



多情景模式

本章介绍如何在 ASA 上配置多个安全情景。

- [关于安全情景，第 1 页](#)
- [多情景模式许可，第 11 页](#)
- [多情景模式的先决条件，第 12 页](#)
- [多情景模式准则，第 12 页](#)
- [多情景模式默认设置，第 13 页](#)
- [配置多情景，第 14 页](#)
- [在情景和系统执行空间之间更改，第 22 页](#)
- [管理安全情景，第 23 页](#)
- [监控安全情景，第 26 页](#)
- [多情景模式历史记录，第 29 页](#)

关于安全情景

您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个情景都可以作为独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。有关在多情景模式下不支持的功能，请参阅[多情景模式准则，第 12 页](#)。

本节提供安全情景的概述。

安全情景的公共用途

您可能希望在以下情况下使用多安全情景：

- 您作为运营商，希望向众多客户销售安全服务。通过在 ASA 上启用多个安全情景，可以实施具有成本效益且节约空间的解决方案，这样不仅可以确保所有客户流量的独立性和安全性，还可以简化配置。
- 您所在的组织是一家大型企业或大学校园，并且希望保持各部门完全分隔。
- 您所在的组织是一家企业，需要为不同部门提供不同的安全策略。

- 您需要多个 ASA 的网络。

情景配置文件

本部分介绍 ASA 如何实施多情景模式配置。

情景配置

对于每个情景，ASA 都包括一项配置，用于确定安全策略、接口以及可以在独立设备中配置的所有选项。您可以在闪存中存储情景配置，也可以从 TFTP、FTP 或 HTTP(S) 服务器下载情景配置。

系统配置

系统管理员通过在系统配置（与单模式配置类似的启动配置）中配置每个情景配置位置、分配的接口以及其他情景运行参数，从而添加并管理情景。系统配置可标识 ASA 的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。系统配置中包含一个仅用于故障转移流量的专用故障转移接口。

管理情景配置

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。管理情景必须位于闪存中，而不是远程位置。

如果您的系统已处于多情景模式下，或者您从单模式进行转换，则管理情景会自动在内部闪存中创建名为 `admin.cfg` 的文件。此情景名为“`admin`”。如果您不希望将 `admin.cfg` 用作管理情景，则可以更改管理情景。

ASA 如何对数据包分类

必须对进入 ASA 的每个数据包进行分类，以便 ASA 能够确定将数据包发送到哪个情景。



注释 如果目标 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个情景。

有效分类器条件

本节介绍分类器使用的条件。



注释 对于以接口为目标的管理流量，使用接口 IP 地址进行分类。
不使用路由表对数据包进行分类。

唯一接口

如果仅有一个情景与传入接口相关联，则ASA会将数据包分类至该情景。在透明防火墙模式下，要求情景具有唯一接口，因此总是使用此方法对数据包进行分类。

唯一 MAC 地址

如果多情景共享一个接口，则分类器在每个情景中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一 MAC 地址的情景。您可以启用 MAC 地址的自动生成。在配置每个接口时，您也可以手动设置 MAC 地址。

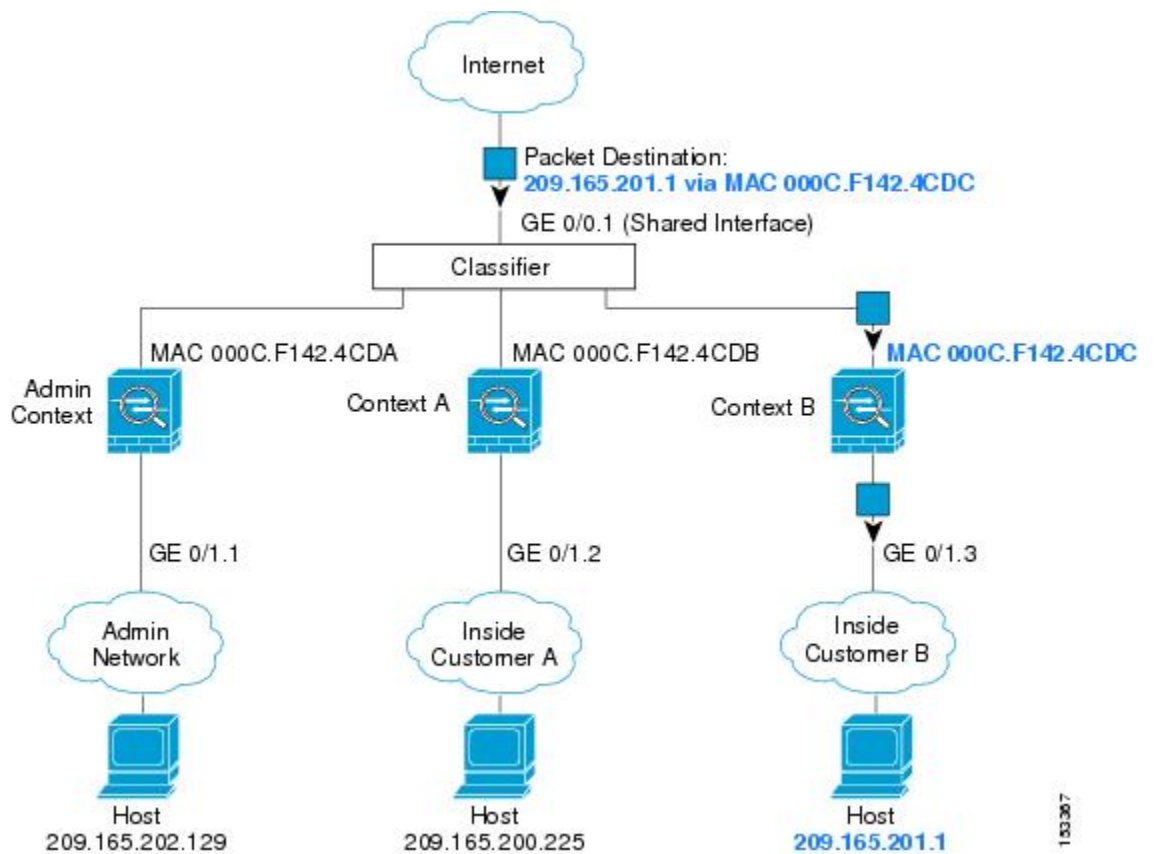
NAT 配置

如果不使用唯一 MAC 地址，ASA 将在您的 NAT 配置中使用映射地址对数据包进行分类。我们建议使用 MAC 地址而不是 NAT，这样，无论 NAT 配置的完整性如何，都可以进行流量分类。

