策略组名称为 *ProxyGroupName/ProxyServerName*。 当事务匹配全局路由策略时，该值为“DefaultRouting”。当未使用任何上游代理服务器时，该值为“DIRECT”。 策略组名称中包含的任何空格均使用下划线 (_) 来替换。

格式说明符	字段值	字段描述
%Xr	<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"","-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	扫描判定信息。在尖括号内，访问日志包括来自各个扫描引擎的判定信息。 有关尖括号中包括的值的详细信息，请参阅解释访问日志扫描判定条目，第 354 页和恶意软件扫描判定值，第 375 页。
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%	-	可疑用户代理。

事务结果代码

访问日志文件中的事务结果代码说明了设备如何解决客户端请求。例如，如果一个对象的请求可通过缓存解决，则结果代码为 TCP_HIT。但是，如果对象不存在于缓存中，设备从原始服务器提取对象，则结果代码为 TCP_MISS。下表介绍事务结果代码。

结果代码	说明
TCP_HIT	请求的对象从磁盘缓存中获取。
TCP_IMS_HIT	客户端发送了一个 IMS (If-Modified-Since) 对象请求，并在缓存中找到了该对象。代理产生 304 响应。
TCP_MEM_HIT	请求的对象从内存缓存中获取。
TCP_MISS	未在缓存中找到对象，因此从源服务器获取了该对象。
TCP_REFRESH_HIT	对象在缓存中，但已过期。代理向源服务器发送了一个 IMS (If-Modified-Since) 请求，服务器确认未修改该对象。因此，设备从磁盘缓存或内存缓存获取了该对象。
TCP_CLIENT_REFRESH_MISS	客户端发送了一个“don’t fetch response from cache”请求，该请求报头为“Pragma: no-cache”。由于该报头来自客户端，设备从源服务器获取了该对象。
TCP_DENIED	客户端请求因访问策略而被拒绝。
UDP_MISS	对象从源服务器获取。

结果代码	说明
NONE	事务中有错误。例如，DNS 故障或网关超时。

ACL 决策标记

ACL 决策标记是访问日志条目中的字段，用于指示 Web 代理如何处理事务。它包括来自 Web 信誉过滤器、URL 类别和扫描引擎的信息。

注释 ACL 决策标记的末尾包括一个动态生成的数字，Web 代理在内部使用该数字提高性能。您可以忽略此数字。

下表介绍了 ACL 决策标记值。

ACL 决策标记	说明
ALLOW_ADMIN_ERROR_PAGE	Web 代理允许了到通知页面和到该页面上使用的任何徽标的事务。
ALLOW_CUSTOMCAT	Web 代理基于访问策略组的自定义 URL 类别过滤设置允许了事务。
ALLOW_REFERER	Web 代理基于嵌入/引用的内容免除允许了事务。
ALLOW_WBRS	Web 代理基于访问策略组的 Web 信誉过滤器设置允许了事务。
AMP_FILE_VERDICT	表示文件的 AMP 信誉服务器所提供的判定的值： • 1 - 未知 • 2 - 正常 • 3 - 恶意 • 4 - 不可扫描

ACL 决策标记	说明
ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDFILETYPE ARCHIVESCAN_NESTEDTOODEEP ARCHIVESCAN_UNKNOWNFMT ARCHIVESCAN_UNSCANABLE ARCHIVESCAN_FILETOOBIG	**存档扫描判定** ARCHIVESCAN_ALLCLEAR - 已检查的存档中没有阻止的文件类型。 ARCHIVESCAN_BLOCKEDFILETYPE - 已检查的存档中有一个阻止的文件类型。日志条目（判定详细信息）中的下一个字段提供详细信息，具体是指阻止的文件的类型以及阻止的文件的名称。 ARCHIVESCAN_NESTEDTOODEEP - 存档被阻止，因为它包含的“封装”或嵌套的存档数多于所配置的最大值。“判定详细信息”字段包含“阻止了不可扫描的存档"。 ARCHIVESCAN_UNKNOWNFMT - 存档被阻止，因为它包含未知格式的文件类型。“判定详细信息”是“阻止了不可扫描的存档"。 ARCHIVESCAN_UNSCANABLE - 存档被阻止，因为它包含无法扫描的文件。“判定详细信息”是“阻止了不可扫描的存档"。 ARCHIVESCAN_FILETOOBIG - 存档被阻止，因为存档的大小超过了配置的最大值。“判定详细信息”是“阻止了不可扫描的存档"。 **存档扫描判定详细信息** 日志条目中“判定”字段后面的字段提供有关判定的其他信息，例如阻止的文件的类型和阻止的文件的名称、“阻止了不可扫描的存档”或“-”，以指示存档不包含任何阻止的文件类型。 例如，如果基于“访问策略: 自定义对象阻止”设置阻止了可检查存档文件 (ARCHIVESCAN_BLOCKEDFILETYPE)，则“判定详细信息”条目包括阻止的文件的类型以及阻止的文件的名称。 有关存档检查的详细信息，请参阅访问策略：阻止对象，第 185 页和存档检查设置，第 187 页。
BLOCK_ADMIN	基于访问策略组的某些默认设置阻止了事务。
BLOCK_ADMIN_CONNECT	基于访问策略组的 HTTP CONNECT 端口设置中定义的目标 TCP 端口阻止了事务。
BLOCK_ADMIN_CUSTOM_USER_AGENT	基于访问策略组的阻止自定义用户代理设置中定义的用户代理阻止了事务。
BLOCK_ADMIN_TUNNELING	Web 代理基于访问策略组的 HTTP 端口上的非 HTTP 流量隧道阻止了事务。
BLOCK_ADMIN_HTTPS_ NonLocalDestination	事务被阻止；客户端尝试使用 SSL 端口作为显式代理来绕过身份验证。为防止这种情况发生，如果 SSL 连接到 WSA 自身，则只允许向实际 WSA 重定向主机名发送请求。

ACL 决策标记	说明
BLOCK_ADMIN_IDS	基于数据安全策略组中定义的请求正文内容的 MIME 类型阻止了事务。
BLOCK_ADMIN_FILE_TYPE	基于访问策略组中定义的文件类型阻止了事务。
BLOCK_ADMIN_PROTOCOL	基于访问策略组的阻止协议设置中定义的协议阻止了事务。
BLOCK_ADMIN_SIZE	基于访问策略组的对象大小设置中定义的响应大小阻止了事务。
BLOCK_ADMIN_SIZE_IDS	基于数据安全策略组中定义的请求正文内容的大小阻止了事务。
BLOCK_AMP_RESP	Web 代理基于访问策略组的高级恶意软件保护设置阻止了响应。
BLOCK_AMW_REQ	Web代理基于出站恶意软件扫描策略组的防恶意软件设置阻止了请求。请求正文生成了肯定的恶意软件判定。
BLOCK_AMW_RESP	Web 代理基于访问策略组的防恶意软件设置阻止了响应。
BLOCK_AMW_REQ_URL	Web 代理发现 HTTP 请求中的可疑 URL 可能不安全，因此基于访问策略组的防恶意软件设置在请求时间阻止了事务。
BLOCK_AVC	基于访问策略组的已配置应用设置阻止了事务。
BLOCK_CONTENT_UNSAFE	基于访问策略组的站点内容评分设置阻止了事务。客户端请求适用于成人内容，并且策略配置为阻止成人内容。
BLOCK_CONTINUE_CONTENT_UNSAFE	基于访问策略组的站点内容分级设置阻止了事务并显示了“警告并继续”(Warn and Continue) 页面。客户端请求针对成人内容，但策略配置为向访问成人内容的用户发出警告。
BLOCK_CONTINUE_CUSTOMCAT	基于配置为“警告”(Warn)的访问策略组中的自定义URL类别阻止了事务并显示了“警告并继续”(Warn and Continue) 页面。
BLOCK_CONTINUE_WEBCAT	基于配置为“警告”(Warn)的访问策略组中的预定义URL类别阻止了事务并显示了“警告并继续”(Warn and Continue) 页面。
BLOCK_CUSTOMCAT	基于访问策略组的自定义 URL 类别过滤设置阻止了事务。
BLOCK_ICAP	Web 代理基于外部 DLP 策略组中定义的外部 DLP 系统的判定阻止了请求。
BLOCK_SEARCH_UNSAFE	客户端请求包括了不安全的搜索查询，并且访问策略配置为实施安全搜索，因此原始客户端请求被阻止。
BLOCK_SUSPECT_USER_AGENT	基于访问策略组的“可疑用户代理”设置阻止了事务。

ACL 决策标记	说明
BLOCK_UNSUPPORTED_SEARCH_APP	基于访问策略组的安全搜索设置阻止了事务。事务适用于不受支持的搜索引擎，并且策略配置为阻止不受支持的搜索引擎。
BLOCK_WBRS	基于访问策略组的 Web 信誉过滤器设置阻止了事务。
BLOCK_WBRS_IDS	Web 代理基于数据安全策略组的 Web 信誉过滤器设置阻止了上传请求。
BLOCK_WEBCAT	基于访问策略组的 URL 类别过滤设置阻止了事务。
BLOCK_WEBCAT_IDS	Web代理基于数据安全策略组的URL类别过滤设置阻止了上传请求。
DECRYPT_ADMIN	Web 代理基于解密策略组的某些默认设置解密了事务。
DECRYPT_ADMIN_EXPIRED_CERT	尽管服务器证书已过期，但 Web 代理对事务进行了解密。
DECRYPT_WEBCAT	Web 代理基于解密策略组的 URL 类别过滤设置解密了事务。
DECRYPT_WBRS	Web 代理基于解密策略组的 Web 信誉过滤器设置解密了事务。
DEFAULT_CASE	由于事务中没有发生 AsyncOS 服务（如 Web 信誉或防恶意软件扫描），Web 代理允许了客户端访问服务器。
DROP_ADMIN	Web 代理基于解密策略组的某些默认设置丢弃了事务。
DROP_ADMIN_EXPIRED_CERT	由于服务器证书已过期，因此 Web 代理丢弃了该事务。
DROP_WEBCAT	Web 代理基于解密策略组的 URL 类别过滤设置丢弃了事务。
DROP_WBRS	Web 代理基于解密策略组的 Web 信誉过滤器设置丢弃了事务。
MONITOR_ADMIN_EXPIRED_CERT	由于服务器证书已过期，因此 Web 代理监控了服务器响应。
MONITOR_AMP_RESP	Web代理基于访问策略组的高级恶意软件保护设置监控了服务器响应。
MONITOR_AMW_RESP	Web 代理基于访问策略组的防恶意软件设置监控了服务器响应。
MONITOR_AMW_RESP_URL	Web代理发现HTTP请求中的可疑URL可能不安全，因此基于访问策略组的防恶意软件设置监控了事务。
MONITOR_AVC	Web 代理基于访问策略组的应用设置监控了事务。

ACL 决策标记	说明
MONITOR_CONTINUE_CONTENT_UNSAFE	Web 代理最初基于访问策略组的站点内容分级设置阻止了事务并显示了“警告并继续”(Warn and Continue) 页面。客户端请求针对成人内容，但策略配置为向访问成人内容的用户发出警告。用户收到了警告并继续前往最初请求的站点，随后没有任何其他扫描引擎阻止该请求。
MONITOR_CONTINUE_CUSTOMCAT	Web 代理最初基于配置为“警告”(Warn) 的访问策略组中的自定义 URL 类别阻止了事务并显示了“警告并继续”(Warn and Continue) 页面。用户收到了警告并继续前往最初请求的站点，随后没有任何其他扫描引擎阻止该请求。
MONITOR_CONTINUE_WEBCAT	Web 代理最初基于配置为“警告”(Warn) 的访问策略组中的预定义 URL 类别阻止了事务并显示了“警告并继续”(Warn and Continue) 页面。用户收到了警告并继续前往最初请求的站点，随后没有任何其他扫描引擎阻止该请求。
MONITOR_IDS	Web 代理使用数据安全策略或外部 DLP 策略扫描了上传请求，但未阻止该请求。它根据访问策略评估了该请求。
MONITOR_SUSPECT_USER_AGENT	Web 代理基于访问策略组的可疑用户代理设置监控了事务。
MONITOR_WBRS	Web 代理基于访问策略组的 Web 信誉过滤器设置监控了事务。
NO_AUTHORIZATION	Web 代理未允许用户访问应用，因为虽然用户已针对身份验证领域通过了身份验证，但未对应用身份验证策略中配置的任何身份验证领域进行身份验证。
NO_PASSWORD	用户身份验证失败。
PASSTHRU_ADMIN	Web 代理基于解密策略组的某些默认设置通过了事务。
PASSTHRU_ADMIN_EXPIRED_CERT	尽管服务器证书已过期，但 Web 代理通过了事务。
PASSTHRU_WEBCAT	Web 代理基于解密策略组的 URL 类别过滤设置通过了事务。
PASSTHRU_WBRS	Web 代理基于解密策略组的 Web 信誉过滤器设置通过了事务。
REDIRECT_CUSTOMCAT	Web 代理基于配置为“重定向”(Redirect) 的访问策略组中的自定义 URL 类别将事务重定向到了其他 URL。
SAAS_AUTH	Web 代理允许了用户访问应用，因为用户已针对应用身份验证策略中配置的身份验证领域，以透明方式通过了身份验证。
OTHER	Web 代理未完成请求，因为出现了错误，例如身份验证失败、服务器断开或客户端中止。

解释访问日志扫描判定条目

访问日志文件条目汇聚并显示各个扫描引擎（例如，URL 过滤、Web 信誉过滤和防恶意软件扫描）的结果。设备在每个访问日志条目末尾的尖括号中显示此信息。

以下文本是来自访问日志文件条目的扫描判定信息。在本示例中，Webroot扫描引擎发现恶意软件：

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",-,-,

IW_infr,-,"Trojan Phisher","-","Unknown","Unknown","-","-",489.73,0,-,

[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf",

"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e”,-

,ARCHIVESCAN_BLOCKEDFILETYPE,"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```

注释 有关完整访问日志文件条目的示例，请参阅访问日志文件中的 Web 代理信息，第 345 页。

如下表所示，本示例中的每个元素与一个日志文件格式说明符对应：

位置	字段值	格式说明符	说明
1	`IW_infr`	%XC	分配给事务的自定义 URL 类别，缩写。当未分配类别时，此字段显示“nc”。
2	`ns`	%XW	Web 信誉过滤器得分。当出现 DNS 查找错误时，此字段将分数显示为数字、“ns”（无得分）或“dns”。
3	`24`	%Xv	恶意软件扫描判定 Webroot 传递到 DVS 引擎。仅适用于由 Webroot 检测到的响应。 有关详细信息，请参阅恶意软件扫描判定值，第 375 页。
4	“`Trojan-Phisher-Gamec`”	“%Xn”	与对象关联的间谍软件的名称。仅适用于由 Webroot 检测到的响应。
5	`0`	%Xt	与用于确定恶意软件存在几率的威胁风险比率 (TRR) 值相关联的 Webroot 特定值。仅适用于由 Webroot 检测到的响应。
6	`354385`	%Xs	Webroot 用作威胁标识符的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Webroot 检测到的响应。

位置	字段值	格式说明符	说明
7	12559	%Xi	Webroot 用作跟踪标识符的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Webroot 检测到的响应。
8	-	%Xd	恶意软件扫描判定 McAfee 传递到 DVS 引擎。仅适用于由 McAfee 检测到的响应。 有关详细信息，请参阅恶意软件扫描判定值，第 375 页。
9	“-”	“%Xe”	McAfee 已扫描文件的名称。仅适用于由 McAfee 检测到的响应。
10	-	%Xf	McAfee 用作扫描错误的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 McAfee 检测到的响应。
11	-	%Xg	McAfee 用作检测类型的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 McAfee 检测到的响应。
12	-	%Xh	McAfee 用作病毒类型的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 McAfee 检测到的响应。
13	“-”	“%Xj”	McAfee 已扫描病毒的名称。仅适用于由 McAfee 检测到的响应。
14	-	%XY	恶意软件扫描判定 Sophos 传递到 DVS 引擎。仅适用于由 Sophos 检测到的响应。 有关详细信息，请参阅恶意软件扫描判定值，第 375 页。
15	-	%Xx	Sophos用作扫描返回代码的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Sophos 检测到的响应。
16	“-”	“%Xy”	Sophos 在其中发现不良内容的文件的名称。仅适用于由 Sophos 检测到的响应。
17	“-”	“%Xz”	Sophos用作威胁名称的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Sophos 检测到的响应。

位置	字段值	格式说明符	说明
18	-	%Xl	思科数据安全基于思科数据安全策略的“内容”(Content)列中的操作扫描判定。以下列表说明此字段的可能值： • **0.**允许 • **1.**阻止 • **-**（**连字符**）。思科数据安全过滤器没有启动扫描。当思科数据安全过滤器禁用时，或者当 URL 类别操作设置为“允许”(Allow)时，显示该值。
19	-	%Xp	基于 ICAP 响应中所给出结果的外部 DLP 扫描判定。以下列表说明此字段的可能值： • **0.**允许 • **1.**阻止 • **-**（**连字符**）。外部 DLP 服务器没有启动扫描。当外部DLP扫描禁用时，或者因“外部 DLP 策略”(External DLP Policies)>“目标”(Destinations)页面上存在免除 URL 类别而导致内容未被扫描时，显示该值。
20	`IW_infr`	%XQ	在请求端扫描期间确定的预定义 URL 类别判定，缩写。此字段列出了禁用 URL 过滤时的连字符 (-)。 有关 URL 类别缩写的列表，请参阅URL 类别说明，第 165 页。
21	-	%XA	在响应端扫描过程中由动态内容分析引擎确定的 URL 类别判定，缩写。仅适用于思科网络使用控件 URL 过滤引擎。仅当动态内容分析引擎已启用，且在请求时未分配任何类别（请求端扫描判定中列出“nc”值）时才适用。 有关 URL 类别缩写的列表，请参阅URL 类别说明，第 165 页。
22	“Trojan Phisher”	“%XZ”	统一响应端防恶意软件扫描判定，不管启用了哪个扫描引擎，均提供恶意软件类别。适用于因服务器响应扫描被阻止或监控的事务。

位置	字段值	格式说明符	说明
23	“-”	“%Xk”	Web 信誉过滤器返回的威胁类型，会导致目标网站收到欠佳的信誉。通常，对于信誉为 -4 及更低的网站填入此字段。
24	“Unknown”	“%XO”	如果适用，应用名称由 AVC 引擎返回。仅当 AVC 引擎启用时才适用。
25	“Unknown”	“%Xu”	如果适用，应用类型由 AVC 引擎返回。仅当 AVC 引擎启用时才适用。
26	“-”	“%Xb”	如果适用，应用行为由 AVC 引擎返回。仅当 AVC 引擎启用时才适用。
27	“-”	“%XS”	安全浏览扫描判定。该值表示安全搜索或网站内容评级功能应用于事务。 有关可能值的列表，请参阅记录对成人内容的访问，第 157 页。
28	489.73	%XB	为满足服务请求而消耗的平均带宽，以 Kb/sec 来表示。
29	0	%XT	用来指示请求是否因为带宽限制控制设置而被阻止的值，其中“1”表示请求被阻止，“0”表示未被阻止。
30	[Local]	%l	提交请求的用户的类型：“[本地]”(Local) 或“[远程]”(Remote)。仅当 AnyConnect 安全移动启用时才适用。当它未启用时，该值是连字符 (-)。
31	“-”	“%X3”	统一请求端防恶意软件扫描判定，不管启用了哪个扫描引擎。当出站恶意软件扫描策略适用时，应用于由于客户端请求扫描而阻止或监控的事务。
32	“-”	“%X4”	向由于适用的出站恶意软件扫描策略而被阻止或监控的客户端请求分配的威胁名称。 此威胁名称与防恶意软件扫描引擎是否已启用无关。

位置	字段值	格式说明符	说明
33	37	%X#1#	来自高级恶意软件防护文件扫描的判定： • 0：文件不是恶意的 • 1：由于其文件类型限制，文件未扫描 • 2：文件扫描超时 • 3：扫描错误 • 大于 3：文件是恶意的
34	"W32.CiscoTestVector"	%X#2#	威胁名称，根据高级恶意软件防护文件扫描来确定；“-”表示没有威胁。
35	33	%X#3#	来自高级恶意软件防护文件扫描的信誉分数。仅当云信誉服务无法确定文件的明确判定时使用此得分。 有关详细信息，请参阅此中有关威胁得分和信誉阈值的信息：文件信誉过滤和文件分析：，第 233 页
36	0	%X#4#	上传和分析请求的指示器： “0”表示高级恶意软件防护没有请求上传文件进行分析。 “1”表示高级恶意软件防护请求了上传文件以供分析。
37	"WSA-INFECTED-FILE.pdf"	%X#5#	正在下载和分析的文件的名称。
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"	%X#6#	此文件的 SHA-256 标识符。
39	-	%X#7#	来自文件的 AMP 信誉服务器的判定： • 1 - 未知 • 2 - 正常 • 3 - 恶意 • 4 - 不可扫描
40	ARCHIVESCAN_BLOCKEDFILETYPE	%X#8#	存档扫描判定。

位置	字段值	格式说明符	说明
41	"BlockedFileType: application/x-rpm, BlockedFile: allfiles/linuxpackage.rp"	%X#9#	存档扫描判定详细信息。如果基于“访问策略：自定义对象阻止”设置阻止了可检查的存档文件 (ARCHIVESCAN_BLOCKEDFILETYPE)，此“判定详细信息”条目包括阻止的文件的类型以及阻止的文件的名称。

请参阅日志文件字段和标签，第 365 页，了解每种格式说明符功能的说明。

相关主题

- 访问日志文件中的 Web 代理信息，第 345 页
- 自定义访问日志，第 361 页
- 符合 W3C 标准的访问日志文件，第 359 页
- 查看日志文件，第 344 页
- 日志文件字段和标签，第 365 页

符合 W3C 标准的访问日志文件

网络安全设备提供了两种不同的日志类型用于记录 Web 代理事务信息：访问日志和 W3C 格式化访问日志。W3C 访问日志符合万维网联盟 (W3C) 标准，以 W3C 扩展日志文件 (ELF) 格式记录事务历史记录。

- W3C 字段类型，第 359 页
- 解释 W3C 访问日志，第 359 页

W3C 字段类型

在定义 W3C 访问日志订用时，必须选择要包括哪些日志字段，例如 ACL 决策标记或客户端 IP 地址。您可以包括以下其中一种日志字段类型：

- **“预定义”(Predefined)**。Web 界面包括您可以选择的字段列表。
- **“用户定义”(User defined)**。您可键入未包括在预定义列表中的日志字段。

解释 W3C 访问日志

在解释 W3C 访问日志时，请考虑以下规则和指南：

- 管理员决定在每个 W3C 访问日志订用中记录哪些数据；因此，W3C 访问日志没有设置字段格式。
- W3C 日志是自我描述类型。文件格式（字段列表）在每个日志文件开头的报头中定义。
- W3C 访问日志中的字段用空格来分隔。
- 如果一个字段不包含任何特定条目的数据，则在日志文件中包括连字符 (-)。

- W3C 访问日志文件中的每行与一个事务相关，并且每行用 LF 序列来终止。
- W3C 日志文件标题，第 360 页
- W3C 字段前缀，第 360 页

W3C 日志文件标题

每个 W3C 日志文件在文件开头部分包含报头文本。每行均以 # 字符开头，提供有关创建日志文件的网络安全设备的信息。W3C 日志文件标题还包括文件格式（字段列表），使日志文件可自我描述。

下表介绍了每个 W3C 日志文件开头列出的标题字段。

标题字段	说明
版本 (Version)	使用的 W3C ELF 格式的版本。
日期 (Date)	标题（和日志文件）的创建日期和时间。
系统 (System)	以“Management_IP - Management_hostname”格式生成日志文件的网络安全设备。
软件 (Software)	生成这些日志的软件
字段 (Fields)	日志中记录的字段

W3C 日志文件示例：

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip
x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username
x-hierarchy-origin cs-mime-type x-acltag x-result-code x-suspect-user-agent
```

W3C 字段前缀

大多数 W3C 日志字段名称都包括前缀，用于识别值来自哪个报头，例如客户端或服务器。没有前缀的日志字段引用独立于事务所涉及的计算机的值。下表介绍了 W3C 日志字段前缀。

前缀报头	说明
c	客户端
s	服务器
cs	客户端到服务器
	服务器到客户端
x	应用特定标识符。

例如，W3C 日志字段“cs-method”是指客户端向服务器发送的请求中的方法，“c-ip”是指客户端的 IP 地址。

相关主题

- 访问日志文件中的 Web 代理信息，第 345 页.
- 自定义访问日志，第 361 页.
- 流量监控日志文件，第 364 页.
- 日志文件字段和标签，第 365 页.
- 查看日志文件，第 344 页.

自定义访问日志

您可以自定义常规和W3C访问日志以包括许多不同字段，从而使用预定义的字段或用户定义的字段来捕获有关网络内的网络流量的综合信息。

相关主题

- 有关预定义字段的列表，请参阅日志文件字段和标签，第 365 页。
- 有关用户定义字段的信息，请参阅访问日志用户定义字段，第 361 页。

访问日志用户定义字段

如果预定义访问日志和 W3C 日志字段列表不包括要从 HTTP/HTTPS 事务记录的所有报头信息，在配置访问日志和 W3C 日志订用时，可以在“自定义字段”文本框中输入用户定义的日志字段。

自定义日志字段可以是客户端或服务器发送的任何报头的任何数据。如果请求或响应不包括添加到日志订用的报头，日志文件会包括连字符，作为日志字段值。

下表定义了用于访问日志和 W3C 日志的语法：

报头类型	访问日志格式说明符语法	**W3C** 日志自定义字段语法
来自客户端应用的报头	%<*ClientHeaderName*：	cs(*ClientHeaderName*)
来自服务器的报头	%<*ServerHeaderName*：	sc(*ServerHeaderName*)

例如，如果要记录客户端请求中的 If-Modified-Since 报头值，则在“自定义字段”(Custom Fields) 框中为 W3C 日志订用输入以下文本。

```
cs(If-Modified-Since)
```

相关主题

- 自定义常规访问日志，第 362 页.

- 自定义 W3C 访问日志，第 362 页.

自定义常规访问日志

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**。

步骤 2 点击访问日志文件名来编辑访问日志订用。

步骤 3 在“自定义字段”(Custom Field) 中输入所需的格式说明符。

在“自定义字段”(Custom Field) 中输入格式说明符的语法如下：

```
<format_specifier_1> <format_specifier_2> ...
```

例如：`%a %b %E`

可以在格式说明符之前添加令牌，以在访问日志文件中显示描述性文本。例如：

```
client_IP %a body_bytes %b error_type %E
```

其中 `client_IP` 是日志格式说明符 `%a` 的说明令牌，依此类推。

注释 您可为客户端请求或服务器响应中的任何报头创建自定义字段。

步骤 4 提交并确认更改。

下一步做什么

相关主题

- 访问日志文件中的 Web 代理信息，第 345 页.
- 日志文件字段和标签，第 365 页.
- 访问日志用户定义字段，第 361 页.

自定义 W3C 访问日志

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**

步骤 2 点击 W3C 日志文件名来编辑 W3C 日志订用。

步骤 3 在“自定义字段”(Custom Field) 框中键入一个字段，然后点击**添加 (Add)**。

“所选日志字段”(Selected Log Fields) 列表中显示的字段顺序确定了 W3C 访问日志文件中的字段顺序。您也可以使用**上移 (Move Up)** 和**下移 (Move Down)** 按钮来更改字段的顺序。您可以通过在“所选日志字段”(Selected Log Fields) 列表中选择待删除的字段，然后点击**删除 (Remove)** 来删除它。

您可在“自定义字段”(Custom Fields) 框中输入多个用户定义的字段并同时添加它们，只要在点击**添加 (Add)** 之前将每个条目用新行（点击 Enter 键）来分隔。

当您更改W3C日志订用中包括的日志字段时，日志订用会自动转换。这样，最新版本的日志文件便会包含正确的新字段信头

注释　　您可为客户端请求或服务器响应中的任何报头创建自定义字段。

步骤 4 提交并确认更改。

下一步做什么

相关主题

- 符合 W3C 标准的访问日志文件，第 359 页.
- 日志文件字段和标签，第 365 页.
- 访问日志用户定义字段，第 361 页.
- 配置 CTA 特定的自定义 W3C 日志，第 363 页.
-

配置 CTA 特定的自定义 W3C 日志

开始之前

在思科 ScanCenter 中为您的 WSA 创建一个设备帐户，选择 **SCP** 作为自动上传协议（有关详细信息，请参阅《思科 *ScanCenter* 管理员指南》的“代理设备上传”部分）。请注意 SCP（安全复制协议）主机名以及为您的 WSA 生成的用户名（区分大小写，因设备而不同）。

您可以将 W3C 配置为向思科云网络安全服务“推送”感知威胁分析 (CTA) 特定的自定义 W3C 访问日志，以进行分析和报告。思科 ScanCenter 是进入云网安全 (CWS) 的管理门户。

步骤 1 按照自定义 W3C 访问日志，第 362 页中的说明添加新的 W3C 访问日志订用，选择 **W3C 日志 (W3C Logs)** 作为**日志类型(Log Type)**。

步骤 2 启用 **CTA 模板 (CTA Template)**。

启用 CTA 模板时，将自动选择并输入发送 CTA 日志所需的条件和值。如果需要，可以更改指定的默认值。当选择 CTA 模板时，检索方法默认为 SCP。

步骤 3 提供描述性的**日志名称 (Log Name)**。

步骤 4 在**用户名 (Username)** 字段中，输入在思科 ScanCenter 中为您的设备生成的用户名。设备用户名区分大小写，并且因代理设备的不同而不同。

步骤 5 选中**启用主机密钥检查 (Enable Host Key Checking)**，然后选择**自动扫描 (Automatically Scan)**。

步骤 6 查看**回滚 (Rollover)** 选项。

- **按文件大小回滚 (Rollover by File Size)**；我们推荐 500 M。
- **按时间回滚 (Rollover by Time)**：

  我们建议采用**自定义时间间隔 (Custom Time Interval)**，其**回滚间隔： (Rollover every:)** 时间间隔基于以下准则：

代理后的用户数	建议的回滚期限
未知或少于 2000	55 分钟
2000 - 4000 件	30 分钟
4000 - 6000 件	20 分钟
超过 6000 种	10 分钟

步骤 7 启用**日志压缩 (Log Compression)**。

步骤 8 点击 WSA 上的**提交 (Submit)**。

公共 SSH 密钥由 WSA 生成，并显示在管理控制台中。

步骤 9 将 WSA 生成的公共 SSH 密钥复制到剪贴板。

步骤 10 切换到思科 ScanCenter 门户，选择适当的设备帐户，然后将公用 SSH 密钥粘贴到“CTA 设备调配”页面中。（有关附加信息，请参阅《思科 *ScanCenter* 管理员指南》的“代理设备上传”部分。）

在您的代理设备与 CTA 系统之间成功进行身份验证将允许日志文件从您的代理设备上传到 CTA 系统进行分析。

思科 ScanCenter 是思科云网络安全的管理门户。请参阅http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html。

步骤 11 切换回 WSA，然后点击**提交更改 (Commit Changes)**。

注释 在提交配置更改时，WSA 将重启，因此连接的用户可能会临时断开连接。

流量监控日志文件

第 4 层流量监控日志文件提供第 4 层监控活动的详细记录。您可以查看第 4 层流量监控日志文件条目，跟踪防火墙阻止列表和防火墙允许列表的更新。

流量监控器日志说明

使用以下示例解释流量监控器日志中的各个条目类型。

示例 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.
```

