部署方案

现场部署

内部部署是一种可让您在公司网络上设置、管理和维护所有服务的部署。

您可以在Cisco Jabber以下模式中部署：

- **完全 UC** — 部署完全 UC 模式、启用即时消息和在线状态功能、配置语音邮件和会议功能，以及为用户提供音频和视频设备。
- **仅 IM** — 要部署仅 IM，要启用即时消息和在线状态功能。不为用户提供设备。
- **仅电话模式** — 在仅电话模式下，用户的主要验证是面向 Cisco Unified Communications Manager。要部署仅电话模式，需要为用户提供用于音频和视频功能的设备。您还可以为用户提供其他服务，例如语音邮件。

在默认产品模式下，用户的主要验证是面向 IM 和在线状态服务器。

内部部署， 支持 Cisco Unified Communications Manager IM and Presence Service

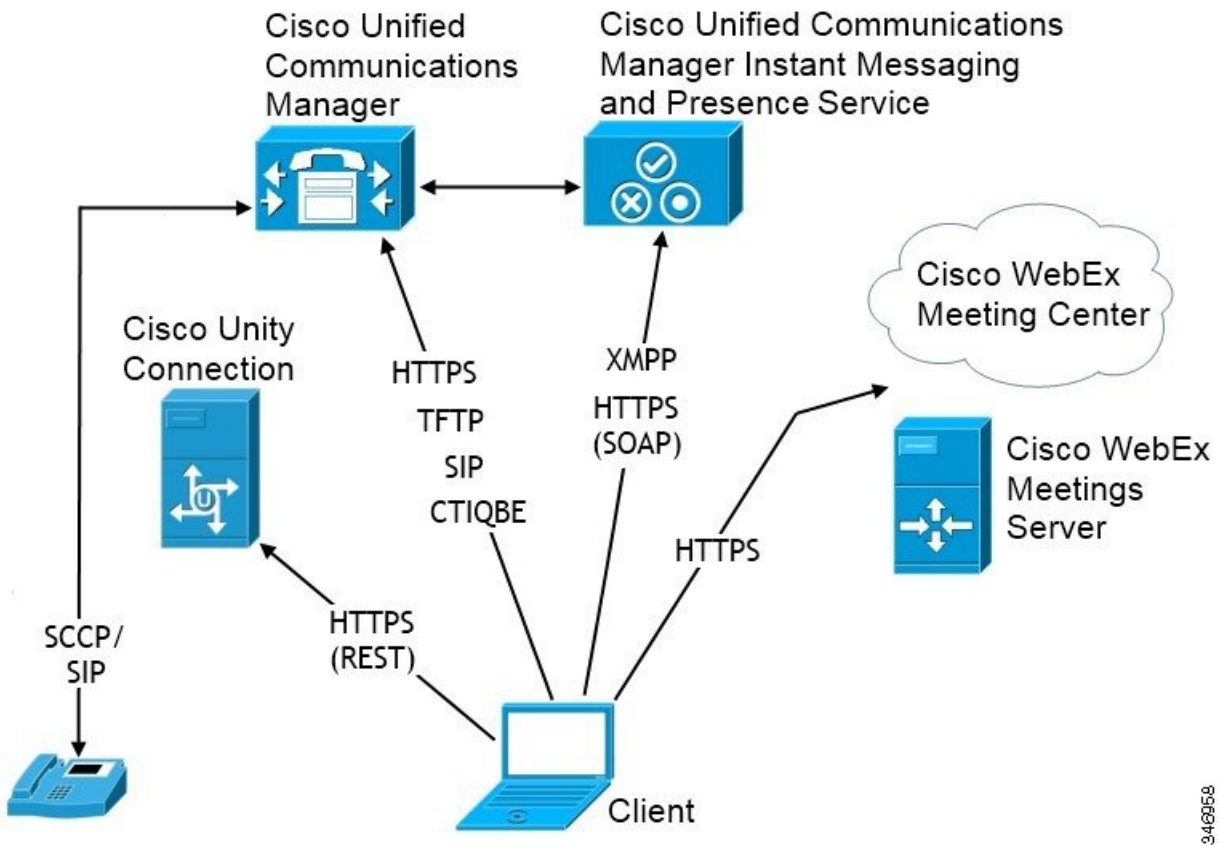
通过 Cisco Unified Communications Manager IM and Presence Service 在内部部署中提供以下服务：

- **在线状态** — 用户可以通过 Cisco Unified Communications Manager IM and Presence Service 发布其忙闲状态，并预订其他用户的忙闲状态。
- **IM** — 通过 Cisco Unified Communications Manager IM and Presence Service 发送和接收即时消息。

- **文件传输** — 通过 Cisco Unified Communications Manager IM and Presence Service 发送和接收文件以及屏幕截图。
- **音频呼叫** — 通过桌面电话设备或使用 Cisco Unified Communications Manager 的计算机发出音频呼叫。
- **视频** — 通过 Cisco Unified Communications Manager 发出视频呼叫。
- **语音邮件** — 通过 Cisco Unity Connection 发送和接收语音留言。
- **会议** — 集成以下各项之一：
  - Cisco Webex Meetings 中心 — 提供托管的会议功能。
  - Cisco Webex Meetings 服务器 — 提供内部会议功能。

下图所示为包含 Cisco Unified Communications Manager IM and Presence Service 的内部部署的架构。

图 *1:* 包含以下内容的内部部署 *Cisco Unified Communications Manager IM and Presence Service*



计算机电话集成

Cisco Jabber Windows 版本 和 Cisco Jabber Mac 版本 适用于第三方应用程序中 Cisco Jabber 的 Mac 支持 CTI。

在拨打、接收和管理电话呼叫时，计算机电话集成 (CTI) 允许您使用计算机处理功能。CTI 应用程序可让您基于主叫方 ID 提供的信息从数据库检索客户信息，并可让您使用交互式语音应答 (IVR) 系统捕获的信息。

有关 CTI 的详细信息，请参阅*Cisco Unified Communications Manager*《系统指南》相应版本中的“CTI”部分。或者对于通过 Cisco Unified Communications Manager API 创建 CTI 控制应用程序的信息，您可访问 Cisco 开发者网络上的以下站点：

- Cisco TAPI： https://developer.cisco.com/site/jtapi/overview/
- Cisco JTAPI： https://developer.cisco.com/site/jtapi/overview/

