配置 Mobile and Remote Access

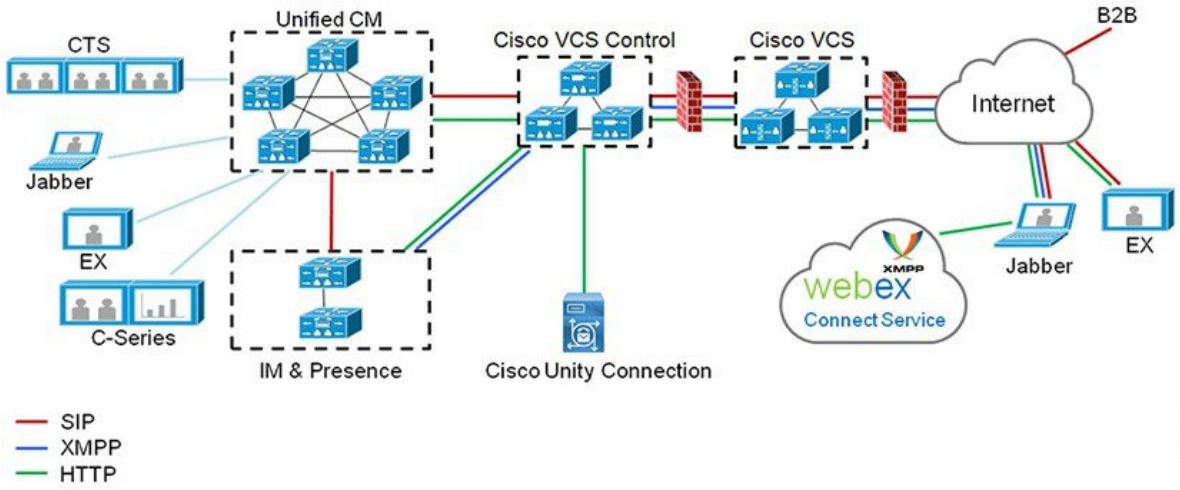
Mobile and Remote Access 概述

Unified Communications Manager Mobile and Remote Access 是思科协作边缘架构的核心部分。它允许 Cisco Jabber 等终端不在企业网络范围内时，有 Unified Communications Manager 提供的注册、呼叫控制、设置、消息传送和在线状态服务。Cisco Expressway 会将移动终端连接到内部网络，为 Unified CM 注册提供安全的防火墙穿越和线路端支持。

总解决方案可以提供：

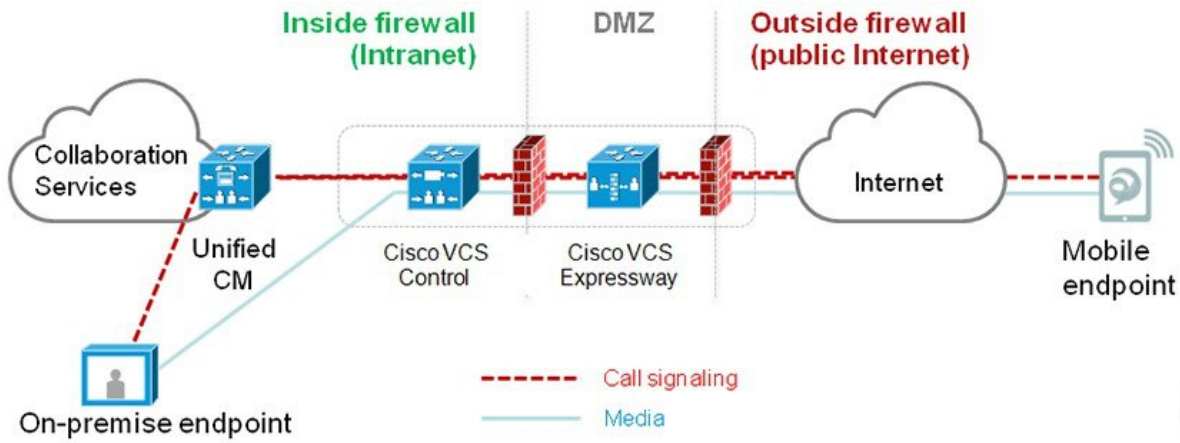
- 非内部访问：为 Jabber 和 EX/MX/SX 系列客户端提供一致的网络外侧体验
- 安全：安全的企业对企业通信
- 云服务：企业级灵活性和可扩展解决方案，提供丰富的 Cisco Webex 集成和服务商服务
- 网关和互操作性服务：媒体和信令标准化并支持非标准终端。