在此示例中，匹配项成为阻止列表防火墙条目。第 4 层流量监控器基于通过设备的 DNS 请求将 IP 地址与阻止列表中的域名匹配。然后将 IP 地址输入了防火墙的阻止列表。

示例 2

```
172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow list.
```

在此示例中，匹配项成为允许列表防火墙条目。第 4 层流量监控器匹配了域名条目并将其添加到了设备允许列表。然后将 IP 地址输入了防火墙的允许列表。

示例 3

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

在此示例中，第 4 层流量监控器记录在内部 IP 地址与阻止列表中的外部 IP 地址之间传送的数据记录。此外，第 4 层流量监控器设置为监控，而不是阻止。

相关主题

- 查看日志文件，第 344 页

日志文件字段和标签

访问日志格式说明符和 W3C 日志文件字段

日志文件使用变量来表示构成每个日志文件条目的各个信息项。这些变量在访问日志中称为格式说明符，在 W3C 日志中称为日志字段，并且每个格式说明符有对应的日志字段。

要将访问日志配置为显示这些值，请参阅自定义访问日志，第 361 页以及添加和编辑日志订用，第 338 页中有关自定义字段的信息。

下表说明了这些变量：

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%:<1	x-p2s-first-byte-time	从 Web 代理开始连接至服务器到其首次能够写入服务器所经过的时间。如果 Web 代理必须连接到多个服务器才能完成事务，则为这些时间的总和。
%:<a	x-p2p-auth-wait-time	Web 代理发送请求后，从 Web 代理身份验证进程收到响应的等待时间。
%:<b	x-p2s-body-time	在报头之后将请求正文写入到服务器的等待时间。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%:<d	x-p2p-dns-wait-time	Web 代理将 DNS 请求发送到 Web 代理 DNS 进程所花费的时间。
%:<h	x-p2s-header-time	在第一个字节之后将请求报头写入到服务器的等待时间。
%:<r	x-p2p-reputation- wait-time	Web 代理发送请求后，从 Web 信誉过滤器收到响应的等待时间。
%:<s	x-p2p-asw-req- wait-time	Web 代理发送请求后，从 Web 代理防间谍软件进程收到判定的等待时间。
%:>1	x-s2p-first-byte-time	从服务器收到第一个响应字节的等待时间
%:>a	x-p2p-auth-svc-time	从 Web 代理身份验证进程收到响应的等待时间，包括 Web 代理发送请求所需的时间。
%:>b	x-s2p-body-time	收到报头后针对完整响应正文的等待时间
%:>c	x-p2p-fetch-time	Web 代理从磁盘缓存读取响应所需的时间。
%:>d	x-p2p-dns-svc-time	Web 代理 DNS 进程将 DNS 结果发回 Web 代理所花费的时间。
%:>h	x-s2p-header-time	在第一个响应字节后针对服务器报头的等待时间
%:>g		SSL 服务器握手延迟信息。
%:>r	x-p2p-reputation-svc- time	从 Web 信誉过滤器收到判定的等待时间，包括 Web 代理发送请求所需的时间。
%:>s	x-p2p-asw-req-svc- time	从 Web 代理防间谍软件进程收到判定的等待时间，包括 Web 代理发送请求所需的时间。
%:1<	x-c2p-first-byte-time	从新客户端连接收到第一个请求字节的等待时间。
%:1>	x-p2c-first-byte-time	向客户端写入第一个字节的等待时间。
%:A<	x-p2p-avc-svc-time	从 AVC 进程收到响应的等待时间，包括 Web 代理发送请求所需的时间。
%:A>	x-p2p-avc-wait-time	Web 代理发送请求后，从 AVC 进程收到响应的等待时间。
%:b<	x-c2p-body-time	完整客户端正文的等待时间。
%:b>	x-p2c-body-time	向客户端写入完整正文的等待时间。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%:C<	x-p2p-dca-resp- svc-time	从动态内容分析引擎收到判定的等待时间，包括 Web 代理发送请求所需的时间。
%:C>	x-p2p-dca-resp- wait-time	Web 代理发送请求后，从动态内容分析引擎收到响应的等待时间。
%:h<	x-c2p-header-time	在第一个字节后针对完整客户端报头的等待时间
%:h>	x-s2p-header-time	针对将完整报头写入客户端的等待时间
%:m<	x-p2p-mcafee-resp- svc-time	从 McAfee 扫描引擎收到判定的等待时间，包括 Web 代理发送请求所需的时间。
%:m>	x-p2p-mcafee-resp- wait-time	Web 代理发送请求后，从 McAfee 扫描引擎收到响应的等待时间。
%:p<	x-p2p-sophos-resp- svc-time	从 Sophos 扫描引擎收到判定的等待时间，包括 Web 代理发送请求所需的时间。
%:p>	x-p2p-sophos-resp- wait-time	Web 代理发送请求后，从 Sophos 扫描引擎收到响应的等待时间。
%:w<	x-p2p-webroot-resp -svc-time	从 Webroot 扫描引擎收到判定的等待时间，包括 Web 代理发送请求所需的时间。
%:w>	x-p2p-webroot-resp-wait- time	Web 代理发送请求后，从 Webroot 扫描引擎收到响应的等待时间。
%aBLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%	x-suspect-user-agent	可疑用户代理（若适用）。如果 Web 代理确定用户代理可疑，便会在此字段中记录用户代理。否则，会记录一个连字符。在访问日志中写入此字段时使用双引号。
%<Referer:	cs(Referer)	引用方
%>Server:	sc(Server)	响应中的服务器报头。
%a	c-ip	客户端 IP 地址。
%A	cs-username	经过身份验证的用户名。在访问日志中写入此字段时使用双引号。
%b	sc-body-size	从 Web 代理发送到客户端的正文内容字节数。
%B	bytes	使用的总字节数（请求大小 + 响应大小，即 %q + %s）。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%c	cs-mime-type	响应正文 MIME 类型。在访问日志中写入此字段时使用双引号。
%C	cs(Cookie)	Cookie 报头。在访问日志中写入此字段时使用双引号。
%d	s-hostname	数据源或服务器 IP 地址。
%D	x-acltag	ACL 决策标签。
%e	x-elapsed-time	已用时间（毫秒）。 对于 TCP 流量，这是从打开 HTTP 连接到关闭该连接所经过的时间。 对于 UDP 流量，这是从发送第一个数据报到最后一个数据报被接受所经过的时间。如果 UDP 流量已用时间值较大，可能表示超时值较大并且 UDP 关联允许的活动数据报等待接受的时间较长，超出了需要值。
%E	x-error-code	错误代码编号，可帮助客户支持对事务失败的原因进行故障排除。
%f	cs(X-Forwarded-For)	X-Forwarded-For 报头。
%F	c-port	客户端源端口
%g	cs-auth-group	授权组名称。在访问日志中写入此字段时使用双引号。 此字段用于对策略/身份验证问题进行故障排除，以确定用户是否匹配正确的组或策略。
%G		人类可读时间戳。
%h	sc-http-status	HTTP 响应代码。
%H	s-hierarchy	层次结构检索。
%i	x-icap-server	处理请求时最后联系的 ICAP 服务器的 IP 地址。
%I	x-transaction-id	事务 ID。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%j	DCF	不要缓存响应代码；DCF 标志。 响应代码说明： • 基于客户端请求的响应代码： • 1 = 请求拥有“无缓存”(no-cache) 报头。 • 2 = 请求没有获得缓存授权。 • 4 = 请求缺少“变体”(Variant) 报头。 • 8 = 用户请求所需的用户名或密码。 • 20 = 指定 HTTP 方法的响应。 • 基于设备收到的响应的响应代码： • 40 = 响应包含“缓存-控制：私有”(Cache-Control: private) 报头。 • 80 = 响应包含“缓存-控制：无存储”(Cache-Control: no-store) 报头。 • 100 = 响应指示请求是查询。 • 200 = 响应具有小“到期”(Expires) 值（即将到期）。 • 400 = 响应没有“最近更改”(Last Modified) 报头。 • 1000 = 响应马上过期。 • 2000 = 响应文件过大，无法缓存。 • 20000 = 文件有新副本。 • 40000 = 响应的“变化”(Vary) 报头中有错误/无效值。 • 80000 = 响应需要 cookie 设置。 • 100000 = HTTP 状态代码不可缓存。 • 200000 = 设备收到的对象不完整（基于大小）。 • 800000 = 响应尾部指示没有缓存。 • 1000000 = 响应需要重写。
%k	s-ip	数据源 IP 地址（服务器 IP 地址） 此值用于在网络上的入侵检测设备标记 IP 地址时确定请求者。允许您查找访问了已如此进行标记的 IP 地址的客户端。
%l	user-type	用户的类型，本地或远程。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%L	x-local_time	以人类可读格式请求本地时间：DD/MMM/YYYY : hh:mm:ss +nnnn。在访问日志中写入此字段时使用双引号。 启用此字段可以使日志与问题相关联，而不必根据新纪元时间计算每个日志条目的本地时间。
%m	cs-auth-mechanism	用于对身份验证问题进行故障排除。 事务使用的身份验证机制。可能的值包括： • **BASIC**。用户名使用“基本”(Basic) 身份验证方案完成身份验证。 • **NTLMSSP**。用户名使用 NTLMSSP 身份验证方案完成身份验证。 • **NEGOTIATE**。已使用 Kerberos 身份验证方案对用户名进行身份验证。 • **SSO_TUI**。用户名通过将客户端 IP 地址与使用透明用户标识完成身份验证的用户名匹配获得。 • **SSO_ISE**。用户由 ISE 服务器进行身份验证。（如果访客已被选为 ISE 身份验证的回退机制，则日志会显示访客。） • **SSO_ASA**。用户是远程用户并且用户名使用 Secure Mobility 从思科 ASA 获取。 • **FORM_AUTH**。用户访问应用时在网络浏览器的表单中输入了身份验证凭证。 • **GUEST**。用户身份验证失败，因此获得访客访问权限。
%M	CMF	缓存缺少标志：CMF 标志。
%N	s-computerName	服务器名称或目标主机名。在访问日志中写入此字段时使用双引号。
%p	s-port	目标端口号。
%P	cs-version	协议。
%q	cs-bytes	请求大小（报头 + 正文）。
%r	x-req-first-line	请求第一行 - 请求方法，URI。
%s	sc-bytes	响应大小（报头 + 正文）。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%t	timestamp	UNIX 时期中的时间戳。 注：如果要将第三方日志分析器工具用于读取和解析 W3C 访问日志，则可能需要包括“时间戳”(timestamp) 字段。大多数日志分析器只能理解采用此字段提供格式的时间。
%u	cs(User-Agent)	用户代理。在访问日志中写入此字段时使用双引号。 此字段有助于确定应用是否导致身份验证失败并且/或者需要不同的访问权限。
%U	cs-uri	请求 URI。
%v	date	YYYY-MM-DD 格式的日期。
%V	time	HH:MM:SS 格式的时间。
%w	sc-result-code	结果代码。例如：TCP_MISS、TCP_HIT。
%W	sc-result-code-denial	结果代码否决。
%x	x-latency	延迟。
%X0	x-resp-dvs-scanverdict	统一响应端防恶意软件扫描判定，不管启用了哪个扫描引擎，均提供恶意软件类别号。适用于因服务器响应扫描被阻止或监控的事务。 在访问日志中写入此字段时使用双引号。
%X1	x-resp-dvs-threat-name	统一响应端防恶意软件扫描判定，不管启用了哪个扫描引擎，均提供恶意软件威胁名称。适用于因服务器响应扫描被阻止或监控的事务。 在访问日志中写入此字段时使用双引号。
%X2	x-req-dvs-scanverdict	请求端 DVS 扫描判定
%X3	x-req-dvs-verdictname	请求端 DVS 判定名称
%X4	x-req-dvs-threat-name	请求端 DVS 威胁名称

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%X6	x-as-malware-threat-name	指示自适应扫描是否在未调用任何防恶意软件扫描引擎的情况下阻止了事务。可能的值包括： • **1.**事务被阻止。 • **0.**事务未被阻止。 此变量包含在扫描判定信息中（在每个访问日志条目末尾的尖括号内）。
%XA	x-webcat-resp-code- abbr	在响应端扫描期间确定的 URL 类别判定缩写。仅适用于思科网络使用控件 URL 过滤引擎。
%Xb	x-avc-behavior	AVC 引擎识别的 Web 应用行为。
%XB	x-avg-bw	用户的平均带宽（如果AVC引擎定义了带宽限制）。
%XC	x-webcat-code-abbr	分配给事务的自定义 URL 类别的 URL 类别缩写。
%Xd	x-mcafee-scanverdict	McAfee 特定标识符：（扫描判定）。
%Xe	x-mcafee-filename	McAfee 特定标识符：（文件名生成判定）在访问日志中写入此字段时使用双引号。
%Xf	x-mcafee-av-scanerror	McAfee 特定标识符：（扫描错误）。
%XF	x-webcat-code-full	分配给事务的 URL 类别的全称。在访问日志中写入此字段时使用双引号。
%Xg	x-mcafee-av-detecttype	McAfee 特定标识符：（检测类型）。
%XG	x-avc-reqhead-scanverdict	AVC 请求报头判定。
%Xh	x-mcafee-av-virustype	McAfee 特定标识符：（病毒类型）。
%XH	x-avc-reqbody- scanverdict	AVC 请求正文判定。
%Xi	x-webroot-trace-id	Webroot 特定扫描标识符：（跟踪 ID）
%Xj	x-mcafee-virus-name	McAfee 特定标识符：（病毒名称）。在访问日志中写入此字段时使用双引号。
%Xk	x-wbrs-threat-type	Web 信誉威胁类型。
%XK	x-wbrs-threat-reason	Web 信誉威胁原因。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%Xl	x-ids-verdict	思科数据安全策略扫描判定。如果包括此字段，它将显示 IDS 判定；如果 IDS 活跃但已扫描文档为空，则显示“0”；如果该请求未激活任何 IDS 策略，则显示“-”。
%XL	x-webcat-resp-code- full	在响应端扫描期间确定的 URL 类别判定全称。仅适用于思科网络使用控件 URL 过滤引擎。
%XM	x-avc-resphead- scanverdict	AVC 响应报头判定。
%Xn	x-webroot-threat-name	Webroot 特定标识符：（威胁名称）在访问日志中写入此字段时使用双引号。
%XN	x-avc-reqbody-scanverdict	AVC 响应正文判定。
%XO	x-avc-app	AVC 引擎识别的 Web 应用。
%Xp	x-icap-verdict	外部 DLP 服务器扫描判定。
%XP	x-acl-added-headers	无法识别的报头。使用此字段记录客户端请求中的额外报头。它支持为将报头添加到客户端请求中（作为一种验证和重定向那些请求的方式，例如，学校的 YouTube）的专门系统排除故障。
%XQ	x-webcat-req-code- abbr	在请求端扫描期间确定的预定义 URL 类别判定，缩写。
%Xr	x-result-code	扫描判定信息。
%XR	x-webcat-req-code-full	在请求端扫描期间确定的 URL 类别判定全称。
%Xs	x-webroot-spyid	Webroot 特定标识符：（侦察 ID）
%XS	x-request-rewrite	安全浏览扫描判定。 表示安全搜索或网站内容评级功能应用于事务。
%Xt	x-webroot-trr	Webroot 特定标识符：（威胁风险比率 [TRR]）。
%XT	x-bw-throttled	用于表明带宽限制是否适用于事务的标记。
%Xu	x-avc-type	AVC 引擎识别的 Web 应用类型。
%Xv	x-webroot-scanverdict	来自 Webroot 的恶意软件扫描判定。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%XV	x-request-source-ip	当为 Web 代理设置启用了“使用 X-Forwarded-For 启用客户端 IP 地址的标识”(Enable Identification of Client IP Addresses using X-Forwarded-For) 复选框时的下游 IP 地址。
%XW	x-wbrs-score	解码 WBRS 得分 <-10.0-10.0>。
%Xx	x-sophos-scanerror	Sophos 特定标识符：（扫描返回代码）。
%Xy	x-sophos-file-name	Sophos 在其中发现不良内容的文件的名称。仅适用于由 Sophos 检测到的响应。
%XY	x-sophos-scanverdict	Sophos 特定标识符：（扫描判定）。
%Xz	x-sophos-virus-name	Sophos 特定标识符：（威胁名称）。
%XZ	x-resp-dvs-verdictname	统一响应端防恶意软件扫描判定，不管启用了哪个扫描引擎，均提供恶意软件类别。适用于因服务器响应扫描被阻止或监控的事务。 在访问日志中写入此字段时使用双引号。
%X#1#	x-amp-verdict	来自高级恶意软件防护文件扫描的判定： • 0：文件不是恶意的。 • 1：由于其文件类型限制，文件未扫描。 • 2：文件扫描超时。 • 3：扫描错误。 • 大于 3：文件是恶意的。
%X#2#	x-amp-malware-name	威胁名称，如高级恶意软件保护文件扫描所确定。“-”表示没有威胁。
%X#3#	x-amp-score	来自高级恶意软件防护文件扫描的信誉分数。 仅当云信誉服务无法确定文件的明确判定时使用此得分。 有关详细信息，请参阅此中有关威胁得分和信誉阈值的信息：文件信誉过滤和文件分析：，第 233 页
%X#4#	x-amp-upload	上传和分析请求的指示器： “0”表示高级恶意软件防护没有请求上传文件进行分析。 “1”表示高级恶意软件防护请求了上传文件以供分析。

访问日志中的格式说明符	W3C 日志中的日志字段	说明
%X#5#	x-amp-filename	正在下载和分析的文件的名称。
%X#6#	x-amp-sha	此文件的 SHA-256 标识符。
%y	cs-method	方法。
%Y	cs-url	整个 URL。
不适用	x-hierarchy-origin	用于说明与哪台服务器联系以检索请求内容的代码（例如，DIRECT/www.example.com）。
不适用	x-resultcode-httpstatus	结果代码和 HTTP 响应代码，用正斜杠 (/) 分隔。
不适用	x-archivescan-verdict	显示存档检查的判定。
不适用	x-archivescan-verdict- reason	存档扫描阻止的文件的详细信息。

相关主题

- 访问日志文件中的 Web 代理信息，第 345 页.
- 解释 W3C 访问日志，第 359 页.

恶意软件扫描判定值

恶意软件扫描判定是分配给 URL 请求或服务器响应的值，用于确定其中包含恶意软件的可能性。Webroot、McAfee 和 Sophos 扫描引擎将恶意软件扫描判定返回到 DVS 引擎，以便 DVS 引擎可以确定是否监控或阻止扫描的对象。当您编辑特定访问策略的防恶意软件设置时，每个恶意软件扫描判定对应于“访问策略”(Access Policies) >“信誉和防恶意软件设置”(Reputation and Anti-Malware Settings) 页面上列出的一个恶意软件类别。

下表列出了不同的恶意软件扫描判定值和每个相应的恶意软件类别：

恶意软件扫描判定值	恶意软件类别
-	未设置
0	未知
1	未扫描
2	Timeout
3	Error
4	不可扫描

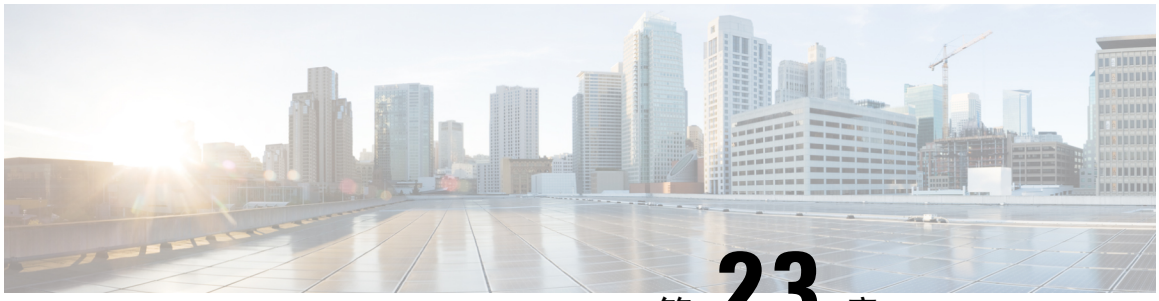
恶意软件扫描判定值	恶意软件类别
10	常规间谍软件
12	浏览器助手对象
13	广告软件
14	系统监视程序
18	商业系统监视程序
19	拨号程序
20	劫持程序
21	网络钓鱼 URL
22	特洛伊木马下载程序
23	特洛伊木马
24	特洛伊木马钓鱼程序
25	蠕虫
26	加密文件
27	病毒
33	其他恶意软件
34	PUA
35	已中止
36	病毒爆发启发式扫描
37	已知的恶意和高风险文件

相关主题

- 访问日志文件中的 Web 代理信息，第 345 页.
- 解释 W3C 访问日志，第 359 页.

日志记录故障排除

- 自定义 URL 类别不显示在访问日志条目中，第 438 页



第 23 章

执行系统管理任务

本章包含以下部分：

系统管理概述

S 系列设备提供各种用于管理系统的工具。“系统管理”(System Administration) 选项卡上的“功能”(Functionality) 可帮助您管理以下任务：

- 设备配置
- 功能密钥
- 添加、编辑和删除用户帐户
- AsyncOS 软件升级和更新

- 系统时间

保存、加载和重置设备配置

网络安全设备中的所有配置设置均使用同一个 XML 配置文件来管理。

- 查看和打印设备配置， 第 380 页
- 保存设备配置文件， 第 380 页
- 加载设备配置文件， 第 381 页
- 将设备配置重置为出厂默认设置， 第 381 页

查看和打印设备配置

步骤 1 依次选择**系统管理 (System Administration) > 配置摘要 (Configuration Summary)**。

步骤 2 根据需要查看或打印“配置摘要”(Configuration Summary) 页面。

保存设备配置文件

步骤 1 依次选择**系统管理 (System Administration) > 配置文件 (Configuration File)**。

步骤 2 完成“配置文件”(Configuration File) 选项。

选项	说明
指定文件处理选项	选择对生成的配置文件的处理方式： • 下载文件到本地的计算机,用于查看或保存. • **将文件保存到此设备 (Save file to this appliance)** (wsa_example.com)。 • **通过邮件发送文件至 (Email file to)** - 提供一个或多个邮件地址。
指定密码处理选项	• **在配置文件中屏蔽密码 (Mask passphrases in the Configuration Files)** - 在导出或保存的文件中，将原始密码替换为“*****”。请注意，含屏蔽密码的配置文件无法直接加载回 AsyncOS for Web。 • **在配置文件中加密密码 (Encrypt passphrases in the Configuration Files)** - 仅当 FIPS 模式已启用时，此选项才可用。有关启用 FIPS 模式的信息，请参阅启用或禁用 FIPS 模式， 第 403 页。
选择文件命令选项	选择配置文件的命名方式： • **使用系统生成的文件名 (Use system-generated file name)** • **使用用户定义的文件名 (Use user-defined file name)**

步骤 3 点击**提交 (Submit)**。

加载设备配置文件

注意 加载配置将永久删除所有当前配置设置。强烈建议您在执行这些操作之前保存配置。

不建议从以前的版本加载配置到最新版本。可以通过升级路径保留配置设置。

注释 如果兼容的配置文件基于比当前安装于设备上的版本更早的URL类别集版本，则可以自动修改配置文件中的策略和身份。

步骤 1 依次选择**系统管理 (System Administration) > 配置文件 (Configuration File)**。

步骤 2 选择“加载配置”(Load Configuration) 选项和要上传的文件。注意：

注释

- 无法加载含屏蔽密码的文件。
- 文件必须包含以下报头：

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

  以及一个采用正确格式的配置部分：

  `<config>` *...your configuration information in valid XML* `</config>`

步骤 3 点击**加载 (Load)**。

步骤 4 阅读显示的警告。如果您了解继续操作的后果，请点击**继续 (Continue)**。

将设备配置重置为出厂默认设置

重置设备配置时，您可以选择是否保留现有网络设置。

此操作不需要进行确认。

开始之前

将配置保存到设备外的位置。

步骤 1 依次选择**系统管理 (System Administration) > 配置文件 (Configuration File)**。

步骤 2 向下滚动以查看**重复配置 (Reset Configuration)** 部分。

步骤 3 阅读页面上的信息，并选择选项。

步骤 4 点击**重置 (Reset)**。

使用功能密钥

功能密钥在 system.Keys 中启用特定功能，是特定于设备序列号的密钥（您无法在系统间重复使用该类密钥）。

- 显示和更新功能密钥，第 382 页
- 更改功能密钥更新设置，第 382 页

显示和更新功能密钥

步骤 1 依次选择**系统管理 (System Administration) > 功能密钥 (Feature Keys)**。

步骤 2 要刷新挂起的密钥列表，请点击**检查新密钥 (Check for New Keys)** 刷新挂起的密钥列表。

步骤 3 要手动添加新功能密钥，请将该密钥粘贴或键入到“功能密钥”(Feature Key) 字段，然后点击**提交密钥 (Submit Key)**。如果该功能密钥有效，则会被添加到显示中。

步骤 4 要从“待激活”(Pending Activation) 列表中激活新功能密钥，请选中其“选择”(Select) 复选框，然后点击**激活选定的密钥 (Activate Selected Keys)**。

可以将设备配置为在发放新密钥时自动下载并安装。在这种情况下，“待激活”(Pending Activation) 列表将始终为空。您可以随时通过点击**检查新密钥 (Check for New Keys)** 按钮告知 AsyncOS 查找新密钥，即使您已通过“功能密钥设置”(Feature Key Settings) 页面禁用自动检查也是如此。

更改功能密钥更新设置

“功能密钥设置”(Feature Key Settings) 页面用于控制您的设备是否检查并下载新密钥，以及是否自动激活这些密钥。

步骤 1 依次选择**系统管理 (System Administration) > 功能密钥设置 (Feature Key Settings)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 根据需要更改功能密钥设置。

选项	说明
功能密钥的自动服务 (Automatic Serving of Feature Keys)	用于自动检查并下载功能密钥和自动激活已下载功能密钥的选项。 自动检查通常每月执行一次，但当功能密钥不足 10 天就要到期，则更改为一天检查一次，密钥过期后长达一个月内，仍是每天检查一次。一个月后，即将过期/已过期密钥列表中将不再包含这个过期的密钥。

步骤 4 提交并确认更改。

虚拟设备许可证

思科网络安全虚拟设备需要额外许可证，才能在主机中运行该虚拟设备。

有关虚拟设备许可的详细信息，请参阅以下位置中的《思科内容安全虚拟设备安装指南》：
http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html。

注释 安装虚拟设备许可证之后，才能打开“技术支持”隧道。

许可证到期后，设备将继续作为 Web 代理，但不提供 180 天的安全服务。在此期间，不会进行安全服务更新。

您可以配置设备，以便接收有关许可证到期的警报。

相关主题

- 管理警报，第 392 页

安装虚拟设备许可证

请参阅可从以下位置获取的《思科内容安全虚拟设备安装指南》：
http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html。

启用远程电源循环

开始之前

- 使用线缆将专用的远程电源循环 (RPC) 端口直接连接到安全网络。有关信息，请参阅相关设备型号的硬件指南。有关此文档的位置，请参阅文档集，第 475 页。
- 确保设备可以远程访问；例如，通过防火墙打开任何必要的端口。
- 此功能需要专用的远程电源循环接口使用唯一的 IPv4 地址。此接口仅可按照本节所述的过程配置，而不能使用 ipconfig 命令配置。
- 要循环设置设备电源，需要使用可管理设备（这些设备支持智能平台管理接口 (IPMI) 版本 2.0）的第三方工具。确保您已准备好使用这些工具。
- 有关访问命令行界面的详细信息，请参阅 。命令行界面，第 453 页

