配置 AS-SIP 终端

- AS-SIP 概述， 第 1 页
- AS-SIP 前提条件， 第 3 页
- AS-SIP 终端配置任务流程， 第 3 页

AS-SIP 概述

受保障服务 SIP (AS-SIP) 终端符合 MLPP、DSCP、TLS/SRTP 和 IPv6 要求。AS-SIP 可用于 Unified Communications Manager 上的多个终端接口。

许多 Cisco IP 电话都支持 AS-SIP。此外，第三方 AS-SIP 终端设备类型允许配置第三方 AS-SIP 合规终端并让其与 Cisco Unified Communications Manager 一起使用。此外，第三方 AS-SIP 终端设备类型允许配置第三方 AS-SIP 合规通用终端并让其与 Cisco Unified Communications Manager 一起使用。

AS-SIP 功能

以下功能已实现或可用于 AS-SIP 终端：

- MLPP
- TLS
- SRTP
- 优先级的 DSCP
- 错误响应
- V.150.1 MER
- 会议工厂流支持
- AS-SIP 线路 Early Offer

第三方 AS-SIP 电话

第三方电话可在使用第三方 AS-SIP 终端设备类型的 Cisco Unified Communications Manager 中预配置。

运行 AS-SIP 的第三方电话不能通过 Cisco Unified Communications Manager TFTP 服务器配置。客户必须使用本地电话配置机制（通常是网页或 TFTP 文件）来配置。客户必须在与本地电话配置（如电话上的分机 1002 和 Cisco Unified Communications Manager 中的 1002）保持同步的 Cisco Unified Communications Manager 数据库中保存设备和线路配置。另外，如果线路的目录号码发生变更，客户必须确保在 Cisco Unified CM 管理和本地电话配置机制中进行相应的变更。

第三方电话的识别

运行 SIP 的第三方电话不发送 MAC 地址，它们必须使用用户名来标识自己。REGISTER 消息包含以下标头：

```
Authorization: Digest
username=”swhite”,realm=”ccmsipline”,nonce=”GBauADss2qoWr6k9y3hGGVDAqnLfoLk5”,uri
=”sip:172.18.197.224”,
algorithm=MD5,response=”126c0643a4923359ab59d4f53494552e”
```

用户名 **swhite** 必须与在 Cisco Unified CM 管理的**最终用户配置**窗口中配置的某个用户相匹配。管理员配置用户的 SIP 第三方电话；例如，在**电话配置**窗口的 **Digest 用户**字段中配置 **swhite**。

注释 您只能为每个用户 ID 分配一个第三方电话。如果将同一个用户 ID 分配作为多个电话的“Digest 用户”，则它们所分配到的第三方电话将无法成功注册。

第三方 AS-SIP 电话和 Cisco IP 电话配置

下表比较概述 Cisco Unified IP 电话与运行 AS-SIP 的第三方电话之间的配置差异。

表 *1: Cisco IP* 电话与第三方电话之间的配置差异比较

运行 AS-SIP 的电话	与集中式 TFTP 集成	发送 MAC 地址	下载软键文件	下载拨号方案文件	支持 Unified Communications Manager 故障转移和回退	支持重置和重启
Cisco IP 电话	是	是	是	是	是	是
第三方 AS-SIP 设备	否	否	否	否	否	否

注释 并非所有 Cisco IP 电话都支持 AS-SIP。有关支持信息，请参阅您电话型号的电话管理指南

使用 Cisco Unified CM 管理配置运行 SIP 的第三方电话（有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的“配置 SIP 配置文件”主题

）。管理员必须在运行 SIP 的第三方电话上执行配置步骤；请参阅以下示例：

- 确保电话中的代理服务器地址是 Cisco Unified Communications Manager 的 IP 或完全限定域名 (FQDN)。
- 确保电话中的目录号码与 Cisco Unified CM 管理中为设备配置的目录号码匹配。
- 确保电话中的 Digest 用户 ID（有时称为“授权 ID”）与 Cisco Unified CM 管理中的 Digest 用户 ID 匹配。

