Cisco Jabber 14.0 规划指南

首次发布日期: 2021 年 3 月 25 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

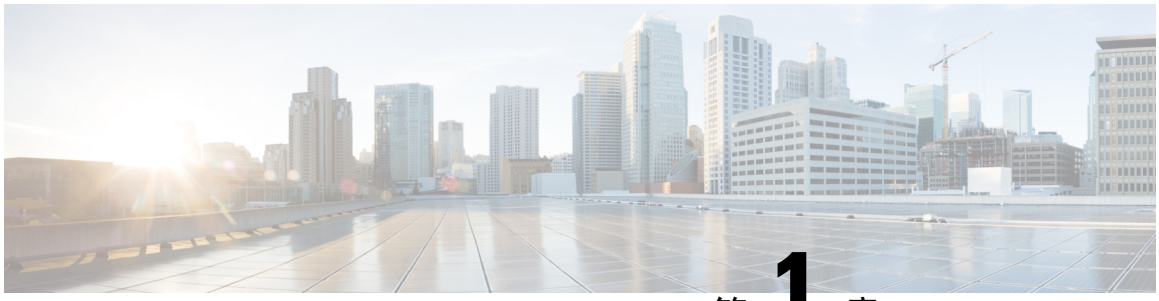
目录

新增和变更内容

新信息及变更内容

日期	状态	说明	位置
2021 年 3 月		首次发布	
	已更新	已添加 macOS Big Sur	Cisco Jabber Mac 版本的操作系统
	已更新	新增支持的硬件	Cisco Jabber Android 版本的软件要求

新增和变更内容



第 1 章

要求

服务器要求

此版本中的所有 Cisco Jabber 客户端都通用以下软件要求：

服务	软件要求	支持的版本
IM and Presence	Cisco Unified Communications Manager IM and Presence Service	10.5(2) 及更高版本（最低） 11.5(1) SU3 或更高版本（推荐）
	Cisco Webex Messenger	
电话	Cisco Unified Communications Manager	10.5(2) 及更高版本（最低） 11.5(1) SU3 或更高版本（推荐）
	Cisco Unified Survivable Remote Site Telephony	Unified SIP SRST 12.8 及更高版本
联系人搜索	LDAP 目录	LDAP v3 兼容目录（例如 Microsoft Active directory 2008 R2 和 Open LDAP 2.4 或更高版本）
语音邮件	Cisco Unity Connection	10.5 和更高版本
多线路	Cisco Unified Contact Center Express	11.6

服务	软件要求	支持的版本
会议	Cisco Meeting Server	2.2 和更高版本
	Cisco TelePresence Server	3.1 及更高版本
	Cisco TelePresence MCU	4.3 及更高版本
	Cisco ISR PVDM3	Cisco Unified Communications Manager 9.x 及以上版本
	云 CMR	Cisco Webex Meetings 带有协作会议室的服务器
	Cisco Webex Meetings 服务器	2.8 MR1 及更高版本
	Cisco Webex Meetings 居中	WBS33 及更高版本
Remote Access	Cisco Adaptive Security Appliance 仅适用于 Cisco Jabber Android 版本。	8.4(1) 及更高版本
	Cisco AnyConnect Secure Mobility Client 仅适用于 Cisco Jabber Android 版本及 Cisco Jabber iPhone 和 iPad 版本。	与平台相关的思科 850
	Cisco Expressway C	X8.10.1 及更高版本
	Cisco Expressway E	X 8.10.1 和更高版本。

Cisco Jabber 在启动期间使用域名系统（DNS）服务器，对于 Cisco Jabber 设置，必须使用 DNS 服务器。

操作系统要求

Cisco Jabber Windows 版本的操作系统

您可以在以下操作系统上安装Cisco Jabber Windows 版本：

- Microsoft Windows 7、8 和 10（桌面模式）
- Microsoft Windows 7、8 和 10（桌面模式）
- Microsoft Windows 7、8 和 10（桌面模式）

Cisco Jabber Windows 版本不要求 Microsoft .NET Framework 或任何 Java 模块。

Windows 10 服务选项

Cisco Jabber Windows 版本支持以下 Windows 10 服务选项：

- 当前分支（CB）
- 当前的业务分支（CBB）
- 长期服务分支（LTSB）—使用此选项，您负责确保部署任何相关的服务更新。

有关 Windows 10 服务选项的详细信息，请参阅以下 Microsoft 文档：https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx。

注释 Cisco Jabber 默认情况下将所需的文件安装到以下目录：

- %temp%\Cisco Systems\Cisco Jabber-启动程序属性文件和安装日志
- %LOCALAPPDATA%\Cisco\Unified 通信-日志和临时遥测数据
- %APPDATA%\Cisco\Unified 通信-缓存的配置和帐户凭证
- %ProgramFiles%\Cisco Systems\Cisco Jabber-x86 Windows 的安装文件
- % ProgramFiles（x86）% \ Cisco Systems\Cisco Jabber 安装文件（适用于 x64 Windows）

Cisco Jabber Mac 版本的操作系统

您可以在以下操作系统上安装 Cisco Jabber Mac 版本 版本：

- macOS Catalina 10.15 或更高版本
- macOS Mojave 10.14 或更高版本
- Apple Mac OS High Sierra 10.13（或更高版本）
- Apple Mac OS Sierra 10.12（或更高版本）
- macOC Big Sur

Cisco Jabber Android 版本的操作系统

有关支持的最新操作系统版本信息，请参阅 "Play 店"。

注释 Cisco Jabber Android 版本可用作 32 位应用程序和 64 位应用程序。如果您的 Android 设备具有 64 位的操作系统，则运行 64 位 Jabber 客户端可以更快、更丰富的体验。

您无法在 32 位操作系统上安装 64 位应用程序。如果在大多数 64 位平台上使用 32 位应用程序，您将收到升级到 64 位应用程序的通知。

注释 如果 Cisco Jabber 安装在 Android 6.0 Marshmallow 操作系统或更高版本中，并且保持空闲：

- 到 Cisco Jabber 的网络连接已禁用。
- 用户不会收到任何呼叫或消息。

轻触**更改**设置并忽略电池优化以接收呼叫和消息。

最后一个支持 Android 5.x 的 Jabber 版本

Cisco Jabber 12.8 是最后一个支持运行 Android 5. x 的设备的版本。

下一个 Jabber 版本将终止对无法升级到 Android 6. x 的所有设备的支持。

Cisco Jabber iPhone 和 iPad 版本的操作系统

有关支持的最新操作系统版本信息，请参阅应用商店。

重要事项 Cisco 只支持当前应用商店版本的 Cisco Jabber iPhone 和 iPad 版本。在任何适用于 Cisco Jabber iPhone 和 iPad 版本中发现的缺陷都将根据当前版本进行评估。

硬件要求

桌面客户端的硬件要求

要求	Cisco Jabber Windows 版本	Cisco Jabber Mac 版本
安装的 RAM	2 GB RAM	2 GB RAM
可用物理内存	128 MB	1 GB
可用磁盘空间	256 MB	300 MB

要求	Cisco Jabber Windows 版本	Cisco Jabber Mac 版本
CPU 速度和类型	移动式 AMD Sempron处理器3600+ 2 GHz 英特尔酷睿 2 双核处理器 T7400 @ 2。16 GHz	在以下任何 Apple 硬件中使用 Intel Core 2 Duo 或更高版本处理器： • Mac Pro • MacBook Pro（包括带 Retina 显示屏的型号） • MacBook • MacBook Air • iMac • Mac Mini
I/O 端口	USB 2.0（适用于 USB 摄像头和音频设备）。	USB 2.0（适用于 USB 摄像头和音频设备）

CTI 支持设备

要查看 Unified Communications Manager 支持的计算机电话集成 (CTI) 设备列表，请执行以下操作：

1. 从 **Cisco Unified 报告**页面的**系统报告**菜单中选择 **Unified CM 电话功能列表**。
2. 打开报告后，从**功能**下拉列表中选择 **CTI 控制**。

Cisco Jabber Android 版本的软件要求

Android 设备的最低要求：

Android 操作系统	CPU	显示屏
6.0 或更高版本	1.5 GHz 双核 建议：1.2-GHz 四核或更高版本	对于双向视频：480p x 800p 或更高版本。 仅适用于 IM：320p x 480p 或更高版本。

Cisco Jabber Android 版本在采用以下操作系统版本的设备中支持完全 UC 模式：

表 *1:* 支持的 *Android* 设备

设备	型号	操作系统最低版本	备注
BlackBerry	Priv	6.0.1	如果您从最近查看的应用程序列表中删除了 Jabber，并且使设备闲置了一段时间，那么 Jabber 将变为非活动状态。

设备	型号	操作系统最低版本	备注
Fujitsu	Arrows M357	6.0.1	
Google	Nexus 5	6.0	
	Nexus 5X	6.0	
	Nexus 6	6.0	
	Nexus 6P	6.0	对于具有 Android OS 版本6.x或7.0的 Google Nexus 6P，管理员必须将 Jabber 电话服务设置为安全电话服务。否则，您的设备可能不响应。 Android OS 7.1 或更高版本不需要任何操作。
	Nexus 7	6.0	
	Nexus 9	6.0	
	Pixel	7.0	
	Pixel C	6.0	
	Pixel XL	7.0	
	Pixel 2	8.0	在 Jabber 呼叫期间，如果用户将音频从移动设备切换到头戴式耳机，则可能会出现暂时的音频问题。
	Pixel XL	8.0	在 Jabber 呼叫期间，如果用户将音频从移动设备切换到头戴式耳机，则可能会出现暂时的音频问题。
	Pixel 3	8.0	如果您在电话上使用连接的头戴式耳机，则音频可能会出现一些问题，并且可能需要几秒钟的时间。
	Pixel XL	8.0	如果您在电话上使用连接的头戴式耳机，则音频可能会出现一些问题，并且可能需要几秒钟的时间。
	Pixel 4	10.0	
	Pixel 4 XL	10.0	
	Pixel 4a 5G	10.0	

设备	型号	操作系统最低版本	备注
Honeywell Dolphin	CT50	6.0	
	CT40	7.1.1	
	CT60	7.1.1 和 8.1	我们仅支持使用 Android OS 7.1.1 和 8.1 的 CT60。
HTC	10	6.0	
	A9	6.0	
	M8	6.0	
	M9	6.0	
	X9	6.0	
华为 [1]	Honor7	6.0	
	Mate 8	6.0	
	Mate 9	6.0	
	Nova	7.0	
	Mate 10	8.0	
	Mate 10 Pro	8.0	
	P8	6.0	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.0	
	P20 Pro	8.0	
	Mate20	8.0	
	Mate20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	

设备	型号	操作系统最低版本	备注
LG	G3	6.0	
	G4	6.0	
	G5	6.0	
	G6	7.0	
	V10	6.0	
	V30	8.0	
Motorola	Moto G4	6.0	
	Moto G5	7.0	
	Moto G6	8.0	
	Moto Z Droid	6.0	
Nokia	6.1	8.0	
	8.1	8.1	
OnePlus	1	6.0	
	5	8.0	
	5T	8.0	
	6	9.0	
	6T	9.0	
	7T	10.0	
	8	11.0	
	8 Pro	11.0	
	8T	11.0	

设备	型号	操作系统最低版本	备注
Samsung	すべて	6.0	• 不再支持无法升级到 Android OS 6.x 或更高版本的设备。 • 为 Jabber 启用自动运行选项。 对于 Android 操作系统 6.x 及更高版本，您可以在**应用程序智能管理器**下找到自动运行选项。 • Jabber 针对加拿大延迟 Samsung Galaxy Tab Pro 8.4（型号 T320UEU1AOC1）上的弹出式来电通知。 • 失去 Wi-Fi 连接时，Jabber 延迟重新连接到 Samsung Xcover 3 上的网络。 • 采用芯片组 Exynos 7580 的 Samsung 设备中存在音频质量问题。当设备屏幕关闭时，音频变得不清晰。以下是设备列表： • Samsung Galaxy A3 2016 • Samsung Galaxy A5 2016 • Samsung Galaxy A7 2016 • Samsung Galaxy S5 Neo • Samsung Galaxy J7 • Samsung Galaxy View
Seuic	Cruise 1	9.0	
Sonim	XP8	7.1.1	

设备	型号	操作系统最低版本	备注
Sony Xperia	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z2	6.0	
	Z2 Tablet	6.0	
	Z3	6.0	采用 Android 操作系统 5.0.2 的 Sony Xperia Z3 (Model SO-01G) 进行 Jabber 呼叫时音频质量差。
	Z3 Tablet Compact	6.0	
	Z3+/Z4	6.0	在索尼 Z3 +/Z4. 上，视频呼叫不稳定尝试为视频呼叫禁用自己的视频。否则，仅进行语音呼叫。
	Z4 TAB	6.0	
	Z5 Premium 和 Z5	6.0	
	Xperia 5 Mark II	11.0	

设备	型号	操作系统最低版本	备注
Xiaomi	4C	6.0	这些设备上仅运行32位版本。
	MAX	6.0	
	Mi 4	6.0	
	Mi5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Mi 10	10.0	
	Mi 10 Ultra	10.0	
	Pocophone	8.0	
	Mi Note	6.0	这些设备上仅运行32位版本。
	Mi Note 2	7.0	
	Mi 组合 2	8.0	
	Mi A1	8.0	
	Redmi Note 3	6.0	
	Redmi Note 4	6.0.1	
	Redmi Note 5	8.0	
	Redmi Note 6 Pro	8.1	
Zebra	TC75X	6.0	
	TC51	6.0	

[1] 由于 EMUI 10 中发生变更，当您的设备锁定时，可能不会出现来电提示。在 Jabber 中，转至**设置** > **通知**，然后选择**横幅**。

用于 Samsung Knox 的 Jabber 支持

Cisco Jabber Android 版本支持这些设备上的 Samsung Knox 2.6 版本：

Knox 版本	Samsung 设备
2.6	Note 4 Note 5 Note Edge S5 S6 S6 Edge S6 Edge Plus S7 S7 Edge Note 10.1（2014 年款）
2.7.1	Galaxy Note5
3.1	Galaxy A5（2017）
3.2	Galaxy On5（2016）
3.3	Galaxy S10

注释 在 Samsung 中运行 Cisco Jabber Android 版本时，Samsung Knox 的安全性设计要求先解锁 Knox。在解锁 Knox 之前，您无法使用 Jabber 应答或拒绝呼叫。

Jabber 支持 Samsung Dex

Cisco Jabber Android 版本支持 samsung S8、S8 Plus 和 Note 8 中的 Samsung Dex。

采用较早 Android 版本的设备对于 Cisco Jabber 的支持策略

由于 Android 内核问题，Cisco Jabber 无法在部分 Android 设备上注册到 Cisco Unified Communications Manager。要解决此问题，请尝试以下操作：

将 Android 内核升级到 3.10 或最新版本。

设置 Cisco Unified Communications Manager 为使用混合模式安全性，启用安全 SIP 呼叫信令，并使用 5061 端口。有关使用 Cisco CTL 客户端配置混合模式的说明，请参阅《*Cisco Unified Communications Manager* 安全指南》。您可以在 Cisco Unified Communications Manager 的维护和操作指南中找到安全指南。此解决方法适用于以下支持的设备：

设备型号	操作系统
HTC M8	Android 操作系统 6.0 或更高版本

设备型号	操作系统
HTC M9	Android 操作系统 6.0 或更高版本
Sony Xperia Z2	Android OS 6.0 或更高版本，且内核版本早于 3.10.49。 如果设备的 Android OS 为 6.0 或更高版本，且内核版本为 3.10.49 或更高版本，则该设备可支持非安全模式。
Sony Xperia Z2 平板电脑	
Sony Xperia Z3	
Sony Xperia Z3 Tablet Compact	
小米 Mi4	Android 操作系统 6.0 或更高版本
小米 Mi Note	Android 操作系统 6.0 或更高版本
Honeywell Dolphin CT50	Android 操作系统 6.0 或更高版本

支持的蓝牙设备

蓝牙设备	依赖关系
Cisco 561	
Cisco 562	
Plantronics Voyager Legend	
Plantronics Voyager Legend UC	
Plantronics Voyager edge UC	
Plantronics Voyager edge	
Plantronics PLT focus	
Plantronics BackBeat 903+	如果您使用 Samsung Galaxy S4，则由于这些设备之间的兼容性问题，可能会遇到问题。
Jabra Motion	将 Jabra Motion 蓝牙头戴式耳机升级至固件版本 3.72 或以上。 固件版本为 3.72 或以上的 Jabra Motion 蓝牙头戴式耳机支持 Cisco Jabber 呼叫控制。
Jabra Wave+	
Jabra Biz 2400	
Jabra Easygo	
Jabra PRO 9470	
Jabra Speak 510	

蓝牙设备	依赖关系
Jabra Supreme UC	
Jabra Stealth	
Jabra Evolve 65 UC Stereo	
适用于 Cisco 蓝牙头戴式耳机的 Jawbone ICON	如果您使用 Samsung Galaxy S4，则由于这些设备之间的兼容性问题，可能会遇到问题。

蓝牙限制：

- 在 Samsung Galaxy SIII 上使用蓝牙设备可能会造成铃声和呼叫音频失真。
- 如果用户在使用 Jabber 呼叫期间将蓝牙头戴式耳机断开再重新连接，则用户听不到音频。此限制适用于操作系统版本为 Android 5.0 之前的智能手机。
- 在具有 OS Android 6.0 的索尼 Z4/LG G4/Devices 中，用户在开始 Jabber 呼叫后切换到蓝牙头戴式耳机时，可能会遇到音频损耗。解决方法是，将音频输出切换到扬声器，然后再切换回蓝牙。或者在进行 Cisco Jabber 呼叫之前连接蓝牙头戴式耳机。

支持的 Android Wear

Cisco Jabber 可在所有装有 Android OS 5.0 或更高版本以及 Google 服务 8.3 或更高版本的 Android Wear 设备上运行。Cisco Jabber 在这些 Android Wear 设备上经过测试：

- Fossil Gen 3 SmartWatch
- 华为手表
- LG G Watch R
- LG Watch Urbane
- Moto 360
- Moto 360（第 2 代）
- Samsung Gear live
- Sony SmartWatch 3

注释 Cisco Jabber 安装程序 for Android Wear 设备与主 Jabber APK 文件不同。用户在将磨损设备与移动设备配对时，从 Google Play store 获取 Android Wear 安装程序。

支持的 Chromebook 型号

Chromebook 必须有 Chrome OS 53 或更高版本。用户可以从 Google Play 商店下载 Cisco Jabber Android 版本。

- HP Chromebook 13 G1 笔记本 PC
- Google Chromebook 像素
- Google Chromebook Pixelbook
- Samsung Chromebook Pro
- Asus C302

Cisco Jabber iPhone 和 iPad 版本的硬件要求

iOS 13.X 及 iPadOS 上的 Cisco Jabber iPhone 和 iPad 版本支持以下 Apple 设备。未升级到这些版本的设备不受支持。

Apple 设备	版本
iPad	第五、第六和第七代
iPad Air	Air 2 和 Air 3
iPad Pro	9.7 和 10.5 英寸 12.9 英寸、第 1、第二和第三代
iPad mini	Mini 4 和 mini 5
iPhone	6s、6s Plus、7、7 Plus、8、8 Plus、X、Xs、Xs Max、11、11 Pro、11 Pro Max、XR 和 SE
iPod touch	第六代
Apple Watch	在 Apple Watch 和 Apple Watch 2、3 和 4 上运行的 WatchOS 5。

iPhone 和 iPad 支持以下蓝牙头戴式耳机：

制造商	型号
Apple	AirPod
Cisco	561, 562
Jabra	BIZ 2400、Easygo、演化 65 UC 立体声、至尊 2、移动[2]，PRO 9470，讲话 450（适用于 Cisco），发言 510，隐匿 Supreme UC，波形 +
Jawbone	适用于 Cisco 蓝牙头戴式耳机的 Jawbone ICON
Plantronics	Voyager Edge、Voyager Edge UC、Voyager 图例、Voyager 图例 UC

制造商	型号
索尼 Eriksson	MW-600

[2] 支持 Cisco Jabber 呼叫蓝牙控制。只有固件版本 3.72 支持此功能。

网络要求

通过企业 Wi-Fi 网络使用 Cisco Jabber 时，我们建议您执行以下操作：

- 设计 Wi-Fi 网络时尽可能消除覆盖空白区，覆盖范围应包括电梯、楼梯和外部走廊等区域。
- 确保所有访问点为移动设备分配相同的 IP 地址。如果通话期间 IP 地址变更，呼叫将中断。
- 确保所有访问点都具有相同的服务集标识符（SSID）。如果 SSID 不匹配，越区切换可能会比较慢。
- 确保所有访问点广播其 SSID。如果访问点不广播其 SSID，则移动设备可能会提醒用户加入另一个 Wi-Fi 网络，这将中断呼叫。
- 确保将企业防火墙配置为允许用于 NAT（STUN）信息包的会话遍历实用程序。

充分开展现场调查，以最大限度减少可能影响语音质量的网络问题。我们建议您执行以下操作：

- 验证信道配置没有重叠，验证访问点覆盖范围及所需的数据和通信速率。
- 消除异常访问点。
- 识别并减轻潜在干扰源的影响。

有关详细信息，请参阅以下文档：

- 《企业移动设计指南》中的 “VoWLAN 设计建议”部分。
- 《*Cisco 7925G Unified* 无线 *IP* 电话部署指南》。
- 《*IEEE 802.11g* 的容量覆盖与部署注意事项》白皮书。
- 适用于您的 Cisco Unified Communications Manager 版本的解决方案参考网络设计 *(SRND)*。

要求：

Cisco Jabber 完全支持 IPv6，它在纯 IPv6 和混合网络中正常运行，但存在本节中列出的限制。思科协作解决方案目前完全不支持 IPv6。例如，Cisco VCS Expressway for Mobile and Remote Access 在纯 IPv6 网络中的限定条件是，NAT64/DNS64 必须部署在移动供应商网络中。Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence 目前在纯 IPv6 网络中不支持 HTTPS。

Jabber中使用IP_Mode参数配置功能，将协议设置为IPv4，IPv6或双栈。默认设置为双堆栈。IP_Mode参数可包含在Jabber客户端配置中（请参阅最新版本的《*Cisco Jabber*的参数参考指南》）、Windows 引导 For Windows 以及适用于 Mac 和移动设备的 URL 配置机时。

连接到服务时 Jabber 所用的网络 IP 协议取决于以下因素：

- jabber-config.xml IP 模式参数。
- 客户端操作系统 IP 功能。
- 服务器操作系统 IP 功能。
- IPv4 和 IPv6 的 DNS 记录的可用性。
- Cisco Unified Communications Manager 针对 IPv4、IPv6 或两者的软终端设备配置的 SIP 设置。软终端设备的 SIP 连接设置必须与 Jabber IP 模式参数设置匹配，连接才会成功。
- 底层网络 IP 功能。

在 Cisco Unified Communications Manager 上，IP 功能取决于通用服务器设置和设备特定设置。下表列出了各种设置下的预期 Jabber 连接；此列表假定 IPv4 和 IPv6 的 DNS 记录均已配置。

客户端 OS、服务器 OS 和 Jabber IP_Mode 参数设置为两个堆栈时，Jabber 将根据 RFC6555 使用 IPv4 或 IPv6 地址与服务器连接。