图 *1: Unified Communications*： *Mobile and Remote Access*



第三方 SIP 或 H.323 设备可以注册到 Expressway-C，并在必要时通过 SIP 干线与 Unified CM 注册的设备进行互操作。

图 *2:* 典型的呼叫流程：信令和媒体路径



- Unified CM 为移动及内部终端提供呼叫控制。
- 信令穿越移动终端与 Unified CM 之间的 Expressway 解决方案。
- 媒体穿越Expressway解决方案，直接在终端之间中继；所有媒体在Expressway-C与移动终端之间加密。

配置 Mobile and Remote Access

要启用具有 Mobile and Remote Access 功能的 Cisco Jabber 用户，在 Unified Communications Manager 的**用户配置文件配置**窗口中设置 Mobile and Remote Access 用户策略。非 Jabber 终端不需要 Mobile and Remote Access 用户策略。

此外，您必须使用 Mobile and Remote Access 配置 Cisco Expressway。有关详细信息，请参阅《通过 Cisco Expressway 的 Mobile and Remote Access 部署指南》。

Mobile and Remote Access 前提条件

Cisco Unified Communications Manager 要求

以下要求适用：

- 如果要部署多个 Unified Communications Manager群集，请设置 ILS 网络。
- Mobile and Remote Access 要求您为部署设置 NTP 服务器。确保已为网络部署了 NTP 服务器，并为 SIP 终端配置了电话 NTP 首选项。
- 如果要部署 ICE 进行媒体路径优化，则需要部署可以提供 TURN 和 STUN 服务的服务器。

DNS 要求

对于到 Cisco Expressway 的内部连接，配置以下指向 Unified Communications Manager 的本地可解析 DNS SRV：

```
_cisco-uds._tcp<domain>
```

对于与 Mobile and Remote Access 一起使用的所有 Unified Communications 节点，必须为前向和反向查找创建内部 DNS 记录。当使用 IP 地址或主机名代替 FQDN 时，这使得 Expressway-C 可以找到节点。确保 SRV 记录在本地网络之外不可解析。

Cisco Expressway 要求

此功能要求您将 Unified Communications Manager 与 Cisco Expressway 集成。对于适合 Mobile and Remote Access 的 Cisco Expressway 配置详细信息，请参阅《通过 Cisco Expressway 的 Mobile and Remote Access 部署指南》。

Cisco Jabber 的 Mobile and Remote Access 访问策略支持的最低 Expressway 版本是 X8.10。

证书前提条件

必须在 Unified Communications Manager、IM and Presence Service 与 Cisco Expressway-C 之间交换证书。Cisco 建议您为每个系统使用具有相同 CA 的 CA 签名的证书。在这种情况下：

- 在每个系统上安装 CA 根证书链（对于 Unified Communications Manager 和 IM and Presence Service 服务，将证书链安装到 tomcat-trust 存储区）。
- 对于 Unified Communications Manager，颁发 CSR 来请求 CA 签名的 tomcat（用于 AXL 和 UDS 流量）和 Cisco CallManager（用于 SIP）证书。
- 对于 IM and Presence Service 服务，颁发 CSR 来请求 CA 签名的 tomcat 证书。

注释 如果使用其他 CA，则必须在 Unified Communications Manager、IM and Presence Service 服务、Expressway-C 上安装每个 CA 的根证书链。

注释 您也可以同时对 Unified Communications Manager 和 IM and Presence Service 服务使用自签证书。在这种情况下，必须将 Unified Communications Manager 的 tomcat 和 Cisco CallManager 证书以及 IM and Presence Service 服务的 tomcat 证书上传到 Expressway-C。

