思科 ASDM 7.12(x) 版本说明

Release Notes for Cisco ASDM, 7.12(x)

This document contains release information for Cisco ASDM Version 7.12(x) for the Cisco ASA series.

重要说明

- 将适用于 ASA 5506-X、5508 和 5516-X 的 ROMMON 升级到版本 1.1.15 — 对于这些 ASA 型号有一个新的 ROMMON 版本（2019 年 5 月 15 日）；我们强烈建议您升级到最新版本。要进行升级，请参阅 《ASA 配置指南》https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/general/asa-912-general-config/admin-swconfig.html#task_90917D0EBAC2427487F6F51D21ABC235中的说明。

  注意 ROMMON 升级到 1.1.15 所花费的时间是升级到 ROMMON 上一版本的两倍，大约 15 分钟。升级流程中**请勿**重启设备 。如果升级未在 30 分钟内完成或升级失败，请联系思科技术支持； **请勿**重启或重置设备。

- ASDM 升级向导 — 由于内部更改，该向导仅支持使用 ASDM 7.10(1) 及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。
- 9.12(1) 中的 SSH 安全改进和新默认值 — 请参阅以下 SSH 安全改进：
  - 不再支持 SSH 版本 1；仅支持版本 2。**ssh version 1** 命令将迁移到 **ssh version 2**。
  - 支持 Diffie-Hellman 组 14 SHA256 密钥交换。此设置现在为默认值（**ssh key-exchange group dh-group14-sha256**）。先前默认值为组 1 SHA1。请确保 SSH 客户端支持 Diffie-hellman 组 14SHA256。否则，您可能会看到一个错误，例如“不同意密钥交换算法”。例如，OpenSSH 支持 Diffie-hellman 组 14 SHA256。
  - 支持 HMAC-SHA256 完整性加密。默认值现在是高安全性的密码集（hmac-sha1 和 hmac-sha2-256，如 **ssh cipher integrity high**命令所定义）。先前默认值为介质集。
- 9.10(1) 及更高版本不支持 ASA 5506-X 系列和 ASA 5512-X 上的 ASA FirePOWER 模块 — 由于内存限制，9.10(1) 及更高版本中，ASA 5506-X 系列和 5512-X 不再支持 ASA FirePOWER 模块。您必须保持 9.9(x) 或更低版本以继续使用该模块。仍然支持其他模块类型。如果升级到 9.10(1) 及更高本版，则将流量发送到 FirePOWER 模块的 ASA 配置将被清除；请确保在升级之前备份配置。SSD 上的 FirePOWER 映像及其配置保持不变。如果想要降级，可以从备份复制 ASA 配置以恢复功能。

- NULL-SHA TLSv1 密码已弃用并已从 9.12(1) 中删除 — 因为 NULL-SHA 不提供加密，不再是针对现代威胁的安全保护，所以在 **tls-proxy** 模式命令/选项和 **show ssl ciphers all** 输出中列出 TLSv1 支持的密码时，系统将会删除该密码。**ssl cipher tlsv1 all** 和 **ssl cipher tlsv1 custom NULL-SHA** 命令也将被弃用并删除。
- 9.12(1) 中已启用本地 CA 服务器，并将在后续版本中删除 — 当 ASA 配置为本地 CA 服务器时，系统会启用该服务器以颁发数字证书、发布证书吊销列表 (CRL)，并安全地撤销已颁发的证书。此功能已过时，因此弃用 **crypto ca server** 命令。
- 9.12(1) 中删除了默认信任池 — 为符合 PSB 要求，SEC-AUT-DEFROOT，将从 ASA 映像中删除“默认”受信任 CA 捆绑包。因此， **crypto ca trustpool import default** 和 **crypto ca trustpool import clean default** 命令也会随其他相关逻辑一起删除。但是，在现有部署中的以前使用这些命令导入的证书将保留在原来的位置。
- 9.12(1) 中删除了 **ssl encryption** 命令 — 在 9.3(2) 中，已宣布弃用该命令并将其替换为 **ssl cipher**。在 9.12(1) 中，**ssl encryption** 已删除，不再受支持。