只有在 80 系列硬件上，才能远程重置设备机箱的电源。

如果您希望能够远程重置设备电源，必须事先按照本节所述的过程启用和配置此功能。

步骤 1 使用 SSH 或串行控制台端口访问命令行界面。

步骤 2 使用具有“管理员 (Administrator)”访问权限的帐户登录。

步骤 3 输入以下命令：

```
remotepower

setup
```

步骤 4 按照提示指定以下信息：

- 此功能的专用 IP 地址，以及网络掩码和网关。
- 执行电源循环命令所需的用户名和密码。

  这些凭证与用来访问设备的其他凭证不同。

步骤 5 输入 `commit` 保存更改。

步骤 6 测试您的配置，以确定是否可以远程管理设备电源。

步骤 7 确保您输入的凭证可供您无限期使用。例如，将此信息存储在安全位置，并确保可能需要执行此任务的管理员可访问所需的凭证。

下一步做什么

相关主题

- 硬件设备：远程重置设备电源， 第 445 页

管理用户帐户

以下用户类型可以登录设备来管理设备：

- **本地用户**。可以在设备本地定义用户。
- **外部系统中定义的用户**。可以将设备配置为连接到外部 LDAP 或 RADIUS 服务器，来对登录设备的用户进行身份验证。

注释 您定义的所有用户均可使用任意方法（如登录 Web 界面或使用 SSH）登录设备。

相关主题

- 管理本地用户帐户， 第 385 页
- RADIUS 用户身份验证， 第 387 页
- 通过 LDAP 服务器配置外部身份验证， 第 86 页

管理本地用户帐户

您可以在网络安全设备本地定义任意数量的用户。

默认系统管理员账户拥有所有管理权限。您可以更改管理员账户密码，但不能编辑或删除此账户。

注释 如果管理员用户密码丢失，请联系思科支持提供商。

添加本地用户帐户

开始之前

定义所有用户帐户必须遵循的密码要求。请参阅设置管理用户的密码要求，第 389 页。

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 点击**添加用户 (Add User)**。

步骤 3 输入用户名，注意以下规则：

- 用户名可以包含小写字母、数字和短划线 (-) 字符，但不能以短划线开头。
- 用户名不能大于 16 个字符。
- 用户名不能是系统保留的专用名称，例如“operator”或“root”。
- 如果您还使用外部身份验证，则用户名不应与进行外部身份验证的用户名重复。

步骤 4 为用户输入完整名称。

步骤 5 选择用户类型。

用户类型	说明
管理员	允许对所有系统配置设置进行完全访问。但是 `upgradecheck` 和 `upgradeinstall` CLI 命令只能从系统定义的“管理员”帐户发出。
操作员	限制用户创建、编辑或删除用户帐户。操作员组还限制使用以下 CLI 命令： • `resetconfig` • `upgradecheck` • `upgradeinstall` 操作员组还限制使用系统设置向导。

用户类型	说明
只读操作员	具有此角色的用户帐户： • 可以查看配置信息。 • 可以进行更改并提交更改以了解如何配置功能，但无法确认更改。 • 无法对设备进行任何其他更改，例如清除缓存或保存文件。 • 无法访问文件系统、FTP 或 SCP。
访客	访客组用户只能查看系统状态信息，包括报告和跟踪。

步骤 6 输入或生成密码。

步骤 7 提交并确认更改。

删除用户帐户

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 点击与所列的用户名对应垃圾桶图标并在出现提示时确认。

步骤 3 提交并确认更改。

编辑用户帐户

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 点击用户名。

步骤 3 根据需要在“编辑用户”(Edit User) 页面上对用户进行更改。

步骤 4 提交并确认更改。

更改密码

要更改当前登录帐户的密码，请从窗口右上方依次选择“**选项**”**(Options) >** “**更改密码**”**(Change Passphrase)**。

对于其他帐户，请在“本地用户设置”(Local User Settings) 页面上编辑帐户并更改密码。

相关主题

- 编辑用户帐户， 第 386 页
- 设置管理用户的密码要求， 第 389 页

RADIUS 用户身份验证

网络安全设备可以使用 RADIUS 目录服务对使用 HTTP、HTTPS、SSH 和 FTP 登录设备的用户进行身份验证。可以使用 PAP 或 CHAP 身份验证，将设备配置为联系多个外部服务器来执行身份验证。您可以将外部用户组映射到不同的网络安全设备用户角色类型。

Radius 身份验证的事件序列

当启用外部身份验证并且用户登录网络安全设备时，设备：

1. 确定用户是否是系统定义的“管理员”帐户。
2. 如果不是，则检查配置的第一个外部服务器，确定该用户是否在该服务器定义。
3. 如果设备无法连接到第一个外部服务器，则会检查列表中的下一个外部服务器。
4. 如果设备无法连接到任何外部服务器，则会尝试将该用户作为在网络安全设备上定义的本地用户来进行身份验证。
5. 如果用户不存在于任何外部服务器或设备上，或者如果用户输入错误的密码，则对该设备的访问将被拒绝。

使用 RADIUS 启用外部身份验证

步骤 1 在**系统管理 (System Administration) > 用户 (Users)** 页面上，点击**启用外部身份验证 (Enable External Authentication)**。

步骤 2 选择 **RADIUS** 作为身份验证类型。

步骤 3 输入 RADIUS 服务器的主机名、端口号和共享密钥密码。默认端口为 `1812`。

步骤 4 输入超时之前设备等待服务器响应的秒数。

步骤 5 选择 RADIUS 服务器使用的身份验证协议。

步骤 6 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。为每个 RADIUS 服务器重复**步骤 1 - 5**。

注释 最多可以添加十个 DNS 服务器。

步骤 7 在**外部身份验证缓存超时 (External Authentication Cache Timeout)** 字段中，输入再次联系 RADIUS 服务器重新进行身份验证前 AsyncOS 存储外部身份验证凭证的秒数。默认值为零。

注释 如果 RADIUS 服务器使用一次性密码（例如基于令牌创建的密码），请输入零 (0)。如果该值设置为零，在当前会话期间，AsyncOS 不会再次联系 RADIUS 服务器进行身份验证。

步骤 8 配置组映射 - 选择是否将所有外部身份验证用户映射至管理员角色或不同设备 - 用户角色类型。

设置	说明
将通过外部身份验证的用户映射到多个本地角色。	输入组名称（如 RADIUS CLASS 属性中所定义），并选择设备角色类型。您可以通过点击“添加行”(Add Row) 添加更多角色映射。 AsyncOS 将基于 RADIUS“类 (CLASS)”属性向设备角色分配 RADIUS 用户。CLASS 属性要求： • 至少三个字符 • 最多 253 个字符 • 不含冒号、逗号或换行符 • 每个 RADIUS 用户有一个或多个映射的“类 (CLASS)”属性（有了此设置，AsyncOS 可拒绝访问没有映射“类 (CLASS)”属性的 RADIUS 用户。） 对于具有多个“类 (CLASS)”属性的 RADIUS 用户，AsyncOS 将分配限制性最高的角色。例如，如果 RADIUS 用户具有两个 RADIUS 属性，分别映射到“操作员”(Operator) 和“只读操作员”(Read-Only Operator) 角色，则 AsyncOS 会将 RADIUS 用户分配到“只读操作员”(Read-Only Operator) 角色，因为该角色的限制比操作员角色更严格。 这些是从最严格到最不严格进行排序的设备角色： • 管理员 • 操作员 • 只读操作员 • 访客
将所有外部身份验证的用户映射为管理员角色。	AsyncOS 将所有 RADIUS 用户分配给“管理员”(Administrator) 角色。

步骤 9 提交并确认更改。

下一步做什么

相关主题

- 外部身份验证， 第 86 页
- 添加本地用户帐户， 第 385 页.

定义用户首选项

系统为每个用户存储首选项设置（如报告显示格式），无论用户从哪个客户端计算机登录设备，这些设置保持不变。

步骤 1 依次选择**选项 (Options) > 首选项 (Preferences)**。

步骤 2 在“用户首选项”(User Preferences) 页面上，点击**编辑首选项 (Edit Preferences)**。

步骤 3 根据需要配置首选项设置。

首选项设置	说明
语言显示 (Language Display)	AsyncOS for Web 在 Web 界面和 CLI 中使用的语言。
登录页 (Landing Page)	用户登录到设备后显示的页面。
显示的报告时间范围 (Reporting Time Range Displayed)（默认）	“报告 (Reporting)”选项卡上为报告显示的默认时间范围。
显示的报告行数 (Number of Reporting Rows Displayed)	默认情况下为每份报告显示的数据行数。

步骤 4 提交并确认更改。

配置管理员设置

设置管理用户的密码要求

要为设备本地定义的管理用户设置密码要求，请执行以下操作：

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 在**密码设置 (Password Settings)** 部分中，点击**编辑设置 (Edit Settings)**。

步骤 3 选择选项：

选项	说明
不允许在口令中使用的单词列表	创建一个 .txt 文件，每个被禁止的单词单独一行，然后选择要上传的文件。后续上传会覆盖之前的上传。

选项	说明
口令长度	当管理员用户输入新密码时，可以显示密码强度指示器。 此设置不强制创建强密码，只显示猜测所输入的密码的难易程度。 选择要为其显示指示器的角色。然后，对于每个所选的角色，输入一个大于0的数字。数字越大，意味着注册为强密码的密码越难破解。此设置没有最大值，但是非常高的数值会导致实际上无法输入评估为“良好”的密码。 进行试验以了解最符合您的要求的数值。 密码强度是按对数衡量的。根据美国国家标准与技术研究院在 NIST SP 800-63 中定义的熵值规则（附录 A）进行评估。 通常，高强度密码具有以下特征： • 长度较长 • 包括大写、小写、数字和特殊字符 • 不含任何语言的任何词典中的单词。 要实施具有上述这些特征的密码，请使用此页面中的其他设置。

步骤 4 提交并确认更改。

用于访问设备的其他安全设置

可以使用 CLI 命令 `adminaccessconfig` 配置网络安全设备对登录设备的管理员采用更严格的访问权限要求。

命令	说明
`adminaccessconfig > banner`	将设备配置为在管理员尝试登录时显示指定的任何文本。当管理员通过任何接口（例如通过网络用户接口、CLI 或 FTP）访问设备时，系统会显示自定义登录横幅。 您可以通过将自定义文本粘贴到 CLI 提示或从位于网络安全设备上的文本文件复制自定义文本，来加载该自定义文本。要从文件上传文本，您必须先使用 FTP 将文件传输到设备上的配置目录中。
`adminaccessconfig > welcome`	此横幅将在管理员成功登录后显示。此文本会以与登录 `adminaccessconfig > banner` 文本相同的方式添加到设备配置。

命令	说明
`adminaccessconfig > ipaccess`	IP 地址管理员访问网络安全设备所使用的控件。管理员可以从任何计算机或从 IP 地址在所指定列表中的计算机访问设备。 在限制对允许列表的访问权限时，您可以指定 IP 地址、子网或 CIDR 地址。默认情况下，当您列出可以访问设备的地址时，当前计算机的 IP 地址将列为允许列表中的第一个地址。您无法从允许列表中删除当前计算机的 IP 地址。也可以通过使用 Web UI 提供此信息。请参阅用户网络接入，第 391 页。
`adminaccessconfig > csrf`	启用/禁用 Web UI 跨站点请求伪造保护，用于识别和防止恶意或伪造请求。为获得最佳安全性，建议启用 CSRF 保护。
`adminaccessconfig > hostheader`	配置在 HTTP 请求中对主机报头的使用。 默认情况下，Web UI 以 HTTP 请求中网络客户端所发送的主机报头提供响应。为提高安全性，可以将 Web UI 配置为仅以设备特定的主机名提供响应，即已为设备配置的名称（例如 `wsa_04.local`）。
`adminaccessconfig > timeout`	提供非活动超时时间间隔，即用户被注销前处于非活动状态的时间（分钟）。此值可介于 5 到 1440 分钟（24 小时）之间，默认值为 30 分钟。也可以通过使用 Web UI 提供此信息。请参阅用户网络接入，第 391 页。
`adminaccessconfig > strictssl`	对设备进行配置以便管理员可以使用更强的 SSL 密码（大于 56 位加密）登录端口 8443 上的 Web 界面。 当您将设备配置为需要更强的 SSL 密码时，更改仅适用于使用 HTTPS 访问设备以管理设备的管理员。不适用于使用 HTTPS 连接到 Web 代理的其他网络流量。

用户网络接入

可以指定用户因不活动而被 AsyncOS 注销前可登录设备的时长。还可以指定允许的用户连接类型。

会话超时适用于所有用户，包括登录 Web UI 或 CLI 的管理员。当 AsyncOS 注销用户时，用户会重定向到设备的登录页面。

注释 还可以使用 CLI `adminaccessconfig > timeout` 来设置超时值。

步骤 1 依次选择**系统管理 (System Administration)** > **网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在**会话不活动超时 (Session Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。

可以将超时间隔定义为介于 5 到 1440 分钟 （24 小时）之间的值，默认值为 30 分钟。

步骤 4 在**用户访问 (User Access)** 部分中控制用户的系统访问权限：选择**允许任何连接 (Allow Any Connection)** 或 **仅允许特定连接 (Only Allow Specific Connections)**。

如果选择**仅允许特定连接 (Only Allow Specific Connections)**，将为特定连接定义 IP 地址、IP 范围或 CIDR 范围。客户端 IP 地址以及设备 IP 地址会自动添加到 **用户访问 (User Access)** 部分。

步骤 5 提交并确认更改。

重置管理员密码

开始之前

- 如果您不知道管理员帐户的密码，请联系您的客户支持提供商进行密码重置。
- 了解密码更改会立即生效但不要求您确认更改。

任何管理员级别的用户都可以更改“管理员”用户的密码。

步骤 1 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **用户 (Users)**。

步骤 2 点击用户列表中的**管理员 (admin)** 链接。

步骤 3 选择 **更改密码 (Change the passphrase)**。

步骤 4 生成或输入新的密码。

为生成的邮件配置返回地址

您可以针对 AsyncOS 为报告生成的邮件配置返回地址。

步骤 1 依次选择**系统管理 (System Administration)** > **返回地址 (Return Addresses)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 输入显示名称、用户名和域名。

步骤 4 提交并确认更改。

管理警报

警报是包含发生在思科网络安全设备上事件相关信息的邮件通知。这些事件可以拥有从次要（信息）到重要（严重）等不同级别的重要性（严重性），并且通常与设备的特定组件或功能相关。

注释 要接收警报和邮件通知，必须配置设备用于发送邮件的 SMTP 中继主机。

警报分类和严重性

警报中包含的信息由警报分类和严重性决定。您可以指定将哪些严重性的哪些警报分类发送给任意警报收件人。

警报分类

AsyncOS 发送以下类型的警报：

- 系统
- 硬件
- 更新程序
- Web 代理
- 防恶意软件
- L4 流量监控器
- 外部 URL 类别
-

警报严重性

可以针对以下严重性发送警报：

- **严重 (Critical)**：需要立即进行处理。
- **警告 (Warning)**：问题或错误可能需要进一步监控并且可能需要立即进行处理。
- **信息 (Information)**：此设备的例行运行中生成的信息。

管理警报收件人

注释 如果在系统设置期间启用了自动支持，则默认情况下，您指定的邮件地址将接收所有严重性和类别的警报。您可以随时更改此配置。

添加和编辑警报收件人

步骤 1 依次选择**系统管理 (System Administration) > 警报 (Alerts)**。

步骤 2 点击“警报收件人”(Alert Recipients) 列表中的收件人进行编辑，或者点击**添加收件人 (Add Recipient)** 添加新收件人。

步骤 3 添加或编辑收件人的邮件地址。可以输入多个以逗号分隔的地址。

步骤 4 为每个警报类型选择要接收的警报严重性。

步骤 5 提交并确认更改。

删除警报收件人

步骤 1 依次选择**系统管理 (System Administration) > 警报 (Alerts)**。

步骤 2 点击“警报收件人”(Alert Recipient) 列表中与警报收件人对应的垃圾桶图标并确认。

步骤 3 确认您的更改。

配置警报设置

警报设置是全局设置，这意味着其影响所有警报的行为。

步骤 1 依次选择**系统管理 (System Administration) > 警报 (Alerts)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 根据需要配置警报设置。

选项	说明
用于发送警报的发件人地址 (From Address to Use When Sending Alerts)	用于发送警报的符合 RFC 2822 的“报头来源：”(Header From:) 地址。提供的选项可以基于系统主机名（“alert@<hostname>”）自动生成地址
发送重复警报前等待 (Wait Before Sending a Duplicate Alert)	指定重复警报的时间间隔。具有两种设置： **发送重复警报前等待的初始秒数 (Initial Number of Seconds to Wait Before Sending a Duplicate Alert)**。如果将此值设置为 0，则不会发送重复警报摘要，而是发送所有重复警报，无任何延迟（这会在短时间内产生大量邮件）。发送每个警报后，发送重复警报之间等待的秒数（警报间隔）将增加。增加值是等待的秒数加上最后间隔的两倍。因此，如果等待 5 秒，警报发送时间将是 5 秒、15 秒、35 秒、75 秒、155 秒、315 秒，以此类推。 **发送重复警报前等待的最大秒数 (Maximum Number of Seconds to Wait Before Sending a Duplicate Alert)**。您可以通过“发送重复警报前等待的最大秒数”(Maximum Number of Seconds to Wait Before Sending a Duplicate Alert) 字段设置间隔之间等待秒数上限。例如，如果将初始值设置为 5 秒，最大值设置为 60 秒，则警报发送间隔将为 5 秒、15 秒、35 秒、60 秒、120 秒等

选项	说明
思科自动支持 (Cisco AutoSupport)	指定是否向思科发送以下支持信息： • 系统生成的所有警报消息的副本。 • 记录系统正常运行时间、status 命令的输出以及所用的 AsyncOS 版本的周报告。 还指定是否将发送给思科的每封邮件的副本发送给内部警报收件人。这仅适用于设置为接收严重性为“信息”(Information) 级别的系统警报的收件人。

步骤 4 提交并确认更改。

警报列表

以下各部分按照分类列出警报。每个部分中的表格包括警报名称（内部使用的描述符）、警报的实际文本、说明、严重性（严重、信息或警告）以及消息文本中包含的参数（如有）。

功能密钥警报

下表包含可通过 AsyncOS 生成的各种功能密钥警报的列表，包括对警报和警报严重性的说明：

消息	警报严重性	参数
“$feature”密钥从关键服务器下载并放置到待定区域。需要接受 EULA。(A “$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required.)	信息。	**$feature**：功能的名称。
“$feature”评估密钥已过期。请与您的授权服务代表联系。(Your "$feature" evaluation key has expired. Please contact your authorized sales representative.)	警告。	**$feature**：功能名称。
“$feature”评估密钥将在 $days 天内到期。请与您的授权服务代表联系。(Your "$feature" evaluation key will expire in under $days day[s]. Please contact your authorized sales representative.)	警告。	**$feature**：功能的名称。 **$days**：功能密钥到期之前将经过的天数。

硬件风险通告

下表包含可通过 AsyncOS 生成的各种硬件警报的列表，包括对警报和警报严重性的说明：

消息	警报严重性	参数
发生 RAID 事件： $error (A RAID-event has occurred: $error)	警告	**$error**：RAID 错误的文本。

记录警报

下表包含可通过 AsyncOS 生成的各种日志记录警报的列表，包括对警报和警报严重性的说明：

消息	警报严重性	参数
$error.	信息。	**$error**：错误的回溯字符串。
日志错误：订用 $name：日志分区已满。(Log Error: Subscription $name: Log partition is full.)	严重。	**$name**：日志订用名称。
日志错误：订用 $name 推送错误：无法连接到 $ip：$reason。(Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.)	严重。	**$name**：日志订用名称。 **$ip**：远程主机的 IP 地址。 **$reason**：描述连接错误的文本
日志错误：订用 $name 推送错误：$ip 的 FTP 命令失败：$reason。(Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.)	严重。	**$name**：日志订用名称。 **$ip**：远程主机的 IP 地址。 **$reason**：描述错误的文本。
日志错误：订用 $name 推送错误：SCP 传输到 $ip:$port 失败：$reason'，(Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',)	严重。	**$name**：日志订用名称。 **$ip**：远程主机的 IP 地址。 **$port**：远程主机上的端口号。 **$reason**：描述哪里出错的文本。
日志错误：'订用 $name：无法连接到 $hostname ($ip)：$error。(Log Error: 'Subscription $name: Failed to connect to $hostname [$ip]: $error.)	严重。	**$name**：日志订用名称。 **$hostname**：系统日志服务器的主机名。 **$ip**：系统日志服务器的 IP 地址。 **$error**：错误消息文本。
日志错误：订用 $name：将日志数据发送到系统日志服务器 $hostname ($ip) 时发生网络错误：$error (Log Error: Subscription $name: Network error while sending log data to syslog server $hostname [$ip]: $error)	严重。	**$name**：日志订用名称。 **$hostname**：系统日志服务器的主机名。 **$ip**：系统日志服务器的 IP 地址。 **$error**：错误消息文本。

消息	警报严重性	参数
订用 $name：将数据发送到系统日志服务器 $hostname ($ip) $timeout 秒后超时。(Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname [$ip].)	严重。	**$name**：日志订用名称。 **$timeout**：超时（秒）。 **$hostname**：系统日志服务器主机名。 **$ip**：系统日志服务器的 IP 地址。
订用 $name：系统日志服务器 $hostname ($ip) 接受数据的速度不够快。(Subscription $name: Syslog server $hostname [$ip] is not accepting data fast enough.)	严重。	**$name**：日志订用名称。 **$hostname**：系统日志服务器的主机名。 **$ip**：系统日志服务器的 IP 地址。
订用 $name：已删除最早的日志文件，因为日志文件达到最大数量 $max_num_files。删除的文件包括： $files_removed。(Subscription $name: Oldest log file[s] were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.)	信息。	**$name**：日志订用名称。 **$max_num_files**：每个日志订用允许的最大文件数量。 **$files_removed**：删除的文件列表。

报告警报

下表包含可通过 AsyncOS 生成的各种报告警报的列表，包括对警报和警报严重性的说明：

消息	警报严重性	参数
报告系统无法保持生成数据的速率。生成的所有新数据都将丢失。(The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.)	严重。	不适用。
报告系统现在可以处理新数据。(The reporting system is now able to handle new data.)	信息。	不适用。
生成定期报告“$report_title”时发生故障。 应检查此订用，如果其配置详细信息不再有效，应将其删除。(A failure occurred while building periodic report ‘$report_title’. This subscription should be examined and deleted if its configuration details are no longer valid.)	严重。	**$report_title**：报告的标题。

消息	警报严重性	参数
通过邮件发送定期报告“$report_title”时发生故障。 已从调度程序中删除此订用。(A failure occurred while emailing periodic report ‘$report_title’. This subscription has been removed from the scheduler.)	严重。	**$report_title**：报告的标题。
由于日志记录磁盘空间不足，对所收集报告数据的处理功能已禁用。磁盘使用率超过 $threshold%。(Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent.)对报告事件的记录功能很快将会受到限制，并且如果不释放磁盘空间（通过删除旧日志等），报告数据可能会丢失。 一旦磁盘使用率降至 $threshold% 以下，将自动重新启动对报告数据的完全处理功能。(Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up [by removing old logs, etc]. Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.)	警告。	**$threshold**：阈值。
定期报告：生成定期报告“$report_title”时，在“$file_name”找不到预期的域规范文件。未发送报告。(PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at ‘$file_name’. No reports were sent.)	严重。	**$report_title**：报告的标题。 **$file_name**：文件的名称。
计数器组“$counter_group”不存在。(Counter group “$counter_group” does not exist.)	严重。	**$counter_group**：counter_group 的名称。
定期报告：生成定期报告“$report_title”时，域规范文件“$file_name”为空。未发送报告。	严重。	**$report_title**：报告的标题。 **$file_name**：文件的名称。
定期报告：为定期报告“$report_title”处理域规范文件“$file_name”时出现错误。具有任何报告问题的任何行均未发送报告。$error_text (PERIODIC REPORTS: Errors were encountered while processing the domain specification file ‘$file_name’ for the periodic report ‘$report_title’. Any line which has any reported problem had no report sent. $error_text)	严重。	**$report_title**：报告的标题。 **$file_name**：文件的名称。 **$error_text**：遇到的错误列表。

消息	警报严重性	参数
由于日志记录磁盘空间不足，对所收集报告数据的处理功能已禁用。磁盘使用率超过 $threshold%。(Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent.)对报告事件的记录功能很快将会受到限制，并且如果不释放磁盘空间（通过删除旧日志等），报告数据可能会丢失。 一旦磁盘使用率降至 $threshold% 以下，将自动重新启动对报告数据的完全处理功能。(Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up [by removing old logs, etc]. Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.)	警告。	**$threshold**：阈值。
报告系统在打开数据库时遇到严重错误。为了防止中断其他服务，应在此计算机上禁用报告。请与客户支持联系，以启用报告。 错误消息如下： $err_msg (The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg)	严重。	**$err_msg**：错误消息文本。

系统警报

下表包含可通过 AsyncOS 生成的各种系统警报的列表，包括对警报和警报严重性的说明：

消息	警报严重性	参数
启动脚本 $name 因出现以下错误而退出：$message (Startup script $name exited with error: $message)	严重。	**$name**：脚本名称。 **$message**：错误消息文本。
系统中止失败：$exit_status: $output'，(System halt failed: $exit_status: $output',)	严重。	**$exit_status**：命令的退出代码。 **$output**：命令的输出。
系统重新启动失败：$exit_status: $output (System reboot failed: $exit_status: $output)	严重。	**$exit_status**：命令的退出代码。 **$output**：命令的输出。

消息	警报严重性	参数
进程 $name 将 $dependency 作为依赖关系项列出，但该项不存在。(Process $name listed $dependency as a dependency, but it does not exist.)	严重。	**$name**：进程的名称。 **$dependency**：列出的依赖关系项的名称。
进程 $name 将 $dependency 作为依赖关系项列出，但 $dependency 不是 wait_init 进程。(Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.)	严重。	**$name**：进程的名称。 **$dependency**：列出的依赖关系项的名称。
进程 $name 将自己作为依赖关系项列出。(Process $name listed itself as a dependency.)	严重。	**$name**：进程的名称。
进程 $name 多次将 $dependency 作为依赖关系项列出。(Process $name listed $dependency as a dependency multiple times.)	严重。	**$name**：进程的名称。 **$dependency**：列出的依赖关系项的名称。
检测到依赖关系项循环：$cycle。(Dependency cycle detected: $cycle.)	严重。	**$cycle**：循环涉及的进程名称的列表。
尝试通过网络参与功能共享统计信息时发生错误。请将此跟踪信息转发给您的支持提供商： 错误：$error。(An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.)	警告。	**$error**：与异常情况关联的错误消息。
“$name”出现错误。(There is an error with “$name”.)	严重。	**$name**：生成核心文件的进程名称。
发生应用故障：“$error”(An application fault occurred: “$error”)	严重。	**$error**：错误的文本，通常为回溯文本。
设备：$appliance，用户：$username，源 IP：$ip，事件：由于 X 次登录尝试失败，帐户被锁定。(Appliance: $appliance, User: $username, Source IP: $ip, Event: Account locked due to X failed login attempts.) X 次连续登录失败后，用户 $username 被锁定。(User $username is locked after X consecutive login failures.)上次从 $ip 尝试登录。(Last login attempt was from $ip.)	信息。	**$appliance**：特定 WSA 的标识符。 **$username**：特定用户帐户的标识符。 **$ip**：尝试进行登录的 IP 地址。
技术支持：服务隧道已启用，端口 $port (Tech support: Service tunnel has been enabled, port $port)	信息。	**$port**：用于服务隧道的端口号。

消息	警报严重性	参数
技术支持：服务隧道已禁用。(Tech support: Service tunnel has been disabled.)	信息。	不适用。
• 由于 SSH DOS 攻击，位于 $ip 的主机已添加到黑名单。(The host at $ip has been added to the blacklist because of an SSH DOS attack.) • 已将 $ip 的主机永久添加到 ssh 白名单。 • 位于 $ip 的主机已从黑名单删除 (The host at $ip has been removed from the blacklist)	警告。	**$ip**：尝试进行登录的 IP 地址。 **说明：** 对于尝试通过 SSH 连接到设备，但未提供有效凭证的 IP 地址，如果两分钟内失败尝试次数大于 10 次，则将其添加到 SSH 黑名单。 如果用户从同一 IP 地址成功登录，则将该 IP 地址添加到白名单。 白名单的地址即使在黑名单中，也允许它们访问。 条目将于大约一天后自动从该黑名单删除。

更新程序警报

下表包含可通过 AsyncOS 生成的各种更新程序警报的列表，包括对警报和警报严重性的说明：

消息	警报严重性	参数
$app 应用尝试完成更新，失败 $attempts 次后，成功完成更新。这可能是由于网络配置问题或临时中断所致。(The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.)	警告。	**$app**：网络安全设备安全服务名称。 **$attempts**：尝试的次数。
更新程序至少 $threshold 无法与更新服务器通信。(The updater has been unable to communicate with the update server for at least $threshold.)	警告。	**$threshold**：阈值时间。
出现未知错误：$traceback。(Unknown error occurred: $traceback.)	严重。	**$traceback**：回溯信息。

防恶意软件警报

有关与高级恶意软件保护相关的警报的信息，请参阅确保接收有关高级恶意软件防护问题的警报，第 245 页。

FIPS 合规性

联邦信息处理标准 (FIPS) 规定所有政府机构用于保护敏感但未分类信息的加密模块要求。FIPS 有助于确保符合联邦安全和数据隐私要求。当不存在符合联邦要求的自愿性标准，则使用由国家标准与技术研究所 (NIST) 制定的 FIPS。

WSA 使用思科通用加密模块 (C3M) 在 FIPS 模式下实现 FIPS 140-2 合规性。默认情况下，FIPS 模式处于禁用状态。

相关主题

- FIPS 模式问题， 第 424 页

FIPS 证书要求

FIPS 模式要求网络安全设备上启用的所有加密服务均使用符合 FIPS 的证书。这适用于以下加密服务：

- HTTPS 代理
- 身份验证
- SaaS 的身份提供程序
- 设备管理 HTTPS 服务
- 安全 ICAP 外部 DLP 配置
- 身份服务引擎
- SSL 配置
- SSH 配置

