配置干线

SIP 干线概述

如果要部署 SIP 进行呼叫控制信令，请配置 SIP 干线将 Cisco Unified Communications Manager 连接到外部设备，例如 SIP 网关、SIP 代理服务器、Unified Communications applications、会议桥、远程群集或会话管理版本。

在 Cisco Unified CM 管理中，**SIP 干线配置**窗口中包含 Cisco Unified Communications Manager 用于管理 SIP 呼叫的 SIP 信令配置。

您可以使用 IPv4 或 IPv6 寻址、完全限定域名或单个 DNS SRV 记录为 SIP 干线分配多达 16 个不同的目标地址。

SIP 干线前提条件

在配置 SIP 干线之前，请执行以下操作：

- 规划您的网络拓扑，使您能够了解干线连接。
- 确保您了解干线所要连接的设备以及这些设备如何实施 SIP。
- 确保为干线配置了设备池。
- 如果您在干线上部署 IPv6，则必须通过群集范围企业参数或通过可应用到干线的通用设备配置来配置干线的寻址首选项。

- 如果存在与使用干线的应用程序的 SIP 互操作性问题，您可能需要使用默认的 SIP 标准化或透明脚本之一。如果没有任何默认脚本满足您的需要，您可以创建自己的脚本。有关创建自定义的 SIP 标准化和透明度脚本的详细信息，请参阅《*Cisco Unified Communications Manager* 功能配置指南》。

SIP 干线配置任务流程

完成这些任务以设置您的 SIP 干线。

过程

	命令或操作	目的
步骤 1	配置 SIP 配置文件，第 2 页	配置将应用到 SIP 干线的通用 SIP 设置。
步骤 2	配置 SIP 干线安全性配置文件，第 3 页	使用 TLS 信令或 Digest 验证等安全设置配置安全性配置文件。
步骤 3	配置 SIP 干线，第 3 页	设置 SIP 干线并将 SIP 配置文件和安全性配置文件应用到干线。

配置 SIP 配置文件

使用此程序配置具有通用 SIP 设置的 SIP 配置文件，您可分配给使用此配置文件的 SIP 设备和干线。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**设备** > **设备设置** > **SIP 配置文件**。

步骤 2 请执行以下步骤之一：

- 单击**查找**并选择 SIP 配置文件以编辑现有配置文件。
- 单击**新增**以创建新的配置文件。

步骤 3 如果想要您的 SIP 电话和干线支持 IPv4 和 IPv6 堆栈，请选中**启用 ANAT** 复选框。

步骤 4 如果要分配 SDP 透明配置文件以解析 SDP 互操作性，请从 **SDP 透明配置文件** 下拉列表进行。

步骤 5 如果要分配标准化或透明度脚本来解决 SIP 互操作性问题，请从**标准化脚本**下拉列表中选择脚本。

步骤 6 （可选） 对于您可能需要在 Cisco Unified Border Element 中路由呼叫的全局拨号方案复制部署，选中**发送 ILS 学习目标路由字符串**复选框。

步骤 7 完成 **SIP 配置文件配置**窗口中其余字段的设置。 有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 8 单击**保存**。

配置 SIP 干线安全性配置文件

使用 Digest 验证或 TLS 信令加密等安全设置配置 SIP Trunk 安全性配置文件。 将配置文件分配到 SIP 干线时，干线将采用安全性配置文件的设置。

注释 如果没有将 SIP Trunk 安全性配置文件分配给 SIP 干线，Cisco Unified Communications Manager 默认会分配不安全的配置文件。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **安全性** > **SIP Trunk 安全性配置文件**。

步骤 2 单击**新增**。

步骤 3 要启用使用 TLS 的 SIP 信令加密，请执行以下操作：

a) 从**设备安全模式**下拉列表中，选择**已加密**。
b) 从**传入传输类型**和**传出传输类型**下拉列表中，选择 **TLS**。
c) 对于设备验证，在 **X.509 使用者名称**字段中，输入 X.509 证书的使用者名称。
d) 在**传入端口**字段中，输入您要在其上接收 TLS 请求的端口。 TLS 的默认值为 5061。