电话模式下的内部部署

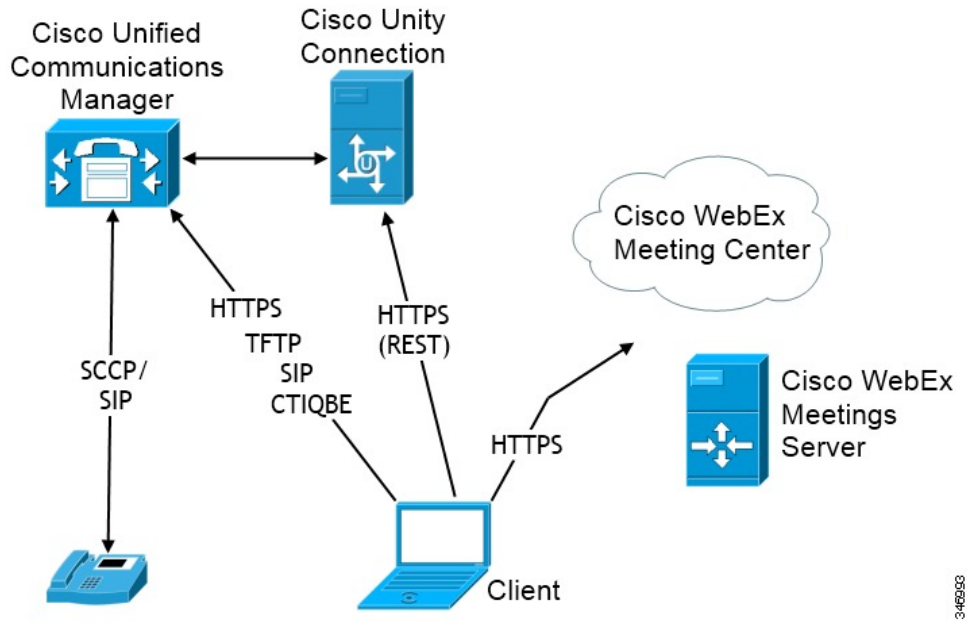
电话模式部署中提供以下服务：

- **联系人** — 这仅适用于移动客户端。Cisco Jabber 会更新电话联系人通讯簿中的联系人信息。
- **音频呼叫** — 通过桌面电话设备或通过 Cisco Unified Communications Manager 在计算机上发出音频呼叫。
- **视频** — 通过 Cisco Unity Connection 发出视频呼叫。
- **语音邮件** — 通过 Cisco Unity Connection 发送和接收语音留言。
- **会议** — 集成以下各项之一：
  - **Cisco Webex Meetings中心** — 提供托管的会议功能。
  - **Cisco Webex Meetings服务器** — 提供内部会议功能。

注释 Cisco Jabber Android 版本 和 Cisco Jabber iPhone 和 iPad 版本 在电话模式下不支持会议。

下图所示为内部部署在电话模式下的架构。

图 2: 电话模式下的内部部署



软终端

软终端模式从 TFTP 服务器下载配置文件，并作为 SIP 注册终端运行。客户端使用 CCMCIP 或 UDS 服务获取要向 Cisco Unified Communications Manager 注册的设备名称。

桌面电话

桌面电话模式使用 Cisco Unified Communications Manager 来创建用于控制 IP 电话的 CTI 连接。客户端使用 CCMCIP 收集与用户相关联的设备的相关信息，并创建可供客户端控制的 IP 电话列表。

在桌面电话模式下，Cisco Jabber Mac 版本不支持桌面电话视频。

扩展与连接

Cisco Unified Communications Manager 的扩展与连接功能可让用户控制设备上的呼叫，例如公共交换电话网 (PSTN) 电话和专用交换机 (PBX) 设备。有关详细信息，请参阅 Cisco Unified Communications Manager 版本的扩展与连接功能。

我们建议您使用 Cisco Unified Communications Manager 9.1 (1) 和更高版本的扩展与连接功能。

“带有联系人功能的电话模式”部署

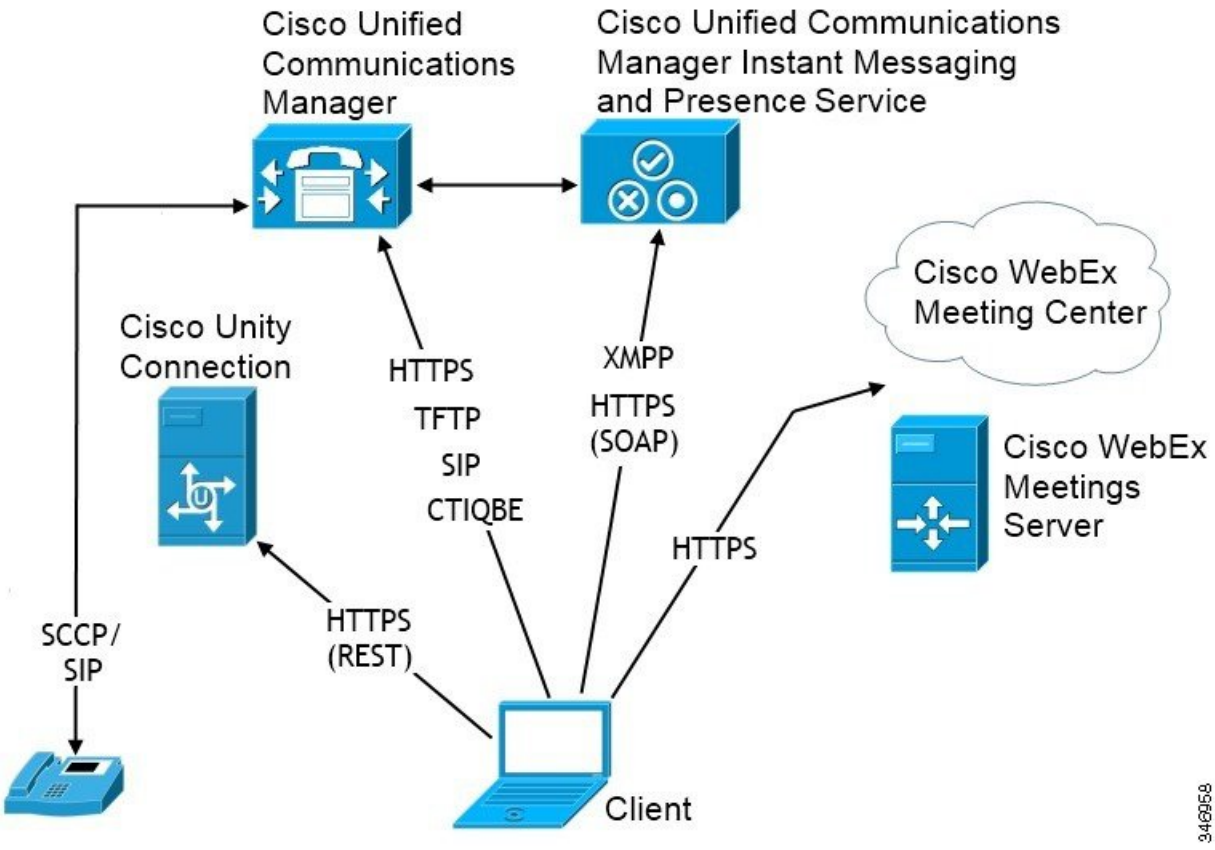
在“带有联系人功能的电话模式”部署中提供以下服务：

- **联系人** — 通过 Cisco Unified Communications Manager IM and Presence Service 提供的联系信息。
- **在线状态** — 用户可以通过 Cisco Unified Communications Manager IM and Presence Service 发布其忙闲状态，并预订其他用户的忙闲状态。

- **音频呼叫** — 通过桌面电话设备或使用 Cisco Unified Communications Manager 的计算机发出音频呼叫。
- **视频** — 通过 Cisco Unified Communications Manager 发出视频呼叫。
- **语音邮件** — 通过 Cisco Unity Connection 发送和接收语音留言。
- **会议** — 集成以下各项之一：
  - Cisco Webex Meetings 中心 — 提供托管的会议功能。
  - Cisco Webex Meetings 服务器 — 提供内部会议功能。

下图所示为包含 Cisco Unified Communications Manager IM and Presence Service 的内部部署的架构。

图 *3*:“带有联系人功能的电话模式”部署



基于云的部署

基于云的部署的使用 Cisco Webex 托管服务。

对于采用 Cisco Webex Messenger 的云和混合部署，可以使用 Cisco Webex 管理工具来管理和监控基于云的部署。您无需为您的用户设置服务配置文件。