系统要求

本部分列出了运行此版本的系统要求。

ASDM Java 要求

您可以使用 Oracle JRE 8.0 (**asdm-*version*.bin**) 或 OpenJRE 1.8.x (**asdm-openjre-*version*.bin**) 安装 ASDM。

表 *1: ASA* 和 *ASA FirePOWER*：*ASDM* 操作系统和浏览器要求

操作系统	浏览器				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
Microsoft Windows（英文版和日文版）： 10 8 7 Server 2012 R2 Server 2012 Server 2008	支持	支持	不支持	是	8.0	1.8 注释 不支持 Windows 7 32 位
Apple OS X 10.4 及更高版本	不支持	支持	支持	是（仅限 64 位版本）	8.0	1.8

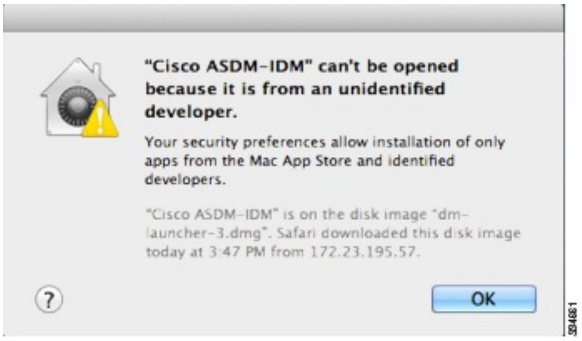
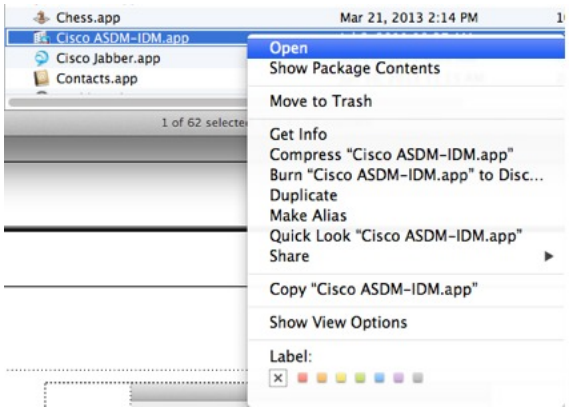
操作系统	浏览器				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
Ubuntu Linux 14.04 Debian Linux 7	不适用	是	不适用	是	8.0	1.8

ASDM 兼容性说明

下表列出了 ASDM 兼容性警告。

条件	说明
ASA 需要有强加密许可证 (3DES/AES) 注释 智能许可模式允许在没有强加密许可证的情况下使用 ASDM 进行初始访问。	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. 转到 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**获取其他许可证 (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。
• 自签证书或不可信任证书 • IPv6 • Firefox 和 Safari	如果 ASA 使用自签证书或不可信任证书，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）。为了避免此警告，请为 ASA 配置一个由可信证书颁发机构签发的正确证书。
• 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。我们建议您重新启用这些算法之一（请参阅**配置 (Configuration)** > **设备管理 (Device Management)** > **高级 (Advanced)** > **SSL 设置 (SSL Settings)** 面板）；或者可以在 Chrome 中使用 **--disable-ssl-false-start** 标记根据使用标记运行 Chromium 禁用 SSL 虚假启动。

条件	说明
服务器专用 IE9	对于服务器中的 Internet Explorer 9.0，默认情况下“**不将加密的页面保存到磁盘 (Do not save encrypted pages to disk)**”选项处于启用状态（请参阅**工具 (Tools)** > **Internet 选项 (Internet Options)** > **高级 (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。

