思科 ASDM 7.4(x) 版本说明

首次发布日期：2015 年 3 月 23 日
最后更新日期：2015 年 7 月 16 日

本文档包含思科 ASA 系列的思科 ASDM 7.4(x) 版本信息。

重要说明

- 统一通信电话代理和公司间媒体引擎代理已弃用 – ASA 9.4 版本不再支持电话代理和 IME 代理。

系统要求

ASDM 客户端操作系统和浏览器要求

下表列出支持的建议用于 ASDM 的客户端操作系统和 Java。

表 1 操作系统和浏览器要求

操作系统	浏览器				Java SE 插件
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英文版和日文版）： ■ 8 ■ 7 ■ Server 2008 ■ Server 2012	是	是	不支持	是	7.0 或更高版本
Apple OS X 10.4 及更高版本	不支持	是	是	是（仅限 64 位版本）	7.0 或更高版本
Red Hat Enterprise Linux 5（GNOME 或 KDE）： ■ 桌面版 ■ 带工作站选项的桌面版	不适用	是	不适用	是	7.0 或更高版本

Java 和浏览器兼容性

下表列出了 Java、ASDM 和浏览器兼容性的兼容性警告。

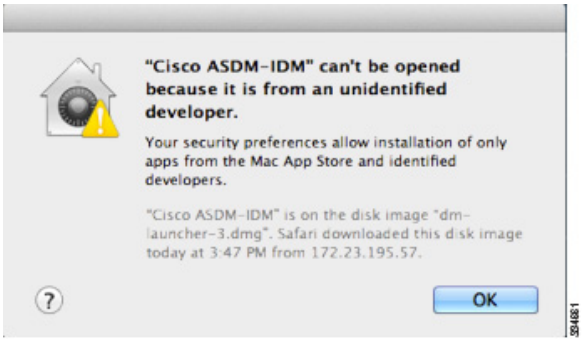
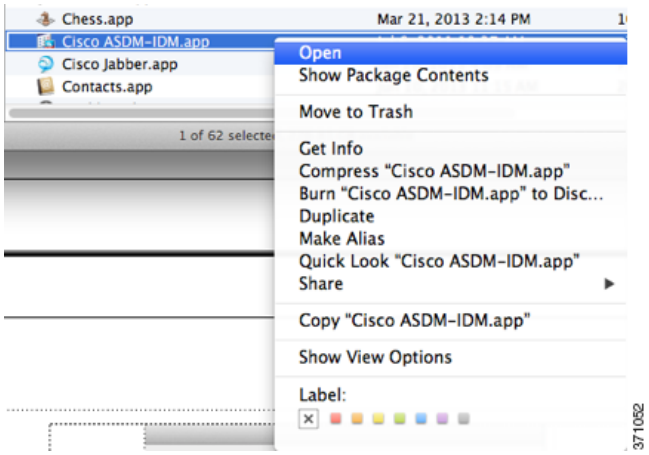
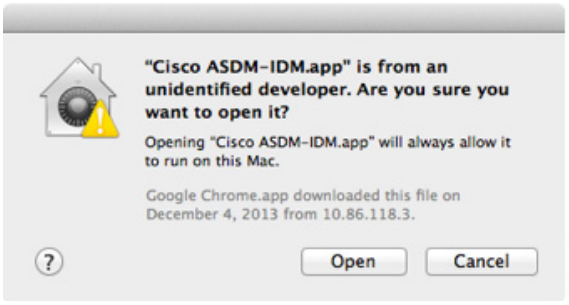
表 2 Java 与 ASDM 兼容性相关注意事项