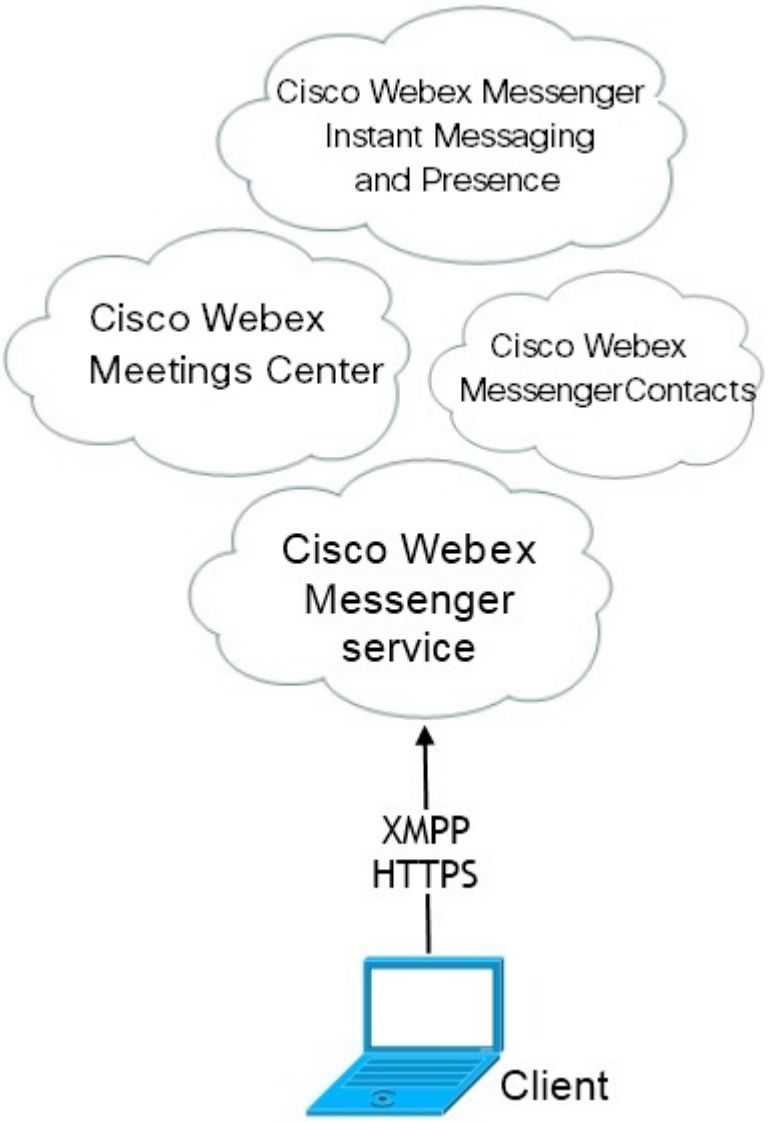
对于采用 Cisco Webex 平台服务 的云和混合部署，可以使用 Cisco 控制中心来管理和监控您的部署。

采用 Cisco Webex Messenger 的基于云的部署

在使用 Webex Messenger 的基于云的部署中提供以下服务：

- **联系人来源** — Cisco Webex Messenger 提供联系人解析。
- **在线状态** — Cisco Webex Messenger 可让用户显示其忙闲状态，并注意其他用户的忙闲状态。
- **即时消息** — Cisco Webex Messenger 可让用户发送和接收即时消息。
- **会议**—Cisco Webex Meetings 中心提供托管的会议功能。

下图所示为基于云的部署的架构。

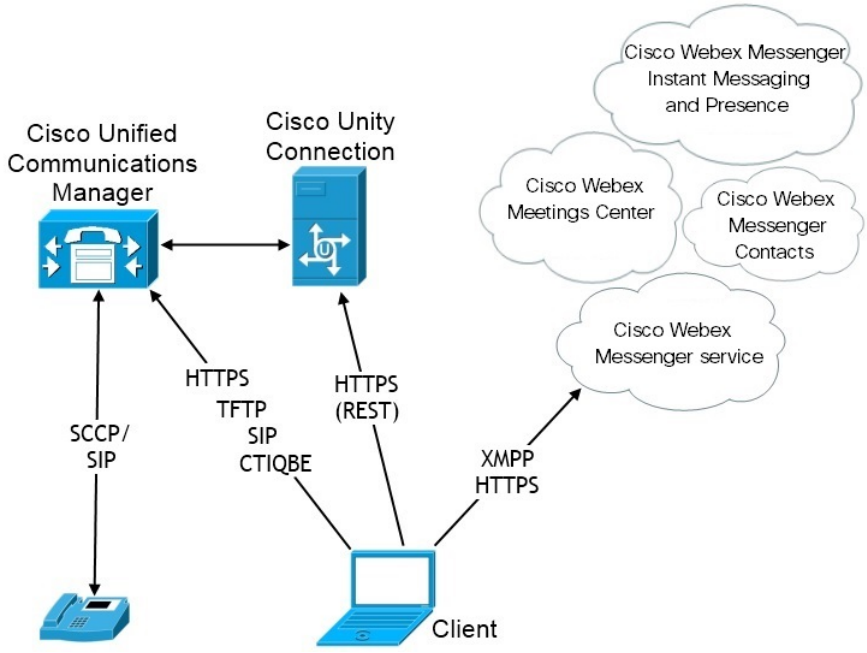


采用 Cisco Webex Messenger 服务的基于云的混合部署

在使用 Webex Messenger 服务的基于云的混合部署中提供以下服务：

- **联系人来源** — Cisco Webex Messenger 服务提供联系人解析。
- **在线状态** — Cisco Webex Messenger 服务可让用户发布其忙闲状态，并预订其他用户的忙闲状态。
- **即时消息** — Cisco Webex Messenger 服务可让用户发送和接收即时消息。
- **音频** — 通过桌面电话设备或使用 Cisco Unified Communications Manager 的计算机发出音频呼叫。
- **视频** — 通过 Cisco Unified Communications Manager 发出视频呼叫。
- **会议**—Cisco Webex Meetings 中心提供托管的会议功能。
- **语音邮件** — 通过 Cisco Unity Connection 发送和接收语音留言。

下图所示为基于云的混合部署的架构。



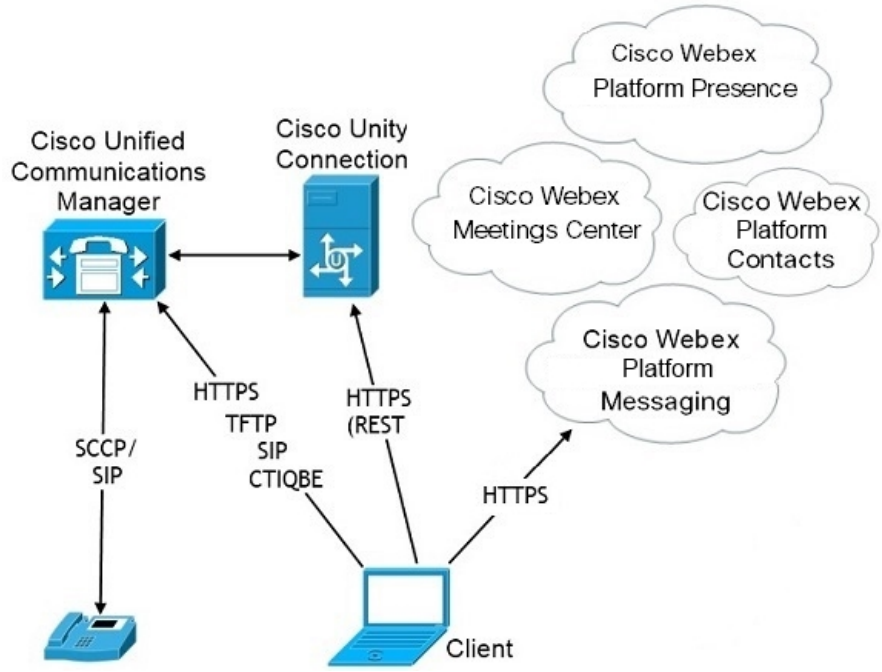
基于云的混合云部署，采用 Cisco Webex 平台服务

在采用 Cisco Webex 平台服务 的基于云的 Jabber 混合部署中提供以下 Jabber 组消息模式服务：

- 联系人来源 — Cisco Webex 平台服务 提供联系人。
- 在线状态 — Cisco Webex 平台服务 可让用户发布其忙闲状态以及查看其他用户的忙闲状态。
- 消息 — Cisco Webex 平台服务 可让用户发送和接收消息。