客户端操作系统	服务器操作系统	Jabber IP_Mode 参数	Jabber 连接结果
仅 IPv4	仅 IPv4	仅 IPv4	IPv4 连接
		仅 IPv6	连接失败
		两个堆栈	IPv4 连接
仅 IPv4	仅 IPv6	仅 IPv4	连接失败
		仅 IPv6	连接失败
		两个堆栈	连接失败
仅 IPv6	仅 IPv4	仅 IPv4	连接失败
		仅 IPv6	连接失败
		两个堆栈	连接失败
仅 IPv6	仅 IPv6	仅 IPv4	连接失败
		仅 IPv6	IPv6 连接
		两个堆栈	IPv6 连接

客户端操作系统	服务器操作系统	Jabber IP_Mode 参数	Jabber 连接结果
仅 IPv4	两个堆栈	仅 IPv4	IPv4 连接
		仅 IPv6	连接失败
		两个堆栈	IPv4 连接
仅 IPv6	两个堆栈	仅 IPv4	连接失败
		仅 IPv6	IPv6 连接
		两个堆栈	IPv6 连接
两个堆栈	仅 IPv4	仅 IPv4	IPv4 连接
		仅 IPv6	连接失败
		两个堆栈	IPv4 连接
两个堆栈	仅 IPv6	仅 IPv4	连接失败
		仅 IPv6	IPv6 连接
		两个堆栈	IPv6 连接
两个堆栈	两个堆栈	仅 IPv4	IPv4 连接
		仅 IPv6	IPv6 连接
		两个堆栈	IPv6 连接

在仅 IPv6 模式下使用 Jabber 时，必须使用 NAT64/DNS64 连接到 IPv4 基础设施（例如Cisco Webex Messenger服务、用于移动和 Remote Access 的 Cisco VCS Expressway）和Cisco Webex 平台服务。

桌面设备支持适用于仅 IPv6 内部部署。所有 Jabber 移动设备必须配置为两个堆栈。

有关 IPv6 部署的详细信息，请参阅《思科协作系统版本 12.0 的 IPv6 部署指南》。

限制

- HTTPS 连接
  - 在内部部署中，Cisco Jabber 支持仅 IPv4 和两个堆栈模式以连接到 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service。这些服务器当前不支持 IPv6 HTTPS 连接。

    Cisco Jabber 可以使用仅 IPv6 模式的语音邮件连接到 Cisco Unity Connection。

- Cisco Webex Messenger 限制
  - Cisco Webex Messenger IPv6 上不受支持。

- 电话限制
  - 将 Cisco Unified Communications Manager 的用户设备升级到仅两个堆栈或 IPv6 时，相应的 Jabber 客户端必须升级到 11.6 或更高版本。
  - 当安装中包含 IPv4 端点和 IPv6 端点时，我们建议您使用硬件 MTP 在这些设备之间桥接音频和视频。此功能在 Cisco IOS 版本为 15.5 的硬件 MTP 上受支持。例如，Cisco 3945路由器必须运行以下T列构建：c3900e-universalk9-mz.SPA.155-2.T2.bin。
  - 目前，我们没有解决方案路线图在 Cisco 端点（包括 Jabber）中同时支持 IPv4 和 IPv6。Cisco Unified Communications Manager 支持仅 IPv4 和仅 IPv6 的当前功能。需要 MTP 来支持仅 IPv4 与仅 IPv6 端点之间的呼叫，或者支持仅 IPv4 或仅 IPv6 的网关。
  - IPv6 上不支持 Jabber 到 Jabber 呼叫。
- 文件传输限制
  - 高级文件传输-当客户端配置用于两个堆栈和 Cisco Unified Communications Manager IM and Presence Service 时，将启用两个堆栈。以下 Cisco Unified Communications Manager IM and Presence Service 版本支持高级文件传输：
    - 10.5.2 SU2
    - 11.0.1 SU2
    - 11.5
  - 人员到个人文件传输-不支持在 IPv4 与 IPv6 客户端之间进行用户间文件传输的内部部署人员。如果您有 IPv4 和 IPv6 客户端的网络配置，我们建议配置高级文件传输。
- 移动和远程接入限制
  - 用于移动和的思科 VCS 快速通道不支持 IPv6。
  - 如果为 IPv6 SIP 连接配置了 Cisco Unified Communications Manager，则无法使用 Cisco VCS Expressway 连接到 Cisco Unified Communications Manager 以进行移动和 Remote Access 以使用电话服务。

在 Android 中支持 IPv6 的要求

Android 操作系统要求

Android 5.0 和更高版本

网络要求

- 仅 IPv4 模式（仅限 Android 接收 IPv4 地址）
- 采用 SLAAC 的双堆栈（Android 接受 IPv4 和 IPv6 地址）
- NAT64 或 DNS64（服务器使用 IPv4 地址，而客户端使用 IPv6 地址）

限制

- DHCPv6 限制
  - DHCPv6 在 Android 设备上不受支持。
- Android 操作系统限制
  - Android 操作系统不支持仅 IPv6 网络。有关此限制的详细信息，请参阅《Android 开发者链接》。

端口和协议

客户端使用下表所列的端口和协议。如果您计划在客户端与服务器之间部署防火墙，必须将防火墙配置为允许这些端口和协议。

	端口	应用层协议	传输层协议	说明
配置				
	6970	HTTP	TCP	连接至 TFTP 服务器以下载客户端配置文件。
	6972	HTTPS	TCP	连接至 TFTP 服务器，为 Cisco Unified Communications Manager 11.0 版及更高版本安全下载客户端配置文件。
	53	DNS	UDP	主机名解析。
	3804	CAPF	TCP	向 IP 电话颁发当地有效证书 (LSC)。该端口是用于 Cisco Unified Communications Manager 证书权限代理功能 (CAPF) 注册的侦听端口。
	8443	HTTPS		流量到 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service。
	8191	SOAP	TCP	连接至本地端口，以提供简单对象访问协议 (SOAP) Web 服务。
目录集成 — 对于 LDAP 联系人解析，将基于 LDAP 配置使用以下端口之一。				
	389	LDAP	TCP	LDAP TCP (UDP) 连接至 LDAP 目录服务。
	3268	LDAP	TCP	连接至全局编录服务器进行联系人搜索。
	636	LDAPS	TCP	LDAPS TCP 安全连接至 LDAP 目录服务。
	3269	LDAPS	TCP	LDAPS TCP 安全连接至全局编录服务器。
即时消息和在线状态				

	端口	应用层协议	传输层协议	说明
	443	XMPP	TCP	服务的 Webex Messenger XMPP 流量。仅在基于云的部署中，客户端才通过此端口发送 XMPP。如果阻止端口 443，客户端会重新通过端口 5222 发送。
	5222	XMPP	TCP	连接至 Cisco Unified Communications Manager IM and Presence Service 查看即时消息和在线状态。
	37200	SOCKS5 字节流	TCP	对等文件传输，在内部部署中，客户端还使用此端口发送屏幕截图。
	7336	HTTPS	TCP	MFT 文件传输（仅限内部）。
Communication Manager 信令				
	2748	CTI	TCP	用于桌面电话控制的计算机电话接口 (CTI)。
	5060	SIP	TCP	提供会话发起协议 (SIP) 呼叫信令。
	5061	通过 TLS 的 SIP	TCP	通过 TCP 的 SIP 提供安全的 SIP 呼叫信令。（在设备启用安全 SIP 时使用。）
	3000-3999	FECC	UDP	远端摄像机控制 (FECC)。
	5070-6070	BFCP	UDP	二进制层控制协议 (BFCP)，提供视频屏幕共享功能。
语音或视频媒体交换				
	16384-32766	RTP/SRTP	UDP	用于音频、视频和 BFCP 视频桌面共享的 Cisco Unified Communications Manager 媒体端口范围。
	33434-33598	RTP/SRTP	UDP	用于音频和视频的 Cisco 混合服务（Jabber 至 Jabber 呼叫）媒体端口范围。
	8000	RTP/SRTP	TCP	由 Jabber 桌面电话视频界面使用。该界面可让用户通过 Jabber 客户端接收传输到其桌面电话的视频。
统一连接				
	7080	HTTP	TCP	用于 Cisco Unity Connection 以接收语音留言通知（新留言、留言更新和删除的留言）。
	7443	HTTPS	TCP	用于 Cisco Unity Connection 以安全接收语音留言通知（新留言、留言更新和删除的留言）。
	8443	HTTPS	TCP	连接到 Cisco Unity Connection 进行配置。
	443	HTTPS	TCP	连接至 Cisco Unity Connection，用于语音邮件。

	端口	应用层协议	传输层协议	说明
Cisco Webex Meetings				
	80	HTTP	TCP	连接至 Cisco Webex Meetings 中心，用于会议。
	443	HTTPS	TCP	连接至 Cisco Webex Meetings 中心，用于会议。
	8443	HTTPS	TCP	Cisco Unified Communications Manager 的 Web 访问，包括以下各项的连接： • 已分配设备的 Cisco Unified Communications Manager IP 电话 (CCMCIP) 服务器 • 用于联系人解析的用户数据服务 (UDS)
附件管理器				
	8001		TCP	在 Cisco Jabber Windows 版本和 Mac 版本中，Sennheiser 插件使用此端口用于呼叫控制的本地主机通信。

其他服务和协议端口

除了在本节中列出的端口之外，查看您部署中的所有协议和服务所需的端口。您可以在以下文档中找到适用于不同服务器的端口和协议要求：

- 对于 Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service，请参阅《*TCP* 和 *UDP* 端口使用情况指南》。
- 对于 Cisco Unity Connection，请参阅《系统管理指南》。
- 对于 Cisco Webex Meetings服务器，参阅 《管理指南》。
- 对于 Cisco Meeting Server，请参阅《*Cisco Meeting Server 2.6* 和 *2.7* 版：单一组合的会议服务器部署》。
- 对于 Cisco Webex服务，参阅《管理员指南》。
- 对于 Expressway for Mobile and Remote Access，请参阅用于防火墙穿越的 *Cisco Expressway IP* 端口的使用。
- 对于文件传输端口使用情况，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的配置和管理》。

支持的编解码器

类型	编解码器	编解码器类型	**Cisco Jabber Android** 版本	**Cisco Jabber iPhone** 和 **iPad** 版本	**Cisco Jabber Mac** 版本	**Cisco Jabber Windows** 版本
音频	G.711	A-法律	是 支持正常模式。		是	是
		μ-法律/Mu-法律	是 支持正常模式。		是	是
	G.722		是		是	是
	G.722.1	24 kb/s 和 32 kb/s	是 支持正常模式。		是	是
	G.729		不支持带 g.729 的视觉语音邮件；不过，您可以使用 g.729 和**呼叫语音邮件**功能访问语音留言。		否	否
	G.729a		是 低带宽可用性的最低要求。 只有支持低带宽模式的编解码器。 支持正常模式。		是	是
	Opus		是		是	是
视频	H.264/AVC	基线配置文件	是		是	是
		高配置文件	否		是	是
语音邮件	G.711	A-法律	是		是	是
		μ-法律/Mu-法律（默认值）	是		是	是
	PCM 线性格式		是		是	是

如果用户在使用Cisco Jabber Android 版本或Cisco Jabber iPhone 和 iPad 版本时有语音质量问题，可以在客户端设置中打开和关闭低带宽模式。

虚拟环境要求

软件要求

要在Cisco Jabber Windows 版本虚拟环境中部署，请从以下支持的软件版本中进行选择：

软件	支持的版本
Citrix XenDesktop	7.9, 7.8, 7.6, 7.5, 7.1
Citrix XenApp	7.9 发布的应用和桌面 7.8 发布的应用和桌面 7.6 发布的应用和桌面 7.5 发布的桌面 6.5 发布的桌面
VMware Horizon View	6.x 到 8.x

网络电话要求

对于网络电话呼叫，请使用 Jabber VDI 软终端。有关详细信息，请参阅《**Cisco Jabber VDI 软终端版本 12.9 发行说明**》

音频和视频性能参考

注意 以下数据基于在实验室环境中测试。此数据旨在提供您可以在带宽用量方面期望什么的想法。本主题中的内容并非面面俱到，也不是为了反映可能影响带宽用量的所有媒体情景。

媒体保证

确保所有网络类型上的实时媒体质量，保证会议不会因媒体质量差而中断。媒体确保可以最多减少 25% 的丢包。

Cisco Unified Communications Manager 10.x 版或更高版本上的视频以及音频和视频，支持媒体确保 Cisco Unified Communications Manager Release 版本 11.5 或更高版本。

对于 Expressway for Mobile and Remote Access 部署，Media Assure 要求 Cisco Expressway 8.8.1 版或更高版本。

对于轻微到严重的网络状况，Jabber可以：

- 暂时限制流上的带宽。

- 重新同步视频。
- 对数据包进行同步，以避免基于不必要的拥塞的突发丢失。
- 通过使用来自第一个媒体数据包的预先 SDP 信令提供弹性机制。
- 保护丢包。
- 避免因媒体生产而造成的基于拥塞的损失。
- 改进低帧速率/低比特率流的保护。
- 支持经过验证和加密的 FEC。

快速通道支持

快速通道支持可确保网络上的业务关键应用程序的优先顺序，即使在流量较高的情况下也是如此。Jabber 支持语音和视频流量的快速通道。对于 iOS 10，使用接入点（AP）快速 lane 功能时，Cisco Unified Communications Manager 上配置的 DSCP 值将不再使用。而对于ios 9版本或 ios 10 ios 11，Jabber 将继续使用 Cisco Unified Communications Manager 上配置的 DSCP 值。

无论 Cisco Unified Communications Manager 上的 DSCP 配置如何，如果您的无线 AP 支持快速通道功能，则 Jabber 会自动设置以下 DSCP 和用户优先级（UP）值：

- 对于视频呼叫中的音频呼叫或音频部分，DSCP 设置为 "0x2e"，“向上”设置为 6。
- 对于视频呼叫中的视频部分，DSCP 设置为 "0x22"，“向上”设置为 5。
- 如果您的 AP 不支持快速通道或不使用，则会自动将 DSCP 值设置为 Cisco Unified Communications Manager 指定的值。

先决条件：

- 运行 AireOS 8.3 和更高版本的 WLC
- AP1600/2600 系列接入点、AP1700/2700 系列接入点、AP3500 系列接入点、AP3600 系列接入点 + 11ac 模块、WSM、Hyperlocation Module、3602P、AP3700 系列接入点 + WSM、3702P、OEAP600 系列 OfficeExtend 接入点 AP700 系列接入点、AP700W 系列接入点、AP1530 系列接入点、AP1550 系列接入点、AP1570 系列接入点和 AP1040/1140/1260 系列接入点
- ios 11或更高版本上运行的 ios 设备。

Cisco Jabber 桌面客户端的音频比特率

适用于 Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本。

编解码器	RTP（千/秒）	实际比特率（千/秒）	备注
G.722.1	24/32	54/62	高品质压缩

编解码器	RTP（千/秒）	实际比特率（千/秒）	备注
G.711	64	80	标准未压缩
G.729a	8	38	低质量压缩

Cisco Jabber 移动客户端的音频比特率

以下音频比特率适用于 Cisco Jabber iphone 版本和 Cisco Jabber Android 版本。

编解码器	编解码器比特率（千比特/秒）	使用的网络带宽（千位/秒）
g.711	64	80
g.722.1	32	48
g.722.1	24	40
g.729a	8	24

Cisco Jabber 桌面客户端的视频比特率

以下视频比特率（使用 g.711 音频）适用于 Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本。此表未列出所有可能的分辨率。

解决方案	Pixels	含 g.711 音频的测量比特率（千比特/秒）
w144p	256 x 144	156
w288p 这是 Cisco Jabber 的视频渲染窗口的默认大小。	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300
1080p	1920 x 1080	2500-4000

注释 测量比特率是指所用的实际带宽（RTP 负载 + IP 数据包开销）。

Cisco Jabber Android 版本的视频比特率

视频	解决方案	带宽
HD	1280 x 720	1024
VGA	640 x 360	512
CIF	488x211	310

注释 在呼叫过程中发送和接收高清视频：

- 在 Cisco Unified Communications Manager 中配置高于 1024 kbps 的视频呼叫的最大比特率。
- 在路由器上启用 DSCP，以传输具有高优先级的视频 RTP 包。

Cisco Jabber iPhone 和 iPad 版本的视频比特率

客户端以 20 fps 的速率捕获和传输。

解决方案	Pixels	使用 g.711 音频的比特率（千位/秒）
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415
w720p	1280 x 720	1024

演示视频比特率

Cisco Jabber 以 8 fps 捕获，并以 2 – 8 fps 传输。

此表中的值不包括音频。

Pixels	估计的线位速率为2 fps（千比特/秒）	估计的线速为8 fps（千比特/秒）
720 x 480	41	164
704 x 576	47	188
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400

Pixels	估计的线位速率为2fps（千比特/秒）	估计的线速为8 fps（千比特/秒）
1920 x 1080	150-300	500-1000

在版本 12.5 中，当视频带宽总量低于 300 kb 时，我们将更改比特率分配以改善主要视频质量。但是，此更改还会设置主视频的最大比特率，以 450 千比特/秒为单位。

在视频带宽较高的情况下，您可能会看到在主视频中与以前版本相比，较低的分辨率。

最大的协商比特率

您可以在“Cisco Unified Communications Manager”的“区域配置”窗口中指定最大有效负载比特率。此最大负载比特率不包括数据包开销，因此实际使用的比特率大于您指定的最大负载比特率。

下表描述了 Cisco Jabber 如何分配最大有效负载比特率：

桌面共享会话	音频	交互视频（主视频）	演示视频（桌面共享视频）
否	Cisco Jabber 使用最大音频比特率。	Cisco Jabber 分配剩余的比特率，如下所示： 最大视频呼叫比特率减去音频比特率。	—
是	Cisco Jabber 使用最大音频比特率。	Cisco Jabber 在减去音频比特率后分配剩余带宽的一半。	Cisco Jabber 在减去音频比特率后分配剩余带宽的一半。

音频	交互视频（主视频）
Cisco Jabber 使用最大音频比特率	Cisco Jabber 分配剩余的比特率，如下所示： 最大视频呼叫比特率减去音频比特率。

带宽

Cisco Unified Communications Manager 的区域配置可限制客户端可用的带宽。

通过指定音频和视频呼叫中与传输无关的最大比特率，使用区域来限制用于区域内和现有区域之间的音频和视频呼叫的带宽。有关区域配置的更多信息，请参见您所用版本的 Cisco Unified Communications Manager 文档。

Cisco Jabber 桌面客户端的带宽性能期望

Cisco Jabber Mac 版本分离音频的比特率，然后在交互式视频和演示视频之间平均分配剩余带宽。下表提供的信息可帮助您了解，每个带宽应该实现什么性能：

上传速度	音频	音频 + 交互视频（主视频）
在 VPN 下，125 kbps	适用于 g.711的带宽阈值处。g.729a 和 g.722.1有足够的带宽。	视频带宽不足。
在 VPN 下，384 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w288p (512 x 288)
在企业网络中，384 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w288p (512 x 288)
1000 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w576p (1024 x 576)
2000 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w720p30 (1280 x 720)

Cisco Jabber Windows 版本分离音频的比特率，然后在交互式视频和演示视频之间平均分配剩余带宽。下表提供的信息可帮助您了解，每个带宽应该实现什么性能：

上传速度	音频	音频 + 交互视频（主视频）	音频 + 演示视频（桌面共享视频）	音频 + 交互视频 + 演示视频
在 VPN 下，125 kbps	适用于 g.711的带宽阈值处。g.729a 和 g.722.1有足够的带宽。 。	视频带宽不足。	视频带宽不足。	视频带宽不足。
在 VPN 下，384 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w288p (512 x 288)	在 2+ fps 时，1280 x 800	在 30 fps 时，w144p (256 x 144) 在 2+ fps 时， + 1280 x 720
在企业网络中，384 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w288p (512 x 288)	在 2+ fps 时，1280 x 800	在 30 fps 时，w144p (256 x 144) 在 2+ fps 时， + 1280 x 800
1000 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w576p (1024 x 576)	在 8 fps 时，1280 x 800	在 30 fps 时，w288p (512 x 288) 在 8 fps 时， + 1280 x 800
2000 kbps	足够的带宽适合任何音频编解码器。	在 30 fps 时，w720p30 (1280 x 720)	在 8 fps 时，1280 x 800	在 30 fps 时，w288p (1024 x 576) 在 8 fps 时，+ 1280 x 800

请注意，VPN 会增加负载大小，从而增加带宽消耗。

Cisco Jabber Android 版本的带宽性能期望值

请注意，VPN 会增加负载大小，从而增加带宽消耗。

上传速度	音频	音频 + 交互视频（主视频）
在 VPN 下，125 kbps	适用于 g.711 的带宽阈值处。视频带宽不足。 g.729a 和 g.722.1 有足够的带宽。	视频带宽不足。
256 kbps	足够的带宽适合任何音频编解码器。	传输速率（Tx）-256 x 144，每 15 fps 接收速率（Rx）-256 x 144，速度为 30 fps
在 VPN 下，384 kbps	足够的带宽适合任何音频编解码器。	15 fps 时，Tx-640 x 360 30 fps 时，Rx — 640 x 360
在企业网络中，384 kbps	足够的带宽适合任何音频编解码器。	15 fps 时，Tx-640 x 360 30 fps 时，Rx — 640 x 360

注释 由于设备限制，Samsung Galaxy SII 和 Samsung Galaxy SIII 设备无法达到此表中列出的最大分辨率。

Cisco Jabber iPhone 和 iPad 版本的带宽性能期望值

客户端会为音频分配比特率，然后将剩余的带宽在交互视频和演示视频之间平分。下表提供的信息可帮助您了解，每个带宽应该实现什么性能。

请注意，VPN 会增加负载大小，从而增加带宽消耗。

上传速度	音频	音频 + 交互视频（主视频）
在 VPN 下，125 kbps	适用于 g.711 的带宽阈值处。视频带宽不足。 g.729a 和 g.722.1 有足够的带宽。	视频带宽不足。
290 kbps	足够的带宽适合任何音频编解码器。	20 fps 时为 256 x144
415 kbps	足够的带宽适合任何音频编解码器。	20 fps 时为 640 x 360
1024 kbps	足够的带宽适合任何音频编解码器。	20 fps 时为 1280 x 720

视频速率调整

Cisco Jabber 使用视频速率调整来协调最佳视频质量。视频速率调整会动态增加或减少视频比特率吞吐量，以处理可用 IP 路径带宽上的实时变化。

Cisco Jabber 用户应该期望视频呼叫以较低的分辨率开始，并在较短的时间内向较高的分辨率调整。Cisco Jabber 会保存历史记录，以便后续视频呼叫应以最佳分辨率开始。

H.264 配置文件对带宽的影响

在早期版本中，我们仅支持 H.264 基线配置文件。在版本 12.8 中，我们为桌面客户端添加了对 H.264 高配置文件的支持。您不能对 VDI 或移动客户端使用高配置文件。

高配置文件可提供相同的视频质量，最多可减少 10% 的带宽。或者，您也可以使用相同的带宽获得更好的视频质量。

Jabber 的默认值为 H.264 基准配置文件。要启用高配置文件，我们是 H264HighProfileEnable 参数。

呼叫管理记录

呼叫结束时，Cisco Jabber 会将呼叫性能和质量信息发送到 Cisco Unified Communications Manager。Cisco Unified Communications Manager 使用这些指标填充 Cisco Unified Communications Manager 呼叫管理记录 (CMR)。Cisco Jabber 会发送音频和视频呼叫的下列信息：