分类示例

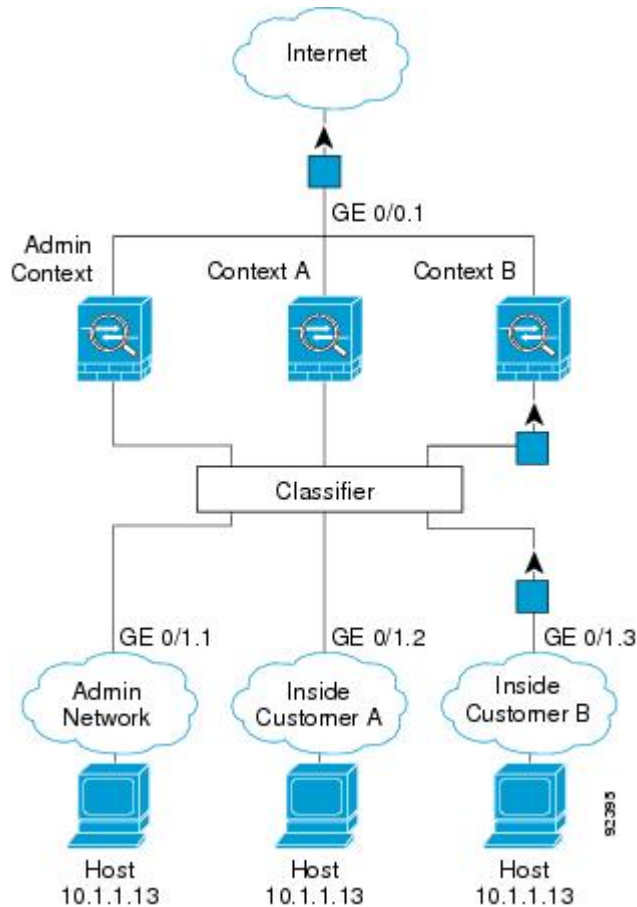
下图显示共享外部接口的多个情景。因为情景 B 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至情景 B。

图 1: 使用 MAC 地址通过共享接口进行数据包分类



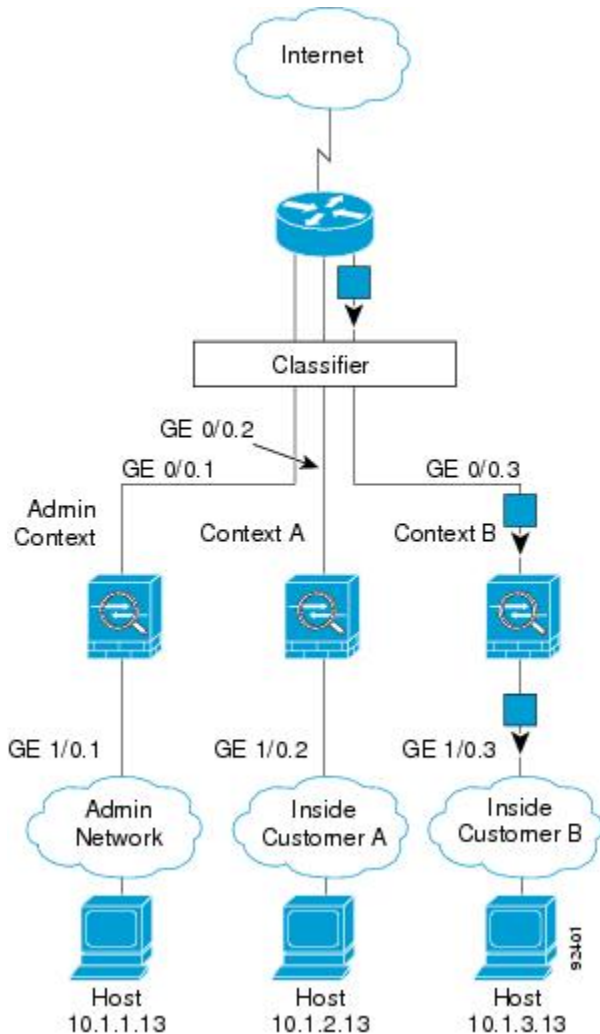
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了情景 B 内部网络上的主机访问互联网。由于传入接口是分配至情景 B 的千兆以太网 0/1.3，因此分类器会将数据包分配至情景 B。

图 2: 来自内部网络的传入流量



对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以情景 B 内部网络上的主机为目标的数据包。由于传入接口是分配至情景 B 的千兆以太网 1/0.3，因此分类器会将数据包分配至情景 B。

图 3: 透明防火墙情景



级联安全情景

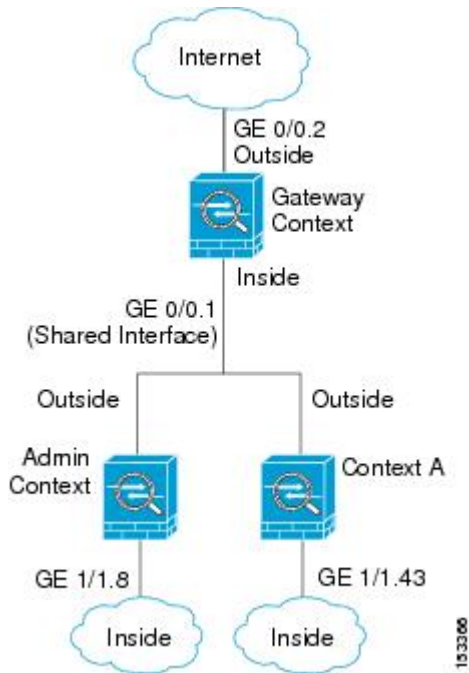
将一个情景直接置于另一情景之前称为级联情景；一个情景的外部接口与另一个情景的内部接口是同一接口。如果您希望通过在顶级情景中配置共享参数，从而简化某些情景的配置，则可能要使用级联情景。



注释 级联情景要求每个情景接口具有唯一 MAC 地址。由于在不具有 MAC 地址的共享接口上对数据包进行分类存在限制，我们不建议在不具有唯一 MAC 地址的情况下使用级联情景。

下图显示了在网关后有两个情景的网关情景。

图 4: 级联情景



对安全情景的管理访问

ASA 提供了多情景模式下的系统管理员访问以及面向单个情景管理员的访问。

系统管理员访问

您可以通过两种方式以系统管理员身份访问 ASA：

- 访问 ASA 控制台。
您可以从控制台访问系统执行空间，这意味着您输入的所有命令仅会影响系统配置或系统的运行（对于运行时命令而言）。
- 使用 Telnet、SSH 或 ASDM 访问管理情景。

作为系统管理员，您可以访问所有情景。

系统执行空间不支持任何 AAA 命令，但是，您可以在本地数据库中配置其自己的启用密码及用户名，以便提供单独的登录。

情景管理员访问

您可以使用 Telnet、SSH 或 ASDM 来访问情景。如果您登录到一个非管理情景，则只能访问该情景的配置。您可以提供该情景的单独登录。

管理接口使用情况

管理接口是一个仅用于管理流量的独立接口。

在路由防火墙模式下，您可以在所有情景中共享管理接口。

在透明防火墙模式下，管理接口是特殊的。除了允许的最大通过流量接口之外，您还可以将管理接口用作单独的仅管理接口。然而，在多情景模式下，您无法跨情景共享任何接口。您可以改为使用管理接口的子接口，并为每个情景分配一个子接口。但是，只有 Firepower 设备型号 允许管理接口上的子接口。ASA 5585-X，必须使用数据接口或数据接口的子接口，并将其添加到情景中的桥接组。

对于 Firepower 4100/9300 机箱透明情景，管理接口和子接口都不会保留其特殊状态。在这种情况下，必须将其视为数据接口，并将其添加到桥接组。（请注意，在单情景模式下，管理接口会保留其特殊状态。）

有关透明模式的另一个注意事项：当您启用多情景模式时，所有配置的接口都会自动分配到管理情景。例如，如果您的默认配置包括管理接口，则该接口将分配给管理情景。一个选项是让主接口分配给管理情景，并使用本地 VLAN 对其进行管理，然后使用子接口管理每个情景。请记住，如果将管理情景设为透明，其 IP 地址将被删除；您必须将其分配给网桥组，并将 IP 地址分配给 BVI。

关于资源管理

默认情况下，除非为每个情景强制设置了最大限制，否则所有安全情景对 ASA 资源的访问都是不受限制的；但 VPN 资源是唯一一种例外情况，这些资源默认是禁用的。例如，如果您发现一个或者多个情景使用了过多资源，并且导致其他情景出现拒绝连接的情况，则您可以配置资源管理来限制每个情景对资源的使用。对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