Mobile and Remote Access 配置任务流程

如果要部署 Mobile and Remote Access 终端，请在 Unified Communications Manager 中完成这些任务。

过程

	命令或操作	目的
步骤 1	激活 Cisco AXL Web 服务，第 5 页	确保在发布方节点上激活 Cisco AXL Web 服务。
步骤 2	配置视频的最大会话比特率，第 5 页	**可选**。为您的 Mobile and Remote Access 终端配置区域特定设置。例如，如果您希望Mobile and Remote Access 终端使用视频，可能想要增加**视频通话的最大会话比特率**，因为对于某些视频终端而言，默认设置 384 kbps 可能会过低。
步骤 3	配置 Mobile and Remote Access 的设备池，第 6 页	将日期/时间组和区域配置分配给您的 Mobile and Remote Access 终端使用的设备池。
步骤 4	配置 ICE，第 6 页	**可选**。ICE 是一种可选的部署，它使用 STUN 和 TURN 服务分析 Mobile and Remote Access 呼叫的可用媒体路径，然后选择最佳路径。ICE 可能会延长呼叫设置时间，但会提高 Mobile and Remote Access 呼叫的可靠性。
步骤 5	配置 Mobile and Remote Access 的电话安全性配置文件，第 7 页	此程序用于设置要由 Mobile and Remote Access 终端使用的电话安全性配置文件。
步骤 6	配置 Cisco Jabber 用户的 Mobile and Remote Access 访问策略，第 8 页	仅 Cisco Jabber。设置 Cisco Jabber 用户的 Mobile and Remote Access 访问策略。必须使用用户配置文件中的 Mobile and Remote Access 访问权限来启用 Cisco Jabber 用户，才能使用 Mobile and Remote Access 功能。

	命令或操作	目的
步骤 7	为 Mobile and Remote Access 配置用户，第 9 页	对于 Cisco Jabber 用户，您设置的用户策略必须应用于其最终用户配置。
步骤 8	配置 Mobile and Remote Access 终端，第 9 页	配置和预配置使用 Mobile and Remote Access 功能的终端。
步骤 9	为 Mobile and Remote Access 配置 Cisco Expressway，第 9 页	为 Mobile and Remote Access 配置 Cisco Expressway。

激活 Cisco AXL Web 服务

确保在发布方节点上激活 Cisco AXL Web 服务。

过程

步骤 1 从 Cisco Unified 功能配置中，选择 **工具** > **服务激活**。
步骤 2 从**服务器**下拉列表中，选择发布方节点并单击**前往**。
步骤 3 在**数据库和管理服务**下，确认 **Cisco AXL Web 服务已激活**。
步骤 4 如果服务未激活，请选中相应的复选框，然后单击**保存**以激活服务。

配置视频的最大会话比特率

为您的 Mobile and Remote Access 终端配置区域设置。许多情况下，默认设置可能已经足够，但如果您希望 Mobile and Remote Access 终端使用视频，可能需要在区域配置中增大**视频呼叫的最大会话比特率**。对于某些视频终端（例如 DX 系列），384 kbps 的默认设置可能过低。

过程

步骤 1 从 Cisco Unified CM 管理中，选择 **系统** > **区域信息** > **区域**。
步骤 2 执行下列操作之一：

- 单击**查找**并选择用于编辑现有区域中的比特率的区域。
- 单击**新增**以创建新的区域。

步骤 3 在**修改与其他区域的关系**区域中，为**视频呼叫的最大会话比特率**配置新设置。例如 6000 kbps。
步骤 4 配置**区域配置**窗口中的任何其他字段。有关字段及其配置选项的更多信息，请参阅联机帮助。。
步骤 5 单击**保存**。

配置 Mobile and Remote Access 的设备池

当您创建新的区域时，将区域分配给 Mobile and Remote Access 终端使用的设备池。

过程

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

步骤 2 执行以下任一操作：

- 单击**查找**并选择要编辑的现有设备池。
- 单击**新增**以创建新的设备池。

步骤 3 输入**设备池名称**。

步骤 4 选择冗余的 **Cisco Unified Communications Manager 组**。

步骤 5 分配您设置的**日期/时间组**。此组包括您为 Mobile and Remote Access 终端设置的电话 NTP 引用。

步骤 6 从**区域**下拉列表中，选择您为 Mobile and Remote Access 配置的区域。

步骤 7 完成**设备池配置**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 ICE

如果要部署 ICE 来处理 Mobile and Remote Access 呼叫的呼叫设置，请遵照此程序执行。ICE 是一种可选的部署，使用 STUN 和 TURN 服务来分析 Mobile and Remote Access 呼叫的可用媒体路径，并选择最佳路径。ICE 可能会延长呼叫设置时间，但会提高 Mobile and Remote Access 呼叫的可靠性。