条件	说明
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，将会出现一个错误窗口。  1. 要使 ASDM 运行，请右击（或者按住 Ctrl 点击）思科 ASDM-IDM 启动程序图标，然后选择**打开 (Open)**。  2. 随即将会出现一个类似的错误窗口；但您可以通过该窗口打开 ASDM。点击 **Open**。系统将打开 ASDM-IDM Launcher。 

条件	说明
Windows 10	“此应用无法在您的 PC 上运行”错误消息。 当您安装 ASDM 启动程序时，Windows 10 可能会将 ASDM 快捷方式目标替换为 Windows 脚本主机路径，这会导致此错误。要修复快捷方式目标，请执行以下操作： 1. 依次选择**启动** > **思科 ASDM-IDM 启动程序**，然后右键单击**思科 ASDM-IDM 启动程序**应用。 2. 选择**更多** > **打开文件位置**。 Windows 将打开带有快捷方式图标的目录。 3. 右键单击快捷方式图标，然后选择**属性**。 4. 将**目标**更改为： **C:\Windows\System32\wscript.exe invisible.vbs run.bat** 5. 点击**确定**。

为 ASDM 安装身份证书

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

请参阅安装用于 ASDM 的身份证书在 ASA 上安装适用于 ASDM 的自签名身份证书，并在 Java 中注册该证书。

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

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

过程

步骤 1 转到 ASDM 安装目录，例如 C:\Program Files (x86)\Cisco Systems\ASDM。

步骤 2 使用任意文本编辑器编辑 **run.bat** 文件。

步骤 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。

步骤 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。

过程

步骤 1 右键点击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。

步骤 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。

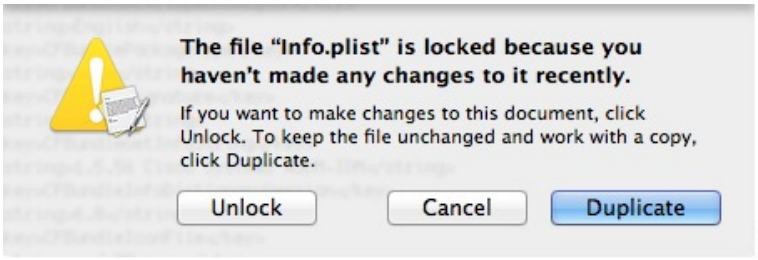
步骤 3 在 **Java** > **VMOptions** 下面，更改前缀为“-Xmx”的字符串以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

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

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


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

步骤 4 如果该文件已锁定，则将看到如下错误：



步骤 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 与 ASDM 兼容性

有关 ASA/ASDM 软件和硬件要求及兼容性信息（包括模块兼容性），请参阅思科 ASA 兼容性。

VPN 兼容性

有关 VPN 兼容性，请参阅 受支持的 VPN 平台和思科 ASA 5500 系列。

新增功能

本部分列出了每个版本的新功能。

注释 系统日志消息指南中列出了新增的、更改的和已弃用的系统日志消息。

ASA 9.12(2)/ASDM 7.12(2) 的新功能

发布日期：2019 年 5 月 30 日

特性	说明
Firepower 9300 SM-56 支持	引入了以下安全模块：SM-56。 需要 FXOS 2.6.1.157 未修改任何菜单项。
ASDM 功能	
ASDM 的 OpenJRE 版本	您可以安装使用 OpenJRE 1.8.x 而不是 Oracle JRE 的 ASDM 版本。OpenJRE 版本的文件名为 **asdm-openjre-*version*.bin**。
工具 > **首选项**选项，用于指定 ASA FirePOWER 模块本地管理文件文件夹	现在，您可以指定安装 ASA FirePOWER 模块本地管理文件的位置。您必须具有已配置位置的读/写权限。 新的/修改后的屏幕： **工具** > **首选项** > **SFR 位置向导**区域