有关详细信息，请参阅第三方电话随附的文档。

AS-SIP 会议

如果功能调用者（保留者、转接者或会议发起人）支持思科专有功能信令，MOH将会应用到其目标（被保留方、转接前的被转接方、加入会议前的会议参与者）。如果功能调用者不支持思科专有功能信令，则 MOH 不会应用到其目标。此外，如果终端明确指示其为会议混合器，MOH 也不会向目标播放。AS-SIP 会议有两种形式：

- 本地混合
- 会议工厂

本地混合

在 Unified CM 上，看起就像会议发起人同时建立了许多活动的呼叫，其他会议参与者各有一个。发起者在本地主持会议，语音也在那里混合。来自会议发起人的呼叫具有特殊的信令，可防止它连接到 MOH 来源。

会议工厂

会议发起人呼叫位于 SIP 干线外部的会议工厂服务器。通过 IVR 信令，会议发起人构建会议工厂来保留会议桥。会议工厂为会议发起人提供数字地址（可路由的目录号码），然后会议发起人预订会议桥，接收会议列表信息以跟踪参加者。会议工厂发送特殊信令，防止它连接到 MOH 来源。

AS-SIP 前提条件

确定是否有足够的设备许可证单元数。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“智能软件许可证”一章。

AS-SIP 终端配置任务流程

完成以下任务以配置 AS-SIP 终端。

过程

	命令或操作	目的
步骤 1	配置 Digest 用户， 第 4 页	配置最终用户以对 SIP 请求使用 Digest 验证。
步骤 2	配置 SIP 电话安全端口， 第 5 页	Cisco Unified Communications Manager 使用此端口通过 TLS 监听 SIP 电话的 SIP 线路注册。
步骤 3	重新启动服务， 第 5 页	在配置安全端口之后，重新启动 Cisco CallManager 和 Cisco CTL 提供程序服务。
步骤 4	配置 AS-SIP 的 SIP 配置文件， 第 5 页	使用适用于 AS-SIP 终端和 SIP 干线的 SIP 设置配置 SIP 配置文件。 注释 电话特定参数不会下载到第三方 AS-SIP 电话。它们仅由 Cisco Unified Communications Manager 使用。第三方电话必须在本地配置相同的设置。
步骤 5	配置 AS-SIP 的电话安全性配置文件， 第 6 页	您可以使用电话安全性配置文件分配 TLS、SRTP 和 Digest 验证等安全设置
步骤 6	配置 AS-SIP 终端， 第 7 页	使用 AS-SIP 支持配置 Cisco IP 电话或第三方终端。
步骤 7	将设备与最终用户关联， 第 8 页	将终端与用户关联。
步骤 8	配置 AS-SIP 的 SIP 干线安全性配置文件， 第 8 页	您可以使用 SIP 干线安全性配置文件将 TLS 或 Digest 验证等安全功能分配给 SIP 干线。
步骤 9	配置 AS-SIP 的 SIP 干线， 第 8 页	使用 AS-SIP 支持配置 SIP 干线。
步骤 10	配置 AS-SIP 功能， 第 9 页	配置 MLPP、TLS、V.150 和 IPv6 等其他 AS-SIP 功能。

配置 Digest 用户

此程序用于将最终用户配置为使用 digest 验证的 digest 用户。与用户关联设备将通过用户的 digest 凭证进行验证。

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **最终用户**。

步骤 2 执行以下任一操作：

- 单击**新增**以创建新用户。
- 单击**查找**并选择现有用户。

步骤 3 请确保填写以下必填字段：

- 用户 ID

- 姓氏

步骤 4 在 **Digest 凭证**字段中，输入密码。最终用户在使用终端时必须通过此密码进行验证。

步骤 5 填写所有剩余字段。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 单击**保存**。

配置 SIP 电话安全端口

请按照以下步骤操作以配置 SIP 电话安全端口。Cisco Unified Communications Manager 使用此端口通过 TLS 监听 SIP 电话的 SIP 线路注册。