步骤 4 要启用 digest 验证，请执行以下操作

a) 选中**启用 Digest 验证**复选框。
b) 输入**随机数有效性计时器**值以指示系统生成新的随机数之前必须经过的秒数。默认值为 600（10 分钟）。
c) 要对应用程序启用 digest 验证，请选中**启用应用程序级授权**复选框。

步骤 5 完成 **SIP Trunk 安全性配置文件配置**窗口中的其他字段。有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 6 单击**保存**。

注释 必须在**干线配置**窗口中将配置文件分配给干线，以便干线能够使用这些设置。

配置 SIP 干线

使用此程序配置 SIP 干线。 您可以为 SIP 干线分配多达 16 个目标地址。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **干线**。

步骤 2 单击**新增**。

步骤 3 从**干线类型**下拉列表中，选择 **SIP 干线**。

步骤 4 从**协议类型**下拉列表中，选择与您的部署匹配的 SIP 干线类型，然后单击**下一步**：

- **无（默认）**
- **呼叫控制发现**
- **跨群集分机移动**
- **Cisco 公司间媒体引擎**
- **IP 多媒体系统服务控制**

步骤 5 （可选）如果想要将**通用设备配置**应用到此干线，从下拉列表中选择配置。

步骤 6 如果要在干线上允许加密的媒体，请选中**允许 SRTP** 复选框。

步骤 7 如果要启用所有群集节点的干线，请选中**在所有活动的 Unified CM 节点上运行**复选框。

步骤 8 配置 SIP 干线的目标地址：

a) 在**目标地址**文本框中，输入您要连接到干线的服务器或端点的 IPv4 地址、完全限定的域名或 DNS SRV 记录。

b) 如果干线为双堆栈干线，在**目标地址 IPv6** 文本框中，输入您要连接到干线的服务器或端点的 IPv6 地址、完全限定的域名或 DNS SRV 记录。

c) 如果目标为 DNS SRV 记录，选中**目标地址是 SRV** 复选框。

d) 要添加其他目标，请单击 **(+)**。

步骤 9 从 **SIP Trunk 安全性配置文件**下拉列表框中，分配安全性配置文件。 如果不选择此选项，则会分配不安全的配置文件。

步骤 10 从 **SIP 配置文件**下拉列表中，分配 SIP 配置文件。

步骤 11 （可选） 如果想要将标准化脚本分配给此 SIP 干线，从**标准化脚本**下拉列表中，选择您要分配的脚本。

步骤 12 在**干线配置**窗口中配置任何其他字段。 有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 13 单击**保存**。

SIP 干线相互作用和限制

功能	说明
多个安全 SIP 干线到同一目标	从版本 12.5(1) 开始，Cisco Unified Communications Manager 支持将多个安全 SIP 干线配置到相同的目标 IP 地址和目标端口号。 此功能可提供以下优势： • 带宽优化—为紧急呼叫提供路由，不限制带宽 • 基于特定区域或呼叫搜索空间配置的选择性路由
多个非安全 SIP 干线到同一目标	当具有不同监听端口的多个非安全 SIP 干线指向同一目标或端口时，它们可能会在中间呼叫 INVITE 中错误地使用该端口。 因此，呼叫会被丢弃。

功能	说明
Unified Communications Manager 在收到 SIP 180 振铃时发送 SIP-UPDATE 消息	sip 干线会在“183 会话进度”后收到“180 振铃”时发送“更新”SIP 消息，前提是呼叫流程中支持“更新”值。
通过 BFCP 共享显示	如果要为 Cisco 终端部署演示共享，请确保在所有中间 SIP 干线的 SIP 配置文件中选中**允许通过 BFCP 显示共享**复选框。 **注释** 对于第三方 SIP 终端，您还必须确保在**电话配置**窗口中选中相同的复选框。
iX 通道	如果要部署 iX 媒体通道，请确保在所有中间 SIP 干线使用的 SIP 配置文件中选中**允许 iX 应用程序媒体**复选框。 **注释** 有关加密 iX 通道的详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》。
90 天评估许可证	在 90 天评估期内运行时，您无法部署安全 SIP 干线。 要部署安全的 SIP 干线，您的系统必须已注册到 Smart Software Manager 帐户，并且选择了**允许导出受控的功能**产品注册令牌。