ASA 9.12(1)/ASDM 7.12(1) 的新功能

发布日期：2019 年 3 月 13 日

特性	说明
平台功能	

特性	说明
适用于 Firepower 4115、4125 和 4145 的 ASA	我们推出了 Firepower 4115、4125 和 4145。 需要 FXOS 2.6.1。 未修改任何菜单项。
支持在同一个 Firepower 9300 上使用独立的 ASA 和 FTD 模块	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 FTD 逻辑设备。 需要 FXOS 2.6.1。 未修改任何菜单项。
Firepower 9300 SM-40 和 SM-48 支持	引入了以下两个安全模块：SM-40 和 SM-48。 需要 FXOS 2.6.1。 未修改任何菜单项。
防火墙功能	
支持 GTPv1 版本 10.12。	系统现在支持 GTPv1 版本 10.12。以前，系统支持版本 6.1。在支持新版本后，系统可以多识别 25 种 GTPv1 消息以及 66 种信息元素。 此外，系统行为也有所变化。现在，系统可以接受任何未知的消息 ID。而在过去，未知消息会被丢弃并记入日志。 未修改任何菜单项。
思科 Umbrella 增强功能。	您现在可以标识需要绕过思科 Umbrella 的本地域名。发向这些域的 DNS 请求将直接流向 DNS 服务器，而不经过 Umbrella 处理。此外，您还可以标识用于解析 DNS 请求的 Umbrella 服务器。最后，您可以定义 Umbrella 检测策略以实现故障时自动开放，以确保 Umbrella 服务器不可用时，DNS 请求不会被阻止。 新增/修改的菜单项：**配置** > **防火墙** > **对象** > **Umbrella**、**配置** > **防火墙** > **对象** > **检测映射** > **DNS**。
现在，对象组搜索阈值将默认禁用。	在以前，如果您启用对象组搜索功能，此功能将受阈值限制，这是为了防止性能出现下降。该阈值现在默认将被禁用。您可以使用 **object-group-search threshold** 命令启用该阈值。 更改了以下菜单项：**配置** > **访问规则** > **高级**。
NAT 端口块分配的临时日志。	当对 NAT 启用端口块分配功能后，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志，系统会按您指定的时间间隔生成消息 305017。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。 新增/修改的菜单项：**配置** > **防火墙** > **高级** > **PAT 端口块分配**。
VPN 功能	

特性	说明
适用于 **debug aaa** 的新 **condition** 选项。	我们为 **debug aaa** 命令添加了 **condition** 选项。利用该选项，您可以根据组名、用户名或对等 IP 地址筛选 VPN 调试结果。 未修改任何菜单项。
IKEv2 中支持 RSA SHA-1	现在，您可以使用 RSA SHA-1 散列算法为 IKEv2 生成签名。 新建/修改的菜单项：
查看 DES 和3DES 加密许可证的默认 SSL 配置以及可用密码	现在，您在有无 3DES 加密许可证的情况下均可查看默认 SSL 配置。此外，您还可以查看设备上支持的所有密码。 新增/修改的命令：**show ssl information** 未修改任何菜单项。
将子域添加到 webVPN HSTS	允许域所有者提交应包含在 Web 浏览器的 HSTS 预载列表中的那些域。 新建/修改的菜单项： **配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 代理 > 启用 HSTS 子域**字段
高可用性和扩展性功能	
适用于集群的每站点免费 ARP	现在，ASA 可以生成免费 ARP (GARP) 数据包，以确保交换基础设施始终处于最新状态：它将作为每个站点优先级最高的成员，定期生成流向全局 MAC/IP 地址的 GARP 流量。当使用来自群集的各站点 MAC 和 IP 地址数据包使用站点特定的 MAC 地址和 IP 地址时，群集接收的数据包使用全局 MAC 地址和 IP 地址。如果流量不是定期从全局 MAC 地址生成的，您的全局 MAC 地址交换机上可能会出现 MAC 地址超时。发生超时后，以全局 MAC 地址为目标的流量将在整个交换基础设施中进行泛洪，这有可能造成性能和安全问题。当您为每台设备设置站点 ID 和为每个跨区以太网通道设置站点 MAC 地址时，默认情况下会启用 GARP。 新增/修改的菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 群集 > 群集配置 > 站点周期 GARP** 字段
路由功能	

