# SIP OAuth 模式



## SIP OAuth 模式概述

Unified Communications Manager 安全注册涉及更新 CTL 文件、设置相互证书信任存储库等。如果设备在内部和非内部之间切换，则每次完成安全注册后，都很难更新 LSC 并续订证书权限代理功能 (CAPF)。

SIP OAuth 模式允许您在安全环境中使用 OAuth 刷新令牌进行所有设备身份验证。此功能增强了 Unified Communications Manager 的安全性 。

Unified Communications Manager 验证端点提供的令牌，并将配置文件仅提供给授权的令牌。在 Unified Communications Manager 群集和其他 Cisco 设备上启用基于 OAuth 的授权时，SIP 注册期间的 OAuth 令牌验证将完成。

SIP 注册的 OAuth 支持扩展为

- Cisco Unified Communications Manager12.5 及更高版本的 Cisco Jabber 设备
- Cisco Unified Communications Manager14 及更高版本的 SIP 电话

**注释** 默认情况下，启用 SIP OAUth 时，TFTP 对 SIP 电话而言是安全的。TFTP 文件下载通过受保护的通道进行，并且仅适用于已验证的电话。SIP OAuth 提供端到端的安全信令和媒体加密，无需 CAPF 内部部署和 MRA。

以下是可以为 OAuth 配置的电话安全性配置文件类型。

- Cisco Dual Mode For iPhone（TCT 设备）
- Cisco Dual Mode For Android（BOT 设备）
- Cisco Unified 客户端服务框架（CSF 设备）

- Cisco Jabber 平板电脑版本（TAB 设备）
- 通用设备模板
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 8832NR

# SIP OAuth 模式前提条件

此功能假设您已经完成以下操作：

- 确保已配置 Mobile and Remote Access，并且 Unified Communication Manager 与 Expressway之间已建立连接。
- 确保已通过 **allow export-controlled** 功能将 Unified Communications Manager 注册到智能或虚拟帐户。
- 确保客户端固件支持 SIP OAuth。

# SIP OAuth 模式配置任务流程

完成以下任务为系统配置 SIP OAuth。

过程

| | 命令或操作 | 目的 |
|---|---|---|
| 步骤 1 | 将 CA 证书上载到电话边缘信任 | 将 CA 证书上载到电话边缘信任以获取令牌。此步骤不适用于 Cisco Jabber 设备。 |
| 步骤 2 | 配置刷新登录，第 3 页 | 在 Unified Communications Manager 上启用使用刷新登录流程的 oauth 以通过 SIP OAuth 注册设备。 |
| 步骤 3 | 配置 OAuth 端口，第 4 页 | 为具有 OAuth 注册的每个节点分配用于 OAuth 的端口。 |
| 步骤 4 | 配置到 Expressway-C 的 OAuth 连接，第 4 页 | 配置到 Expressway-C 的经过相互验证的 TLS 连接。 |
| 步骤 5 | 启用 SIP OAuth 模式，第 5 页 | 在发布方节点上使用 CLI 命令启用 OAuth 服务。 |
| 步骤 6 | 重新启动 Cisco CallManager 服务，第 5 页 | 在具有 OAuth 注册的所有节点上重新启动此服务。 |
| 步骤 7 | 在电话安全性配置文件中配置设备安全模式 | 如果要为终端部署加密，请在电话安全性配置文件中配置 OAuth 支持。 |

# 将 CA 证书上载到电话边缘信任

使用此程序将 Tomcat 签名证书的根证书上载到电话边缘信任。

注释 此程序仅对 Cisco 电话执行，不适用于 Cisco Jabber。

**步骤 1** 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

**步骤 2** 单击**上传证书/证书链**。

**步骤 3** 在**上传证书/证书链**窗口中，在**证书用途**下拉列表中选择**Phone-Edge-Trust**。

**步骤 4** 在**上传文件**字段中，单击**浏览**并上传证书。

**步骤 5** 单击**上传**。

# 配置刷新登录

此程序用于为 Cisco Jabber 客户端配置采用 OAuth 访问令牌和刷新令牌的刷新登录。

**步骤 1** 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

**步骤 2** 在 **SSO 和 OAuth 配置**下，将**采用刷新登录流程的 OAuth** 参数设置为**启用**。

**步骤 3** （可选） 在 **SSO 和 OAuth 配置**部分设置任何其他参数。有关参数说明，请单击参数名称。

**步骤 4** 单击**保存**。

# 配置 OAuth 端口

此程序旨在分配用于 SIP OAuth 的端口。

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

**步骤 2** 对每个使用 SIP OAuth 的服务器执行以下操作。

**步骤 3** 选择服务器。

**步骤 4** 在 Cisco Unified Communications Manager **TCP 端口设置**下，设置以下字段的端口值：

- SIP 电话 OAuth 端口

  默认值为 5090。可接受的可配置范围是 1024 到 49151。

- SIP Mobile and Remote Access 端口

  默认值为 5091。可接受的可配置范围是 1024 到 49151。

**注释** Cisco Unified Communications Manager 使用 SIP 电话 OAuth 端口 (5090) 通过 TLS 侦听来自 Jabber 内部设备的 SIP 线路注册。但是，Unified CM 使用 SIP 移动远程访问端口（默认 5091）通过 mLTS 侦听来自 Expressway 上的 Jabber 的 SIP 线路注册。