注释 在启用 FIPS 模式前，必须为设备管理 HTTPS 服务配置符合 FIPS 的证书。不需要启用其他加密服务。

符合 FIPS 的证书必须满足以下要求：

证书	算法	签名算法	备注
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	思科建议位密钥大小为 1024，以便实现最佳解密性能并保证足够的安全性。更大的位大小将会提升安全性，但会影响解密性能。

FIPS 证书验证

启用 FIPS 模式时，设备会执行以下证书检查：

- 验证所有上传至 WSA 的证书（无论是通过 UI 还是 `certconfig` CLI 命令上传）是否严格遵守 CC 标准。不能上传在 WSA 的信任存储区中没有适当信任路径的任何证书。
- 受信任路径通过验证的证书签名；篡改所有签名者证书经过验证的 `basicConstrains` 和 `CAFlag` 集合的证书/公钥。
- 可以采用 OCSP 验证来根据吊销列表验证证书。这可以使用 `certconfig` CLI 命令进行配置。

另请参阅严格证书验证，第 406 页。

启用或禁用 FIPS 模式

开始之前

- 备份设备配置。请参阅 保存设备配置文件，第 380 页
- 确保 FIPS 模式下要使用的证书使用 FIPS 140-2 已批准公钥算法（请参阅 FIPS 证书要求，第 402 页）。

注释

- 更改 FIPS 模式会导致重新启动设备。
- 禁用 FIPS 模式时，在 FIPS 模式启用时自动符合 FIPS 标准的 SSL 和 SSH 设置不会重置为其默认值。如果要允许使用较弱的 SSH/SSL 设置的客户端连接，必须明确更改这些设置。有关其他信息，请参阅SSL 配置，第 404 页。

步骤 1 依次选择**系统管理 (System Administration) > FIPS 模式 (FIPS Mode)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用 FIPS 合规性 (Enable FIPS Compliance)** 以启用 FIPS 合规性。

选中“启用 FIPS 合规性”(Enable FIPS Compliance) 时，**启用重要敏感参数加密 (Enable encryption of Critical Sensitive Parameters (CSP)** 复选框已启用。

步骤 4 选中**启用重要敏感参数加密 (Enable encryption of Critical Sensitive Parameters (CSP)** 以启用对配置数据（例如密码、认证信息、证书、共享密钥等）的加密。

步骤 5 点击**提交 (Submit)**。

步骤 6 点击**继续 (Continue)** 允许重新启动设备。

系统日期和时间管理

设置时区

步骤 1 依次选择**系统管理 (System Administration) > 时区 (Time Zone)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择您所在的地区、国家和时区或选择 GMT 时差。

步骤 4 提交并确认更改。

将系统时钟与 NTP 服务器同步

思科建议将网络安全设备设置为通过查询网络时间协议 (NTP) 服务器来跟踪当前日期和时间，而不是在设备上手动设置时间。如果您的设备与其他设备集成，这一点尤其正确。所有集成设备应使用同一台 NTP 服务器。

步骤 1 依次选择**系统管理 (System Administration) > 时间设置 (Time Settings)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择**使用网络时间协议 (Use Network Time Protocol)** 作为计时方法。

步骤 4 输入完全限定的主机名或 NTP 服务器的 IP 地址，根据需要点击**添加行 (Add Row)** 添加服务器。

步骤 5 （可选）选择与设备网络接口类型（管理或数据）关联的路由表用于 NTP 查询。这是发起 NTP 查询的 IP 地址。

注释 仅在设备对数据和管理流量使用拆分路由的情况下此选项才可编辑。

步骤 6 提交并确认更改。

SSL 配置

为增强安全性，您可以为多个服务启用和禁用 SSL v3 和不同版本的 TLS。为实现最大程度的安全，建议为所有服务禁用 SSL v3。默认情况下，已启用所有版本的 TLS，并禁用 SSL。

注释 您还可以使用 `sslconfig` CLI 命令启用或禁用这些功能。请参阅网络安全设备 CLI 命令，第 457 页。

步骤 1 依次选择**系统管理 (System Administration) > SSL 配置 (SSL Configuration)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中相应框可为这些服务启用 SSL v3 和 TLS 1.x：

- **设备管理 Web 用户界面 (Appliance Management Web User Interface)** – 更改此设置将断开所有活动用户的连接。
- **代理服务 (Proxy Services)** - 包括 HTTPS 代理和安全客户端的凭证加密。此部分还包括：
  - **使用密码 (Cipher(s) to Use)** - 您可以输入与代理服务通信使用的其他密码套件。使用冒号 (:) 分隔各套件。要防止使用特定密码，请在该字符串前面添加一个感叹号 (!)。例如：`!EXP-DHE-RSA-DES-CBC-SHA`。

    请务必输入与您已选中的 TLS/SSL 版本相适应的套件。有关其他信息，请参阅https://www.openssl.org/docs/manmaster/man1/ciphers.html和密码列表。

    对于 AsyncOS 9.0 及更早版本，默认密码是 `DEFAULT:+kEDH`。对于 AsyncOS 9.1 和更高版本，默认密码是

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
    !AES256-SHA:DHE-RSA-AES128-SHA
    ```

    在这两种情况下，这可能会根据您选择的 ECDHE 密码更改。

    注释 但是，无论是什么版本，升级到更高版本的 AsyncOS 版本时，都不会更改默认密码。例如，当您从较早版本升级到 AsyncOS 9.1，默认密码是 `DEFAULT:+kEDH`。换言之，在升级后，您必须更新当前密码套件。思科建议更新为：

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
    !AES256-SHA:DHE-RSA-AES128-SHA
    ```

  - **禁用 TLS 压缩（推荐）(Disable TLS Compression (Recommended))** - 您可以选中此框禁用 TLS 压缩；此为最佳安全推荐。
- **安全 LDAP 服务 (Secure LDAP Services)** - 包括身份验证、外部身份验证和安全移动。
- **安全 ICAP 服务（外部 DLP) (Secure ICAP Services (External DLP))** - 选择用于保护设备与外部 DLP （防数据丢失）服务器之间的 ICAP 通信的协议。有关详细信息，请参阅配置外部 DLP 服务器，第 270 页。
- **更新服务 (Update Service)** - 选择用于设备和可用更新服务器之间的通信的协议。有关更新服务的更多信息，请参阅AsyncOS for Web 升级和更新，第 410 页。

注释 思科的更新服务器不支持 SSL v3，因此必须为思科更新服务启用 TLS 1.0 或以上版本。但是，SSL v3 仍然可以在本地更新服务器使用，因此，如果是这种配置，您必须确定该服务器支持哪个 SSL/TLS 版本。

步骤 4 点击**提交 (Submit)**。

证书管理

设备使用数字证书建立、确认和保护各种连接。“证书管理”(Certificate Management) 页面让您可以查看和更新当前的证书列表、管理受信任的根证书，以及查看阻止的证书。

相关主题

- 证书和密钥简介，第 406 页
- 证书更新，第 407 页
- 管理受信任的根证书，第 407 页
- 查看已阻止证书，第 408 页

严格证书验证

随着 AsyncOS 10.5 FIPS 模式更新的发布，所有提交的证书在上传前都要严格进行验证，以符合通用标准 (CC)。可执行 OCSP 验证以根据吊销列表验证证书。

您必须确保将有效的合适证书上传到 WSA，且在所有相关服务器上配置安全的有效证书，以便顺利与这些服务器完成 SSL 握手。

严格证书验证适用于以下证书上传：

- HTTPS 代理（“安全服务”(Security Services) > “HTTPS 代理”(HTTPS Proxy)）
- 文件分析服务器（“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation) > “文件分析高级设置”(Advanced Settings for File Analysis) > “文件分析服务器：私有云和证书授权：使用已上传的证书授权”(File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority)）
- 受信任根证书（“网络”(Network) > “证书管理”(Certificate Management)）
- 全局身份验证设置（“网络”(Network) > “身份验证”(Authentication) > “全局身份验证设置”(Global Authentication Settings)）
- SaaS 的标识提供程序（“网络”(Network) > “SaaS 的标识提供程序”(Identity Provider for SaaS)）
- 身份服务引擎（“网络”(Network) > “身份服务引擎”(Identity Services Engine)）
- 外部 DLP 服务器（“网络”(Network) > “外部 DLP 服务器”(External DLP Servers)）
- LDAP 和 安全 LDAP（“网络”(Network) > “身份验证”(Authentication) > “领域”(Realm)）

另请参阅FIPS 合规性，第 402 页。

证书和密钥简介

浏览器提示其用户进行身份验证时，该浏览器会使用安全的 HTTPS 连接将身份验证凭证发送到 Web 代理。默认情况下，网络安全设备使用附带的“思科网络安全设备演示证书”与客户端建立 HTTPS

连接。大多数浏览器将会警告用户证书无效。为防止用户查看无效的证书消息，您可以上传应用自动识别的证书和密钥对。

相关主题

- 上传或生成证书和密钥，第 408 页
- 证书签名请求，第 409 页
- 中间证书，第 409 页

管理受信任的根证书

网络安全设备随附并维护受信任根证书列表。具有受信任证书的网站无需解密。

您可以管理受信任证书列表、向其中添加证书以及在功能上将证书从列表中删除。虽然网络安全设备不会从主列表中删除证书，但它允许在证书中覆盖信任，这可在功能上从受信任列表中删除该证书。

要添加、覆盖或下载受信任的根证书，请执行以下操作：

步骤 1 依次选择**网络 (Network)** > **证书管理 (Certificate Management)**。

步骤 2 点击“证书管理”(Certificate Management) 页面上的**管理受信任根证书 (Manage Trusted Root Certificates)**。

步骤 3 要通过思科认可的列表中没有的证书颁发机构添加自定义受信任根证书，请执行以下操作：

点击**导入 (Import)**，然后浏览到所需位置，进行选择并点击**提交 (Submit)** 提交证书文件。

步骤 4 要覆盖一个或多个思科认可的证书的信任，请执行下列操作之一：

a) 选中要覆盖的各条目的**覆盖信任 (Override Trust)** 复选框。

b) 点击**提交 (Submit)**。

步骤 5 要下载特定证书的副本，请执行以下操作：

a) 点击思科受信任根证书列表中的证书名称以展开该条目。

b) 点击**下载证书 (Download Certificate)**。

证书更新

“更新”(Updates) 部分列出了设备上思科受信任根证书和黑名单捆绑包的最新更新信息。系统会定期更新这些捆绑包。

点击“证书管理”(Certificate Management) 页面上的 **立即更新 (Update Now)**，以更新存在可用更新的所有捆绑包。

查看已阻止证书

要查看思科确定为无效并已阻止的证书的列表，请执行以下操作：

点击**查看已阻止证书 (View Blocked Certificates)**。

上传或生成证书和密钥

某些 AsyncOS 功能需要证书和密钥建立、确认或保护连接，如身份服务引擎 (ISE) 和。您可以上传现有证书和密钥，也可以在配置功能时生成证书和密钥。

上传证书和密钥

上传至设备的证书必须符合以下要求：

- 必须使用 X.509 标准。
- 必须包括匹配的 PEM 格式私钥。不支持 DER 格式。

步骤 1 选择**使用上传的证书和密钥 (Use Uploaded Certificate and Key)**。

步骤 2 在**证书 (Certificate)** 字段中，点击“浏览”(Browse)；找到要上传的文件。

注释 Web 代理使用文件中的第一个证书或密钥。证书文件必须是 PEM 格式。不支持 DER 格式。

步骤 3 在**密钥 (Key)** 字段中，点击“浏览”(Browse)；找到要上传的文件。

注释 密钥长度必须为 512 位、1024 位或 2048 位。私钥文件必须是 PEM 格式。不支持 DER 格式。

步骤 4 如果密钥已加密，则选择**密钥已加密 (Key is Encrypted)**。

步骤 5 点击**上传文件 (Upload Files)**。

生成证书和密钥

步骤 1 选择**使用生成的证书和密钥 (Use Generated Certificate and Key)**。

步骤 2 点击**生成新的证书和密钥 (Generate New Certificate and Key)**。

a) 在“生成证书和密钥”(Generate Certificate and Key) 对话框中，输入必要的生成信息。

注释 您可以在“公用名”(Common Name) 字段中输入除正斜杠 (/) 以外的任何 ASCII 字符。

b) 在“生成证书和密钥”(Generate Certificate and Key) 对话框中点击**生成 (Generate)**。

当生成完成后，证书信息会显示在“证书”(Certificate) 部分，并会提供两个链接：**下载证书 (Download Certificate)** 和**下载证书签名请求 (Download Certificate Signing Request)**。此外，当您从证书颁发机构 (CA) 收到证书时，还会有一个“已签名证书”(Signed Certificate) 选项用于上传已签名证书。

步骤 3 点击**下载证书 (Download Certificate)** 下载用于上传到设备的新证书。

步骤 4 点击**下载证书签名请求 (Download Certificate Signing Request)** 下载用于传输到证书颁发机构 (CA) 以供签名的新证书文件。有关此流程的更多信息，请参阅证书签名请求，第 409 页。

a) 当 CA 返回已签名证书时，点击“证书”(Certificate) 字段的“已签名证书”(Signed Certificate) 部分中的“浏览”(Browse) 以查找已签名证书文件，然后点击“上传文件”(Upload File) 将文件上传到设备。

b) 确保 CA 的根证书显示在设备的受信任根证书列表中。否则，请进行添加。有关详细信息，请参阅管理受信任的根证书，第 407 页。

证书签名请求

网络安全设备无法为上传到设备的证书生成证书签名请求 (CSR)。因此，要为设备创建证书，您必须从其他系统发出签名请求。保存来自该系统的 PEM 格式密钥，因为稍后需将其安装到设备上。

可以使用已安装了最新版本 OpenSSL 的任何 UNIX 计算机。确保将设备主机名置于 CSR 中。有关使用 OpenSSL 生成 CSR 的相关信息，请使用位于以下位置的指南：

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

生成 CSR 后，将其提交至证书颁发机构 (CA)。CA 将返回 PEM 格式的证书。

如果您首次获得证书，则在互联网上搜索“证书颁发机构服务 SSL 服务器证书”，然后选择最符合贵组织需求的服务。按照服务说明获得 SSL 证书。

注释 也可以生成和签署自己的证书。`http://www.openssl.org` 上提供的免费软件 OpenSSL 中包含用于执行此操作的工具。

中间证书

除了根证书颁发机构 (CA) 证书验证外，AsyncOS 还支持使用中间证书验证。中间证书是由受信任根 CA 颁发然后用于创建其他证书的证书。这会创建链接信任行。例如，可从 example.com 发出证书，反过来受信任根 CA 授权 example.com 颁发证书。必须根据 example.com 的私钥以及受信任根 CA 的私钥验证 example.com 签发的证书。

服务器在 SSL 握手报文中会发送“证书链”，以使客户端（例如浏览器，在此情况下是 WSA，即 HTTPS 代理）对服务器进行身份验证。通常情况下，服务器证书由中间证书签署，而中间证书由受信任根证书签署。在握手期间，服务器证书和整个证书链都会向客户端呈现。由于根证书通常呈现在 WSA 的受信任证书存储库中，因而对证书链验证将成功。

但是，有时当服务器上的终端实体证书被更改时，不会对新链执行必要的更新。因此，在 SSL 握手期间转到服务器会仅呈现服务器证书，并且由于中间证书丢失，WSA 代理无法验证证书链。

以前的解决方案是人工干预，由 WSA 管理员将所需的中间证书上传到受信任证书存储区。现在，可以使用 CLI 命令 `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` 来启用“中间证书发现”(intermediate certificate discovery) 进程，在此进程中 WSA 会尝试消除这些情况下的手动操作。

中间证书发现程序采用一种称为“AIA 追踪”的方法：当呈现给 WSA 的是不受信任证书时，WSA 检查此证书的扩展的名称是否是“授权信息访问”(Authority Information Access)。此扩展中包括可选的 CA 签发机构 URI 字段，可查询用于签署存在问题的服务器证书的颁发机构证书。如果有，WSA 会递归查找颁发机构的证书，直到获得根 CA 证书，然后尝试再次验证证书链。

AsyncOS for Web 升级和更新

思科会定期针对 AsyncOS for Web 及其组件发布升级（新软件版本）以及更新（对当前软件版本的更改）。

升级 AsyncOS for Web 的最佳实践

- 在开始升级前，从“**系统管理**”**(System Administration)** >“**配置文件**”**(Configuration File)** 页面，或通过使用 saveconfig 命令，从网络安全设备保存 XML 配置文件。
- 保存存储在设备上的其他文件，如 PAC 文件或自定义最终用户通知页面。
- 升级时，不要在各种提示处暂停太长时间。如果 TCP 会话在下载期间超时，则升级将会失败。
- 升级完成后，将配置信息保存到 XML 文件。

相关主题

- 保存、加载和重置设备配置 ， 第 380 页

升级和更新 AsyncOS 和安全服务组件

下载和安装升级

开始之前

保存设备配置文件（请参阅保存、加载和重置设备配置 ， 第 380 页）。

注释 在一次操作中从本地服务器（而不是 Cisco 服务器）下载并升级 AsyncOS 时，升级将在下载时即时安装。升级流程开始时，系统会显示横幅 10 秒。显示此标语时，您可以在下载开始之前键入 Control-C 退出升级过程。

可以在单个操作中下载并安装，也可以在后头下载，稍后安装。

步骤 1 依次选择**系统管理 (System Administration)** > **系统升级 (System Upgrade)**。

步骤 2 点击**升级选项 (Upgrade Options)**。

选择升级选项和升级映像：

设置	说明
选择升级选项	• **下载并安装 (Download and install)** - 在单次操作中下载并安装升级。 如果您已下载安装程序，系统将提示您会覆盖现有的下载。 • **仅下载 (Download only)** - 下载升级安装程序，但不安装。 如果您已下载安装程序，系统将提示您会覆盖现有的下载。安装程序在后台下载，而不会中断服务。 在下载完成时会显示**安装 (Install)** 按钮。点击可安装之前下载的升级。
	从 **升级服务器可用升级映像文件列表 (List of available upgrade images files at upgrade server)** 中选择需要下载或者需要下载并安装的升级映像。
升级准备	• 要将当前配置的备份副本保存到设备上的**配置 (configuration)** 目录，请勾选**升级之前将当前配置保存到配置目录 (Save the current configuration to the configuration directory before upgrading)**。 • 如果已选中**保存当前配置 (Save current configuration)** 选项，您可以勾选**在配置文件中屏蔽密码 (Mask passwords in the configuration file)**，以在备份副本中屏蔽所有当前配置密码。但是，不能使用 **Load Configuration** 命令和 CLI **loadconfig** 命令加载包含屏蔽密码的配置文件。 如果已启用 FIPS 模式，您可以选择**在配置文件中加密密码 (Encrypt passphrases in the Configuration Files)**。可以重新加载这些文件。 • 如果已勾选**保存当前配置 (Save current configuration)** 选项，您可以在**邮件文件至 (Email file to)** 字段中输入一个或多个电子邮件地址。备份配置文件副本会发送至每个地址。多个地址之间用逗号分隔。

步骤 3 点击**继续 (Proceed)**。

如果您正在进行安装：

a) 请准备好在这个过程中响应提示。

b) 显示完成提示时，点击**立即重启 (Reboot Now)**。

c) 大约 10 分钟后，请再次访问设备并登录。

如果认为需要循环设置设备电源，以解决升级问题，则请在您重启后经过至少 20 分钟再执行此操作。

查看后台下载状态、取消或删除后台下载

步骤 1 依次选择**系统管理 (System Administration)** > **系统升级 (System Upgrade)**。

步骤 2 点击**升级选项 (Upgrade Options)**。

步骤 3 选择一个选项：

目标	请
查看下载状态	在页面中间查找。 如果没有正在进行的下载，且无完成的下载等待安装，则不会看到下载状态信息。
取消下载	点击页面中间的**取消下载 (Cancel Download)** 按钮。 只有正在进行下载时，才会显示此选项。
删除已下载的安装程序	点击页面中间的**删除文件 (Delete File)** 按钮。 只有下载安装程序后，才会显示此选项。

步骤 4 （可选）查看升级日志。

下一步做什么

相关主题

- 本地和远程更新服务器，第 413 页

自动和手动更新和升级查询

AsyncOS 会定期查询更新服务器的所有安全服务组件是否有新更新，但不会查询是否有新 AsyncOS 升级。要升级 AsyncOS，必须手动提示 AsyncOS 查询可用的升级。也可以手动提示 AsyncOS 查询可用的安全服务更新。有关详细信息，请参阅恢复到以前的 AsyncOS for Web 版本，第 417 页。

当 AsyncOS 查询更新服务器是否有更新或升级时，将执行以下步骤：

1. 与更新服务器联系。

   思科允许以下来源的更新服务器：

   - **思科更新服务器**。有关详细信息，请参阅从思科更新服务器更新和升级，第 414 页。
   - **本地服务器**。有关详细信息，请参阅从本地服务器升级，第 414 页。

2. 接收列出可用更新或 AsyncOS 升级版本的 XML 文件。此 XML 文件称为“清单”。
3. 下载更新或升级映像文件。

手动更新安全服务组件

默认情况下，各安全服务组件定期从思科更新服务器接收数据库表更新。但是，您可以手动更新数据库表。

注释 某些更新可以根据需要从与该功能相关的 GUI 页面获取。

提示 在更新程序日志文件中查看更新活动记录。在**系统管理 (System Administration) > 日志订用(Log Subscriptions)** 页面中订用更新程序日志文件。

注释 正在进行的更新无法中断。必须完成所有正在进行的更新，才能应用新更改。

步骤 1 依次选择**系统管理 (System Administration) > 升级和更新设置 (Upgrade and Update Settings)**。

步骤 2 点击**编辑更新设置 (Edit Update Settings)**。

步骤 3 指定更新文件的位置。

步骤 4 使用“安全服务”(Security Services) 选项卡的组件页面上的“立即开始”(Update Now) 功能键开始更新。例如，“安全服务”(Security Services) >“Web 信誉过滤器”(Web Reputation Filters) 页面。

在更新过程中，CLI 和 Web 应用界面可能会反应速度慢或不可用。

本地和远程更新服务器

默认情况下，AsyncOS 会与思科更新服务器通信，获取更新和升级映像以及 XML 清单文件。但您可以选择下载升级和更新映像以及清单文件的位置。使用本地更新服务器的映像或清单文件的原因如下：

- **您要同时升级多个设备**。您可以将升级映像下载到网络中的 Web 服务器并应用到网络中的所有设备。
- **您的防火墙设置需要思科更新服务器使用静态 IP 地址**。思科更新服务器使用动态 IP 地址。如果您具有严格的防火墙策略，可能需要为更新和 AsyncOS 升级配置静态位置。有关详细信息，请参阅为思科更新服务器配置静态地址，第 414 页。

注释 本地更新服务器不会自动接收安全服务更新，仅接收 AsyncOS 升级。在使用本地更新服务器升级 AsyncOS 后，请将更新和升级设置改回使用思科更新服务器，以保证安全服务更新重新自动执行。

从思科更新服务器更新和升级

网络安全设备可以直接连接到思科更新服务器并下载升级映像和安全服务更新。每个设备单独下载更新和升级映像。

为思科更新服务器配置静态地址

思科更新服务器使用动态 IP 地址。如果您具有严格的防火墙策略，可能需要为更新和 AsyncOS 升级配置静态位置。

步骤 1 请与思科客户支持联系，获取静态 URL 地址。

步骤 2 导航到**系统管理 (System Administration)** > **升级和更新设置 (Upgrade and Update Settings)** 页，然后点击**编辑更新设置 (Edit Update Settings)**。

步骤 3 在“编辑更新设置”(Edit Update Settings) 页面的“更新服务器（映像）”(Update Servers (images)) 部分，选择**本地更新服务器 (Local Update Servers)** 并在输入步骤 1 中接收的静态 URL 地址。

步骤 4 验证是否为“更新服务器（列表）”(Update Servers [list]) 部分选择了“思科更新服务器”(Cisco Update Servers)。

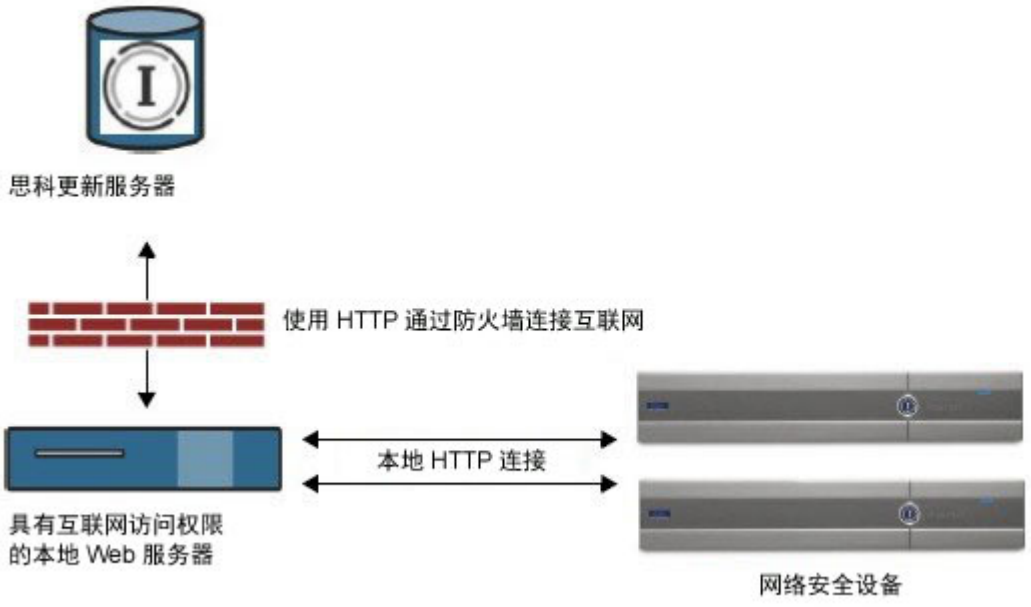
步骤 5 提交并确认更改。

从本地服务器升级

网络安全设备可以从网络中的服务器下载 AsyncOS 升级，而不是直接从思科更新服务器下载。当您使用此功能时，只能从思科下载一次升级映像，然后将其应用到网络中的所有网络安全设备。

下图显示网络安全设备如何从本地服务器下载升级映像。

图 *9:* 从本地服务器升级



本地升级服务器的硬件和软件要求

要下载 AsyncOS 升级文件，您的内部网络中必须有一个安装了 Web 浏览器并且具有思科更新服务器访问权限的系统。

注释 如果您需要将防火墙设置配置为允许通过 HTTP 访问该地址，则必须使用 DNS 名称（而不是特定 IP 地址）对其进行配置。

要托管 AsyncOS 升级文件，内部网络中的服务器必须具有 Web 服务器，例如 Microsoft IIS（互联网信息服务），或者具有以下功能的 Apache开源服务器：

- 支持显示超过 24 个字符的目录或文件名。
- 已启用目录浏览。
- 针对匿名（无身份验证）或基本（“简单”）身份验证进行配置。
- 每个 AsyncOS 升级映像至少包含 350MB 的可用磁盘空间。

从本地服务器配置升级

注释 思科建议在升级完成后，将更新和升级设置更改为使用思科更新服务器（使用动态或静态地址），以确保安全服务组件继续自动更新。

步骤 1 配置本地服务器，以检索和提供升级文件。

步骤 2 下载升级 zip 文件。

使用本地服务器上的浏览器，转到 http://updates.ironport.com/fetch_manifest.html 下载升级映像的 zip 文件。要下载映像，请输入设备的序列号（对于物理设备）或 VLN（对于虚拟设备）以及版本号。然后，系统将显示可用的升级列表。点击要下载的升级版本。

步骤 3 解压缩本地服务器上根目录中的 zip 文件，同时保持目录结构不变。

步骤 4 使用**系统管理 (System Administration) > 升级和更新设置 (Upgrade and Update Settings)** 页面或 updateconfig 命令，将设备配置为使用本地服务器。

步骤 5 在**系统管理 (System Administration) > 系统升级 (System Upgrade)** 页面上，点击**可用升级 (Available Upgrades)** 或运行 upgrade 命令。

本地和远程升级方法之间的差异

如果从本地服务器而不是从思科更新服务器升级 AsyncOS，会有以下差异：

- 下载时会立即安装升级。

- 升级过程开始时，标语将显示 10 秒。显示此标语时，您可以选择在下载开始之前键入 Control+C 以退出升级过程。

配置升级和服务更新设置

可以配置网络安全设备如何下载安全服务更新和 AsyncOS for Web 升级。例如，可以选择下载文件时使用的网络接口、配置更新间隔或禁用自动更新。

步骤 1 依次选择**系统管理 (System Administration) > 升级和更新设置 (Upgrade and Update Settings)**。

步骤 2 点击**编辑更新设置 (Edit Update Settings)**。

步骤 3 参考以下信息配置设置：

设置	说明
自动更新 (Automatic Updates)	选择是否启用安全组件的自动更新。如果选择自动更新，请输入时间间隔。默认情况下为已启用，并且更新间隔为 5 分钟。
升级通知 (Upgrade Notifications)	选择当 AsyncOS 有可用新升级时是否在 Web 界面顶部显示通知。设备仅向管理员显示此通知。 有关详细信息，请参阅AsyncOS for Web 升级和更新，第 410 页。
更新服务器（列表）(Update Servers [list])	是否从思科更新服务器或本地 Web 服务器下载可用升级和更新列表（XML 清单文件）。 如果选择本地更新服务器，请输入列表 XML 清单文件的完整路径，包括文件名和服务器的端口号。如果将端口字段留空，则 AsyncOS 将使用端口 80。如果服务器需身份验证，则也可以输入有效用户名和密码。 • 用于获取硬件设备清单的 URL 为： https://update-manifests.ironport.com • 用于获取虚拟设备清单的 URL 为： https://update-manifests.sco.cisco.com
更新服务器（映像）(Update Servers [images])	是否从思科更新服务器或本地 Web 服务器下载升级和更新映像。 如果选择本地更新服务器，请输入服务器的基本 URL 和端口号。如果将端口字段留空，则 AsyncOS 使用端口 80。如果服务器需身份验证，则也可以输入有效用户名和密码。
路由表 (Routing Table)	选择与更新服务器联系时要使用的网络接口的路由表。
代理服务器(可选) (Proxy Server (optional))	如果存在上游代理服务器并且需要身份验证，请在此处输入服务器信息以及用户名和密码。

步骤 4 提交并确认更改。

下一步做什么

相关主题

- 本地和远程更新服务器， 第 413 页
- 自动和手动更新和升级查询， 第 412 页
- 升级和更新 AsyncOS 和安全服务组件， 第 410 页

恢复到以前的 AsyncOS for Web 版本

AsyncOS for Web 支持将 AsyncOS for Web 操作系统恢复为以前合格的版本供紧急情况下使用。

注释 您不能将 AsyncOS for Web 版本恢复为 7.5 之前的版本。

恢复虚拟设备上的 AsyncOS 会影响许可证

如果您恢复到 AsyncOS 8.0，则没有 180 天的宽限期，在此期间，设备无需安全功能便能处理 Web 事务。许可证到期日期不会受到影响。

恢复过程中的配置文件使用

在有效版本 7.5 下，如果升级到更高版本，升级过程会自动将当前系统配置保存到网络安全设备上的一个文件中。（但思科建议手动将配置文件保存到本地计算机作为备份。）这样，如果将 AsyncOS for Web 恢复到更低版本，其便会加载与更低版本关联的配置文件。但在执行恢复时，其会为管理接口使用当前网络设置。

通过 SMA 为托管设备恢复 AsyncOS

可以从网络安全设备恢复 AsyncOS for Web。但如果网络安全设备由安全管理设备托管，请考虑以下规则和指南：

- 如果网络安全设备上启用了集中报告功能，AsyncOS for Web 会在开始恢复前将报告数据传输到安全管理设备。如果文件传输到安全管理设备耗时超过 40 秒，AsyncOS for Web 会提示您继续等待传输文件，或继续恢复而不传输所有文件。
- 在恢复之后，您必须将网络安全设备与相应的主配置关联。否则，将配置从安全管理设备推送到网络安全设备可能失败。

将 AsyncOS for Web 恢复到之前版本

注意 在网络安全设备上恢复操作系统是一项目极具破坏性的操作，会销毁所有配置日志和数据库。恢复还会中断 Web 流量的处理，直至重新配置设备后才能继续处理。根据初始网络安全设备配置，此操作可能会破坏网络配置。如果发生这种情况，您在执行恢复后需要通过本地物理访问方式访问设备。

注释 如果 URL 类别集合有可用更新，则系统会在 AsyncOS 恢复完成后应用这些更新.

