系统配置

本章介绍如何在 Cisco Secure Firewall Management Center上配置系统配置设置。

系统配置的要求和前提条件

型号支持

管理中心

支持的域

全局

用户角色

管理员

管理 Cisco Secure Firewall Management Center 系统配置

系统配置可标识 管理中心 的基本设置。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 使用导航面板选择要更改的配置。

访问列表

您可以按 IP 地址和端口限制对 FMC 的访问。默认情况下，可为任何 IP 地址启用以下端口：

- 443 (HTTPS) 用于 Web 接口访问。
- 22 (SSH) 用于 CLI 访问。

也可以在端口 161 上添加轮询 SNMP 信息的访问权限。由于默认情况下会禁用 SNMP，因此必须先启用 SNMP，然后才能添加 SNMP 访问规则。有关详细信息，请参阅配置 SNMP 轮询，第 58 页。

注意 默认情况下，访问不受限制。要在更安全的环境中操作，请考虑为特定 IP 地址添加访问权限，然后删除默认的 **any** 选项。

配置访问列表

此访问列表不会控制外部数据库访问。请参阅启用对数据库的外部访问，第 21 页。

注意 对于您目前用来连接到 FMC 的 IP 地址，如果您删除了它的访问权限，而且无“`IP=any port=443`”这一条目，您将失去访问权限。

开始之前

默认情况下，访问列表包括 HTTPS 和 SSH 规则。要将 SNMP 规则添加到访问列表，必须先启用 SNMP。有关详细信息，请参阅配置 SNMP 轮询，第 58 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 （可选）如果要将 SNMP 规则添加到访问列表，请点击 **SNMP** 以配置 SNMP。默认情况下，SNMP 处于禁用状态；请参阅 配置 SNMP 轮询，第 58 页。

步骤 3 点击**访问列表 (Access List)**。

步骤 4 要添加对一个或多个 IP 地址的访问权限，请点击**添加规则 (Add Rules)**。

步骤 5 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 6 选择 **SSH**、**HTTPS**、**SNMP** 或其组合，以指定要为这些 IP 地址启用哪些端口。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

相关主题

Firepower 系统 IP 地址约定

访问控制首选项

在 **系统**（⚙）> **配置 (Configuration)** > **访问控制首选项 (Access Control Preferences)** 上配置访问控制首选项。

需要对规则更改添加注释

您可以通过允许（或要求）用户在保存时添加注释来跟踪对访问控制规则的更改。这使您可以快速评估为什么修改了部署中的关键策略。默认情况下，此功能处于禁用状态。

对象优化

将规则策略部署到防火墙设备时，可以配置管理中心以评估和优化在设备上创建关联网络对象组时在规则中使用的网络/主机策略对象。优化会合并相邻网络并删除冗余网络条目。这会减少运行时访问列表数据结构和配置大小，这对某些内存受限的防火墙设备有利。

例如，请考虑包含以下条目并在访问规则中使用的网络/主机对象：

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

启用优化后，在部署策略时，会生成生成的对象组配置：

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

禁用优化时，组配置如下：

```
object-group network test
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

此优化不会更改网络/主机对象的定义，也不会创建新的网络/主机策略对象。如果网络对象组包含另一个网络、主机对象或对象组，则不会合并这些对象。相反，每个网络对象组都单独优化。此外，在部署期间，作为优化过程的一部分，仅修改网络对象组的内联值。

重要事项 在管理中心启用该功能（包括是否通过升级启用）后，在首次部署时在托管设备上进行优化。如果您有大量规则，系统可能需要几分钟到一个小时来评估您的策略并执行对象优化。在此期间，您可能还会发现设备上的CPU使用率更高。禁用该功能后，在第一次部署时会发生类似的情况。启用或禁用该功能后，建议您在影响最小的时候部署，比如维护窗口或流量较低的时段。

此功能受以下支持：

- 在版本 7.4.0 中，默认情况下为重新映像和升级的 管理中心启用此功能。要禁用它，请联系 思科 TAC。
- 在版本 7.4.1+ 中，此功能是可配置的。默认情况下，它会为重新映像的 管理中心启用，但在升级时会考虑您的当前设置。

审核日志

管理中心 以只读审核日志形式记录管理用户的活动。您可以使用多种方式查看审核日志数据：

- 使用 Web 接口： 审核和系统日志。

  审核日志显示在标准事件视图中，您可以依据审核视图中的任何项目查看、排序和过滤审核日志消息。您可以轻松删除和报告审核信息，也可以查看用户所做更改的详细报告。

- 将审核日志消息发送到系统日志： 将审核日志流传输到系统日志，第 5 页。。

- 将审核日志流传输到 HTTP 服务器： 将审核日志流传输到 HTTP 服务器，第 7 页。

将审核日志数据流式传输到外部系统日志或HTTP服务器，可以节省 管理中心 上的空间。 请注意，将审核信息发送到外部 URL 可能会影响系统性能。

或者，您可以确保审核日志流式传输通道安全，可以使用 TLS 证书启用 TLS 和相互身份验证；有关详细信息，请参阅 审核日志 ID证书，第 8 页。

流传输到多个系统日志服务器

您最多可以将审核日志数据传输到五个系统日志服务器。但是，如果为安全审核日志流启用了TLS，则只能将流传输到单个系统日志服务器。

将配置更改流传输到系统日志

您可以通过指定配置数据格式和主机，将配置更改作为审核日志数据的一部分传输到系统日志。管理中心支持备份和恢复审核配置日志。在高可用性的情况下，只有主用管理中心会将配置更改系统日志发送到外部系统日志服务器。日志文件在 HA 对之间同步，以便在故障转移或切换期间，新的主用管理中心将继续发送更改日志。如果 HA 对在裂脑模式下工作，则对中的两个管理中心都会将配置更改系统日志发送到外部服务器。

将审核日志流传输到系统日志

如果启用此功能，审核日志记录会按以下格式显示在系统日志中：

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

其中，本地日期、时间和发起主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如，如果为来自管理中心的审核日志消息指定 `FMC-AUDIT-LOG` 标记，则来自 管理中心 的审核日志消息示例可能如下所示：

```
Mar 01 14:45:24 localhost [FMC-AUDIT-LOG] Dev-MC7000: admin@10.1.1.2, 操作 > 监控，页面查看
```

如果你指定了严重性和设施，这些值不会出现在系统日志消息中；相反，它们会告诉接收系统日志消息的系统如何对它们进行归类。

开始之前

确保 管理中心 可以与系统日志服务器通信。保存配置时，系统使用 ICMP / ARP 和 TCP SYN 数据包验证系统日志服务器是否可访问。然后，默认情况下，系统使用端口 514 / UDP 传输审核日志。如果保护通道 （可选，请参阅 审核日志 ID证书，第 8 页），则必须为 TCP 手动配置端口 1470。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击**审核日志 (Audit Log)**。

步骤 3 从**将审核日志发送到系统日志 (Send Audit Log to Syslog)** 下拉菜单中选择**已启用 (Enabled)**。

步骤 4 以下字段仅适用于发送到系统日志的审核日志：

选项	说明
发送配置更改	要在审核日志流中包含配置更改系统日志，请从下拉列表中选择相关选项： • JSON - 系统日志包括配置更改中的详细差异。 • API - 系统日志包括用于检索配置更改中详细差异的 API。 • 无 - 具有除配置更改详细信息以外的所有其他审核日志。
Host	将审核日志发送到的系统日志服务器的IP地址或完全限定名称。最多可以添加五个系统日志主机，以逗号分隔。 **注释** 仅当为审核服务器证书禁用TLS时，才能指定多个系统日志主机。
设施	创建消息的子系统。 选择 系统日志警报设施中所述的设施。例如，选择审核。
严重性	消息的严重性。 选择如 系统日志严重性级别描述的严重性。
标签	要包含在审核日志系统日志消息中的可选标记。 最佳实践：在此字段中输入值，以轻松区分审核日志消息与其他类似的系统日志消息，例如运行状况警报。 例如，如果要在发送到系统日志的所有审核日志记录之前标为 `FROMMC`，请在字段中输入 `FMC-AUDIT-LOG` 。

步骤 5 （可选）要测试系统日志服务器的IP地址是否有效，请点击 **测试系统日志服务器**。

系统发送以下数据包以验证系统日志服务器是否可访问：

1. ICMP 回应请求
2. 443 和 80 端口上的 TCP SYN

3. ICMP 时间戳查询
4. 随机端口上的 TCP SYN

注释　如果 管理中心 和系统日志服务器位于同一子网中，则使用 ARP 而不是 ICMP。

系统显示每个服务器的结果。

步骤 6 点击**保存 (Save)**。

将审核日志流传输到 HTTP 服务器

如果启用此功能，设备会按以下格式将审核日志记录发送到 HTTP 服务器：

Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action

其中，本地日期、时间和发起主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如，如果指定标记为 FROMMC，则审核日志消息示例可能显示如下：

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

开始之前

确保设备能够与 HTTP 服务器通信。 或者，保护信道；请参阅 审核日志 ID证书，第 8 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志 (Audit Log)**。

步骤 3 或者，在**标记 (Tag)** 字段中，输入要与消息一起显示的标记名称。例如，如果要在所有审核日志记录之前添加 FROMMC，请在字段中输入 FROMMC。

步骤 4 从**将审核日志发送到 HTTP 服务器 (Send Audit Log to HTTP Server)** 下拉列表中选择**启用 (Enabled)**。

步骤 5 在**发送审核的 URL (URL to Post Audit)** 字段中，指定要用于发送审核信息的 URL。输入与将会监听下列 HTTP POST 变量的监听程序相对应的 URL：

- subsystem
- actor
- event_type
- message
- action_source_ip
- action_destination_ip

- `result`
- `time`
- `tag`（如果已定义；请参阅第 3 步）

注意 要允许加密的信息，请使用HTTPS URL。将审核信息发送到外部URL可能会影响系统性能。

步骤 6 点击**保存 (Save)**。

审核日志 ID证书

您可以使用传输层安全（TLS）证书保护 管理中心 和受信任审核日志服务器之间的通信。

客户端证书（需要）

生成证书签名请求（CSR），将其提交给证书颁发机构（CA）进行签名，然后将签名证书导入到管理中心 上。使用本地系统配置： 获取管理中心的已签署的审核日志客户端证书，第 9 页 和 将审核日志客户端证书导入管理中心，第 10 页。

服务器证书（可选）

为了提高安全性，我们建议您在管理中心和审核日志服务器之间进行相互身份验证。为此，请加载一个或多个证书吊销列表（CRL）。您无法将审核日志流传输到在这些CRL中列出的已吊销证书的服务器。

Cisco Secure Firewall 支持以可区别编码规则 (DER) 格式加密的 CRL。请注意，这些是系统用于验证管理中心 Web 界面的 HTTPS 客户端证书的相同 CRL。

使用本地系统配置： 需要有效的审核日志服务器证书，第 11 页。

安全地传输审核日志

如果将审核日志传输到可信的 HTTP 服务器或系统日志服务器，您可以使用传输层安全 (TLS) 证书保护 管理中心 和服务器之间的通道。您必须为要审核的每个设备生成唯一的客户端证书。

开始之前

请参阅审核日志 ID证书，第 8 页，了解所需的客户端和服务器证书信息。

过程

步骤 1 在 管理中心上获取并安装签名的客户端证书：

a) 获取管理中心的已签署的审核日志客户端证书，第 9 页：

根据系统信息和您提供的标识信息从 管理中心 生成证书签名请求 (CSR)。

将 CSR 提交至认可的可信证书颁发机构 (CA) 以请求签名的客户端证书。

如果 管理中心 和审核日志服务器之间需要相互身份验证，则签名客户端证书的 CA 必须与用于连接的服务器证书的签名 CA 相同。

b) 收到证书颁发机构签名的证书后，将其导入到 管理中心中。请参阅将审核日志客户端证书导入管理中心，第 10 页。

步骤 2 配置与服务器之间的通信通道，以使用传输层安全 (TLS) 协议并启用相互身份验证。

请参阅需要有效的审核日志服务器证书，第 11 页。

步骤 3 配置审核日志流，如果尚未执行此操作。

请参阅将审核日志流传输到系统日志，第 5 页或将审核日志流传输到 HTTP 服务器，第 7 页。

获取管理中心的已签署的审核日志客户端证书

重要事项 **审核日志证书**页在高可用性设置的备用 管理中心中不可用。无法从备用 管理中心执行此任务。

系统生成 Base-64 编码的 PEM 格式的证书请求密钥。

开始之前

记住以下几点：

- 为确保安全，请使用全球公认且可信的证书颁发机构 (CA) 签署您的证书。
- 如果您将需要在设备和审核日志服务器之间进行相互身份验证，则同一证书颁发机构必须同时签署客户端证书和服务器证书。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

步骤 3 点击 **Generate New CSR**。

步骤 4 在**国家/地区名称（两字母代码）(Country Name [two-letter code])** 字段中输入国家/地区代码。

步骤 5 在**省/自治区/直辖市 (State or Province)** 字段中输入省/自治区/直辖市的邮编缩写。

步骤 6 输入**地区或城市 (Locality or City)**。

步骤 7 在**组织 (Organization)** 中输入组织名称。

步骤 8 输入**组织单位 (部门)** 名称。

步骤 9 在**公用名 (Common Name)** 字段中输入要为其请求证书的服务器的完全限定域名。

注释 如果公用名和 DNS 主机名不匹配，则审核日志流将失败。

步骤 10 点击**生成 (Generate)**。

步骤 11 使用文本编辑器打开新的空白文件。

步骤 12 复制证书请求中的整个文本块（包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 13 将该文件另存为 *`clientname`*`.csr`，其中，*`clientname`* 是计划使用证书的设备的名称。

步骤 14 点击 **Close**。

下一步做什么

- 将证书签署请求提交到您使用此程序的“开始之前”部分中的指南选择的证书颁发机构。
- 在收到已签署的证书后，请将其导入到设备；请参阅将审核日志客户端证书导入管理中心，第 10 页。

将审核日志客户端证书导入管理中心

在 管理中心 高可用性设置中， 必须 使用主用对等体。

开始之前

- 获取管理中心的已签署的审核日志客户端证书，第 9 页。
- 请确保您正在导入的是正确 管理中心的已签名证书。
- 如果生成证书的签名机构要求您信任某个中间CA，请准备好提供必要的证书链（或证书路径）。签署客户端证书的 CA 与签署证书链中任何中间证书的 CA 必须相同。

过程

步骤 1 在管理中心上，选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

步骤 3 点击**导入审核客户端证书 (Import Audit Client Certificate)**。

步骤 4 在文本编辑器中打开客户端证书，复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。将此文本粘贴到**客户端证书 (Client Certificate)** 字段。

步骤 5 要上传私钥，请打开私钥文件并复制整个文本块，包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行。将此文本粘贴到**私钥 (Private Key)** 字段。

步骤 6 打开任何所需的中间证书，复制整个文本块，然后将其复制到**证书链 (Certificate Chain)** 字段中。

步骤 7 点击**保存 (Save)**。

需要有效的审核日志服务器证书

系统支持使用可区别编码规则 (DER) 格式的导入 CRL 来验证审核日志服务器证书。

注释 如果选择使用 CRL 验证证书，系统将使用相同的 CRL 来验证审核日志服务器证书和用于保护设备和 Web 浏览器之间的 HTTP 连接的证书。

重要事项 您无法在高可用性对中的备用 管理中心 上执行此程序。

开始之前

- 了解需要相互身份验证自己使用证书吊销列表 (CRL) 的后果，确保证书仍然有效。请参阅审核日志 ID证书，第 8 页。
- 按照安全地传输审核日志，第 8 页中的步骤以及该程序中引用的主题获取并导入客户端证书。

过程

步骤 1 在管理中心上，选择**系统**（⚙）>**配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

步骤 3 要使用传输层安全将审核日志安全地流式传输到外部服务器，请选择 **启用 TLS**。

启用 TLS 时，系统日志客户端 (管理中心) 验证从服务器接收的证书。仅当服务器证书验证成功时，客户端和服务器之间的连接才会成功。对于此验证过程，必须满足以下条件：

- 配置系统日志服务器以将证书发送到客户端。
- 向客户端添加（导入）CA 证书以验证服务器证书：
  - 您必须在导入客户端证书期间导入 CA 证书。
  - 如果颁发 CA 是从属 CA，则必须先添加颁发 CA，然后再从从属 CA（根 CA）添加签名 CA，依此类推。

步骤 4 如果您不希望客户端根据服务器对自身进行身份验证，但在证书由同一 CA 颁发时接受服务器证书（不推荐）：

a) 取消选择**启用相互身份验证**。

重要事项 确保服务器配置为信任客户端，而不验证任何客户端证书。

b) 点击**保存**并跳过此过程的其余部分。

步骤 5 （可选）要通过审核日志服务器启用客户端证书验证，请选择 **启用相互身份验证**。

重要事项 仅当启用 TLS 时，**启用相互身份验证** 选项才适用。

启用相互身份验证后，系统日志客户端(管理中心)会将客户端证书发送到系统日志服务器进行验证。客户端使用与系统日志服务器的服务器证书签名的 CA 相同的 CA 证书。仅当客户端证书验证成功时，连接才会成功。对于此验证过程，必须满足以下条件：

- 配置系统日志服务器以验证从客户端收到的证书。
- 添加要发送到系统日志服务器的客户端证书。该证书必须由签署系统日志服务器的服务器证书的 CA 签署。

注释 要使用相互身份验证将审核日志流式传输到系统日志服务器，请对私钥使用 PKCS#8 格式，而不是 PKCS#1 格式。使用以下命令行将 PKCS#1 密钥转换为 PKCS#8 格式：