资源类

ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。要使用某个类的设置，请在定义情景时向该类分配情景。所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。只能将情景分配给一个资源类。此规则的例外是，在成员类中未定义的限制继承自默认类；因此，一个情景实际可能是默认类和另一个类的成员。

资源限制

您可以将单一资源的限制设置为百分比（如果存在硬性系统限制）或绝对值。

对于大多数资源，ASA 不会为分配至该类的每个情景预留部分资源，而是会由 ASA 为情景设置最大限制。如果您超订用资源或允许某些资源不受限制，则少数情景可能会“用尽”这些资源，从而潜在影响为其他情景提供服务。VPN 资源类型除外，您不能超订用此类资源，因此，分配给每个情景的资源量可以得到保证。为应对 VPN 会话数临时激增超过所分配数量的情况，ASA 会支持“突发”VPN 资源类型，其数量等于剩余的未分配 VPN 会话。突发会话可以超订用，并按照先到先得原则供情景使用。

默认类

所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。

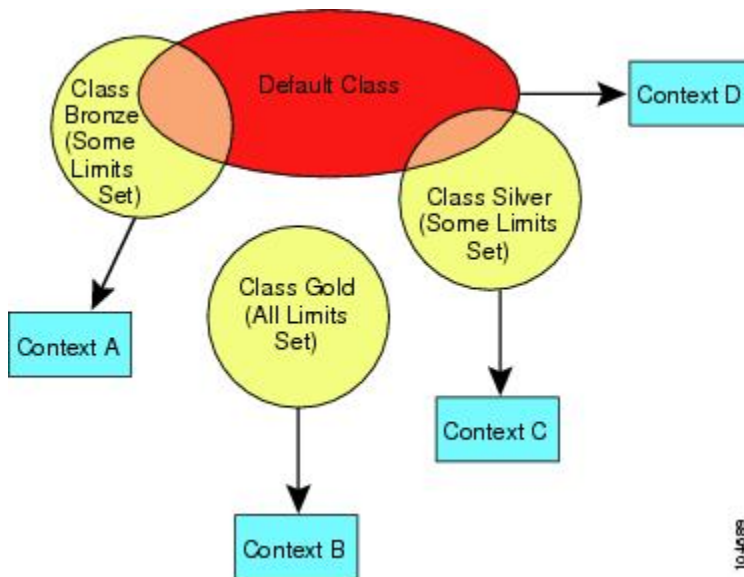
如果某个情景属于除默认类以外的类，则其类设置始终覆盖默认类设置。但是，如果另一个类具有任何未定义的设置，则成员情景为这些限制使用默认类。例如，如果创建的类对所有并发连接具有 2% 的限制，但没有任何其他限制，则所有其他限制都继承自默认类。相反，如果创建对所有资源都有限制的类，则该类不使用默认类中的任何设置。

对于大多数资源，默认类会为所有情景提供无限制的资源访问，但以下限制除外：

- Telnet 会话 - 5 个会话。（每个情景的最大值。）
- SSH 会话 - 5 个会话。（每个情景的最大值。）
- ASDM 会话 - 5 个会话。（每个情景的最大值。）
- IPsec 会话 - 5 个会话（每个情景的最大值。）
- MAC 地址 - （因型号而异）。（系统最大值。）
- Secure Client 对等体 - 0 个会话。（您必须将该类手动配置为允许任何 Secure Client 对等体。）
- VPN 站点间隧道 - 0 个会话。（您必须将该类手动配置为允许任何 VPN 会话。）
- HTTPS 会话 - 6 个会话。（每个情景的最大值。）

下图显示了默认类与其他类之间的关系。情景 A 和 C 属于设置了某些限制的类；其他限制继承自默认类。情景 B 不会从默认类继承任何限制，因为所有限制都在其类（Gold 类）中进行设置。情景 D 未分配给某个类，因此会默认成为默认类的成员。

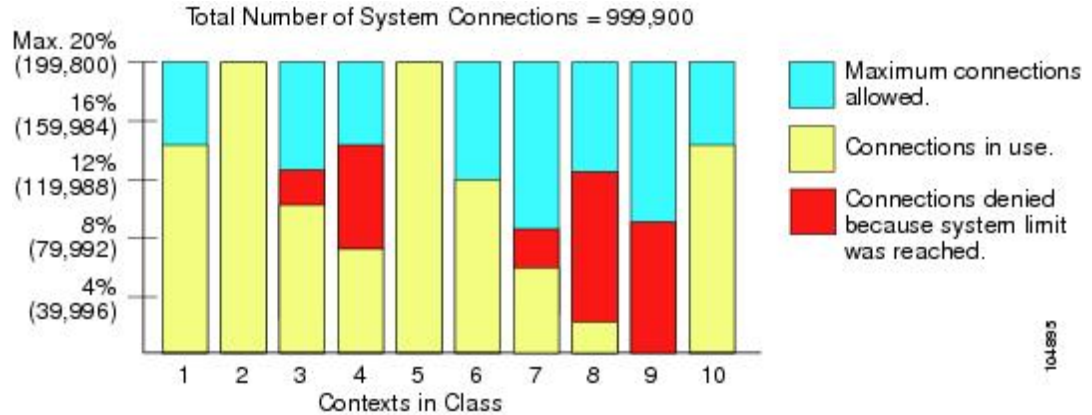
图 5: 资源类



使用超订用资源

您可以通过在所有情景范围内分配超过 100% 的资源（非突发 VPN 资源除外）来超订用 ASA。例如，您可以设置 Bronze 类，以便将连接限制为每个情景 20%，然后将 10 个情景分配给该类（总计 200%）。如果情景并发使用超过系统限制，则每个情景获得的数量少于您希望设置的 20%。

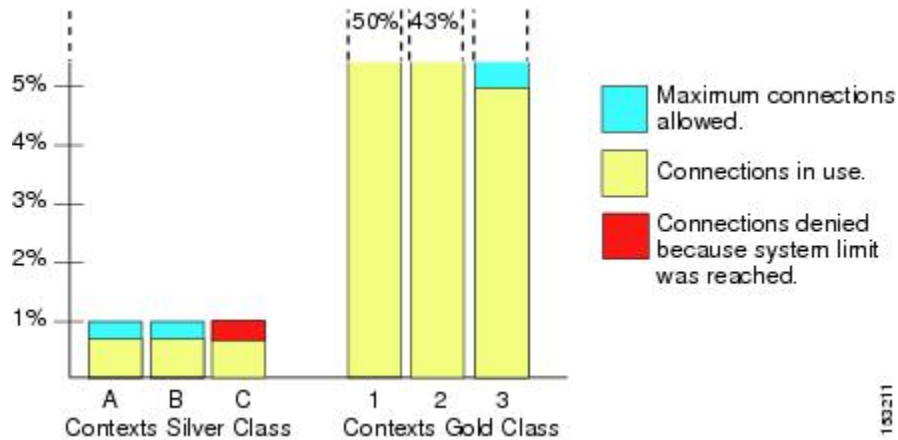
图 6: 资源超订用



使用不受限制的资源

通过 ASA，您可以分配对类中一个或多个资源的不受限制访问权限，而不是只分配一定的百分比或是一个绝对的数字。当资源不受限制时，情景可以使用系统可提供的所有资源。例如，情景 A、B 和 C 属于 Silver 类，该类限制每个类成员可使用 1% 的连接（总计 3%）；但是，三个情景当前仅在使用共计 2% 的连接。Gold 类不限制对连接的访问。Gold 类中的情景可使用超过 97% 的“未分配”连接；它们还可以使用情景 A、B 和 C 当前未使用的 1% 的连接，即使这意味着情景 A、B 和 C 无法达到其 3% 的合并限制。设置不受限制的访问权限类似于超额订用 ASA，只是对您超额订用系统的量不太好控制。