- 音频 — 通过桌面电话设备或使用 Cisco UC Manager 的计算机发起音频呼叫。
- 视频 — 使用 Cisco UC Manager 发起视频呼叫。
- 会议 — Webex 会议中心提供托管的会议功能。
- 语音邮件 — 通过 Cisco Unity Connection 发送和接收语音留言。

下图所示为采用 Cisco Webex 平台服务 的基于云的 Jabber 混合部署的架构。



Jabber 组消息模式中的联系人

登录流

在 Webex Control Hub 中启用组消息模式时，您必须迁移用户的联系人。

此登录流量概述了迁移用户联系人的过程。流从用户登录到其当前 Jabber 部署开始。您可以启用 Jabber 组消息模式，然后迁移其联系人。

1. 用户登录到其当前的 Jabber 部署，该部署连接到 Cisco UC Manager IM&P 或 Cisco Webex Messenger。
2. 管理员可在 Webex Control Hub 中更改配置，以启用 Jabber 组消息模式，可选启用联系人迁移和 Jabber 呼叫。
3. 第二天，用户登录到其当前的 Jabber 部署。在五分钟内，Jabber 执行服务发现过程，检测到存在该用户的 Cisco Webex 平台服务 部署。
4. Jabber 通过消息“检测到配置更改”提示用户注销 Jabber。

5. 用户再次登录回后，这次对 Cisco Webex 平台服务 进行验证。
6. 如果您启用了联系人迁移，将会显示一则消息，提示用户获取其 Jabber 联系人。如果单击“确定”，Jabber 会取得联系人列表缓存并将其上传到 Cisco Webex 平台服务。如果用户选择“**取消**”，则 Jabber 不会迁移其联系人列表。他们稍后可以单独搜索和添加自己的联系人。

   在联系人迁移期间，Jabber 仅迁移针对 Cisco Webex 平台服务 启用的联系人。Jabber 不会在 Cisco Webex 平台服务 中存储自定义联系人，也无法将其添加到用户的联系人列表。
7. 在 Jabber 连接到 Cisco Webex 平台服务 后，它将连接到 Cisco UC Manager 以下载服务配置文件。如果在具有不同 IdP 的 Cisco Webex 平台服务 和 UC Manager 上启用 SSO，或者仅在一个程序上启用 SSO，则会提示用户输入其凭证。但是，如果 SSO 在使用相同 IdP 的两个程序上，则无需登录。

Jabber 组消息模式和联系人迁移的部署注意事项

您的 Cisco Webex 平台服务 组织需要拥有与服务域相同的域。如果它们是不同的域，则不可能为用户进行联系人迁移。

虚拟环境中的部署

您可以在虚拟环境中部署 Cisco Jabber Windows 版本。

虚拟环境支持以下功能：

- 使用其他 Cisco Jabber 客户端的即时消息和在网状态
- Desk phone control
- 语音邮件
- 在线状态与 Microsoft Outlook 2007、2010 和 2013 的集成
- 移动和远程访问 (MRA)

虚拟环境和漫游配置文件

在虚拟环境中，用户不是总是访问相同的虚拟桌面。为保证一致的用户体验，这些文件在每次启动客户端时必须可供访问。Cisco Jabber 会将用户数据存储在以下位置：

- `C:\Users\`*`username`*`\AppData\Local\Cisco\Unified Communications\Jabber\CSF`
  - **联系人** — 联系人缓存文件
  - **历史记录** — 呼叫和聊天历史记录
  - **照片缓存** — 在本地缓存通讯簿照片
- `C:\Users\`*`username`*`\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`
  - **配置** — 维护用户配置文件并存储配置存储缓存

- **凭证** — 存储加密的用户名和密码文件

由于文件加密和解密与 Windows 用户配置文件关联，因此请确保可访问以下文件夹：

- `C:\Users\username\AppData\Roaming\Microsoft\Crypto`
- `C:\Users\username\AppData\Roaming\Microsoft\Credentials`
- `C:\Users\username\AppData\Local\Microsoft\Crypto`
- `C:\Users\username\AppData\local\Microsoft\Credentials`

注释 在非持久性虚拟部署基础设施 (VDI) 模式下使用 Cisco Jabber 时，不支持缓存 Cisco Jabber 凭证。

如果需要，您可以通过将文件和文件夹添加到排除列表来将它们从同步中排除。要同步已排除文件夹中的子文件夹，请将子文件夹添加到包含列表。

要保留个人用户设置，请执行以下操作：

- 请勿排除以下目录：
  - `AppData\Local\Cisco`
  - `AppData\Local\JabberWerxCPP`
  - `AppData\Roaming\Cisco`
  - `AppData\Roaming\JabberWerxCPP`
- 使用以下专用的配置文件管理解决方案：
  - **Citrix 配置文件管理** — 提供适用于 Citrix 环境的配置文件解决方案。在采用随机托管虚拟桌面分配的部署中，Citrix 配置文件管理在安装在其上的系统和用户存储之间同步每个用户的整个配置文件。
  - **VMware View Persona Management** — 保留用户配置文件，并将其与远程配置文件存储库动态地同步。VMware View Persona Management 不需要配置 Windows 漫游配置文件，并且可以绕过 VMware Horizon View 用户配置文件管理中的 Windows Active Directory。Persona Management 增强了现有漫游配置文件的功能。

部署 Jabber VDI 软终端

要在具有呼叫功能的虚拟环境中部署 Jabber，您需要部署 Jabber Softphone for VDI。

部署 Jabber VDI 软终端的工作流程取决于部署在本地还是混合环境中，并遵循 Jabber 部署工作流程，直至应用程序安装，在此时，您可以遵循 Jabber VDI 软终端部署和安装工作流程。

要获取用于 Jabber VDI 软终端的内部部署工作流程，请参阅 Cisco Jabber 内部部署部署和安装工作流程部分中的完全 *UC* 部署工作流程。

要获取用于 Jabber VDI 软终端的混合部署工作流程，请参阅Cisco Jabber 的云和混合部署云和混合部署工作流流程部分中的使用 *Webex Messenger* 的混合部署工作流程。

企业移动性管理部署

Jabber 支持将两个基于 SDK 的客户端用于企业移动性管理 (EMM) 部署：

- Cisco Jabber Intune 版本
- Cisco Jabber BlackBerry 版本

您的组织可以部署这些客户端，以在允许“自带设备”的部署中，实施在移动设备上使用 Jabber 的策略。例如，这些策略可以：

- 防止使用不安全的越狱或根设备。
- 强制实施最低操作系统和应用程序版本。
- 阻止用户复制 Jabber 中的数据并将其粘贴到另一个应用程序中。

使用新的 EMMType 参数控制用户可以登录的 Jabber 客户端。

记住 这些客户端的发布周期会有延迟。客户端的发布要晚于对应的 Jabber Android 版本以及 Jabber iPhone 和 iPad 版本。

通过 Jabber Intune 版本进行 EMM

在部署中使用 Jabber Intune 版本客户端时，管理员会在 Microsoft Azure 中配置您的管理策略。用户需从 App Store 或 Google Play Store 下载新的客户端。用户运行新客户端时，其会与管理员创建的策略同步。