- 发出和收到的信息包数。
- 发出和收到的八位字节数。
- 丢失的数据包数量。
- 平均抖动。

客户端还将发送以下视频相关的信息：

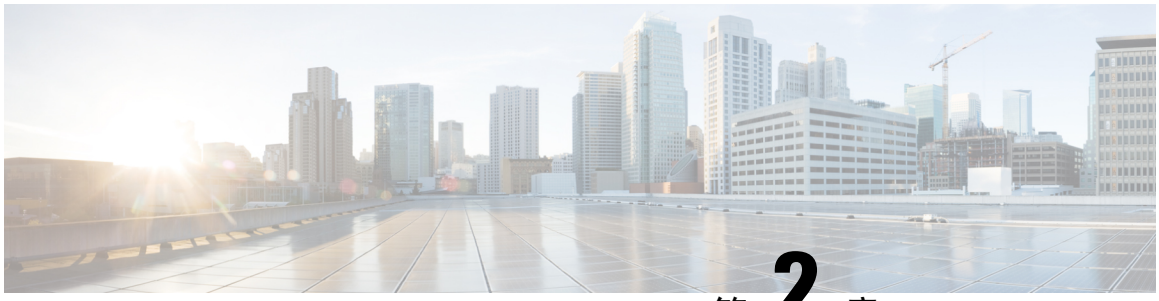
- 已发送和接收编解码器。
- 已发送和已接收分辨率。
- 发送和接收的帧率。
- 平均往返时间 (RTT)

客户端将发送以下音频相关的信息：

- 隐蔽秒数。
- 严重隐蔽秒数。

这些指标在 Cisco Unified Communications Manager CMR 记录输出中以纯文本格式显示；此数据可以直接读取，也可以由遥测或分析应用程序使用。

有关配置 Cisco Unified Communications Manager CMR 记录的详细信息，请参阅您 Cisco Unified Communications Manager 版本的《呼叫详细记录管理指南》的呼叫管理记录一章。



第 2 章

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

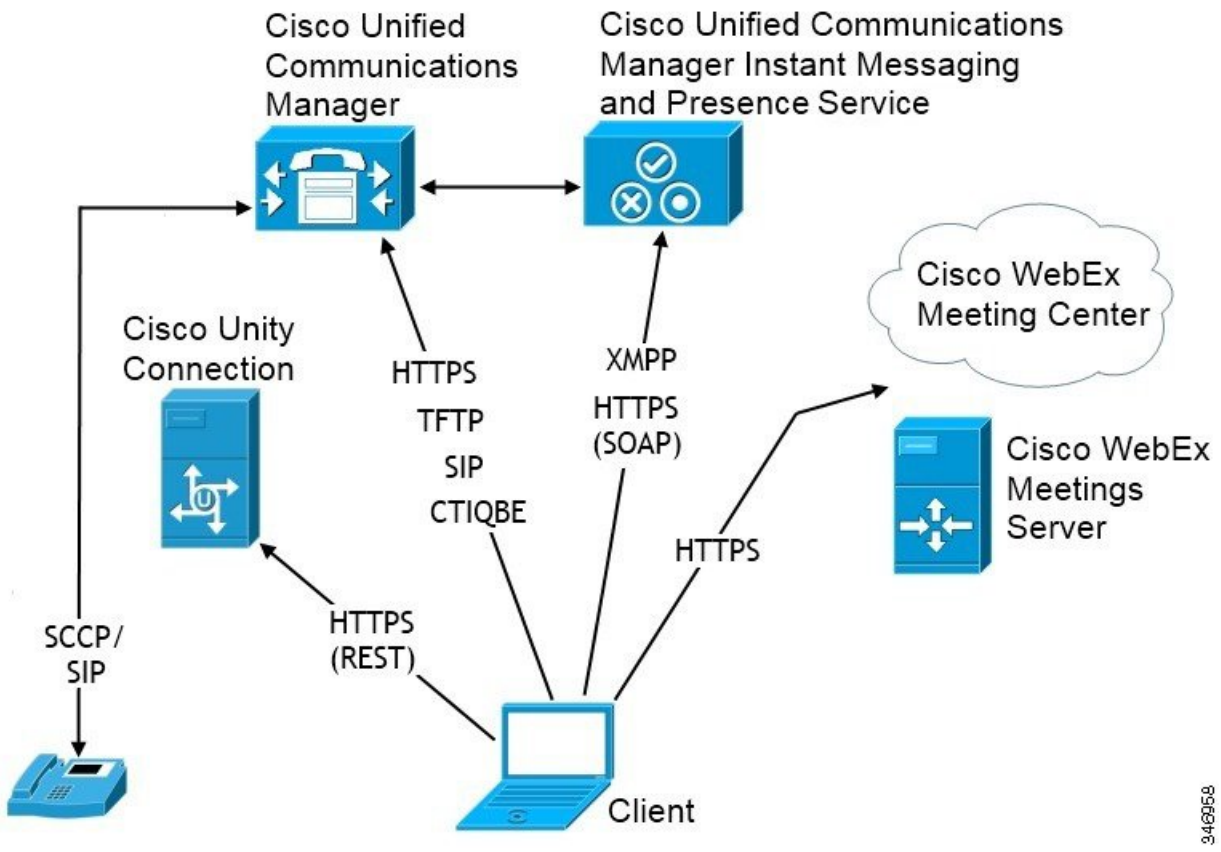
通过 Cisco Unified Communications Manager IM and Presence Service 在内部部署中提供以下服务：

- **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

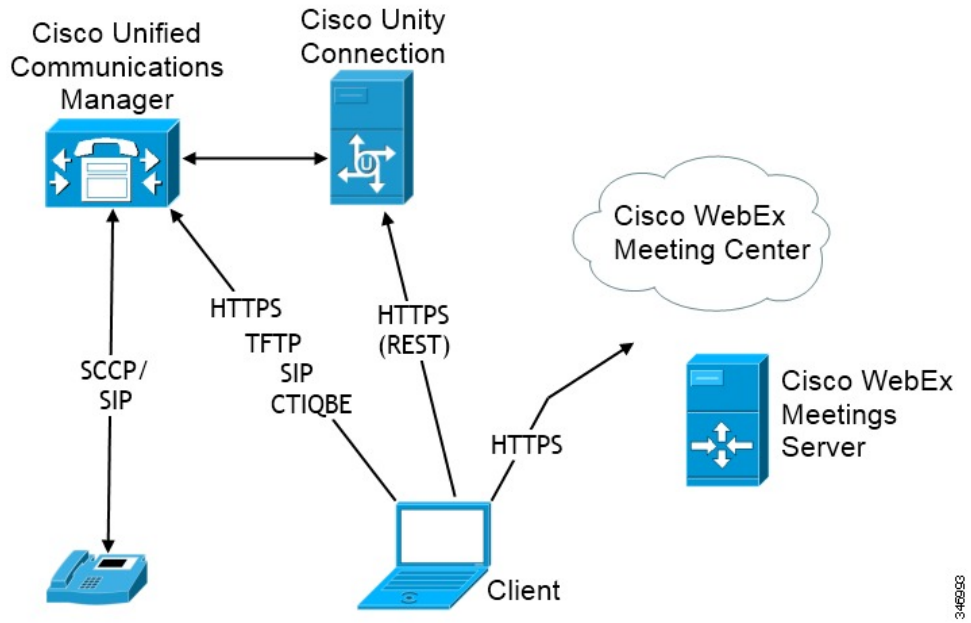
电话模式部署中提供以下服务：

- **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

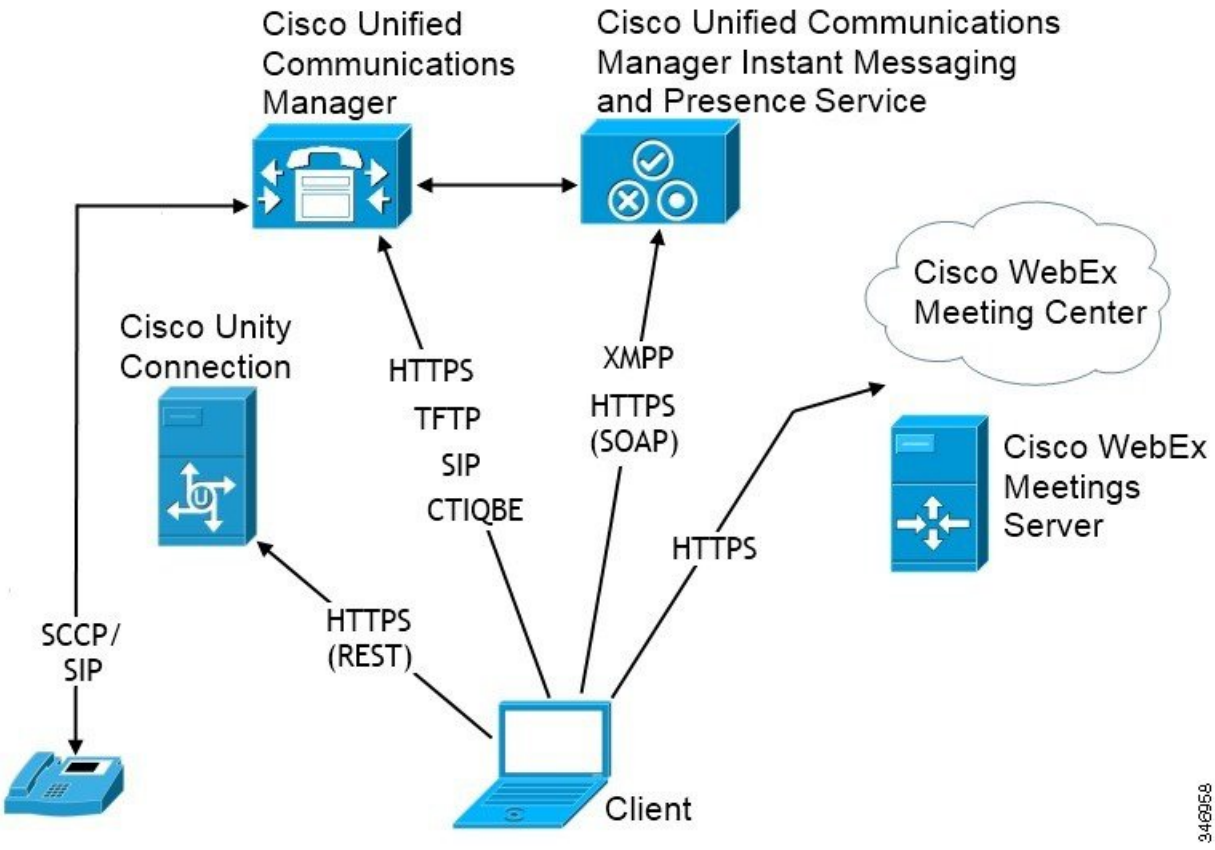
在“带有联系人功能的电话模式”部署中提供以下服务：

- **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。

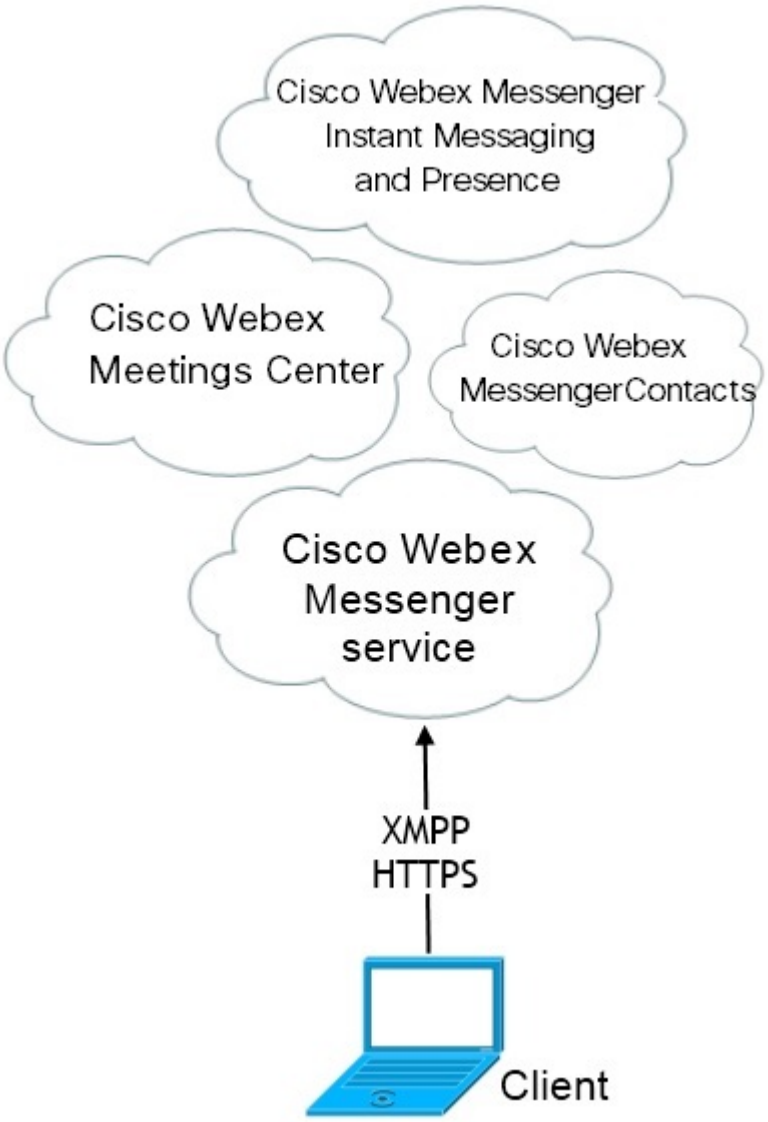
对于采用 Cisco Webex 平台服务 的云和混合部署，可以使用 Cisco 控制中心来管理和监控您的部署。

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。

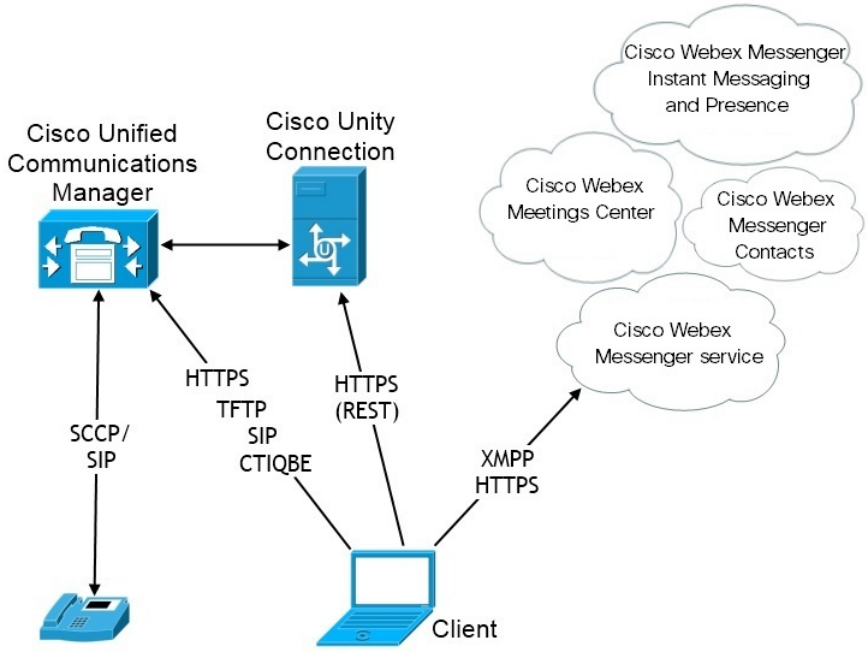


采用 Cisco Webex Messenger 服务的基于云的混合部署

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。



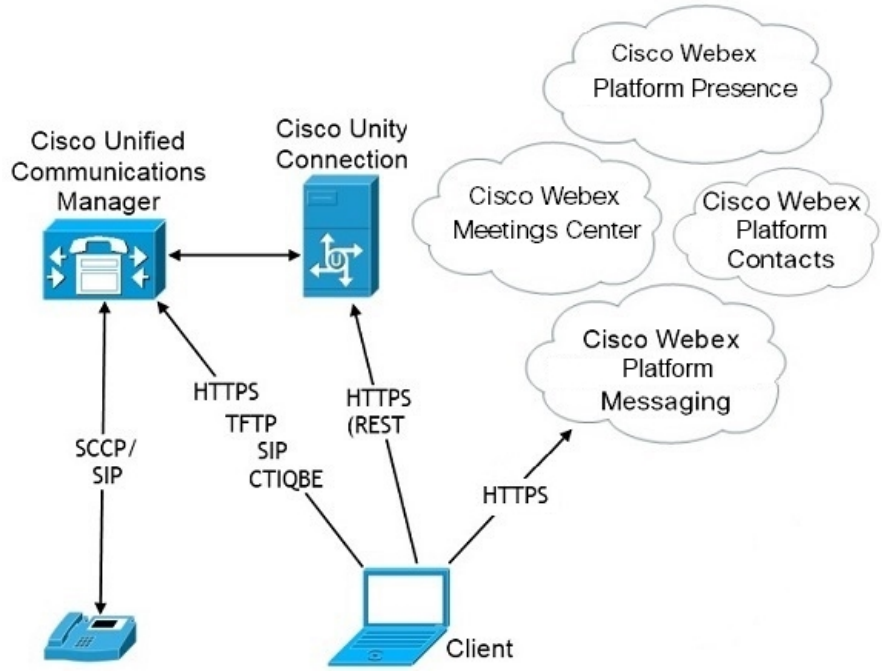
基于云的混合云部署，采用 Cisco Webex 平台服务

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 [3]	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

[3] 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。

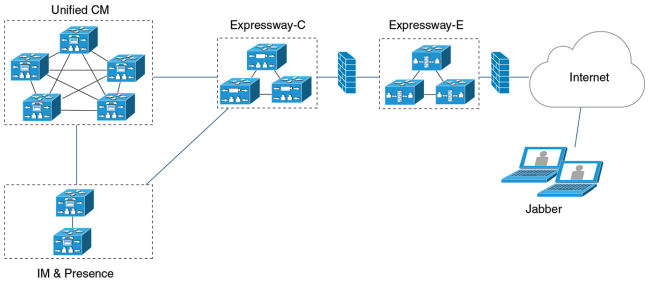
Jabber 未经任何第三方 VPN 客户端测试或验证。

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 *2:* 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：

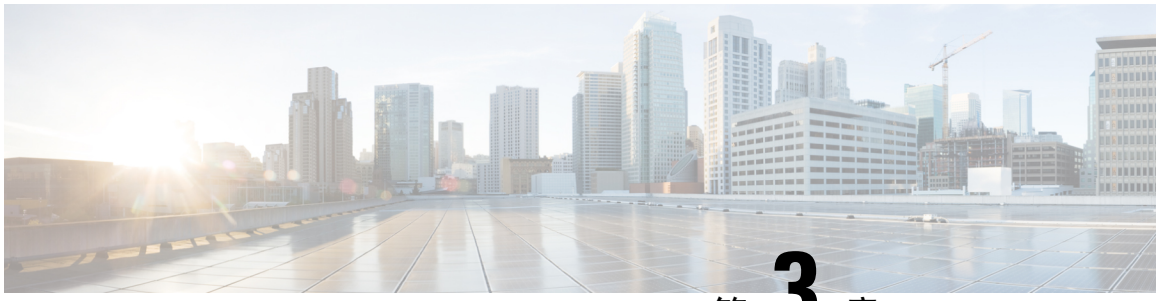
产品	所需浏览器
Cisco Jabber Windows 版本	Internet Explorer
Cisco Jabber Mac 版本	Safari
Cisco Jabber iPhone 和 iPad 版本	Safari
Cisco Jabber Android 版本	Chrome 或 Internet Explorer

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。



第 3 章

用户管理

Jabber ID

Cisco Jabber 使用 Jabber ID 标识联系人来源中的联系人信息。

使用用户 ID 和在线状态域创建默认 Jabber ID。

例如，Adam McKenzie 的用户 ID 为 `amckenzie`，他的域为 `example.com`，其 Jabber ID 为 `amckenzie@example.com`。

Cisco Jabber 用户 ID 或电子邮件地址支持下列字符：

- 大写字符（A 到 Z）
- 小写字符（a 到 z）
- 数字 (0-9)
- 点号 (.)
- 连字符 (-)
- 下划线 (_)
- 代字号 (~)
- 井号标签 (#)

当填充联系人列表时，客户端将使用 Jabber ID 搜索联系人来源以解析联系人，并显示“名字”、“姓氏”和任何其他联系信息。

IM 地址方案

Cisco Jabber 10.6 和更高版本支持在域处于相同的在线状态架构（例如 example-us.com 和 example-uk.com 中的用户）时用于内部部署的多个在线状态域架构模型。Cisco Jabber 支持使用 Cisco Unified Communications Manager IM and Presence 10. x 或更高版本的灵活 IM 地址方案。IM 地址方案是用于识别 Cisco Jabber 用户的 Jabber ID。

为支持多域模型，部署的所有组件都需要以下版本：

- Cisco Unified Communications IM and Presence 服务器节点和呼叫控制节点版本 10. x 或更高版本。
- 在 Windows、Mac、IOS 和 Android 版本 10.6 或更高版本上运行的所有客户端。

在以下情况下，仅部署具有多个域架构的 Cisco Jabber：

- Cisco Jabber 10.6 或更高版本经部署为所有平台（Windows、Mac、IOS 和 Android，包括基于 Android 的 IP Phones（例如 DX 系列））上组织中所有用户的全新安装。
- 在在线状态服务器上更改任何域或 IM 地址之前，Cisco Jabber 将为所有平台（Windows、Mac、IOS 和 Android，包括基于 Android 的 IP 电话（例如 DX 系列））上的所有用户升级到版本 10.6 或更高版本。

高级在线状态设置中的可用 IM 地址方案包括：

- UserID@[默认域]
- 目录 URI

UserID@[默认域]

将“用户 ID”字段映射到 LDAP 字段。这是默认的 IM 地址方案。

例如，用户 Anita Perez 的帐户名称为 aperez，且将“用户 ID”字段映射到 sAMAccountName LDAP 字段。使用的地址方案为 aperez@example.com。

目录 URI

将目录 URI 映射到**邮件**或 **msrtcsip-primaryuseraddress msrtcsip-primaryuseraddress** LDAP 字段。此选项提供独立于用于身份验证的用户 ID 的方案。

例如，用户 Anita Perez 的帐户名称为 aperez，“邮件”字段为 Anita.Perez@domain.com，使用的地址方案为 Anita.Perez@domain.com。

使用 Jabber ID 的服务发现

服务发现使用以 `[userid]@[domain.com]` 格式输入的 Jabber ID，并且默认情况下会提取 Jabber ID 的 `domain.com` 部分以发现可用的服务。对于在线状态域与服务发现域不同的部署，您可以在安装期间包含服务发现域信息，如下所示：

- 在 Cisco Jabber Windows 版本中，此操作使用 `SERVICES_DOMAIN` 命令行参数完成。
- 在 Cisco Jabber Mac 版本、Cisco Jabber Android 版本或 Cisco Jabber iPhone 和 iPad 版本中，可以使用与 URL 配置配用的 `ServicesDomain` 参数设置服务发现域。

。

SIP URI

SIP URI 与每个用户关联。SIP URI 可以是电子邮件地址、IMAddress 或 UPN。

SIP URI 使用 Cisco Unified Communications Manager 中的“目录 URI”字段进行配置。以下是可用的选项：

- 邮件
- msRTCSIP-primaryuseraddress

用户可以通过输入 SIP URI 搜索联系人并给联系人拨号。

LDAP 用户 ID

您从目录来源同步到 Cisco Unified Communications Manager 时，可以从目录属性填充用户 ID。保留用户 ID 的默认属性为 `sAMAccountName`。