Java 版本	条件	备注
7 Update 51	ASDM Launcher 需要可信证书	要继续使用 Launcher，请执行以下其中一项操作： ■ 将 Java 升级到 Java 8 或降级到 Java 7 update 45 或更低版本。 ■ 在 ASA 上安装由已知 CA 颁发的可信证书。 ■ 安装自签证书并使用 Java 进行注册。请参阅为 ASDM 安装身份证书。 ■ 或者，使用 Java Web Start。 **注意：**Java 7 update 51 不支持 ASDM 7.1(5) 及更低版本。如果您已升级 Java，并且无法再启动 ASDM 以将其升级到 7.2 版本或更高版本，则可以使用 CLI 升级 ASDM，也可以在 Java 控制面板中为每个要使用 ASDM 管理的 ASA 添加安全性异常。请参阅“解决方法”一节，网址： http://java.com/en/download/help/java_blocked.xml 添加安全性异常后，启动旧版本 ASDM，然后升级到 7.2 或更高版本。
	在极少数情况下，使用 Java Web Start 时无法加载在线帮助	在极少数情况下，启动在线帮助时，浏览器窗口会加载，但内容无法显示。浏览器报告以下错误：“Unable to connect”。 解决方法： ■ 使用 ASDM Launcher 或： ■ 清除 Java 运行时参数中的 **-Djava.net.preferIPv6Addresses=true** 参数： a. 启动 Java 控制面板。 b. 点击 **Java** 选项卡。 c. 点击 **View**。 d. 清除以下参数：**-Djava.net.preferIPv6Addresses=true** e. 点击 **OK**，然后点击 **Apply**，再次点击 **OK**。
7 Update 45	使用不可信证书时，ASDM 将显示一条有关缺失“权限”属性的黄色警告	由于 Java 中存在的一个漏洞，因此，如果没有在 ASA 上安装可信证书，您将会在 JAR 清单中看到指示缺少权限属性的黄色警告。**可忽略此警告**。ASDM 7.2 或更高版本包含“权限”属性。为了防止出现该警告，请安装可信证书（由已知 CA 颁发）；或者依次选择 **Configuration > Device Management > Certificates > Identity Certificates** 以在 ASA 上生成自签证书。启动 ASDM，当出现证书警告时，选中 **Always trust connections to websites** 复选框。
7	ASA 需要有强加密许可证 (3DES/AES)	ASDM 需要一个与 ASA 的 SSL 连接。您可以向思科申请一个 3DES 许可证： 1. 转至 www.cisco.com/go/license。 2. 点击 **Continue to Product License Registration**。 3. 在许可门户中，点击文本字段旁边的 **Get Other Licenses**。 4. 从下拉列表中选择 **IPS、Crypto、Other...**。 5. 将 **ASA** 键入至 **Search by Keyword** 字段。 6. 在 **Product** 列表中选择 **Cisco ASA 3DES/AES License**，然后点击 **Next**。 7. 输入 ASA 的序列号，然后按照提示为 ASA 申请 3DES/AES 许可证。

表 2 Java 与 ASDM 兼容性相关注意事项（续）

Java 版本	条件	备注
全部	■ 自签证书或不可信证书 ■ IPv6 ■ Firefox 和 Safari	如果 ASA 使用自签证书或不可信证书，当使用 HTTPS 通过 IPv6 浏览时，Firefox 和 Safari 将无法添加安全性异常。请访问 https://bugzilla.mozilla.org/show_bug.cgi?id=633001。此警告会影响从 Firefox 或 Safari 到 ASA 的所有 SSL 连接（包括 ASDM 连接）。要避免此警告，请为 ASA 配置由可信证书颁发机构颁发的正确证书。
	■ ASA 上的 SSL 加密必须包括 RC4-MD5 和 RC4-SHA1，*或者*在 Chrome 中禁用 SSL 虚假启动 ■ Chrome	如果更改 ASA 上的 SSL 加密以排除 RC4-MD5 和 RC4-SHA1 算法（默认情况下已启用这些算法），Chrome 将由于 Chrome“SSL 虚假启动”功能而无法启动 ASDM。我们建议重新启用其中一种算法（参阅 **Configuration > Device Management > Advanced > SSL Settings** 窗格）；您也可以根据 Run Chromium with flags 使用 **--disable-ssl-false-start** 标签在 Chrome 中禁用 SSL 虚假启动。
	服务器专用 IE9	对于服务器专用 Internet Explorer 9.0，“Do not save encrypted pages to disk”选项在默认情况下处于启用状态（请参阅 Tools > Internet Options > Advanced）。此选项会导致初始 ASDM 下载失败。请务必禁用此选项以允许 ASDM 下载。
	OS X	在 OS X 上，第一次运行 ASDM 时，系统可能会提示您安装 Java，根据需要按照提示进行安装。安装完成后，ASDM 将启动。