图 7: 不受限制的资源



关于 MAC 地址

您可以手动分配 MAC 地址以覆盖默认值。对于多情景模式，您可以自动生成唯一的 MAC 地址（适用于分配给情景的所有接口）和单情景模式（适用于子接口）。



注释 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

多情景模式下的 MAC 地址

MAC 地址用于在情景中对数据包进行分类。如果您共享某个接口，但在每个情景中没有该接口的唯一 MAC 地址，则可尝试可能不会提供完全覆盖的其他分类方法。

为了允许情景共享接口，您应该为每个共享情景接口启用自动生成虚拟 MAC 地址的功能。

自动 MAC 地址

在多情景模式下，自动生成会为分配给情景的所有接口分配唯一的 MAC 地址。

如果您手动分配 MAC 地址，并且同时启用自动生成，则会使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址（如果已启用）。

在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。

由于自动生成的地址（使用前缀时）以 A2 开头，因此如果您同时希望使用自动生成，则不能使用以 A2 开头的手动 MAC 地址。

ASA 使用以下格式生成 MAC 地址：

A2xx.yyzz.zzzz

其中，xx.yy 是用户定义的前缀或根据接口 MAC 地址的最后两个字节自动生成的前缀，zz.zzzz 是由 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

如何使用前缀的示例如下：如果将前缀设置为 77，则 ASA 会将 77 转换为十六进制值 004D (yyxx)。在 MAC 地址中使用时，该前缀会反转 (xxyy)，以便与 ASA 的本地形式匹配：

A24D.00zz.zzzz

对于前缀 1009 (03F1)，MAC 地址为：

A2F1.03zz.zzzz



注释 没有前缀的 MAC 地址格式是旧式版本。有关传统格式的详细信息，请参阅命令参考中的 `mac-address auto` 命令。

VPN 支持

对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

您可以在多情景模式下使用站点间 VPN。

对于远程访问 VPN，您必须使用 AnyConnect 3.x 及更高版本的 SSL VPN 和 IKEv2 协议。您可以按情景自定义用于 Secure Client 映像和定制的闪存，以及跨所有情景使用共享闪存。有关不支持的功能，请参阅[多情景模式准则](#)，第 12 页。有关每个 ASA 版本支持的 VPN 功能的详细列表，请参阅[多情景模式历史记录](#)，第 29 页。



注释 多情景模式下需要 Secure Client Premier Apex 许可证；您无法使用默认或传统许可证。

多情景模式许可

型号	许可证要求
Firepower 1010	不支持。
Firepower 1100	基础许可证：2 个情景。 可选许可证，最多： <i>Firepower 1120: 5</i> <i>Firepower 1140: 10</i> <i>Firepower 1150: 25</i>
Firepower 2100	基础许可证：2 个情景。 可选许可证，最多： <i>Firepower 2110: 25</i> <i>Firepower 2120: 25</i> <i>Firepower 2130: 30</i> <i>Firepower 2140: 40</i>
Secure Firewall 3100	基础许可证：2 个情景。 可选许可证，最多： <i>Secure Firewall 3110: 100</i> <i>Secure Firewall 3120: 100</i> <i>Secure Firewall 3130: 100</i> <i>Secure Firewall 3140: 100</i>
Firepower 4100	基础许可证：10 个情景。 可选许可证：最多 250 个情景。

型号	许可证要求
Firepower 9300	基础许可证：10 个情景。 可选许可证：最多 250 个情景。
ISA 3000	不支持。
ASA Virtual	不支持。



注释 如果管理情景仅包含管理接口，并且不包括直通流量的任何数据接口，则不计入限制。



注释 多情景模式下需要 Secure Client Premier Apex 许可证；您无法使用默认或传统许可证。

多情景模式的先决条件

在进入多情景模式后，请连接到管理情景，以便访问系统配置。不能在非管理情景配置系统。默认情况下，在启用多情景模式之后，可以使用默认管理 IP 地址连接到管理情景。

多情景模式准则

故障转移

仅在多情景模式下支持主用/主用模式故障转移。

IPv6

跨情景 IPv6 路由不受支持。

不支持的功能

多情景模式不支持以下功能：

- RIP
- OSPFv3。（支持 OSPFv2。）
- 组播路由
- 威胁检测
- 统一通信

- QoS
- 虚拟隧道接口 (VTI)
- 静态路由跟踪

多情景模式当前不支持远程访问 VPN 的以下功能：

- AnyConnect 2.x 及更低版本
- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN 负载均衡
- 可以定制
- L2TP

其他准则

- 情景模式（单情景或多情景）不会存储在配置文件中，即使该模式经过重新启动也是如此。如果您需要将配置复制到另一台设备，请将新设备设置为匹配的模式。
- 如果将情景配置存储在闪存的根目录中，则在某些型号上可能会用尽该目录中的空间，即使有可用内存也是如此。在这种情况下，请为配置文件创建子目录。背景：某些型号使用 FAT 16 文件系统的内部闪存，并且，如果您未使用兼容 8.3 格式的短名称，或使用大写字符，则只能存储少于 512 个的文件和文件夹，因为文件系统会用尽所有插槽来存储长文件名（请参阅 <http://support.microsoft.com/kb/120138/en-us>）。
- 在 ACI 中，使用所有枝叶上的相同 MAC 地址执行基于策略的重定向 (PBR) 运行状况检查 (L2 ping)。这会导致 MAC 摆动。要解决 MAC 摆动问题，可以在内联集上配置分流模式选项。但是，如果威胁防御配置了高可用性，则必须在故障转移期间启用 MAC 获知以进行连接处理。因此，在威胁防御使用内联集接口的高可用性对的 ACI 环境中，为避免丢包，请在独立或集群中部署威胁防御。

多情景模式默认设置

- 默认情况下，ASA 处于单情景模式下。
- 请参阅[默认类](#)，第 7 页。

配置多情景

过程

步骤 1 启用或禁用多情景模式，第 14 页。

步骤 2 （可选）配置用于资源管理的类，第 16 页。

注释 要支持 VPN，必须在资源类中配置 VPN 资源；默认类不允许使用 VPN。

步骤 3 在系统执行空间中配置接口。

- Firepower 1100、设备模式下的 Firepower 2100、Cisco Secure Firewall 3100—[基本接口配置](#)。
- 平台模式下的 Firepower 2100：请参阅《[入门指南](#)》。
- Firepower 4100/9300-[逻辑设备 Firepower 4100/9300](#)

步骤 4 配置安全情景，第 19 页。

步骤 5 （可选）自动为情景接口分配 MAC 地址，第 22 页。

步骤 6 完成情景中的接口配置。请参阅[路由模式接口](#)和[透明模式接口](#)。

启用或禁用多情景模式

根据您从思科订购 ASA 的方式，您的 ASA 可能以针对多个安全情景进行了配置。如果您需要从单模式转换为多模式，请遵循本节中的程序。

如果您使用 High Availability and Scalability Wizard 并启用主用/主用故障转移，则 ASDM 支持将模式从单模式更改为多模式。有关详细信息，请参阅[通过故障转移实现高可用性](#)。如果您不想使用主用/主用故障转移，或者希望切换回单模式，则必须使用 CLI 更改模式；因为更改模式要求确认，不能使用命令行界面工具。本节介绍如何在 CLI 中更改模式。