用于联合的用户 ID 规划

对于联合，Cisco Jabber 需要每个用户的联系人 ID 或用户 ID，以便在联系人搜索期间解析联系人。

在 SipUri 参数中设置用户 ID 的属性。默认值为 `msRTCSIP-PrimaryUserAddress`。如果存在要从您的用户 ID 中删除的某个前缀，您可以在 UriPrefix 参数中设置一个值，请参阅《*Cisco Jabber* 的参数参考指南》的最新版本。

用于用户联系人照片的代理地址

Cisco Jabber 访问照片服务器以检索联系人照片。如果您的网络配置包含 Web 代理，则需要确保 Cisco Jabber 能够访问照片服务器。

身份验证和授权

Cisco Unified Communications Manager LDAP 身份验证

在 Cisco Unified Communications Manager 上配置 LDAP 验证，以通过目录服务器进行验证。

当用户登录到客户端时，在线状态服务器会将身份验证路由到 Cisco Unified Communications Manager。Cisco Unified Communications Manager 随后会将该身份验证代理到目录服务器。

Cisco Webex Messenger 登录验证

使用 Cisco Webex 管理工具配置 Cisco Webex Messenger 身份验证。

当用户登录到客户端时，该信息将发送到 Cisco Webex Messenger，并且身份验证令牌会发送回客户端。

单点登录身份验证

使用身份提供程序 (IdP) 和服务配置单点登录验证。

当用户登录到客户端时，该信息将发送到 IdP，一旦接受凭证，身份验证令牌就会发送回 Cisco Jabber。

用于 Cisco Jabber iPhone 和 iPad 版本的基于证书的验证

Cisco Jabber 通过客户端证书在 IdP 服务器上进行身份验证。此证书验证可让用户无需输入用户凭证即可登录到服务器。客户端使用 Safari 框架来实施此功能。

要求

- Cisco Unified Communications Manager 11.5、IM and Presence Service 11.5、Cisco Unity Connection 11.5 及更高版本。
- Expressway for Mobile and Remote Access server 8.9 及更高版本。
- SSO 已针对统一通信基础设施启用。
- 所有服务器证书均已由 CA 签署，包括 Cisco Unified Communications Manager、IM and Presence Service、Cisco Unity Connection 和 IdP 服务器。如果 iOS 设备使用 OS 的受信任授权机构，请在安装 Cisco Jabber 应用程序之前安装 CA 证书。
- 在 Cisco Unified Communications Manager 中为 SSO 配置本机浏览器（嵌入式 Safari）。有关详细信息，请参阅 *Cisco Jabber* 内部部署中基于证书的 SSO 身份验证部分。
- 在 Expressway for Mobile and Remote Access server 中配置用于 SSO 的本机浏览器（嵌入式 Safari）。有关详细信息，请参阅 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html 处的《Cisco Expressway 安装指南》。

您可以通过 EMM 解决方案在 iOS 设备上部署 Cisco 证书。

建议 — **Cisco** 建议使用 EMM 解决方案在 iOS 设备上部署证书。

用于 Cisco Jabber Android 版本的基于证书的验证

Cisco Jabber 使用客户端证书登录到单点登录服务器（Webex Messenger 和内部）。

要求

- Android 操作系统 5.0 或更高版本
- 已启用单点登录
- Jabber 客户端通过移动和Remote Access (MRA) 和非 MRA 部署模式得到支持。
- Jabber 始终在 Android 7.0 和更高版本上显示无效证书的通知，即使 Android OS 上已安装自定义 CA 签名的证书也是如此。面向 Android 7.0 的应用程序仅信任系统提供的证书，不再信任用户添加的证书权限。

证书部署

Cisco 建议使用 EMM 解决方案在 Android 设备上部署证书。

语音邮件验证

用户需要在 Cisco Unity Connection 上存在。Cisco Unity Connection 支持多个验证类型。如果 Cisco Unified Communications Manager 和 Cisco Unity Connection 使用相同的验证，我们建议将 Cisco Jabber 配置为使用相同的凭证。

OAuth

您可以将 Cisco Jabber 设置为使用 OAuth 协议来授权用户对服务的访问权限。如果用户登录到启用 OAuth 的环境，则无需在每次用户登录时都输入凭证。但是，如果服务器没有启用 OAuth，则 Jabber 可能无法正常工作。

如果您使用 Cisco Unified Communication Manager 12.5 或更高版本，您也可以启用 SIP OAuth。它允许 Jabber 向 SIP 自行授权，从而允许 Jabber 通过 TLS 连接到 SIP 服务。它还可让 Jabber 通过安全连接 (sRTP) 发送媒体。SIP OAuth 意味着不再需要 CAPF 注册来启用安全 SIP 和媒体。

先决条件：

- 如果部署为功能，则必须跨所有这些组件打开 OAuth 刷新令牌
- Cisco Unified Communication Manager、Cisco Unified Communication ManagerInstant Messaging and Presence 以及 Cisco Unity Connection 必须是版本 11.5(SU3) 或 12.0
- Cisco Expressway for Mobile and Remote Access 版本 X8.10 或更高版本

- 对于 SIP OAuth：Cisco Unified Communication Manager 12.5 或更高版本、Cisco Expressway for Mobile and Remote Access 版本 X12.5 或更高版本。

在配置 OAuth 之前，请检查您拥有的部署类型：

- 如果您有本地验证部署，则不需要 IdP 服务器，Cisco Unified Communication Manager 负责进行验证。
- 您可以配置或不配置 SSO 来设置 OAuth。如果您正使用 SSO，请确保将其为所有服务启用。如果您有启用 SSO 的部署，则部署 IdP 服务器，IdP 服务器负责进行验证。

您可以为您的用户启用以下服务的 OAuth：

- Cisco Unified Communications Manager
- Cisco Expressway
- Cisco Unity Connection

默认情况下，这些服务器上禁用 OAuth。要在这些服务器上启用 OAuth：

- 对于 Cisco Unified Communications Manager 和 Cisco Unity Connection 服务器，请转到**具有刷新登录流 > 的企业参数配置 OAuth**。
- 对于 Cisco Expressway，转至**通过刷新由 OAuth 令牌授权的配置统一通信 > 配置**。

当在任何这些服务器上启用或禁用 OAuth 时，Jabber 会在配置重新提取间隔内识别它，并让用户注销并登录到 Jabber。

在注销期间，Jabber 会删除缓存中存储的用户凭证，然后让用户使用常规登录流登录，其中 Jabber 首先获取所有配置信息，然后让用户访问 Jabber 服务。

要配置 Cisco Unified Communication Manager 上的 OAuth：

1. 转至 **Cisco Unified Communications Manager 管理 > 系统 > 企业参数 > SSO 配置**。
2. 将 **O-Auth 访问令牌到期计时器（分钟）**设置为所需的值。
3. 将 **O-Auth 刷新令牌到期计时器（天）**设置为所需的值。
4. 点击**保存**按钮。

要在 Cisco Expressway 上配置 OAuth：

1. 转至**配置 > 统一通信 > 配置 > MRA 访问控制**。
2. 将 **O-Auth 本地身份验证**设置为“开”。

要在 Cisco Unity 上配置 OAuth：

1. 转至 **AuthZ 服务器**并选择**新增**。
2. 在所有字段中输入详细信息，然后选择“**忽略证书错误**”。
3. 单击**保存**。

限制

Jabber 触发自动入侵保护

条件：

- 配置您的 Expressway for Mobile and Remote Access 部署以通过 OAuth 令牌（带有或不带刷新令牌）进行授权。
- Jabber 用户的访问令牌已过期。

Jabber 执行以下一项操作：

- 从桌面休眠恢复
- 恢复网络连接
- 在注销后几个小时尝试快速登录

行为:

- 一些 Jabber 模块尝试使用过期的访问令牌在 Expressway-E 上进行授权。
- Expressway-E（正确）拒绝这些请求。
- 如果特定 Jabber 客户端上有五个以上的此类请求，Expressway-E 将阻止该 IP 地址十分钟（默认）。

症状：

受影响的 Jabber 客户端的 IP 地址将添加到 HTTP 代理授权失败类别中 Expressway-E 的被阻止地址列表 。您可以在**系统** > **保护** > **自动检测** > **阻止的地址**上查看这些地址。.

暂时解决办法：

您可以通过两种方式解决此问题；您可以增加该特定类别的检测阈值，也可以为受影响的客户端创建例外。我们在此处介绍阈值选项，因为例外在您的环境中可能不实用。

1. 转至**系统** > **保护** > **自动检测** > **配置**。
2. 单击 **HTTP 代理授权失败**。
3. 将**触发器级别**从 5 更改为 10。10 必须足以容许显示到期令牌的 Jabber 模块。
4. 保存配置，此操作会立即生效。
5. 取消阻止任何受影响的客户端。

多资源登录

当用户登录到系统时，所有 Cisco Jabber 客户端都会向以下中心 IM and Presence Service 节点之一注册。此节点跟踪 IM and Presence Service 环境的可用性、联系人列表和其他方面。

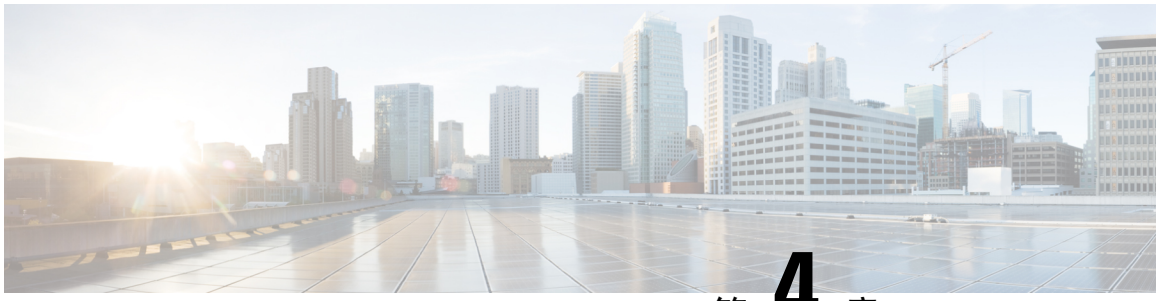
- 内部部署：Cisco Unified Communications Manager IM and Presence Service。

- 云部署：Cisco Webex。

此 IM and Presence Service 节点按以下顺序跟踪与每个唯一网络用户相关联的所有已注册客户端：

1. 当在两个用户之间启动新的 IM 会话时，第一个传入消息被广播给接收用户的所有注册的客户端。
2. IM and Presence Service 节点会等待其中一个注册的客户端的第一个响应。
3. 第一个响应的客户端然后会收到剩余的传入消息，直到用户使用另一个注册的客户端开始响应。
4. 然后，节点将后续消息重新路由到此新客户端。

注释 如果用户登录到多个设备时没有活动的资源，则优先级将给予具有最高在线状态优先级的客户端。如果所有设备上的在线状态优先级相同，则优先级将分配给用户登录到的最新客户端。



第 4 章

服务发现

客户端连接到服务的方式

要连接到服务，Cisco Jabber 需要以下信息：

- 使用户能够登录客户端的身份验证源。
- 服务的定位。

您可以使用以下方法为客户端提供该信息：

URL 配置

将从用户管理员处向用户发送电子邮件。该电子邮件包含的 URL 将配置服务发现所需的域。

服务发现

客户端会自动定位和连接服务。

手动连接设置

用户在客户端用户界面中手动输入连接设置。

Cisco Webex 平台服务 发现

Cisco Jabber 会将 HTTPS 请求发送到 Cisco Webex 平台服务，以检查是否已针对组消息模式启用用户。如果已针对组消息启用用户，则 Jabber 继续检查是否提供内部服务。

Cisco Webex Messenger 服务发现

Cisco Jabber 将云 HTTP 请求发送到 Cisco Webex Messenger 服务的 CAS URL。Cisco Jabber 使用 Cisco Webex Messenger 服务验证用户，并连接到可用的服务。

在 Cisco Webex 管理工具上配置服务。

Cisco 群集间查询服务

在具有多个 Cisco Unified Communications Manager 群集的环境中，您可以配置群集间查询服务 (ILS)。ILS 使得客户端能够查找用户的主群集和发现服务。

Expressway for Mobile and Remote Access 服务发现

Expressway for Mobile and Remote Access 可让远程用户访问服务。

客户端需要名称服务器来查询 SRV 记录。通过 `_collab-edge` SRV 记录，客户端通过 Expressway for Mobile and Remote Access 连接到内部网络并发现服务。

名称服务器返回 `_collab-edge` SRV 记录，客户端获取 Cisco Expressway-E 服务器的位置。然后，Cisco Expressway-E 服务器向客户端提供查询结果到内部名称服务器。这必须包括 `_cisco-uds` SRV 记录，然后客户端从 Cisco Unified Communication Manager 检索服务配置文件

注释 当您的语音服务域与登录域相同时，请勿为 MRA 配置 voiceservicesdomain。仅在域不同时配置 voiceservicesdomain。

建议的连接方法

您用来为客户端提供连接到服务所需信息的方法取决于您的部署类型、服务器版本和产品模式。下表重点介绍各种部署方法以及为客户端提供必要信息的方式。

表 *3:* 以下项的内部部署 ***Cisco Jabber Windows*** 版本

产品模式	服务器版本	发现方法	非 **DNS SRV** 记录方法
完全 UC（默认模式）	版本 9.1.2 及更高版本： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	针对 `_cisco-uds .<domain>` 的 DNS SRV 请求	使用以下安装程序交换机和值： • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=<presence_server_address>`
仅 IM（默认模式）	版本 9 及更高版本： Cisco Unified Communications Manager IM and Presence Service	针对 `_cisco-uds .<domain>` 的 DNS SRV 请求	使用以下安装程序交换机和值： • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=<presence_server_address>`
电话模式	版本 9 及更高版本： Cisco Unified Communications Manager	针对 `_cisco-uds .<domain>` 的 DNS SRV 请求	使用以下安装程序交换机和值： • `AUTHENTICATOR=CUCM` • `TFTP=<CUCM_address>` • `CCMCIP=<CUCM_address>` • `PRODUCT_MODE=Phone_Mode` 使用这种部署方法时不支持高可用性。

Cisco Unified Communications Manager 版本 9.x 和更低版本——如果启用了 Cisco Extension Mobility，则必须在用于 CCMCIP 的 Cisco Unified Communications Manager 节点上激活 `Cisco Extension Mobility` 服务。有关 Cisco Extension Mobility 的详细信息，请参阅您的 Cisco Unified Communications Manager 版本的功能和服务指南。

注释 Cisco Jabber 版本 9.6 和更高版本仍可使用 `_cuplogin` DNS SRV 请求（但 `_cisco-uds` 请求存在时会优先）发现完全统一通信和仅 IM 服务。

如果希望用户在初次登录全新安装期间绕过电子邮件屏幕，请使用 SERVICES_DOMAIN 安装程序交换机指定 DNS 记录所在域的值。

表 *4:* 以下项的内部部署 ***Cisco Jabber Mac*** 版本

产品模式	服务器版本	发现方法
完全UC（默认模式）	版本 9 及更高版本： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	针对 `_cisco-uds .<domain>` 的 DNS SRV 请求

表 *5:* ***Cisco Jabber Android*** 版本 和 ***Cisco Jabber iPhone*** 和 ***iPad*** 版本 的内部部署

产品模式	服务器版本	发现方法
完全 UC（默认模式）	版本 9 及更高版本： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	针对 `_cisco-uds.<domain>` 和 `_cuplogin.<domain>` 的 DNS SRV 请求
仅 IM（默认模式）	版本 9 及更高版本： Cisco Unified Communications Manager IM and Presence Service	针对 `_cisco-uds.<domain>` 和 `_cuplogin.<domain>` 的 DNS SRV 请求
电话模式	版本 9 及更高版本： Cisco Unified Communications Manager	针对 `_cisco-uds .<domain>` 的 DNS SRV 请求

注释 Cisco Unified Communications Manager 版本 9 和更高版本仍可使用 `_cuplogin` DNS SRV 请求（但 `_cisco-uds` 请求存在时会优先）发现完全统一通信和仅 IM 服务。

表 *6:* 基于云的混合部署

服务器版本	连接方法
Cisco Webex Messenger	针对 `https://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>` 的 HTTPS 请求
Cisco Webex 平台服务	针对 `atlas-a.wbx2.com` 的 HTTPS 请求

表 7: 基于云的部署

部署类型	连接方法
已针对单点登录 (SSO) 启用	Cisco Webex 管理工具 引导程序文件以设置 SSO_ORG_DOMAIN 参数。
没有针对 SSO 启用	Cisco Webex 管理工具

身份验证源

使用户能够登录客户端的身份验证源或身份验证器。

三种可能的身份验证源如下：

- Cisco Unified Communications Manager IM and Presence — 处于完全 UC 或仅 IM 的内部部署。
- Cisco Unified Communications Manager — 处于电话模式的内部部署。
- Cisco Webex Messenger 服务 — 基于云的或基于云的混合部署。
- Cisco Webex 平台服务基于云的或基于云的混合部署。

客户端如何查找服务

以下步骤介绍客户端如何利用 SRV 记录定位服务：

1. 客户端的主计算机或设备获取网络连接。

   当客户端的主计算机获取网络连接时，它也会从 DHCP 设置中获取域名系统 (DNS) 名称服务器的地址。

2. 用户在第一次登录期间采用以下方法之一来发现服务：

   - 手动 — 用户启动 Cisco Jabber，然后在欢迎屏幕上输入类似电子邮件的地址。
   - URL 配置 — URL 配置允许用户在不手动输入电子邮件的情况下单击链接以交叉启动 Cisco Jabber。
   - 使用企业移动性管理的移动配置 — 作为 URL 配置的替代，您还可以使用在 Cisco Jabber Android 版本上采用 Android for Work 和在 Cisco Jabber iPhone 和 iPad 版本上采用 Apple 托管的应用配置的企业移动性管理 (EMM) 配置 Cisco Jabber。您需要在用于创建 URL 配置链接的 EMM 控制台中配置相同的参数。

   要创建 URL 配置链接，请包括以下内容：

   - ServicesDomain — Cisco Jabber 用于服务发现的域。
   - VoiceServicesDomain — 对于混合部署，Cisco Jabber 用于检索 DNS SRV 记录的域可能不同于用于发现 Cisco Jabber 域的 ServicesDomain。

- ServiceDiscoveryExcludedServices — 在某些部署情况下，可以从服务发现过程中排除服务。这些值可以是以下各项的组合：
  - WEBEX
  - CUCM

注释 在包括所有三个参数时，不会进行服务发现，并且系统会提示用户手动输入连接设置。

按以下格式创建配置链接：

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
```

示例：

- `ciscojabber://provision?servicesdomain=example.com`
- `ciscojabber://provision?servicesdomain=example.com &VoiceServicesDomain=VoiceServices.example.com`
- `ciscojabber://provision?servicesdomain=example.com &ServiceDiscoveryExcludedServices=WEBEX,CUCM`

提供指向使用电子邮件或网站的用户的链接。

注释 如果您的组织使用支持跨启动专有协议或自定义链接的邮件应用程序，您可以为使用电子邮件的用户提供链接，否则向使用网站的用户提供链接。

3. 此客户端从 DHCP 设置获取 DNS 名称服务器的地址。
4. 客户端向 Cisco Webex Messenger 服务的中央验证服务 (CAS) URL 发出 HTTP 查询。

   此查询使得此客户端能够确定域是否为有效的 Cisco Webex 域。
5. 客户端以优先顺序查询以下 SRV 记录的名称服务器：
   - `_cisco-uds`
   - `_collab-edge`

注释 此客户端将缓存随后启动时要加载的 DNS 查询的结果。

注释 此客户端将缓存随后启动时要加载的 DNS 查询的结果。

以下是 SRV 记录条目的示例：

```
_cisco_uds._tcp.DOMAIN SRV service location:
 priority = 0
 weight = 0
 port = 8443
 svr hostname=192.168.0.26
```

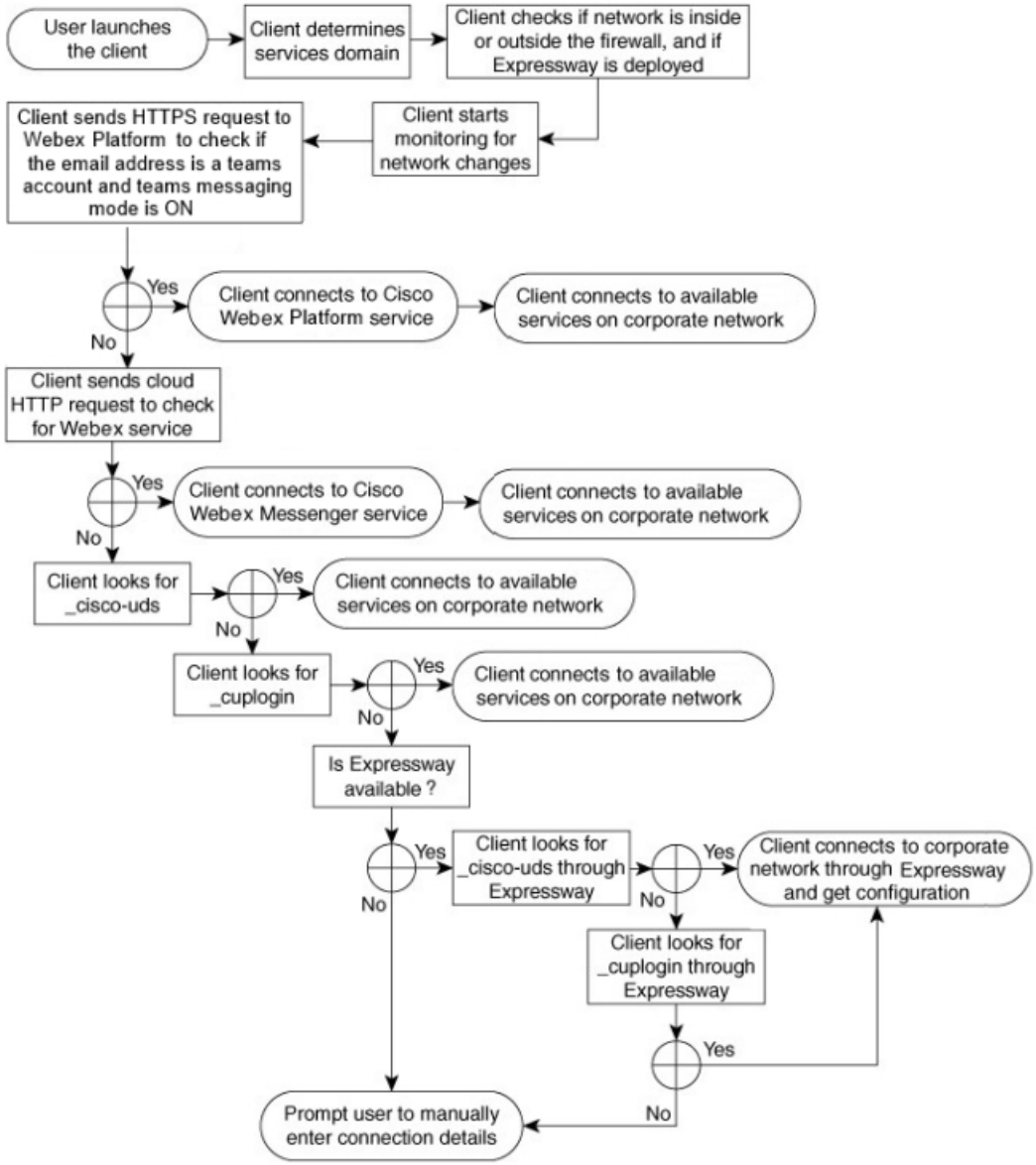
方法 1：搜索服务

我们建议您使用此方法了解 Cisco Jabber 检测哪些服务和功能可供用户使用的方式。搜索服务意味着客户端使用 DNS 服务 (SRV) 记录来确定哪些服务可供客户端使用。

客户端如何发现可用的服务

下图显示客户端用于连接到服务的流程。

图 *5:* 服务发现的登录流



要查找可用的服务，客户端会执行以下操作：

1. 检查网络是在防火墙内部还是外部，以及是否部署了 Expressway for Mobile and Remote Access。客户端将查询发送到名称服务器以获取 DNS 服务 (SRV) 记录。
2. 开始监控网络更改。

   在部署 Expressway for Mobile and Remote Access 时，客户端会监控网络，以确保它在网络从防火墙内部或外部发生更改时能够重新连接。
3. 发出几个 HTTPS 请求Cisco Webex 平台服务来确定 Jabber 是否进入组的留言传送模式。请求会检查用户的电子邮件地址，以了解用户是否已针对 Webex Control Hub 中的组消息启用。

4. 向 CAS URL 发出 Cisco Webex Messenger 服务的 HTTP 请求。

   此查询使得此客户端能够确定域是否为有效的 Cisco Webex 域。

   在部署 Expressway for Mobile and Remote Access 时，客户端连接到 Cisco Webex Messenger 服务并使用 Expressway for Mobile and Remote Access 连接到 Cisco Unified Communications Manager。当客户端首次启动时，用户将看到电话服务连接错误且必须在“客户端选项”屏幕中输入其凭证，后续启动将使用缓存的信息。

5. 查询名称服务器以获取DNS服务(SRV)记录，这些记录存在于上一个查询的缓存中的情况除外。

   此查询可让客户端执行以下操作：

   - 确定哪些服务可用。
   - 确定是否可以通过 Expressway for Mobileand Remote Access 连接到公司网络。

客户端发出 Cisco Webex Messenger 服务的 HTTP 查询

除了查询 SRV 记录的名称服务器以查找可用的服务外，Cisco Jabber 还将 HTTP 查询发送到 Cisco Webex Messenger 服务的 CAS URL。此请求使客户端能够确定基于云的部署并验证用户以使用Cisco Webex Messenger服务。

当客户端从用户处获取服务域时，它会将该域追加到以下 HTTP 查询：

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=
```