```
openssl pkcs8 -topk8 -inform PEM -outform PEM
-nocrypt -in PKCS1 key file name -out PKCS8 key filename
```

步骤 6 （可选）要自动识别不再是有效的服务器证书，请执行以下步骤：

a) 选择**启用 CRL 提取**。

重要事项 仅当您选中 **启用相互身份验证** 复选框时，才会显示此选项。但是，仅当启用 TLS 选项时，**启用 CRL 获取** 选项才适用。CRL 用于服务器证书验证，不依赖于用于启用客户端证书验证的相互身份验证。

启用获取 CRL 会为客户端创建一个计划任务，以便定期更新（下载）CRL 或 CRL。CRL 用于服务器证书验证，其中，如果来自 CA 的 CRL 指定要验证的服务器证书已被 CA 吊销，则验证会失败。

b) 输入现有 CRL 文件的有效 URL 并点击**添加 CRL (Add CRL)**。

重复以上步骤以添加 25 个 CRL。

c) 点击**刷新 CRL (Refresh CRL)** 以从指定的 URL 加载当前 CRL。

步骤 7 验证您是否拥有由创建客户端证书的同一证书颁发机构生成的有效服务器证书。

步骤 8 点击**保存 (Save)**。

下一步做什么

（可选）设置 CRL 更新的频率。请参阅配置证书撤销列表下载。

查看管理中心上的审核日志客户端证书

只能查看您登录的设备的审核日志客户端证书。在管理中心高可用性对中，只能在活动对等体上查看证书。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

更改调节

要监控用户进行的更改并确保它们符合您的组织的首选标准，可以将系统配置为通过邮件发送有关过去24小时内进行的更改的详细报告。每当用户保存对系统的配置更改时，就会生成更改快照。更改调节报告将汇总这些快照的信息，以提供最新系统更改的清晰摘要。

以下示例图表显示更改调节报告示例的“用户”部分，并且列出每个配置更改前和更改后的值。如果用户多次更改同一配置，报告会按时间顺序列出每次不同更改的摘要，最近的更改最先列出。

可以查看过去 24 小时内所做的更改。

配置更改调节

开始之前

- 配置邮件服务器，以接收过去 24 小时对系统进行的更改的报告邮件；有关详细信息，请参阅配置邮件中继主机和通知地址，第 20 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**更改调节**。

步骤 3 选中**启用**复选框。

步骤 4 从**运行时间 (Time to Run)** 下拉列表中选择您希望系统每天发出更改调节报告的具体时间。

步骤 5 在**邮件收件人 (Email to)** 字段中输入邮箱地址。

提示 添加邮箱地址后，点击**重新发送上一报告 (Resend Last Report)** 以向收件人发送另一个最新更改调节报告的副本。

步骤 6 如果要包含策略更改，请选中**包含策略配置 (Include Policy Configuration)** 复选框。

步骤 7 如果要包含过去24小时进行的所有更改，请选中**显示完整更改历史记录 (Show Full Change History)** 复选框。

步骤 8 点击**保存 (Save)**。

相关主题

使用审核日志检查更改

更改调节选项

包括策略配置 (Include Policy Configuration) 选项用于控制系统是否在更改调节报告中包括策略更改记录。这包括对访问控制策略、入侵策略、系统策略、运行状况策略和网络发现策略的更改。如果未选择该选项，报告将不会显示对任何策略的更改。此选项仅适用于 管理中心。

显示完整更改历史记录 (Show Full Change History) 选项用于控制系统是否在更改调节报告中包括过去24小时内发生的所有更改的记录。如果未选择该选项，报告仅包括每个类别的更改的整合视图。

注释 更改调节报告不包括对 威胁防御 接口和路由设置的更改。

变更管理

如果您的组织需要实施更加正式的配置更改流程，包括在部署更改之前进行审核跟踪和正式审批，则可以启用“更改管理”。

启用“变更管理”(Change Management) 时，系统会将 **工单**（） 快捷方式添加到菜单栏，并将**变更管理工作流程 (Change Management Workflow)** 添加到 **系统**（） 菜单。用户可以使用这些方法来管理故障单。

有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的“变更管理”一章。

在 **系统**（） > **配置** 页面上，您可以配置以下设置。点击**保存 (Save)** 保存更改。

- **启用更改管理 (Enable Change Management)** - 打开故障单和更改管理工作流程。启用后，您必须批准或放弃所有故障单才能关闭更改管理。

  要禁用该功能，请取消选择该选项。要禁用变更管理，必须批准或丢弃所有故障单。无法禁用变更管理，如果任何故障单处于“进行中”、“暂时搁置”、“已拒绝”或“待审批”状态。

- **需要审批的数量**-要批准和部署故障单，必须有多少管理员批准更改。默认值为 1，但每个故障单最多可以有 5 个审批人。用户可以在创建故障单时覆盖此编号。

注释 当更改管理启用并在使用时，无法更改审批人数量，如果至少有一个故障单处于“进行中”、“暂时搁置”、“已拒绝”或“待审批”状态。要更改所需的审批人数量，必须批准或丢弃所有故障单。

- **故障单清除持续时间**-保留已批准的故障单的天数，范围为 1-100 天。默认值为 5 天。

- **邮件通知**（可选）- 输入 **审批者列表**的 **回复地址** 和组邮件地址。您还必须配置邮件通知系统设置，邮件才能正常工作。

  对于 云交付的防火墙管理中心，不会显示对地址的回复。相反，请在邮件通知系统设置中配置此地址。

备注

有几个系统进程会阻止您启用/禁用更改管理。如果正在执行以下任何操作，则需要等待它们完成后才能更改这些设置：备份/恢复；导入/导出；域移动；升级； Flexconfig 迁移； 设备注册；高可用性注册、创建、中断或切换；集群创建、注册、中断、编辑、添加或删除节点； EPM 中断或加入。

更改这些设置时，无法锁定访问控制策略。如果策略已锁定，则必须等待锁定被释放，然后才能启用/禁用此功能。

DNS 缓存

可以将系统配置为在事件视图页面上自动解析 IP 地址。还可以为设备执行的 DNS 缓存配置基本属性。配置 DNS 缓存让您可以识别之前解析过的 IP 地址，而无需执行额外查找。这样，启用 IP 地址解析后，可以减少网络上的流量并加快事件页面的显示速度。

配置 DNS 缓存属性

DNS 解析缓存是针对整个系统的设置，它允许对以前解析过的 DNS 查找进行缓存。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **DNS 缓存 (DNS Cache)**。

步骤 3 从 **DNS 解析缓存 (DNS Resolution Caching)** 下拉列表中，选择以下选项之一：

- **已启用 (Enabled)** - 启用缓存。
- **已禁用 (Disabled)** - 禁用缓存。

步骤 4 在 **DNS 缓存超时（以分钟为单位）(DNS Cache Timeout [in minutes])** 字段中，输入 DNS 条目在因无活动而被删除前在内存中缓存的分钟数。

默认设置为 300 分钟（5 小时）。

步骤 5 点击**保存 (Save)**。

相关主题

配置事件视图设置

控制面板

控制面板通过使用构件提供当前系统状态的概要视图；构件是一些独立的小组件，可提供有关系统不同方面的信息。系统配置了数个预定义控制面板构件。

您可以配置 管理中心，以便在控制面板上启用“自定义分析”构件。

相关主题

关于控制面板

启用控制面板的自定义分析构件

使用“自定义分析”(Custom Analysis) 控制面板构件，根据灵活的用户可配置查询创建事件的直观表示。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**控制面板 (Dashboard)**。

步骤 3 选中**启用自定义分析构件 (Enable Custom Analysis Widgets)** 复选框以允许用户将“自定义分析”(Custom Analysis) 构件添加到控制面板。

步骤 4 点击**保存 (Save)**。

相关主题

关于控制面板

数据库

为管理磁盘空间，管理中心定期删除设备数据库中的入侵事件、发现事件、审核记录、安全情报数据或 URL 过滤数据。对于每种事件类型，可以指定 管理中心 修剪后保留的记录数；从不依赖包含的任何类型记录数超过为该类型配置的保留限制的事件数据库。为提高性能，应将事件数量限制设置为您通常处理的事件数量。您可以选择在发生修剪时接收邮件通知。对于某些事件类型，可以禁用存储功能。

要手动删除单个事件，请使用事件查看器。（请注意，在版本 6.6.0+ 中，不能以这种方式手动删除连接或安全情报事件。）您还可以手动清除数据库；请参阅 数据清除和存储。

配置数据库事件限制

开始之前

- 如果希望在从 管理中心数据库中删除事件时收到邮件通知，则必须配置邮件服务器，请参阅配置邮件中继主机和通知地址，第 20 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**数据库 (Database)**。

步骤 3 对于每个数据库，请输入要存储的记录的数量。

有关每个数据库可维护的记录的数量，请参阅数据库事件限制，第 17 页。

步骤 4 或者，在**数据修剪通知地址 (Data Pruning Notification Address)** 字段中，输入要接收修剪通知的邮箱地址。

步骤 5 点击**保存 (Save)**。

数据库事件限制

下表列出每个 管理中心可存储的每种事件类型记录的最小和最大数量。

表 *1:* 数据库事件限制

事件类型	上限	下限
入侵事件	1000 万（管理中心虚拟） 3000 万 (管理中心1000, 管理中心1600) 6000 万 (管理中心2500, 管理中心2600, FMCv 300) 3 亿 (管理中心4500, 管理中心4600) 4 亿 (管理中心4700)	10,000
发现事件	1000 万 (管理中心 虚拟) 2000 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	0（禁用存储）

事件类型	上限	下限
连接事件 安全情报事件	5000 万 (管理中心 虚拟) 1 亿 (管理中心1000, 管理中心1600) 3 亿 (管理中心2500, 管理中心2600, FMCv 300) 10 亿 (管理中心4500, 管理中心4600, 管理中心4700) 连接事件和安全情报事件共用数量限制。配置的最大数量总和不能超过此限制。	0（禁用存储） 如果将**最大连接事件 (Maximum Connection Events)** 值设置为零，则未与安全情报、入侵、文件和恶意软件事件关联的连接事件不会存储在 管理中心 上。 **注意** 将 **最大连接事件** 设置为零会立即清除除安全情报事件以外的现有连接事件。 有关此设置对最大流量的影响，请参阅下文。 这些设置不会影响连接摘要。
连接摘要（汇聚连接事件）	5000 万 (管理中心 虚拟) 1 亿 (管理中心1000, 管理中心1600) 3 亿 (管理中心2500, 管理中心2600, FMCv 300) 10 亿 (管理中心4500, 管理中心4600, 管理中心4700)	0（禁用存储）
关联事件和合规 allow 列表事件	100 万 (管理中心 Virtual) 200 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	一个
恶意软件事件	1000 万 (管理中心 Virtual) 200 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	10,000
文件事件	1000 万 (管理中心 虚拟) 200 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	0（禁用存储）
运行状况事件	100 万	0（禁用存储）
审核记录	100,000	一个
补救状态事件	1000 万	一个

事件类型	上限	下限
允许列表违例历史记录	30 天的违例历史记录	1 天的历史记录
用户活动（用户事件）	1000 万	一个
用户登录（用户历史记录）	1000 万	一个
入侵规则更新导入日志记录	100 万	一个
VPN 故障排除数据库	1000 万	0（禁用存储）

最大流速

管理中心 硬件型号的 **最大流量 (Maximum flow rate)**（每秒流量）值在 https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh 的 管理中心 数据表的 **平台规格 (Platform Specifications)** 部分中指定

如果将平台设置中的**最大连接事件数**值设置为零，则不与安全情报、入侵、文件和恶意软件事件关联的连接事件不会计入 管理中心 硬件的最大流量。

此字段中的任何非零值都会导致将所有连接事件计入最大流量。

此页面上的其他事件类型不计入最大流量。

电子邮件通知

如果要执行以下操作，请配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关预定任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 将邮件用于发现事件、影响标志、关联事件警报，入侵事件警报和运行状况事件警报.

配置邮件通知时，可以为系统与邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置后，可以测试连接。

配置邮件中继主机和通知地址

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Email Notification**。

步骤 3 在**邮件中继主机 (Mail Relay Host)** 字段中，输入要使用的邮件服务器的主机名或 IP 地址。输入的邮件主机**必须**允许从设备进行访问。

步骤 4 在**端口号 (Port Number)** 字段，请输入邮件服务器上使用的端口号。

典型的端口包括：

- 25，使用加密时
- 465，使用 SSLv3 时
- 587，使用 TLS 时

步骤 5 在**加密方法 (Encryption Method)** 中选择一种加密方法。

- **TLS** - 使用传输层安全加密通信。
- **SSLv3** - 使用安全套接字层加密通信。
- **无 (None)** - 允许未加密的通信。

注释 设备和邮件服务器之间的加密通信不要求进行证书验证。

步骤 6 在**源地址 (From Address)** 字段，输入要将其用作设备发送消息的源邮箱地址的有效邮箱地址。

步骤 7 或者，要在连接到邮件服务器时提供用户名和密码，请选择**使用身份验证 (Use Authentication)**。在**用户名 (Username)** 字段中输入用户名。在**密码 (Password)** 字段中输入密码。

步骤 8 要使用已配置的邮件服务器发送测试邮件，请点击**测试邮件服务器设置 (Test Mail Server Settings)**。

系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 9 点击**保存 (Save)**。

外部数据库访问

您可以将 管理中心配置为允许第三方客户端对其数据库进行只读访问。这样，您可以通过以下任何方式使用 SQL 来查询数据库：

- 行业标准报告工具（例如，Actuate BIRT、JasperSoft iReport 或 Crystal Reports）
- 其他任何支持 JDBC SSL 连接的报告应用（包括自定义应用）

- 思科提供的命令行 Java 应用，名为 RunQuery，可以交互方式运行或用于获取单一查询的以逗号分隔的结果

使用 管理中心的系统配置启用数据库访问，并创建允许选定主机查询数据库的访问列表。请注意，该访问列表不用于控制设备访问。

您也可以下载包含以下工具的软件包：

- RunQuery（这是思科提供的数据库查询工具）
- InstallCert 工具，可用于从要访问的 管理中心 检索和接受 SSL 证书
- 连接到数据库时必须使用的 JDBC 驱动程序

有关使用下载包中的工具来配置数据库访问的信息，请参阅《《*Firepower* 系统数据库访问指南》》。

启用对数据库的外部访问

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**外部数据库访问 (External Database Access)**。

步骤 3 选中**允许外部数据库访问 (Allow External Database Access)** 复选框。

步骤 4 在**服务器主机名 (Server Hostname)** 字段中输入相应的值。根据第三方应用要求，此值可以是 管理中心的完全限定域名 (FQDN)、IPv4 地址或 IPv6 地址。

注释 在管理中心高可用性设置中，仅输入活动对等体详细信息。我们不建议输入备用对等体的详细信息。

步骤 5 点击 **Client JDBC Driver** 旁边的 **Download** 并按照浏览器提示下载 `client.zip` 软件包。

步骤 6 要为一个或多个IP地址添加数据库访问权限，请点击**添加主机**。此时，**访问列表**字段中将会显示**IP地址**字段。

步骤 7 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 8 点击**添加 (Add)**。

步骤 9 点击**保存 (Save)**。

提示 如果要恢复为上次保存的数据库设置，请点击**刷新 (Refresh)**。

相关主题

Firepower 系统 IP 地址约定

HTTPS 证书

借助安全套接字层(SSL)证书，管理中心可以在系统和Web浏览器之间建立加密通道。所有Firepower设备都随附默认证书，但其不是由任何全球知名的证书颁发机构(CA)所信任的CA生成。因此，请考虑将其替换为由全球知名或内部信任的CA签名的自定义证书。

注意 管理中心支持4096位HTTPS证书。如果管理中心使用的证书是通过大于4096位的公共服务器密钥生成的，则您将无法登录管理中心Web界面。如果出现此情况，请联系思科TAC。

注释 管理中心 REST API不支持HTTPS证书。

默认 HTTPS 服务器证书

如果使用随设备一起提供的默认服务器证书，请不要将系统配置为需要有效的HTTPS客户端证书以访问Web界面，因为默认服务器证书并非由签署客户端证书的CA签署。