启用多情景模式

当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件：一个是包含系统配置的新启动配置，另一个是包含管理情景的 `admin.cfg`（位于内部闪存的根目录中）。原始运行配置另存为 `old_running.cfg`（位于内部闪存的根目录中）。系统不会保存原始启动配置。ASA 自动向系统配置中添加一个管理情景的条目，名称为“admin”。

开始之前

如果启动配置与运行配置不同，请备份启动配置。当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件。系统不会保存原始启动配置。请参阅[管理文件](#)。

过程

切换到多情景模式。

mode multiple

示例:

系统将提示您更改模式并转换配置，然后系统将会重新加载。

注释 您必须在管理情景中重新生成 RSA 密钥对，才能重新建立 SSH 连接。在控制台中，输入 **crypto key generate rsa modulus** 命令。有关详细信息，请参阅 [配置 SSH 访问](#)。

示例:

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#

***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

恢复单情景模式

要将旧运行配置复制到启动配置，并将模式切换到单情景模式，请执行以下步骤：

开始之前

在系统执行空间中执行此程序。

过程

步骤 1 将原始运行配置的备份版本复制到当前启动配置：

copy disk0:old_running.cfg startup-config

示例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

步骤 2 将模式设置为单模式：

mode single

示例：

```
ciscoasa(config)# mode single
```

系统将提示您重新启动 ASA。

配置用于资源管理的类

要在系统配置中配置某个类，请执行下述步骤。您可以通过重新输入带有新值的命令来更改特定资源限制的值。

开始之前

- 在系统执行空间中执行此程序。
- 下表列出了资源类型和限制。



注释 如果系统限制为“不适用”，则无法设置该资源的百分比，因为该资源不存在硬性系统限制。

表 1: 资源名称和限制

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
ASDM 会话	并发	1 (最小值) 5 (最大值)	200	ASDM 管理会话。 ASDM 会话使用两个 HTTPS 连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，系统限制为 200 个 ASDM 会话表示 HTTPS 会话数限制为 400。
连接 连接/秒。	并发或速率	不适用	并发连接数：有关适用于您的型号的连接限制，请参阅 每个型号支持的功能许可证 。 速率：不适用	任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。 注释 对于值小于 xlates 或 conns 的任一限制，会生成相应的系统日志消息。例如，如果将 xlates 限制设置为 7 并将 conns 限制设置为 9，则 ASA 仅会生成系统日志消息 321001（“Resource 'xlates' limit of 7 reached for context 'ctx1'”），而不会生成 321002（“Resource 'conn rate' limit of 5 reached for context 'ctx1'”）。
主机数	并发	不适用	不适用	可以通过 ASA 连接的主机数。
检查/秒	Rate	不适用	不适用	每秒应用检测数。
MAC 条目数	并发	不适用	(因型号而异)	对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
路由	并发	不适用	不适用	动态路由数。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
Secure Client 突发	并发	不适用	您型号的 Secure Client 高级对等体数减去为 Secure Client 向所有情景分配的会话总和。	所允许的 Secure Client 会话数超过了分配到某一包含 Secure Client 的情景的会话数。例如，如果您的型号支持 5000 个对等体，而您为包含 Secure Client 的所有情景共分配了 4000 个对等体，则剩余 1000 个对等体可用于 Secure Client Burst。不同于能保证情景会话的 Secure Client，Secure Client Burst 有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
Secure Client	并发	不适用	有关适用于您的型号的 Secure Client 高级对等体数的信息，请参阅 每个型号支持的功能许可证 。	Secure Client 对等体。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的对等体数保证可供相应情景使用。
其他 VPN 突发	并发	不适用	您型号的其他 VPN 会话数量减去为其他 VPN 向所有情景分配的会话总和。	所允许的站点间 VPN 会话数超过了分配到某一包含 Other VPN 的情景的会话数。例如，如果您的产品型号支持 5000 个会话，您为具有其他 VPN 的所有情景分配了 4000 个会话，其余 1000 个会话可用于其他 VPN 突发。不同于能保证情景会话的其他 VPN，其他 VPN 突发有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
其他 VPN	并发	不适用	有关适用于您的型号的其他 VPN 会话数的信息，请参阅 每个型号支持的功能许可证 。	站点间 VPN 会话数。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的会话数保证可供相应情景使用。
在协商的 IKEv1 SA	并发（仅百分比）	不适用	分配到此情景的其他 VPN 会话的百分比。请参阅其他 VPN 资源，为情景分配会话。	传入 IKEv1 SA 协商，占情景其他 VPN 限制的百分比。
SSH	并发	1（最小值） 5（最大值）	100	SSH 会话数。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
存储	MB	最大值取决于您指定的闪存驱动器	最大值取决于您指定的闪存驱动器	情景目录的存储限制 (MB)。
系统日志/秒	Rate	不适用	不适用	每秒系统日志消息数。
Telnet	并发	1 (最小值) 5 (最大值)	100	Telnet 会话数。
Xlate	并发	不适用	不适用	网络地址转换数。

过程

步骤 1 如果您未处于系统配置模式下，请在“设备列表”窗格中，双击主用设备 IP 地址下的“系统”。

步骤 2 依次选择配置 > 上下文管理 > 资源类，然后点击添加。

系统将显示“添加资源类”对话框。

步骤 3 在 **Resource Class** 字段中输入最大长度为 20 个字符的类名。

步骤 4 在 **Count Limited Resources** 区域中，设置资源的并发限制。

有关每个资源类型的描述，请参阅前面的表。

对于没有系统限制的资源，不能设置百分比；只能设置绝对值。如果不设置限制，则会从默认类继承限制。如果默认类不设置限制，则表示资源不受限制，或使用系统限制（如果适用）。对于大多数资源，0 表示将限制设置为不受限制。对于 VPN 类型，0 表示将限制设置为无。

注释 如果您还在情景中设置配置设备管理管理访问管理会话配额以设置最大管理会话数（SSH 等），则将使用较低的值。> > >

步骤 5 在“速率受限资源”区域中，设置资源的速率限制。

有关每个资源类型的描述，请参阅前面的表。

如果不设置限制，则会从默认类继承限制。如果默认类不设置限制，则其在默认情况下不受限制。0 表示将限制设置为不受限制。

步骤 6 点击确定。

配置安全情景

系统配置中的安全情景定义确定情景名称、配置文件 URL、情景可使用的接口以及其他设置。

开始之前

- 在系统执行空间中执行此程序。
- 配置接口。对于透明模式情景，您无法在情景之间共享接口，因此您可能需要使用子接口。要计划管理接口使用，请参阅 [管理接口使用情况](#)，第 7 页。
 - Firepower 1100、设备模式下的 Firepower 2100、Cisco Secure Firewall 3100—[基本接口配置](#)。
 - 平台模式下的 Firepower 2100：请参阅《[入门指南](#)》。
 - Firepower 4100/9300-[逻辑设备 Firepower 4100/9300](#)

过程

步骤 1 如果您未处于系统配置模式下，请在 **Device List** 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2 依次选择配置 > 情景管理 > 安全情景，然后点击添加。

系统将显示 **Add Context** 对话框。

步骤 3 在 **Security Context** 字段中，输入最大长度为 32 个字符的情景名称。

此名称区分大小写，因此您可以具有名为“customerA”和“CustomerA”的两个情景。“System”或“Null”（采用大写或小写字母）是保留名称，因此不能使用。