H.323 干线概述

注释 从版本 15 开始，Unified Communications Manager 中将不再提供 H.323 网闸控制选项。 因此，我们建议您将 SIP 干线与位置带宽管理器 (LBM) 结合使用。

如果采用 H.323 部署，H.323 干线提供远程群集和其他 H.323 设备（例如网关）的连接。 H.323 干线支持 Unified Communications Manager 支持的用于群集内通信的大多数音频和视频编解码器，宽带音频和宽带视频除外。 H.323 干线将 H.225 协议用于呼叫控制信令，并将 H.245 协议用于媒体信令。

在 Cisco Unified CM 管理内，H.323 干线可通过群集间干线（非网闸控制）干线类型和协议选项进行配置。

如果采用非网守 H.323 部署，必须为本地 Cisco Unified Communications Manager 可以通过 IP WAN 呼叫的远程群集中的每个设备池配置单独的群集间干线。 群集间干线静态指定远程设备的 IPv4 地址或主机名。

您可以为一个干线配置多达 16 个目标地址。

群集间干线

在两个远程群集之间配置群集间干线连接时，必须在每个群集上配置群集间干线，并匹配干线配置，以使一个干线使用的目标地址与远程群集中干线使用的呼叫处理节点相匹配。 例如：

- 远程群集干线使用“在所有活动节点上运行”—远程群集干线使用所有节点进行呼叫处理和负载均衡。在源自本地群集的本地群集间干线中，为远程群集中的每个服务器添加IP地址或主机名。
- 远程群集未使用“在所有活动节点上运行”—远程群集干线使用Unified Communications Manager组中分配给该干线设备池的服务器进行呼叫处理和负载均衡。在本地群集间干线配置中，您必须添加远程群集干线设备池使用的 Unified Communications Manager 组中的每个节点的 IP 地址或主机名。

保证干线安全

要为 H.323 干线配置安全信令，必须在干线上配置 IPSec。有关详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》。要配置干线以允许媒体加密，请选中**干线配置**窗口中的“允许 SRTP”复选框。

H.323 干线前提条件

计划您的 H.323 部署拓扑。对于群集间干线，请确保您知道相应的远程群集干线使用哪些服务器进行呼叫处理和负载均衡。您必须配置本地群集间干线以连接到远程群集中的干线使用的每个呼叫处理服务器。

如果使用分配给干线设备池的 Cisco Unified Communications Manager 组进行干线上的负载均衡，请完成设备池的核心设置配置任务流程一节中的配置。

配置 H.323 干线

使用此程序可为 H.323 部署配置干线。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **干线**。

步骤 2 单击**新增**。

步骤 3 从**干线类型**下拉列表框中，选择**群集间干线（非网守控制）**。

步骤 4 从**协议**下拉列表框中，选择**群集间 SCCP**。

步骤 5 在**设备名称**文本框中，输入干线的唯一标识符。

步骤 6 从**设备池**下拉列表框中，选择您为此干线配置的设备池。

步骤 7 如果要使用本地群集中的每个节点来处理此干线，请选中**在所有活动的 Unified CM 节点上运行**复选框。

步骤 8 如果要在干线上允许加密的媒体，请选中**允许 SRTP** 复选框。

步骤 9 如果要配置 H.235 传递，请选中**允许通过允许传递**复选框。

步骤 10 在**远程 Cisco Unified Communications Manager 信息**部分，输入此干线连接到的每个远程服务器的 IP 地址或主机名。

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。