默认服务器证书的生命周期取决于证书的生成时间。要查看默认服务器证书到期日期，请选择**系统**（⚙）>**配置**>**HTTPS证书**。

请注意，某些Firepower软件升级可以自动续订证书。有关详细信息，请参阅Firepower热补丁发行说明。

在管理中心上，您可以在**系统**（⚙）>**配置**>**HTTPS证书**页面上续订默认证书。

自定义 HTTPS 服务器证书

您可以使用管理中心Web界面根据系统信息和您提供的识别信息生成服务器证书请求。如果安装有受浏览器信任的内部证书颁发机构(CA)，则可以使用该请求对证书进行签署。您还可以将生成的请求发送到证书颁发机构以请求服务器证书。获得证书颁发机构(CA)的签名证书后，您可以导入该证书。

HTTPS 服务器证书要求

使用HTTPS证书保护Web浏览器和Firepower设备Web界面之间的连接时，必须使用符合互联网X.509公钥基础设施证书和证书撤销列表（CRL）配置文件（RFC 5280）的证书。当您将服务器证书导入设备时，如果该证书不符合该标准的版本3（X.509 v3），则系统会拒绝该证书。

在导入HTTPS服务器证书之前，请确保其包含以下字段：

证书字段	说明
版本	编码的证书的版本。使用版本 3。请参阅 RFC 5280，第 4.1.2.1 节。
序列号	由颁发 CA 分配给证书的正整数。颁发者和序列号唯一标识证书。请参阅 RFC 5280，第 4.1.2.2 节。
签名	CA 用于签署证书的算法的标识符。必须与 signatureAlgorithm 字段匹配。请参阅 RFC 5280，第 4.1.2.3 节。
签发实体	标明签署和签发证书的实体。请参阅 RFC 5280，第 4.1.2.4 节。
有效性	CA 保证其将维护有关证书状态的信息的间隔。请参阅 RFC 5280，第 4.1.2.5 节。
使用者	标识与存储在使用者公钥字段中的公钥关联的实体；必须是X.500可分辨名称（DN）。请参阅 RFC 5280，第4.1.2.6 节。
使用者可选名称	证书保护的域名和 IP 地址。使用者可选名称在 RFC 5280，第 4.2.1.6 节中定义。 如果证书用于多个域或IP地址，我们建议您使用此字段。
对象公钥信息	公钥及其算法的标识符。请参阅 RFC 5280，第 4.1.2.7 节。
授权密钥标识符	提供识别与用于签署证书的私钥对应的公钥的方法。请参阅 RFC 5280，第 4.2.1.1 节。
主体密钥标识符	提供一种识别包含特定公钥的证书的方法。请参阅 RFC 5280，第 4.2.1.2 节。
密钥使用	定义证书中包含的密钥的用途。请参阅 RFC 5280，第 4.2.1.3 节。
基本限制	确定证书主体是否为 CA，以及包括此证书的最大验证认证路径深度。请参阅 RFC 5280，第 4.2.1.9 节。对于 Firepower 设备中使用的服务器证书，请使用 关键 CA：FALSE。

证书字段	说明
扩展密钥使用扩展	表示除“密钥使用”扩展中指示的基本用途之外或替代其用途的已认证公钥的一个或多个用途。请参阅 RFC 5280，第 4.2.1.12 节。请确保导入可用作服务器证书的证书。
signatureAlgorithm	CA 用于对证书签名的算法的标识符。必须与签名字段匹配。请参阅 RFC 5280，第 4.1.1.2 节。
signatureValue	数字签名。请参阅 RFC 5280，第 4.1.1.3 节。

HTTPS 客户端证书

您可以使用客户端浏览器证书检查功能来限制对 Firepower 系统 Web 服务器的访问。启用用户证书时，网络服务器会检查用户的浏览器客户端是否选择了有效的用户证书。此用户证书必须由生成服务器证书的同一个可信证书颁发机构生成。浏览器无法在以下任何情况下加载 Web 界面：

- 用户在浏览器中选择的证书无效。
- 用户在浏览器中选择的证书不是由签署服务器证书的证书颁发机构生成。
- 用户在浏览器中选择的证书不是由设备上的证书链中的证书颁发机构生成。

要验证客户端浏览器证书，请将系统配置为使用在线证书状态协议 (OCSP) 或加载一个或多个证书撤销列表 (CRL)。使用 OCSP，当 Web 服务器接收到连接请求时，它会与证书颁发机构进行通信，以在建立连接之前确认客户端证书的有效性。如果将服务器配置为加载一个或多个 CRL，则 Web 服务器会将该客户端证书与 CRL 中所列的客户端证书进行比较。如果用户选择在 CRL 中列为已撤销证书的证书，则浏览器无法加载 Web 界面。

注释 如果选择使用 CRL 验证证书，则系统会使用相同的 CRL 验证客户端浏览器证书和审核日志服务器证书。

查看当前 HTTPS 服务器证书

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击 **HTTPS Certificate**。

生成 HTTPS 服务器证书签名请求

如果安装不是由全球知名或内部受信任的 CA 签名的证书，则当他们尝试连接 Web 界面时，浏览器会显示安全警告。

证书签名请求 (CSR) 对于生成该证书的设备是唯一的。您无法从单个设备为多个设备生成 CSR。虽然所有字段都是可选的，但我们建议输入以下值：CN、组织、组织单位、城市/区域、省/自治区、国家/地区和使用者可选名称。

为证书请求生成的密钥采用 Base-64 编码的 PEM 格式。

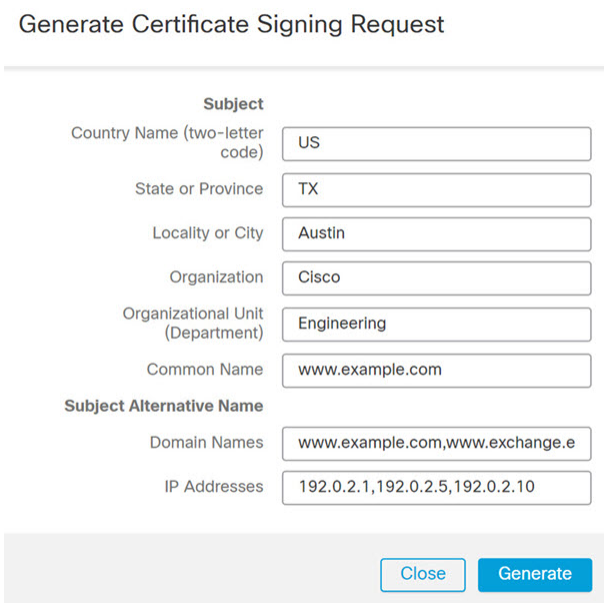
过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 点击 **Generate New CSR**。

下图显示了一个示例。



步骤 4 在**国家/地区名称（两字母代码）(Country Name [two-letter code])** 字段中输入国家/地区代码。

步骤 5 在**省/自治区/直辖市 (State or Province)** 字段中输入省/自治区/直辖市的邮编缩写。

步骤 6 输入**地区或城市 (Locality or City)**。

步骤 7 在**组织 (Organization)** 中输入组织名称。

步骤 8 输入**组织单位 (部门)** 名称。

步骤 9 在**公用名 (Common Name)** 字段中输入要为其请求证书的服务器的完全限定域名。

注释 在**公用名 (Common Name)** 字段中输入与在证书中所显示完全相同的服务器的完全限定域名。如果公用名与 DNS 主机名不匹配，则在连接到设备时会接收到警告。

步骤 10 要请求用于保护多个域名或 IP 地址的证书，请在“使用者可选名称”部分中输入以下信息：

a) **域名**：输入由使用者可选名称保护的完全限定域和子域（如果有）。

b) **IP 地址**：输入由使用者可选名称保护的 IP 地址。

步骤 11 点击**生成 (Generate)**。

步骤 12 打开一个文本编辑器。

步骤 13 复制证书请求中的整个文本块（包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 14 将该文件另存为 *`servername`*`.csr`，其中，*servername* 是计划使用证书的服务器的名称。

步骤 15 点击 **Close**。

下一步做什么

- 将证书请求提交到证书颁发机构。
- 收到签名证书后，请将其导入 管理中心；请参阅 导入 HTTPS 服务器证书，第 26 页。

导入 HTTPS 服务器证书

如果生成证书的签发机构要求您信任某个中间CA，那么您还必须提供一个证书链（即证书路径）。

如果请求了客户端证书，则当服务器证书不符合以下任一条件时，通过 Web 界面访问设备将会失败：

- 证书由签发客户端证书的同一 CA 签名。
- 证书由签发证书链中某个中间证书的 CA 签名。

注意 管理中心 支持 4096 位 HTTPS 证书。如果 管理中心 使用的证书是由大于 4096 位的公共服务器密钥生成的，则您将无法登录 Cisco Secure Firewall Management Center Web 界面。有关将 HTTPS 证书更新到版本 6.0.0 的详细信息，请参阅*Firepower* 系统发行说明，版本 *6.0*中的“将管理中心 HTTPS 证书更新到版本 6.0”。如果要生成或导入 HTTPS 证书且无法登录 管理中心 Web 界面，请联系支持部门。

开始之前

- 生成证书签名请求；请参阅生成 HTTPS 服务器证书签名请求，第 25 页。
- 将 CSR 文件上传至您想要向其请求证书的证书颁发机构，或者使用 CSR 来创建自签证书。
- 确认证书符合 HTTPS 服务器证书要求，第 22 页中所述的要求。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 点击**导入 HTTPS 证书**。

注释　无法导入加密的 HTTPS 证书。

步骤 4 在文本编辑器中打开服务器证书，复制整个文本块（包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行）。将此文本粘贴到**服务器证书 (Server Certificate)** 字段中。

步骤 5 是否需要提供**私钥**取决于您生成证书签名请求的方式：

- 如果使用 Cisco Secure Firewall Management Center Web 界面生成证书签名请求（如生成 HTTPS 服务器证书签名请求，第 25 页中所述），则系统已有私有密钥，您无需在此输入。
- 如果通过其他方式生成证书签名请求，则必须在此提供私有密钥。打开私有密钥文件并复制整个文本块，包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行。将此文本粘贴到**私钥 (Private Key)** 字段。

步骤 6 打开任何所需的中间证书，复制整个文本块，然后将其复制到**证书链 (Certificate Chain)** 字段中。如果收到根证书，请将其粘贴到此处。如果收到中间证书，请将其粘贴到根证书下方。在两种案例下，复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。

步骤 7 点击**保存 (Save)**。

需要有效的 HTTPS 客户端证书

使用此程序可要求连接到 管理中心 Web 界面的用户提供用户证书。系统支持使用 OCSP 或以隐私增强电子邮件 (PEM) 格式导入的 CRL 验证 HTTPS 客户端证书。

如果选择使用 CRL，要确保撤销证书列表是最新的，您可以创建计划任务来更新 CRL。系统显示 CRL 的最新刷新。

注释　要在启用客户端证书后访问 Web 界面，浏览器中**必须**有一个有效客户端证书（或您的阅读器中插入的 CAC）。

开始之前

- 导入由签署用于连接的客户端证书的同一证书颁发机构签署的服务器证书；请参阅导入 HTTPS 服务器证书，第 26 页。
- 必要时导入服务器证书链；请参阅导入 HTTPS 服务器证书，第 26 页。

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 选择**启用客户端证书 (Enable Client Certificates)**。如有提示，请从下拉列表中选择相应的证书。

步骤 4 您会看到三个选项：

- 要用一个或多个 CRL 验证客户端证书，请选择**启用 CRL 获取 (Enable Fetching of CRL)** 并继续执行步骤 5。
- 要使用 OCSP 验证客户端证书，请选择**启用 OCSP** 并跳转至步骤 7。
- 要在不检查撤销的情况下接受客户端证书，请跳转至步骤 8。

步骤 5 输入现有 CRL 文件的有效 URL 并点击**添加 CRL (Add CRL)**。重复以上步骤以添加 25 个 CRL。

步骤 6 点击**刷新 CRL (Refresh CRL)** 以从指定的 URL 加载当前 CRL。

注释 启用 CRL 获取功能可创建定期更新 CRL 的计划任务。编辑任务以设置更新的频率。

步骤 7 验证客户端证书是否由加载到设备上的证书颁发机构签署，以及服务器证书是否由加载到浏览器证书存储区中的证书颁发机构签署。（这些证书的证书颁发机构相同。）

注意 保存已启用客户端证书的配置时，如果在您的浏览器证书存储区中无有效客户端证书，则会禁用对设备的所有 Web 服务器访问。请在保存设置之前确保已安装有效客户端证书。

步骤 8 点击**保存 (Save)**。

相关主题

配置证书撤销列表下载

续订默认 HTTPS 服务器证书

只能查看您登录的设备的服务器证书。

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击 **HTTPS Certificate**。

仅当系统配置为使用默认 HTTPS 服务器证书时，才会显示此按钮。

步骤 3 点击 **续约 HTTPS 证书**。（仅当系统配置为使用默认 HTTPS 服务器证书时，此选项才会显示在证书信息下方的显示屏上。）

步骤 4 （可选）在**续订 HTTPS 证书**对话框中，选择**生成新密钥**以生成证书的新密钥。

步骤 5 在**续订 HTTPS 证书**对话框中，点击**保存**。

下一步做什么

您可以通过检查 **HTTPS 证书**页面上显示的证书有效期是否已更新，来确认证书是否已续订。

信息

Web 界面的 **系统 > 配置** 页面包含下表中列出的信息。除非另有说明，否则所有字段都为只读。

注释 另请参阅 **帮助 > 关于** 页面，其中包含类似但略有不同的信息。

字段	说明
名称	您为 管理中心 设备指定的描述性名称。尽管您可以使用主机名作为设备的名称，但在此字段中输入其他名称不会更改主机名。 此名称用于某些集成。例如，它显示在与 SecureX 和 SecureX 威胁响应集成的设备列表中。 如果更改名称，则所有已注册的设备都将被标记为过期，并且需要部署才能将新名称推送到设备。
产品型号	设备的型号名称。
序列号	设备的序列号。
软件版本	设备上当前安装的软件版本。
操作系统	当前在设备上运行的操作系统。
操作系统版本	当前设备上运行的操作系统的版本。
IPv4 地址	默认 (`eth0`) 管理接口的 IPv4 地址。如果 IPv4 管理处于禁用状态，此字段会予以指出。
IPv6 地址	默认 (`eth0`) 管理接口的 IPv6 地址。如果 IPv6 管理处于禁用状态，此字段会予以指出。
当前策略	当前部署的系统级策略。如果策略自上一次部署以来已更新，则策略的名称以斜体显示。
型号编号	存储在内部闪存驱动器上的设备特定型号。此编号可能对于故障排除非常重要。

入侵策略首选项

配置各种入侵策略首选项，以监控和跟踪部署中关键策略的更改。

设置入侵策略首选项

配置入侵策略首选项。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**入侵策略首选项 (Intrusion Policy Preferences)**。

步骤 3 您有以下选择：

- **有关策略更改的注释 (Comments on policy change)**：当用户修改入侵策略时，选中此复选框可以配置系统以使用注释功能跟踪与策略相关的更改。在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。

  如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，管理中心 都会提示用户输入注释。

- **将入侵策略中的更改写入审核日志 (Write changes in Intrusion Policy to audit log)**：选中此复选框可将入侵策略的更改记录到审核日志中。默认情况下，此选项已启用。

- **保留已删除的 Snort 3 规则的用户覆盖 (Retain user overrides for deleted Snort 3 rules)**：选中此复选框可在 LSP 更新过程中获得任何覆盖系统定义规则的更改通知。如果启用，系统会在 LSP 更新过程中添加的新替换规则中保留规则覆盖。在管理中心菜单栏上，点击**通知 (Notifications)** > **任务 (Tasks)** 以查看通知。默认情况下，此选项已启用。

语言

可以使用 Language 页面为网络界面指定不同的语言。

设置 Web 接口的语言

在该页面上指定的语言将用于每个用户所用的网络接口。您可以选择：

- 英语
- 法语
- 中文（简体）

- 中文（繁体）
- 日语
- 韩语

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Language**。

步骤 3 选择要使用的语言。

步骤 4 点击**保存 (Save)**。

登录标识

可以使用“登录横幅”(Login Banner) 页面为安全设备或共享策略指定会话、登录或自定义消息横幅。

您可以使用 ASCII 字符和回车创建自定义登录横幅。系统不保留制表符间距。如果登录横幅过大或导致错误，则系统尝试显示横幅时 Telnet 或 SSH 会话可能会失败。

自定义登录横幅

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**登录横幅 (Login Banner)**。

步骤 3 在**自定义登录横幅 (Custom Login Banner)** 字段中，输入要使用的登录横幅。

步骤 4 点击**保存 (Save)**。

管理接口

安装后，您可以更改管理网络设置，包括在 管理中心上添加更多管理接口、主机名、搜索域、DNS 服务器和 HTTP 代理。

关于管理中心管理接口

默认情况下，管理中心通过单个管理接口管理所有设备。您还可以对管理接口执行初始设置，并以管理员身份通过该接口登录到管理中心 。管理接口还用于与智能许可服务器通信、下载更新以及执行其他管理功能。

关于设备管理接口的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的关于管理设备接口 。

关于设备管理

在 管理中心 管理设备时，它会在自己和设备之间设置双向、SSL 加密的通信信道。管理中心使用此信道向设备发送有关要如何分析和管理流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到管理中心。

通过使用 管理中心管理设备，您可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向受管设备推送运行状况策略并监控其运行状态 管理中心

注释 如果您有 CDO 托管设备，并且仅将本地部署 管理中心 用于分析，则本地部署 管理中心 不支持策略配置或升级。本指南中与设备配置和其他不支持的功能有关的章节和程序不适用于主管理器为CDO的设备。

管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用 管理中心来管理设备行为的几乎每个方面。