特性	说明
OSPF 密钥链支持身份验证	OSPF 可对使用 MD5 密钥邻居和路由更新进行身份验证。在 ASA 中，用于生成 MD5 摘要的密钥没有与之关联的生存期。因此，需要用户干预以定期更改密钥。为克服这种限制，OSPFv2 支持使用轮换密钥进行 MD5 身份验证。 根据密钥链中密钥的接受和发送有效期限，OSPF 进行身份验证、接受或拒绝密钥，形成邻接关系。 新增/修改的屏幕： • **配置** > **设备设置** > **密钥链** • **配置** > **设备设置** > **路由** > **OSPF** > **设置** > **身份验证** • **配置** > **设备设置** > **路由** > **OSPF** > **设置** > **虚拟链路**
证书功能	
用于注册 URL 的本地 CA 可配置 FQDN	要使注册 URL 的 FQDN 可配置，而不是使用 ASA 的已配置 FQDN，引入新的 CLI 选项。此新选项将添加到 **crypto ca server**的 **smpt** 模式中。 新增/修改的命令：**fqdn**
管理、监控和故障排除功能	
enable 登录时需要更改密码	**enable** 默认密码为空。现在，如果您尝试在 ASA 上进入特权 EXEC 模式，系统会要求您将密码改为一个至少包含 3 个字符的值，而不能将密码留空。**no enable password** 命令今后将不受支持。 在 CLI 中，您可以使用 **enable** 命令、**login** 命令（用户权限级别应在 2 级以上）或者 SSH 或 Telnet 会话（如果启用 **aaa authorization exec auto-enable**）来进入特权 EXEC 模式。无论使用哪种方法，您都必须设置密码。 但是在登录 ASDM 时，则没有这项更改密码的要求。默认情况下，在 ASDM 中，您无需使用用户名和 **enable** 密码即可登录。 未修改任何菜单项。
可配置管理会话限制	现在，您可以配置汇聚管理会话数、每用户管理会话数和每协议管理会话数的最大值。以前，您只能配置汇聚会话数。此功能不会影响控制台会话。需要注意的是，在多情景模式下，如果最大 HTTPS 会话数固定为 5，则无法配置会话数。此外，系统配置中也不再接受 **quota management-session** 命令，您只能在情景配置中进行此设置。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。 新增/修改的菜单项：**配置** > **设备管理** > **管理访问** > **管理会话配额**

特性	说明
管理权限级别更改通知	现在，在您授予访问权限 (**aaa authentication enable console**) 或允许直接进行特权 EXEC 访问 (**aaa authorization exec auto-enable**) 后，如果用户已分配的访问权限级别在上次登录后发生更改，ASA 会向用户显示通知。 新建/修改的菜单项： **状态栏 > 登录历史记录**图标
支持对 NTP 使用 IPv6 地址	现在，您在设置 NTP 服务器时可以使用 IPv6 地址。 新增/修改的菜单项：**配置 > 设备设置 > 系统时间 > NTP > 添加**按钮 **> 添加 NTP 服务器配置**对话框
SSH 增强安全性	请参阅以下 SSH 安全改进： • 不再支持 SSH 版本 1；仅支持版本 2。 • 支持 Diffie-Hellman 组 14 SHA256 密钥交换。此设置现在为默认值。先前默认值为组 1 SHA1。 • 支持 HMAC-SHA256 完整性加密。默认值现在是高安全性的密码集（hmac-sha1 和 hmac-sha2-256）。先前默认值为介质集。 新增/修改的屏幕： • **配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH** • **配置 > 设备管理 > 高级 > SSH 密码**
允许基于非浏览器的 HTTPS 客户端访问 ASA	您可以允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。 新增/修改的屏幕。 **配置 > 设备管理 > 管理访问 > HTTP 非浏览器客户端支持**
仅在群集控制链路上捕获控制平面数据包	现在，您仅可以在群集控制链路上捕获控制平面数据包（无数据平面数据包）。此选项在多情景模式下的系统中很有用，在此模式下，您无法使用 ACL 来匹配流量。 新建/修改的菜单项： **向导 > 数据包捕获向导 > 群集选项**
debug conn 命令	添加 **debug conn** 命令是为了提供两个记录连接处理的历史记录机制。第一个历史记录列表是一个记录线程操作的每线程列表。第二个历史记录列表是将操作记录到 conn 组中的列表。启用连接后，连接锁、解锁和删除等处理事件将记录到两个历史记录列表中。当出现问题时，可以使用这两个列表来回顾处理情况，以确定不正确的逻辑。 新增/修改的命令：**debug conn**