例如，如果客户端将 `example.com` 作为用户的服务域获取，则会发出以下查询：

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

该查询返回一个 XML 响应，客户端使用该响应确定服务域是否为有效的 Cisco Webex 域。

如果客户端确定服务域是有效的 Cisco Webex 域，它将提示用户输入其 Cisco Webex 凭证。然后，客户端对 Cisco Webex Messenger 服务进行验证，并检索在 Cisco Webex 组织管理中配置的配置和 UC 服务。

如果客户端确定服务域不是有效的 Cisco Webex 域，它将使用名称服务器的查询结果来查找可用的服务。

当客户端将 HTTP 请求发送到 CAS URL 时，它将使用配置的系统代理。

有关详细信息，请参阅《*Cisco Jabber* 部署和安装指南》中的“配置代理设置”部分。

客户端查询名称服务器

当客户端查询名称服务器时，它会将单独的同步请求发送到 SRV 记录的名称服务器。

客户端按以下顺序请求以下 SRV 记录：

- `_cisco-uds`
- `_collab-edge`

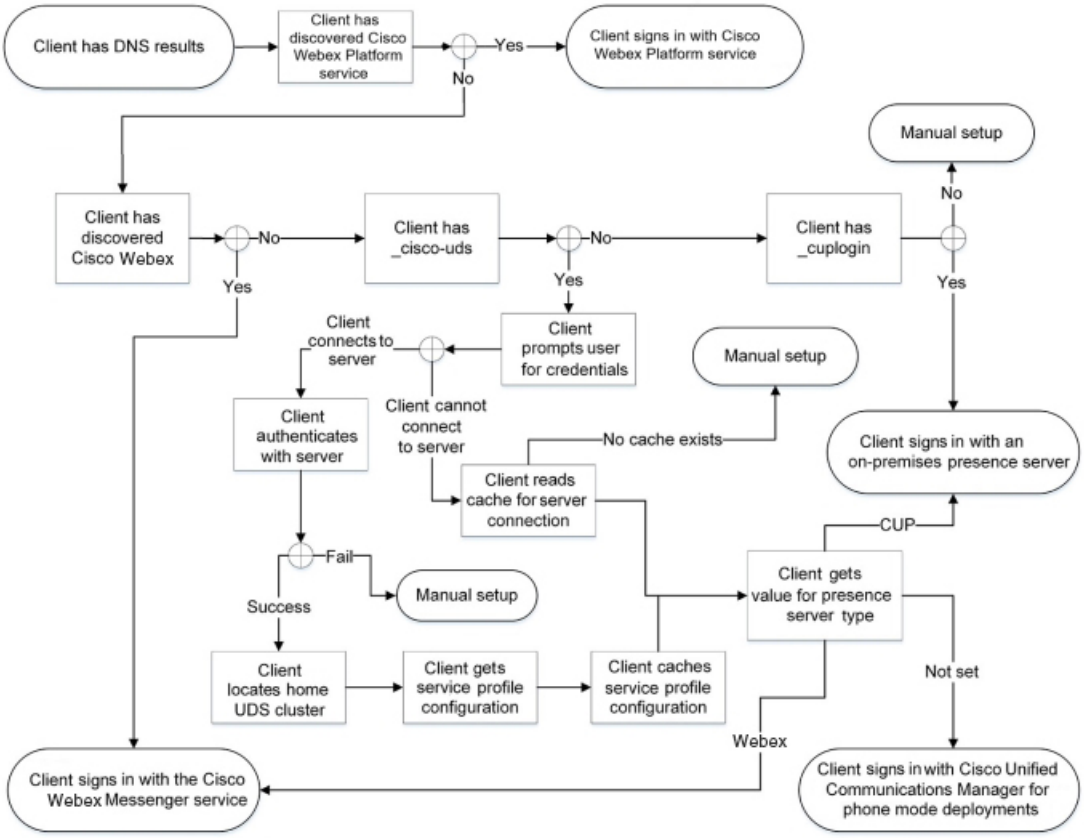
如果名称服务器返回：

- _cisco-uds — 客户端检测到其在公司网络内部并连接到 Cisco Unified Communications Manager。
- _collab-edge — 客户端通过 Expressway for Mobile and Remote Access 连接到内部网络并发现服务。
- 没有任何 SRV 记录 — 客户端提示用户手动输入设置和登录详细信息。

客户端连接到内部服务

下图显示客户端如何连接到内部服务：

图 *6:* 客户端连接到内部服务



连接到内部服务时，目标是确定身份验证器、让用户登录并连接到可用的服务。

在登录屏幕上，用户通过以下一项服务进行验证：

- Cisco Webex 平台服务— 云或混合部署。
- Cisco Webex Messenger 服务 — 云或混合部署。
- Cisco Unified Communications Manager—电话模式下的内部部署。

客户端连接到它发现的任何服务，具体视部署而异。

1. 如果客户端发现用户已针对组消息模式启用，则客户端会执行以下操作：
   1. 确定 Cisco Webex 平台服务 是身份验证的主要来源。
   2. 自动连接到 Cisco Webex 平台服务。
   3. 提示用户输入凭证。
2. 如果客户端发现 CAS URL 查找指示 Cisco Webex 用户，则客户端会执行以下操作：
   1. 确定 Cisco Webex Messenger 服务是身份验证的主要来源。
   2. 自动连接到 Cisco Webex Messenger 服务。
   3. 提示用户输入凭证。
   4. 检索客户端和服务配置。
3. 如果客户端发现 `_cisco-uds` SRV 记录，客户端将执行以下操作：

   提示用户输入凭证以使用 Cisco Unified Communications Manager 进行身份验证。
   1. 查找用户的主群集。

      查找主群集可让客户端自动获取用户的设备列表并向其注册 Cisco Unified Communications Manager。

      在具有多个 Cisco Unified Communications Manager 群集的环境中，配置群集间查询服务 (ILS)。ILS 使得客户端能够查找用户的主群集。

重要事项 请参阅相应版本的 *Cisco Unified Communications Manager* 功能和服务指南，了解如何配置 ILS。

   2. 检索服务配置文件。

      服务配置文件为客户端提供身份验证器以及客户端和 UC 服务配置。

      客户端从 IM and presence 配置文件中的“产品类型”字段的值确定身份验证器，如下所示：

      - Cisco Unified Communications Manager—Cisco Unified Presence 或 Cisco Unified Communications Manager IM and Presence Service 是身份验证器。
      - Webex (IM and Presence)Cisco Webex Messenger — 服务是身份验证器。

注释 在此版本中，除了 SRV 记录查询之外，客户端还会发出 HTTP 查询。HTTP 查询允许客户端确定是否应向 Cisco Webex Messenger 服务进行身份验证。

HTTP 查询的结果是，客户端在基于云的部署中连接到服务 Cisco Webex Messenger。如果客户端已经发现使用 CAS 查找的 Webex 服务，则将“**产品类型**”字段的值设置为 Webex 不会生效。

- 未设置 — 如果服务配置文件不包含 IM and Presence Service 配置，则身份验证器为 Cisco Unified Communications Manager。

3. 登录到身份验证器。

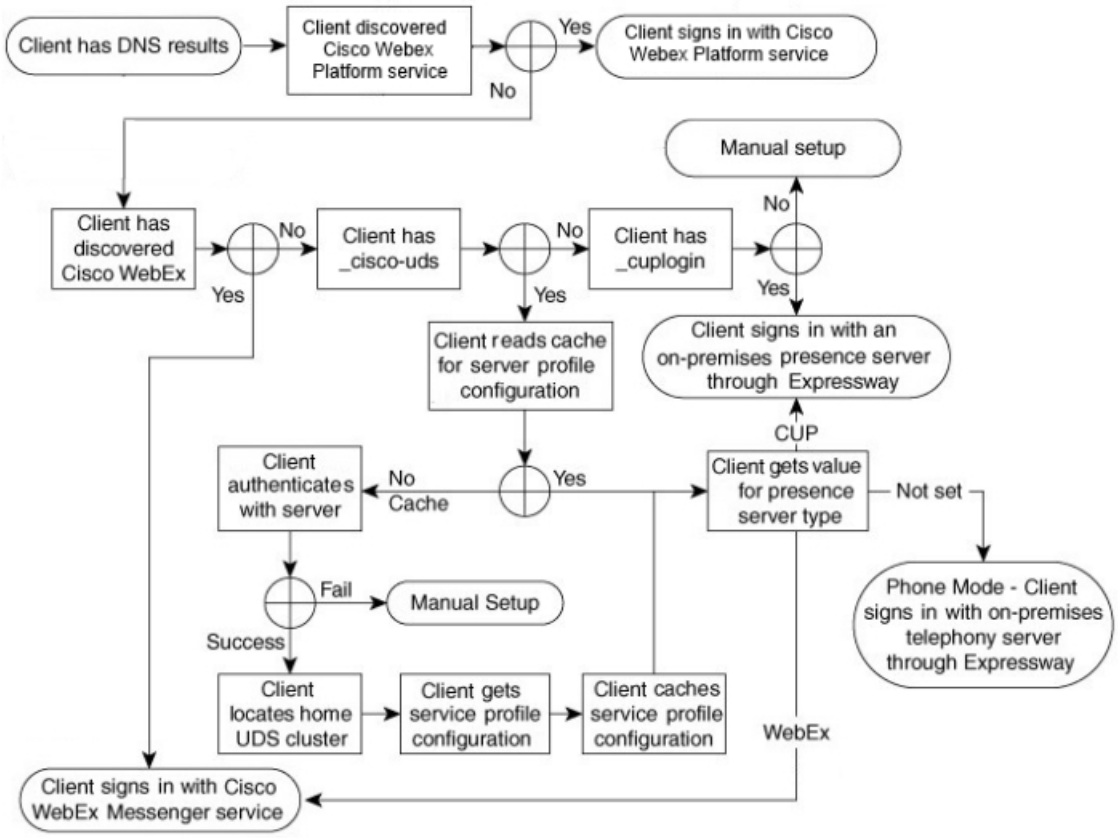
   在客户端登录后，它可以确定产品模式。

客户端通过 Expressway for Mobile and Remote Access 进行连接

如果名称服务器返回 `_collab-edge` SRV 记录，客户端会尝试通过 Expressway for Mobile and Remote Access 连接到内部服务器。

下图显示客户端通过 Expressway for Mobile and Remote Access 连接到网络时，客户端如何连接到内部服务：

图 *7:* 客户端通过 ***Expressway for Mobile and Remote Access*** 进行连接



当名称服务器返回 `_collab-edge` SRV 记录时，客户端将获取 Cisco Expressway-E 服务器的位置。然后，Cisco Expressway-E 服务器向客户端提供查询结果到内部名称服务器。

注释 Cisco Expressway-C 服务器查找内部 SRV 记录，并向 Cisco Expressway-E 服务器提供记录。

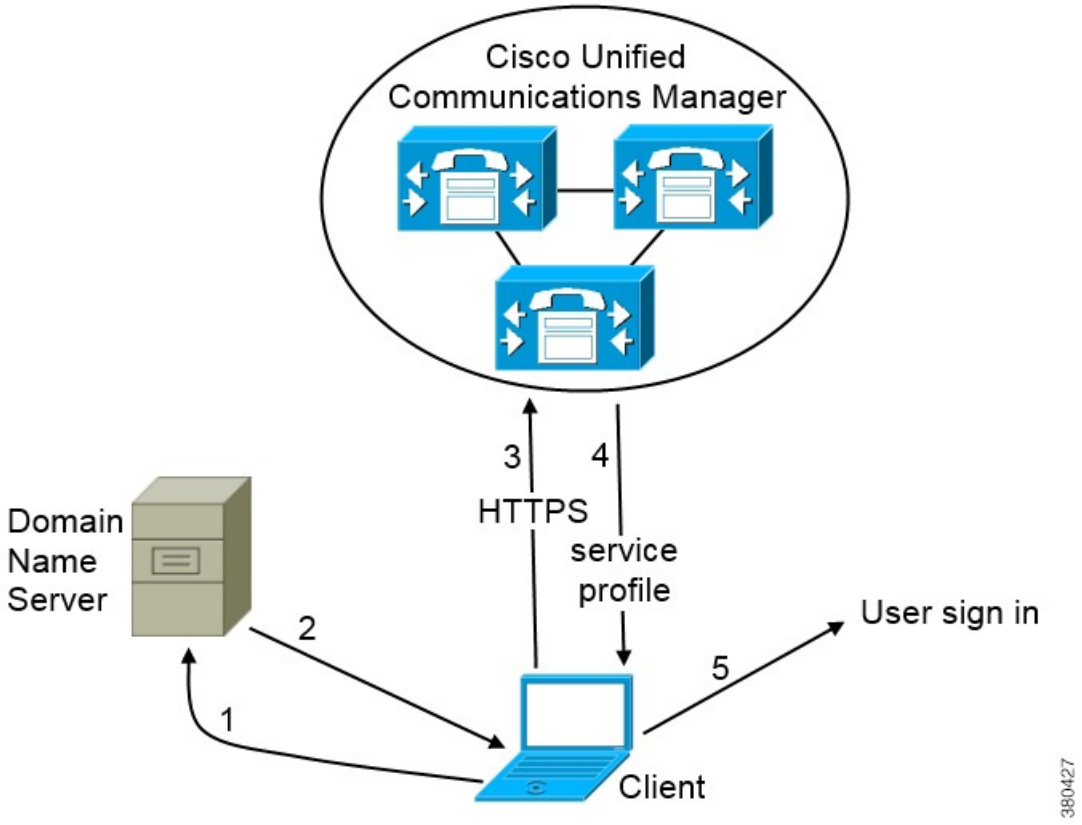
客户端获取内部 SRV 记录（必须包含 _cisco-uds SRV 记录）后，它将从 Cisco Unified Communications Manager 中检索服务配置文件。然后，服务配置文件为客户端提供用户的主群集、主要身份验证来源和配置。

Cisco UDS SRV 记录

在采用 Cisco Unified Communications Manager 版本 9 及更高版本的部署中，客户端可以使用 _cisco-uds SRV 记录自动发现服务和配置。

下图显示客户端如何使用 _cisco-uds SRV 记录。

图 *8: UDS SRV* 记录登录流



1. 客户端在域名服务器中查询 SRV 记录。
2. 域名服务器将返回 _cisco-uds SRV 记录。
3. 客户端查找用户的主群集。

   因此，客户端可以检索用户的设备配置并自动注册电话服务。

重要事项 在具有多个 Cisco Unified Communications Manager 群集的环境中，您可以配置群集间查询服务 (ILS)。ILS 使得客户端能够查找用户的主群集和发现服务。

如果不配置 ILS，则必须手动配置远程群集信息，类似于跨群集分机移动 (EMCC) 远程群集设置。有关详细的远程群集配置信息，请参阅《*Cisco Unified Communications Manager* 功能和服务指南》。