注释 尽管 管理中心 可以按照 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html 处可用的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本 威胁防御 软件的新功能不适用于这些以前发布的设备。某些 管理中心 功能可能适用于早期版本。

管理连接

使用 管理中心 信息配置设备并将设备添加到 管理中心后，设备或 管理中心 可以建立管理连接。根据初始设置：

- 设备或 管理中心 都可以启动。
- 只有设备可以启动。

- 只有 管理中心 可以发起。

启动始终使用 管理中心 上的 eth0 或设备上编号最低的管理接口。如果未建立连接，则会尝试其他管理接口。管理中心 上的多个管理接口可让您连接到离散网络或隔离管理和事件流量。但是，发起方不会根据路由表选择最佳接口。

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。

注释 管理连接是信道自身与设备之间的 TLS-1.3 加密的安全通信信道。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

管理中心上的管理接口

管理中心使用 eth0 接口进行初始设置、对管理员的 HTTP 访问、设备管理，以及其他管理功能（如许可和更新）。

您还可以配置其他管理接口。当管理中心在不同网络上管理大量设备时，添加更多管理接口可以提高吞吐量和性能。还可以将这些接口用于所有其他管理功能。您可能希望将每个管理接口用于特定功能；例如，您可能希望将一个接口用于 HTTP 管理员访问，而将另一个接口用于设备管理。

对于设备管理，管理接口可以承载两个独立的流量隧道：管理流量隧道承载所有内部流量（如特定于管理设备的设备间流量），事件流量隧道承载所有事件流量（如 Web 事件）。可以选择在 管理中心上配置独立的仅事件接口，用于处理事件流量，可以仅配置一个事件接口。您还必须始终具有用于管理流量通道的管理接口。事件流量这能会占用大量带宽，因此将事件流量从管理流量中分离出来可以提高 管理中心的性能。例如，您可以分配一个 10 千兆以太网接口作为事件接口（如果可用），同时将多个 1 千兆以太网接口用于管理。例如，您可能希望在一个完全安全的专用网络上配置一个仅事件接口，同时在一个包括互联网访问的网络上使用常规管理接口。尽管您可以在同一网络上同时使用管理接口和事件接口，但我们建议将每个接口放在单独的网络上，以避免潜在的路由问题，包括从其他设备到 Cisco Secure Firewall Management Center 的路由问题。受管设备会将管理流量发送到管理中心的管理接口，并将事件流量发送到管理中心的仅事件接口。如果受管设备无法访问仅事件接口，则它将回退到将事件发送到管理接口。但是，无法通过仅事件接口建立管理连接。

始终首先从 eth0 尝试从 管理中心 发起管理连接，然后按顺序尝试其他接口；路由表不用于确定最佳接口。

注释 所有管理接口均支持由“访问列表”配置 (配置访问列表 ， 第 3 页)控制的 HTTP 管理员访问。相反，您不能将某个接口限制为仅 HTTP 访问；管理接口始终支持设备管理（管理流量、事件流量或两者）。

注释 仅 eth0 接口支持 DHCP IP 寻址。其他管理接口仅支持静态 IP 地址。

每个管理中心型号的管理接口支持

有关管理接口位置，请参阅您的型号的硬件安装指南。

有关每个管理中心型号上支持的管理接口，请参阅下表。

表 *2:* 管理中心上的管理接口支持

型号	管理接口
MC1000	eth0（默认） eth1
MC2500、MC4500	eth0（默认） eth1 eth2 eth3
MC1600、MC2600、MC4600	eth0（默认） eth1 eth2 eth3 CIMC（仅支持无人值守管理。）
FMC1700、FMC2700、FMC4700	eth0（默认） eth1 eth2 eth3 CIMC（仅支持无人值守管理。）
Management Center Virtual	eth0（默认）

管理中心管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置 管理中心时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。

在某些平台上，可以配置多个管理接口。默认路由不包括出口接口，因此选择的接口取决于您指定的网关地址以及网关属于哪个接口的网络。如果默认网络上有多个接口，设备将使用编号较低的接口作为出口接口。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到 管理中心的路由问题。

注释 用于管理连接的接口不由路由表决定。始终首先使用 eth0 尝试连接，然后按顺序尝试后续接口，直到到达受管设备。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及重新分配源或目标 IP 地址。NAT 最常见的用途是允许专用网络与互联网进行通信。静态 NAT 执行 1:1 转换，这不会引发管理中心与设备的通信问题，但端口地址转换 (PAT) 更为常用。PAT 允许您使用单一的公共 IP 地址和独特端口来访问公共网络；这些端口是根据需要动态分配的，因此您无法启动与 PAT 路由器后的设备的连接。

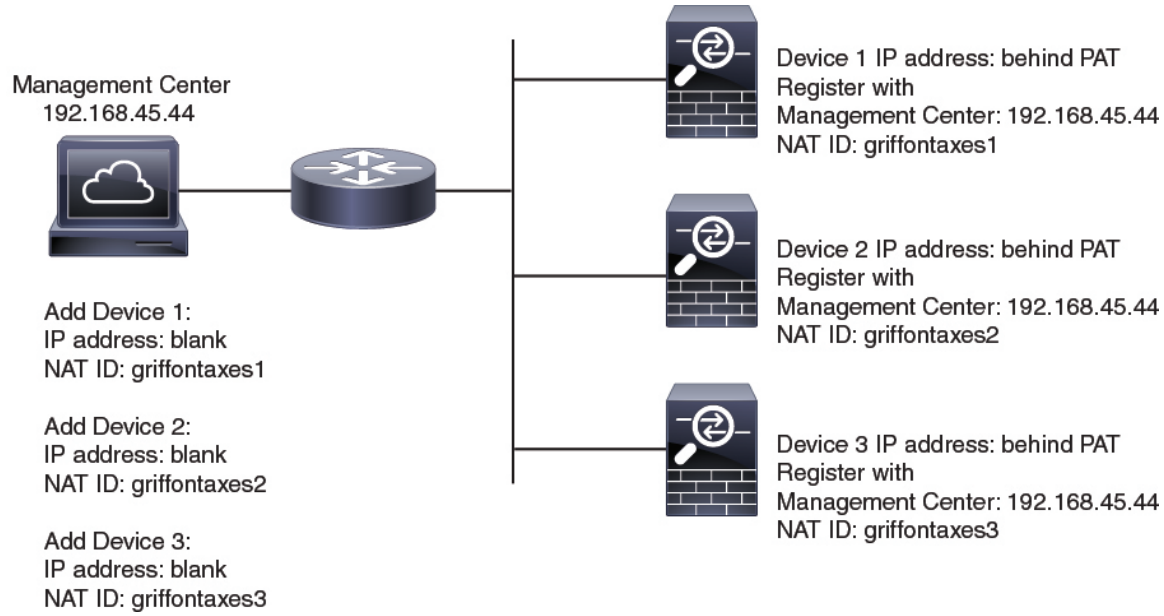
通常，无论是路由目的还是身份验证，都需要两个IP地址（连同一个注册密钥）：管理中心 当添加一个设备时，指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

例如，您将设备添加到 管理中心，但不知道设备 IP 地址（例如，设备在 PAT 路由器后），因此只需要在 管理中心 上指定 NAT ID 和注册密钥；将 IP 地址留空。在设备上，指定 管理中心 IP 地址、相同的 NAT ID 和相同的注册密钥。设备将注册到 管理中心的 IP 地址。此时，管理中心将使用 NAT ID 而不是 IP 地址对设备进行身份验证。

尽管 NAT ID 最常用于 NAT 环境，但您可以选择使用 NAT ID 来简化向 管理中心添加多个设备的过程。在 管理中心上，在将 IP 地址留空的同时为要添加的每个设备指定唯一的 NAT ID，然后在每个设备上指定 管理中心 IP 地址和 NAT ID。注意：每个设备的 NAT ID 必须是唯一的。

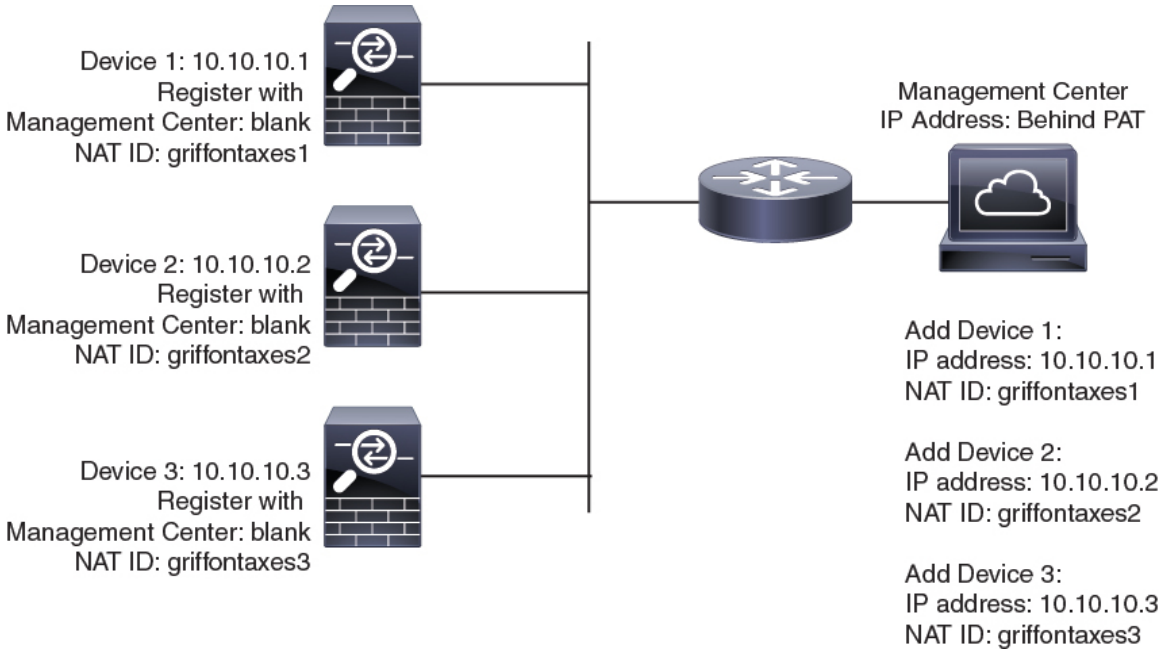
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定 管理中心 IP 地址。

图 *1: PAT* 后的受管设备 ***NAT ID***



以下示例为 PAT IP 地址后的 管理中心。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在 管理中心 上指定设备 IP 地址。

图 *2: PAT* 后的 ***FMC NAT ID***

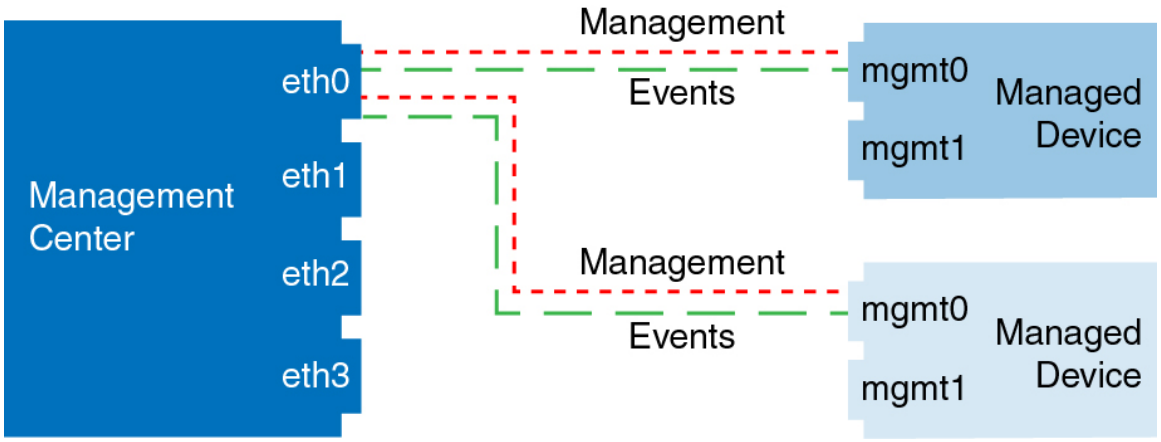


管理和事件流量通道示例

注释 如果在 威胁防御上使用数据接口进行管理，则不能对该设备使用单独的管理接口和事件接口。

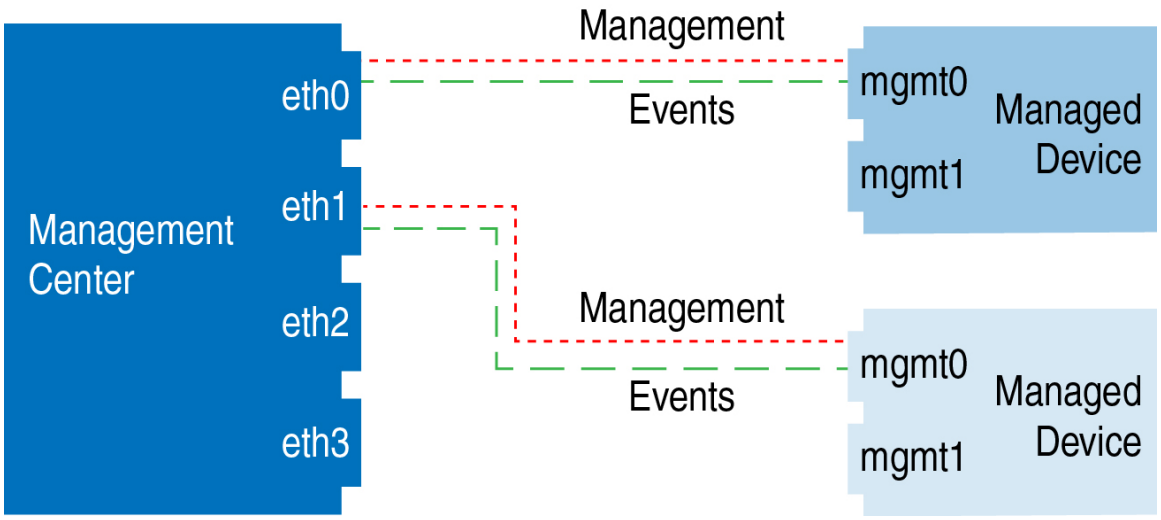
以下示例显示仅使用默认管理接口的 管理中心和受管设备。

图 *3: Cisco Secure Firewall Management Center*上的单个管理接口



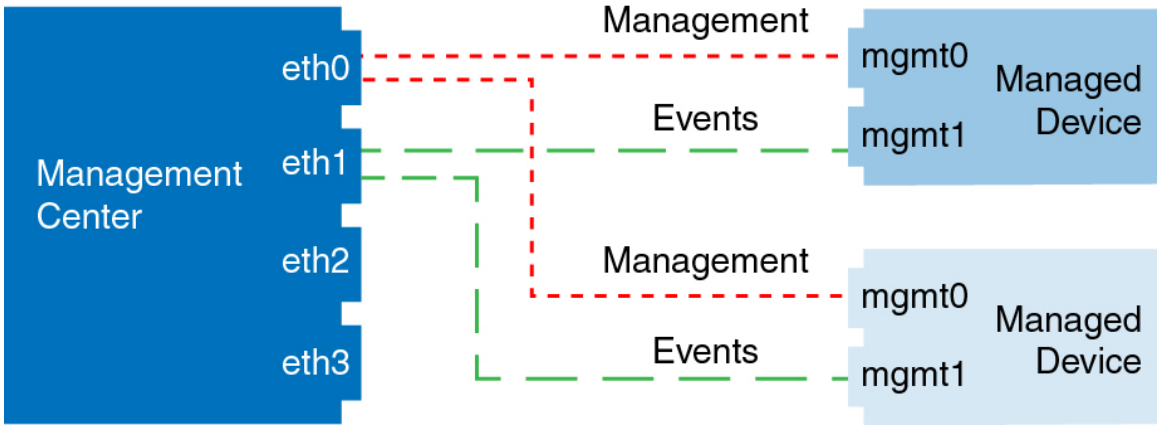
以下示例显示为设备使用单独管理接口的 管理中心；每台受管设备均使用 1 管理接口。

图 *4: Cisco Secure Firewall Management Center*上的多个管理接口



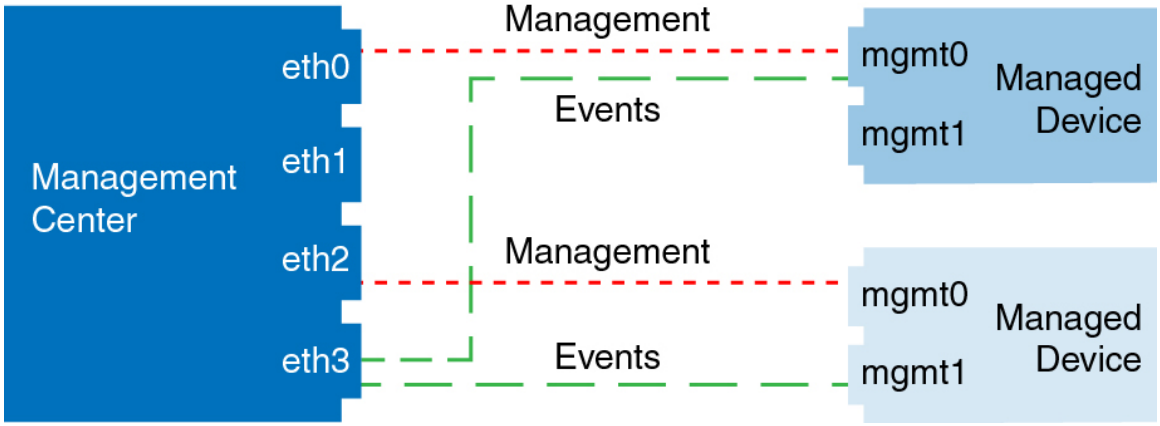
以下示例显示使用单独事件接口的 管理中心和受管设备。

图 *5: Cisco Secure Firewall Management Center*和受管设备上的单独事件接口



以下示例显示 管理中心上多个管理接口与单个事件接口的混合，以及使用单独事件接口或使用单个管理接口的受管设备的混合。

图 *6:* 混合管理和事件接口用法



修改 管理中心 管理接口

修改管理中心上的管理接口设置。您可以选择性地启用其他管理接口或配置仅限事件的接口。

⚠

注意 对所连接的管理接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 管理中心控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

如果更改 管理中心 IP 地址，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的编辑设备上的 管理中心 *IP* 地址或主机名 。如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到 管理中

心 并指定仅 NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

在高可用性配置中，当您从设备 CLI 或 管理中心修改已注册设备的管理 IP 地址时，即使在 HA 同步后，辅助 管理中心 也不会反映更改。要确保辅助 管理中心 也更新，请在两个 管理中心之间切换角色，使辅助 管理中心 成为主用设备。在当前活动的 管理中心的设备管理页面上修改已注册设备的管理 IP 地址。

开始之前

- 有关多个管理接口的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 关于管理设备接口 。
- 如果使用代理：
  - 使用 NT LAN Manager (NTLM) 身份验证的代理不受支持。
  - 如果使用或将要使用智能许可，则代理 FQDN 不能超过 64 个字符。

过程

步骤 1 选择 **系统**（⚙）> **配置**，然后选择**管理接口**。

步骤 2 在**接口**区域中，点击要配置的接口旁边的**编辑**。

本节列出了所有可用接口。不能再添加接口。

可以在每个管理接口上配置以下选项：

- **已启用** - 启用管理接口。请**不要**禁用默认的 eth0 管理接口。某些进程需要 eth0 接口。
- **信道**-必须始终至少有一个启用 **管理流量** 的接口。可选地配置一个仅事件接口。只能在 管理中心上配置一个事件接口。要执行此操作，请取消选中**管理流量**复选框，并保持**事件流量**复选框处于选中状态。对于其余管理接口，可以选择禁用 **事件流量**。无论哪种情况，设备都会尝试将事件发送到仅限事件接口；如果该接口关闭，则在管理接口上发送事件，即使已禁用事件通道。无法同时禁用接口上的事件通道和管理通道。
- **模式** - 指定链路模式。请注意，您对“自动协商”作出的所有更改将被千兆以太网接口忽略。
- **MDI/MDIX** - 设置**自动 MDIX** 设置。
- **MTU**-设置最大传输单位 (MTU)，1280-1500。默认值为 1500。
- **IPv4 配置** - 设置 IPv4 IP 地址。选择:
  - **静态** - 手动输入 **IPv4 管理 IP** 地址和 **IPv4 网络掩码**。
  - **DHCP** - 将接口设置为使用 DHCP（仅 eth0）。

    如果使用 DHCP，则必须使用 DHCP 预留，因此分配的地址不会更改。如果 DHCP 地址更改，设备注册将失败，因为 管理中心 网络配置不同步。要从 DHCP 地址更改中恢复，请连

接到 管理中心 （使用主机名或新 IP 地址）并导航至 **系统**（⚙）> **配置** > **管理接口** 以重置网络。

- **已禁用** - 禁用 IPv4。请勿同时禁用 IPv4 和 IPv6。

- **IPv6 配置** - 设置 IPv6 IP 地址。选择:
  - **静态** - 手动输入 **IPv6 管理 IP** 地址和 **IPv6 前缀长度**。
  - **DHCP** - 将接口设置为使用 DHCPv6（仅限 eth0）。
  - **已分配路由器** - 启用无状态自动配置。
  - **已禁用** - 禁用 IPv6。请勿同时禁用 IPv4 和 IPv6。
  - **IPv6 DAD** - 当您启用 IPv6 时，启用或禁用重复地址检测 (DAD)。您可能希望禁用 DAD，因为使用DAD可能会导致拒绝服务攻击。如果禁用此设置，则需要手动检查此接口是否未使用已分配的地址。

步骤 3 在 **路由** 区域中，通过点击 **编辑**（✎）编辑静态路由，或通过点击 **添加**（+）添加路由。

通过点击 👁 来查看路由表。

每个额外的接口均需要静态路由，才能访问远程网络。有关何时需要新路由的详细信息，请参阅 管理中心管理接口上的网络路由 ，第 34 页。

注释 对于默认路由，只能更改网关 IP 地址。通过将指定网关匹配到此接口网络，系统会自动选择出口接口。

您可以为静态路由配置以下设置：

- **目标** - 设置要创建路由的网络的目标地址。
- **网络掩码**或**前缀长度** - 设置网络的网络掩码 (IPv4) 或前缀长度 (IPv6)。
- **接口** - 设置出口管理接口。
- **网关** - 设置网关 IP 地址。

步骤 4 在**共享设置**区域中，设置所有接口共享的网络参数。

注释 如果为 eth0 接口选择了 **DHCP**，则无法手动指定从 DHCP 服务器派生的某些共享设置。

可以配置以下共享设置：

- **主机名** - 设置 管理中心主机名。主机名最多包含 64 个字符，并且必须以字母或数字开头和结尾，并且只能包含字母、数字或连字符。更改主机名后，如果您希望在系统日志消息中反映新的主机名，请重启 管理中心。在重启之后，系统日志消息才会反映新的主机名。
- **域** - 为 管理中心设置搜索域，用逗号分隔。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

- **主 DNS 服务器、辅助 DNS 服务器、第三级 DNS 服务器** - 设置要按首选顺序使用的 DNS 服务器。
- **远程管理端口** - 设置远程管理端口用于与受管设备进行通信。管理中心和受管设备使用双向、SSL 加密的通信通道（默认情况下在端口 8305 上）进行通信。

  注释　思科强烈建议保留远程管理端口的默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，则必须在部署中需要相互通信的**所有**设备上做出该更改。

步骤 5 在 **ICMPv6** 区域中，配置 ICMPv6 设置。

- **允许发送回应应答数据包** - 启用或禁用回应应答数据包。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到管理中心管理接口，以进行测试。
- **允许发送目的地不可达数据包** - 启用或禁用目的地不可达数据包。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。

步骤 6 在**代理**区域中，配置 HTTP 代理设置。

管理中心配置为通过端口 TCP/443 (HTTPS) 和 TCP/80 (HTTP) 直接连接到互联网。您可以使用代理服务器，以通过 HTTP 摘要对代理服务器进行身份验证。

请参阅本主题前提条件中的代理要求。

a) 选中**已启用 (Enabled)** 复选框。
b) 在 **HTTP 代理**字段中，输入代理服务器的 IP 地址或完全限定域名。

   请参阅本主题前提条件中的要求。

c) 在**端口 (Port)** 字段中，输入端口号。
d) 通过选择**使用代理身份验证**来提供身份验证凭证，然后提供**用户名**和**密码**。

步骤 7 点击**保存 (Save)**。

步骤 8 如果更改 管理中心 IP 地址，请参阅。如果更改 管理中心 IP 地址，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 编辑设备上的 管理中心 *IP* 地址或主机名 。

如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到管理中心 并指定仅NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

更改管理中心和威胁防御 IP 地址

如果需要将 管理中心 和 威胁防御 IP 地址移至新网络，则可能需要同时更改这些地址。

过程

步骤 1 禁用管理连接。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 选择**设备** > **设备管理**。

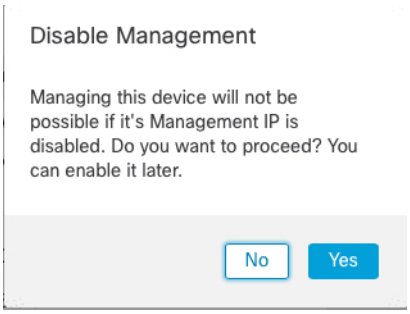
b) 点击设备旁边的 **编辑**（）。

c) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

d) 点击滑块暂时禁用管理，使其处于禁用状态（）。

图 *7:* 禁用管理

系统将提示您继续禁用管理；点击 **是**。



步骤 2 将 管理中心 中的设备 IP 地址更改为新的设备 IP 地址。

稍后您将更改设备上的 IP 地址。

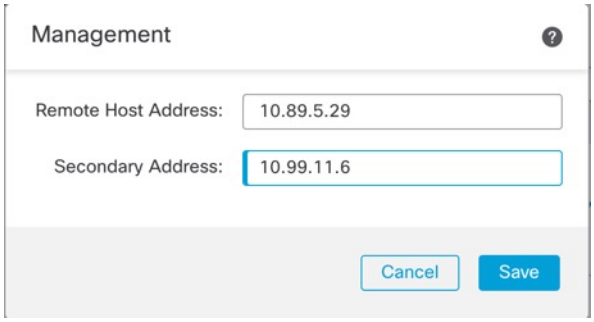
对于高可用性对或集群，在所有设备上执行这些步骤。

a) 通过点击 **编辑**（） 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

图 *8:* 编辑管理地址

b) 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存 (Save)**。

图 *9:* 管理 *IP* 地址



步骤 3 请更改 管理中心 IP 地址。

注意 对所连接的管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 管理中心 控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择 **系统**（⚙）> **配置**，然后选择**管理接口**。
b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存 (Save)**。

步骤 4 更改设备上的管理器 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 在 威胁防御 CLI 中，查看 管理中心 标识符。

show managers

示例：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
```

```
Management type           : Configuration
```