特性	说明
show tech-support 包括其他输出	**show tech-support** 的输出已得到增强，可以显示以下内容的输出： • **show ipv6 interface** • **show aaa-server** • **show fragment** 新增/修改的命令：**show tech-support**
ASDM 支持，用于在 SNMP 审核操作期间启用和禁用可用内存和已用内存统计信息的结果	为避免 CPU 资源的过度占用，您可以启用和禁用通过 SNMP 审核操作收集的可用内存和已用内存统计数据的查询。 新增或修改的菜单项：**配置** > **设备管理** > **管理访问** > **SNMP**
在多情景模式下，适用于系统的 ASDM 主窗格的可配置图形更新间隔	对于多情景模式下的系统，您现在可以在“主页”窗格上设置图表更新之间间隔的时间量。 新增/修改的屏幕： **工具** > **首选项** > **系统情景中图形用户时间间隔**

升级软件

本节提供了升级路径信息以及用来完成升级的链接。

ASA 升级路径

要查看您当前的版本和型号，请使用以下方法之一：

- CLI — 使用 **show version** 命令。
- ASDM — 选择**主页** > **设备控制面板** > **设备信息**。

请参阅下表以获取您的版本的升级路径。某些早期版本需要先进行中间升级，然后才能升级到较新版本。建议的版本以**粗体显示**。

当前版本	临时升级版本	目标版本
9.10(x)	—	以下任何一个： **→ 9.12(x)** **→ 9.10(x)**

当前版本	临时升级版本	目标版本
9.9(x)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)**
9.8(x)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)**
9.7(x)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x)
9.6(x)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x)

当前版本	临时升级版本	目标版本
9.5(x)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x)
9.4(x)	-	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x)
9.3(x)	-	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x)

当前版本	临时升级版本	目标版本
9.2(x)	-	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x)
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6) 或 9.1(7.4)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

当前版本	临时升级版本	目标版本
9.1(1)	→ 9.1(2)	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
9.0（2）、9.0（3）或9.0（4）	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

当前版本	临时升级版本	目标版本
9.0(1)	→ 9.0(2)、9.0(3) 或 9.0(4)	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.6(1)	→ 9.0(2)、9.0(3) 或 9.0(4)	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6) 或 9.1(7.4)

当前版本	临时升级版本	目标版本
8.5(1)	→ 9.0(2)、9.0(3) 或 9.0(4)	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.4(5+)	—	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

当前版本	临时升级版本	目标版本
8.4(1) 至 8.4(4)	以下任何一个： → 9.0(2)、9.0(3) 或 9.0(4) → 8.4(6)	→ **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.3(x)	→ 8.4(6)	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

当前版本	临时升级版本	目标版本
8.2(x) 及更早版本	→ 8.4(6)	以下任何一个： → **9.12(x)** → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

