SIP OAuth 模式

- SIP OAuth 模式概述，第 1 页
- SIP OAuth 模式前提条件，第 2 页
- SIP OAuth 模式配置任务流程，第 2 页

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 Cisco Jabber 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 Cisco Jabber 身份验证。在 Unified Communications Manager SIP 线路上支持 OAuth，可在没有 CAPF 的情况下实现安全的信令和媒体。在 Unified Communication Manager 群集和 Cisco Jabber 终端上启用基于 OAuth 的授权时，SIP 注册期间的 OAuth 令牌验证将完成。

从 Cisco Unified Communications Manager 12.5 版开始，针对 Cisco Jabber 设备扩展了对 SIP 注册的 OAuth 支持。

以下是可以为 OAuth 配置的电话安全性配置文件类型。目前，仅 Cisco Jabber 支持此功能。

- 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

从 Cisco Unified Communications Manager 14.0 版开始，对 SIP 注册的 OAuth 支持扩展到以下 Cisco IP 电话系列企业型号：

- 8811
- 8841

- 8851
- 8851NR
- 8861
- 7811
- 7821
- 7841
- 7861
- 8845
- 8865
- 8865NR
- 7832
- 8832
- 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。

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	为设备启用 OAuth 访问令牌	为 Cisco 7800 和 8800 企业系列 IP 电话中的 SIP 注册启用 OAuth。此步骤不适用于 Cisco Jabber 设备。

	命令或操作	目的
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 5 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 6 页	在具有 OAuth 注册的所有节点上重新启动此服务。
步骤 7	在安全性配置文件中配置 OAuth 支持， 第 6 页	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。

为设备启用 OAuth 访问令牌

此程序用于启用电话的 OAuth 访问令牌。

注释 仅针对电话 SIP 注册的 OAuth 支持配置此企业参数。

过程

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**部分，确保**设备的 OAuth 访问令牌**下拉列表的值设置为**隐式：已注册设备**。

注释 将**设备的 OAuth 访问令牌**的值设置为**显式：需要激活码设备自行激活**，以禁用 OAuth 支持用于电话的 SIP 注册。

步骤 3 单击**保存**。

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。

过程

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。

过程

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。

过程

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。

过程

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。
系统会将只读的**群集 SIPOAuth 模式**企业参数更新为**启用**。

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。

过程

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**。

在安全性配置文件中配置 OAuth 支持

如果您部署支持 SIP OAuth 注册的加密终端，请遵照此程序配置 OAuth 验证。

过程

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

步骤 2 单击 **查找** 并选择电话使用的安全性配置文件。

步骤 3 确保**设备安全模式**为**已加密**且**传输类型**为 **TLS**。

步骤 4 选中**启用 OAuth 验证**复选框。

步骤 5 单击**保存**。

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。