开始之前

确定您要部署 ICE 的方式。您可以通过与单一 Cisco Jabber 桌面设备关联的通用电话配置文件或者适用于所有电话的系统范围的默认值，为成组的电话配置 ICE。

作为回退机制，ICE 可以使用 TURN 服务器来中继媒体。请确保您已部署 TURN 服务器。

过程

步骤 1 从 Cisco Unified CM 管理：

- 选择**系统** > **企业电话**以配置 ICE 系统默认值。
- 选择**设备** > **设备设置** > **通用电话配置文件**为终端组配置 ICE，然后选择要编辑的配置文件。
- 选择**设备** > **电话**配置单个 Cisco Jabber 桌面终端的 ICE，然后选择要编辑的终端。

步骤 2 向下滚动到**交互式连接建立 (ICE)** 部分。

步骤 3 将 **ICE** 下拉列表设置为**启用**。

步骤 4 设置**默认候选人类型**：

- **主机**—通过选择主机设备上的 IP 地址获得的候选者。这是默认值。
- **服务器自反**—通过发送 STUN 请求获得的 IP 地址和端口候选者。在许多情况下，这可能代表 NAT 的公共 IP 地址。
- **已中继**—从 TURN 服务器获得的 IP 地址和端口候选者。IP 地址和端口驻留在 TURN 服务器上，以便媒体通过 TURN 服务器中继。

步骤 5 从**服务器自反地址**下拉列表中，选择是否要通过将此字段设置为**启用**或**禁用**来启用类似 STUN 的服务。如果将服务器自反配置为默认候选者，则必须将此字段设置为“启用”。

步骤 6 输入主要和辅助 TURN 服务器的 IP 地址或主机名。

步骤 7 将 **TURN 服务器传输类型**设置为**自动**（**默认设置**）、**UDP**、**TCP** 或 **TLS**。

步骤 8 输入 TURN 服务器的**用户名**和**密码**。

步骤 9 单击**保存**。

注释 如果为通用电话配置文件配置了 ICE，则必须将电话关联到通用电话配置文件，这样电话才能使用配置文件。您可以通过**电话配置**窗口将配置文件应用至电话。

配置 Mobile and Remote Access 的电话安全性配置文件

此程序用于设置要由 Mobile and Remote Access 终端使用的电话安全性配置文件。

过程

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 单击**新增**。

步骤 3 从**电话安全性配置文件类型**下拉列表中，选择您的设备类型。例如，您可以为 Jabber 应用程序选择 **Cisco Unified 客户端服务框架**。

步骤 4 单击**下一步**。

步骤 5 输入配置文件的**名称**。对于 Mobile and Remote Access，名称必须采用 FQDN 格式，并且必须包括企业域。

步骤 6 从**设备安全模式**下拉列表中，选择**已加密**。

注释 此字段必须设置为**已加密**。否则，Expressway 会拒绝通信。

步骤 7 将**传输类型**设置为 **TLS**。

步骤 8 为以下电话保持 **TFTP 已加密配置**复选框为未选中状态，因为对于这些电话，如果启用此选项，Mobile and Remote Access 将不适用：DX 系列；7800 IP 电话；8811、8841、8845、8861 和 8865 IP 电话

步骤 9 完成**电话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 10 单击**保存**。

注释 必须将此配置文件应用于每个 Mobile and Remote Access 终端的电话配置。

配置 Cisco Jabber 用户的 Mobile and Remote Access 访问策略

此程序用于设置 Cisco Jabber 用户的 Mobile and Remote Access 访问策略。必须使用用户配置文件中的 Mobile and Remote Access 访问权限来启用 Cisco Jabber 用户，才能使用 Mobile and Remote Access 功能。Cisco Jabber 的 Mobile and Remote Access 策略支持的最低 Expressway 版本是 X8.10。

注释 Mobile and Remote Access 策略对非 Jabber 用户而言并非必需。

有关用户配置文件的详细信息，请参阅Cisco Unified Communications Manager 系统配置指南中的用户配置文件概述部分。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户配置文件**。