表 2 Java 与 ASDM 兼容性相关注意事项（续）

Java 版本	条件	备注
全部	OS X 10.8 及更高版本	您需要允许 ASDM 运行，因为它未使用 Apple 开发人员 ID 进行签名。如果未更改安全首选项，将会出现一个错误屏幕。  1. 要允许 ASDM 运行，请右键点击 （或按住 Ctrl 键并点击） **Cisco ASDM-IDM Launcher** 图标，然后选择 **Open**。  2. 随即将会出现一个类似的错误屏幕，但您可以通过该屏幕打开 ASDM。点击 **Open**，系统将打开 ASDM-IDM Launcher。 

为 ASDM 安装身份证书

使用 Java 7 update 51 及更高版本时，ASDM 启动程序需要可信证书。满足证书要求的一个简单方法就是安装自签身份证书。可使用 Java Web Start 启动 ASDM，直到安装证书。

请参阅为 ASDM 安装身份证书，以便在 ASA 上安装用于 ASDM 的自签身份证书，并向 Java 注册证书。

增加 ASDM 配置内存

ASDM 最多支持 512 KB 的配置。如果超出此数量，可能会遇到性能问题。例如加载配置时，状态对话框显示已完成配置的百分比，但如果有大型配置，它将停止递增并显示为暂停操作，即使 ASDM 仍可能在处理配置。如果发生此情况，我们建议考虑增加 ASDM 系统堆内存。

- 增加 Windows 中的 ASDM 配置内存（第 6 页）
- 增加 Mac 操作系统中的 ASDM 配置内存（第 6 页）

增加 Windows 中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **run.bat** 文件。

程序

1. 转到 ASDM 安装目录，例如 C:\Program Files (x86)\Cisco Systems\ASDM。
2. 使用任意文本编辑器编辑 **run.bat** 文件。
3. 在以“start javaw.exe”开头的行中，更改前缀为“-Xmx”的参数以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。
4. 保存 **run.bat** 文件。

增加 Mac 操作系统中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **Info.plist** 文件。

程序

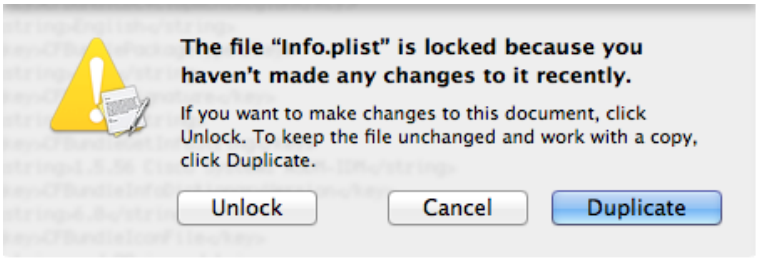
1. 右键点击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。
2. 在 **Contents** 文件夹中，双击 **Info.plist** 文件。如果已安装开发人员工具，该文件会在 **Property List Editor** 中打开。否则，它将在 **TextEdit** 中打开。
3. 在 **Java > VMOptions** 下方，更改前缀为“-Xmx”的字符串以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

4. 如果该文件已锁定，则将看到如下错误：



5. 点击 **Unlock** 并保存文件。

   如果未看到 **Unlock** 对话框，请退出编辑器，右键点击 **Cisco ASDM-IDM** 图标，选择 **Copy Cisco ASDM-IDM**，并将其粘贴到您拥有写入权限的位置，例如桌面。然后从该副本更改堆大小。