开始之前

- 联系思科质量保证部门确认可以执行预期恢复。（BS：这是原始章节中“可用版本”一节的摘要。已咨询是否正确。）
- 从网络安全设备将以下信息备份到单独的计算机：
  - 系统配置文件（不屏蔽密码）。
  - 要保留的日志文件。
  - 要保留的报告。
  - 存储在设备上的自定义最终用户通知页面。
  - 存储在设备上的 PAC 文件。

步骤 1 登录要恢复的设备的 CLI。

注释 在下一步中运行 `revert` 命令时，系统会发出多个警告提示。接受这些警告提示后，系统会立即执行恢复操作。因此，在完成恢复前步骤之前，请勿开始恢复过程。

步骤 2 输入 `revert` 命令。

步骤 3 两次确认要继续进行恢复。

步骤 4 选择其中一个要恢复到的可用版本。

设备会重新启动两次。

注释 恢复过程比较耗时。可能需要十五到二十分钟才能完成恢复，并且可再次通过控制台访问设备。

现在，设备应使用所选的 AsyncOS for Web 版本运行。您可以从 Web 浏览器访问 Web 界面。

使用 SNMP 监控系统运行状况和状态

AsyncOS 操作系统通过 SNMP（简单网络管理协议）支持系统状态监控。（有关 SNMP 的详细信息，请参阅 RFC 1065、1066 和 1067）。

请注意：

- 默认情况下，SNMP 已**关闭**。
- 未实施 SNMP SET 操作（配置）。
- AsyncOS 支持 SNMPv1、v2 和 v3。有关 SNMPv3 的详细信息，请参阅 RFC 2571-2575。
- 当启用 SNMPv3 时，必需进行邮件身份验证和加密。用于身份验证和加密的密码应不同。加密算法可以是 AES（推荐）或 DES。身份验证算法可以是 SHA-1（推荐）或 MD5。在您下次运行 snmpconfig 命令时，该命令会“记住”您的密码。
- SNMPv3 用户名为：v3get。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- 如果仅使用 SNMPv1 或 SNMPv2，则必须设置社区字符串。社区字符串的默认值不是 `public`。
- 对于 SNMPv1 和 SNMPv2，必须指定在其中接受 SNMP GET 请求的网络。
- 要使用陷阱，SNMP 管理器（不包括在 AsyncOS 中）必须正在运行，并且其 IP 地址输入为陷阱目标。（可以使用主机名，但如果使用主机名，则仅在 DNS 工作时陷阱才有效。）

MIB 文件

可从以下地址获取 MIB 文件：
http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html。

使用每个 MIB 文件的最新版本。

有多个 MIB 文件：

- asyncoswebsecurityappliance-mib.txt - 网络安全设备的企业 MIB 文件的 SNMPv2 兼容说明。
- ASYNCOS-MAIL-MIB.txt - 邮件安全设备的企业 MIB 文件的 SNMPv2 兼容说明。
- IRONPORT-SMI.txt - 此“管理信息结构”文件定义 asyncoswebsecurityappliance-mib 的角色。

此版本可实现 RFC 1213 和 1907 中定义的 MIB-II 只读子网。

请参阅https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html了解如何使用 SNMP 监控设备上的 CPU 使用情况。

启用和配置 SNMP 监控

要将 SNMP 配置为收集设备的系统状态信息，请在命令行界面 (CLI) 中使用 snmpconfig 命令。选择并配置接口的值以后，设备会响应 SNMPv3 GET 请求。

使用 SNMP 监控时，请注意以下几点：

- 这些第 3 版请求必须包含匹配密码。
- 默认情况下，第 1 版和第 2 版请求会被拒绝。
- 如果启用，第 1 版和第 2 版请求必须具有匹配的社区字符串。

硬件对象

符合智能平台管理接口规格 (IPMI) 的硬件传感器会报告温度、风扇速度以及电源状态等信息。

要确定可监控的硬件相关对象（例如，风扇的数量或工作温度范围），请参阅您的设备型号的硬件指南。

相关主题

- 文档集，第 475 页

SNMP 陷阱

SNMP 能够发送陷阱或通知，当一个或多个条件匹配时给予管理应用建议。陷阱是网络数据包，其中包含与发送陷阱的系统组件相关的数据。当在 SNMP 代理上满足某个条件时（此情况下是思科网络设备）就会生成陷阱。在满足条件后，SNMP 代理就会形成 SNMP 数据包并将其发送到运行 SNMP 管理控制台软件的主机。

当您为接口启用 SNMP 时，可以配置 SNMP 陷阱（启用或禁用特定陷阱）。

要指定多个陷阱目标：当系统提示输入陷阱目标时，您最多可以输入 10 个用逗号分隔的 IP 地址。

相关主题

- 关于 connectivityFailure SNMP 陷阱，第 420 页

关于 connectivityFailure SNMP 陷阱

connectivityFailure 陷阱用于监控您的设备与互联网的连接。主要通过尝试连接到单台外部服务器，并每隔 5 到 7 秒向服务器发送 HTTP GET 请求来实现此陷阱。默认情况下，监控的 URL 是端口 80 上的 `downloads.ironport.com`。

要更改监控的 URL 或端口，请运行 `snmpconfig` 命令，并启用（即使已经启用）connecivityFailure 陷阱。您将看到用于更改 URL 的提示。

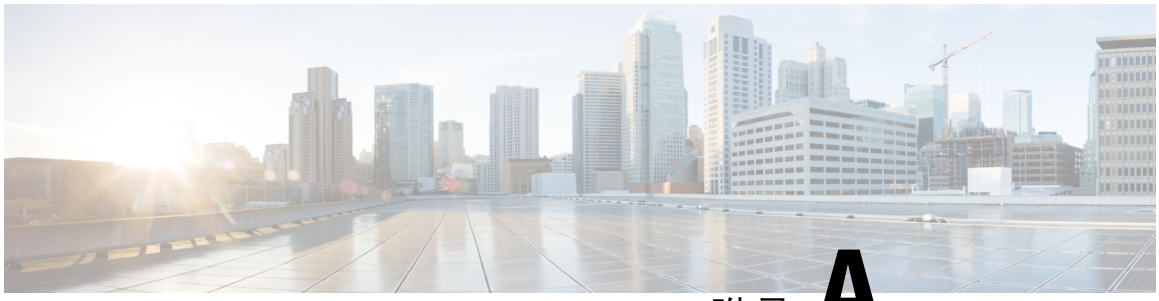
提示 要模拟 connectivityFailure 陷阱，可以使用 `dnsconfig` CLI 命令进入非工作 DNS 服务器。此时查找 downloads.ironport.com 的操作会失败，并且会每隔 5-7 秒发送陷阱报文。请务必在完成测试后将 DNS 服务器改回为工作服务器。

CLI 示例：snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
```

```
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>

Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
```

```
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

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

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```



附录 A

故障排除

本附录包含以下部分：

通用故障排除最佳实践

配置访问日志以包含下列自定义字段：

%u、%g、%m、%k、%L（这些值区分大小写。）

有关这些字段的说明，请参阅访问日志格式说明符和 W3C 日志文件字段，第 365 页。

有关配置说明，请参阅自定义访问日志，第 361 页和添加和编辑日志订用，第 338 页。

FIPS 模式问题

如果您在将 WSA 升级到 AsyncOS 10.5 且启用 FIPS 模式和 CSP 加密后遇到加密和证书问题，请参考以下主题进行检查。

CSP 加密

如果某项功能在启用 FIPS 模式 CSP 加密之前有效，但在启用加密后无效，则需确定是否存在 CSP 加密问题。禁用 CSP 加密和 FIPS 模式，然后测试此功能。如果起作用，则启用 FIPS 模式并再次测试。如果起作用，则启用 CSP 加密并再次测试。请参阅启用或禁用 FIPS 模式，第 403 页。

证书验证

在升级到 AsyncOS 10.5 前 WSA 所接受的证书在再次上传时可能会被拒绝，而不论采用何种上传方法。（即，通过诸如“HTTPS 代理”(HTTPS Proxy)、“证书管理”(Certificate Management)、“SaaS 标识提供程序”(Identity Provider for SaaS)、ISE 配置（ISE configuration）、“身份验证配置”（Authentication configuration）等 UI 页面，或通过 `certconfig` CLI 命令。）

确保在“证书管理”(Certificate Management) 页面（“网络”(Network) > “证书管理”(Certificate Management)）中，已将证书的签名者 CA 添加为“自定义受信任证书颁发机构”(Custom Trusted Certificate Authorities)。如果完整证书路径不受信任，则证书不能上传到 WSA。

此外，重新加载旧配置时，配置中包含的证书可能不受信任，导致重新加载失败。确保在加载已保存的配置时替换这些证书。

注释 所有证书验证故障都记录在审核日志 (`/data/pub/audit_logs/audit_log.current`) 中。

身份验证问题

- 另请参阅：
  - 通用故障排除最佳实践， 第 423 页
  - HTTPS 和 FTP over HTTP 请求仅匹配不需要身份验证的访问策略， 第 440 页
  - 无法访问不支持身份验证的 URL， 第 446 页
  - 上游代理的客户端请求失败， 第 447 页

排除身份验证工具故障

用于查看和清除 Kerberos 票证缓存的 KerbTray 或 klist（均是 Windows 服务器资源包的一部分）。用于查看和编辑 Active directory 的 Active Directory Explorer。Wireshark 是可用于网络故障排除的数据包分析器。

身份验证失败影响正常操作

当某些用户代理或应用没有通过身份验证或被拒绝访问时，它们会重复发送请求到网络安全设备，而后网络安全设备反复向 Active Directory 发送含计算机凭证的请求，有时这种情况甚至会影响正常的操作。

为获得最佳效果，对这些用户代理绕过身份验证。请参阅绕过有问题的用户代理的身份验证， 第 104 页。

LDAP 问题

- 由于 NTLMSSP 导致 LDAP 用户身份验证失败， 第 425 页
- 由于 LDAP 引用导致 LDAP 身份验证失败， 第 425 页

由于 NTLMSSP 导致 LDAP 用户身份验证失败

LDAP 服务器不支持 NTLMSSP。对于某些客户端应用（如 Internet Explorer），如果让其在 NTLMSSP 和基本身份验证之间选择，其始终会选择 NTLMSSP 身份验证。如果满足以下所有条件，用户的身份验证将失败：

- 用户仅存在于 LDAP 领域中。
- 标识配置文件使用同时包含 LDAP 和 NTLM 领域的序列。
- 标识配置文件使用“基本或 NTLMSSP”身份验证方案。
- 用户从选择 NTLMSSP 而不是基本身份验证的应用发送请求。

重新配置标识配置文件或身份验证领域或应用，以便上述条件中至少有一个条件不满足。

由于 LDAP 引用导致 LDAP 身份验证失败

如果满足以下所有条件，LDAP 身份验证将失败：

- LDAP 身份验证领域使用 Active Directory 服务器。
- Active Directory 服务器使用 LDAP 引用连接到其他身份验证服务器。
- 网络安全设备无法使用引用的身份验证服务器。

解决方法：

- 在设备上配置 LDAP 身份验证领域时，在 Active Directory 林中指定全局目录服务器（默认端口为 3268）。
- 可使用 `advancedproxyconfig > authentication` CLI 命令禁用 LDAP 引用。默认情况下，LDAP 引用处于禁用状态。

基本身份验证问题

- 基本身份验证失败，第 426 页

相关问题

- 上游代理未收到基本凭证，第 447 页

基本身份验证失败

使用基本身份验证方案时，AsyncOS for Web 仅支持 7 位 ASCII 字符的密码。如果密码不是 7 位 ASCII 字符，则基本身份验证会失败。

单点登录问题

- 错误地提示用户输入凭证，第 426 页

错误地提示用户输入凭证

如果网络安全设备连接到支持 WCCP v2 的设备，NTLM 身份验证在某些情况下不起作用。当用户通过不会正确执行透明 NTLM 身份验证的高度锁定 Internet Explorer 版本发出请求并且设备连接到支持 WCCP v2 的设备时，浏览器默认进行基本身份验证。这会导致系统提示用户输入身份验证凭证，而用户本不应收到这样的提示。

解决办法

在 Internet Explorer 中，将网络安全设备重定向主机名添加到“本地内联网”(Local Intranet) 区域（“工具”(Tools) > “Internet 选项”(Internet Options) > “安全性”(Security) 选项卡）的受信任站点列表中。

受阻对象问题

- 未阻止某些 Microsoft Office 文件，第 427 页

• 阻止 DOS 可执行对象类型会阻止 Windows OneCare 的更新，第 427 页

未阻止某些 Microsoft Office 文件

当您在“阻止对象类型”(Block Object Type) 部分中阻止 Microsoft Office 文件时，可能不会阻止某些 Microsoft Office 文件。

如果您需要阻止所有 Microsoft Office 文件，请在“阻止自定义 MIME 类型”(Block Custom MIME Types) 字段中添加 **application/x-ole**。但是，阻止此自定义 MIME 类型还会阻止所有 Microsoft 复合对象格式类型，例如 Visio 文件以及一些第三方应用。

阻止 DOS 可执行对象类型会阻止 Windows OneCare 的更新

当您配置网络安全设备以阻止 DOS 可执行对象类型时，设备也会阻止 Windows OneCare 的更新。

浏览器问题

• WPAD 在 Firefox 中无法正常运行，第 427 页

WPAD 在 Firefox 中无法正常运行

Firefox 浏览器可能不支持使用 WPAD 进行 DHCP 查找。有关最新信息，请参阅 https://bugzilla.mozilla.org/show_bug.cgi?id=356831。

要在 PAC 文件托管于网络安全设备时将 Firefox（或任何其他不支持 DHCP 浏览器）与 WPAD 配合使用，请将设备配置为通过端口 80 为 PAC 文件提供服务。

步骤 1 依次选择**安全服务 (Security Services) > Web 代理 (Web Proxy)**并从**代理的 HTTP 端口 (HTTP Ports to Proxy)** 字段删除端口 80。

步骤 2 将文件上传到设备时，请使用端口 80 作为 PAC 服务器端口。

步骤 3 如果任何浏览器手动配置为指向端口 80 上的 Web 代理，请在“代理的 HTTP 端口”(HTTP Ports to Proxy) 字段中将这些浏览器重新配置为指向另一端口。

步骤 4 更改 PAC 文件中对端口 80 的所有引用。

DNS 问题

• 警报：无法启动 DNS 缓存，第 428 页

警报：无法启动 DNS 缓存

如果重新启动设备时生成包含“无法启动 DNS 缓存”(Failed to bootstrap the DNS cache) 消息的警报，则表示系统无法与其主 DNS 服务器联系。如果在建立网络连接之前 DNS 子系统联机，则在启动时会出现这种情况。如果此消息出现在其他时候，则可能表示存在网络问题或DNS配置未指向有效的服务器。

故障切换问题

- 故障切换配置错误，第 428 页
- 虚拟设备上的故障切换问题，第 428 页

故障切换配置错误

故障切换组的配置错误可能导致多个主设备或其他故障切换问题。使用 CLI `failoverconfig` 命令的 `testfailovergroup` 子命令诊断故障切换问题。

例如：

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: MASTER
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

虚拟设备上的故障切换问题

对于虚拟设备上的部署，请确保您已将虚拟机监控程序上的接口/虚拟交换机配置为使用混合模式。

功能密钥过期

如果您尝试访问（通过 Web 界面）的功能的功能密钥已过期，请与您的思科代表或支持组织联系。

FTP 问题

- URL 类别不阻止某些 FTP 站点，第 429 页

- 大型 FTP 传输断开连接， 第 429 页
- 文件上传后 FTP 服务器上显示零字节文件， 第 429 页
- 在 FTP-over-HTTP 请求中 Chrome 浏览器未被检测为用户代理， 第 429 页
- 另请参阅：
  - 无法通过上游代理路由 FTP 请求， 第 447 页
  - HTTPS 和 FTP over HTTP 请求仅匹配不需要身份验证的访问策略， 第 440 页

URL 类别不阻止某些 FTP 站点

当本地 FTP 请求以透明方式重定向到 FTP 代理时，其不包含 FTP 服务器的主机名信息，仅包含其 IP 地址。因此，某些只有主机名信息的预定义 URL 类别和 Web 信誉过滤器不会与本地 FTP 请求匹配，即使请求的目标是这些服务器。如果要阻止对这些站点的访问，您必须使用其 IP 地址为它们创建自定义 URL 类别。

大型 FTP 传输断开连接

如果 FTP 代理和 FTP 服务器之间的连接速度较慢，则上传大型文件可能需要较长时间，特别是在启用思科数据安全过滤器时。这可能会导致 FTP 客户端在 FTP 代理上传整个文件之前超时，您可能会收到失败的事务通知。但是，事务并未失败，而是继续在后台进行，将由 FTP 代理完成。

您可以通过在 FTP 客户端上增加适当的空闲超时值来解决此问题。

文件上传后 FTP 服务器上显示零字节文件

当 FTP 代理因出站防恶意软件扫描而阻止上传时，FTP 客户端会在 FTP 服务器上创建一个零字节文件。

在 FTP-over-HTTP 请求中 Chrome 浏览器未被检测为用户代理

Chrome 浏览器在 FTP-over-HTTP 请求中不包括用户代理字符串，因而，在这些请求中 Chrome 浏览器不会检测为用户代理。

上传/下载速度问题

WSA 可并行处理数千个客户端和服务器连接，并且对发送和接收缓冲区的大小进行配置以提供最佳性能，而不牺牲稳定性。通常，实际使用是浏览流量，其中包括大量短暂连接，在这些连接中我们具有接收端包控制 (RPS) 和接收端流控制 (RFS) 数据，WSA 已针对这些连接进行了优化。

然而，有时您可能会遇到上传或下载速度显著降低的问题，例如，通过代理传输大文件时。为了说明这一点：假设有一条 10 Mbps 的线路，通过 WSA 下载一个 100 MB 文件比直接从其服务器下载该文件要慢约七到八倍。

在大型文件传输比重较大的非典型环境中，您可以使用 networktuning 命令增大发送和接收缓冲区大小以缓解此问题，但这也会导致网络内存耗尽并影响系统稳定性。请参阅网络安全设备 CLI 命令，第 457 页了解有关 networktuning 命令的详细信息。

注意 更改 TCP 接收和发送缓冲区控制点以及其他 TCP 缓冲区参数时请谨慎。仅在您了解后果后，再使用 networktuning 命令。

以下列出了在两个不同设备上使用 networktuning 命令的示例：

在 S380 上

```
networktuning
sendspace = 131072
recvspace = 131072
send-auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
recv-auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
mbuf clusters = 98304 * (X/Y)  where is X is RAM in GBs on the system and Y is 4GB.
sendbuf-max = 1048576
recvbuf-max = 1048576
```

问题

有哪些参数？

WSA 有多个缓冲区和优化算法，可以根据特定需要进行更改。缓冲区大小最初优化是为了适应“最常见”部署方案。但是，当需要更快的每连接性能时，可以使用更大的缓冲区大小，但请注意，总体内存使用量会增加。因此，缓冲区大小的增加应符合系统可用的内存。发送和接收空间变量控制可用于通过套接字存储的数据通信的缓冲区大小。发送和接收自动选项用于启用和禁用发送和接收 TCP 窗口大小的动态扩展。（这些参数将应用于 FreeBSD 内核。）

这些示例值是如何确定的？

我们在观察到“问题”的客户网络上测试了不同的值集，并对这些值进行了清零。之后，我们在实验室中进一步测试了这些变化带来的稳定性和性能提高情况。您可以自由使用除这些值以外的值，并自承风险。

为什么这些值不是默认值？

如上所述，默认情况下 WSA 已针对最常用部署进行优化，且在众多位置上运行，没有出现任何连接性能方面的投拆。在这里讨论的更改不会增加 RPS 的数量，并且实际上可能会使其有所下降。

硬件问题

- 重启设备，第 431 页
- 设备运行状况和状态指示灯，第 431 页
- 警报：380 或 680 硬件上的电池再记忆超时（RAID 活动），第 431 页

重启设备

重要提示！如果您需要重启 x80 或 x90 设备，请等待至少 20 分钟以便设备再次完成启动准备（所有 LED 均呈绿色亮起），然后再按电源按钮。

设备运行状况和状态指示灯

硬件设备前面板和/或后面板上的指示灯指示设备的运行状况和状态。有关这些指示灯的说明，请参阅硬件指南（例如《思科x90 系列内容安全设备的安装和维护指南》，该指南可通过以下网址获取：http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html）。

这些文档中还会介绍设备规格，例如温度范围。

警报：380 或 680 硬件上的电池再记忆超时（RAID 活动）

此警报不一定会指出问题。电池自身充放电超时并非意味着 RAID 控制器有任何问题。控制器在随后的充放电过程中可以恢复。请在未来 48 个小时监控您的邮件是否存在任何其他 RAID 警报，以确保这不是任何其他问题的负面影响。如果您在系统中没有看到任何其他 RAID 类型的警报，则您可以安全忽略此警报。

HTTPS/解密/证书问题

- 使用路由策略的 URL 类别条件访问 HTTPS 站点， 第 431 页
- HTTPS 请求失败， 第 432 页
- 对特定网站绕过解密， 第 432 页
- 针对阻止嵌入和引用内容的例外情况的条件和限制， 第 432 页
- 警报：安全证书出现问题， 第 433 页
- 另请参阅：
  - 记录 HTTPS 事务， 第 438 页
  - 无法配置 HTTPS 的访问策略， 第 439 页
  - HTTPS 和 FTP over HTTP 请求仅匹配不需要身份验证的访问策略， 第 440 页

使用路由策略的 URL 类别条件访问 HTTPS 站点

对于透明重定向的HTTPS请求，Web代理必须与目标服务器连接以确定服务器名，并因此确定其所属的 URL 类别。因此，当 Web 代理评估路由策略组成员身份时，它尚且无法知道 HTTPS 请求的 URL 类别，因为它尚未连接目标服务器。如果 Web 代理不知晓 URL 类别，就不能将透明 HTTPS 请求于使用 URL 类别作为成员资格条件的路由策略匹配。

因此，透明重定向的 HTTPS 事务仅匹配不按 URL 类别定义路由策略组成员资格条件的路由策略。如果所有用户定义的路由策略均按 URL 类别定义其成员身份，透明 HTTPS 事务会匹配默认路由策略组。

HTTPS 请求失败

具有基于 IP 的代理和透明请求的 HTTPS

如果 HTTPS 请求来自先前 HTTP 请求中没有身份验证信息的客户端，AsyncOS 会根据 HTTPS 代理的配置，让 HTTPS 请求失败或解密 HTTPS 请求以对用户进行身份验证。在“安全服务”(Security Services) >“HTTPS 代理”(HTTPS Proxy) 页面的“HTTPS 透明请求”(HTTPS Transparent Request) 设置中定义此行为。请参阅“解密策略”一章中的“启用 HTTPS 代理”一节。

对应于自定义和默认类别的不同“Client Hello”行为

扫描数据包捕获时，您可能会注意到，对于自定义类别和默认 (Web) 类别 HTTPS 解密通过策略，“Client Hello”握手报文是在不同的时间发送的。

对于经由默认类别通过的 HTTPS 页面，“Client Hello”是在收到请求者的“Client Hello”以及连接失败前发送的。对于经由自定义 URL 类别通过的 HTTPS 页面，“Client Hello”是在收到请求者的“Client Hello”以及连接成功后发送的。

为了解决此问题，可以为仅兼容 SSL 3.0 的网页创建含通过操作的自定义 URL 类别。

对特定网站绕过解密

当某些 HTTPS 服务器的流量未通过代理服务器（例如 Web 代理）解密时，这些服务器不会按预期工作。例如，某些网站及其关联的 Web 应用和小程序（例如高度安全银行站点）维护一个受信任证书硬编码列表，而不是依赖操作系统证书存储库。

您可以忽略这些服务器的 HTTPS 流量的解密，以确保所有用户可以访问这些类型的站点。

步骤 1 通过配置“高级”(Advanced) 属性，创建包含受影响 HTTPS 服务器的自定义 URL 类别。

步骤 2 创建将在步骤 1 中创建的自定义 URL 类别用作其成员身份一部分的解密策略，并将自定义 URL 类别的操作设置为“通过”(Pass Through)。

针对阻止嵌入和引用内容的例外情况的条件和限制

基于引用的例外情况仅在访问策略中受支持。要对 HTTPS 流量使用此功能，则在访问策略中定义例外之前，必须配置您将为例外选择的 URL 类别的 HTTPS 解密。但此功能在某些情况下无效：

- 如果连接采用隧道传输且未启用 HTTPS 解密，此功能对将发往 HTTPS 站点的请求不起作用。
- 根据 RFC 2616，浏览器客户端可能有一个用于控制公开/匿名浏览的切换开关，可分别启用/禁用引用和信息的发送。该功能完全依赖于引用报头，关闭发送它们会导致功能无效。

- 根据 RFC 2616，如果引用页面通过安全的协议传输，客户端在（非安全） HTTP 请求中不应包含引用报头字段。因此，从 HTTPS 站点到 HTTP 站点的所有请求不会有引用报头，导致此功能无法正常运行。
- 当设置解密策略以使得在自定义类别匹配解密策略且操作被设置为“丢弃”(Drop) 时，任何该类传入请求都被丢弃，也不会执行绕过。

警报：安全证书出现问题

通常，您在设备中生成或上传的根证书信息未在客户端应用中列为受信任根证书颁发机构。默认情况下，在大多数网络浏览器中，当用户发送 HTTPS 请求时，他们将看到一条来自客户端应用的警告消息，告知他们网站安全证书有问题。通常，错误消息指出网站的安全证书不是由受信任证书颁发机构所颁发，或者网站是由未知颁发机构认证。其他一些客户端应用不会向用户显示此警告消息，也不允许用户接受无法识别的证书。

注释 **Mozilla Firefox 浏览器**：您上传的证书必须包含“basicConstraints=CA:TRUE”，才能与 Mozilla Firefox 浏览器配合使用。此限制允许 Firefox 将根证书识别为受信任根证书颁发机构。

身份服务引擎问题

- 用于对 ISE 问题进行故障排除的工具，第 433 页
- ISE 服务器连接问题，第 434 页
- ISE 相关的严重日志消息，第 435 页

用于对 ISE 问题进行故障排除的工具

在对 ISE 相关问题进行故障排除时下列内容非常有用：

- 用于测试与 ISE 服务器连接的 ISE 测试实用程序提供宝贵的连接相关信息。这是“身份服务引擎”(Identity Services Engine) 页面上的**开始测试 (Start Test)** 选项；请参阅连接到 ISE 服务，第 134 页。
- ISE 和代理日志；请参阅 通过日志监控系统活动，第 331 页
- ISE 相关的 CLI 命令 `iseconfig` 和 `isedata`，特别是 `isedata`，以确认安全组标记 (SGT) 下载。有关其他信息，请参阅网络安全设备 CLI 命令，第 457 页。
- Web 跟踪和策略跟踪功能可用于调试策略匹配问题；例如，应允许的用户被阻止，反之亦然。有关其他信息，请参阅策略故障排除工具：策略跟踪，第 441 页。
- 数据包捕获，第 448 页 if 使用支持，第 450 页.
- 要检查证书状态，您可以使用 openssl 在线证书状态协议 (OCSP) 实用程序，该实用程序可从 https://www.openssl.org/ 获得。