4. 客户端将检索用户的服务配置文件。

   用户的服务配置文件包含 UC 服务和客户端配置的地址和设置。

   客户端还可从服务配置文件确定身份验证器。

5. 客户端将该用户登录到身份验证器。

以下是 `_cisco-uds` SRV 记录的示例：

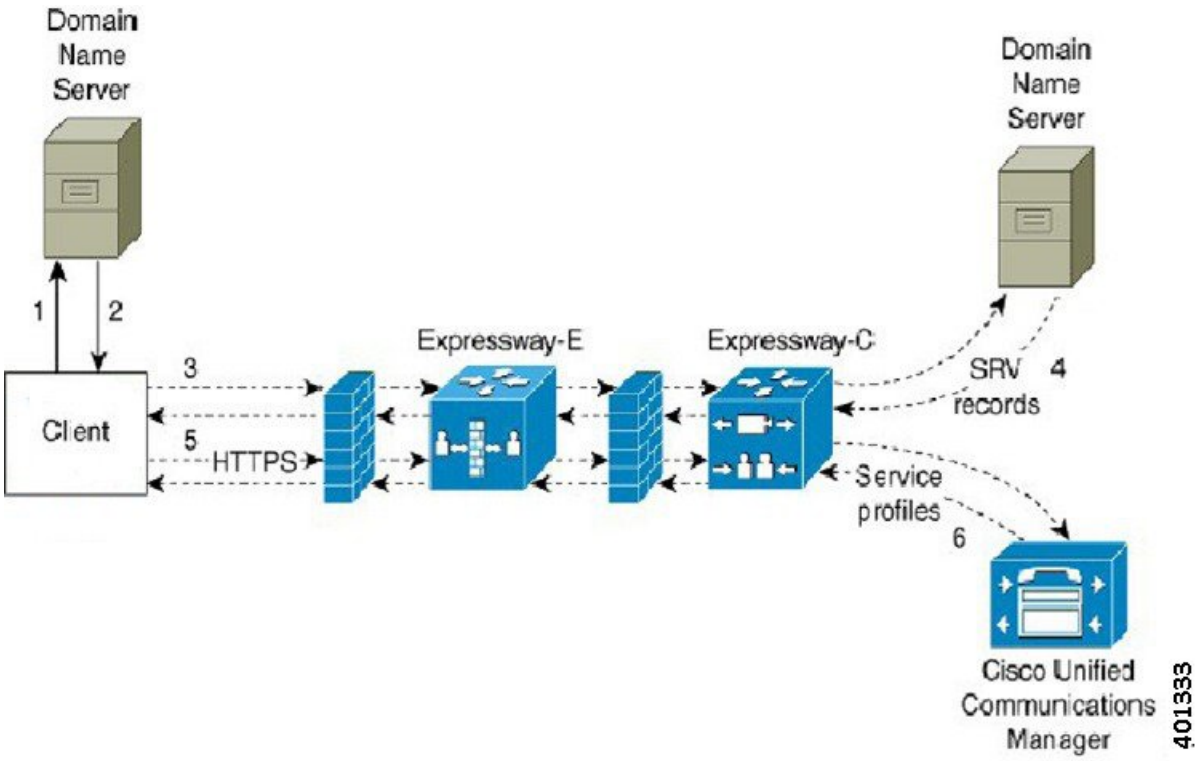
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.example.com
```

Collaboration Edge SRV 记录

Cisco Jabber 可以尝试通过 Expressway for Mobile and Remote Access 连接到内部服务器，以使用以下 `_collab-edge` SRV 记录来发现服务。

下图显示客户端如何使用 `_collab-edge` SRV 记录。

图 *9: Collaboration Edge* 记录登录流



1. 客户端在外部域名服务器中查询 SRV 记录。
2. 名称服务器返回 `_collab-edge` SRV 记录，但不返回 `_cuplogin` 或 `_cisco-uds` SRV 记录。

   因此，Cisco Jabber 可以找到 Cisco Expressway-E 服务器。
3. 客户端从内部域名服务器请求内部 SRV 记录（通过 Expressway）。

   这些 SRV 记录必须包含 `_cisco-uds` SRV 记录。
4. 客户端将获取内部 SRV 记录（通过 Expressway）。

   因此，客户端可以找到 Cisco Unified Communications Manager 服务器。
5. 客户端从 Cisco Unified Communications Manager 请求服务配置文件（通过 Expressway）。
6. 客户端从 Cisco Unified Communications Manager 取回服务配置文件（通过 Expressway）。

   服务配置文件包含用户的主群集、主要身份验证来源以及客户端配置。

DNS 配置

客户端如何使用 DNS

Cisco Jabber 使用域名服务器执行以下操作：

- 确定客户端在公司网络内部还是外部。
- 在公司网络内自动发现内部服务器。
- 在公共互联网上查找 Expressway for Mobile and Remote Access 的接入点。

注释 Android OS 限制：使用 DNS 服务的 Android OS 4.4.2 和 5.0 只能解析域名，但不能解析主机名。

有关详细信息，请参阅《Android 开发者链接》。

客户端查找名称服务器的方式

Cisco Jabber查找来自以下位置的 DNS 记录：

- 公司网络内部的内部名称服务器。
- 公共互联网上的外部名称服务器。

当客户端的主计算机或设备获取网络连接时，主计算机或设备也会从DHCP设置中获取DNS名称服务器的地址。该名称服务器可能在公司网络内部或外部，具体取决于网络连接。

Cisco Jabber 查询主计算机或设备从 DHCP 设置获取的名称服务器。

客户端获取服务域的方式

客户端以不同的方式发现服务域。

新安装：

- 用户在客户端用户界面中以 `username@example.com` 格式输入地址。
- 用户单击包含服务域的配置 URL。此选项仅在以下客户端版本中可用：
  - Cisco Jabber Android 版本 9.6 或更高版本
  - Cisco Jabber Mac 版本 9.6 或更高版本
  - Cisco Jabber iPhone 和 iPad 版本 9.6.1 或更高版本
- 客户端在引导程序文件中使用安装交换机。此选项仅在以下版本的客户端中可用：
  - Cisco Jabber Windows 版本 9.6 或更高版本

现有安装：

- 客户端使用缓存的配置。
- 用户在客户端用户界面中手动输入地址。

在混合部署中，通过中心验证服务 (CAS) 查找发现 Cisco Webex 域所需的域可能与部署 DNS 记录时的域不同。在这种情况下，您将 ServicesDomain 设置为用于发现 Cisco Webex 的域并将 VoiceServicesDomain 设置为部署 DNS 记录时的域。语音服务域的配置如下：

- 客户端在配置文件中使用 VoiceServicesDomain 参数。此选项在支持 `jabber-config.xml` 文件的客户端中可用。
- 用户单击包含 VoiceServicesDomain 的配置 URL。此选项在以下客户端中可用：
  - Cisco Jabber Android 版本 9.6 或更高版本
  - Cisco Jabber Mac 版本 9.6 或更高版本
  - Cisco Jabber iPhone 和 iPad 版本 9.6.1 或更高版本
- 客户端在引导程序文件中使用 Voice_Services_Domain 安装交换机。此选项仅在以下版本的客户端中可用：
  - Cisco Jabber Windows 版本 9.6 或更高版本

Cisco Jabber 获取服务域后，它将查询配置为客户端计算机或设备的名称服务器。

域名系统设计

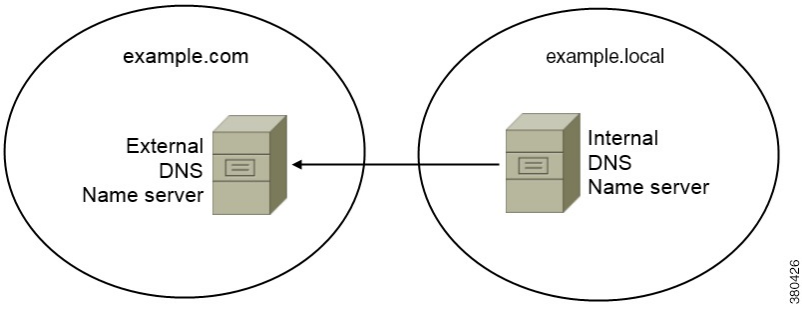
部署 DNS 服务 (SRV) 记录的位置取决于 DNS 命名空间的设计。通常有两种 DNS 设计：

- 在公司网络外部和内部的单独域名。
- 公司网络外部和内部的相同域名。

单独的域设计

下图所示为一个单独的域设计：

图 *10:* 单独的域设计



单独的域设计示例是，您的组织向 Internet 名称机构注册以下外部域：`example.com`。

您的公司还使用为以下各项之一的内部域：

- 外部域的子域，例如 example.local。
- 与外部域不同的域，例如 exampledomain.com。

单独的域设计具有以下特点：

- 内部名称服务器具有包含内部域资源记录的区域。内部名称服务器对内部域是权威的。
- 当 DNS 客户端查询外部域时，内部名称服务器将请求转发给外部名称服务器。
- 外部名称服务器具有包含您所在组织外部域资源记录的区域。外部名称服务器对该域是权威的。
- 外部名称服务器可以将请求转发给其他外部名称服务器。但是，外部名称服务器无法将请求转发给内部名称服务器。

在单独的域结构中部署 *SRV* 记录

在单独的名称设计中有两个域，即内部域和外部域。客户端在服务域中查询 SRV 记录。内部名称服务器必须提供服务域的记录。但是，在单独的名称设计中，服务域的区域可能不在内部名称服务器上存在。

如果内部名称服务器当前不提供服务域，您可以：

- 在服务域的内部区域内部署记录。
- 在内部名称服务器的“精确定位”子域区域内部署记录。

使用服务域的内部区域

如果您在内部名称服务器上没有服务域区域，则可以创建一个。此方法使内部名称服务器成为服务域的权威。由于它是权威的，因此内部名称服务器不会将查询转发给任何其他名称服务器。

此方法更改整个域的转发关系，并有可能中断内部DNS结构。如果您无法为服务域创建内部区域，则可以在内部名称服务器上创建一个精确定位的子域区域。

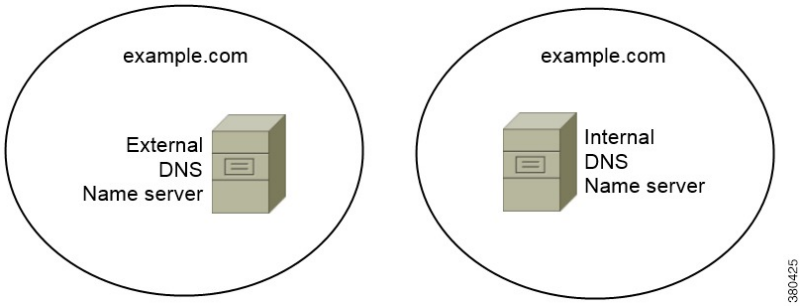
相同的域设计

相同的域设计示例是，您的组织向 Internet 名称机构将 example.com 注册为外部域。您的组织也使用 example.com 作为内部域的名称。

单个域，分区

下图所示为具有分区域设计的单个域。

图 *11:* 单个域，分区



两个 DNS 区域代表单个域；内部名称服务器中的一个 DNS 区域和外部名称服务器中的一个 DNS 区域。

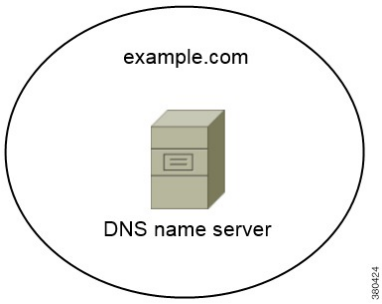
内部名称服务器和外部名称服务器对单个域是权威的，但提供不同的主机社区。

- 公司网络内部的主机只能访问内部名称服务器。
- 公共互联网上的主机只能访问外部名称服务器。
- 在公司网络与公共互联网之间移动的主机在不同的时间访问不同的名称服务器。

单个域，不是分区

下图所示为不具有分区域设计的单个域。

图 *12:* 单个域，不是分区



在单个域中，非分区设计、内部和外部主机通过一组名称服务器提供服务，并且可以访问相同的 DNS 信息。

重要事项 此设计不常见，因为它会向潜在的攻击者公开有关内部网络的详细信息。

方法 2：自定义

您可以使用安装参数、URL 配置或企业移动性管理自定义服务发现。

服务发现自定义

Cisco Jabber Windows 版本的自定义安装

Cisco Jabber Windows 版本提供可通过以下方式使用的 MSI 安装软件包：

- 使用命令行 — 您可以在命令行窗口中指定参数以设置安装属性。

  如果您计划安装多个实例，请选择此选项。

- 手动运行 MSI — 在客户端工作站的文件系统上手动运行 MSI，然后在您启动客户端时指定连接属性。

  如果您计划安装单个实例以进行测试或用于评估目的，请选择此选项。

- 创建自定义安装程序 — 打开默认安装软件包，指定所需的安装属性，然后保存自定义安装软件包。

  如果您计划分发具有相同安装属性的安装软件包，请选择此选项。

- 采用组策略进行部署 — 在同一域中的多个计算机上安装客户端。

安装程序切换到

在尚未部署服务发现的情况下，以及您不希望用户手动指定其连接设置的情况下，引导程序文件提供服务发现回退机制。

客户端仅读取初始启动上的引导程序文件。初始启动后，客户端将缓存服务器地址和配置，然后在后续启动时从缓存加载。

我们建议您不要使用引导程序文件，而是使用您的 Webex 中的呼叫 (Unified CM) 部署的服务发现。

Cisco Jabber Mac、iPhone、iPad 和 Android 版本的自定义安装

您可以使用 URL 配置创建 Cisco Jabber Mac 版本或移动客户端的自定义安装。对于移动客户端，您还可以使用企业移动性管理。这些自定义安装取决于启用服务的安装参数。

URL 配置

要让用户在无需手动输入服务发现信息的情况下启动 Cisco Jabber，请向用户提供一个配置 URL 链接以安装客户端。

直接通过电子邮件或在网站上发布链接来向用户提供配置 URL 链接。

使用企业移动性管理的移动配置

您可以在 Cisco Jabber Android 版本和 Cisco Jabber iPhone 和 iPad 版本上使用企业移动性管理 (EMM) 配置 Cisco Jabber。有关设置 EMM 的详细信息，请参阅 EMM 提供商提供的管理员的说明。

如果想要 Jabber 仅在受管理设备上运行，则可以部署基于证书的身份验证，然后通过 EMM 注册客户端证书。

有关如何部署 EMM 的详细信息，请参阅《*Cisco Jabber* 的内部部署》》或《*Cisco Jabber* 的云部署和混合部署》中有关部署 *Cisco Jabber* 应用程序的部分。

方法 3：手动安装

作为高级选项，用户可以在登录屏幕上手动连接到服务。

高可用性

即时消息和在网状态的高可用性

高可用性是指在子群集中存在多个节点的环境，为即时消息和在网状态服务提供故障转移功能。如果子群集中的一个节点不可用，该节点的即时消息和在网状态服务会将故障转移到子群集中的另一个节点。这样，高可用性可确保 Cisco Jabber 的即时消息和在线状态服务的可靠连续性。

为 LDAP 支持高可用性。使用 UDS 联系人来源时，不支持高可用性。

Cisco Jabber 通过以下服务器支持高可用性：

Cisco Unified Communications Manager IM and Presence Service 版本 9.0 和更高版本

请使用以下 Cisco Unified Communications Manager IM and Presence Service 文档获取有关高可用性的详细信息。

Cisco Unified Communications Manager 上 IM and Presence Service 的配置和管理

高可用性客户端登录配置文件

高可用性故障诊断

故障转移期间保留的活动呼叫

如果从 Cisco Unified Communications Manager 的主实例到辅助实例发生故障转移，则不能保留活动呼叫。

客户端中的高可用性

故障转移期间的客户端行为

如果在服务器上配置了高可用性，则在主服务器故障转移到辅助服务器后，客户端将暂时离线长达一分钟。配置重新登录参数以定义客户端在尝试重新登录到服务器之前等待的时间。

配置登录参数

Cisco Unified Communications Manager IM and Presence Service 可让您配置在尝试重新登录到服务器之前，Cisco Jabber 等待的最长和最短秒数。在服务器上，您可以在以下字段中指定重新登录参数：

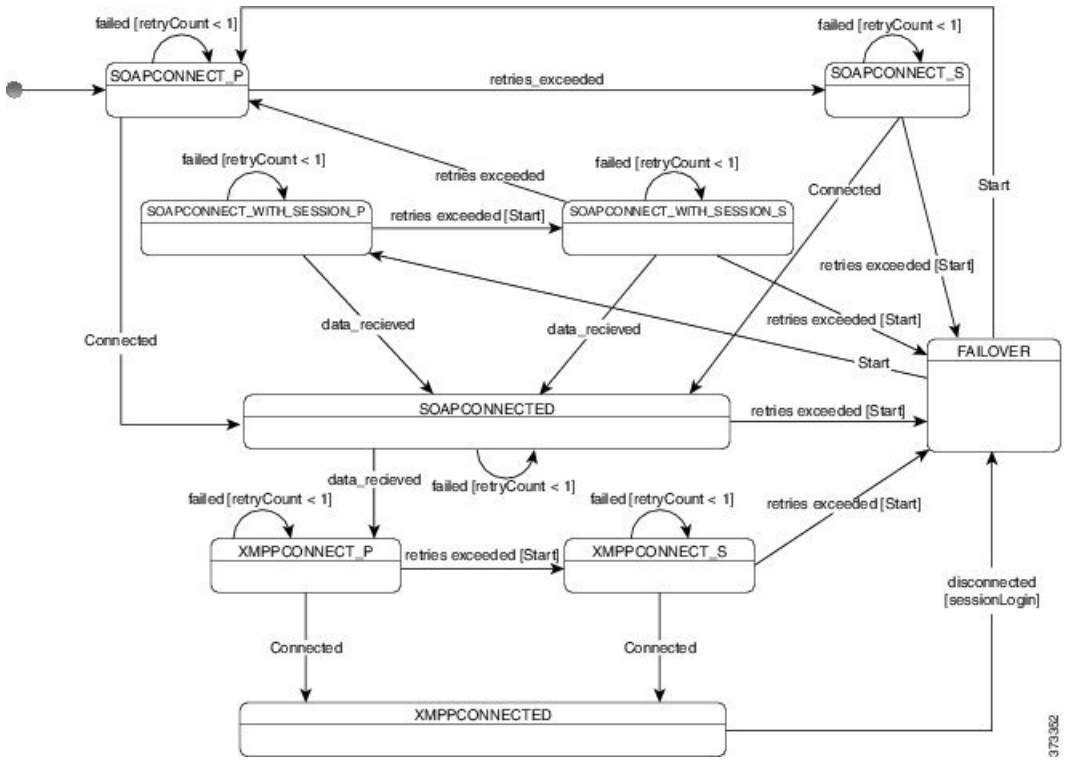
- 客户端重新登录下限

- 客户端重新登录上限

故障转移期间的客户端行为

下图显示了 Cisco Unified Communications Manager IM and Presence Service 在故障转移期间时客户端的行为。

图 *13:* 故障转移期间的客户端行为



1. 客户端从其活动服务器断开后，客户端将从 XMPPCONNECTED 状态变为故障转移状态。
2. 在故障转移状态下，客户端尝试通过尝试 SOAPCONNECT_SESSION_P（作为主服务器）来获得 SOAPCONNECTED 状态，如果失败，则尝试 SOAPCONNECT_SESSION_S（作为辅助服务器）。
   - 如果无法获得 SOAPCONNECT_SESSION_P 或 SOAPCONNECT_SESSION_S，客户端将重新进入故障转移状态。
   - 在故障转移状态下，客户端会尝试获得 SOAPCONNECT_P 状态，如果失败，则会尝试达到 SOAPCONNECT_S 状态。
   - 如果客户端无法达到 SOAPCONNECT_P 或 SOAPCONNECT_S 状态，则在用户发起登录尝试之前，客户端不再尝试自动连接到 IM&P 服务器。
3. 在 SOAPCONNECT_SESSION_P、SOAPCONNECT_SESSION_S、SOAPCONNECT_P 或 SOAPCONNECT_S 状态下，客户端会检索其当前的主辅助 XMPP 服务器地址。在故障转移期间，此地址会发生变化。

4. 在 SOAPCONNECTED 状态下，客户端尝试通过尝试连接到 XMPPCONNECT_P 状态来达到 XMPPCONNECTED 状态，如果失败，将尝试 XMPPCONNECT_S 状态。
   - 如果客户端无法达到 XMPPCONNECT_P 或 XMPPCONNECT_S 状态，则在用户发起登录尝试之前，客户端不再尝试自动连接到 IM&P 服务器。
5. 在客户端处于 XMPPCONNECTED 状态后，客户端将具有 IM&P 功能。

语音和视频的高可用性

如果子群集中的一个节点不可用，语音和视频会将故障转移到子群集中的另一个节点。

默认情况下，软终端设备或桌面电话需要长达 120 秒的时间来向另一个节点完成注册。如果此超时时段太长，请调整您的节点的“SIP 站保持连接间隔”服务参数的值。“SIP 站保持连接间隔”服务参数将修改 Cisco Unified Communications Manager 上的所有电话设备。在调整间隔之前，请分析对 Cisco Unified Communications Manager 服务器的影响。

要为节点配置服务参数，请在 Cisco Unified Communications Manager 管理中选择**系统** > **服务参数**。

对于使用非 DNS SRV 记录方法的电话模式部署，无法对语音和视频进行故障转移，因为只指定了一个 Cisco Unified Communications Manager 节点。

永久聊天的高可用性

支持永久聊天的高可用性。故障转移窗口期间，用户可能会收到无法发送消息的提示。当节点发生故障转移时，用户将自动重新加入聊天室，并可再次发送消息。

联系人搜索和联系人解析的高可用性

支持联系人搜索和联系人解析的高可用性，这两者由 Cisco Unified Communications Manager 用户数据服务 (UDS) 提供。如果主要 UDS 服务器不可用，Jabber 会自动将故障转移到第二个 UDS 服务器或第三个 UDS 服务器（如果已配置）。

语音邮件的高可用性

如果配置了辅助语音邮件服务器，则客户端会在主服务器变为不可用或无法接通时自动故障转移到辅助语音邮件服务器。

SRST

适用于 Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本

当 Cisco Unified Communications Manager 应用程序无法访问或 WAN 关闭时，请使用 Cisco Unified Survivable Remote Site Telephony (SRST) 为您的远程用户保留基本电话服务。当连接中断时，客户端将故障转移到远程站点的本地路由器。

注释 支持 SRST 12.8 及更高版本。

当系统处于故障转移状态且仅启动、结束、保留、恢复、静音、取消静音以及双音多频信令 [DTMF] 启用时，SRST 提供基本呼叫控制。

故障转移期间无法使用以下服务：

- 视频
- 通话切换功能（转接、转移、呼叫保留、会议、发送到手机）
- Dial via Office (DVO)
- 临时会议
- 二进制层控制协议 (BFCP) 共享

有关配置 SRST 的详细说明，请参阅《*Cisco Unified Communications Manager* 管理指南》的相关版本。

配置优先级

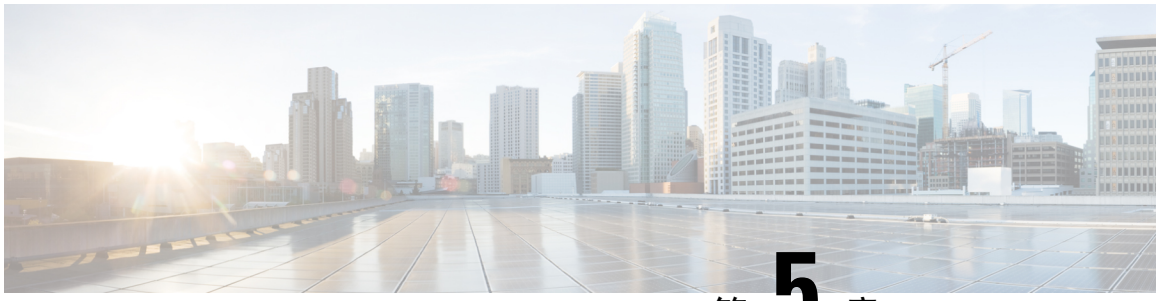
下表中列出了当服务配置文件和配置文件都存在时将优先考虑的参数值。

服务配置文件	配置文件	哪个参数值优先？
参数值已设置	参数值已设置	服务配置文件
参数值已设置	参数值为空白	服务配置文件
参数值为空白	参数值已设置	配置文件
参数值为空白	参数值为空白	服务配置文件空白（默认）值

使用思科支持字段的组配置

组配置文件适用于一组用户。如果您为用户提供 CSF 设备，请在设备配置的 **Cisco 支持字段**字段中指定组配置文件名。如果用户没有 CSF 设备，请在安装期间使用 TFTP_FILE_NAME 参数为每个组设置唯一的配置文件名。

COP 文件版本低于 14122 的 TCT 和 BOT 支持组配置。



第 5 章

联系人来源

什么是联系人来源？

联系人来源是一个用户数据集合。用户搜索联系人或在 Cisco Jabber 客户端中添加联系人时，会从联系人来源读取联系信息。

Cisco Jabber 从联系人来源检索信息以填充联系人列表、更新客户端中的联系人名片以及显示联系信息的其他区域。当客户端收到任何传入通信（例如，即时消息或语音/视频呼叫）时，将使用联系人来源来解析联系信息。

联系人来源服务器

注释 所有 Jabber 客户端都支持用于目录集成的 LDAPv3 标准。支持此标准的任何目录服务器都与这些客户端兼容。

您可以将以下联系人源服务器与 Cisco Jabber 配合使用：

- Active Directory Domain Services，Windows Server 2012 R2
- Active Directory Domain Services，Windows Server 2008 R2
- Cisco Unified Communications Manager用户数据服务器 (UDS)。Cisco Jabber 支持使用 Cisco Unified Communications Manager 10.5 或更高版本的 UDS。
- OpenLDAP
- Active Directory 轻量级目录服务 (AD LDS) 或 Active Directory 应用程序模式 (ADAM)

我为什么需要联系人来源？

Cisco Jabber 通过以下方式使用联系人来源：

- 用户搜索联系人—客户端将使用输入的信息并搜索联系人来源。从联系人来源检索信息后，客户端将显示可用的方法以与联系人进行交互。
- 客户端接收来电通知—客户端将获取来自传入通知的信息并从联系人来源解析 URI、号码和包含联系人的 JabberID。客户端将在警报中显示联系人详细信息。

配置联系人来源服务器的时间

注释 在注册到 Active Directory 域的工作站上安装 Cisco Jabber。在此环境中，无需配置 Cisco Jabber 以连接到目录。客户端会自动发现目录并连接到该域中的全局目录服务器。

如果计划使用以下服务之一作为联系人来源，则配置 Cisco Jabber 以连接到目录服务：

- Active Directory 服务
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight 目录服务
- Active Directory 应用程序模式

您可以选择将目录集成配置为：

- 更改默认属性映射。
- 调整目录查询设置。
- 指定客户端如何检索联系人照片。

- 执行域内联合。

Cisco 目录集成 的联系人来源选项

在内部部署中，客户端需要以下联系人来源之一来解析用户信息的目录查找：

- Lightweight 目录访问协议 (LDAP)— 如果您有公司目录，您可以使用以下基于 LDAP 的联系人来源选项将您的目录配置为联系人来源：
  - Cisco 目录集成 (CDI)— 使用此联系人来源选项部署所有客户端。
- Cisco Unified Communications Manager 用户数据服务 (UDS) — 如果没有公司目录或者您的部署包括与 Expressway Mobile and Remote Access 连接的用户，则可以使用此选项。

轻型目录访问协议

Cisco 目录集成如何与 LDAP 配合使用

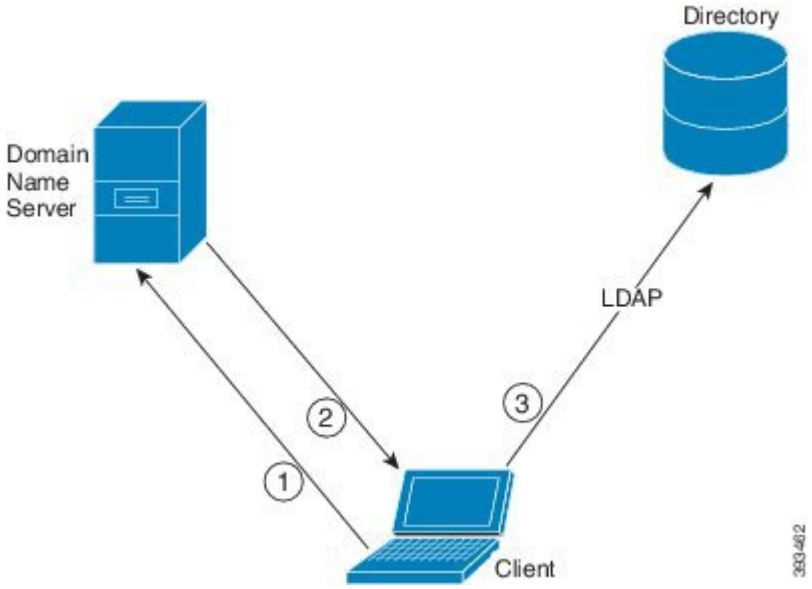
CDI 使用服务发现来确定 LDAP 服务器。

下面是具有 CDI 的内部部署的默认设置：

- Cisco Jabber 与 Active Directory 集成为联系人来源。
- Cisco Jabber 会自动发现并连接到全局目录。

自动服务发现 — 建议

我们建议您使用服务发现，以通过全局目录 (GC) 服务器或 LDAP 服务器自动进行连接和身份验证。如果要自定义您的部署，请查看用于提供 LDAP 服务器信息的选项和可用的验证选项。Jabber 先将 DNS 查询发送到 GC 域以发现 GC 服务器。如果它没有发现 GC 服务器，Jabber 然后将 DNS 查询发送到 LDAP 域以发现 LDAP 服务器。



如果有 GC 可用，客户端会执行以下操作：

1. 从工作站获取 DNS 域，并查找 GC 的 SRV 记录。
2. 从 SRV 记录中检索 GC 的地址。
3. 使用已登录用户的凭证连接到 GC。

使用全局目录域的发现

Jabber 尝试使用 DNS SRV 查询发现 GC 服务器。首先，Jabber 获取 GC 域：

1. 如果可用，Jabber 将 DNSFORESTNAME 环境变量用作 GC 域。
2. 如果 DNSFORESTNAME 不可用，Jabber 将检查 GC 域的以下各项：
   - 在 Windows 上，Jabber 将呼叫 Windows `DsGetDcName API` 以获取 `DnsForestName`。
   - 在非 Windows 平台上，Jabber 从 `jabber-config.xml` 读取 LdapDNSForestDomain。

Jabber 获取 GC 域后，它将发送 DNS SRV 查询以获取 GC 服务器地址：

- 在 Windows 上，Jabber 通过 Windows `DsGetSiteName` API 检查 `SiteName` 是否可用：
  - 如果 `SiteName` 存在，Jabber 会发出 DNS SRV 查询 `_gc._tcp.SiteName._sites.GCDomain`，以获取 GC 服务器地址。
  - 如果 `SiteName` 不存在或没有返回针对 `_gc._tcp.SiteName._sites.GCDomain` 的 SRV 记录，Jabber 将发出 DNS SRV 查询 `_gc._tcp.GCDomain`，以获取 GC 服务器地址。