步骤 4 在 **Interface Allocation** 区域中，点击 **Add** 按钮以为情景分配接口。

a) 从 **Interfaces > Physical Interface** 下拉列表中，选择接口。

您可以分配主接口（在这种情况下，请将子接口 ID 留空），也可以分配与此接口关联的一个子接口或一系列子接口。在透明防火墙模式下，仅会显示尚未分配给其他情景的接口。如果主接口已分配给其他情景，则必须选择子接口。

b) （可选）在 **Interfaces > Subinterface Range** 下拉列表中，选择子接口 ID。

对于子接口 ID 范围，请在第二个下拉列表中选择结束 ID（如果适用）。

在透明防火墙模式下，仅会显示尚未分配给其他情景的子接口。

c) （可选）在别名区域中，选中在情景中使用别名以为要用于情景配置的此接口而不是接口 ID 设置别名。

- 在 **Name** 字段中，输入别名。

别名必须以字母开头，以字母结尾，并且内部字符只能是字母、数字或下划线。此字段允许您指定以字母或下划线结尾的名称；要在名称后面添加可选数字，请在 **Range** 字段中设置数字。

- （可选）在 **Range** 字段中，设置别名的数字后缀。

如果您有一系列子接口，则可以输入要添加到名称之后的数字的范围。

- d) (可选) 选中 **Show Hardware Properties in Context** 以使情景用户可以查看物理接口属性，即使设置了别名也可以。
- e) 点击**确定**返回添加上下文对话框。

步骤 5 (可选) 在 **Resource Assignment** 区域中，从 **Resource Class** 下拉列表中选择一类名称，以将此情景分配给资源类。

可以直接从此区域中添加或编辑资源类。

步骤 6 从 **Config URL** 下拉列表中，选择一个文件系统类型。在此字段中，识别情景配置位置的 URL。例如，FTP 的组合 URL 格式如下：

```
ftp://server.example.com/configs/admin.cfg
```

步骤 7 (可选) 点击 **Login** 以为外部文件系统设置用户名和密码。

步骤 8 (可选) 从 **Failover Group** 下拉列表中，选择组名称以为主用/主用故障转移设置故障转移组。

步骤 9 (可选) 对于 **Cloud Web Security**，点击 **Enable** 以在此情景中启用网络安全检测。要覆盖在系统配置中设置的许可证，请在 **License** 字段中输入许可证。

步骤 10 (可选) 在 **Description** 字段中，添加描述。

步骤 11 (可选) 在 **存储 URL 分配 (Storage URL Assignment)** 区域中，可以允许每个情景使用闪存来存储 VPN 数据包（例如 Secure Client）以及为 Secure Client 和无客户端 SSL VPN 门户自定义提供存储。例如，如果使用多个情景模式来配置具有动态访问策略的 Secure Client 配置文件，则必须计划特定于情景的专用和共享存储。每个情景可使用私有存储空间以及共享的只读存储空间。**注意：**使用 **工具 (Tools) > 文件管理 (File Management)** 确保目标目录在指定的磁盘存在。

a) 选中 **Configure private storage assignment** 复选框，然后从 **Select** 下拉列表中选择私有存储目录。您可以为每个情景指定一个私有存储空间。您可以从情景中的此目录（以及从系统执行空间）执行读取/写入/删除操作。在指定的 path 下，ASA 将在情景后创建一个子目录。例如，对于 contextA，如果指定 **disk1:/private-storage** 作为路径，则 ASA 将在 **disk1:/private-storage/contextA/** 为此情景创建一个子目录。或者，您也可以通过在 **is mapped to** 字段总输入名称在情景内为路径命名，这样文件系统不会暴露给情景管理员。例如，如果您指定映射的名称作为 **context**，则从情景内，此目录称为 **context:**。要控制每个情景允许的磁盘空间量，请参阅[配置用于资源管理的类，第 16 页](#)。

b) 选中 **Configure shared storage assignment** 复选框，然后从 **Select** 下拉列表中选择共享存储目录。您可以对每个情景指定一个只读 **shared** 存储空间，但可以创建多个共享目录。为了减少可以在所有情景之间共享的大型公共文件的副本，例如 Secure Client 包，可以使用共享存储空间。ASA 不会为此存储空间创建情景子目录，因为该存储空间是多个情景的共享空间。只有系统执行空间可以从共享目录写入和删除。

步骤 12 点击**确定**返回到安全上下文窗格。

步骤 13 (可选) 选择情景，并点击**更改防火墙模式**以将防火墙模式设置为透明模式。

如果是新的情景，则没有要擦除的配置。点击**更改模式**切换到透明防火墙模式。

如果是现有情景，则在更改模式之前，请务必备份配置。

注释 不能在 ASDM 中更改当前连接的情景（通常为管理情景）的模式；请参阅[设置防火墙模式（单模式）](#)以在命令行中设置模式。

- 步骤 14** （可选）要自定义 MAC 地址的自动生成，请参阅[自动为情景接口分配 MAC 地址](#)，第 22 页。
- 步骤 15** （可选）选中 **Specify the maximum number of TLS Proxy sessions that the ASA needs to support** 复选框，以指定设备的最大 TLS 代理会话数。有关 TLS 代理的详细信息，请参阅[防火墙配置指南](#)。

自动为情景接口分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。MAC 地址用于在情景中对数据包进行分类。

开始之前

- 当在情景中为接口配置名称时，系统会立即生成新的 MAC 地址。如果在配置情景接口后启用此功能，则在启用之后，会立即为所有接口生成 MAC 地址。如果禁用此功能，则每个接口的 MAC 地址会恢复为默认 MAC 地址。例如，GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。
- 在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以在情景中为接口手动设置 MAC 地址。

过程

-
- 步骤 1** 如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。
- 步骤 2** 依次选择配置 > 情景关管理 > 安全情景，然后选中 **自动生成 Mac 地址**。如果未输入前缀，ASA 根据接口 (ASA 5500-X) 的最后两个字节自动生成前缀。
- 步骤 3** （可选）选中 **Prefix** 复选框，并在字段中输入介于 0 和 65535 之间的一个十进制值。
- 此前缀会转换为一个四位数的十六进制数字，并用作 MAC 地址的一部分。

在情景和系统执行空间之间更改

如果您登录到系统执行空间（或管理情景），则可以在情景之间切换，并在每个情景中执行配置和监控任务。您在配置模式下编辑的运行配置取决于您的位置。当您处于系统执行空间时，运行配置仅包含系统配置；当您处于某个情景时，运行配置仅包含该情景。

过程

-
- 步骤 1** 在 Device List 窗格中，双击主用设备 IP 地址下的 **System** 可配置系统。
- 步骤 2** 在 Device List 窗格中，双击主用设备 IP 地址下的情景名称可配置情景。
-

管理安全情景

本部分介绍如何管理安全情景。

删除安全情景

除非您使用 **clear context** 命令删除所有情景，否则无法删除当前管理情景。



注释 如果使用故障转移，则从主用设备上删除情景到在备用设备上删除该情景之间存在一定延迟。

开始之前

在系统执行空间中执行此程序。

过程

- 步骤 1** 如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。
- 步骤 2** 依次选择配置 > 情景管理 > 安全情景。
- 步骤 3** 选择要删除的情景，然后点击删除 (**Delete**)。
系统将显示 Delete Context 对话框。
- 步骤 4** 如果要以后重新添加此情景，并要保留配置文件以供将来使用，请取消选中 **Also delete config URL file from the disk** 复选框。
如果要删除配置文件，请保持选中该复选框。
- 步骤 5** 点击是 (**Yes**)。