注意 Jabber Intune 版本不支持 iOS 平台上的 Apple 推送通知 (APN)。当您将 Jabber 置于后台时，iOS 设备可能收不到聊天消息和呼叫。

注释 对于 Android 设备，用户首先需安装 Intune 公司门户。然后，他们通过门户运行客户端。

Jabber Intune 版本的一般设置流程如下：

1. 创建新的 Azure AD 租户。
2. 创建新的 AD 用户或同步您的内部 AD 用户。
3. 创建 Office 365 组或安全组并添加您的用户。

4. 将 Jabber Intune 版本客户端添加到 Microsoft Intune。
5. 在 Microsoft Intune 中创建和部署策略。
6. 用户登录到客户端并同步以接收您的策略。

有关这些步骤的详细信息，请参阅 Microsoft 文档。

下表列出了我们在 Cisco Jabber 的应用程序保护策略中支持的 Microsoft Intune 限制：

限制	Android	iPhone 和 iPad
将数据发送到其他应用程序	是	是
保存组织数据的副本	是	是
剪切、复制和粘贴到其他应用程序	是	是
屏幕截图	是	不适用
PIN 尝试次数上限	是	是
离线宽限期	是	是
应用程序最低版本	是	是
在越狱或根设备上使用	是	是
设备操作系统最低版本	是	是
补丁最低版本	是	不适用
用于访问的工作（或学校）帐户凭证	是	是
再次查看访问要求	是	是

通过 Jabber BlackBerry 版本进行 EMM

在部署中使用 Jabber BlackBerry 客户端时，您的管理员会在 BlackBerry 统一终端管理 (UEM) 中配置管理策略。用户需从 App Store 或 Google Play Store 下载新的客户端。Jabber BlackBerry 版本正在申请 BlackBerry 认证，尚未在 BlackBerry 市场推出。

重要事项 由于客户端正在申请 BlackBerry 认证，我们必须向您的组织授予访问权限。要获得访问权限，请联系我们 (jabber-mobile-mam@cisco.com)，并从客户的 BlackBerry UEM 服务器提供其组织 ID。

新客户端集成了 BlackBerry Dynamics SDK，并且可以直接从 BlackBerry UEM 提取策略。客户端绕过 BlackBerry Dynamics 进行连接和存储。BlackBerry Dynamics SDK 不支持 FIPS 设置。

您的聊天、语音和视频流量会绕过 BlackBerry 基础设施。当客户端不在内部时，它需要通过 Cisco Expressway 对所有流量进行移动和远程访问。

注意 Jabber BlackBerry 版本不支持 iOS 平台上的 Apple 推送通知 (APN)。当您将 Jabber 置于后台时，iOS 设备可能收不到聊天消息和呼叫。

注释 适用于 Android 的 Jabber BlackBerry 版本需要 Android 6.0 或更高版本。

适用于 iOS 的 Jabber BlackBerry 版本需要 iOS 11.0 或更高版本。

对于 BlackBerry Dynamics，管理员可设置策略，以控制对 Jabber BlackBerry 版本客户端的使用。

Jabber BlackBerry 版本的一般设置流程如下：

1. 在 UEM 中创建服务器。
2. 将 Jabber BlackBerry 版本客户端加入 BlackBerry Dynamics。
3. 在 BlackBerry Dynamics 中创建或导入用户。

注释 对于 Android 用户，可以选择在 BlackBerry Dynamics 中生成访问密钥。

4. 在 UEM 中创建和部署策略。注意 Jabber BlackBerry 版本应用程序配置上这些设置的行为：
   - 如果启用可选的 DLP 策略，BlackBerry 要求：
     - 使用 BlackBerry Works 发送电子邮件。
     - 在 iOS 设备中使用 BlackBerry Access 进行 SSO 身份验证。在 Expressway 和 Unified Communications Manager 上为 iOS 启用**使用本地浏览器**。然后，将 **ciscojabber** 方案添加到 BlackBerry UEM 中的 Blackberry 访问策略。
   - 此列表显示了 Jabber 参数，这些参数对于在 Jabber BlackBerry 版本部署中通过应用程序配置进行设置非常有用。有关这些参数的更多详情，请参阅部署指南的 *Cisco Jabber Android*、*iPhone* 和 *iPad* 版本的 *URL* 配置部分：

字段	iOS 支持	Android 支持
禁用交叉启动 Webex Meetings [1]	是	是
服务域	是	是
语音服务域	是	是
服务发现排除的服务	是	是

字段	iOS 支持	Android 支持
服务域 SSO 电子邮件提示	是	是
无效的证书行为	是	是
已启用电话	是	是
允许 Url 预配置	是	是
IP 模式	是	是

[1] 启用 Webex Meetings 的交叉启动后，它可以在不允许非 Dynamics 应用程序的 BlackBerry Dynamics 容器中作为例外运行。

5. 用户登录到客户端。

有关这些步骤的详细信息，请参阅 BlackBerry 文档。

下表列出了我们在 Cisco Jabber 的应用程序保护策略中支持的 BlackBerry 限制：

组	功能	Android	iPhone 和 iPad
IT 策略	在没有网络连接的情况下擦除设备	是	是
激活	允许的版本	是	是
BlackBerry Dynamics	密码	是	是
	数据泄露防护 - 不允许将数据从 BlackBerry Dynamics 应用程序复制到非 BlackBerry Dynamics 应用程序	是	是
	数据泄露防护 - 不允许将数据从非 BlackBerry Dynamics 应用程序复制到 BlackBerry Dynamics 应用程序	是	是
	数据泄露防护 - 不允许在 Android 和 Windows 10 设备上截屏	是	不适用
	数据泄露防护 - 不允许在 iOS 设备上录制和分享屏幕	不适用	是
	数据泄露防护 - 不允许在 iOS 设备上自定义键盘	不适用	是
企业管理代理配置文件	允许个人应用程序集合	是	是
合规性配置文件	根操作系统或失败的证明	是	是
	安装了受限的操作系统版本	是	是
	未安装所需的安全修补程序级别	是	不适用

Jabber BlackBerry 版本中的 IdP 连接

在 Jabber Android 以及 iPhone 和 iPad 版本部署中，客户端会连接到 DMZ 中的身份提供程序 (IdP) 代理。然后，代理会将请求传递到内部防火墙背后的 IdP 服务器。

在 Jabber BlackBerry 版本中，您有备用路径可用。如果在 BlackBerry UEM 中启用了 DLP 策略，则 iOS 设备上的客户端可以安全地直接隧道传输到 IdP 服务器。要使用此设置，请按如下方式配置部署：

- 在 Expressway 和 Unified CM 上为 iOS 启用**使用本地浏览器**。
- 将 **ciscojabber** 方案添加到 BlackBerry UEM 中的 Blackberry 访问策略。

Android OS 上的 Jabber BlackBerry 版本始终连接到 SSO 的 IdP 代理。

如果部署中仅包含在 iOS 上运行的设备，不需要在 DMZ 中使用 IdP 代理。但是，如果部署中包含在 Android OS 上运行的设备，则需要 IdP 代理。

iOS 上的应用程序传输安全

iOS 包括应用程序传输安全 (ATS) 功能。ATS 要求 Jabber BlackBerry 版本和 Jabber Intune 版本使用可靠的证书和加密，通过 TLS 建立安全的网络连接。ATS 会阻止与没有 X.509 数字证书的服务器的连接。证书必须通过以下检查：