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

步骤 2 在**此服务器的 Cisco Unified Communications Manager TCP 端口设置**部分的 **SIP 电话安全端口**字段中指定端口号，或者将此字段保留为默认设置。默认值为 5061。

步骤 3 单击**保存**。

步骤 4 单击**应用配置**。

步骤 5 单击**确定**。

重新启动服务

请按照以下步骤重新启动 Cisco CallManager 和 Cisco CTL 提供程序服务。

步骤 1 在 Cisco Unified 功能配置界面中，选择**工具** > **控制中心 - 功能服务**。

步骤 2 从**服务器**下拉列表中，选择 Cisco Unified Communications Manager 服务器。
在“CM 服务”区域，Cisco CallManager 显示在**服务名称**列中。

步骤 3 选择与 Cisco CallManager 服务对应的单选按钮。

步骤 4 单击**重新启动**。
服务会重新启动并显示消息：服务已成功重新启动。

步骤 5 重复步骤 3 和步骤 4 以重新启动 Cisco CTL 提供程序服务。

配置 AS-SIP 的 SIP 配置文件

使用此程序采用适用于 AS-SIP 终端和 SIP 干线的 SIP 设置配置 SIP 配置文件。

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **设备设置** > **SIP 配置文件**。

步骤 2 执行以下任一操作：

- 单击**新增**以创建新的 SIP 配置文件。
- 单击**查找**并选择现有的 SIP 配置文件。

步骤 3 输入 SIP 配置文件的**名称**和**说明**。

步骤 4 选中**受保障服务 SIP 符合性**复选框。

注释 必须为 SIP 干线和第三方 AS-SIP 电话选中此复选框。这对于支持 AS-SIP 的 Cisco IP 电话而言不是必需的。

步骤 5 在**电话中使用的参数**部分，为预期的呼叫类型配置 DSCP 优先级值。

注释 您也可以通过群集范围的服务参数配置 DSCP 值。但是，SIP 配置文件中的 DSCP 值将覆盖使用 SIP 配置文件的所有设备的群集范围设置。

步骤 6 从**适用于语音和视频呼叫的 Early Offer 支持**下拉列表中，选择以下选项之一，以配置使用此配置文件的 SIP 干线的 Early Offer 支持：

- 已禁用
- Best Effort（未插入 MTP）
- 必需 (需要时插入 MTP)

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 AS-SIP 的电话安全性配置文件

此程序用于为 SIP 终端配置电话安全性配置文件。您可以使用安全性配置文件分配安全设置，例如 TLS 和 SRTP。

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

步骤 2 请执行以下步骤之一：

- 单击**新增**以创建新的电话安全性配置文件。
- 单击**查找**以编辑现有的配置文件。

步骤 3 对于新的配置文件，从**电话安全性配置文件**下拉框中选择一个选项，选择电话型号**第三方 AS-SIP 终端**，然后单击**下一步**。

- 对于 Cisco IP 电话，选择电话型号，然后单击**下一步**。
- 对于第三方 AS-SIP 终端，选择**第三方 AS-SIP 终端**，然后单击**下一步**。

步骤 4 对于协议，选择 **SIP**，然后单击**下一步**。

步骤 5 输入协议的**名称**和**说明**。

步骤 6 将**设备安全模式**分配给以下设置之一：

配置 AS-SIP 终端

- **已验证**—Cisco Unified Communications Manager 使用 TLS 信令，为电话提供完整性和验证安全功能。
- **已加密**—Cisco Unified Communications Manager 使用 TLS 信令，为电话提供完整性和验证安全功能。此外，SRTP 还会将媒体流加密。

步骤 7 选中**启用 Digest 验证**复选框。

步骤 8 在**电话安全性配置文件配置**窗口完成其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 9 单击**保存**。