更改管理情景

系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。



注释 对于 ASDM，不能在 ASDM 中更改管理情景，因为 ASDM 会话会断开连接。您可以使用命令行界面工具执行此程序，但请注意，必须重新连接到新的管理情景。

开始之前

- 可以将任何情景设置为管理情景，只要配置文件存储在内部闪存中即可。
- 在系统执行空间中执行此程序。

过程

步骤 1 如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2 依次选择工具 > 命令行界面。

系统将显示 Command Line Interface 对话框。

步骤 3 输入以下命令：

```
admin-context context_name
```

步骤 4 点击发送 (Send)。

连接到管理情景的所有远程管理会话（如 Telnet、SSH 或 HTTPS (ASDM)）都将会终止。必须重新连接到新的管理情景。

注释 某些系统配置命令（包括 **ntp server**）会标识属于管理情景的接口名称。如果您更改管理情景，并且新的管理情景中不存在该接口名称，请务必更新引用该接口的所有系统命令。

更改安全情景 URL

本节介绍如何更改情景 URL。

开始之前

- 在没有通过新的 URL 重新加载配置的情况下，不能更改安全情景 URL。ASA 会将新的配置与当前的运行配置合并。
- 重新输入同一 URL 也可将已保存的配置与运行配置合并。
- 合并会将新配置中的所有新命令添加到运行配置中。
 - 如果配置相同，则不会发生任何更改。

- 如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。如果运行配置为空（例如，如果服务器不可用且从未下载配置），则使用新的配置。
- 如果您不想合并配置，可清除运行配置（该操作通过情景中断所有通信），然后从新的 URL 重新加载配置。
- 在系统执行空间中执行此程序。

过程

步骤 1 如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2 依次选择配置 > 情景管理 > 安全情景。

步骤 3 选择要编辑的情景，点击 **Edit**。

系统将显示 Edit Context 对话框。

步骤 4 在 Config URL 字段中输入新 URL，然后点击 **OK**。

系统会立即加载情景，以便其正常运行。

重新加载安全情景

您可以通过两种方式重新加载情景：

- 清除运行配置，然后导入启动配置。

此操作会清除与情景关联的大多数属性，例如，连接和 NAT 表。

- 从系统配置中删除情景。

此操作会清除其他属性，例如，可能有助于故障排除的内存分配。但是，将情景添加回系统要求重新指定 URL 和接口。

通过清除配置来重新加载

过程

步骤 1 在 Device List 窗格中，双击主用设备 IP 地址下的情景名称。

步骤 2 依次选择工具 > 命令行界面。

系统将显示 Command Line Interface 对话框。

步骤 3 输入以下命令：

clear configure all

步骤 4 点击 **Send**。

系统会清除情景配置。

步骤 5 再次选择工具 > 命令行界面。

系统将显示 Command Line Interface 对话框。

步骤 6 输入以下命令：

copy startup-config running-config

步骤 7 点击 **Send**。

ASA 将重新加载配置。ASA 会从系统配置中指定的 URL 中复制配置。不能在情景中更改此 URL。

通过删除和重新添加情景来重新加载

要通过删除情景再重新添加来重新加载情景，请执行以下步骤。

过程

步骤 1 [删除安全情景，第 23 页](#)。确保取消选中同时从磁盘中删除配置 URL 文件复选框。

步骤 2 [配置安全情景，第 19 页](#)

监控安全情景

本节介绍如何查看和监控情景信息。

监控情景资源使用情况

过程

步骤 1 如果您尚未处于系统模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2 点击工具栏上的 **监控 (Monitoring)** 按钮。

步骤 3 点击情景资源使用 (**Context Resource Usage**)。

点击每种资源类型以查看所有情景的资源使用情况：

- **ASDM/Telnet/SSH** - 显示 ASDM、Telnet 和 SSH 连接的使用情况。

- **Context** - 显示每个情景的名称。
对于每种访问方法，请参阅以下使用情况统计信息：
- **Existing Connections (#)** - 显示现有连接的数量。
- **Existing Connections (%)** - 显示此情景使用的连接数占所有情景使用的连接总数的百分比。
- **Peak Connections (#)** - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，连接数的峰值。

- **Routes** - 显示动态路由的使用情况。
 - **Context** - 显示每个情景的名称。
 - **Existing Connections (#)** - 显示现有连接的数量。
 - **Existing Connections (%)** - 显示此情景使用的连接数占所有情景使用的连接总数的百分比。
 - **Peak Connections (#)** - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，连接数的峰值。

- **Xlates** - 显示网络地址转换的使用情况。
 - **Context** - 显示每个情景的名称。
 - **Xlates (#)** - 显示当前网络地址转换数量。
 - **Xlates (%)** - 显示此情景使用的网络地址转换数占所有情景使用的网络地址转换总数的百分比。
 - **Peak (#)** - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，网络地址转换数的峰值。

- **NATs** - 显示 NAT 规则数。
 - **Context** - 显示每个情景的名称。
 - **NATs (#)** - 显示当前 NAT 规则数。
 - **NATs (%)** - 显示此情景使用的 NAT 规则数占所有情景使用的 NAT 规则总数的百分比。
 - **Peak NATs (#)** - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，NAT 规则数的峰值。

- **Syslogs** - 显示系统日志消息的速率。
 - **Context** - 显示每个情景的名称。
 - **Syslog Rate (#/sec)** - 显示系统日志消息的当前速率。
 - **Syslog Rate (%)** - 显示此情景生成的系统日志消息数占所有情景生成的系统日志消息总数的百分比。

- Peak Syslog Rate (#/sec) - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，系统日志消息的峰值速率。
- VPN - 显示 VPN 站点间隧道的使用情况。
 - Context - 显示每个情景的名称。
 - VPN Connections - 显示有保证的 VPN 会话的使用情况。
 - VPN Burst Connections - 显示突发 VPN 会话的使用情况。
 - Existing (#) - 显示现有隧道的数量。
 - Peak (#) - 显示从上次清除统计信息（使用 **clear resource usage** 命令或因为设备重启）以来，现有隧道数的峰值。

步骤 4 点击刷新 (Refresh) 刷新视图。

查看分配的 MAC 地址

您可以查看系统配置或情景中的自动生成的 MAC 地址。

在系统配置中查看 MAC 地址

本节介绍如何查看系统配置中的 MAC 地址。

开始之前

如果您手动向接口分配 MAC 地址，但也启用了自动生成，则自动生成的地址会继续显示在配置中，即使正在使用的是手动 MAC 地址也如此。如果随后删除手动 MAC 地址，则会使用所显示的自动生成的地址。

过程

步骤 1 如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2 依次选择配置 > 情景管理 > 安全情景，并查看“主 MAC”和“辅助 MAC”列。