- 完整的数字签名
- 有效的到期日期
- 与服务器的 DNS 名称匹配的名称
- 从 CA 到受信任锚点证书的有效证书链

注释 有关属于 iOS 一部分的受信任锚点证书的详细信息，请参阅 *iOS* 中可用的受信任根证书列表，网址：https://support.apple.com/en-us/HT204132。系统管理员或用户也可以安装自己信任的锚点证书，只要同样满足要求即可。

有关 ATS 的详细信息，请参阅阻止不安全的网络连接，网址：https://developer.apple.com/documentation/security/preventing_insecure_network_connections。

Remote Access

您的用户可能需要在公司网络之外的位置访问他们的工作。您可以使用其中一种用于Remote Access 的 Cisco 产品来为他们提供工作访问权限。

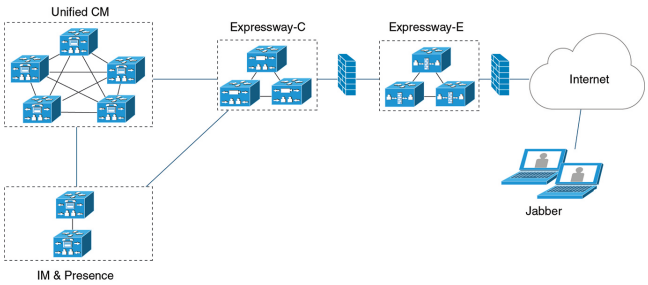
Jabber 未经任何第三方 VPN 客户端测试或验证。

Expressway for Mobile and Remote Access

适用于 Cisco Unified Communications Manager 的 Expressway for Mobile and Remote Access 可让用户从公司防火墙外部访问其协作工具而不使用虚拟专用网 (VPN)。通过思科协作网关，客户端可以从远程位置（例如，公共 Wi-Fi 网络或移动数据网络）安全地连接到企业网络。

图 *4:* 客户端连接到 *Expressway for Mobile and Remote Access* 的方式

下图展示了 Expressway for Mobile and Remote Access 的架构。



使用 Expressway for Mobile and Remote Access 首次登录 Jabber

适用于 Cisco Jabber 移动客户端。

用户首次可从公司防火墙外部使用 Expressway for Mobile and Remote Access 登录到客户端，以连接到服务。不过，在以下情况下，最初可在公司网络上登录：

- 如果语音服务域与其他服务域不同，则用户必须位于公司网络内，以从 `jabber-config.xml` 文件获取正确的语音服务域。对于混合部署，管理员可以配置 VoiceServicesDomain 参数，请参阅最新版本的《*Cisco Jabber* 的参数参考指南》。在此情况下，用户无需在公司网络内登录。
- 如果 Cisco Jabber 必须完成 CAPF 注册过程，此步在使用安全或混合模式群集时需要完成。

如果用户通过 Expressway for Mobile and Remote Access 环境使用安全电话，我们不支持在公共网络上进行首次登录。如果配置适用于带有加密 TFTP 的安全配置文件，则首次登录必须在内部完成，以便进行 CAPF 注册。在没有 Cisco Unified Communications Manager、Expressway for Mobile and Remote Access 以及 Cisco Jabber 增强版的情况下，不支持在公共网络上进行首次登录。但我们支持：

- 加密 TFTP，通过内部进行首次登录。
- 未加密的 TFTP，通过 Expressway for Mobile and Remote Access 或内部进行首次登录。

支持的服务

下表总结了客户端使用 Expressway for Mobile and Remote Access 远程连接到 Cisco Unified Communications Manager 时支持的服务和功能。

表 *1:* 支持的 *Expressway for Mobile and Remote Access* 服务的摘要

服务	支持	不支持
通讯录		

服务	支持	不支持
UDS 目录搜索	X	
LDAP 目录搜索		X
通讯簿照片分辨率	X * 使用 Cisco Expressway-C 上的 HTTP 白名单	
域内联合	X * 联系人搜索支持取决于您的联系人 ID 的格式。有关详细信息，请参阅以下注释。	
域间联合	X	
即时消息和在线状态		
内部	X	
云部署	X	
聊天	X	
群聊	X	
永久聊天	X	
高可用性：内部部署	X	
文件传输：内部部署	X 可用于使用 Cisco Unified Communications Manager IM and Presence Service 10.5(2) 或更高版本进行文件传输的高级选项，请参阅下面的注释。	
文件传输：云部署	X	
视频屏幕共享 — BFCP	X（用于移动客户端的 Cisco Jabber 仅支持 BFCP 接收。）	
仅 IM 屏幕共享		x
音频和视频		
音频和视频呼叫	X * Cisco Unified Communications Manager 9.1(2) 及更高版本	

服务	支持	不支持
桌面电话控制模式 (CTI)（仅限桌面客户端）		X
扩展与连接（仅限桌面客户端）		X
远程桌面控制（仅限桌面客户端）		X
静默监听和呼叫录音		X
Dial via Office — 反转（仅限移动客户端）	X	
会话永久性		X
早期媒体		X
自助门户访问		X
按正常途径注册	X * 适用于 Cisco Jabber Android 版本。 Jabber for Android 支持从 Cisco Unified Communications Manager Release 10.5.(2) 10000-1 通过 Expressway for Mobile and Remote Access 按正常途径注册。	
共用线	X 先决条件： • Cisco Expressway 升级到 X8.9.1 或更高版本 • Cisco Unified Communications Manager 升级到 11.5 SU(2) 或更高版本	
语音邮件		
可视语音邮件	X * 使用 Cisco Expressway-C 上的 HTTP 白名单	
Cisco Webex Meetings		

服务	支持	不支持
内部		X * 不支持，但从 Jabber 11.6 之后的内部 Cisco Webex Meeting Server 除外。
云部署	X	
Cisco Webex 屏幕共享（仅限桌面客户端）	X	
安装（桌面客户端）		
安装程序更新	X * 使用 Cisco Expressway-C 上的 HTTP 白名单	X 在 Cisco Jabber Mac 版本上不受支持
可以定制		
自定义 HTML 选项卡		X
Enhanced911 提示	X * 为确保网页为在公司网络外部运行的所有 Jabber 客户端正确呈现，网页必须是静态 HTML 页面，因为 E911NotificationURL 参数不支持脚本和链接标签。有关详细信息，请参阅最新的《*Cisco Jabber* 参数参考指南》。	
安全		
媒体的 ICE 协议	X	
CAPF 注册		X
单点登录	X	
高级加密标准 (AES) 256 和 TLS1.2	X * 适用于 Cisco Jabber Android 版本。 仅公司 Wi-Fi 支持高级加密	
故障诊断（仅限桌面客户端）		

服务	支持	不支持
问题报告生成	X	
问题报告上传		X
高可用性（故障转移）		
音频和视频服务		X
语音邮件服务		X
IM and Presence Service	X	
联系人搜索	X	
联系人解析	X	
配置管理		
快速登录	X	
验证和授权		
对 SSO Jabber 用户的 O-Auth 支持	X	

通讯录

当客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，其支持具有以下限制的目录集成。

- LDAP 联系人解析 — 在公司防火墙外部时，客户端无法使用 LDAP 进行联系人解析。相反，客户端必须使用 UDS 进行联系人解析。

  当用户在公司防火墙内时，客户端可以使用 UDS 或 LDAP 进行联系人解析。如果您在公司防火墙内部署 LDAP，Cisco 建议您将 LDAP 目录服务器与 Cisco Unified Communications Manager 同步，以让客户端在用户在公司防火墙之外时连接到 UDS。