ISE 服务器连接问题

证书问题

WSA 和 ISE 服务器使用证书对成功的连接进行相互身份验证。因此，一个实体展示的每个证书应可被其他实体识别。例如，如果 WSA 的客户端证书是自签名证书，则必须在相应 ISE 服务器上的受信任证书列表中显示相同的证书。相应地，如果 WSA 客户端证书为 CA 签名证书，则 CA 根证书必须出现在相应的 ISE 服务器上。类似的要求也适用于 ISE 服务器相关的管理员证书和 pxGrid 证书。

证书要求和安装在集成思科身份服务引擎，第 129 页中有所介绍。如果您遇到证书相关的问题，请检查以下条目：

- 如果使用 CA 签名证书：
  - 验证管理员证书和 pxGrid 证书的根 CA 签名证书是否显示在 WSA 上。
  - 验证 WSA 客户端证书的根 CA 签名证书是否显示在 ISE 服务器上的受信任证书列表中。
- 如果使用自签名证书：
  - 验证 WSA 客户端证书（在 WSA 上生成并且已下载）是否已上传到 ISE 服务器并且显示在 ISE 服务器受信任证书列表中。
  - 验证 ISE 管理员证书和 pxGrid 证书（在 ISE 服务器上生成并已下载）是否已上传到 WSA 并显示在其证书列表中。
- 过期的证书：
  - 确认上传时有效的证书未到期。

日志输出指示证书问题

以下 ISE 服务日志片段显示由于缺少证书或者证书无效导致客户端连接超时。

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.ini
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

WSA 上的这些跟踪级别日志条目显示 30 秒后，终止连接到 ISE 服务器的尝试。

网络问题

- 如果与 ISE 服务器的连接在身份服务引擎页面（连接到 ISE 服务，第 134 页）上的开始测试期间失败，请检查端口 443 和 5222 上与配置的 ISE 服务器的连接。

  端口 5222 是正式的客户端到服务器可扩展消息传送和在线状态协议 (XMPP) 端口，用于与 ISE 服务器的连接；此外，它还由 Jabber 和 Google Talk 等应用所使用。注意，某些防火墙已配置为阻止端口 5222。

  可用于检查连接的工具包括 `tcpdump`。

其他 ISE 服务器连接问题

当 WSA 尝试连接 ISE 服务器时，下列问题会导致失败：

- ISE 服务器上的许可证已过期。
- 在 ISE 服务器的“管理”(Administration) > “pxGrid 服务”(pxGrid Services) 页面上，pxGrid 节点状态为“未连接”(not connected)。请确保在此页面上选择“启用自动注册”(Enable Auto-Registration)。
- 过期的 WSA 客户端（尤其是“test_client”或“pxgrid_client”）显示在 ISE 服务器上。这些需要删除；请参阅 ISE 服务器上的“管理”(Administration) > “pxGrid 服务”(pxGrid Services) > “客户端”(Clients)。
- WSA 在其所有服务启动并运行之前尝试连接 ISE 服务器。

  ISE 服务器上的更改（例如证书更新）需要重新启动 ISE 服务器或者其上运行的服务。这段时间内任何连接 ISE 服务器的尝试都将失败，但是最终，连接将会成功。

ISE 相关的严重日志消息

本节包含对 WSA 上 ISE 相关的严重日志消息的说明：

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  WSA 的 ISE 进程无法连接到 ISE 服务器 30 秒。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing.Please check ISE config`

  WSA 客户端证书和密钥未在 WSA 的身份服务引擎配置页面上传或生成。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  WSA 的 ISE 进程无法连接到 ISE 服务器 120 秒并退出。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed ...`

  WSA 的 ISE 进程无法订用 ISE 服务器的更新。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: ...`

  为 ISE 服务器连接创建 WSA 的 ISE 客户端时出现内部错误。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: ...`

  内部错误指示进行连接或重新连接时批量下载 SGT 失败。

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service.Error: ...`

  WSA 的 ISE 服务无法启动。

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal ...`

  WSA 的 ISE 服务无法向 heimdall 发送就绪信号。

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal ...`

  WSA 的 ISE 服务无法向 heimdall 发送重新启动信号。

自定义和外部 URL 类别的问题

下载外部实时源文件时遇到问题

在创建和编辑自定义和外部 URL 类别并提供**外部实时源**文件（无论是**思科源格式**还是 **Office 365 源格式**）时，必须点击**获取文件**按钮，以启动到指定服务器的连接，并下载和分析文件。系统将显示这一过程的进度和结果；如果出现错误，会对错误进行描述。纠正问题，然后尝试再次下载该文件。

可能的错误类型有四种：

- 连接异常

  无法解析服务器主机名 - 作为源文件位置提供的 URL 无效；请提供正确的 URL 来解决此问题。

- 协议错误

  凭证无效导致身份验证失败 - 服务器身份验证失败；为服务器连接提供正确的用户名和密码。

  服务器上找不到请求的文件 - 为源文件提供的URL 指向无效资源。确保指定服务器上有正确的文件。

- 内容验证错误

  无法验证字段的内容 - 源文件的内容无效。

- 解析错误

- 思科源格式 .csv 文件必须包含一个或多个条目，其中每个条目都是站点地址或有效的 regex 字符串，后跟一个逗号，再后跟地址类型（可以是`站点`或 `regex`）。如果源文件中有任何条目不符合此约定，则会引发分析错误。

  此外，不要在文件中的任何`站点`条目中包含 `http://` 或 `https://`，否则会出错。换言之，`www.example.com` 会被正确分析，而 `http://www.example.com` 会出错。

- 从 Microsoft 服务器获得的 XML 源文件由标准 XML 解析器进行解析。XML 标记中的任何不一致也将被标记为解析错误。

解析错误的行号包括在日志中。例如：

`Line 8: 'www.anyurl.com' - Line is missing address or address-type field.`源文件中的第 8 行包含有效的地址或 regex 模式，或地址类型。

`Line 12: 'www.test.com' - Unknown address type.`第 12 行具有无效的地址类型，该地址类型可以是`站点`或 `regex`。

IIS 服务器上 CSV 文件的 MIME 类型问题

如果在创建和编辑自定义和外部 URL 类别时为**外部实时源类别** > **思科源格式**选项提供 .csv 文件时，则在思科源格式服务器正在运行 Internet 信息服务 (IIS) 版本 7 或 8 软件的情况下获取文件时会遇到“406 可不接受”错误。类似地，`feedsd` 日志将会报告类似如下的内容：`31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'`。

这是因为 IIS 上的 .csv 文件的默认 MIME 类型是 `application/csv`，而不是 `text/csv`。您可以通过登录到 IIS 服务器并将 .csv 文件的 MIME 类型条目编辑为 `text/csv` 来纠正此问题。

复制和粘贴后格式错误的提要文件

如果将. csv (文本) 提要文件的内容从 UNIX 或 OS X 系统复制并粘贴到 Windows 系统, 则会自动添加额外的回车 (`\r`), 这会使提要文件格式不正确。

如果手动创建. csv 文件, 或者如果您使用 SCP、FTP 或 POST 将文件从 UNIX 或 OS X 系统传输到 Windows 服务器, 则不应出现任何问题。

日志记录问题

- 自定义 URL 类别不显示在访问日志条目中， 第 438 页
- 记录 HTTPS 事务， 第 438 页
- 警报：无法保持生成数据的速率， 第 438 页
- 将第三方日志分析器工具与 W3C 访问日志结合使用的问题， 第 438 页

自定义 URL 类别不显示在访问日志条目中

当 Web 访问策略组具有设置为“监控”(Monitor) 的自定义 URL 类别和一些其他组件（例如 Web 信誉过滤器或 DVS 引擎）时，做出最终决定以允许或阻止自定义 URL 类别中某 URL 的请求，然后请求的访问日志条目显示预定义的 URL 类别，而不是自定义 URL 类别。

记录 HTTPS 事务

访问日志中的 HTTPS 事务看起来与 HTTP 事务类似，但有些特征略有不同。记录的内容取决于事务是显式发送到 HTTPS 代理还是以透明方式重定向到 HTTPS 代理：

- **TUNNEL**。当 HTTPS 请求以透明方式重定向到 HTTPS 代理时，此内容会写入访问日志。
- **CONNECT**。当 HTTPS 请求显式发送到 HTTPS 代理时，此内容会写入访问日志。

当 HTTPS 流量解密时，访问日志包含事务的两个条目。

- TUNNEL 或 CONNECT，取决于所处理请求类型。
- HTTP 方法和解密的 URL。例如，“GET https://ftp.example.com”。

仅在 HTTPS 代理解密流量的情况下，完整的 URL 才可见。

警报：无法保持生成数据的速率

当内部日志记录进程因缓冲区已满而丢弃 Web 事务事件时，AsyncOS for Web 会向配置的警报收件人发送一封重要邮件。

默认情况下，Web 代理负载很高时，内部日志记录进程会缓冲事件，以在稍后 Web 代理负载降低时再进行记录。如果日志记录缓冲区已完全填满，Web 代理会继续处理流量，但日志记录进程不会在访问日志或 Web 跟踪报告中记录某些事件。Web 流量出现高峰时，很可能会发生这种情况。

但是，如果设备持续一段时间过载，也会发生日志记录缓冲区已满的情况。AsyncOS for Web 会继续每隔几分钟发送重要邮件，直到日志记录进程不再丢弃数据。

该重要邮件包含以下文本：

```
Reporting Client: The reporting system is unable to maintain the rate of data being
generated.Any new data generated will be lost.
```

如果 AsyncOS for Web 持续频繁地发送此重要邮件，设备可能容量不足。请联系思科客户支持，确认是否需要额外的网络安全设备容量。

将第三方日志分析器工具与 W3C 访问日志结合使用的问题

如果要将第三方日志分析器工具用于读取和解析 W3C 访问日志，则可能需要包括“时间戳”(timestamp) 字段。“时间戳 W3C”(timestamp W3C) 字段显示的是 UNIX 时间戳，大多数日志分析器只能识别此格式的时间。

策略问题

无法配置 HTTPS 的访问策略

HTTPS 代理启用后，解密策略会处理所有 HTTPS 策略决策。您无法再通过 HTTPS 定义访问和路由策略组成员身份，也无法再将访问策略配置为阻止 HTTPS 事务。

如果一些访问和路由策略组成员身份由 HTTPS 定义，并且如果一些访问策略阻止 HTTPS，则当您启用 HTTPS 代理时，这些访问和路由策略组将变为禁用状态。您可以随时选择启用策略，但所有 HTTPS 相关配置会被删除。

受阻对象问题

未阻止某些 Microsoft Office 文件

当您在“阻止对象类型”(Block Object Type) 部分中阻止 Microsoft Office 文件时，可能不会阻止某些 Microsoft Office 文件。

如果您需要阻止所有 Microsoft Office 文件，请在“阻止自定义 MIME 类型”(Block Custom MIME Types) 字段中添加 **application/x-ole**。但是，阻止此自定义 MIME 类型还会阻止所有 Microsoft 复合对象格式类型，例如 Visio 文件以及一些第三方应用。

阻止 DOS 可执行对象类型会阻止 Windows OneCare 的更新

当您配置网络安全设备以阻止 DOS 可执行对象类型时，设备也会阻止 Windows OneCare 的更新。

标识配置文件从策略中消失

禁用标识配置文件会将其从相关策略中删除。验证标识配置文件是否已启用，然后再次将其添加到策略中。

策略匹配失败

策略从未应用

如果多个标识配置文件具有相同的条件，AsyncOS 会将事务分配给匹配的第一个标识配置文件。因此，事务从不与其他相同的标识配置文件匹配，从不匹配或应用适用于这些后续相同的标识配置文件的任何策略。

HTTPS 和 FTP over HTTP 请求仅匹配不需要身份验证的访问策略

在启用了凭证加密的情况下，将设备配置为使用 IP 地址作为代理。

当凭证加密已启用并配置为使用 Cookie 作为代理类型时，则身份验证不适用于 HTTPS 或 FTP over HTTP 请求。这是因为 Web 代理将客户端重定向到 Web 代理本身以便启用凭证加密时使用 HTTPS 连接进行身份验证。身份验证成功后，Web代理将客户端重定向回源网站。为了继续识别用户，Web 代理必须使用代理（IP 地址或 Cookie）。但是，如果请求使用 HTTPS 或 FTP over HTTP，则使用 Cookie 跟踪用户会导致以下行为：

- **HTTPS**。Web代理必须在分配解密策略之前解析用户身份（并因此解密事务），但只有在解密事务后才能获取识别用户的 Cookie。
- **FTP over HTTP**。使用 FTP over HTT 访问 FTP 服务器所面临的难题与访问 HTTPS 站点类似。Web 代理必须在分配访问策略之前解决用户身份问题，但却无法设置 FTP 事务的 Cookie。

因此，HTTPS 和 FTP over HTTP 请求将仅匹配不需要身份验证的访问策略。通常，它们会匹配全局访问策略，因为该策略从不需要身份验证。

用户匹配 HTTPS 和 FTP over HTTP 请求的全局策略

当设备使用基于 Cookie 的身份验证时，Web 代理不会从 HTTPS 和 FTP over HTTP 请求的客户端获取 Cookie 信息。因此，无法从 Cookie 获取用户名。

HTTPS 和 FTP over HTTP 请求仍根据其他成员身份条件匹配标识配置文件，但是即使标识配置文件需要身份验证，Web代理也不会提示客户端进行身份验证。相反，Web代理会将用户名设置为NULL并将该用户视为未经过身份验证的用户。

然后，当根据策略对未经身份验证的请求进行评估时，它仅与指定“所有身份”并应用于“所有用户”的策略匹配。通常，这是全局策略，例如全局访问策略。

用户分配到不正确的访问策略

- 您的网络上的客户端使用网络状态指示器 (NCSI)
- 网络安全设备使用 NTLMSSP 身份验证。
- 标识配置文件使用基于 IP 的代理。

系统可能会使用计算机凭证而不是用户自己的凭证来识别用户，因此可能会将用户分配到不正确的访问策略。

解决方法：

减少计算机凭证的代理超时值。

步骤 1 使用 `advancedproxyconfig > authentication` CLI 命令。

步骤 2 输入计算机凭证的代理超时。

修改策略参数后策略跟踪不匹配

修改“访问策略”(Access Policy)、“标识配置文件和用户”(Identification Profiles and Users)、“选择一个或多个标识配置文件”(Select One or More Identification Profiles) 或“选定的组和用户”(Selected Groups and Users) 等策略参数时，所做更改需在几分钟后才会生效。

策略故障排除工具：策略跟踪

关于策略跟踪工具

策略跟踪工具可以模拟客户端请求，然后详细展示 Web 代理如何处理该请求。在排除 Web 代理的故障时，可使用该工具跟踪客户端请求并调试策略处理。您可以执行基本跟踪，也可以输入高级跟踪设置并覆盖选项。

注释 使用策略跟踪工具时，Web 代理不会在访问日志或报告数据库中记录请求。

策略跟踪工具仅根据 Web 代理使用的策略评估请求。这些策略为访问策略、加密 HTTPS 管理策略、路由策略、数据安全策略以及出站恶意软件扫描策略。

注释 策略跟踪工具不评估 SOCKS 和外部 DLP 策略。

跟踪客户端请求

注释 您可以使用 CLI 命令 `maxhttpheadersize` 更改代理请求的 HTTP 信头长度最大值。增加该值可以减少在指定用户属于大量身份验证组，或者响应信头超过当前信头长度最大值时发生的策略跟踪故障。有关此命令的更多信息，请参阅网络安全设备 CLI 命令，第 457 页。

步骤 1 依次选择**系统管理 (System Administration) > 策略跟踪 (Policy Trace)**。

步骤 2 在“目标 URL”(Destination URL) 字段中输入要跟踪的 URL。

步骤 3 （可选）输入其他模拟参数。

要模拟...	请输入...
用于发出请求的客户端源 IP。	在“客户端 IP 地址” (Client IP Address) 字段中输入 IP 地址。 **注释** 如果未指定 IP 地址，AsyncOS 会使用本地主机。此外，无法获取 SGT（安全组标记），并且将不会匹配基于 SGT 的策略。
用于发出请求的身份验证/标识。	在“用户名”(User Name) 字段中输入用户名，然后从身份验证/标识 (Authentication/Identification) 下拉列表中选择身份服务引擎或身份验证领域。 **注释** 仅启用的选项可用。例如，仅当启用身份验证选项和 ISE 选项时这些选项才可用。 对于您在此输入的用户的身份验证，用户必须已经通过网络安全设备成功进行身份验证。

步骤 4 点击**查找策略匹配 (Find Policy Match)**。

策略跟踪输出显示在“结果”(Results) 窗格中。

注释 对于通过 HTTPS 事务，策略跟踪工具会绕过进一步扫描，且没有访问策略与此事务相关联。类似地，对于解密 HTTPS 事务，该工具无法实际解密事务来确定所应用的访问策略。在两种情况下，以及对于丢弃事务，跟踪结果会显示：“Access policy: Not Applicable”。

下一步做什么

相关主题

- 高级：请求详细信息，第 443 页
- 高级：响应详细信息覆盖，第 443 页

高级：请求详细信息

您可以使用“策略跟踪”(Policy Trace) 页面上“高级”(Advanced) 部分的“请求详细信息”(Request Details) 窗格中的设置，调整此策略跟踪的出站恶意软件扫描请求。

步骤 1 展开“策略跟踪”(Policy Trace) 页面上的**高级 (Advanced)** 部分。

步骤 2 根据需要填写“请求详细信息”(Request Details) 窗格中的字段：

设置	说明
代理端口 (Proxy Port)	选择要用于跟踪请求的特定代理端口，以根据代理端口测试策略成员身份。
用户代理 (User Agent)	指定要在请求中模拟的用户代理。
请求时间 (Time of Request)	指定要在请求中模拟的日期和时间。
上传文件 (Upload File)	选择要在请求中模拟上传的本地文件。 在此处指定要上传的文件时，Web 代理会模拟 HTTP POST 请求而不是 GET 请求。
对象大小 (Object Size)	输入请求对象的大小（以字节为单位）。可以输入 K、M 或 G 来表示千字节、兆字节或千兆字节。
MIME 类型 (MIME Type)	输入 MIME 类型。
防恶意软件扫描判定 (Anti-malware Scanning Verdicts)	要覆盖 Webroot、McAfee 或 Sophos 扫描判定，选择要覆盖的特定判定类型。

步骤 3 点击**查找策略匹配 (Find Policy Match)**。

策略跟踪输出显示在“结果”(Results) 窗格中。

高级：响应详细信息覆盖

您可以使用“策略跟踪”(Policy Trace) 页面上“高级”(Advanced) 部分的“响应详细信息覆盖”(Response Detail Overrides) 窗格中的设置，“调整”此跟踪 Web 访问策略响应的各方面。

步骤 1 展开“策略跟踪”(Policy Trace) 页面上的**高级 (Advanced)** 部分。

步骤 2 根据需要填写“响应详细信息覆盖”(Response Detail Overrides) 窗格中的字段：

设置	说明
URL 类别 (URL Category)	使用此设置覆盖跟踪响应的 URL 事务类别。选择要替换响应结果中的 URL 类别的类别。

设置	说明
应用	同样，使用此设置覆盖跟踪响应的应用类别。选择要替换响应结果中的应用类别的类别。
对象大小 (Object Size)	输入响应对象的大小（以字节为单位）。可以输入K、M或G来表示千字节、兆字节或千兆字节。
MIME 类型 (MIME Type)	输入 MIME 类型。
Web 信誉分数 (Web Reputation Score)	输入从 -10.0 到 10.0 的 Web 信誉分数。
防恶意软件扫描判定 (Anti-malware Scanning Verdicts)	使用这些选项覆盖跟踪响应中提供的特定防恶意软件扫描判定。选择要替换响应结果中的 Webroot、McAfee 和 Sophos 扫描判定的判定。

步骤 3 点击**查找策略匹配 (Find Policy Match)**。

策略跟踪输出显示在“结果”(Results) 窗格中。

文件信誉和文件分析问题

请参阅 故障排除文件信誉和分析， 第 249 页

重新启动问题

运行于 KVM 上的虚拟设备重启时挂起

注释 这是 KVM 问题，可随时更改。

有关详细信息，请参阅 https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html 和 https://bugs.launchpad.net/qemu/+bug/1329956。

步骤 1 选中以下复选框：

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

步骤 2 如果上述值设置为 Y：

a) 停止您的虚拟设备并重新安装 KVM 内核模块：

```
rmmod kvm_intel modprobe kvm_intel enable_apicv=N
```

b) 重新启动您的虚拟设备。

硬件设备：远程重置设备电源

开始之前

- 获取并设置可使用 IPMI 2.0 版管理设备的实用程序。
- 了解如何使用受支持的 IPMI 命令。请参阅您的 IPMI 工具文档。

如果硬件设备需要硬重置，则可以使用第三方智能平台管理接口 (IPMI) 工具远程重新启动设备机箱。

限制

- 远程电源重新启动仅适用于特定硬件。有关特定信息，请参阅启用远程电源循环，第 383 页。
- 如果您希望能够使用此功能，必须在需要使用该功能之前提前将其启用。有关详细信息，请参阅启用远程电源循环，第 383 页。
- 仅支持以下 IPMI 命令：status、on、off、cycle、reset、diag、soft。发出不受支持的命令将会引发“权限不足”错误。

步骤 1 使用 IPMI 向分配到“远程电源重新启动”端口（之前配置）的 IP 地址发出支持的电源循环命令，以及所需的凭证。

例如，从支持 IPMI 的 UNIX 类型计算机中可能发出如下命令：

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

其中，`192.0.2.1` 是分配到远程电源重新启动端口的 IP 地址，remoteresetuser 和 passphrase 是您在启用此功能时输入的凭证。

步骤 2 等待至少十一分钟，以便设备重启。

站点访问问题

- 无法访问不支持身份验证的 URL，第 446 页
- 无法通过 POST 请求访问站点，第 446 页
- 另请参阅：对特定网站绕过解密，第 432 页

无法访问不支持身份验证的 URL

在透明模式下部署网络安全设备时，由于有些应用不支持身份验证，因而无法使用，以下是这些应用的部分列表。

- Mozilla Thunderbird
- Adobe Acrobat Updates
- HttpBridge
- CollabNet Subversion
- Microsoft Windows Update
- Microsoft Visual Studio

解决办法：为不需要身份验证的 URL 创建用户类。

相关主题

- 绕过身份验证，第 105 页

无法通过 POST 请求访问站点

当用户的第一个客户端请求是POST请求并且用户仍需要身份验证时，POST正文内容丢失。当POST请求针对访问控制单点登录功能正在使用中的应用时，可能会出现问题。

解决方法：

- 在连接到使用POST作为第一个请求的URL之前，通过浏览器请求一个不同的URL，让用户先对 Web 代理进行身份验证。
- 绕过使用 POST 作为第一个请求的 URL 的身份验证。

注释 使用访问控制时，您可以绕过在应用身份验证策略中配置的断言使用者服务 (ACS) URL 的身份验证。

相关主题

- 绕过身份验证，第 105 页.

上游代理问题

- 上游代理未收到基本凭证，第 447 页
- 上游代理的客户端请求失败，第 447 页

上游代理未收到基本凭证

如果设备和上游代理均采用 NTLMSSP 进行身份验证，根据配置，设备和上游代理可能陷入请求身份验证凭证的无限循环。例如，如果上游代理需要基本身份验证，但设备需要NTLMSSP身份验证，则设备可能永远无法成功将基本凭证传送到上游代理。这是由于身份验证协议的限制导致的。

上游代理的客户端请求失败

配置：

- 网络安全设备和上游代理服务器均采用基本身份验证。
- 下游网络安全设备上启用了凭证加密。

上游代理上的客户端请求失败，因为 Web 代理从客户端收到“Authorization”HTTP 报头，但上游代理服务器需要“Proxy-Authorization”HTTP 报头。

无法通过上游代理路由 FTP 请求

如果网络包含不支持 FTP 连接的上游代理，则您必须创建适用于所有身份以及仅适用于 FTP 请求的路由策略。将该路由策略配置为直接连接到 FTP 服务器或连接到所有代理均支持 FTP 连接的代理组。

虚拟设备

AsyncOS 启动期间请勿使用强制重置 (Force Reset)、关闭电源 (Power Off) 或重置 (Reset) 选项

虚拟主机上的以下操作等同于拔下硬件设备上的插头，这是不支持的，尤其在 AsyncOS 启动期间：

- 在 KVM 中，为“强制重置”(Force Reset) 选项。
- 在 VMWare 中，为“关闭电源”(Power Off) 和“重置”(Reset) 选项。（在设备彻底正常运行后，这些选项可安全使用。）

KVM 部署上的网络连接起初正常，而后失败

问题

网络连接最初正常，随后丢失。

解决方案

这是 KVM 问题。请参阅以下位置的 OpenStack 文档中“KVM：网络连接起初正常，而后失败”一节：http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html。

KVM 部署上出现性能低、监视程序问题和 CPU 使用率高

问题

在 Ubuntu 虚拟机上运行时，设备性能低，出现监视程序问题，并且设备显示异常高的 CPU 使用率。

解决方案

安装来自 Ubuntu 的最新主机操作系统更新。

在 Linux 主机上运行的虚拟设备的通用故障排除

问题

在 KVM 部署上运行的虚拟设备的问题可能与主机操作系统配置问题有关。

解决方案

参阅可从以下位置获取的《虚拟化部署和管理指南》中的故障排除章节和其他信息：

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

WCCP 问题

最大端口条目数

在使用 WCCP 的部署中，HTTP、HTTPS 和 FTP 端口加起来的最大端口条目数为 30。

数据包捕获

设备可以捕获和显示在设备所连接的网络上传输或接收的 TCP/IP 数据包及其他数据包。

注释 数据包捕获功能类似于 Unix tcpdump 命令。

开始数据包捕获

步骤 1 依次选择**支持和帮助 (Support And Help) > 数据包捕获 (Packet Capture)**。

步骤 2 （可选）点击**编辑设置 (Edit Settings)** 更改数据包捕获设置。

选项	说明
捕获文件大小限制 (Capture File Size Limit)	指定捕获文件可以达到的最大大小。达到限制后，将丢弃数据并开始新文件，除非“捕获持续时间”(Capture Duration) 设置为“达到文件大小限制之前一直运行捕获”(Run Capture Until File Size Limit Reached)。
捕获持续时间 (Capture Duration)	用于是否自动停止捕获以及何时自动停止捕获的选项。选项包括： • **达到文件大小限制之前一直运行捕获 (Run Capture Until File Size Limit Reached)**。在达到上述文件限制之前一直运行捕获。 • **达到所用时间之前一直运行捕获 (Run Capture Until Time Elapsed Reaches)**。在指定持续时间内运行捕获。如果您输入时间值时未指定单位，AsyncOS 会默认使用秒。 • **无限期地运行捕获 (Run Capture Indefinitely)**。运行数据包捕获，直到手动停止。 **注释** 可以随时手动结束捕获。
接口 (Interfaces)	从中捕获流量的接口。
过滤器 (Filters)	捕获数据包时要应用的过滤选项。过滤功能允许您仅捕获所需的数据包。选项包括： • **无过滤器 (No Filters)**。将捕获所有数据包。 • **预定义的过滤器 (Predefined Filters)**。预定义的过滤器按端口和/或 IP 地址提供过滤功能。如果保留空白，则将捕获所有流量。 • **自定义过滤器 (Custom Filter)**。如果您已经知道所需数据包捕获选项的确切语法，则使用此选项。使用标准 tcpdump 语法。

（可选）提交并确认数据包捕获更改。

注释 如果您更改了数据包捕获设置但未确认更改并且之后开始了数据包捕获，则 AsyncOS 会使用新设置。这允许您在当前会话中使用新设置，而不强制使用未来数据包捕获运行的设置。设置仍然有效，直至您将其清除。

步骤 3 点击**开始捕获 (Start Capture)**。要手动停止运行捕获，请点击**停止捕获 (Stop Capture)**。

管理数据包捕获文件

设备将捕获的数据包活动保存到文件并在本地存储该文件。您可以使用 FTP 将数据包捕获文件发送给思科客户支持，以便进行调试和故障排除。

• 下载或删除数据包捕获文件，第 450 页

下载或删除数据包捕获文件

注释 您还可以使用 FTP 连接到设备并从捕获目录检索数据包捕获文件。

步骤 1 依次选择**支持和帮助 (Support And Help) > 数据包捕获 (Packet Capture)**。

步骤 2 从“管理数据包捕获文件”(Manage Packet Capture Files) 窗格中选择要使用的数据包捕获文件。如果此窗格不可见，则设备上未任何存储数据包捕获文件。

步骤 3 根据需要点击**下载文件 (Download File)** 或**删除选定文件 (Delete Selected Files)**。

使用支持

收集信息以获得高效服务

在联系支持部门之前：

- 请启用自定义日志记录字段，如通用故障排除最佳实践， 第 423 页中所述。
- 考虑执行数据包捕获操作。请参阅数据包捕获， 第 448 页。

提出技术支持请求

开始之前

- 验证您的 Cisco.com 用户 ID 是否与此设备的服务协议合同关联。要查看当前与您的 Cisco.com 配置文件相关的服务合同列表，请访问位于 https://sso.cisco.com/autho/forms/CDClogin.html 的 Cisco.com 配置文件管理器。如果没有 Cisco.com 用户 ID，请注册一个。