b) 编辑 管理中心 IP 地址或主机名。

configure manager edit 标识符 {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

如果 管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

步骤 5 在控制台端口更改管理器访问接口的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

如果您使用专用管理接口：

configure network ipv4

configure network ipv6

如果您使用专用管理接口：

configure network management-data-interface disable

configure network management-data-interface

步骤 6 点击滑块重新启用管理，使其处于启用状态 （ ）。

对于高可用性对或集群，在所有设备上执行这些步骤。

图 *10:* 启用管理连接

步骤 7 （如果使用数据接口进行管理器访问）刷新 管理中心中的数据接口设置。

对于高可用性对，请在两台设备上执行此步骤。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理访问权限 - 配置详细信息 (Manager Access - Configuration Details)**，然后点击**刷新 (Refresh)**。

b) 选择**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)**，然后设置 IP 地址以便与新地址匹配。

c) 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

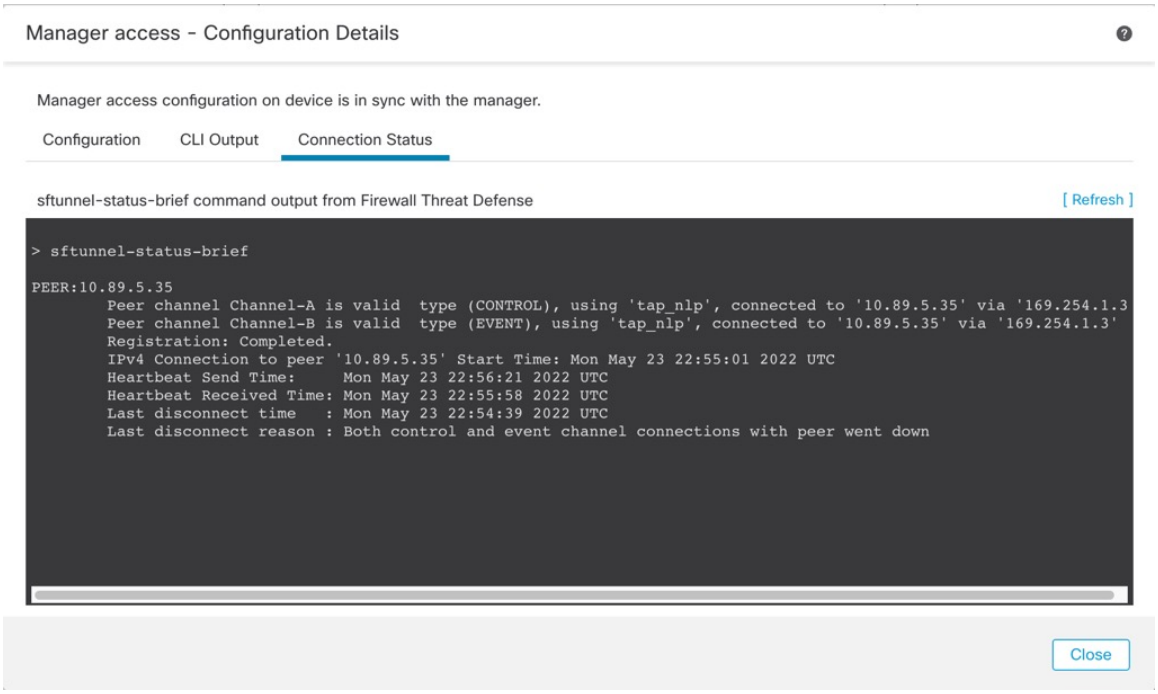
步骤 8 确保管理连接已重新建立。

在 管理中心 中，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *11:* 连接状态



步骤 9 （对于高可用性 管理中心 对）在辅助 管理中心上重复配置更改。

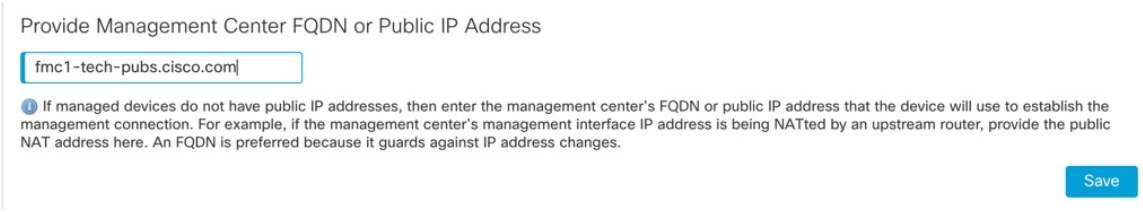
a) 更改辅助 管理中心 IP 地址。
b) 在两台设备上指定新的对等地址。
c) 将辅助设备设置为主用设备。
d) 禁用设备管理连接。
e) 更改 管理中心 中的设备 IP 地址。
f) 重新启用管理连接。