配置 AS-SIP 终端

此程序用于配置 AS-SIP 终端。许多 Cisco IP 电话都支持 AS-SIP。此外，您还可以为第三方终端配置 AS-SIP。

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

步骤 2 单击**新增**。

步骤 3 从“电话类型”下拉列表中，选择支持 AS-SIP 的 Cisco IP 电话。否则，选择**第三方 AS-SIP 终端**。

步骤 4 单击**下一步**。

步骤 5 配置以下必填字段。有关字段及其配置选项的更多信息，请参阅联机帮助。

- 设备信任模式—仅适用于第三方 AS-SIP 终端。选择**信任**或**不信任**。
- MAC 地址
- 设备池
- 电话按键模板
- 所有者用户 ID
- 设备安全性配置文件—选择您为 AS-SIP 设置的电话安全性配置文件。
- SIP 配置文件—选择您配置的支持 SIP 的 SIP 配置文件。
- Digest 用户-选择您配置为 digest 用户的用户 ID。必须为用户启用 digest 验证
- 需要 DTMF 接收—选中此复选框将允许终端接受 DTMF 数字。
- 适用于语音和视频呼叫的 Early Offer 支持—选中此复选框可启用 Early Offer 支持。此字段仅对第三方电话显示。

步骤 6 配置 **MLPP 和保密访问级别信息**部分的字段。

步骤 7 单击**保存**。

步骤 8 添加目录号码：

a) 在左侧导航栏中，单击**添加新目录号码**。**目录号码配置**窗口将会打开。
b) 添加**目录号码**。
c) 完成**目录号码配置**窗口中其余字段的设置
d) 单击**保存**。

步骤 9 从**相关链接**中，选择**配置设备**并单击**转至**。

步骤 10 单击**应用配置**。

将设备与最终用户关联

此程序用于将最终用户关联到 AS-SIP 终端。

步骤 1 从 Cisco Unified CM 管理中，选择 **用户管理** > **最终用户**。

步骤 2 单击**查找**并选择要关联到设备的用户。

步骤 3 在**设备信息**部分，单击**设备关联**。
此时将显示“用户设备关联”窗口。

步骤 4 单击**查找**查看可用设备的列表。

步骤 5 选择要关联设备，然后单击**保存选定项/更改**。

步骤 6 从**相关链接**中，选择**返回到用户**，然后单击**前往**。
此时将显示**最终用户配置**窗口，并且您所选的关联设备将在**受控设备**窗格中显示。

配置 AS-SIP 的 SIP 干线安全性配置文件

此程序用于配置支持 AS-SIP 的 SIP 干线的安全性配置文件

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

步骤 2 单击**新增**。

步骤 3 输入安全性配置文件的**名称**。

步骤 4 在**设备安全模式**下拉列表中，选择**已验证**或**已加密**。

步骤 5 **传入传输类型**和**输出传输类型**字段自动更改为 **TLS**。

步骤 6 选中**启用 Digest 验证**复选框。

步骤 7 如果部署的是 V.150，请配置 **SIP V.150 Outbound SDP Offer 过滤**下拉列表的值。

步骤 8 完成**SIP 干线安全性配置文件配置**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 9 单击**保存**。

配置 AS-SIP 的 SIP 干线

此程序用于设置支持 AS-SIP 的 SIP 干线。

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

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有干线。
- 单击**新增**以创建新的干线。

步骤 3 对于新干线，从**干线类型**下拉列表中，选择 **SIP 干线**。

步骤 4 从**干线服务类型**下拉列表中，选择**无（默认值）**，然后单击**下一步**。

步骤 5 为干线输入**设备名称**。

步骤 6 从**设备池**下拉列表中选择设备池。

步骤 7 在**目标地址**字段中，输入您要将干线连接到的服务器的地址。

步骤 8 从 **SIP 干线安全性配置文件**下拉列表中，选择为 AS-SIP 创建的配置文件。

步骤 9 从 **SIP 配置文件**下拉列表中，选择为 AS-SIP 设置的 SIP 配置文件。

步骤 10 完成**干线配置**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 11 单击**保存**。