ASA 和 ASDM 兼容性

有关 ASA/ASDM 软件与硬件要求和兼容性(包括模块兼容性)的信息，请参阅思科 ASA 兼容性。

VPN 兼容性

有关 VPN 兼容性，请参阅支持的 VPN 平台，思科 ASA 5500 系列。

新功能

ASA 9.4(1.152)/ASDM 7.4(3) 的新功能

发布日期：2015 年 7 月 13 日

下表列出了 Firepower 9300 ASA （9.4(1.152) 版本/ASDM 7.4(3) 版本）的新功能。

注意：此版本仅支持 Firepower 9300 ASA。

表 3 Firepower 9300 ASA（9.4 (1.152) 版本/ASDM 7.4(3) 版本）的新功能。

特性	说明
平台功能	
Firepower 9300 ASA 安全模块	我们引入了 Firepower 9300 ASA 安全模块。
高可用性功能	
Firepower 9300 的机箱内 ASA 集群	您最多可在 Firepower 9300 机箱内集群 3 个安全模块。机箱中的所有模块都必须属于该集群。 我们引入了以下屏幕配置：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > ASA 集群复制 (ASA Cluster Replication)**
许可功能	
Firepower 9300 ASA 的思科智能软件许可	我们为 Firepower 9300 ASA 引入了智能软件许可。 我们修改了以下屏幕配置：**配置 (Configuration) > 设备管理 (Device Management) > 许可 (Licensing) > 智能许可 (Smart License)**

ASA 9.2(4)/ASDM 7.4(3) 的新功能

发布日期：2014 年 7 月 16 日

下表列出了 ASA 9.2(4) 版/ASDM 7.4(3) 版的新功能。

表 4 ASA 9.2(4) 版本/ASDM 7.4(3) 版本的新功能

特性	**说明**
平台功能	
在系统日志消息中显示无效用户名	现在可在失败登录尝试的系统日志消息中显示无效的用户名。当用户名无效或有效性未知时，默认设置是隐藏用户名。例如，如果用户意外键入密码而不是用户名，则在结果系统日志消息中隐藏“用户名”更为安全。您可能希望显示无效的用户名来帮助排除登录问题。 我们引入了以下命令：**no logging hide username**。 我们修改了以下屏幕配置：**配置 (Configuration) > 设备管理 (Device Management) > 日志 (Logging) > 系统日志设置 (Syslog Setup)**

表 4 ASA 9.2(4) 版本/ASDM 7.4(3) 版本的新功能（续）

特性	说明
DHCP 功能	
DHCP 中继服务器会验证用于应答的 DHCP 服务器标识符	如果 ASA DHCP 中继服务器收到来自错误的 DHCP 服务器的应答，现在它会验证该应答是否来自正确的服务器，然后对应答做出反应。
监控功能	
NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 将允许 Xlate count 轮询	添加对 NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 的支持以支持 SNMP xlate_count 和 max_xlate_count。 此数据等同于 **show xlate count** 命令。 未修改任何 ASDM 屏幕。 *此外，还在 8.4(5) 和 9.1(5) 版本中提供。*

ASA 9.4(1.200)/ASDM 7.4(2) 中的新功能

发布日期：2015 年 5 月 12 日

下表列出了 ASAv（9.4(1.200) 版本/ASDM 7.4(2) 版本）的新功能。

注意：此版本仅支持 ASAv。

表 5 ASAv 9.4(1.200)/ASDM 7.4(2) 中的新功能

特性	说明
平台功能	
VMware ASAv 不再需要 vCenter 支持	您现在可以使用 vSphere 客户端安装 VMware ASAv，而无需 vCenter，或使用 Day 0 配置安装 OVFTool。
亚马逊网络服务 (AWS) ASAv	您现在可以将 ASAv 与亚马逊网络服务 (AWS) 和 Day 0 配置结合使用。 注意　亚马逊网络服务仅支持 ASAv10 和 ASAv30 模式。