- 目录照片分辨率—要确保客户端能够下载联系人照片，您必须将您托管联系人照片所在的服务器添加到 Cisco Expressway-C 服务器的白名单中。要将服务器添加到 Cisco Expressway-C 白名单，请使用 **HTTP 服务器允许**设置。有关详细信息，请参阅相关的 Cisco Expressway 文档。

- 域内联合 — 当您部署域内联合并且客户端与防火墙外部的 Expressway for Mobile and Remote Access 连接时，仅当联系人 ID 使用以下格式之一时，才支持联系人搜索：

  - sAMAccountName@domain
  - UserPrincipleName (UPN)@domain
  - EmailAddress@domain
  - employeeNumber@domain

- telephoneNumber@domain

- 使用 XMPP 进行域间联合 — Expressway for Mobile and Remote Access 不会自行启用 XMPP 域间联合。通过 Expressway for Mobile and Remote Access 进行连接的 Cisco Jabber 客户端如果已在 Cisco Unified Communications Manager IM and Presence 上启用，则可以使用 XMPP 域间联合。

即时消息和在线状态

当客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，其支持具有以下限制的即时消息和在线状态。

文件传输对桌面和移动客户端具有以下限制：

- 对于 Cisco Webex 云部署，支持文件传输。
- 对于使用 Cisco Unified Communication IM and Presence Service 10.5(2) 或更高版本的内部部署，支持**托管文件传输**选择，但不支持**对等**选项。
- 对于采用 Cisco Unified Communications Manager IM and Presence Service 10.0(1) 的内部部署或早期部署，不支持文件传输。
- 对于采用不受限 Cisco Unified Communications Manager IM and Presence 服务器的 Expressway for Mobile and Remote Access 部署，不支持托管文件传输。

音频和视频呼叫

当客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，其支持具有以下限制的音频和视频呼叫。

- Cisco Unified Communications Manager — Expressway for Mobile and Remote Access 通过 Cisco Unified Communications Manager 版本 9.1.2 和更高版本支持视频和语音呼叫。
- 桌面电话控制模式 (CTI)（仅限桌面客户端）— 客户端不支持桌面电话控制模式 (CTI)，包括分机移动性。
- 扩展与连接（仅限桌面客户端）— 客户端不可用于：
  - 在办公室的 Cisco IP 电话上发起和接收呼叫。
  - 在住宅电话、酒店电话或办公室中的 Cisco IP 电话上执行通话切换控制（例如保留和恢复）。
- 会话持久性—客户端在发生网络转换时无法从音频和视频呼叫中断恢复。例如，如果用户在其办公室内启动 Cisco Jabber 呼叫，然后走到大楼外部并失去 Wi-Fi 连接，则呼叫将随着客户端切换使用 Expressway for Mobile and Remote Access 而中断。
- 早期媒体—早期媒体可让客户端在连接建立之前在终端之间交换数据。例如，如果用户向不属于同一组织的一方发出呼叫，而对方拒接或不应答呼叫，则早期媒体将确保用户听到忙音或将呼叫发送至语音邮件。

使用 Expressway for Mobile and Remote Access 时，如果对方拒接或不应答呼叫，用户将不会听到忙音。相反，用户在呼叫终止之前大约会听到一分钟的静音。

- 自助门户访问（仅限桌面客户端）— 用户在防火墙之外无法访问 Cisco Unified Communications Manager 自助门户。无法在外部访问 Cisco Unified Communications Manager 用户页面。

  Cisco Expressway-E 代理防火墙内客户端与 Unified Communications 服务之间的所有通信。但是，Cisco Expressway-E 不代理从不属于 Cisco Jabber 应用程序的浏览器访问的服务。

语音邮件

客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，支持语音邮件服务。

注释 要确保客户端能够访问语音邮件服务，您必须将语音邮件服务器添加到 Cisco Expressway-C 服务器的白名单中。要将服务器添加到 Cisco Expressway-C 白名单，请使用 **HTTP 服务器允许**设置。有关详细信息，请参阅相关的 Cisco Expressway 文档。

安装

Cisco Jabber Mac 版本 — 当客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，它不支持安装程序更新。

Cisco Jabber Windows 版本 — 当客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，它支持安装程序更新。

注释 要确保客户端能够下载安装程序更新，您必须将托管安装程序更新的服务器添加到 Cisco Expressway-C 服务器的白名单中。要将服务器添加到 Cisco Expressway-C 白名单，请使用 **HTTP 服务器允许**设置。有关详细信息，请参阅相关的 Cisco Expressway 文档。

安全

当客户端连接到使用 Expressway for Mobile and Remote Access 的服务时，其支持大多数具有以下限制的安全功能。

- 初始 CAPF 注册 — 证书权限代理功能 (CAPF) 注册是在将证书颁发给 Cisco Jabber（或其他客户端）的 Cisco Unified Communications Manager 上运行的安全服务。要为 CAPF 成功进行注册，客户端必须从防火墙内部或使用 VPN 进行连接。
- 端到端加密 — 当用户通过 Expressway for Mobile and Remote Access 进行连接并参与呼叫时：
  - 媒体始终在 Cisco Expressway-C 与使用 Expressway for Mobile and Remote Access 注册到 Cisco Unified Communications Manager 的设备之间的呼叫路径上加密。
  - 如果 Cisco Jabber 或内部设备未配置加密安全模式，则媒体不在 Cisco Expressway-C 与本地注册到 Cisco Unified Communications Manager 的设备之间的呼叫路径上加密。

- 如果 Cisco Jabber 和内部设备都配置了加密安全模式，则媒体在 Expressway-C 与本地注册到 Cisco Unified Communication Manager 的设备之间的呼叫路径上加密。
- 在 Cisco Jabber 客户端始终通过 Expressway for Mobileand Remote access 进行连接的情况下，则无需 CAPF 注册即可实现端到端加密。不过，Cisco Jabber 设备仍必须配置有加密安全模式，并且必须启用 Cisco Unified Communications Manager 以支持混合方式。
- 您可以在 Expressway-C 或 Expressway-E 服务器上配置 ICE 直通支持，以确保在公司网络外部时加密通过 Jabber 发送的媒体。有关如何将其设置的详细信息，请参阅《*Mobile and Remote Access Through Cisco Expressway* 部署指南》。

故障诊断

仅限 Cisco Jabber Windows 版本。问题报告上传 — 当使用 Expressway for Mobile and Remote Access 将桌面客户端连接到服务时，其无法发送问题报告，因为客户端通过 HTTPS 将问题报告上传到指定的内部服务器。

要解决此问题，用户可以本地保存报告并以另一种方式发送报告。

高可用性（故障转移）

高可用性意味着如果客户端无法连接到主服务器，它将故障转移到辅助服务器，而很少或不会中断服务。对于 Expressway for Mobile and Remote Access 上支持的高可用性，高可用性是指特定服务的服务器将故障转移到辅助服务器（例如即时消息和在线状态）。

Expressway for Mobile and Remote Access 上提供一些不支持高可用性的服务。这意味着，如果用户从公司网络外部连接到客户端，并且即时消息和在线状态服务器发生故障转移，则这些服务将继续正常工作。但是，如果音频和视频服务器或语音邮件服务器发生故障转移，则这些服务将无法工作，因为相关服务器不支持高可用性。

Cisco AnyConnect 部署

Cisco AnyConnect 是指服务器/客户端基础架构，可让客户端从远程位置（例如，Wi-Fi 网络或移动数据网络）安全地连接到企业网络。

Cisco AnyConnect 环境包括以下组件：

- Cisco 自适应安全设备 — 提供一种安全Remote Access的服务。
- Cisco AnyConnect 安全移动客户端 — 从用户的设备建立与 Cisco 自适应安全设备的安全连接。