管理器远程访问

如果受管设备没有公共 IP 地址，则输入设备在建立管理连接时使用的 管理中心的 FQDN 或公共 IP 地址。例如，如果上游路由器对 管理中心的管理接口 IP 地址执行 NAT，请在此处提供 公共 NAT 地址。首选 FQDN，因为它可以防止 IP 地址更改。

如果使用序列号 (零接触调配) 方法注册设备，则此字段将自动用于管理器 IP 地址/主机名的初始配置。如果使用手动方法，则在执行设备的初始配置时，可以参考此屏幕上的值来识别公共 管理中心 IP 地址/主机名。

图 *12:* 管理器远程访问



网络分析策略首选项

当用户修改入侵策略时，可以配置系统以使用注释功能跟踪与策略相关的更改。在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。

如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，系统都会提示用户输入注释。

或者，可以将对网络分析策略的更改写入到审核日志中。

进程

使用 Web 界面来控制 管理中心上的进程的关闭和重新启动。您可以执行以下操作：

- 关闭：启动设备的正常关闭。

注意 请**勿**使用电源按钮关闭 Firepower 设备；这样做可能导致数据丢失。通过使用 Web 界面（或 CLI），可让系统做好准备，在不丢失配置数据的情况下安全断电和重新启动。

- 重新引导：关闭并正常重启。
- 重新启动控制台：重新启动通信、数据库和 HTTP 服务器进程。这通常在故障排除过程中使用。

提示 对于虚拟设备，请参阅您的虚拟平台的文档。特别是对于 VMware，自定义电源选项是 VMware 工具的一部分。

关闭或重新启动 FMC

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 选择**进程 (Process)**。

步骤 3 执行以下操作之一：

关闭	点击 **关闭管理中心**旁边的 **运行命令** 。
重新启动	点击 **重新引导管理中心**旁边的 **运行命令** 。 **注释** 重新启动会让您退出，系统会执行可能需要一小时才能完成的数据库检查。
重新启动控制台	点击 **重新启动管理中心**旁边的 **运行命令** 。 **注释** 重新启动可能导致已删除的主机重新显示在网络映射中。

REST API 首选项

管理中心 REST API 提供轻量级接口，以供第三方应用使用 REST 客户端和标准 HTTP 方法查看和管理设备配置。有关 管理中心 REST API 的更多信息，请参阅 Secure Firewall Management Center REST API 快速入门指南。

注释 管理中心 REST API 不支持 HTTPS 证书。

默认情况下，管理中心使用 REST API 允许来自应用的请求。可以将 管理中心配置为阻止此访问。

启用 Rest API 访问

注释 在使用 管理中心高可用性的部署中，此功能仅在主用 管理中心中可用。

过程

步骤 1 选择右上角的**齿轮**（⚙）以打开系统菜单。

步骤 2 点击 **REST API 首选项 (REST API Preferences)**。

步骤 3 要启用或禁用对 管理中心 的 REST API 访问，请选中或取消选中**启用 REST API** 复选框。

步骤 4 点击**保存 (Save)**。

步骤 5 访问 REST API Explorer，网址为：

```
https://<management_center_IP_or_name>:<https_port>/api/api-explorer
```

远程控制台访问管理

您可以通过物理设备上的VGA端口（默认端口）或串行端口使用Linux系统控制台在受支持系统上进行远程访问。使用“控制台配置”页面，选择最适合您的组织的Firepower部署的物理布局的选项。

在受支持的基于物理硬件的系统中，可以通过LAN上串行(SOL)连接管理接口上使用无人值守管理(LOM)来远程监控或管理该系统，而无需登录到该系统的管理接口。在带外管理连接上使用命令行界面可以执行有限的任务，例如查看机箱序列号或监控诸如风扇速度和温度之类的状况。支持LOM的电缆连接因 管理中心 型号而异：

- 对于 管理中心 MC1600、MC2600 和 MC4600 型号，使用 CIMC 端口连接以支持 LOM。有关更多信息，请参阅《*1600、2600 和 4600 型 Cisco Firepower 管理中心入门指南*》。
- 对于所有其他 管理中心 硬件型号，请使用具有默认 (eth0) 管理端口的连接来支持 LOM。有关硬件型号，请参阅 思科 *Firepower* 管理中心入门指南 。

您必须对系统和要管理系统的用户均启用LOM。在启用系统和用户后，使用第三方智能平台管理接口 (IPMI) 实用程序访问和管理系统。

配置系统上的远程控制台设置

您必须是管理员用户才能执行此程序。

开始之前

- 禁用与设备管理接口连接的所有第三方交换设备上的生成树协议 (STP)。
- 如果计划启用无人值守管理，请参阅设备的入门指南，了解有关安装和使用智能平台管理接口 (IPMI) 实用程序的信息。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**控制台配置 (Console Configuration)**。

步骤 3 选择远程控制台访问选项：

- 选择 **VGA** 将会使用设备的 VGA 端口。
- 选择 **物理串行端口** 以使用设备的串行端口。
- 选择 **无人值守管理** 以在管理中心上使用 SOL 连接。（这可能使用默认管理端口或 CIMC 端口，具体取决于您的 管理中心 型号。有关详细信息，请参阅您的型号的 入门指南 。

步骤 4 要通过 SOL 配置 LOM，请执行以下操作：

- 选择系统的地址 **配置** （**DHCP** 或 **手动**）
- 如果选择手动配置，请输入必要的 IPv4 设置：
  - 输入要用于 LOM 的 **IP 地址 (IP Address)**。

    注释 LOM IP 地址必须不同于 管理中心 管理接口 IP 地址，并要在同一个子网中。

  - 输入系统的**网络掩码 (Netmask)**。
  - 输入系统的**默认网关 (Default Gateway)**。

步骤 5 点击**保存 (Save)**。

步骤 6 系统显示以下警告：“您必须重新启动系统才能使这些更改生效。” 点击 **确认** 立即重新启动或点击 **取消** 稍后重新启动。

下一步做什么

- 如果配置了串行访问，请确保将后面板串行端口连接到本地计算机、终端服务器或其他可支持通过以太网进行远程串行访问的设备，如适用于您的 管理中心 型号的 入门指南 中所述。
- 如果配置了无人值守管理，请启用无人值守管理用户；请参阅无人值守管理用户访问配置，第 49 页。

无人值守管理用户访问配置

必须将“无人值守管理”权限明确授予使用此功能的用户。LOM 用户还有如下限制：

- 必须为用户指定管理员角色。
- 用户名最多可包含 16 个字母数字字符。不支持将连字符和更长的用户名用作 LOM 用户名。
- 用户的 LOM 密码不得与该用户的系统密码相同。密码必须符合 用户密码中所述的要求。思科建议您为设备使用最大支持长度、不是基于字典的复杂密码，并且每三个月修改一次密码。
- 物理 管理中心的 最多可以有 13 个 LOM 用户。

请注意，如果在一个具有 LOM 权限的用户已登录时取消激活然后再重新激活该用户，那么该用户可能需要重新登录到 Web 界面才能重新获得对 `impitool` 命令的访问权限。

注释 高可用性同步不适用于 LOM 用户，因此它们不会在高可用性 管理中心上复制。您必须在活动 管理中心上创建启用 LOM 的不同管理员用户。

在高可用性配置中，当您为启用了 LOM 权限的本地用户创建本地用户或重置密码时，更改会从基于 UCS 的主用 管理中心同步到主用和备用 管理中心以及主用 管理中心 CIMC。新密码未与 CIMC 登录的备用管理中心同步。要确保备用管理中心也更新，请重置备用管理中心上本地用户的CIMC 登录密码。

启用无人值守管理用户访问

您必须是管理员用户才能执行此程序。

使用此任务向现有用户授予LOM访问权限。要向新用户授予LOM访问权限，请参阅添加或编辑内部用户。

过程

步骤 1 选择**系统**（⚙）> **用户** > **用户**。

步骤 2 要向现有用户授予 LOM 用户访问权限，请点击列表中用户名旁边的 **编辑**（✎）。

步骤 3 在**用户配置 (User Configuration)** 下，启用管理员角色。

步骤 4 选中**允许无人值守管理访问 (Allow Lights-Out Management Access)** 复选框。

步骤 5 点击**保存 (Save)**。

LAN 上串行连接配置

使用计算机上的第三方 IPMI 实用程序可通过 LAN 上串行与设备建立连接。如果您的计算机使用类似 Linux 的环境或 Mac 环境，请使用 IPMItool；对于 Windows 环境，请使用 IPMIutil 或 IPMItool，取决于您的 Windows 版本。

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

Linux

IPMItool 是许多发行版的标准配置，可立即使用。

Mac

必须在 Mac 上安装 IPMItool。首先，请确认 Mac 上安装了 Apple 的 XCode 开发者工具，确保安装了用于命令行开发的可选组件（在较新版本中为 UNIX 开发和系统工具，或在较旧版本中为命令行

支持）。然后您可以安装 macports 和 IPMItool。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows 的 ISE 安全评估代理

对于启用了适用于 Linux 的 Windows 子系统 (WSL) 的 Windows 版本 10 及更高版本，以及某些较早版本的 Windows Server，您可以使用 IPMItool。否则，您必须在 Windows 系统上编译 IPMIutil；您可以使用 IPMIutil 本身进行编译。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

了解 IPMI 实用程序命令

用于 IPMI 实用程序的命令由若干段组成，如以下 Mac 上的 IPMItool 示例：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

其中：

- `ipmitool` 调用实用程序。
- `-I lanplus` 指定对会话使用加密的 IPMI v2.0 RMCP+ LAN 接口。
- `-H IP_地址` 表示已配置的要访问的设备的 Lights-Out 管理 IP 地址。
- `-U 用户_名称` 是授权远程会话用户的名称。
- `命令` 是您想使用的命令的名称。

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 Windows 上的 IPMIutil，以上命令如下所示：

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

使用此命令可连接到设备的命令行，就像您本人在设备旁边一样。系统会提示您输入密码。

使用 IPMItool 配置 LAN 上串行

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

使用 IPMItool，输入以下命令，并在提示时输入密码：

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

使用 IPMIutil 配置 LAN 上串行

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

使用 IPMIutil，输入以下命令，如果出现提示则输入密码：

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

无人值守管理概述

通过无人值守管理 (LOM)，您可以在默认 (eth0) 管理接口上利用 SOL 连接执行有限的系列操作，而无需登录设备。可以使用命令创建 SOL 连接，然后使用其中一个 LOM 命令。命令执行完成后，连接将终止。

⚠

注意 在极少数情况下，如果您的计算机与系统的管理接口位于不同子网，而系统配置为使用 DHCP，则尝试访问 LOM 功能可能失败。如果发生这种情况，可以禁用然后在系统上重新启用 LOM，或者使用与系统位于同一子网的计算机来 ping 设备的管理接口。这样应该就可以使用 LOM。

⚠

注意 思科了解智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 固有的漏洞。在系统上启用无人值守管理 (LOM) 会暴露该漏洞。为了降低这种漏洞，请将您的系统部署在只有受信任用户才可以访问的安全管理网络上，并且使用最大支持长度、不是基于字典的复杂密码并且每三个月修改一次密码。为防止暴露此漏洞，请勿启用 LOM。

如果所有访问系统的尝试均失败，则可以使用 LOM 远程重新启动系统。请注意，如果在 SOL 连接处于活动状态时重新启动系统，LOM 会话可能会断开连接或超时。

⚠

注意 请**勿**重新启动系统，除非它不响应任何其他重新启动操作。远程重新启动系统不能正常重新启动系统，而且可能会丢失数据。

表 *3:* 无人值守管理命令

IPMItool	IPMIutil	说明
（不适用）	`-V 4`	启用 IPMI 会话的管理员权限
`-I lanplus`	`-J 3`	启用 IPMI 会话加密
`-H 主机名/IP 地址`	`-N 节点名/IP 地址`	表示 管理中心的 LOM IP 地址或主机名
`-U`	`-U`	表示已获授权 LOM 帐户的用户名
`sol activate`	`sol -a`	开始 SOL 会话
`sol deactivate`	`sol -d`	结束 SOL 会话
`chassis power cycle`	`power -c`	重新启动设备
`chassis power on`	`power -u`	打开设备电源
`chassis power off`	`power -d`	关闭设备电源
`sdr`	`sensor`	显示设备信息，例如风扇速度和温度

例如，显示设备信息列表的 IPMItool 命令是：

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 IPMIutil 实用程序，以上命令如下：

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

使用 IPMItool 配置无人值守管理

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

为 IPMItool 输入以下命令以及密码（如果提示）：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

使用 IPMIutil 配置无人值守管理

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

为 IPMIutil 输入以下命令以及密码（如果提示）：

```
ipmiutil -J 3 -N IP_address -U username command
```

远程存储设备

在 管理中心上，您可以将本地或远程存储的以下系统用于备份和报告：

- 网络文件系统 (NFS)
- 服务器消息块 (SMB)/通用互联网文件系统 (CIFS)
- 安全外壳 (SSH)

不能将备份发送到一个远程系统而将报告发送到另一个，但是，可以选择这二者之一发送到远程系统，并将另一个存储在 管理中心。

提示 在配置并选择远程存储之后，只有在未增加连接数据库限制的情况下，才可以切换回本地存储。

管理中心远程存储 - 支持的协议和版本

管理中心版本	NFS 版本	SSH 版本	SMB 版本
6.4	V3/V4	openssh 7.3p1	V2/V3
6.5	V3/V4	ciscossh 1.6.20	V2/V3
6.6	V3/V4	ciscossh 1.6.20	V2/V3
6.7	V3/V4	ciscossh 1.6.20	V2/V3

用于启用协议版本的命令

以 root 用户身份运行以下命令以启用协议版本：

- **NFS**—`/bin/mount -t nfs '10.10.4.225':'/home/manual-check' '/mnt/remote-storage' -o 'rw,vers=4.0'`

- **SMB**—`/usr/bin/mount.cifs //10.10.0.100/pyallapp-share/testing-smb /mnt/remote-storage -o username=administrator,password=******,vers=3.0`

配置本地存储

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**远程存储设备 (Remote Storage Device)**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择**本地（无远程存储）(Local [No Remote Storage])**。

步骤 4 点击**保存 (Save)**。

为远程存储配置 NFS

开始之前

- 确保外部远程存储系统可正常工作且能够从 管理中心 进行访问。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **NFS**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IPv4 地址或主机名。
- 在**目录 (Directory)** 字段中输入存储区域的路径。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 58 页。

步骤 6 在**系统使用 (System Usage)** 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。
- 然后，在 **Disk Space Threshold** 中输入要备份远程存储的磁盘空间阈值。默认值为 90%。

步骤 7 要测试设置，请点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

故障排除

当与防火墙设备的 NFS 连接中存在随机延迟时，请执行以下活动，然后联系思科 TAC 进行故障排除：

- 在设备出现问题之前或之后收集故障排除文件。您可以从 Web 界面或使用 CLI 命令生成故障排除文件。有关如何生成故障排除文件的信息，请参阅 Firepower 文件生成程序故障排除。
- 收集传入和退出流量 PCAP 记录。有关程序的信息，请参阅数据包捕获概述。
- 在设备中使用以下命令（CLISH 模式）在 NFS 应用失败时收集系统支持跟踪数据：

  ```
  > system support trace
  ```

- 在故障期间，使用 **show snort counters** 命令收集 Snort 计数器两次，以查看 Snort 预处理器连接的统计信息。有关此命令的信息，请参阅 show snort counters。

为远程存储配置 SMB

开始之前

确保外部远程存储系统可正常工作且能够从 管理中心进行访问：

- 请注意，系统只能识别顶级 SMB 共享，不能识别完整文件路径。您必须使用 Windows 来共享要使用的确切目录。
- 确保您将用于从 FMC 访问 SMB 共享的 Windows 用户具有共享位置的所有权和读取/更改权限。
- 为确保安全，应安装 SMB 2.0 或更高版本。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **SMB**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IPv4 地址或主机名。
- 在**共享 (Share)** 字段中输入存储区域共享。
- 或者，在**域 (Domain)** 字段中输入远程存储系统的域名。
- 在**用户名 (Username)** 字段中输入存储系统的用户名，在**密码 (Password)** 字段中输入该用户的密码。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 58 页。