两个端口都将 Tomcat 证书和 Tomcat-trust 用于传入的 TLS/mTLS 连接。确保您的 Tomcat-trust 存储区能够验证用于 Mobile and Remote Access 的 SIP OAuth 模式的 Expressway-C 证书以准确运行。

在以下情况下，您需要执行额外的步骤将 Expressway-C 证书上传到 Unified Communications Manager 的 Tomcat 证书：

- Expressway-C 证书和 Tomcat 证书不是由同一个 CA 证书签名的。
- Unified CM Tomcat 证书不是 CA 签名的。

**步骤 5** 单击**保存**。

**步骤 6** 对使用 SIP OAuth 的每个服务器重复此程序。

# 配置到 Expressway-C 的 OAuth 连接

此程序用于将 Expressway-C 连接添加到 Cisco Unified Communications Manager 管理。对于使用 SIP OAuth 处于 Mobile and Remote Access 模式的设备，您需要此配置。

**步骤 1** 从 Cisco Unified CM 管理中，选择 **设备** > **Expressway-C**。

**步骤 2** （可选） 在**查找并列出 Expressway-C** 窗口中，单击**查找**以验证从 Expressway-C 推送到 Unified Communications Manager 的 X.509 主题名称/主题备用名称。

**注释** 如果需要，您可以修改这些值。或者，如果条目缺失，请添加 Expressway-C 信息。

如果 Expressway-C 与 Unified Communications Manager 具有不同的域，则管理员需要访问 Cisco Unified CM 管理用户界面，并在 Unified CM 配置中将该域添加到 Expressway C 中。

**步骤 3** 单击**新增**。

**步骤 4** 输入 Expressway-C 的 IP 地址、主机名或完全限定域名。

**步骤 5** 输入说明。

**步骤 6** 输入 Expressway-C 证书中 Expressway-C 的 X.509 主题名称/主题备用名称。

**步骤 7** 单击**保存**。

# 启用 SIP OAuth 模式

使用命令行界面启用 SIP OAuth 模式。在发布方节点上启用此功能也会在所有群集节点上启用此功能。

**步骤 1** 在 Unified Communications Manager 发布方节点上，登录到命令行界面。

**步骤 2** 运行 `utils sipOAuth-mode enable` CLI 命令。

# 重新启动 Cisco CallManager 服务

通过 CLI 启用 SIP OAuth 后，在通过 SIP OAuth 注册终端的所有节点上重新启动 Cisco CallManager 服务。

**步骤 1** 从 Cisco Unified 功能配置中，选择 **工具** > **控制中心** > **功能服务**。

**步骤 2** 从**服务器**下拉列表中，选择服务器。

**步骤 3** 选中 **Cisco CallManager** 服务并单击**重新启动**。

# 在电话安全性配置文件中配置设备安全模式

仅当您将电话的**电话安全性配置文件**中的**设备安全模式**设置为**已加密**时，才需要执行此程序。

**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** 执行下列操作之一：

- 搜索现有电话安全性配置文件
- 单击**新增**

**步骤 3** 在电话安全性配置文件信息部分的 **设备安全模式** 下拉列表中，选择 **已加密**。

**步骤 4** 从 **传输类型** 下拉列表中，选择 **TLS**。

**步骤 5** 选中**启用 OAuth 验证**复选框。

**步骤 6** 单击**保存**。

**步骤 7** 将电话安全性配置文件关联至电话。有关如何应用电话安全电话的详细信息，请参阅Cisco Unified Communications Manager 安全指南中的“将安全性配置文件应用至电话”一节。

注释 重置电话才能使更改生效。

注释 启用 SIP OAuth 模式时，不支持**启用 Digest 验证**和 **TFTP 加密配置**选项。电话将通过 **https(6971)** 安全地下载 TFTP 配置文件，并使用令牌进行验证。

# 为 MRA 模式配置 SIP Oauth 注册电话

使用此程序将 SIP OAuth 注册电话配置为 MRA 模式。

### 开始之前

请确保您的电话已配置为使用激活代码。有关详细信息，请参阅 中的设置注册方法以使用激活代码 Cisco Unified Communications Manager 系统配置指南部分。

注释 在 MRA 上使用 SIP OAuth 时，用户无法使用用户名/密码进行登录，但必须使用基于激活代码的加入

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

**步骤 2** 单击**查找**并选择您要为其配置场外模式的设备。

**步骤 3** 在**设备信息**部分，执行以下步骤：

- 选中 **允许通过 MRA** 激活代码复选框。
- 从**激活代码 MRA 服务域**下拉列表中，选择所需的 MRA 服务域。有关如何配置 MRA 服务域的详细信息，请参阅Cisco Unified Communications Manager 系统配置指南中的 *MRA* 服务域配置一节。

注释 对于 SIP OAuth over MRA 模式，仅使用激活代码，而不使用基于用户名/密码的登录。

**步骤 4** 在**协议特定信息**部分的**设备安全性配置文件**下拉列表中，选择启用 OAuth 的 SIP 配置文件。请确保电话支持 OAuth 固件。有关如何创建安全性配置文件的详细信息，请参阅Cisco Unified Communications Manager 系统配置指南中的配置电话安全性配置文件一节。

步骤 5 点击保持并应用配置。

注释 电话将切换到 MRA 模式并发起与 Expressway 的通信。如果您的内部网络不允许从现场与 Expressway 通信，则电话不会注册，但会准备好在场外接通电源时联系 Expressway。