- 在非 Windows 平台上，Jabber 会发出 DNS SRV 查询 `_gc._tcp.GCDomain`，以获取 GC 服务器地址。

使用 LDAP 域的发现

如果 Jabber 无法发现 GC 服务器，它将尝试发现 LDAP 域：

1. 如果可用，Jabber 将 USERDNSDOMAIN 环境变量用作 LDAP 域。
2. 如果 USERDNSDOMAIN 不可用，Jabber 将从 `jabber-config.xml` 读取 LdapUserDomain 。
3. 如果 LdapUserDomain 不可用，Jabber 将使用用户作为 LDAP 域登录的电子邮件域。

Jabber 获取 LDAP 域后，它将发送 DNS SRV 查询以获取 LDAP 服务器地址：

- 在 Windows 上，Jabber 通过 Windows `DsGetSiteName` API 检查 `SiteName` 是否可用。
  - 如果 `SiteName` 存在，Jabber 会发出 DNS SRV 查询 `_ldap._tcp.SiteName.sites.LdapDomain`，以获取 LDAP 服务器地址。
  - 如果 `SiteName` 不存在或没有返回针对 `_ldap._tcp.SiteName.sites.LdapDomain` 的 SRV 记录，Jabber 将发出 DNS SRV 查询 `_ldap._tcp.LdapDomain`，以获取 LDAP 服务器地址。
- 在非 Windows 平台上，Jabber 会发出 DNS SRV 查询 `_ldap._tcp.LdapDomain`，以获取 LDAP 服务器地址。

一旦 Jabber 连接到 LDAP 服务器，它将读取 LDAP 服务器的指定要使用的验证机制列表和顺序的 `SupportedSaslMechanisms` 属性。

LDAP 服务的手动配置

LDAP 服务的手动配置

1. 您可以配置 PrimaryServerName 参数以定义 Jabber 要连接到的特定 LDAP 服务器。
2. 您可以在 `jabber-config.xml` 文件中配置 LdapSupportedMechanisms 参数，以覆盖 supportedSaslMechanisms 属性中的列表。

   联系人服务和 LDAP 服务器必须支持所有这些机制。使用空格分隔多个值。

   - GSSAPI — Kerberos v5
   - EXTERNAL — SASL external
   - PLAIN（默认）— 简单 LDAP 绑定，匿名是简单绑定的子集。

   示例：

   ```
   <LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</LdapSupportedMechanisms>
   ```

3. 如有必要，配置 LdapUserDomain 参数以设置 Jabber 用于通过 LDAP 服务器进行验证的域。例如：

   ```
   CUCMUsername@LdapUserDomain
   ```

LDAP 考虑因素

Cisco 目录集成 (CDI) 取代基本目录集成 (BDI) 和增强型目录集成 (EDI) 参数。CDI 参数适用于所有客户端。

Cisco Jabber 部署方案

方案 1：如果您不熟悉 11.8 中的 Jabber

我们建议您使用服务发现，以通过LDAP服务器自动进行连接和身份验证。如果要自定义您的部署，请查看用于提供 LDAP 服务器信息的选项和可用的验证选项。

方案 2：如果您从 EDI 配置升级到 11.8

如果您的配置只使用 EDI 参数，则 Jabber 将读取 EDI 参数并将其用于您的目录来源集成。我们仍建议您升级 EDI 参数，并将其替换为等效的 CDI 参数。

方案 3：如果您从 BDI 配置升级到 11.8

如果您的配置只使用 BDI 参数，则必须将 BDI 参数更新为等效的 CDI 参数。例如，对于 BDIPrimaryServerName，您需要将参数替换为 PrimaryServerName。BDIEnableTLS 被替换为 UseSSL 参数。

方案 4：如果您从混合 EDI/BDI 配置升级到 11.8

如果您的配置同时使用 EDI 和 BDI，则必须检查 BDI 的配置，因为 Jabber 在连接到 LDAP 服务器时将使用 EDI 参数。

目录参数

下表列出了 BDI 和 EDI 参数，指明 CDI 参数名称或者其是否适用于 Jabber 11.8 或更高版本。

BDI 参数	EDI 参数	CDI 参数
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername

BDI 参数	EDI 参数	CDI 参数
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL
-	UseSecureConnection	-
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards
-	MinimumCharacterQuery	MinimumCharacterQuery
BDISearchBase1	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5
BDIGroupSearchBase1	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	UseSipUriToResolveContacts
BDIUriPrefix	UriPrefix	UriPrefix
BDISipUri	SipUri	SipUri
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms

BDI 参数	EDI 参数	CDI 参数
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName
BDIFirstname	Firstname	Firstname
BDILastname	Lastname	Lastname
BDIEmailAddress	EmailAddress	EmailAddress
BDISipUri	SipUri	SipUri
BDIPhotoSource	PhotoSource	PhotoSource
BDIBusinessPhone	BusinessPhone	BusinessPhone
BDIMobilePhone	MobilePhone	MobilePhone
BDIHomePhone	HomePhone	HomePhone
BDIOtherPhone	OtherPhone	OtherPhone
BDIDirectoryUri	DirectoryUri	DirectoryUri
BDITitle	Title	Title
BDICompanyName	CompanyName	CompanyName
BDIUserAccountName	UserAccountName	UserAccountName
BDIDomainName	DomainName	DomainName
BDICountry	Country	Country
BDILocation	Location	Location
BDINickname	Nickname	Nickname
BDIPostalCode	PostalCode	PostalCode
BDICity	City	City
BDIState	State	State
BDIStreetAddress	StreetAddress	StreetAddress

Cisco Unified Communications Manager User Data Service

用户数据服务 (UDS) 是提供联系人解析的 Cisco Unified Communications Manager 上的 REST 接口。

在以下情况下，UDS 用于进行联系人解析：

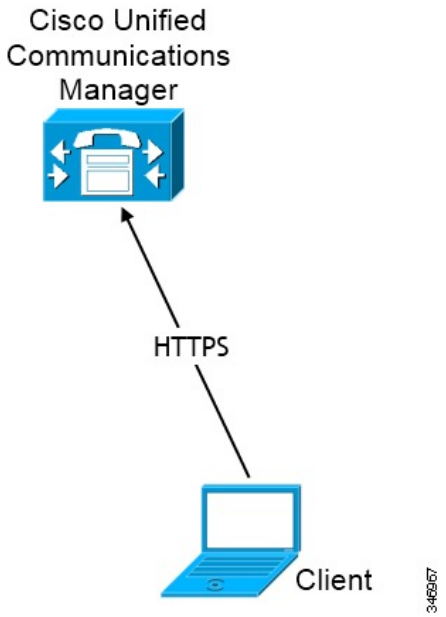
- 如果设置 DirectoryServerType 参数以使用客户端配置文件中的 UDS 值。

使用此配置时，客户端在公司防火墙内部或外部均使用 UDS 进行联系人解析。

- 如果您部署 Expressway for Remote and Mobile Access。

  使用此配置时，客户端在公司防火墙外部自动使用 UDS 进行联系人解析。

您将联系人数据与目录服务器中的 Cisco Unified Communications Manager 同步。Cisco Jabber 然后自动从 UDS 检索该联系人数据。



多个群集的联系人解析

对于有多个 Cisco Unified Communications Manager 群集的联系人解析，将公司目录中的所有用户同步到每个群集。提供适当群集中的那些用户子集。

例如，您的组织有 40,000 个用户。20,000 个用户居住在北美。20,000 个用户居住在欧洲。您所在组织的每个位置都具有以下 Cisco Unified Communications Manager 群集：

- `cucm-cluster-na`（北美）
- `cucm-cluster-eu`（欧洲）

在此示例中，将所有 40,000 个用户同步到两个群集。在 `cucm-cluster-na` 中提供北美的 20,000 个用户，在 `cucm-cluster-eu` 提供欧洲的 20,000 个用户。

当欧洲用户呼叫北美用户时，Cisco Jabber 会从 `cucm-cluster-na` 中检索欧洲用户的详细联系信息。

当北美用户呼叫欧洲用户时，Cisco Jabber 会从 `cucm-cluster-eu` 中检索北美用户的详细联系信息。

扩展的 UDS 联系人来源

将联系人搜索从 UDS 扩展到您的 LDAP 服务器。在 Cisco Unified Communications Manager 11.5 (1) 或更高版本中，您可以配置 Jabber 是否搜索您的 LDAP 服务器。

LDAP 先决条件

Cisco Jabber 使用不同的属性搜索联系人来源，默认情况下，并非对所有这些属性都进行索引。为确保有效搜索，必须对 Cisco Jabber 使用的属性进行索引。

如果您使用默认的属性映射，请确保在 LDAP 服务器上索引以下属性：

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

LDAP 服务帐户

在 Unified Communications Manager 12.5(1) SU2 版中，Unified CM 添加了对在服务配置文件中安全传递加密的 LDAP 凭证的支持。此更新通过确保始终以加密格式存储和发送密码来保护对目录的访问。此更改包括在以下过程中的加密：

- 目录访问验证
- 客户端配置文件下载
- BAT 导入/导出
- 升级

有关详细信息，请参阅《*Cisco Unified Communications Manager* 和 *IM and Presence Service 12.5(1) SU2* 版发行说明》。

在搭配此 Unified CM 发行版或更高版本的 Jabber 12.8 中，我们会在最终用户验证后将 LDAP 凭证下载为用户配置文件的一部分，以充分利用这一功能。

要将 Jabber 连接到 LDAP 服务器，需定义 LDAP 验证 Jabber 用户的方式：

- 默认选项是 Jabber 使用 Kerberos 或客户端证书 (SASL External) 自动连接到联系人来源服务器。我们建议使用此选项，因为它是最安全的。
- 如果您在服务配置文件或 `jabber-config.xml` 文件中定义凭证，它们始终优先于默认选项。
- 如果您为 LdapSupportedMechanisms 参数配置 PLAIN 值，但未配置目录配置文件用户名或密码，则用户可以直接在客户端中输入其目录凭证。
- 否则，如果连接到服务配置文件中的安全端口，可以定义 Jabber 如何连接到联系人来源服务器。您还可以通过以下方式定义：在 `jabber-config.xml` 文件的 LDAP_UseCredentialsFrom 参数中指定 Cisco Unified Communications Manager 凭证。
- 如果上述选项不可用，则使用服务配置文件或 `jabber-config.xml` 文件提供的一组众所周知的凭证。该选项的安全系数最低。Jabber 使用帐户通过联系人来源服务器进行验证。我们建议此帐户对目录拥有只读访问权限，并且是通常已知的公共凭证集。在此情况下，所有 Jabber 用户都使用这些凭证进行搜索。

注释 自 Cisco Unified Communications Manager 12.0 版本起，您无法在服务配置文件中配置用户名和密码。Jabber 用户将获得自行进行验证以使用目录服务的选项。用户第一次登录到 Jabber 时会收到通知。如果用户第一次没有自行进行验证，则当他们尝试访问联系人列表时，他们会收到警报。

Jabber ID 属性映射

用户 ID 的 LDAP 属性为 sAMAccountName。这是默认属性。

如果用户 ID 的属性不是 sAMAccountName，并且您在 Cisco Unified Communications Manager IM and Presence Service 中使用默认的 IM 地址方案，则必须将该属性指定为客户端配置文件中的参数值，如下所示：

CDI 参数为 UserAccountName。<UserAccountName>attribute-name</UserAccountName>

如果未在配置中指定该属性，且该属性不是 sAMAccountName，则客户端将无法解析目录中的联系人。结果，用户不会获取在网状态，并且不能发送或接收即时消息。

搜索 Jabber Id

Cisco Jabber 使用 Jabber ID 搜索目录中的联系人信息。有几个选项可用于优化目录中的搜索：

- **搜索库**—默认情况下，客户端在目录树的根目录处开始搜索。您可以使用搜索库指定不同的搜索开始，或者将搜索限制为特定的组。例如，只能您的用户子集具有即时消息功能。包括 OU 中的那些用户，然后将这指定为搜索库。
- **基本过滤器** — 在查询目录时，仅指定目录子项名称，以检索除用户对象以外的对象。
- **预测性搜索过滤器** — 您可以定义多个用逗号分隔的值以过滤搜索查询。默认值为 ANR（不明确的名称解析。）

有关这些选项的详细信息，请参阅《*Cisco Jabber* 的参数参考指南》中有关目录集成的章节。

本地联系人来源

Cisco Jabber 能够访问和搜索本地联系人来源。这些本地联系人来源包括以下各项：

- Microsoft Outlook 中存储的本地联系人可通过 Cisco Jabber Windows 版本访问。
- 存储在 IBM Notes 中的本地联系人可通过 Cisco Jabber Windows 版本（版本 11.1）访问。
- 本地通讯簿联系人可通过 Cisco Jabber Mac 版本、Cisco Jabber Android 版本和 Cisco Jabber iPhone 和 iPad 版本访问。

自定义联系人来源

所有客户端的 Cisco Jabber 让用户能够将自定义联系人导入到其客户端。

联系人缓存

Cisco Jabber 会创建本地缓存。此外，缓存也存储用户的联系人列表。当用户在其联系人列表中搜索某个人时，Jabber 会在开始目录搜索之前搜索本地缓存中的匹配项。

如果用户搜索的某个人不在其联系人列表中，Jabber 先搜索本地缓存，然后搜索公司目录。如果用户随后开始聊天或与此联系人通话，Jabber 会将该联系人添加到本地缓存中。

本地缓存信息将在 24 小时后过期。

解析重复的联系人

Jabber 中的联系人可来自多种不同的来源。Jabber 可以在多个联系人来源中找到同一个联系人的匹配项。在此情况下，Jabber 会确定哪些记录与同一个人匹配，并将该人员的所有数据组合在一起。要确定其中一个联系人来源中的记录是否与联系人相匹配，Jabber 会按以下顺序查找这些字段：

1. **Jabber ID (JID)** — 如果记录包含 JID，Jabber 将基于此匹配记录。Jabber 不会根据“邮件”或“电话号码”字段作进一步比较。

2. **邮件** — 如果记录包含“邮件”字段，Jabber 将基于此匹配记录。Jabber 不会根据电话号码进一步比较记录。
3. **电话号码** — 如果记录包含电话号码，Jabber 将基于此匹配记录。

当Jabber比较记录并确定哪个记录与同一个人匹配时，它将合并联系人数据以创建一个联系人记录。

拨号方案映射

您配置拨号方案映射以确保 Cisco Unified Communications Manager 上的拨号规则与您目录中的拨号规则匹配。

应用程序拨号规则

应用程序拨号规则会自动添加或删除用户拨打的电话号码中的位数。应用程序拨号规则会从客户端处理用户拨打的号码。

例如，您可以配置拨号规则，将数字 9 自动添加到 7 位电话号码的开头，以访问外线。

目录查找拨号规则

目录查找拨号规则可将主叫方ID号码转换成客户端可以在目录中查找的号码。您定义的每个目录查找规则，可根据初始位数和号码长度指定要转换哪些数字。

例如，您可以创建目录查找规则，从10位电话号码中自动删除区号和两位前缀数字。此类型的规则示例是将 `4089023139` 转换为 `23139`。

Cisco Unified Communication Manager UDS（适用于移动和 Remote Access）

Cisco Unified Communication Manager UDS 是 Cisco Jabber 使用 Expressway for Mobile and Remote Access 进行连接时使用的联系人来源。如果您在公司防火墙内部署 LDAP，我们建议您将 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。

云联系人来源

Cisco Webex 联系人来源

对于云部署，可在 Cisco Webex Messenger 管理工具中或通过用户更新配置联系人数据。联系信息可使用 Cisco Webex Messenger 管理工具导入。有关详细信息，请参阅 Cisco Webex Messenger管理指南的用户管理部分。

联系人照片格式和尺寸

要使用Cisco Jabber取得最佳结果，您的联系人照片应该有特定的格式和尺寸。检查支持的格式和最佳尺寸。了解客户端对联系人照片进行的调整。

联系人照片格式

对于您的目录中的联系人照片， Cisco Jabber 支持以下格式：

- JPG
- PNG
- BMP

重要事项 对于 GIF 格式的联系人照片， Cisco Jabber 不会应用任何修改以增强呈现效果。因此，GIF 格式的联系人照片可能不正确地呈现，或者质量欠佳。为获得最佳质量，将PNG格式用于您的联系人照片。

联系人照片尺寸

提示 联系人照片的最佳尺寸为 128 x 128 像素，且高宽比 1:1。

128 像素 x 128 像素是 Microsoft Outlook 中本地联系人照片的最大尺寸。

下表列出了 Cisco Jabber 中联系人照片的不同尺寸。

位置	尺寸
音频呼叫窗口	128 x 128 像素
邀请和提醒，例如： • 来电窗口 • 会议提醒窗口	64 x 64 像素
联系人清单，例如： • 联系人列表 • 参与者名录 • 呼叫历史记录 • 语音邮件消息	32 x 32 像素

联系人照片调整

Cisco Jabber 按如下方式调整联系人照片：

- 调整大小 — 如果目录中的联系人照片小于或大于 128 像素 x 128 像素， 会自动重新调整照片大小。例如，目录中的联系人照片为 64 像素 x 64 像素。当 Cisco Jabber 从目录中检索联系人照片时，它会将照片大小向 128 像素 x 128 像素重新调整。

  提示 重新调整联系人照片大小会导致低于最佳分辨率。因此，使用 128 像素 x 128 像素的联系人照片，这样客户端就不会自动重新调整其大小。

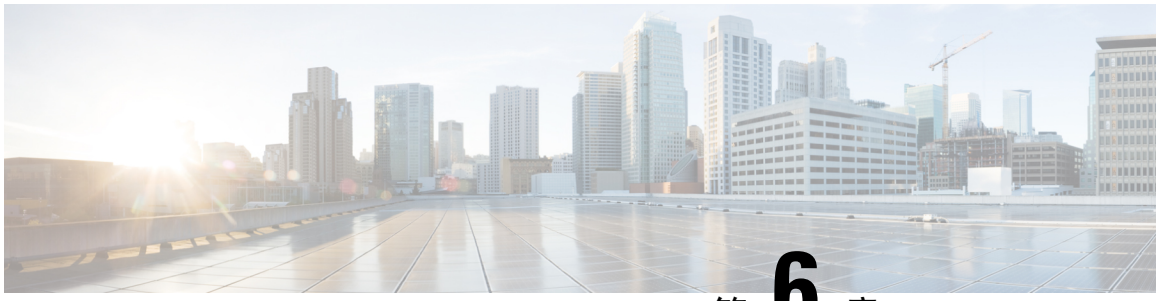
- 裁剪 — Cisco Jabber 会将非正方形联系人照片自动裁剪成正方形宽高比，或宽度与高度相同的 1:1 宽高比。

- 纵向方向 — 如果目录中的联系人照片为纵向方向，客户端会从顶部裁剪 30%，从底部裁剪 70%。

  例如，如果目录中的联系人照片宽度为 100 像素，高度为 200 像素，Cisco Jabber 需要从高度上裁剪 100 像素，以实现 1:1 的宽高比。在此情况下，客户端会从照片顶部裁剪 30 像素，从照片底部裁剪 70 像素。

- 横向方向 — 如果目录中的联系人照片为横向方向，客户端会从每侧裁剪 50%。

  例如，如果目录中的联系人照片宽度为 200 像素，高度为 100 像素，Cisco Jabber 需要从宽度上裁剪 100 像素，以实现 1:1 的宽高比。在此情况下，客户端会从照片右侧裁剪 50 像素，从照片左侧裁剪 50 像素。



第 6 章

安全和证书

加密

文件传输和屏幕捕获的合规性和策略控制

如果您在 Cisco Unified Communications Manager IM and Presence 10.5(2) 或更高版本上使用托管文件传输选项发送文件传输和屏幕捕获，您可以将文件发送到合规性服务器以进行审核和策略实施。

有关合规性的详细信息，请参阅 *Cisco Unified Communications Manager* 上 *IM and Presence Service* 的即时消息合规性指南。

有关配置文件传输和屏幕捕获的详细信息，请参阅《*Cisco Unified Communications Manager IM and Presence* 部署和安装指南》。

即时消息加密

Cisco Jabber 使用传输层安全 (TLS) 在客户端与服务器之间的网络上保护可扩展消息传送和网真协议 (XMPP) 流量。Cisco Jabber 会将点对点即时消息加密。

内部加密

下表概述了内部部署中即时消息加密的详细信息。

连接	协议	协商证书	预期的加密算法
客户端至服务器	通过 TLS v1.2 的 XMPP	X.509 公钥基础架构证书	AES 256 位

服务器与客户端协商

以下服务器使用 X.509 公钥基础架构 (PKI) 证书和以下项与 Cisco Jabber 协商 TLS 加密：

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

在服务器与客户端协商 TLS 加密之后，客户端和服务器都会生成和交换会话密钥，以加密即时消息流量。

下表列出了 Cisco Unified Communications Manager IM and Presence Service 的 PKI 证书密钥长度。

版本	密钥长度
Cisco Unified Communications Manager IM and Presence Service 版本 9.0.1 和更高版本	2048 位

XMPP 加密

Cisco Unified Communications Manager IM and Presence Service 使用采用 AES 算法加密的 256 位长度会话密钥，以保护 Cisco Jabber 与在线状态服务器之间的即时消息流量。

如果您需要提高服务器节点之间的流量的安全，可以在 Cisco Unified Communications Manager IM and Presence Service 上配置 XMPP 安全设置。有关安全设置的详细信息，请参阅以下内容：

- Cisco Unified Communications Manager IM and Presence Service — *IM and Presence* 的安全配置

即时消息记录

您可以根据监管指引记录即时消息并存档。要记录即时消息，您可以配置外部数据库，或与第三方合规性服务器集成。Cisco Unified Communications Manager IM and Presence Service 不加密您在外部数据库或第三方合规性服务器中记录的即时消息。您必须按需要配置外部数据库或第三方合规性服务器，以保护您记录的即时消息。