ASA 9.4(1)/ASDM 7.4(2) 版本的新功能

发布日期：2015 年 5 月 6 日

下表列出了 ASDM 7.4(2) 版本的新功能。

表 6 ASDM 7.4(2) 版本的新功能

特性	说明
远程访问功能	
支持 AnyConnect 4.1 版本	ASDM 现在支持 AnyConnect 4.1 版本。 我们修改了以下屏幕配置：**配置 (Configuration) > 远程访问 (Remote Access VPN) >网络（客户端）访问 (Network (Client) Access) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**（名为 **AMP 启用服务配置 (AMP Enabler Service Profile)** 的新配置文件）

ASA 9.4(1)/ASDM 7.4(1) 版本的新功能

注意：新增、已更改和已弃用的系统日志消息在系统日志消息指南中列出。

发布日期：2015 年 3 月 23 日

下表列出了 ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能。

表 7 ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能

功能	说明
平台功能	
ASA 5506W-X、ASA 5506H-X、ASA 5508-X 和 ASA 5516-X	引入了以下型号：带有无线接入点的 ASA 5506W-X、强化型 ASA 5506H-X、ASA 5508-X 和 ASA 5516-X。 引入了以下命令：**hw-module module wlan recover image** 和 **hw-module module wlan recover image**。
认证功能	
美国国防部统一功能要求 (UCR) 2013 认证	更新了 ASA，以满足 DoD UCR 2013 要求。请参阅下表中的各行，了解下列为 UCR 2013 认证添加的功能： ■ 定期证书身份验证 ■ 证书到期警报 ■ 执行基本约束 CA 标记 ■ 从证书配置 ASDM 用户名 ■ IKEv2 无效选择器通知配置 ■ IKEv2 十六进制预共享密钥
FIPS 140-2 认证合规更新	当在 ASA 上启用 FIPS 模式时，将会对 ASA 实施其他限制，以使其符合 FIPS 140-2。限制包括： ■ RSA 和 DH 密钥大小限制 - 仅允许使用大小为 2K（2048 位）或以上的 RSA 和 DH 密钥。对于 DH，这意味着不允许使用第 1 组（768 位）、第 2 组（1024 位）和第 5 组（1536 位）密钥。 **注意：**密钥大小限制禁止 IKEv1 与 FIPS 结合使用。 ■ 数字签名的散列算法限制 - 仅允许使用 SHA256 或更安全的算法。 ■ SSH 密码限制 - 允许的密码为：aes128-cbc 或 aes256-cbc。MAC：SHA1 要查看 ASA 的 FIPS 认证状态，请参阅： http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf 此 PDF 每周更新一次。 有关详细信息，请访问计算机安全部门的计算机安全资源中心网站： http://csrc.nist.gov/groups/STM/cmvp/inprocess.html 修改了以下命令：**fips enable**
防火墙功能	
改进了多核心 ASA 的 SIP 检测性能	如果有多条 SIP 信令流通过具有多核心的 ASA，则表明 SIP 检测性能已经过改进。但是，如果您使用的是 TLS、电话或 IME 代理，则不会看到性能改进。 未修改任何屏幕。