升级链接

要完成升级，请参阅《 ASA 升级指南》https://www.cisco.com/c/en/us/td/docs/security/asa/migration/upgrade/upgrade.html。

尚未解决和已解决的漏洞

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。

注释 您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果您还没有此帐户，请注册一个帐户。如果您没有思科支持合同，您只能通过 ID 查找缺陷，而无法使用搜索功能。

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及常见问题。

遗留漏洞

本节列出了每个版本的遗留漏洞。

7.12(2) 版本中的遗留漏洞

下表列出了在发布此版本说明时尚未解决的漏洞。

Caveat ID 号码	说明
CSCvo10929	访问列表错误 - 同时取消选中站点到站点 VPN 中的 RSA 签名

7.12(1) 版本中的遗留漏洞

下表列出了在发布此版本说明时尚未解决的漏洞。

Caveat ID 号码	说明
CSCvo10929	访问列表错误 - 同时取消选中站点到站点 VPN 中的 RSA 签名

已修复的漏洞

本部分列出了每个版本的已解决问题。

7.12(2) 版本中已解决的漏洞

下表列出了在发布此版本说明时已解决的选定漏洞。

Caveat ID 号码	说明
CSCvo26166	ASDM 无法将外部组策略应用于 AnyConnect/IKEv1/IKEv2 RA 隧道组
CSCvp01248	ASDM 启动向导上的“接口编辑”按钮不起作用。
CSCvp67520	ASDM 7.12.1：编辑现有的 NAT 规则无法成功推送到 ASA (9.12.1)
CSCvp69678	AnyConnect 映像从 ASDM 消失

7.12(1) 版本中已解决的漏洞

下表列出了在发布此版本说明时已解决的选定漏洞。

Caveat ID 号码	说明
CSCuz09934	ASDM：登录后未显示密码到期警告消息
CSCvi21519	编辑多个 ACL 备注时，ASDM 7.8(2)151“指定的注释不存在”
CSCvi38815	当更改 ACL 行上的日志级别时，ASDM 会删除备注
CSCvi66705	只读用户无法多情景模式下的 ASDM
CSCvi87301	ASDM：未显示ASA 群集详细信息未显示“页面未找到”错误，而是显示管理情景

Caveat ID 号码	说明
CSCvj37182	无法在 ASDM 的启动远程接入 VPN 中启动 DAP
CSCvj91403	通过 ASDM 编辑端口通道时，始终要求 MIO 端口通道 ID
CSCvk71176	ASDM 7.9(2)152 警告“已上传的文件不是有效的 ASA-SM 映像”
CSCvm21655	正在对 ASDM、ACL 备注进行复制，并将其显示在每个子条目中
CSCvm37098	ASDM 尝试在不进行更改的情况下编辑站点到站点隧道，删除 Nat 免除规则
CSCvm64354	ASDM 映像特殊版本的图表更新频率设置为 30 秒
CSCvm68799	ASDM 恢复功能按多个相同的类别文件对覆盖 AC 配置文件的文件执行了覆盖
CSCvn08410	从 CLI 中启用 split-tunnel-all-dns 不会反映在 ASDM 上。从 ASDM 到 CLI 会起作用。
CSCvn20484	如果类映射具有单个规则，则在尝试禁用/否定规则操作时，ASDM 会引发错误
CSCvn32924	在多情景环境上使用 ASDM v7.9.2.X 时，ASA v9.9 (2) 的 ASDM 上不显示 Firepower 选项卡。
CSCvn38874	将 TCT/HTTP 替换为 ACL 上的 IP 时 ASDM 会出现错误
CSCvn72617	ASDM：嵌套的 TCP UDP 对象组未和子对象未列出显示
CSCvo23506	ASDM 在多情景模式下无法打开，显示消息“显示分流信息”

最终用户许可证协议

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

相关文档

有关 ASA 的更多信息，请参阅思科 ASA 系列文档导航。