步骤 2 单击**新增**。

步骤 3 输入用户配置文件的**名称**和**描述**。

步骤 4 分配**通用设备模板**以应用到用户的**桌面电话**、**移动和桌面设备**，以及**远程目标/设备配置文件**。

步骤 5 分配**通用线路模板**以应用到此用户配置文件中的用户的电话线路。

步骤 6 如果您希望此用户配置文件中的用户能够使用自我部署功能部署他们自己的电话，请执行以下操作：

a) 选中**允许最终用户部署自己的电话**复选框。

b) 在**一旦最终用户拥有这么多电话即限制部署**字段中，输入允许用户部署的最大电话数量。最大值为 20。

c) 选中**允许预配置已分配给其他最终用户的电话**复选框以确定与此配置文件关联的用户是否有迁移或重新分配已归其他用户所有的设备的权限。默认情况下，此复选框未选中。

步骤 7 如果您希望与此用户配置文件关联的 Cisco Jabber 用户能够使用 Mobile and Remote Access 功能，请选中**启用 Mobile and Remote Access** 复选框。

注释
- 默认情况下，此复选框为选中状态。当取消选中此复选框时，**Jabber 策略**部分会被禁用，并且默认情况下会选中“无服务”客户端策略选项。
- 此设置仅对使用 OAuth 刷新登录名的 Cisco Jabber 用户是必需的。非 Jabber 用户无需此设置即可使用 Mobile and Remote Access。Mobile and Remote Access 功能仅适用于 Jabber Mobile and Remote Access 用户，不适用于任何其他终端或客户端。

步骤 8 为此用户配置文件分配 Jabber 策略。从 **Jabber 桌面客户端策略**以及 **Jabber 移动客户端策略**下拉列表中，选择以下选项之一：

- 无服务 — 此策略禁止访问所有 Cisco Jabber 服务。
- 仅 IM & Presence—此策略仅启用即时消息和在线状态功能。
- IM & Presence、语音和视频呼叫—此策略为所有拥有音频和视频设备的用户启用即时消息、在线状态、语音邮件和会议功能。这是默认选项。

注释 Jabber 桌面客户包括 Cisco Jabber Windows 版本用户和 Cisco Jabber Mac 版本用户。Jabber 移动客户包括 Cisco Jabber iPad 和 iPhone 版本用户以及 Cisco Jabber Android 版本用户。

步骤 9 如果想要此用户配置文件中的用户通过 Cisco Unified Communications Self Care 门户为分机移动或跨群集分机移动设置最长登录时间，选中**允许最终用户设置其分机移动最长登录时间**复选框。

注释 **允许最终用户设置其分机移动最长登录时间**复选框默认未选中。

步骤 10 单击**保存**。

为 Mobile and Remote Access 配置用户

对于 Cisco Jabber 用户，您配置的 Mobile and Remote Access 策略必须在 LDAP 同步期间与您的 Cisco Jabber 用户关联。有关如何预配置最终用户的详细信息，请参阅Cisco Unified Communications Manager 系统配置指南中的“最终用户配置”部分。

配置 Mobile and Remote Access 终端

预配置和配置 Mobile and Remote Access 终端：

- 对于 Cisco Jabber 客户端，请参阅Cisco Unified Communications Manager 系统配置指南中的 *Cisco Jabber* 配置任务流程部分。
- 有关其他终端，请参阅Cisco Unified Communications Manager 系统配置指南中的终端设备配置部分。

为 Mobile and Remote Access 配置 Cisco Expressway

有关如何为 Mobile and Remote Access 配置 Cisco Expressway 的详细信息，请参阅《Mobile and Remote Access Through Cisco Expressway 部署指南》。

具有轻量级保持连接的 MRA 故障转移

终端注册的 MRA 高可用性允许 Cisco Webex 和 Cisco Jabber 检测任何网络元素故障，如 Cisco Expressway-E、Cisco Expressway-C 以及注册路径中的 Cisco Unified Communications Manager 管理，采取纠正措施以通过下一个可用路径注册到 Unified CM。

终端发送轻量级 STUN 保持连接消息以检查注册路径中的连接。当 Unified Communications Manager 收到轻量级 STUN 保持连接消息时，会验证 Cisco Expressway-C IP 并响应该消息。如果 STUN 保持连接消息是从任何其他 IP 接收的，Unified CM 会将其丢弃。

如果注册路径中的节点出现故障，终端将通过其收到的轻量级 STUN 保持连接响应来了解故障，并为未来的消息选择不同的路由路径。此服务可帮助用户进行平稳和连续的来电和去电呼叫，而不考虑中断或其他维护模式。

有关详细信息，请参阅《Mobile and Remote Access Through Cisco Expressway 部署指南》。