表 7 ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	说明
取消了对电话代理和 UC-IME 代理的 SIP 检测支持	当配置 SIP 检测后，您将无法再使用电话代理或 UC-IME 代理。使用 TLS 代理检测加密流量。 从 **Select SIP Inspect Map** 服务策略对话框中删除了 Phone Proxy 和 UC-IME Proxy。
DCERPC 检测支持 ISystemMapper UUID 消息 RemoteGetClassObject opnum3	ASA 从版本 8.3 开始支持非 EPM DCERPC 消息，支持 ISystemMapper UUID 消息 RemoteCreateInstance opnum4。此更改扩展了对 RemoteGetClassObject opnum3 消息的支持。 未修改任何屏幕。
每个情景的 SNMP 服务器陷阱主机数没有限制	ASA 支持每个情景的 SNMP 服务器陷阱主机数不受限制。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。 未修改任何屏幕。
VXLAN 数据包检测	ASA 可检测 VXLAN 报头以强制遵守标准格式。 修改了以下屏幕：**Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > Protocol Inspection**
IPv6 的 DHCP 监控	您现在可以监控 IPv6 的 DHCP 统计信息和 DHCP 绑定。 引入了以下屏幕： **Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics** **Monitoring > Interfaces > DHCP > IPV6 DHCP Binding**。
高可用性功能	
阻止在备用 ASA 上生成系统日志	您现在可以阻止在备用设备上生成特定系统日志。 未修改任何屏幕。
按接口启用和禁用 ASA 集群运行状况监控	您现在可以按接口启用或禁用运行状况监控。默认情况下，运行状况监控在所有端口通道冗余接口和单一物理接口上处于启用状态。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。 引入了以下屏幕：**Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Interface Health Monitoring**
DHCP 中继的 ASA 集群支持	现在可以在 ASA 集群上配置 DHCP 中继。通过使用客户端 MAC 地址散列，使客户端 DHCP 请求在集群成员中实现了负载均衡。仍然不支持 DHCP 客户端和服务器功能。 未修改任何屏幕。
ASA 集群中的 SIP 检测支持	您现在可以在 ASA 集群上配置 SIP 检测。控制流可以在任何设备上创建（由于负载均衡），但其子数据流必须驻留在同一设备上。不支持 TLS 代理配置。 未修改任何屏幕。
路由功能	
基于策略的路由	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容，ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 引入或修改了以下屏幕： **Configuration > Device Setup > Routing > Route Maps > Policy Based Routing** **Configuration > Device Setup > Routing > Interface Settings > Interfaces。**

表 7 ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	说明
接口功能	
VXLAN 支持	增加了 VXLAN 支持，包括 VXLAN 隧道终端 (VTEP) 支持。每个 ASA 或安全情景可以定义一个 VTEP 源接口。 我们引入了以下屏幕配置： **Configuration > Device Setup > Interface Settings > Interfaces > Add > VNI Interface** **Configuration > Device Setup > Interface Settings > VXLAN**
监控功能	
EEM 的内存跟踪	添加了一项新的调试功能来记录内存分配和内存使用情况，以响应内存日志记录封装事件。 我们修改了以下屏幕配置：**配置 (Configuration) > 设备管理 (Device Management) > 高级 (Advanced) > 嵌入式事件管理器 (Embedded Event Manager)** > 添加事件管理器小应用程序 (Add Event Manager Applet) > 添加事件管理器小应用程序事件 (Add Event Manager Applet Event)。
对崩溃进行故障排除	**show tech-support** 命令输出和 **show crashinfo** 命令输出包含最新生成的 50 行系统日志。请注意，必须启用 **logging buffer** 命令才能出现这些结果。
远程访问功能	
支持 ECDHE-ECDSA 密码	TLSv1.2 增加了对以下密码的支持： ■ ECDHE-ECDSA-AES256-GCM-SHA384 ■ ECDHE-RSA-AES256-GCM-SHA384 ■ DHE-RSA-AES256-GCM-SHA384 ■ AES256-GCM-SHA384 ■ ECDHE-ECDSA-AES256-SHA384 ■ ECDHE-RSA-AES256-SHA384 ■ ECDHE-ECDSA-AES128-GCM-SHA256 ■ ECDHE-RSA-AES128-GCM-SHA256 ■ DHE-RSA-AES128-GCM-SHA256 ■ RSA-AES128-GCM-SHA256 ■ ECDHE-ECDSA-AES128-SHA256 ■ ECDHE-RSA-AES128-SHA256 **注意：**ECDSA 和 DHE 密码具有最高优先级。 修改了以下屏幕：**Configuration > Remote Access VPN > Advanced > SSL Settings**。