配置 AS-SIP 功能

上一任务流程中的程序介绍了如何在终端和干线上配置 AS-SIP 支持。下表列出了您可以部署的 AS-SIP 功能，并针对每项功能提供了配置参考。

AS-SIP 功能	**配置说明**
Early Offer	SIP Early Offer 允许您的终端在 INVITE 请求和 200OK 响应期间协商媒体。对于 Early Offer，有两种模式： • Best Effort Early Offer（未插入 MTP） • 必需的 Early Offer (需要时插入 MTP) 通过以下配置窗口中的字段配置 Early Offer 支持。请参阅联机帮助，查看详细的字段说明： **SIP 配置文件配置**窗口 • 适用于语音和视频呼叫的 Early Offer 支持—将此字段配置为在 SIP 干线上启用 Early Offer 支持 • 适用于 Early Offer 和 Re-invite 的 SDP 会话级带宽限定符 • 在呼叫中邀请中发送发送-接收 SDP **电话配置**窗口（仅在使用第三方 AS-SIP 终端设备类型时） • 适用于语音和视频呼叫的 Early Offer 支持 - 选中此复选框可启用 Early Offer 支持

AS-SIP 功能	配置说明
会议工厂	指定 IMS 客户端用于设置会议的 URI： 1. 从 Cisco Unified CM 管理中，选择**系统** > **服务参数**。 2. 从**服务器**下拉列表中，选择 Cisco Unified Communications Manager 服务器。 3. 从**服务**中选择 **Cisco CallManager**。 4. 在**群集范围参数（功能 - 会议）**下，分配 **IMS 会议出厂 URI**。 5. 单击**保存**。
DSCP 标记	DSCP 设置允许您在网络中管理 QoS 和带宽。DSCP 设置用于为每个呼叫分配优先的流量类标签。 您可以通过服务参数配置群集范围 DSCP 设置，并且可以使用 SIP 配置文件为使用该配置文件的用户分配自定义的 QoS 策略。例如，您可以为主管（例如 CEO）或销售团队的呼叫分配较高的优先级，以确保其呼叫在网络带宽问题出现时不会中断。 要配置 DSCP，请参阅DSCP 设置配置任务流程。
IPv6	默认情况下，Cisco Unified Communications Manager 配置为使用 IPv4 寻址。不过，您可以将系统配置为支持 IPv6 堆栈，从而部署具有仅 IPv6 终端的 SIP 网络。 有关配置 IPv6 的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的“双堆栈 IPv6 配置任务流程”一章。
多级优先与预占 (MLPP)	多级优先与预占 (MLPP) 服务可以布置优先呼叫。此功能为与重要组织通信的高级人员以及处于网络压力情况下的人员提供保障，例如全国紧急状态或降级网络情况。 要配置 MLPP，请参阅多级优先与预占任务流程。
安全实时传输协议 (SRTP)	安全实时传输协议 (SRTP) 可用于在您的呼叫中提供对媒体流的加密和验证。 可以在电话使用的**电话安全性配置文件配置**中为电话配置 SRTP。必须将**设备安全模式**字段设置为**已加密**。
传输层信令 (TLS)	传输层安全 (TLS) 通过使用安全端口和证书交换，在两个系统或设备之间提供安全可靠的信令和数据传输。 有关配置 TLS 的详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》中的“TLS 设置”一章。

AS-SIP 功能	配置说明
V.150	V.150 最低基本要求功能使您可以通过 IP 网络在调制解调器中进行安全呼叫。该功能对在传统公用电话交换网络 (PSTN) 上运行的调制解调器和电话设备的大型安装群使用拨号调制解调器。 有关配置 V.150 的详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》中的“Cisco V.150 最低基本要求 (MER)”一章。