您可以使用设备发送非紧急的请求，寻求思科客户支持的帮助。当设备发送请求时，其还会发送设备的配置。设备必须能够发送邮件到互联网，才能发送支持请求。

注释 如果遇到紧急问题，请致电思科全球支持中心。

步骤 1 依次选择**支持和帮助 (Support And Help) > 联系技术支持 (Contact Technical Support)**。

步骤 2 （可选）选择请求的其他收件人。默认情况下，支持请求和配置文件发送到思科客户支持部。

步骤 3 输入您的联系信息。

步骤 4 输入问题详细信息。

- 如果您有此问题的客户支持申请单，请输入。

步骤 5 点击 **Send**（**发送**）。故障单通过思科创建。

获取虚拟设备技术支持

如果您为思科内容安全虚拟设备提交一个支持请求，则必须提供您的虚拟许可证号 (VLN)、合同编号和产品标识符代码 (PID)。

您可以根据虚拟设备上运行的软件许可证，通过参考采购订单或从下表识别 PID。

功能	PID	说明
网络安全基本版	WSA-WSE-LIC=	包括： • Web 使用控制 • Web 信誉
网络安全高级版	WSA-WSP-LIC=	包括： • Web 使用控制 • Web 信誉 • Sophos 和 Webroot 防恶意软件签名
网络安全防恶意软件	WSA-WSM-LIC=	包括 Sophos 和 Webroot 防恶意软件签名
McAfee 防恶意软件	WSA-AMM-LIC=	—
高级恶意软件防护	WSA-AMP-LIC=	—

启用对设备的远程访问

通过“远程访问”(Remote Access) 选项，思科客户支持部门可远程访问您的设备以提供支持。

步骤 1 依次选择**支持和帮助 (Support And Help) > 远程访问 (Remote Access)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 完成“客户支持远程访问”(Customer Support Remote Access) 选项：

选项	说明
种子字符串 (Seed String)	如果您输入字符串，该字符串不应与任何现有或未来的密码匹配。 当您点击“提交”(Submit) 后，该字符串将显示在页面顶部附近。 您将会把该字符串提供给您的支持代表。
安全隧道 (Secure Tunnel)（推荐）	指定是否为远程访问连接使用安全隧道。 启用时，设备会通过服务器 upgrades.ironport.com 的指定端口（默认情况下通过端口 443）创建 SSH 隧道。建立连接后，思科客户支持可以使用 SSH 隧道获取对设备的访问权限。 启用 techsupport 隧道后，会将与 upgrades.ironport.com 的连接保持 7 天。7 天后，无法使用 techsupport 隧道建立任何新连接，但所有现有连接将继续存在并正常运行。 远程访问帐户将保持活动状态，直到明确停用。

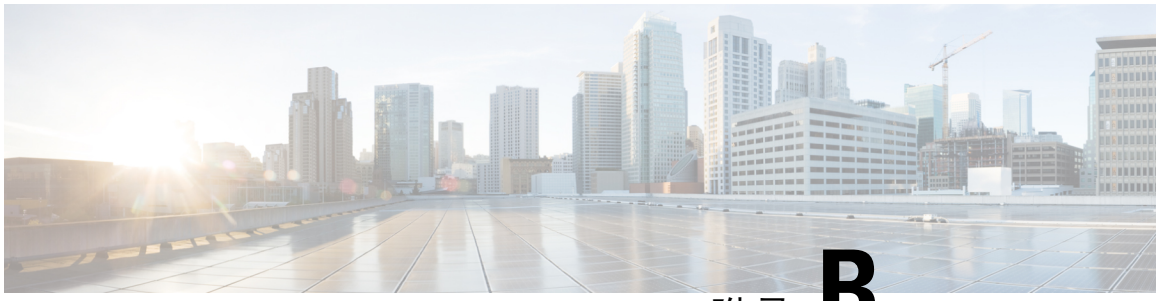
步骤 4 提交并确认更改。

步骤 5 在页面顶部附近的“成功”(Success) 消息中查找种子字符串并进行记录。

出于安全原因，此字符串不会存储在设备中，因此稍后无法查找此字符串。

将此字符串保存在一个安全的位置。

步骤 6 将此种子字符串提供给您的支持代表。



附录 B

命令行界面

本附录包含以下部分：

命令行界面概述

AsyncOS 命令行界面 (CLI) 允许您配置和监控网络安全设备。命令行界面可通过 IP 接口上的 SSH 访问，IP 接口上已配置启用这些 SSH 服务，或者使用串行端口的终端仿真软件上进行了配置。默认情况下，SSH 配置在管理端口上。

输入带有或不带任何参数的命令名称调用命令。如果输入不带参数的命令，命令会提示您所需的信息。

访问命令行界面

您可以使用以下方法之一进行连接：

- **以太网**。启动与网络安全设备 IP 地址的 SSH 会话。出厂默认 IP 地址为 192.168.42.42。SSH 配置为使用端口 22。
- **串行连接**。在已经连接了串行电缆的个人计算机上，启动与通信端口的终端会话。

首次访问

在您使用**管理员 (admin)**帐户首次访问 CLI（输入默认**管理员 (admin)**用户名和密码登录设备）后，可以添加不同权限的其他用户。

- 用户名：**admin**
- 密码：**ironport**

首次使用默认密码登录时，系统设置向导会提示您更改**管理员 (admin)** 帐户的密码。

您还可以随时使用 passwd 命令重置**管理员 (admin)** 帐户的密码。

后续访问

您可以随时使用有效用户名和密码连接和登录设备。请注意，在登录时会自动显示当前用户名的最近设备访问次数列表（包括成功和失败登录）。

请参阅以下 userconfig 命令说明，或参阅管理用户帐户，第 384 页了解有关配置其他用户的信息。

使用命令提示符

顶层命令提示符包括完全限定的主机名，依次后跟大于号 (>) 和空格。例如：

```
example.com>
```

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

例如：

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

当有默认设置时，设置显示在命令提示符括号中。例如：

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

当显示默认设置时，键入 Return 与接受默认值效果相同。

命令语法

当在交互模式下运行时，CLI 命令语法由单个命令组成，不带空格以及变量或参数。例如：

```
example.com> logconfig
```

选择列表

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

例如：

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

是/否查询

当需要您做出“是”或“否”的选择时，问题结尾会在方括号中提供一个默认值。您可以回答 **Y**、**N**、**是 (Yes)** 或**否 (No)**。大小写并不重要。

例如：

```
Do you want to enable the proxy? [Y]> Y
```

子命令

有些命令允许您使用子命令指令，如 NEW、EDIT 和 DELETE。EDIT 和 DELETE 功能提供以前配置过的值的列表。

例如：

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (172.xxx.xx.xx/xx: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
```

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

子命令转义

您可以随时在子命令内使用 Ctrl+C 键盘快捷键，以立即退出并返回到 CLI 的最顶级。

命令历史记录

CLI 会保存会话期间输入的所有命令的历史记录。使用键盘上的 Up 和 Down 箭头键，或者使用 Ctrl+P 和 Ctrl+N 组合键，可以滚动查看最近运行的命令的列表。

命令补全

AsyncOS CLI 支持命令补全。您可以输入某些命令的前几个字母，然后按 Tab 键，CLI 会补全字符串。如果您输入的字母在命令中不是唯一的，则 CLI 会提供范围缩小的一组备选命令。例如：

```
example.com> set (press the Tab key)
```

```
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

使用 CLI 确认配置更改

- 许多配置更改在提交后才会生效。
- 当其他操作可正常进行时，使用 commit 命令可以更改配置设置。
- 要成功确认更改，命令提示符必须位于最顶级处。在空命令提示符处键入 **Return**，可将命令提示符上移一个命令行层级。
- 系统会记录尚未确认的配置更改，但是在运行 commit 命令前，这些更改不会生效。但并非所有的命令均需要运行 commit 命令。以下操作会清除尚未提交的更改：退出 CLI 会话、系统关闭、重新启动、故障或下发 clear 命令。
- 在您收到确认消息和时间戳前，系统不会实际确认更改。

通用 CLI 命令

本节介绍您在典型 CLI 会话可能使用的一些基本命令，例如确认和清除更改。

CLI 示例：提交配置更改

您可以选择在 commit 命令后输入评论。

```
example.com> commit

Please enter some comments describing your changes:
[]> Changed “psinet” IP Interface to a different IP address
Changes committed: Wed Jan 01 12:00:01 2007
```

CLI 示例：清除配置更改

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

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Wed Jan 01 12:00:01 2007
example.com>
```

CLI 示例：退出命令行界面会话

exit 命令可用于从 CLI 应用注销。尚未提交的配置更改会被清除。

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.
```

```
Are you sure you wish to exit?  [N]> y
```

CLI 示例：在命令行界面中搜索帮助信息

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

```
example.com> help
```

此外，您可以通过输入 **help** commandname 访问特定命令的帮助。

相关主题

- 网络安全设备 CLI 命令，第 457 页

网络安全设备 CLI 命令

网络安全设备 CLI 支持通过一组代理和 UNIX 命令访问、升级和管理系统。

注释 并非所有 CLI 命令都可适用/用于所有操作模式（标准和云网络安全连接器模式）。

adminaccessconfig

您可以配置网络安全设备对登录到设备的管理员具有更严格的访问要求，并且可以指定非活动超时值。有关详细信息，请参阅用于访问设备的其他安全设置，第 390 页和用户网络接入，第 391 页。

advancedproxyconfig

配置高级的 Web 代理选项；子命令如下：

AUTHENTICATION - 身份验证配置选项：

- 您什么时候想要将授权请求信头转发给父代理
- 输入要在最终用户身份验证对话框中显示的代理授权领域
- 是否要记录请求 URI 中出现的用户名
- 组成员属性是否应用于 Web UI 中的目录查找(如果未使用，则显示成员属性不同的空组或组)
- 是否要使用高级 Active Directory 连接检查
- 是否要允许在策略中使用不区分大小写的用户名匹配
- 是否要允许对 LDAP 组名称使用字符 * 进行通配符匹配
- 输入客户端用于基本身份验证的字符集 [ISO-8859-1/UTF-8]
- 是否要启用 LDAP 推荐
- 是否要启用安全身份验证
- 输入主机名以重定向身份验证的客户端
- 输入用户凭证的代理超时

命令行界面

- 输入计算机凭证的代理超时
- 输入由于身份验证服务不可用而允许流量时的代理超时
- 输入被拒绝请求的重新验证选项 [禁用 / embedlinkinblockpage]
- 是否要发送 Negotiate 邮件头和 NTLM 邮件头，以进行 NTLMSSP 身份验证
- 配置日志和报告中的用户名和 IP 地址屏蔽

CACHING - 代理缓存模式；选择一项：

- 安全模式
- 优化模式
- 积极模式
- 自定义模式

另请参阅选择 Web 代理缓存模式，第 64 页。

DNS - DNS 配置选项：

- 输入在 DNS 查找失败时用于 HTTP 307 重定向的 URL 格式
- 是否希望代理在 DNS 查找失败时发出 HTTP 307 重定向指令
- 当上游代理 (对等) 不响应时是否希望代理不要对 DNS 结果进行自动故障转移
- 是否要禁用在主机报头的 IP 地址
- 通过以下方式查找 Web 服务器：

  0 = 始终按顺序使用 DNS 应答

  1 = 使用客户端提供的地址，然后使用 DNS

  2 = 有限的 DNS 使用率

  3 = 非常有限的 DNS 使用率

  默认值为 0。对于选项 1 和 2，如果启用 Web 信誉，将使用 DNS。对于选项 2 和 3，如果无上游代理或配置的上游代理失败，DNS 将用于显式代理请求。对于所有选项，当在策略成员身份中使用目标 IP 地址时，使用 DNS。

EUN - 最终用户通知参数：

- 选择：

  1.刷新 EUN 页面

  2.使用自定义 EUN 页面

  3.使用标准的 EUN 页面

- 是否开启“用户确认”页的显示？

另请参阅Web 代理使用协议，第 68 页和最终用户通知概述，第 275 页。

NATIVEFTP - 本地 FTP 配置：

- 是否要启用 FTP 代理
- 输入 FTP 代理监听的端口

- 输入代理对于主动 FTP 连接要监听的端口号范围
- 输入代理对于主动 FTP 连接要监听的端口号范围
- 输入身份验证格式：

  1.检查点

  2.无代理身份验证

  3.报告
- 是否要启用缓存
- 是否要启用服务器 IP 欺骗
- 是否要将 FTP 服务器欢迎消息传递到客户端
- 输入 FTP 服务器目录的最大路径长度

另请参阅FTP 代理服务概述， 第 71 页。

FTPOVERHTTP - FTP Over HTTP 选项：

- 输入要用于匿名 FTP 访问的登录名
- 输入要用于匿名 FTP 访问的密码

另请参阅FTP 代理服务概述， 第 71 页。

HTTPS - HTTPS 相关的选项：

- HTTPS URI 日志记录 - fulluri 或 stripquery
- 是否要解密未经身份验证的透明 HTTPS 请求以进行身份验证
- 是否要解密 HTTPS 请求以用于通知最终用户
- HTTPS 服务器握手期间请求客户端证书时要采取的操作：

  1.通过事务

  2.回复无可用证书
- 是否要启用服务器名称指示 (SNI) 扩展？
- 是否要启用自动发现和下载缺失的中间证书？
- 是否要启用会话恢复？

另请参阅创建解密策略以控制 HTTPS 流量概述， 第 199 页。

SCANNING - 扫描选项：

- 是否让代理对所有内容执行恶意软件扫描而不考虑内容类型
- 输入等待防恶意软件扫描引擎 (Sophos、McAfee 或 Webroot) 响应的时间，以秒为单位
- 是否希望禁用 Webroot 正文扫描

命令行界面

另请参阅防恶意软件扫描概述， 第 222 页和扫描出站流量概述， 第 213 页。

PROXYCONN - 管理无法接受代理连接报头的用户代理的列表。列表条目将解释为快速词法分析器 (Flex) 用语正则表达式。如果用户代理的任何子字符串匹配列表中的任何正则表达式，则此用户代理将匹配。

- 请选择要执行的操作：

  新建 - 新增条目到用户代理列表中

  删除 - 从列表中删除条目

CUSTOMHEADERS - 管理特定域的自定义请求报头。

- 请选择要执行的操作：

  删除 - 删除条目

  新建 - 新增条目

  编辑 - 编辑条目

另请参阅将自定义报头添加到 Web 请求中， 第 66 页。

MISCELLANEOUS - 与代理相关的其他参数：

- 是否希望代理响应来自第 4 层交换机的运行状况检查 （如果 WSA 处于第 4 层透明模式时始终启用）
- 是否希望代理对 TCP 接收窗口大小执行动态调整
- 是否希望代理对 TCP 发送窗口大小执行动态调整
- 是否要过滤非 HTTP 响应？

  （默认情况下将过滤非 HTTP 响应。如果您要通过代理允许非 HTTP 响应，请输入 **N**）
- 启用 HTTPS 响应缓存
- 输入用于检查无响应上游代理的最小空闲超时时间 （以秒为单位）
- 输入用于检查无响应上游代理的最大空闲超时时间 （以秒为单位）
- 代理模式：

  1.仅显式转发模式

  2.第 4 层交换机，或没有用于重定向设备的透明模式

  3.与用于重定向 WCCP v2 路由器的透明模式
- 通过代理欺骗客户端 IP：

  1.禁用

  2.为所有请求启用

  3.仅对透明请求启用
- 是否要为信头发送转发的 HTTP X？
- 是否要启用服务器连接共享？

- 是否要允许在 HTTP 端口上通过隧道传输非 HTTP 请求？
- 是否要阻止在 SSL 端口上通过隧道传输非 SSL 事务？
- 是否希望代理在传入连接 IP 地址的位置上记录 X 转发标题的值？
- 是否希望代理限制缓存提供的内容？
- 是否希望代理使用 X-Forwarded-For 报头中的客户端 IP 地址吗？
- 是否要将服务器发送的 TCP RST 转发到客户端？
- 是否要启用 WCCP 代理运行状况检查？
- 是否要为 Velocity Regex 启用 URL 小写转换？

另请参阅将 P2 数据接口用于 Web 代理数据，第 28 页和配置 Web 代理设置，第 61 页。

SOCKS - SOCKS 代理选项：

- 是否要启用 SOCKS 代理
- 代理协商超时
- UDP 隧道超时
- SOCKS 控制端口
- UDP 请求端口

另请参阅将 P2 数据接口用于 Web 代理数据，第 28 页和SOCKS 代理服务，第 73 页。

CONTENT-ENCODING - 允许和阻止内容编码类型。

当前允许的内容编码类型：压缩、紧缩、gzip

当前阻止的内容编码类型：不适用

要更改特定内容编码类型的设置，请选择以下选项：

1. 压缩
2. 紧缩
3. gzip

[1]>

当前允许的编码类型是“压缩”

是否要对其阻止？[N]>

adminaccessconfig

您可以将网络安全设备配置为对登录设备的管理员具有更严格的访问权限要求。

alertconfig

指定发送系统警报的警报收件人和设置参数。

authcache

让您可以从身份验证缓存中删除一个或所有条目（用户）。您还可以列出目前身份验证缓存中包含的所有用户。

bwcontrol

在默认代理日志文件中启用带宽控制调试消息。

certconfig

SETUP - 配置安全证书和密钥。

OCSPVALIDATION - 启用/禁用上传时证书的 OCSP 验证。

clear

清除自上次确认以来的待定配置更改。

commit

将待定更改提交到系统配置。

createcomputerobject

在您指定的位置创建一个计算机对象。

curl

将 cURL 请求直接发送给 Web 服务器，或者通过代理发送到 Web 服务器，并返回请求和响应 HTTP 报头，以便您确定导致 Web 页面无法加载的原因。

注释 此命令仅供管理员或操作员在 TAC 监督下使用。

子命令如下：

- DIRECT - 直接进行 URL 访问
- APPLIANCE - 通过设备进行 URL 访问

datasecurityconfig

定义最小请求正文大小，思科数据安全过滤器不会扫描小于该大小的上传请求。

date

显示当前日期。示例：

```
Thu Jan 10 23:13:40 2013 GMT
```

诊断

代理和报告相关子命令：

NET – 网络诊断实用程序

此命令已弃用。使用 packetcapture 捕获设备上的网络流量。

PROXY – 代理调试实用程序

请选择要执行的操作：

- SNAP - 拍摄代理的快照
- OFFLINE -对代理执行离线操作（通过 WCCP）
- RESUME - 恢复代理流量（通过 WCCP）
- CACHE - 清除代理缓存

REPORTING - 报告实用程序

报告系统目前已启用。

请选择要执行的操作：

- DELETEDB - 重新初始化报告数据库
- DISABLE - 禁用报告系统
- DBSTATS -列出数据库并导出文件（显示 export_files 和 always_onbox 文件夹下未处理的文件和文件夹的列表。）
- DELETEEXPORTDB - 删除导出文件（删除 export_files 和 always_onbox 文件夹下所有未处理的文件和文件夹）。
- DELETEJOURNAL - 删除日志文件（删除所有 aclog_journal_files。)

dnsconfig

配置 DNS 服务器参数。

dnsflush

刷新设备上的 DNS 条目。

etherconfig

配置以太网端口连接。

externaldlpconfig

定义最小请求正文大小，外部 DLP 服务器不会扫描小于该大小的上传请求。

externaldlpconfig

定义最小请求正文大小，外部 DLP 服务器不会扫描小于该大小的上传请求。

featurekey

提交有效密钥以激活许可功能。

featurekeyconfig

自动检查和更新功能密钥。

fipsconfig

SETUP - 启用/禁用 FIPS 140-2 合规性和重要敏感参数 (CSP) 的加密。请注意，需立即重新启动。

FIPSCHECK - 检查 FIPS 模式合规性。指示各证书和服务是否符合 FIPS 标准。

有关其他信息，请参阅FIPS 合规性，第 402 页。

grep

搜索命名输入文件中包含给定模式匹配项的行。

help

返回命令列表。

iccm_message

清除 Web 界面和 CLI 中表示此网络安全设备由安全管理设备（M 系列）管理的消息。

ifconfigorinterfaceconfig

配置和管理网络接口，包括 M1、P1 和 P2。显示当前配置的接口，并提供用于创建、编辑或删除接口的操作菜单。

iseconfig

此命令用于显示当前的 ISE 配置参数，以及指定所要执行的 ISE 配置操作：

- `setup` - 配置 ISE 设置，包括：启用/禁用、ISE 服务器名称或 IPv4 地址、代理缓存超时时间，以及统计信息备份时间间隔。

isedata

指定与 ISE 数据相关的操作：

`statistics` - 显示 ISE 服务器状态和 ISE 统计信息。

`cache` – 显示 ISE 缓存或检查 IP 地址：

`show` - 显示 ISE ID 缓存。

`checkip` - 在 ISE 本地缓存中查询某个 IP 地址。

`sgts` - 显示 ISE 安全组标记 (SGT) 表。

iseconfig

此命令用于显示当前的 ISE 配置参数，以及指定所要执行的 ISE 配置操作：

- `setup` - 配置 ISE 设置，包括：启用/禁用、ISE 服务器名称或 IPv4 地址、代理缓存超时时间，以及统计信息备份时间间隔。

isedata

指定与 ISE 数据相关的操作：

`statistics` - 显示 ISE 服务器状态和 ISE 统计信息。

`cache` – 显示 ISE 缓存或检查 IP 地址：

`show` - 显示 ISE ID 缓存。

`checkip` - 在 ISE 本地缓存中查询某个 IP 地址。

`sgts` - 显示 ISE 安全组标记 (SGT) 表。

last

按照反向时间顺序列出特定于用户的用户信息（包括 tty 和主机），或者列出在指定日期和时间登录的用户。

loadconfig

加载系统配置文件。

logconfig

配置对日志文件的访问。

mailconfig

通过邮件将当前配置文件发送到指定地址。

maxhttpheadersize

设置最大 HTTP 报头大小或代理请求 URL 大小；以字节为单位输入值，或将 K 附加到数值中以表示千字节。

对于属于许多身份验证组的用户策略跟踪会失败。如果 HTTP 响应报头大小或 URL 大小大于当前“最大报头大小”，策略跟踪也会失败。增大此值可以缓解此失败。最小值是 32 Kb；默认值是 32 Kb；最大值是 1024 KB。

musconfig

使用此命令启用 Secure Mobility 并配置如何识别远程用户（通过 IP 地址或通过集成一个或多个思科自适应安全设备。

命令行界面

注释 使用此命令所做的更改会导致 Web 代理重新启动。

musstatus

当网络安全设备与自适应安全设备集成时，使用此命令可显示与 Secure Mobility 相关的信息。

此命令会显示以下信息：

- 网络安全设备与每个自适应安全设备连接的状态。
- 网络安全设备与每个自适应安全设备连接的持续时间（分钟）。
- 每个自适应安全设备的远程客户端数量。
- 服务的远程客户端数量，其定义为通过网络安全设备传递流量的远程客户端的数量。
- 远程客户端的总数。

networktuning

WSA 利用多个缓冲区和优化算法同时处理数百个 TCP 连接，为典型 Web 流量提供高性能，即持续时间极短的 HTTP 连接。

在某些情况下，例如频繁下载大型文件 (100 + MB)，大缓冲区可提供更好的每个连接性能。但是，会增加总的内存使用率，因而，任何缓冲区的增加应符合系统上可用的内存。

发送和接收空间变量代表用于存储通过给定的 TCP 套接字的通信数据的缓冲区。发送和接收自动变量用于启用和禁用动态控制窗口大小的 FreeBSD 自动调整算法。这两个参数直接在 FreeBSD 内核内应用。

`SEND_AUTO` 和 `RECV_AUTO`启用时，系统根据系统负载和可用资源动态调整窗口大小。在轻量级负载 WSA 上，系统会尝试保持大的窗口大小以减少每个事务延迟。动态调整的窗口大小最大值取决于所配置的 mbuf 集群数量，而 mbuf 集群数量依赖于系统上的总可用 RAM。随着客户端连接总数的增加或可用的网络缓冲区资源变得稀缺，系统会调低窗口大小，以保护其自身避免将所有的网络缓冲区资源都用于代理流量。

有关使用此命令的更多信息，请参阅上传/下载速度问题，第 429 页。

`networktuning` 子命令如下：

`SENDSPACE` – TCP 发送空间缓冲区大小；范围为 8192 至 131072 字节；默认值为 16000 字节。

`RECVSPACE` – TCP 接收空间缓冲区大小；范围为 8192 至 131072 字节；默认值为 32768 字节。

`SEND-AUTO` – 启用/禁用 TCP 发送自动调整；1 = 启用，0 = 禁用；默认值是禁用。如果启用 TCP 发送自动调整，请务必使用 `advancedproxyconfig > miscellaneous > 是否希望代理对 TCP 发送窗口大小执行动态调整？`来禁用发送缓冲区自动调整。

`RECV-AUTO` – 启用/禁用 TCP 接收自动调整；1 = 启用，0 = 禁用；默认值是禁用。如果启用 TCP 接收自动调整，请务必使用 `advancedproxyconfig > miscellaneous > 是否希望代理对 TCP 接收窗口大小执行动态调整？`来禁用接收缓冲区自动调整。

`MBUF CLUSTER COUNT` – 更改可用 mbuf 集群的数量；可接受的范围为 98304 至 1572864。值应取决于安装的系统内存，使用以下公式计算：98304 * (X / Y)，其中 X 是系统上的 RAM 大小（千兆字节），

Y 为 4 GB。例如，对于 4 GB RAM，建议的值是 98304 * (4/4) = 98304。在增加 RAM 后，建议采用线性扩展。

SENDBUF-MAX – 指定最大发送缓冲区大小；范围为 131072 bytes 至 2097152 字节；默认值为 1 MB（1048576 字节）。

RECVBUF-MAX – 指定最大接收缓冲区大小；范围为 131072 bytes 至 2097152 字节；默认值为 1 MB（1048576 字节）。

CLEAN-FIB-1 – 从数据路由表中删除所有 M1/M2 条目，本质是启用控制平面/数据平面的分离。换言之，启用“单独路由”时，禁用任何数据平面进程通过 M1 接口发送数据。数据平面进程启用了“使用数据路由表”的进程，或者严格执行非管理流量的进程。控制平面进程仍可以通过 M1 或 P1 接口发送数据。

对这些参数进行更改后，请务必确认更改并重新启动设备。

⚠

注意 仅在您了解后果后再使用此命令。建议仅在 TAC 指导下使用。

nslookup

查询互联网域名服务器上有关指定主机和域的信息或打印域中的主机列表。

ntpconfig

配置 NTP 服务器。显示当前配置的接口，并提供用于从发出 NTP 查询的 IP 地址添加、删除或设置接口的操作菜单。

packetcapture

截获和显示 TCP/IP 数据包以及在设备所连接的网络上传输或接收的其他数据包。

passwd

设置密码。

pathmtudiscovery

启用或禁用路径 MTU 发现。

如果需要数据包分段，您可能要禁用路径 MTU 发现。

ping

将 ICMP ECHO REQUEST 发送到指定主机或网关。

proxyconfig <enable | disable>

启用或禁用 Web 代理。

proxystat

显示 Web 代理统计信息。

quit、q、exit

终止活动进程或会话。

reboot

刷新磁盘的文件系统缓存，停止正在运行的所有进程，并重新启动系统。

reportingconfig

配置报告系统。

resetconfig

将配置恢复为出厂默认设置。

revert

将 AsyncOS for Web 操作系统恢复到之前的合格版本。这是极具破坏性的操作，会销毁所有配置日志和数据库。请参阅恢复到以前的 AsyncOS for Web 版本，第 417 页了解有关使用此命令的信息。

rollovernow

滚动更新日志文件。

routeconfig

配置流量的目标 IP 地址和网关。显示当前配置的路由，并提供用于创建、编辑、删除或清除条目的操作菜单。

saveconfig

将当前配置设置的副本保存到文件。如果需要，可使用此文件恢复默认设置。

如果 FIPS 模式是启用，提供密码处理选项：屏蔽密码或加密密码。

setgateway

配置计算机的默认网关。

sethostname

设置主机名参数。

setntlmsecuritymode

将 NTLM 身份验证领域的安全设置更改为“ads”或“domain”。

- `domain` - AsyncOS 通过域安全信任帐户加入 Active Directory 域。在此模式下，AsyncOS 要求 Active Directory 仅使用 Active Directory 嵌套组。
- `ads` - AsyncOS 作为本地 Active Directory 成员加入域。

默认值为 `ads`。

settime

设置系统时间。

settz

显示当前时区和时区版本。提供操作菜单来设置本地时区。

showconfig

显示所有配置值。

注释 用户密码是加密的。

shutdown

终止连接并关闭系统。

smtprelay

配置内部生成的邮件的 SMTP 中继主机。需要 SMTP 中继主机来接收系统生成的邮件和警报。

smtpconfig

配置本地主机以侦听 SNMP 查询和允许 SNMP 请求。

sshconfig

配置受信任服务器的主机名和主机密钥选项。

sslconfig

AsyncOS 9.0 及更早版本的默认密码是 `DEFAULT:+kEDH`。对于 AsyncOS 9.1 和更高版本，默认密码是

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:
!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:
!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA
```

在这两种情况下，这可能会根据您选择的 ECDHE 密码更改。

注释 但是，无论是什么版本，升级到更高版本的 AsyncOS 版本时，都不会更改默认密码。例如，当您从较早版本升级到 AsyncOS 9.1，默认密码是 DEFAULT:+kEDH。换言之，在升级后，您必须更新当前密码套件。思科建议更新为：

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:
!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-
AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA
```

FALLBACK - 启用/禁用 SSL/TLS 回退选项。如果启用，与远程服务器的通信将在握手失败后回退到最低配置协议。

客户端和服务器之间协商协议版本后，由于实现问题会导致握手失败。如果启用此选项，代理会尝试使用当前配置的 TLS/SSL 协议的最低版本进行连接。

注释 在新的 AsyncOS 9.x 装置上，默认已禁用回退。从存在回退选项的早期版本升级时，会保留当前的设置；否则，从不存在回退选项的版本升级时，默认情况下回退是启用的。

ECDHE - 启用/禁用使用 LDAP 的 ECDHE 密码。

在后续版本中，会支持额外的 ECDH 密码功能；但是，一些额外密码所附带的某些指定曲线会导致设备在安全 LDAP 身份验证和 HTTPS 流量解密时关闭连接。请参阅SSL 配置，第 404 页了解有关指定其他密码的详细信息。