查看情景中的 MAC 地址

本节介绍如何查看情景中的 MAC 地址。

过程

步骤 1 如果您未处于系统配置模式下，请在 Device List 窗格中，双击主用设备 IP 地址下的 **System**。

步骤 2 依次选择配置 > 接口，然后查看“MAC 地址”地址列。

此表显示正在使用的 MAC 地址；如果您手动分配 MAC 地址，并且也启用了自动生成，则只能查看系统配置中未使用的自动生成地址。

多情景模式历史记录

表 2: 多情景模式历史记录

功能名称	平台版本	功能信息
多个安全情景	7.0(1)	引入了多情景模式。 引入了以下屏幕：Configuration > Context Management。
自动 MAC 地址分配	7.2(1)	引入了将 MAC 地址自动分配给情景接口的功能。 修改了以下屏幕：Configuration > Context Management > Security Contexts。
资源管理	7.2(1)	引入了资源管理。 引入了以下屏幕：Configuration > Context Management > Resource Management。
适用于 IPS 的虚拟传感器	8.0(2)	运行 IPS 软件版本 6.0 及更高版本的 AIP SSM 可以运行多个虚拟传感器，这意味着您可以在该 AIP SSM 上配置多个安全策略。您可以向一个或多个虚拟传感器分配每个情景或单模式 ASA，也可以向同一个虚拟传感器分配多个安全情景。 修改了以下屏幕：Configuration > Context Management > Security Contexts。
自动 MAC 地址分配增强功能	8.0(2) 8.0(2)	MAC 地址格式更改为使用前缀，以便使用固定起始值(A2)，并在故障转移对中为主设备和辅助设备 MAC 地址使用不同方案。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。 修改了以下屏幕：Configuration > Context Management > Security Contexts。
增加了 ASA 5550 和 5580 的最大情景数量。	8.4(1)	ASA 5550 的最大安全情景数量已从 50 增加到 100。ASA 5580 的最大安全情景数量已从 50 增加到 250。
默认情况下会启用自动 MAC 地址分配。	8.5(1)	现在，默认情况下会启用自动 MAC 地址分配。 修改了以下屏幕：Configuration > Context Management > Security Contexts。

功能名称	平台版本	功能信息
自动生成 MAC 地址前缀	8.6(1)	<p>在多情景模式下，ASA 现在支持将自动 MAC 地址生成配置转换为使用默认前缀。ASA 基于接口 (ASA 5500-X) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。前缀生成方法提供许多好处，包括更好地保证 MAC 地址在网段上的唯一性。如果要更改前缀，可以使用自定义前缀重新配置此功能。传统的 MAC 地址生成方法不再可用。</p> <p>注释 为了保持故障转移对无中断升级，如果已启用故障转移，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。但是，我们强烈建议您在使用故障转移时手动更改前缀生成方法，特别是对于 ASASM。如果没有前缀方法，安装在不同插槽编号的 ASASM 在故障转移时会遇到 MAC 地址变更，并可能会遇到流量中断。升级后，要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址生成来使用前缀。</p> <p>修改了以下屏幕：Configuration > Context Management > Security Contexts</p>
默认所有型号（除 ASASM 之外）上均已禁用自动 MAC 地址分配	9.0(1)	<p>现在，自动 MAC 地址分配默认处于禁用状态（除 ASASM 之外）。</p> <p>修改了以下屏幕：Configuration > Context Management > Security Contexts。</p>
安全情景中的动态路由	9.0(1)	<p>现在，在多情景模式下支持 EIGRP 和 OSPFv2 动态路由协议。不支持 OSPFv3、RIP 和组播路由。</p>
用于路由表条目的新资源类型	9.0(1)	<p>系统创建了新的资源类型 routes，用于设置每个情景中的最大路由表条目数。</p> <p>修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class</p>
多情景模式下的站点间 VPN	9.0(1)	<p>现在，在多情景模式下支持站点间 VPN 隧道。</p>
用于站点间 VPN 隧道的新资源类型	9.0(1)	<p>系统创建了新的资源类型（即 vpn other 和 vpn burst other），用于设置每个情景中站点间 VPN 隧道的最大数量。</p> <p>修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class</p>
SA IKEv1 SA 协商的新资源类型	9.1(2)	<p>创建了新的资源类型 ikev1 in-negotiation，用于在每个情景中设置 IKEv1 SA 协商的最大百分比，以防 CPU 和加密引擎被淹没。在某些情况下（大型证书、CRL 检查），您可能希望限制此资源。</p> <p>修改了以下屏幕：Configuration > Context Management > Resource Class > Add Resource Class</p>

功能名称	平台版本	功能信息
支持多情景模式下的远程访问 VPN	9.5(2)	<p>现在您可在多情景模式中使用以下远程访问功能：</p> <ul style="list-style-type: none"> • AnyConnect 3.x 及更高版本（仅支持 SSL VPN；无 IKEv2 支持） • 集中 Secure Client 映像配置 • Secure Client 映像升级 • 对 Secure Client 连接进行情景资源管理 <p>注释 多情景模式下需要 Secure Client Premier Apex 许可证；您无法使用默认或传统许可证。</p> <p>修改了以下菜单项：配置 > 情景管理 > 资源类 > 添加资源类</p>
多情景模式的 Pre-fill/Username-from-cert 功能	9.6(2)	<p>Secure Client SSL 支持已扩展，允许 pre-fill/username-from-certificate 功能 CLI（以前其仅在单情景模式下可用）在多情景模式下也可启用。</p> <p>未修改任何菜单项。</p>
使用闪存虚拟化实现远程访问 VPN	9.6(2)	<p>多情景模式下的远程访问 VPN 现在支持闪存虚拟化。每个情景都可以根据可用的总闪存拥有专用存储空间和共享存储位置：</p> <ul style="list-style-type: none"> • 专用存储 - 仅存储与该用户关联且特定于您希望该用户具有的内容的文件。 • 共享存储 - 将文件上传到此空间，并且将其启用后，可供任何用户情景进行读/写访问。 <p>修改了以下菜单项：配置 > 情景管理 > 资源类 > 添加资源类 配置 > 情景管理 > 安全情景</p>
在多情景设备中支持 Secure Client 客户端配置文件	9.6(2)	<p>在多情景设备中支持 Secure Client 客户端配置文件要使用 ASDM 添加新配置文件，您必须要有 Secure Client 版本 4.2.00748 或 4.3.03013 及更高版本。</p>
多情景模式下 Secure Client 连接的有状态故障转移	9.6(2)	<p>现在，多情景模式下 Secure Client 连接支持有状态故障转移</p> <p>未修改任何菜单项。</p>
多情景模式下支持远程访问 VPN 动态访问策略 (DAP)	9.6(2)	<p>现在，可以在多情景模式下按情景配置 DAP。</p> <p>未修改任何菜单项。</p>
多情景模式下支持远程访问 VPN CoA（授权更改）	9.6(2)	<p>现在，可以在多情景模式下按情景配置 CoA。</p> <p>未修改任何菜单项。</p>
多情景模式下支持远程访问 VPN 本地化	9.6(2)	<p>支持全局本地化。只有一组跨不同情景共享的本地化文件。</p> <p>未修改任何菜单项。</p>

功能名称	平台版本	功能信息
支持多情景模式下的 IKEv2 远程访问 VPN	9.9(2)	您可以为 IKEv2 配置多情景模式的远程访问 VPN。
可配置管理会话限制	9.12(1)	<p>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。</p> <p>新增/修改的菜单项：配置 > 设备管理 > 管理访问 > 管理会话配额</p>
HTTPS 资源管理	9.12(1)	<p>现在，您可以在资源类中设置非 ASDM HTTPS 会话的最大数量。默认情况下，限制设置为每个情景最多 6 个。在所有情景中最多可使用 100 个 HTTPS 会话。</p> <p>新增/修改的命令：limit-resource http</p> <p>无 ASDM 支持。</p>
Firepower 1140 最大情景数从 5 增加到 10	9.16 (1)	Firepower 1140 现在最多支持 10 个情景。

当地语言翻译版本说明

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