步骤 6 在**系统使用 (System Usage)** 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。

步骤 7 要测试设置，请点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

为远程存储配置 SSH

开始之前

- 确保外部远程存储系统可正常工作且能够从 管理中心 进行访问。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **SSH**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IP 地址或主机名。
- 在**目录 (Directory)** 字段中输入存储区域的路径。
- 在 **Username** 字段中输入存储系统的用户名，在 **Password** 字段中输入该用户的密码。要将网络域指定为连接用户名的一部分，请在用户名前面加上域后跟正斜杠 (/)。
- 要使用 SSH 密钥，请将 **SSH Public Key** 字段中的内容复制到 authorized_keys 文件中。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 58 页。

步骤 6 在“系统使用”(System Usage) 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。

步骤 7 如果要测试设置，必须点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

远程存储管理高级选项

如果选择网络文件系统 (NFS) 协议、服务器消息阻止 (SMB) 协议或 SSH 以使用文件传输协议 (SFTP) 来存储报告和备份，您可以选择**使用高级选项**复选框，以使用其中一个安装二进制选项，如 NFS、SMB 或 SSH 安装主页面所记录。

如果选择 SMB 或 NFS 存储类型，则可以使用以下格式在**命令行选项**字段中指定远程存储的版本号：

`vers=version`

其中 *版本* 是要使用的 SMB 或 NFS 远程存储的版本号。例如，要选择 NFSv4，请输入 `vers=4.0`。

如果为文件服务器启用了 SMB 加密，则仅允许 SMB 3.0 版客户端访问文件服务器。要从 管理中心 访问加密的 SMB 文件服务器，请在**命令行选项**字段中键入以下内容：

`vers=3.0`

选择加密的 SMBv3，将备份文件从 管理中心 复制或保存到加密的 SMB 文件服务器。

SNMP

您可以启用简单网络管理协议 (SNMP) 轮询。此功能支持使用 SNMP 协议第 1 版、第 2 版和第 3 版。此功能允许访问标准管理信息库 (MIB)，包括联系人、管理、位置、服务信息、IP 寻址和路由信息以及传输协议使用统计信息等系统详细信息。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

启用 SNMP 轮询不会导致系统发送 SNMP 陷阱；这样做只会使 MIB 中的信息可供网络管理系统轮询。

配置 SNMP 轮询

开始之前

为计划用于轮询系统的每台计算机添加 SNMP 访问权限。请参阅配置访问列表，第 3 页。

注释 SNMP MIB 包含可用于攻击您的部署的信息。我们建议您将 SNMP 访问权限的访问列表限制为将被用于轮询 MIB 的特定主机。我们还建议您针对网络管理访问权限使用 SNMPv3 和强密码。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **SNMP**。

步骤 3 从 **SNMP 版本** 下拉列表中，选择要使用的 SNMP 版本：

- **版本 1** 或 **版本 2**：在 **社区字符串** 字段中输入只读 SNMP 社区名称，然后跳至程序末尾。

  注释 不包含特殊字符 (< > / % # & ? ' 等）在 SNMP 社区字符串名称中。

- **版本 3**：请点击 **添加用户** 显示用户定义页面。SNMPv3 仅支持只读用户和使用 AES128 加密。

步骤 4 输入**用户名 (Username)**。

步骤 5 从**身份验证协议 (Authentication Protocol)** 下拉列表中选择要用于身份验证的协议。

步骤 6 在**身份验证密码 (Authentication Password)** 字段中输入使用 SNMP 服务器进行身份验证时所需的密码。

步骤 7 在**验证密码 (Verify Password)** 字段中重新输入身份验证密码。

步骤 8 从**隐私协议 (Privacy Protocol)** 列表中选择要使用的隐私协议，或者选择**无 (None)** 以不使用隐私协议。

步骤 9 在**隐私密码 (Privacy Password)** 字段中输入 SNMP 服务器需要的 SNMP 隐私密钥。

步骤 10 在**验证密码 (Verify Password)** 字段中重新输入隐私密码。

步骤 11 点击**添加 (Add)**。

步骤 12 点击**保存 (Save)**。

会话超时

无人参与的登录会话可能存在安全风险。可以配置用户的登录会话因无活动而超时之前允许经过的空闲时间。

请注意，对于计划长期安全地被动监控系统的场景，可以免除特定 Web 界面用户的超时。具有“管理员”(Administrator) 角色的用户拥有对菜单选项的完整访问权限，这些访问权限受损会构成额外风险，因此他们不能获得会话超时豁免。

配置会话超时

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **CLI 超时**。

步骤 3 配置会话超时：

- Web 界面（仅限于管理中心）：配置 **浏览器会话超时（分钟）**。默认值为 `60`；最大值为 `1440`（24 小时）。

  使用户免受会话超时影响的信息，请参阅 添加或编辑内部用户。

- CLI：配置 **CLI 超时（分钟）** 字段。默认值为 `0`；最大值为 `1440`（24 小时）。

步骤 4 点击**保存 (Save)**。

时间

时间设置在大多数页面上均使用您在“用户首选项”的“时区”页面上设置的时区（默认值是“美国/纽约”）以本地时间显示，但使用 UTC 时间存储在设备中。

限制 时区功能（在“用户首选项”中）假设，默认系统时钟设置为UTC时间。请勿尝试更改系统时间。请注意，不支持从UTC更改系统时间，而执行此操作将需要您重新映像设备以从不支持的状态中恢复。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Time**。

使用在“用户首选项”中为您的账户指定的时区显示当前时间。

如果您的设备使用 NTP 服务器：有关表条目的信息，请参阅NTP 服务器状态，第 60 页。

NTP 服务器状态

如果要从 NTP 服务器同步时间，则可以在 **时间** 页面（选择 **系统 > 配置**）上查看连接状态。

表 *4: NTP* 状态

列	Description
NTP 服务器	已配置的 NTP 服务器的 IP 地址或名称。

列	Description
状态	NTP 服务器时间同步的状态。 • **已在使用 (Being Used)** 表示设备已与 NTP 服务器同步。 • **可用 (Available)** 表示 NTP 服务器可供使用，但时间尚未同步。 • **不可用 (Not Available)** 表示 NTP 服务器在您的配置中，但 NTP 后台守护程序无法使用该服务器。 • **待定 (Pending)** 表示 NTP 服务器是新的或 NTP 后台守护程序最近重新启动过。随着时间的推移，此选项的值应更改为**已在使用 (Being Used)**、**可用 (Available)** 或**不可用 (Not Available)**。 • **未知 (Unknown)** 表示 NTP 服务器的状态未知。
身份验证	管理中心 与 NTP 服务器之间通信的身份验证状态： • **无** 表示未配置身份验证。 • **不良** 表示已配置身份验证，但失败。 • **确认** 表示身份验证成功。 如果已配置身份验证，系统会在状态值后面显示密钥编号和密钥类型（SHA-1、MD5 或 AES-128 CMAC）。例如： **bad**、**key 2**、**MD5**。
偏移 (Offset)	设备时间与已配置的 NTP 服务器上时间所相差的毫秒数。负值表示设备时间晚于 NTP 服务器，正值表示设备时间早于 NFP 服务器。
上次更新 (Last Update)	自上次与 NTP 服务器同步时间以来过去的秒数。NTP 后台守护程序会根据若干条件自动调整同步时间。例如，如果显示更长的更新时间（例如 300 秒），表示时间相对稳定，这样，NTP 后台守护程序将会确定不需要使用更小的更新增量。

时间同步

要使系统成功运行，必须在Cisco Secure Firewall Management Center (管理中心) 及其受管设备上同步系统时间。我们建议您在 管理中心 初始配置期间指定 NTP 服务器，但您可以在初始配置完成后使用此部分中的信息建立或更改时间同步设置。

请使用网络时间协议 (NTP) 服务器在 管理中心 和所有设备上同步系统时间。 管理中心 支持使用 MD5、SHA-1 或 AES-128 CMAC 对称密钥认证与 NTP 服务器进行安全通信；为了系统安全，我们建议使用此功能。

管理中心还可以将配置为仅连接经过身份验证的NTP服务器；使用此选项可提高混合身份验证环境中或将系统迁移到不同 NTP 服务器时的安全性。在对所有可访问的 NTP 服务器进行身份验证的环境中使用此设置是多余的。

注释 如果在初始配置期间为 管理中心 指定了 NTP 服务器，则与该 NTP 服务器的连接不会受到保护。您必须编辑该连接的配置，以指定 MD5、SHA-1 或 AES-128 CMAC 密钥。

注意 如果 管理中心和受管设备之间的时间不同步，会导致意外后果。

要同步 管理中心 和托管设备上的时间，请参阅：

- 推荐： 将管理中心上的时间与 NTP 服务器同步，第 62 页

  本主题提供有关将 管理中心 配置为与一台或多台 NTP 服务器同步的说明，并包含有关将受管设备配置为与同一台或多台 NTP 服务器同步的说明的链接。

- 否则： 同步时间但不访问网络 NTP 服务器，第 64 页

  本主题提供有关设置 管理中心上的时间、配置 管理中心 以用作 NTP 服务器的说明，以及有关配置受管设备以与 管理中心 NTP 服务器同步的说明的链接。

将管理中心上的时间与 NTP 服务器同步

系统的所有组件之间的时间同步至关重要。

确保 管理中心和所有受管设备之间正确同步时间的最佳方式是使用网络上的 NTP 服务器。

管理中心 支持 NTPv4。

您必须具有管理员或网络管理员权限才能执行此程序。

开始之前

请注意以下提示：

- 如果 管理中心 和托管设备无法访问网络 NTP 服务器，请不要使用此程序。参阅同步时间但不访问网络 NTP 服务器，第 64 页。
- 请勿指定不受信任的 NTP 服务器。
- 如果您计划与 NTP 服务器建立安全连接（建议用于系统安全），请获取该 NTP 服务器上配置的 SHA-1、MD5 或 AES-128 CMAC 密钥编号和值。
- 与 NTP 服务器之间的连接不使用已配置的代理设置。
- Firepower 4100 系列设备和 Firepower 9300 设备无法使用此程序设置系统时间。相反，请将这些设备配置为使用您使用此程序配置的相同 NTP 服务器。有关说明，请参阅硬件型号对应的文档。

注意 如果 管理中心已重新启动，并且 DHCP 服务器设置了不同于您在这里指定的记录的 NTP 服务器记录，则会使用 DHCP 提供的 NTP 服务器。为避免这种情况，请将 DHCP 服务器配置为会使用相同的 NTP 服务器。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击 **Time Synchronization**。

步骤 3 如果**通过 NTP 提供时间 (Serve Time via NTP)** 处于**已启用 (Enabled)** 状态，请选择**已禁用 (Disabled)** 以禁用管理中心作为 NTP 服务器。

步骤 4 对于“**设置我的时钟**”选项，选择“**通过 NTP**”。

步骤 5 点击“**添加**”。

步骤 6 在“**添加 NTP 服务器**”对话框中，输入 NTP 服务器的主机名或 IPv4 或 IPv6 地址。

步骤 7 （可选）要保护您的 管理中心 与 NTP 服务器之间的通信，请执行以下操作：

a) 从“**密钥类型**”下拉列表中选择 **MD5**、**SHA-1** 或 **AES-128 CMAC**。

b) 输入指定的 NTP 服务器对应的 MD5、SHA-1 或 AES-128 CMAC **密钥号**和**密钥值**。

步骤 8 点击“**添加**”。

步骤 9 当仅配置两个 NTP 服务器时，它们之间的偏移量差异会很大。这将导致 管理中心 使用本地时间。因此，我们建议您配置至少三个 NTP 服务器。

要添加更多 NTP 服务器，请重复步骤 5 至 8。

步骤 10 （可选）要强制 管理中心 仅使用成功进行身份验证的NTP服务器，请选中“**仅使用经过身份验证的 NTP 服务器**”复选框。

步骤 11 点击**保存 (Save)**。

下一步做什么

将受管设备设置为与同一台 NTP 服务器或服务器同步：

- 配置设备平台设置：在 《Cisco Secure Firewall Management Center 设备配置指南》中为威胁防御配置 NTP 时间同步。

  请注意，即使您强制 管理中心 与 NTP 服务器建立安全连接（**仅使用经过身份验证的 NTP 服务器**），与该服务器的设备连接也不使用身份验证。

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

同步时间但不访问网络 NTP 服务器

如果设备无法直接访问网络 NTP 服务器，或您的组织没有网络 NTP 服务器，可使用物理硬件管理中心来充当 NTP 服务器。

重要事项

- 除非没有其他 NTP 服务器，否则请勿使用此程序。相反，请使用 将管理中心上的时间与 NTP 服务器同步，第 62 页 中的程序。
- 不要将虚拟 管理中心 用作 NTP 服务器。

将 管理中心配置为NTP服务器**之后**，则要手动更改时间，则必须先禁用NTP选项，手动更改时间，然后重新启用 NTP 选项。

过程

步骤 1 在 管理中心上手动设置系统时间：

a) 选择**系统**（⚙）> **配置**。
b) 点击 **Time Synchronization**。
c) 如果**通过 NTP 提供时间 (Serve Time via NTP)** 处于**已启用 (Enabled)** 状态，请选择**已禁用 (Disabled)**。
d) 点击**保存 (Save)**。
e) 对于**设置我的时钟**，选择**在本地配置中手动设置**。
f) 点击**保存 (Save)**。
g) 在屏幕左侧的导航窗格中，点击**时间**。
h) 使用**设置时间 (Set Time)** 下拉列表设置时间。

注释 当您在管理中心上更改时间超过两个小时时，必须尽快重新启动设备，例如在维护窗口中，以避免任何故障。

i) 如果显示的时区不是 UTC，请点击该时区，并将时区设置为 **UTC**。
j) 点击**保存 (Save)**。
k) 点击 **Done**。
l) 点击 **Apply**。

步骤 2 设置 管理中心作为 NTP 服务器：

a) 在屏幕左侧的导航窗格中，点击**时间同步**。
b) 对于**通过 NTP 提供时间**，选择**已启用**。
c) 点击**保存 (Save)**。

步骤 3 设置受管设备，以便与 管理中心 NTP 服务器同步：

a) 在分配给托管设备的平台设置策略的“时间同步”设置中，将时钟设置为**通过管理中心的 NTP** 同步。

b) 将更改部署到托管设备。

说明：

对于 威胁防御 设备，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的为威胁防御配置 *NTP* 时间。

关于更改时间同步设置

- 管理中心 管理中心及其托管设备高度依赖准确的时间。系统时钟是维护系统时间的系统设施。系统时钟设置为协调世界时 (UTC)，它是全球规定时钟和时间的主要时间标准。

  请勿尝试更改系统时间。不支持从UTC更改系统时区，而执行此操作将需要您重新映像设备以从不支持的状态中恢复。

- 如果将管理中心配置为使用 NTP 提供时间，然后又将其禁用，受管设备上的 NTP 服务仍会尝试与管理中心同步时间。必须更新并重新部署任何适用的平台设置策略，以建立新的时间源。

- 将 管理中心配置为 NTP 服务器**之后**，则要手动更改时间，则必须先禁用 NTP 选项，手动更改时间，然后重新启用 NTP 选项。

UCAPL/CC 合规性

组织只能使用符合由美国国防部和全球认证组织制定的安全标准的设备和软件。有关此设置的详细信息，请参阅安全认证合规性模式。

升级配置

策略属性、对象或其他设备配置可能会在 管理中心 升级过程中发生更改。默认情况下，将 管理中心 升级到主要版本可能会启用某些功能。 **升级配置** 设置允许您在完成 管理中心的下一个主要版本升级时生成待处理的配置更改报告。此报告显示升级后待部署在受管设备上的策略和设备配置更改。管理中心 升级完成后，选择 **消息中心** > **任务** 以下载报告。

待处理的配置更改报告包括：

- **比较视图**：将待部署在受管设备上的所有升级后配置更改与当前设备配置进行比较。
- **高级视图**：使用 CLI 预览待处理的配置更改。

有关待处理配置更改报告的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 部署预览 。

启用升级后报告

在 管理中心的下一个主要版本升级后，生成要在托管设备上部署的待定配置更改报告。

过程

步骤 1 选择 **系统**（⚙）> **配置**

步骤 2 选中 **启用升级后报告** 复选框以启用该选项。

报告在 管理中心的下一次主要版本升级后生成。此选项会在升级后为所有受管设备生成报告，生成报告所需的时间取决于配置的大小和受管设备的数量。

步骤 3 点击**保存 (Save)**。

用户配置

全局用户配置设置影响 管理中心上的所有用户。在“用户配置”(User Configuration) 页面 (**系统**（⚙）> **配置** > **用户配置**) 上配置以下设置：