表 7 ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	说明
无客户端 SSL VPN 会话 Cookie 访问限制	您现在可以防止第三方通过 JavaScript 等客户端侧脚本访问无客户端 SSL VPN 会话 Cookie。 **注意：**请仅遵照思科 TAC 的建议使用此功能。启用此功能会引发安全风险，因为系统在以下无客户端 SSL VPN 功能不运行时不提供任何警告。 ■ Java 插件 ■ Java 重写工具 ■ 端口转发 ■ 文件浏览器 ■ 需要桌面应用的 Sharepoint 功能（例如 MS Office 应用） ■ AnyConnect Web 启动 ■ Citrix Receiver、XenDesktop 和 Xenon ■ 其他不基于浏览器和浏览器插件的应用 引入了以下屏幕：**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > HTTP Cookie**。 *9.2(3) 中也包含此功能。*
使用安全组标记的虚拟桌面访问控制	ASA 现在支持基于安全组标记的策略控制，从而可对内部应用和网站进行无客户端 SSL 远程访问。此功能将 Citrix 的虚拟桌面基础架构 (VDI) 与 XenDesktop 配合使用，将其用作交付控制器和 ASA 的内容转换引擎。 有关详细信息，请参阅以下 Citrix 产品文档： ■ 用于 XenDesktop 和 XenApp 的策略：http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html ■ 管理 XenDesktop 7 中的策略：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html ■ 将组策略编辑器用于 XenDesktop 7 策略：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html
为无客户端 SSL VPN 添加了 OWA 2013 功能支持	无客户端 SSL VPN 支持 OWA 2013 中除以下功能外的新功能： ■ 支持平板电脑和智能手机 ■ 离线模式 ■ Active Directory 联合身份验证服务 (AD FS) 2.0。ASA 和 AD FS 2.0 无法协商加密协议 未修改任何屏幕。
为无客户端 SSL VPN 添加了 Citrix XenDesktop 7.5 和 StoreFront 2.5 支持	无客户端 SSL VPN 支持访问 XenDesktop 7.5 和 StoreFront 2.5。 有关 XenDesktop 7.5 功能的完整列表以及详细信息，请参阅 http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html。 有关 StoreFront 2.5 功能的完整列表以及详细信息，请参阅 http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html。 未修改任何屏幕。

表 7 ASA 9.4(1) 版/ASDM 7.4(1) 版的新功能（续）

功能	说明
定期证书身份验证	启用定期证书身份验证时，ASA 存储从 VPN 客户端接收的证书链，并且定期重新进行身份验证。 修改了以下屏幕： **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
证书到期警报	ASA 每 24 小时检查一次信任点中的所有 CA 和 ID 证书是否到期。如果证书即将到期，则会将一条系统日志作为警报发出。可以配置提醒和重现间隔。默认情况下，提醒将在到期之前 60 天启动，每 7 天重现一次。 修改了以下屏幕： **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
执行基本约束 CA 标记	默认情况下，现在不带 CA 标记的证书无法作为 CA 证书安装在 ASA 上。基本约束扩展标可确定证书的主题是否为 CA，及包含此证书的有效证书路径的最大深度。如果需要，可将 ASA 配置为允许安装这些证书。 修改了以下屏幕：**Configuration > Device Management > Certificate Management > CA Certificates**
IKEv2 无效选择器通知配置	目前，如果 ASA 在 SA 上接收到入站数据包，并且数据包的报头字段与 SA 的选择器不一致，则 ASA 会丢弃该数据包。您现在可以启用或禁用向对等方发送 IKEv2 通知。默认情况下会禁用发送此通知。 **注意：**在 AnyConnect 3.1.06060 和更高版本中支持此功能。
IKEv2 十六进制预共享密钥	您现在可以配置十六进制形式的 IKEv2 预共享密钥。 修改了以下屏幕：**Configuration > Site-to-Site VPN > Connection Profiles**
管理功能	
从证书配置 ASDM 用户名	利用此功能，能够通过从证书提取用户名以及使用由用户提供的用户名对 ASDM 用户进行授权。 引入了以下屏幕：**Configuration > Device Management > Management Access > HTTP Certificate Rule** 修改了以下屏幕：**Configuration > Device Management > Users/AAA > AAA Access > Authorization**
terminal interactive 命令用于在 CLI 处输入 **?** 时启用或禁用帮助	通常，当在 ASA CLI 输入 **?** 时，会显示命令帮助。要支持输入 **?** 作为命令中的文本（例如，将 **?** 加入 URL 中），可以使用 **no terminal interactive** 命令禁用交互式帮助。
REST API 版本 1.1	添加了对 REST API 1.1 版的支持。