本部分提供在通过 Cisco AnyConnect 安全移动客户端部署 Cisco 自适应安全设备 (ASA) 时应考虑的信息。Cisco AnyConnect 是 Cisco Jabber Android 版本和 Cisco Jabber iPhone 和 iPad 版本支持的 VPN。如果使用不受支持的 VPN 客户端，请确保您使用相关第三方文档安装与配置 VPN 客户端。

对于运行 Android OS 4.4.x 的 Samsung 设备，使用 Samsung AnyConnect 4.0.01128 版或更高版本。对于 5.0 以上版本的 Android OS，使用的 Cisco AnyConnect 软件版本不能低于 4.0.01287。

Cisco AnyConnect 为远程用户提供与 Cisco 5500 系列 ASA 的安全 IPsec (IKEv2) 或 SSL VPN 连接。Cisco AnyConnect 可以从 ASA 或使用企业软件部署系统部署到远程用户。从 ASA 部署时，远程用

户通过在配置为接受无客户端 SSL VPN 连接的 ASA 浏览器中输入 IP 地址或 DNS 名称，与 ASA 进行初始 SSL 连接。然后，ASA 在浏览器窗口中显示登录屏幕，如果用户满足登录和验证要求，它将下载与计算机操作系统匹配的客户端。下载完成后，客户端将进行安装和自我配置，并建立与 ASA 的 IPsec (IKEv2) 或 SSL 连接。

有关 Cisco 自适应安全设备和 Cisco AnyConnect 安全移动客户端要求的信息，请参阅“软件要求”主题。

相关主题

Cisco ASA 系列文档一览
Cisco AnyConnect 安全移动客户端

通过单点登录进行部署

您可以通过安全断言标记语言 (SAML) 单点登录 (SSO) 启用您的服务。SAML SSO 可用于本地、云或混合部署。

以下步骤说明了用户在启动 Cisco Jabber 客户端后 SAML SSO 的登录流：

1. 用户启动 Cisco Jabber 客户端。如果配置您的身份提供程序 (IdP) 以提示用户使用网络表单登录，该表单将在客户端内显示。
2. Cisco Jabber 客户端将授权请求发送到其连接到的服务，例如 Cisco Webex Messenger 服务、Cisco Unified Communications Manager 或 Cisco Unity Connection。
3. 服务重定向客户端以请求 IdP 的验证。
4. IdP 请求凭证。可用以下一种方法提供凭证：
   - 包含用户名和密码字段的基于表单的身份验证。
   - 用于集成 Windows 身份验证 (IWA) 的 Kerberos（仅限 Windows）
   - 智能卡身份验证（仅限 Windows）
   - 在发出 HTTP 请求时，客户端提供用户名和密码的基本 HTTP 身份验证方法。
5. IdP 为浏览器提供 cookie 或提供其他身份验证方式。IdP 使用 SAML 进行身份验证，从而允许服务为客户端提供令牌。
6. 客户端使用令牌进行身份验证以登录到服务。

身份验证方式

身份验证机制会影响用户登录的方式。例如，如果您使用 Kerberos，客户端不会提示用户输入凭证，因为您的用户已提供身份验证以获取桌面的访问权限。

用户会话

用户登录以进行会话，这将为他们提供一个预定义的时段来使用 Cisco Jabber 服务。要控制会话的持续时间，您需要配置 cookie 和令牌超时参数。

为IdP超时参数配置适当的时间量，以确保不提示用户登录。例如，当Jabber用户切换到外部Wi-Fi、漫游、其笔记本电脑休眠或其笔记本电脑因用户非活动而进入休眠状态时。用户将不必在恢复连接后登录，前提是 IdP 会话仍处于活动状态。

当会话已过期并且 Jabber 无法以静默方式续订该会话时，由于需要用户输入，因此系统会提示用户重新进行身份验证。当授权 cookie 不再有效时，可能会发生这种情况。

如果使用了Kerberos或智能卡，则无需执行任何操作即可重新进行身份验证，除非智能卡需要PIN；没有中断服务（例如语音邮件、传入呼叫或即时消息）的风险。

单点登录要求

SAML 2.0

使用 SAML 2.0 来为使用 Cisco Unified Communications Manager 服务的 Cisco Jabber 客户端启用单点登录 (SSO)。SAML 2.0 与 SAML 1.1 不兼容。选择使用 SAML 2.0 标准的 IdP。由于支持的身份提供程序符合 SAML 2.0，因此您可以使用它们来实施 SSO。

受支持的身份提供程序

IdP 必须与安全声明标记语言 (SAML) 兼容。客户端支持以下身份提供程序：

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

注释 确保全局配置持久性 cookie 以与 OpenAM 一起使用。

配置 IdP 时，配置的设置会影响您登录到客户端的方式。cookie 类型（持久性或会话）等参数或身份验证机制（Kerberos 或网页表单）确定您必须接受身份验证的频率。

Cookie

要让 cookie 与浏览器实现共享，使用永久性 cookie 而不是会话 cookie。持久性 cookie 提示用户在客户端或使用 Internet Explorer 的任何其他桌面应用程序中输入凭证一次。会话 cookie 要求用户在每次启动客户端时输入其凭证。您可以将持久性cookie配置为IdP上的一种设置。如果您使用Open Access Manager 作为 IdP，则全局配置持久性 cookie（而不是特定领域的持久性 Cookie）。

用户使用 SSO 凭证成功登录到 Cisco Jabber iPhone 和 iPad 版本时，默认情况下会将 cookie 保存在 iOS keychain 中。如果 cookie 在 iOS keychain 中，用户下次登录时无需输入登录凭证，除非 cookie 在登录期间过期。在以下情况下，cookie 将从 iOS keychain 中删除：

- 手动注销 Cisco Jabber。
- Cisco Jabber 已重置。
- 重新启动 iOS 设备后

- Cisco Jabber 已手动关闭。

注释 如果您使用嵌入的 Safari 浏览器，Jabber 无法控制 Safari 控制的 cookie。由于 Jabber 无法清除这些 Cookie，因此在这种情况下 Jabber 只能清除 SSO 令牌。如果 Safari 在持久性 cookie 中具有用户凭据，则该 cookie 允许用户避免在 Jabber 清除 SSO 令牌时重新输入其凭证。

如果 iOS 系统在后台停止了 Cisco Jabber iPhone 和 iPad 版本，Jabber 允许用户在不输入密码的情况下自动登录。

所需浏览器

要共享浏览器与客户端之间的身份验证 cookie（由 IdP 颁发），将以下浏览器之一指定为默认浏览器：

产品	所需浏览器
Cisco Jabber Windows 版本	Internet Explorer
Cisco Jabber Mac 版本	Safari
Cisco Jabber iPhone 和 iPad 版本	Safari
Cisco Jabber Android 版本	Chrome 或 Internet Explorer

注释 使用采用 Cisco Jabber Android 版本的 SSO 时，嵌入式浏览器无法与外部浏览器共享 cookie。

单点登录和 Remote Access

对于使用 Expressway Mobile and Remote Access 从公司防火墙外部提供其凭证的用户，单点登录具有以下限制：

- 单点登录 (SSO) 适用于 Cisco Expressway 8.5 和 Cisco Unified Communications Manager 版本 10.5.2 或更高版本。您必须在两者上启用或禁用 SSO。
- 您不能在安全电话上通过 Expressway for Mobile and Remote Access 使用 SSO。
- 使用的身份提供程序必须具有相同的内部和外部 URL。如果 URL 不同，则用户在公司防火墙内部和外部进行变换时可能会收到再次登录的提示。