如果遇到这些问题，请使用此选项为其中一个或两个功能禁用或启用 ECDHE 密码功能。

status

显示系统状态。

supportrequest

将支持请求邮件发送到 Cisco 客户支持。这包括系统信息和主配置的副本。

（可选）如果提供服务请求编号，则会将更大的系统集和配置信息会自动添加到服务请求中。此信息会压缩并使用 FTP 上传到服务请求中。

tail

显示日志文件的结尾。命令接受日志文件名用作参数。

示例 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
...
...
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
```

```
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
…
…
“CTRL-C” + “q”
```

示例 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
…
…
“CTRL-C” + “q”
```

tcpservices

显示有关开放式 TCP/IP 服务的信息。

techsupport

提供临时连接，以使思科客户支持能够访问系统并帮助进行故障排除。

telnet

使用 TELNET 协议与另一台主机通信，通常用于检查连接。

testauthconfig

根据给定身份验证领域中定义的身份验证服务器来测试该领域的身份验证设置。

testauthconfig [-d level] [realm name]

运行不带任何选项的命令会导致设备列出可供选择的已配置身份验证领域。

调试标志 (`-d`) 控制调试信息的级别。级别可以介于 0 到 10 之间。如果未指定，设备使用级别 0。在级别 0 下，该命令将返回成功或失败。如果测试设置失败，该命令将列出失败的原因。

注释 思科建议您使用级别 0。仅在需要更多详细信息来进行故障排除时，才使用其他调试级别。

tuiconfig tuistatus

使用 CLI 配置高级透明用户识别设置，第 85 页中介绍了这两个命令。

traceroute

通过网关并沿着通向目标主机的路径跟踪 IP 数据包。

updateconfig

配置更新和升级设置。

updatenow

更新所有组件。

upgrade

安装 AsyncOS 软件升级。

`downloadinstall` – 下载并立即安装升级包。

`download` – 下载并保存升级包，供以后安装。

输入这两个命令中的任一个命令后，会显示适用于此WSA的升级包列表。输入条目编号然后按Enter来选择需要的软件包；升级包便会在后台开始下载。下载过程中，以下子命令可用：`downloadstatus` 和 `canceldownload`。

下载完成时，如果您最初输入的是`downloadinstall`，安装会立即开始。如果输入`download`，则下载完成后，以下两个命令可用：`install` 和 `delete`。输入 `install` 开始安装之前下载的软件包。使用 `delete` 从 WSA 删除先前下载的软件包。

userconfig

配置系统管理员。

版本

显示常规系统信息、系统软件的已安装版本以及规则定义。

wccpstat

`all` - 显示所有网络高速缓存通信协议 (WCCP) 服务组的详细信息。

`servicegroup` - 显示特定 WCCP 服务组的详细信息。

webcache

检查或修改代理缓存的内容，或配置设备从不缓存的域和 URL。允许管理员从代理缓存中删除特定 URL 或指定代理缓存中从不存储的域或 URL。

who

显示已登录系统 CLI 和 Web 界面会话的用户。

注释 个人用户最多有 10 个并发会话。

whoami

显示用户信息。

命令行界面

附录 C

更多信息

本附录包含以下部分：

思科通知服务

注册可接收与您的思科内容安全设备相关的通知，例如安全建议、现场通知、停止销售或停止支持声明，以及有关软件更新和已知问题的信息。

可以指定通知频率和接收的信息类型等选项。有关使用的每种产品的通知，应单独注册。

要登录，请访问 http://www.cisco.com/cisco/support/notifications.html

需要有 Cisco.com 帐户。如果没有，请参阅注册思科帐户以访问资源，第 477 页。

文档集

可从以下位置获得思科网络安全设备的相关文档：

产品	链接
网络安全设备 （包括硬件文档。）	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

产品	链接
内容安全管理设备（包括硬件文档。）	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
思科云网络安全（包括硬件文档。）	http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

培训

思科邮件和网络安全产品培训：

http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html

知识库文章（技术说明）

步骤 1 转到主产品页面 (http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html)。

步骤 2 查找名称中包含 **TechNotes** 的链接。

思科支持社区

可通过以下 URL 访问有关网络安全和相关管理的思科支持社区：

https://supportforums.cisco.com/community/5786/web-security

思科支持社区是一个讨论常规网络安全问题以及有关具体思科产品的技术信息的地方。例如，文章可能包含故障排除视频。

客户支持

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

针对传统 IronPort 的支持网站： http://www.cisco.com/web/services/acquisitions/ironport.html

有关虚拟设备的说明，请参阅《思科内容安全虚拟设备安装指南》。

对于普通问题，您还可以打开设备中的支持案例。

相关主题

- 使用支持，第 450 页

注册思科帐户以访问资源

要访问 Cisco.com 上的许多资源，都需要有思科帐户。

如果您没有 Cisco.com 用户 ID，可以在此注册一个 ID： https://tools.cisco.com/RPF/register/register.do

思科欢迎您提出意见

思科技术出版物团队将努力提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下邮件地址：contentsecuritydocs@cisco.com

请在邮件的主题行中加入本书的标题以及标题页中的出版日期。

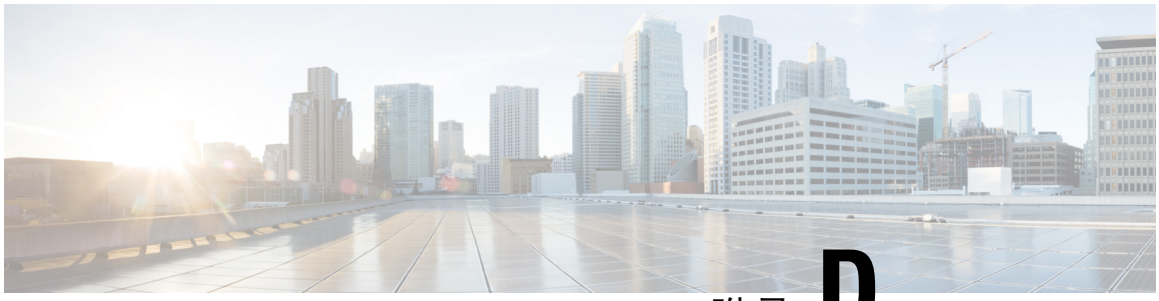
第三方贡献者

AsyncOS 中包含的部分软件的分销遵守 FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc. 和其他第三方贡献者的软件许可协议的条款、公告和条件，并且所有这些条款和条件已纳入许可协议。这些协议的全文可通过以下网站查看：

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

AsyncOS 产品中的软件部分基于 RRDtool 并且得到 Tobi Oetiker 的明确书面许可。

本文档中部分相关内容的复制已取得 Dell Computer Corporation 的许可。本文档中部分相关内容的复制已取得 McAfee, Inc. 的许可。本文档中部分相关内容的复制已取得 Sophos Plc 的许可。



附录 D

最终用户许可协议

本附录包含以下部分：

思科系统公司最终用户许可协议

重要提示：请认真阅读本最终用户许可协议。很重要的一点是，您应确认是从授权来源购买思科软件或设备，并且您或您所代表的实体（统称为“客户”）已经注册成为思科最终用户许可协议中规定的最终用户。如您还未注册成为最终用户，则无权使用本软件。本最终用户许可协议中的有限担保条款对您不适用。如您是从已授权的渠道购买了本软件，一旦下载、安装或使用思科或思科供应软件即构成接受本协议。

CISCO SYSTEMS, INC.或代替 CISCO SYSTEMS INC. 许可本软件的子公司（“思科”）愿意对您许可本软件，前提条件是您购买的软件来自授权来源，并且您接受本最终用户许可协议中的所有条款和条件，以及本产品随附或订购本产品时提供的附加许可协议中列出的对许可证的任何其他限制（统称“协议”）。如果最终用户许可协议与补充许可协议之间存在任何冲突，应以补充许可协议为准。下载、安装或使用本软件即表示您确认您是从授权渠道购买的本软件并同意受本协议的约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此 (a) 您不得下载、安装或使用本软件；和 (b) 您可退还本软件（包括未启封的 CD 包和所有书面资料）并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。只有原始及注册最终用户购买者才享有退货与退款权利，并且该权利从授权渠道购买产品后 30 天失效。在本最终用户许可协议中，“获批来源”指 A) 思科；或 (B) 经思科授权在您所在大区内向最终用户分销/出售思科设备、软件和服务的分销商或系统集成商；或 (C) 由任何该等分销商或系统集成商根据与思科签署的分销商协议条款授权在您所在大区内向最终用户分销/出售思科设备、软件和服务的经销商。

本协议下述条款管辖客户对本软件（定义如下）的使用，除非 *(a)* 客户与思科签订了单独协议以管理客户对本软件的使用；或 *(b)* 本软件包含了单独的“点击接受”许可协议或第三方许可协议，作为安装或下载流程的组成部分以管理客户对本软件的使用。如果前述文件条款之间存在任何抵触，优先顺序应为 *(1)* 经签署后的合同；*(2)* 点击接受协议或第三方协议；和 *(3)* 本协议。在本协议中，“软件”指计算机程序，包括授权来源提供给客户的思科设备中嵌入的固件和计算机程序，以及该固件和计算机程序的升级版、更新版、错误修正版与修改版（统称为“升级版”）；根据思科软件转让或重新许可政策（思科不定期修改后版本）重新许可的程序或前述内容的备份副本。

最终用户许可协议

许可。以遵守本协议条款和条件为前提，思科授予客户非独占性、不可转让许可，允许在客户内部业务中使用客户已向授权渠道支付许可费用的软件和文档。“文档”指该软件授权来源以任何方式（如 CD-ROM、在线提供等）所提供的与本软件相关的书面信息（无论是包含在用户手册、技术手册、培训材料、技术说明或其他材料中）。为使用本软件，客户应输入注册号或产品授权密钥，并在思科的网站在线登记客户的软件副本，以获取必要的许可密钥或许可文件。

客户使用本软件的许可应限于单个硬件机箱或硬件卡，除此以外客户不得在其他地方使用本软件。此外，使用许可权限还应符合相关补充许可协议或采购订单上规定的限制要求，因为此类订单已被授权来源所接受，并且客户已就该订单（“采购订单”）向授权来源支付必要的许可费。

除文档或相关补充许可协议中另有明确规定外，客户仅能使用其持有或租赁的思科设备中嵌入、运行的软件，或（如果相关文档允许在非思科设备上安装的话）为了与客户持有或租赁的思科设备通信使用本软件，以及为了实现客户的内部业务目的使用本软件。未以暗示、禁止反言或其他方式授予其他许可。

对于思科未收取许可费用的评估或测试软件，上述有关支付许可费用的要求不适用。

一般限制要求本协议仅为软件与文档许可协议，并非转让软件与文档的所有权，思科保留本软件与文档副本的所有权利。客户确认本软件与文档中含有思科或其提供商与许可方的商业秘密，包括（但不限于）单个程序的具体内部设计和架构，以及相关接口信息。除非本协议另作明确规定，本软件只能与客户从获批来源购得的思科设备配套使用，客户应无权利且客户明确同意不：

(i) 无权且明确同意不会向他人或实体转让、分配或转授其许可权力（符合思科现行有效的再次许可/转让政策的除外）；无权且明确同意不会在授权渠道以外采购的思科设备上或在二手思科设备上使用本软件；客户确认任何企图转让、分配、转授或使用的行为无效。

(ii) 无权且明确同意不会修正本软件错误、修改本软件或根据本软件制作衍生产品；也不得允许他人实施这种行为；

(iii) 无权且明确同意不会对本软件进行逆向工程、反编译、解码、反汇编或将本软件修改为可读格式。尽管存在该等限制要求，但适用法律明确许可的情况除外，以及根据适用开源协议规定要求思科允许该等活动的除外。

(iv) 无权且明确同意不会公布在本软件上运行的基准测试的结果；

(v) 未征得思科明确书面授权，无权且明确同意不会使用本软件或允许使用本软件向第三方提供服务，无论是以服务机构或分时方式提供服务；或

(vi) 未征得思科事先书面批准，无权且明确同意不会以任何方式向第三方披露、提供本软件和文档中包含的商业秘密。客户应采取合理的安全措施保护该等商业秘密。

在法律要求的范围内，思科将应客户的书面请求，并在客户支付思科的适用费用（如有）后，为客户提供必要的界面信息，以实现软件与其他独立创作的程序之间的互操作性。客户应严格遵守该等信息相关的保密义务。思科提供该等信息后应根据适用条款和条件的要求使用该等信息。

软件、升级版或额外副本。尽管本协议中含有其他相反之规定，(1) 客户无权制作或使用额外副本或更新版本，除非客户在制作或取得该副本或更新版本时，已经持有原始软件的有效许可并就更新版本或新增副本向许可资源支付了的恰当的费用；(2) 升级版本仅限用于授权渠道提供的思科设备，且客户是原始最终用户采购方或租赁方，或持有有效许可使用被升级软件，和 (3) 仅限于备份目的制作和使用额外副本。

专有权通知客户同意采用软件中含有的版权通知和其他专有权通知的格式和方法，针对所有形式的软件副本建立并翻印版权、专有权和其他通知。除本协议明确批准外，未经思科事先书面同意，客户不得制作任何本软件的副本。

期限和终止。本协议与本协议授予的许可在协议终止前始终有效。客户销毁本软件和文档的全部副本后即可终止本协议。如果客户未遵守本协议中的任何条款，则本协议中规定的客户权利应立即终止，无需思科另行通知。协议终止后，客户应销毁其持有或控制和软件与文档的全部副本。本协议终止后，“一般限制要求”部分中规定客户应遵守的所有保密义务、禁止与限制要求、责任限制、免责声明和质保限制要求应继续有效。此外，本协议终止后，标题“美国政府最终用户购买者”和“适用于有限担保声明和最终用户许可协议的通用条款”部分的规定仍然有效。

客户记录客户授予思科及其独立会计师权利，可在客户的正常营业时间内检查客户的帐簿、记录及帐目，以验证客户遵守本协议的情况。如果审计显示客户不符合本协议要求，客户应即时向思科支付恰当的许可费用加上合理的审计费用。

出口、再出口、转让与使用管控思科根据本协议提供的软件、文档和技术或直接产品（以下称为“软件和技术”）受美国法律法规及任何其他适用国家/地区的法律法规的出口控制约束。客户应遵守约束思科软件与技术出口、再出口、转让和使用的相关法律法规，并获取所有必需的美国和当地授权、准许或许可。思科与客户同意向对方提供取得授权或许可相关的其他信息、支持文件与合理要求的协助。有关遵守出口、再出口、转让和使用等方面规定的信息，请访问：

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

美国政府最终用户购买人本软件与文档系“商业物品”，该术语定义见《联邦采购条例》（“FAR”）(48 C.F.R.) 2.101，包括“商业计算机软件”和“商业计算机软件文档”，该术语用于 FAR 12.212。符合 FAR 12.212 和 DoD FAR 增刊227.7202-1 至 227.7202-4 的要求。尽管本协议可能并入含有其他相反之 FAR 或合同条款的协议中，客户可向政府最终用户提供具备本协议规定权利的软件与文档。如果本协议为直接与政府签订的协议，则政府最终用户仅根据协议规定的权利即可获得软件与文档。使用软件或文档或二者均使用，将视为政府同意本软件与文档为“商业计算机软件”与“商业计算机软件文档”，并视作政府接受本协议中规定的权利与限制要求。

标识组件；额外条款 本软件可能含有一个及以上的组件或与该等组件一同交付，这些组件可能含有第三方备件，思科在文档、自述文件、第三方点击接受协议或其他地方（如 http://www.cisco.com/）上对该等组件做出了标识（“标识组件”）。该等组件应遵守不同于本协议规定的许可协议条款、质保免责声明、限制保证或其他条款和条件（统称为“额外条款”）的要求。您同意接受任何此类标识组件的适用附加条款。

有限担保。

以符合本协议中的限制要求与条件为前提，思科保证：自向客户发货之日起（如果是授权来源转售而非思科直接销售，则应从思科最初发货后不超过九十 (90) 天起计算），在随后为期 (a) 九十 (90) 天或 (b) 随产品（本软件系组成部分）一同交付的保修卡上明确规定的质保期（如有）内（以二者中较长日期为准），(a) 安装软件的媒介在正常使用的情况下，材料与工艺上无任何瑕疵；和 (b) 本软件完全符合文档要求。思科发运产品的日期见产品包装。除上述规定外，软件将“按原样”提供。本有限保修仅用于首次注册最终用户从授权渠道购买的软件。本有限担保中的客户专属补救措施与思科和其提供商的全部责任为 (i) 替换缺陷媒介和/或 (ii) 根据思科的选择修复、替换本软件或退款，上述两种情况的前提条件是违反本有限担保的错误或缺陷在质保期内已报告给向客户销售软件的授权渠道。思科或向客户提供软件的授权渠道可不要求返还软件和/或文档作为行使补救措施的前提条

最终用户许可协议

件。思科未保证本软件无任何错误，也未保证客户使用本软件时不会出现任何问题或发生中断。此外，由于入侵和攻击网络的新技术的不断发展，思科并不保证本软件或本软件运行的设备、系统或网络无入侵和攻击漏洞。

限制如果本软件、产品或授权使用本软件的设备发生下述情况，则本保修不适用：(a) 被修改；但思科或其授权代表做出的修改除外；(b) 未按思科的指示安装、操作、修理或维护；(c) 受到非正常物理或电气应力、非正常环境条件、不当使用、疏忽或其他事故的影响；或 (d) 仅授予测试、评估、试验或示范许可。本软件保修也不适用于：(e) 任何临时软件模块；(f) 思科软件中心上未公布的软件；(g) 思科在思科软件中心明确“按原样”提供的软件；(h) 授权来源未收到许可费用的软件；和 (i) 授权来源以外的第三方提供的软件。

保修免责声明

除保修条款中规定的外，所有明示或暗示的条款、陈述与保证，包括（但不限于）对适销性、特殊目的适用性、未涉侵权、合格品质、未涉干扰、信息内容准确性等的暗示保修或条款，或因交易过程、法律、惯例或商业习惯产生的暗示保修或条款在此予以排除，但必须符合适用法律的规定，且思科、其提供商和授权商明确否认这种暗示的保修或条款。某种程度上，同样不能排除该等隐含条款、陈述和（或）保证的持续时间仅限于上文“有限担保”一款中明确规定的明示保修期内的情况。由于部分国家或司法管辖区不允许存在暗示保证时限限制，则上述限制要求在该等地区不适用。本保修赋予了客户特定的法律权利，同时客户也可拥有其他司法管辖区内规定的其他权利。即使上述明示保证未能实现其根本目的，该款免责及排除仍然适用。

免责声明 – 责任限制。如果您是在美国、拉丁美洲、加拿大、日本或加勒比地区购买的本软件，尽管本协议中含有其他相反规定，但是，思科、其关联机构、高管、董事、雇员、代理、提供商和授权商对客户应承担的责任（无论是因合同、侵权 [包括过失行为]、违反保修条款或其他形式引起的责任）不得超过授权渠道提供商提供的被索赔软件的购买价格，如果该软件为其他产品的组成部分，则不得超过该产品的购买价格。本软件责任限制是累加的，不限于每个事故（即，（即，两次或两次以上的索赔不得提高此限制）。

如果您是在欧洲、中东地区、非洲、亚洲或太平洋地区购买的本软件，尽管本协议中含有其他相反规定，但是，思科、其分公司、高管、董事、雇员、代理、提供商和授权商对客户应承担的责任（无论是因合同、侵权（包括过失行为）、违反保修条款或其他形式引起的责任）不得超过思科提供的被索赔软件的购买价格，如果该软件为其他产品的组成部分，则不得超过该产品的购买价格。该软件赔偿责任限制为累积性，不是针对单件事故（即，两次或两次以上的索赔不得提高此限制）。本协议中的任何内容均不限制(I)思科及其附属公司、高级官员、总监、员工、代理、供应商和许可商由于疏忽对客户造成个人伤害或致死的责任；(II) 思科欺诈性误述的责任；或 (III) 适用法律要求不能排除的思科责任。

免责声明 - 针对间接损害及其他损失的免责声明。 如果您是在美国、拉丁美洲、加勒比地区或加拿大购买的本软件，无论本协议中规定的补救措施是否实现了其基本目的，对于任何收益与利润损失、遗失或损坏数据、业务中断、资本损失，或特殊的、间接性、连带性或惩罚性损害赔偿，思科或其提供商均无需承担任何责任，无论导致前述损失损害的原因与责任推断如何，也无论是否是由于使用本软件造成该等损失损害，即使思科或其提供商曾告知将发生该等损害的可能性。由于某些国家或管辖区不允许限制或排除间接或附带损害，因此，上述限制可能对您不适用。

如果您在日本购买软件，除了由死亡或人身伤害、欺诈性失实陈述引起或与之相关的责任，无论本协议中补救措施是否实现其根本目的或其他目的，在任何情况下，思科及其分公司、管理人员、董事、员工、代理、提供商及许可方对任何原因造成的任何收益或利润损失、数据丢失或损坏、业务中断、资本损失、特殊、间接、连带、附带或惩罚性损失概不负责，不论责任推断如何，也无论是

否因使用或无法使用软件或其他原因引起，即使思科或任何经批准的源或其提供商或许可方已被告知发生此类损失的可能性。

如果您在欧洲、中东、非洲、亚洲或大洋洲购买软件，在任何情况下，思科及其分公司、管理人员、董事、员工、代理、提供商及许可方对任何收益或利润损失、数据丢失或损坏、业务中断、资本损失、特殊、间接、从属、附带或惩罚性损失概不负责，无论该损失如何造成，包括（但不限于）合同或侵权（包括疏忽）原因，也无论该损失是否因使用或无法使用软件引起，即使在各种情况下思科及其分公司、管理人员、董事、员工、代理、提供商及许可方已被告知发生此类损失的可能性。由于某些国家或管辖区不允许限制或排除间接或附带损害，因此，上述限制可能对您完全不适用。前述排除免责条款不适用于由下列原因引起或与之相关的责任：(I) 死亡或人身伤害；(II) 欺诈性失实陈述；(III) 与适用法律下任何不可免责条款有关的由思科承担的责任。

客户确认并同意，思科已根据本协议中的免责声明和责任限制确定价格和签订本协议，该价格和协议反映了协议各方之间的风险分担（包括合同补救措施可能不能达到其根本目的而且可能导致间接损失的风险），并构成了协议各方议价的重要依据。

管辖法律和司法权。如果您参照经授权来源所接受的采购订单上的地址，在美国、拉丁美洲或加勒比海采购软件，本协议和保证条款（“保证条款”）受美国加州的法律管辖并持解释权，不管是否存在任何法律条款冲突。加州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在加拿大购买软件，除非当地法律明确禁止，否则本协议和保证条款受加拿大安大略省法律管辖并据其进行解释，不管法律条款是否存在任何冲突；安大略省法庭对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在欧洲、中东、非洲、亚洲或大洋洲（不包括澳大利亚）购买软件，除非当地法律明确禁止，否则本协议和保证条款受英国法律管辖并据其进行解释，尽管法律条款可能存在任何冲突。英国法庭对由本协议或保证条款引起的任何索赔享有专属管辖权。此外，如果本协议受英国法律管辖，依照《1999年合同法（第三方权利）》，不属于本协议一方的任何人无权执行或受益于本协议的任何条款。如果您在日本购买软件，除非当地法律明确禁止，本协议和保证条款受日本法律管辖并依据该法律进行解释，尽管法律条款可能存在任何冲突。日本东京地方裁判所对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在澳大利亚购买软件，除非当地法律明确禁止，本协议和保证条款受澳大利亚新南威尔士州法律管辖并依据该法律进行解释，尽管法律条款可能存在任何冲突。新南威尔士州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在任何其他国家/地区购买软件，除非当地法律明确禁止，否则本协议和保证条款受美国加州管辖并据其进行解释，尽管法律条款可能存在任何冲突。加州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。

对于上述所有国家/地区，协议各方明确放弃使用《联合国国际货物销售合同公约》。尽管有上述规定，各方可以就任何所谓的违反该方知识产权或专有权利之行为，向适当管辖区的任何法庭寻求临时禁令救济。如果任何部分被发现为无效或不可强制执行，本协议和保证条款的其他条款应继续完全有效。除非本协议另有明确规定，否则本协议构成双方之间关于软件和文档许可的完整协议，并且替代任何《采购订单》或其他内容中包含的任何冲突或附加条款，所有此类条款都将被排除。本协议采用英文书写，双方同意以英语版本为准。

在以下 URL，可获得适用于思科产品的产品保修条款及其他信息：

http://www.cisco.com/go/warranty

思科系统公司内容安全软件终端用户补充许可协议

重要信息：请仔细阅读

最终用户许可协议

这种补充终端用户许可协议（“SEULA”）包含您（此处使用“您”，意味着您和所代表的业务实体或“公司”）与思科之间根据终端用户许可协议（“EULA”）许可的软件产品的其他条款和条件（统称为“协议”）。本SEULA中使用，但未定义的大写术语，与EULA中对其分配的含义相同。如果 EULA 和本 SEULA 的条款和条件在某种程度上存在冲突，则此 SEULA 的条款和条件优先。

除了 EULA 中列出的对您的软件访问和使用的限制之外，您同意始终遵守本 SEULA 中提供的条款和条件。

下载、安装或使用本软件即构成接受本协议，您自己及所代表的业务实体均受本协议绑定约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此(a)您不得下载、安装或使用本软件；和(b)您可退还本软件（包括未启封的CD包和所有书面资料）并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。从思科或授权思科经销商购买产品30天后，退货和退款的权利即到期，而且只有您是原始终端用户购买者，此权利才适用。

对于此SEULA，您订购的产品名称和产品说明是以下任意思科系统邮件安全设备（“ESA”）、思科系统网络安全设备（“WSA”）和思科系统安全管理应用（“SMA”）（统称为“内容安全”）及其等效的虚拟设备（“软件”）：

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

思科邮件反垃圾邮件、Sophos 防病毒

思科邮件爆发过滤器

Cloudmark 反垃圾邮件

思科映像分析器

McAfee 防病毒

思科智能多次扫描

思科数据丢失保护

思科邮件加密

思科电邮传送模式

思科网络使用控制

思科网络信誉

Sophos防恶意软件

Webroot防恶意软件

McAfee 防恶意软件

思科邮件报告

思科邮件跟踪

思科邮件集中式隔离区

思科 Web 报告

思科网络策略和配置管理

使用 Splunk 的思科高级网络安全管理

加密设备的邮件加密

系统生成的批量邮件的邮件加密

加密设备的邮件加密和公钥加密

加密设备的大型附件处理

加密设备的安全邮箱许可证

定义

对于此 SEULA，以下定义适用：

“公司服务”是指为了执行公司的内部业务，向终端用户提供的公司邮件、互联网、安全管理服务。

“终端用户”是指：（1）对于 WSA 和 SMA，为公司授权通过公司服务访问互联网和 SMA 的员工、承包商或其他代理；以及（2）对于 ESA，为公司授权通过公司服务访问或使用邮件服务的员工、承包商或其他代理的电子邮箱。

“订购文档”是指公司与思科或公司与思科经销商之间的购买协议、评估协议、试用，发布前协议或类似的协议，或思科接受的与之相关的任何采购订单的有效条款，包括本协议授予的软件许可证购买条款。

“个人身份信息”是指可用于识别个人的任何信息，包括但不限于个人的姓名、用户名、邮件地址及任何其他个人身份信息。

“服务器”是指网络中的一台物理计算机或设备，管理或为多位用户提供网络资源。

“服务”是指思科软件订用服务。

“服务说明”是指以下网站介绍的软件订用支持服务：http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

“遥测数据”是指公司的邮件和网络流量示例，包括有关邮件和网络请求属性的信息，以及有关公司的思科硬件产品如何处理不同类型的邮件和网络请求的信息。遥测数据中的邮件元数据和网络请求已进行匿名和模糊处理，以删除任何个人身份信息。

“期限”是指您购买的软件订用的长度，如订购文档中所示。

“虚拟设备”是指思科邮件安全设备、网络安全设备和安全管理设备的虚拟版本。

“虚拟机”是指可像服务器一样运行自己的操作系统和执行应用程序的软件容器。

其他许可条款和条件

许可证授予并同意数据收集条款

软件许可。

最终用户许可协议

使用本软件及文档，公司即同意遵守本协议的条款。只要公司遵从本协议，思科将在软件使用期限内，授予公司非排他性、不能再许可、不可转让的全球许可，仅限用于思科硬件产品；对于虚拟设备，即在虚拟机中，仅与面向终端用户的公司服务条款相关。许可使用本软件的终端用户数，限制为订购文档中规定的终端用户数。如果与提供公司服务相关的终端用户数量超过订购文档中规定的终端用户数量，公司将联系授权渠道购买更多该软件的许可证。有关此许可证的持续时间和范围等详细定义，请参阅订购文档。在软件许可证条款方面，订购文档可取代 EULA。除了此处授予的许可权限外，思科、思科经销商或其各自许可人不向公司授予任何软件的权利、所有权或利益。您对本软件升级的权利受服务说明约束。本协议和服务的有效期相同。

同意和许可使用数据。

根据思科隐私声明 (http://www.cisco.com/web/siteassets/legal/privacy.html)，公司在此同意并允许思科从公司收集和使用遥测数据。思科不会收集或使用遥测数据中的个人身份信息。思科可以与第三方共享整合和匿名的遥测数据，以帮助我们改进用户体验及本软件与其他思科安全产品和服务。公司可以随时禁用本软件中的“SenderBase 网络参与”，从而终止思科收集遥测数据的权限。有关启用或禁用“SenderBase 网络参与”的说明，请参阅软件配置指南。

其他权利和义务说明

请参阅 Cisco Systems Inc. 终端用户许可协议、隐私声明和软件订用支持服务的服务说明。