升级软件

请参阅下表以获取您的版本的升级路径。某些版本需要先进行临时升级，然后才能升级到最新版本。

注意：除以下例外情况以外，对故障切换和 ASA 集群的零停机时间升级没有特殊要求。ASA 集群从 9.0(1) 或 9.1(1) 进行升级：由于 CSCue72961，不支持无中断升级。

当前 ASA 版本	首先升级到：	然后升级到：
8.2(x)	8.4(6)	9.4(1) 或更高版本
8.3(x)	8.4(6)	9.4(1) 或更高版本
8.4(1) 至 8.4(4)	8.4(6)、 9.0(4) 或 9.1(2)	9.4(1) 或更高版本
8.4(5) 及更高版本	-	9.4(1) 或更高版本
8.5(1)	9.0(4) 或 9.1(2)	9.4(1) 或更高版本
8.6(1)	9.0(4) 或 9.1(2)	9.4(1) 或更高版本
9.0(1)	9.0(4) 或 9.1(2)	9.4(1) 或更高版本
9.0(2) 或更高版本	-	9.4(1) 或更高版本
9.1(1)	9.1(2)	9.4(1) 或更高版本
9.1(2) 或更高版本	-	9.4(1) 或更高版本
9.2(x)	-	9.4(1) 或更高版本
9.3(x)	-	9.4(1) 或更高版本

有关升级的详细步骤，请参阅 9.4升级指南。

遗留的漏洞和已修复的漏洞

此版本的遗留的漏洞和已修复的漏洞可通过思科漏洞搜索工具进行查看。此基于 Web 的工具可让您访问思科漏洞跟踪系统，该系统维护关于此产品和其他思科硬件和软件产品的漏洞信息。

注意：您必须拥有 Cisco.com 帐户才能登录并访问思科漏洞搜索工具。如果没有，您可以注册一个帐户。

有关思科漏洞搜索工具的详细信息，请参阅漏洞搜索工具帮助和常见问题。

遗留的漏洞

每个版本的严重级别为 3 或更高的遗留漏洞列入以下搜索中：

- 7.4(3) 遗留漏洞搜索
- 7.4(2) 遗留漏洞搜索
- 7.4(1) 遗留漏洞搜索

已修复的漏洞

每个版本的所有已修复漏洞列于以下搜索中：

- 7.4(3) 已修复漏洞搜索
- 7.4(2) 已修复漏洞搜索
- 7.4(1) 已修复漏洞搜索

最终用户许可协议

有关最终用户许可协议的信息，请访问 http://www.cisco.com/go/warranty。

相关文档

有关 ASA 的详细信息，请参阅思科ASA 系列文档导航。

获取文档和提交服务请求

有关获取文档、使用思科缺陷搜索工具 (BST)、提交服务请求和收集其他信息的信息，请参阅*思科产品文档更新*，其网址为：http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html。

订用*思科产品文档更新*，其中将所有最新及修订的思科技术文档列为 RSS 源并通过使用阅读器应用将相关内容直接发送至桌面。RSS 源是一种免费服务。