- **密码重用限制**：用户最近历史记录中无法重复使用的密码数量。此限制适用于所有用户的 Web 界面访问。对于管理员用户，此限制还适用于CLI访问；系统为每种访问形式保留单独的密码列表。将限制设置为零（默认值）不会对密码重用执行任何限制。请参阅设置密码重用限制，第 67 页。
- **跟踪成功登录次数 (Track Successful Logins)**：系统会跟踪每个用户通过每种访问方法（Web 界面或CLI）成功登录到 管理中心 的天数 。用户登录后，系统会显示正在使用的接口的成功登录次数。将**跟踪成功登录次数**设置为零（默认值）时，系统不会跟踪或报告成功的登录活动。请参阅跟踪成功登录，第 67 页。
- **最大登录失败次数**：当系统在可配置时间段内临时阻止账户访问之前，用户可以连续输入错误的 Web 界面登录凭证的次数。如果用户在临时锁定生效时继续登录尝试：
  - 系统将在不通知用户临时锁定生效的情况下拒绝访问此账户（即使使用有效密码）。
  - 每次登录尝试时，系统都会继续增加此账户的失败登录次数。
  - 如果用户超过在单个“用户配置”页面上为此账户配置的**最大失败登录次数**，则在管理员用户重新激活此账户之前，此账户将处于锁定状态。
- **设置临时锁定用户的时间（分钟）**： **最大失败登录次数**不为零时临时 Web 界面用户锁定的持续时间（分钟）。
- **允许的最大并发会话数 (Max Concurrent Sessions Allowed)**：可以同时打开的特定类型（只读或读/写）会话数。会话类型由分配给用户的角色决定。如果只为用户分配了只读角色，则该用户的会话会计入（**只读**）会话限制。如果用户具有任何具有写入权限的角色，则会话计入**读/写**会

话限制。例如，如果为用户分配了“管理员”(Admin) 角色，并且**具有读/写权限的用户/CLI 用户的最大会话数**设置为5，则如果已经有五个其他用户登录，则不允许该用户登录。读/写权限。

注释 出于并发会话限制的目的，系统将预定义用户角色和自定义用户角色视为只读，并在 **系统**（⚙）> **用户** > **用户** 和 **系统**（⚙）> **用户** > **用户角色** 上的角色名称中标有（**只读**）。如果用户角色的角色名称中不包含（**只读**），则系统认为该角色为读/写。系统会自动将（**只读**）应用于满足所需条件的角色。不能通过将该文本字符串手动添加到角色名称来将角色设置为只读。

对于每种类型的会话，可以设置从 1 到 1024 的最大限制。当**允许的最大并发会话数 (Max Concurrent Sessions Allowed)** 被设为零（默认值）时，并发会话数不受限制。

如果将并发会话限制更改为更严格的值，系统将不会关闭任何当前打开的会话；但是，它会阻止打开超过指定数量的新会话。

设置密码重用限制

如果启用**密码重用限制 (Password Reuse Limit)**，则系统会为 管理中心 用户保留加密的密码历史记录。用户无法重复使用其历史记录中的密码。您可以为每个用户、每种访问方法（Web接口或CLI）指定存储的密码数量。用户的当前密码会计入此数字。如果降低限制，系统将从历史记录中删除旧密码。增加限制不会恢复已删除的密码。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**用户配置**。

步骤 3 将**密码重用限制**设置为您希望在历史记录中保留的密码数量（最大值为 256）。

要禁用密码重用检查，请输入 0。

步骤 4 点击**保存 (Save)**。

跟踪成功登录

使用此程序可以在指定的天数内为每个用户跟踪成功登录次数。启用此跟踪功能后，系统会在用户登录 Web 界面或 CLI 时显示成功登录次数。

注释 如果减少天数，系统将删除较旧的登录记录。如果随后增加限制，系统不会恢复已删除天数中的登录次数。在这种情况下，报告的成功登录次数可能暂时低于实际次数。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**用户配置**。

步骤 3 将**跟踪成功登录天数**设置为跟踪成功登录的天数（最大值为 365）。

要禁用登录跟踪，请输入 0。

步骤 4 点击**保存 (Save)**。

启用临时锁定

通过指定在锁定生效之前系统允许的连续失败登录尝试次数，来启用临时定时锁定功能。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**用户配置**。

步骤 3 将**最大登录失败次数**设置为临时锁定用户之前最大连续失败登录尝试次数。

要禁用临时锁定，请输入 0。

步骤 4 将**临时锁定用户的时间**（**分钟**）设置为锁定已触发临时锁定的用户的分钟数。

当此值为零时，即使**最大登录失败次数**不为零，用户也不必等待重新尝试登录。

步骤 5 点击**保存 (Save)**。

设置最大并发会话数

可以指定可同时打开的特定类型（只读或读/写）会话的最大数量。会话类型由分配给用户的角色决定。如果为用户分配了只读角色，则该用户的会话计入**只读**会话限制。如果用户具有任何具有写入权限的角色，则会话计入 **读/写** 会话限制。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**用户配置**。

步骤 3 对于每种类型的会话（**只读** 和 **读/写**），将 **允许的最大并发会话数** 设置为可同时打开的该类型会话的最大数量。

要按会话类型对并发用户不应用限制，请输入零。

注释　如果将并发会话限制更改为更严格的值，系统将不会关闭任何当前打开的会话；但是，它会阻止打开超过指定数量的新会话。

步骤 4　点击**保存 (Save)**。

VMware 工具

VMware 工具是专为虚拟机而设计的一套性能增强实用工具。通过这些实用工具，您可以充分利用 VMware 产品方便的功能。在 VMware 上运行的 Firepower 虚拟设备支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

也可以在所有受支持的 ESXi 版本上启用 VMware 工具。有关 VMware 工具全部功能的信息，请参阅 VMware 网站 (http://www.vmware.com/)。

在面向VMware的CiscoSecureFirewallManagementCenter上启用VMware工具

过程

步骤 1　选择**系统**（⚙）> **配置**。

步骤 2　点击 **VMware 工具 (VMware Tools)**.

步骤 3　点击**启用 VMware 工具 (Enable VMware Tools)**。

步骤 4　点击**保存 (Save)**。

漏洞映射

当服务器在发现事件数据库中拥有应用 ID 且流量的数据包报头包含供应商和版本时，系统会针对从主机 IP 地址收到或发送的所有应用协议流量自动将漏洞映射到该地址。

对于在数据包中不包含供应商或版本信息的服务器，可以将系统配置为是否针对这些无供应商和版本信息的服务器将漏洞与服务器流量关联。

例如，在某一主机提供的 SMTP 流量中，其报头不含供应商或版本号。如果在系统配置的“漏洞映射”页面上启用 SMTP 服务器，然后将该配置保存到管理检测到流量的设备的 管理中心，则所有与 SMTP 服务器关联的漏洞都将被添加到该主机的主机配置文件。

尽管检测器会收集服务器信息并将其添加到主机配置文件中，但应用协议检测器不会用于漏洞映射，因为您无法为自定义的应用协议检测器指定供应商或版本，同时也无法为漏洞映射选择服务器。

映射服务器漏洞

此程序需要任何智能许可证或保护经典许可证。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**漏洞映射 (Vulnerability Mapping)**。

步骤 3 有以下选项可供选择：

- 要阻止服务器的漏洞被映射到接收不含供应商或版本信息的应用协议流量的主机上，请为相应服务器清除此复选框。
- 要使服务器的漏洞映射到接收不含供应商或版本信息的应用协议流量的主机上，请选中该服务器对应的复选框。

提示 可以使用**已启用 (Enabled)** 旁边的复选框一次性选中或清除所有复选框。

步骤 4 点击**保存 (Save)**。

Web 分析

默认情况下，为了改善Firepower产品，思科会收集非个人可识别的使用数据，包括但不限于页面交互、浏览器版本、产品版本、用户位置，以及 管理中心 设备的管理 IP 地址或主机名。

接受最终用户许可协议后开始收集数据。如果您不希望思科继续收集这些数据，可以在升级后选择退出。

过程

步骤 1 依次选择**系统 > 配置**。

步骤 2 点击 **Web 分析**。

步骤 3 进行选择，然后点击**保存**。

下一步做什么

（可选）确定是否通过 配置 Cisco Success Network 注册来共享数据。

系统配置的历史记录

功能	最低 管理中心	最低 威胁防御	详情
启用升级后报告	7.4.1	任意	现在，您可以选择在 Cisco Secure Firewall Management Center 的下一个主要版本升级后，生成要在托管设备上部署的待定配置更改报告。 新增/经修改的屏幕：**系统**（⚙）> **配置 (Configuration)** > **升级配置 (Upgrade Configuration)**。 最低威胁防御版本：任意
访问控制性能改进（对象优化）。	7.2.4 7.4.0	任意	**升级影响。管理中心升级到 7.2.4 – 7.2.5 或 7.4.0 后的首次部署可能需要很长时间，并会增加托管设备上的 CPU 使用率。** 当具有重叠网络的访问控制规则时，访问控制对象优化可提高性能并消耗更少的设备资源。在管理中心启用该功能（包括是否通过升级启用）后，在首次部署时在托管设备上进行优化。如果您有大量规则，系统可能需要几分钟到一个小时来评估您的策略并执行对象优化。在此期间，您可能还会发现设备上的 CPU 使用率更高。禁用功能（包括是否通过升级禁用）后，在第一次部署时会发生类似的情况。启用或禁用该功能后，建议您在影响最小的时候部署，比如维护窗口或流量较低的时段。 新增/修改的屏幕 (需要版本 /7.4.1): **系统**（⚙）> **配置** > **f访问控制首选项** > **对象组优化**。 其他版本限制：不支持管理中心版本 7.3.x。
审核日志中的配置更改。	7.4	任意	您可以通过指定配置数据格式和主机，将配置更改作为审核日志数据的一部分传输到外部系统日志服务器。管理中心支持备份和恢复审核配置日志。管理中心高可用性设置中也支持此功能。 新增/修改的屏幕： **系统**（⚙）> **配置** > **审核日志**
法语选项。	7.2	任意	您现在可以将管理中心 Web 接口切换为法语。 新增/修改的屏幕： **系统**（⚙）> **配置** > **语言**。
对大多数连接事件免除事件速率限制。	7.0	任意	现在，将连接数据库的 **最大连接事件数** 值设置为零可免除低优先级连接事件，不计入 FMC 硬件的流量限制。以前，将此值设置为零仅适用于事件存储，不会影响流量限制。 新增/修改的屏幕： **系统**（⚙）> **配置** > **数据库** 支持的平台：硬件 FMC。

功能	最低 管理中心	最低 威胁防御	详情
支持 NTP 服务器的 AES-128 CMAC 认证。	7.0	任意	FMC 和 NTP 服务器之间的连接可以使用 AES-128 CMAC 密钥以及以前支持的 MD5 和 SHA-1 密钥进行保护。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **时间同步**
Subject Alternative Name (SAN)。	6.6	任意	为 FMC 创建 HTTPS 证书时，可以指定 SAN 字段。如果证书确保多个域名或 IP 地址，我们建议您使用 SAN。有关详细信息，请参阅 RFC 5280 第 4.2.1.9 节。 新增/修改的屏幕： **系统**（⚙）> **配置** > **HTTPS 证书**
HTTPS 证书。	6.6	任意	目前，随系统一起提供的默认 HTTPS 服务器证书将在 800 天后自动到期。如果您的设备使用的是在升级到版本 6.6 之前生成的默认证书，则证书有效期因生成证书时使用的 Firepower 版本而异。有关详细信息，请参阅默认 HTTPS 服务器证书，第 22 页。 支持的平台：硬件 FMC。
安全 NTP。	6.5	任意	FMC 支持使用 SHA1 或 MD5 对称密钥身份验证与 NTP 服务器之间的安全通信。 新增/修改的屏幕： **系统**（⚙）> **配置** > **时间同步**
Web 分析。	6.5	任意	接受 EULA 后开始收集网络分析数据。和以前一样，您可以选择不继续共享数据。请参阅Web 分析，第 70 页。
适用于 FMC 的自动 CLI 访问。	6.5	任意	使用 SSH 登录 FMC 时，会自动访问 CLI。虽然强烈建议不要这样做，但您可以使用 CLI `专家` 命令访问 Linux 外壳程序。 **注释** 此功能弃用了为 FMC 启用和禁用 CLI 访问的版本 6.3。由于弃用此选项，虚拟 FMC 不再显示 **系统**（⚙）> **配置** > **控制台配置** 页面，该页面仍显示在物理 FMC 上。
只读和读/写访问的可配置会话限制。	6.5	任意	添加了 **允许的最大并发会话数** 设置。此设置允许管理员指定可同时打开的特定类型（只读或读/写）会话的最大数量。 **注释** 出于并发会话限制的目的，系统认为只读的预定义用户角色和自定义用户角色在 **系统**（⚙）> **用户** > **用户** 和 **系统**（⚙）> **用户** > **用户角色** 名称中标记为 （**只读**）。如果用户角色的角色名称中不包含 （**只读**），则系统认为该角色为读/写。 新增/修改的屏幕： • **系统**（⚙）> **配置** > **用户配置** • **系统**（⚙）> **用户** > **用户角色**

功能	最低 管理中心	最低 威胁防御	详情
能够在管理接口上禁用重复地址检测 (DAD)。	6.4	任意	启用 IPv6 后，可以禁用 DAD。您可能希望禁用 DAD，因为使用 DAD 可能会导致拒绝服务攻击。如果禁用此设置，则需要手动检查此接口是否未使用已分配的地址。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **管理接口** > **接口** > **编辑接口** > **IPv6 DAD** 支持的平台：FMC
能够在管理接口上禁用 ICMPv6 回应应答和目的地不可达消息。	6.4	任意	启用 IPv6 后，此时您可以禁用 ICMPv6 回应应答和目的地不可达消息。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。 新增/经修改的屏幕： **系统**（⚙）> **管理接口** > **ICMPv6** 新增/修改的命令：**configure network ipv6 destination-unreachable**、**configure network ipv6 echo-reply** 支持的平台： FMC (仅限 web 接口)，FTD (仅限 CLI)
全局用户配置设置。	6.3	任意	添加了**跟踪成功登录次数**设置。系统可以跟踪每个 FMC 账户在选定天数内执行的成功登录次数。启用此功能后，用户登录后将看到一条消息，报告他们在过去所配置的天数内成功登录系统的次数。（适用于 Web 界面以及 shell/CLI 访问。） 添加了**密码重用限制**设置。系统可以跟踪每个账户的密码历史记录，以获得可配置的先前密码数量。系统会阻止所有用户重新使用此历史记录中显示的密码。（适用于 Web 界面以及 shell/CLI 访问。） 添加了**最大登录失败次数**和**设置临时锁定用户的时间**（**分钟**）设置。通过这些设置，管理员可以限制系统在可配置时间段内临时阻止账户之前用户可以连续输入错误的 Web 界面登录凭证的次数。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **用户配置** 支持的平台：FMC
HTTPS 证书。	6.3	任意	目前，随系统一起提供的默认 HTTPS 服务器证书将在三年后自动到期。如果设备使用的是在升级到版本 6.3 之前生成的默认服务器证书，则此服务器证书将在首次生成之后的 20 年后到期。如果使用的是默认 HTTPS 服务器证书，则现在系统可以续订此证书。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **HTTPS 证书** > **更新 HTTPS 证书** 支持的平台：FMC

功能	最低 管理中心	最低 威胁防御	详情
能启用和禁用CLI访问权限 FMC。	6.3	任意	FMC Web 接口中对管理员可用的新复选框： 在 **系统**（⚙）> **配置** > **控制台配置**上 **启用 CLI 访问** 。 • 选中：使用 SSH 登录 FMC 可访问 CLI。 • 取消选中：使用 SSH 登录 FMC 可访问 Linux 外壳。此为全新的 6.3 版本以及以往版本至 6.3 版本升级的默认状态。 在版本 6.3 之前，**控制台配置**页面上只有一项设置，它仅适用于物理设备。因此， **控制台配置** 页面在虚拟 FMC 上不可用。通过添加此新选项， **控制台配置** 页面现在显示在虚拟 FMC 和物理设备上。但是，对于虚拟 FMC，此复选框是页面上显示的唯一内容。 支持的平台：FMC

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。