有关合规性的详细信息，请参阅以下内容：

- Cisco Unified Communications Manager IM and Presence Service— *IM and Presence Service* 的即时消息合规性

有关加密层级和加密算法（包括对称密钥算法，如 AES，或公钥算法，如 RSA）的详细信息，请参阅此链接 https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html 上的下一代加密 *(Next Generation Encryption)*。

有关 X.509 公钥基础架构证书的详细信息，请参阅此链接 https://www.ietf.org/rfc/rfc2459.txt 上的《互联网 *X.509* 公钥基础架构证书和 *CRL* 配置文件》文档。

基于云加密

下表概述了基于云部署中即时消息加密的详细信息：

连接	协议	协商证书	预期的加密算法
客户端至服务器	TLS 内的 XMPP	X.509 公钥基础架构证书	AES 128 位
客户端对客户端	TLS 内的 XMPP	X.509 公钥基础架构证书	AES 256 位

服务器与客户端协商

以下服务器通过 Cisco Webex Messenger 服务使用 X.509 公钥基础架构 (PKI) 证书与 Cisco Jabber 协商 TLS 加密。

在服务器与客户端协商 TLS 加密之后，客户端和服务器都会生成和交换会话密钥，以加密即时消息流量。

XMPP 加密

Cisco Webex Messenger 服务使用用 AES 算法加密的 128 位会话密钥，以保护 Cisco Jabber 和 Cisco Webex Messenger 服务之间的即时消息流量安全。

您可以有选择性地启用 256 位客户端对客户端 AES 加密，以保护客户端之间的流量安全。

即时消息记录

Cisco Webex Messenger 服务可以记录即时消息，但它不会以加密格式存档这些即时消息。不过，Cisco Webex Messenger 服务使用严格的数据中心安全性（包括 SAE-16 和 ISO-27001 审核）保护记录的即时消息。

如果您启用 256 位客户端对客户端加密，则 Cisco Webex Messenger 服务无法记录即时消息。

有关加密层级和加密算法（包括对称密钥算法，如 AES，或公钥算法，如 RSA）的详细信息，请参阅此链接 https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html 上的下一代加密 *(Next Generation Encryption)*。

有关 X.509 公钥基础架构证书的详细信息，请参阅此链接 https://www.ietf.org/rfc/rfc2459.txt 上的《互联网 *X.509* 公钥基础架构证书和 *CRL* 配置文件》文档。

客户端至客户端加密

默认情况下，客户端和 Cisco Webex Messenger 服务之间的即时消息流量是安全的。您可以有选择性地在 Cisco Webex 管理工具中指定策略，以保护客户端之间的即时消息流量安全。

以下策略可指定即时消息的客户端对客户端加密：

- **支持对 IM 进行 AES 编码**— 发送客户端使用 AES 256 位算法对即时消息加密。接收客户端会对即时消息加密。

- **不支持对 IM 进行编码** — 客户端可以在不支持加密的其他客户端之间发送和接收即时消息。

下表说明您可以使用这些策略设置的不同组合：

策略组合	客户端至客户端加密	当远程客户端支持 **AES** 加密时	当远程客户端不支持 **AES** 加密时
支持对 IM 进行 AES 编码 = false **不支持对 IM 进行编码** = true	否	Cisco Jabber 发送未加密的即时消息。 Cisco Jabber 不协商密钥交换。因此，其他客户端不发送 Cisco Jabber 加密的即时消息。	Cisco Jabber 发送和接收未加密的即时消息。
支持对 IM 进行 AES 编码 = true **不支持对 IM 进行编码** = true	是	Cisco Jabber 发送和接收已加密的即时消息。 Cisco Jabber 显示图标以指示即时消息已加密。	Cisco Jabber 发送已加密的即时消息。 Cisco Jabber 接收未加密的即时消息。
支持对 IM 进行 AES 编码 = true **不支持对 IM 进行编码** = false	是	Cisco Jabber 发送和接收已加密的即时消息。 Cisco Jabber 显示图标以指示即时消息已加密。	Cisco Jabber 不与远程客户端发送或接收即时消息。 当用户尝试向远程客户端发送即时消息时，Cisco Jabber 显示错误消息。

注释 Cisco Jabber 不支持通过群聊进行客户端到客户端的加密。Cisco Jabber 只对点对点聊天使用客户端到客户端加密。

有关加密和 Cisco Webex 策略的详细信息，请参阅 Cisco Webex 文档中的关于加密层级。

加密图标

查看客户端显示以指示加密级别的图标。

客户端到服务器加密的锁定图标

在本地和基于云的部署中，Cisco Jabber 会显示以下图标以指示客户端到服务器加密：

客户端至客户端加密的锁定图标

在基于云的部署中，Cisco Jabber 会显示以下图标以指示客户端至客户端加密：

本地聊天历史记录

聊天历史在参与者关闭聊天窗口和参与者注销之前得到保留。如果在参与者关闭聊天窗口后不想保留聊天历史，请将 Disable_IM_History 参数设置为 true。此参数可用于所有客户端（仅 IM 用户除外）。

对于 Cisco Jabber Mac 版本的内部部署，如果您在 Cisco Jabber Mac 版本的**聊天首选项**窗口中选择了**将聊天存档保存到：**选项，则聊天历史将存储在本地 Mac 文件系统中，可以使用 Spotlight 进行搜索。

本地聊天历史启用后，Cisco Jabber 不会对存档的即时消息进行加密。

对于桌面客户端，可以通过将存档保存到以下目录来限制对聊天历史的访问：

- Windows：`%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db`
- Mac：`~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`。

对于移动客户端，无法访问聊天历史文件。

语音和视频加密

您可以选择为所有设备设置安全电话功能。安全电话功能可提供安全 SIP 信令、安全媒体流和加密的设备配置文件。

如果您对用户启用安全电话功能，则设备与 Cisco Unified Communications Manager 的连接是安全的。但是，其他设备的呼叫仅在两个设备都有安全连接时才安全。

安全媒体的验证方法

使用 SIP oAuth 在基于令牌的身份验证中启用安全媒体。您可以为 Jabber 的内部、云和混合部署的安全验证设置 SIP oAuth 而非 CAPF 注册。

SIP oAuth
设置 Cisco Unified Communications Manager 时操作。它确保您的 SIP 流量（包括 RTP 媒体）是安全的。

CAPF 注册
启用 CAPF 注册的工作流程如下：

- 创建和配置 Jabber 设备
- 验证字串
- 配置电话安全性配置文件

PIE ASLR 支持

Cisco Jabber Android、iPhone 和 iPad 版本支持与位置无关的可执行地址空间布局随机化 (PIE ASLR)。

联邦信息处理标准

联邦信息处理标准 (FIPS) 140 是指定加密模块的安全要求的美国和加拿大政府标准。这些加密模块包括实施批准的安全功能并包含在加密边界内的硬件、软件和固件集。

FIPS 要求客户端中使用的所有加密、密钥交换、数字签名以及散列和随机号码生成功能符合加密模块安全的 FIPS 140.2 要求。

FIPS 模式导致客户端更严格地管理证书。如果服务证书过期并且没有重新输入其凭证，则 FIPS 模式中的用户可能会在客户端中看到证书错误。用户还会在其中央窗口中看到一个FIPS图标，以指示客户端正在 FIPS 模式下运行。

为 Cisco Jabber Windows 版本启用 FIPS

Cisco Jabber Windows 版本支持两种启用 FIPS 的方法：

- 操作系统已启用 — Windows 操作系统处于 FIPS 模式。
- Cisco Jabber 引导程序设置 — 配置 FIPS_MODE 安装程序交换机。Cisco Jabber 可以在未启用 FIPS 的操作系统上处于 FIPS 模式。在此情况下，只有与非 Windows API 之间的连接处于 FIPS 模式。

表 *8:* 适用于 *FIPS* 的 *Cisco Jabber Windows* 版本设置

平台模式	引导程序设置	Cisco Jabber 客户端设置
FIPS 已启用	FIPS 已启用	FIPS 已启用 — 引导程序设置。
FIPS 已启用	FIPS 已禁用	FIPS 已禁用 — 引导程序设置。
FIPS 已启用	无设置	FIPS 已启用 — 平台设置。
FIPS 已禁用	FIPS 已启用	FIPS 已启用 — 引导程序设置。
FIPS 已禁用	FIPS 已禁用	FIPS 已禁用 — 引导程序设置。
FIPS 已禁用	无设置	FIPS 已禁用 — 平台设置。

注释 在 SSL 连接期间，Jabber 语音邮件服务仅接受 HTTPS 请求 **https://164.62.224.15/vmrest/version**（**FIPS 已启用**）的 TLS 版本 TLS 1.2。

已针对用于移动客户端的 Cisco Jabber 启用 FIPS

要针对用于移动客户端的 Cisco Jabber 启用 FIPS，请在企业移动性管理 (EMM) 中将 FIPS_MODE 参数设置为 TRUE。

重要事项

- 启用 FIPS 将使用户不能接受不可信的证书。在此情况下，用户可能无法使用某些服务。证书信任列表 (CTL) 或 ITL 文件在此处不适用。服务器的证书必须已正确签名，或者必须通过旁加载让客户端信任服务器的证书。
- FIPS 实施 TLS 1.2，因此禁用较旧协议。
- 用于移动客户端的 Cisco Jabber 不支持平台模式。

通用标准

信息技术安全评估的 Common Criteria 包括一组用于评估 IT 产品安全属性的国际标准。您可以在符合 Common Criteria 认证要求的模式下运行 Cisco Jabber。为此，您必须为每个客户端启用该设置。

要在通过 Common Criteria 启用的环境中运行 Jabber：

- 用于 Windows 的 Jabber：将 CC_MODE 安装参数设置为 TRUE。
- 对于 iJabber for Android 和 Jabber for iPhone and iPad：在您的企业移动性管理 (EMM) 中将 CC_MODE 参数设置为 TRUE。
- RSA 密钥长度必须至少为 2048 位。要配置 RSA 密钥长度，请阅读有关如何在 *Cisco Jabber 12.5* 的内部部署指南中创建和配置 *Cisco Jabber* 设备的信息。

有关如何设置 Jabber 以 Common Criteria 模式运行的详细信息，请参阅《*Cisco Jabber 12.5* 的内部部署指南》中有关如何部署 *Cisco Jabber* 应用程序的详细信息。

安全 LDAP

安全 LDAP 通信是 LDAP over SSL/TLS

LDAPS 通过 SSL/TLS 连接启动 LDAP 连接。其打开 SSL 会话，然后使用 LDAP 协议开始。这需要单独的端口 636 或全局目录端口 3269。

已验证的 UDS 联系人搜索

在 Cisco Unified Communications Manager 和 Cisco Jabber 中启用 UDS 联系人搜索的验证将提供凭证以使用 UDS 进行验证来进行联系人搜索。

证书

证书验证

证书验证过程

Cisco Jabber 在其上运行的操作系统在对服务进行验证时验证服务器证书。服务在尝试建立安全连接时会向 Cisco Jabber 提供证书。操作系统根据客户端设备的本地证书存储区中的内容验证提供的证书。如果证书不在证书存储区中，证书将被视为不可信，Cisco Jabber 提示用户接受或拒绝证书。

如果用户接受证书，Cisco Jabber 则连接到服务并将证书保存在设备的证书存储区或 keychain 中。如果用户拒绝证书，Cisco Jabber 则不会连接到服务，并且证书不会保存到设备的证书存储区或 keychain 中。

如果证书在设备的本地证书存储区中，Cisco Jabber 将信任证书。Cisco Jabber 将连接至服务，且不会提示用户接受或拒绝证书。

Cisco Jabber 可以验证多个服务，具体取决于组织中部署的内容。必须为每个服务生成一个证书签名请求 (CSR)。某些公共证书颁发机构不接受每个完全限定域名 (FQDN) 有一个以上的 CSR。这意味着，可能需要将每项服务的 CSR 发送到单独的公共证书颁发机构。

确保在服务配置文件中为每项服务指定 FQDN，而不是 IP 地址或主机名。

已签名证书

证书可由证书颁发机构 (CA) 签名，也可自签。

- CA 签名证书（推荐）— 不提示用户，因为您自行在设备上安装证书。CA 签名证书可由私人 CA 或公共 CA 签名。由公共 CA 签名的许多证书都存储在设备的证书存储区或 keychain 中。使用 Android 7.0 或更高版本的设备只识别 CA 签名的证书。
- 自签证书 — 证书由出示证书的服务签名，并且用户始终收到接受或拒绝证书的提示。

证书验证选项

在设置证书验证之前，必须确定您希望验证证书的方式：

- 您是为内部部署还是基于云的部署部署证书。
- 您使用哪种方法对证书进行签名。
- 如果您部署 CA 签名证书，您将要使用公共 CA 还是私人 CA。

- 您需要为其获取证书的服务。

内部服务器所需证书

内部服务器提供以下证书以与 Cisco Jabber 建立安全连接：

服务器	证书
Cisco Unified Communications Manager IM and Presence Service	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat) 和 CallManager 证书（安全电话的安全 SIP 呼叫信令）
Cisco Unity Connection	HTTP (Tomcat)
Cisco Webex Meetings 服务器	HTTP (Tomcat)
Cisco VCS Expressway Cisco Expressway-E	服务器证书（用于 HTTP、XMPP 和 SIP 呼叫信令）

重要说明

- 安全断言标记语言 (SAML) 单点登录 (SSO) 和身份提供程序 (IdP) 需要 X.509 证书。
- 在开始证书签名过程之前，您应该为 Cisco Unified Communications Manager IM and Presence Service 应用最新的服务更新 (SU)。
- 所需的证书适用于所有服务器版本。
- 每个群集节点、订阅方和发布方运行 Tomcat 服务，可以向客户端提供 HTTP 证书。

  您应该计划为群集中的每个节点签署证书。
- 要在客户端与 Cisco Unified Communications Manager 之间提供安全的 SIP 信令，应使用证书权限代理功能 (CAPF) 注册。

证书签名请求格式和要求

公共证书颁发机构 (CA) 通常要求证书签名请求 (CSR) 符合特定的格式。例如，公共 CA 可能仅接受满足以下要求的 CSR：

- 均为 Base64 编码。
- 在**组织**、**OU** 或其他字段中不包含某些字符，例如 `@&!`。
- 在服务器的公共密钥中使用特定的位长度。

如果您从多个节点提交 CSR，则公共 CA 可能要求所有 CSR 中的信息一致。

为防止 CSR 出现问题，您应从计划提交 CSR 的公共 CA 查看格式要求。然后，您应确保在配置服务器时输入的信息符合公共 CA 所需的格式。

每个 FQDN 一个证书 — 某些公共 CA 仅对每个完全限定域名 (FQDN) 签署一个证书。

例如，要为单个 Cisco Unified Communications Manager IM and Presence Service 节点签署 HTTP 和 XMPP 证书，您可能需要将每个 CSR 提交到不同的公共 CA。

吊销服务器

如果无法接通吊销服务器，Cisco Jabber 无法连接到 Cisco Unified Communications Manager 服务器。此外，如果证书颁发机构 (CA) 吊销证书，Cisco Jabber 不允许用户连接到该服务器。

系统不会通知用户以下结果：

- 证书不包含吊销信息。
- 无法访问吊销服务器。

要验证证书，证书必须在可提供吊销信息的可访问服务器的 **CDP** 或 **AIA** 字段中包含 HTTP URL。

为确保您在获得 CA 颁发的证书时验证您的证书，您必须满足以下要求之一：

- 确保 **CRL 分发点** (CDP) 字段包含吊销服务器上证书吊销列表 (CRL) 的 HTTP URL。
- 确保**颁发机构信息访问** (AIA) 字段包含在线证书状态协议 (OCSP) 服务器的 HTTP URL。

证书中的服务器身份

作为签名过程的一部分，CA 指定证书中的服务器身份。当客户端验证证书时，它会检查：

- 受信任的颁发机构已颁发证书。
- 提供证书的服务器的身份与证书中指定的服务器的身份匹配。

注释 公共 CA 通常要求将完全限定域名 (FQDN) 作为服务器标识，而不是 IP 地址。

标识符字段

客户端在服务器证书中检查标识匹配的以下标识符字段：

- XMPP 证书
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - `Subject CN`

- HTTP 证书
  - SubjectAltName\dnsNames
  - Subject CN

提示 Subject CN 字段可将通配符 (*) 包含为最左边的字符，例如 *.cisco.com。

防止标识不匹配

如果用户尝试连接到具有 IP 地址或主机名的服务器，并且服务器证书使用 FQDN 标识服务器，则客户端无法将该服务器标识为可信任并提示用户。

如果您的服务器证书使用 FQDN 标识服务器，则应计划在服务器的多个位置将每个服务器名称指定为 FQDN。有关详细信息，请参阅故障诊断 TechNotes 中的“防止标识不匹配”部分。

多服务器 SAN 证书

如果使用多服务器 SAN，则每个 tomcat 证书的每个群集和每个 XMPP 证书的每个群集均只需将证书上传到服务一次。如果不使用多服务器 SAN，则必须将证书上传到每个 Cisco Unified Communications Manager 节点的服务。

云部署的证书验证

Cisco Webex Messenger 和 Cisco Webex Meetings 中心默认向客户端提交以下证书：

- CAS
- WAPI

注释 Cisco Webex 证书必须由公共证书颁发机构 (CA) 签名。Cisco Jabber 验证这些证书以与基于云的服务建立安全连接。

Cisco Jabber 验证从 Cisco Webex Messenger 收到的以下 XMPP 证书。如果您的操作系统中不包含这些证书，您必须提供它们。

- VeriSign Class 3 Public Primary Certification Authority - G5 — 此证书存储在受信任的根证书颁发机构中
- VeriSign Class 3 Secure Server CA - G3 — 此证书验证 Webex Messenger 服务器身份并存储在中间证书颁发机构中。
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority Root Certificate

有关 Cisco Jabber Windows 版本的根证书的详细信息，请参阅 https://www.identrust.co.uk/certificates/trustid/install-nes36.html。

有关用于 Cisco Jabber Mac 版本的根证书的详细信息，请参阅 https://support.apple.com。

多租户托管协作解决方案的服务器名称指示支持

Cisco Jabber 在具有多租户托管协作解决方案的移动和Remote Access (MRA) 部署中支持服务器名称指示 (SNI)。

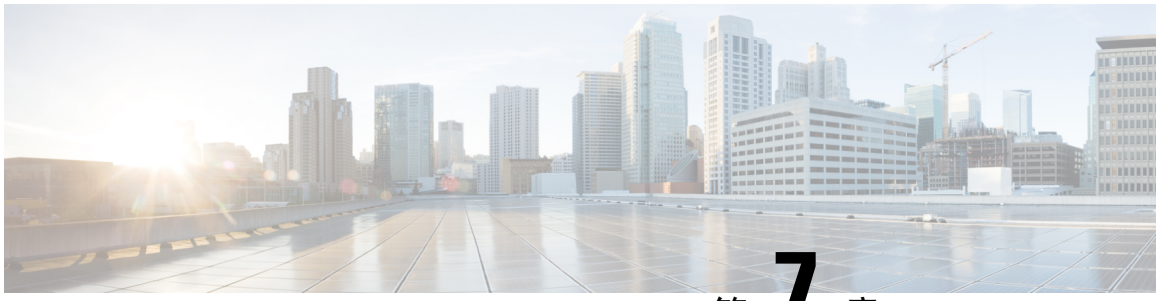
Cisco Jabber 使用 SNI 发送域信息到 Expressway。Expressway 查找证书存储库以查找包含域信息的证书，并将证书返回到 Cisco Jabber 进行验证。

有关多租户部署的详细信息，请参阅《Cisco Hosted Collaboration Solution 版本 11.5 多租户 Expressway 配置指南》中的采用域证书的终端服务发现和不采用域证书的 *Jabber* 服务发现部分。

防病毒排除

如果您部署了防病毒软件，请在防病毒排除列表中包含以下文件夹位置：

- `C:\Users\<User>\AppData\Local\Cisco\Unified Communications\Jabber`
- `C:\Users\<User>\AppData\Roaming\Cisco\Unified Communications\Jabber`
- `C:\ProgramData\Cisco Systems\Cisco Jabber`



第 7 章

配置管理

快速登录

此功能能使您同时登录所有 Cisco Jabber 服务，而无需如早前那样按照顺序登录。每项服务独立连接到其相应的服务器，并基于缓存的数据进行验证。如此一来，登录过程可变得迅速和动态。不过，此功能仅从您第二次登录到 Jabber 时起作用。

您可以通过对所有客户端使用 STARTUP_AUTHENTICATION_REQUIRED 参数配置快速登录。不过，对于移动客户端，您必须配置 STARTUP_AUTHENTICATION_REQUIRED 和 CachePasswordMobile 参数。有关配置这些参数的详细信息，请参阅最新的《*Cisco Jabber* 参数参考指南》。

配置重新提取—在每次登录或注销时，快速登录不会同步检索服务器端设置。只有在第一次登录时才会发生这种情况，如同在之前的 Jabber 版本中一样。

对于后续登录，请求将在不同点（例如登录后的 1 到 5 分钟内、登录后 7 至 9 小时内或者您的用户进行手动刷新以提取配置时）从服务器提取全新配置。

您可以将 ConfigRefetchInterval 参数配置为每 7 或 8 小时从服务器提取配置。有关此参数的详细信息，请参阅最新的《*Cisco Jabber* 参数参考指南》。

动态配置更改的操作

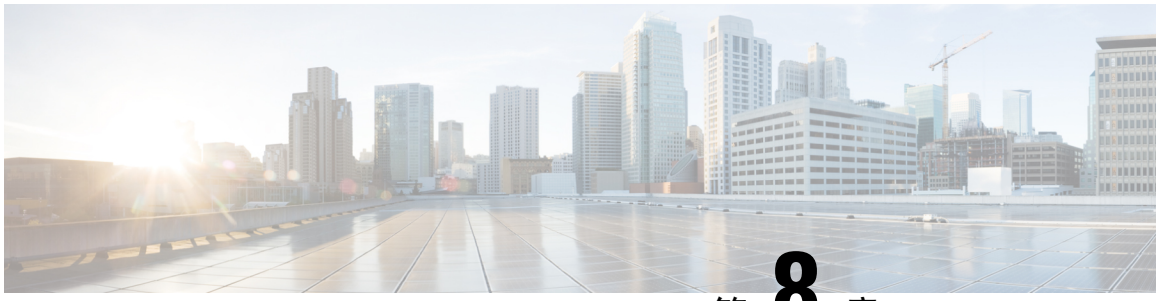
在 Jabber 11.9 中，组件和服务对配置更改做出动态响应。您会收到通知提示，要求您注销或重置 Jabber，具体取决于以下情况：

重置 Jabber — 如果主要服务发生变化，您将收到重置 Jabber 的通知提示。例如，如果 IM&P 和电话帐户更改为仅电话帐户，则 Jabber 将需要重置。

从 Jabber 注销 — 如果下表中列出的配置键出现任何更改，Jabber 将提示用户注销并登录以使用新的配置。

- **Windows**—您将收到配置已更改的弹出通知。您可以忽略通知或注销，然后登录以使用新的配置。
- **移动客户端** — Jabber 会自动注销。然后，您将收到指示配置已更改的弹出通知。单击“**确定**”接受配置更改，以自动登录到 Jabber。

键名称	平台	注销
RemoteAccess	所有客户端	注销
Meetings_Enabled	所有客户端	注销
DirectoryServerType	所有客户端	注销
DirectoryUri	所有客户端	注销
UseSipUriToResolveContacts	所有客户端	注销
SipUri	所有客户端	注销
UriPrefix	所有客户端	注销
DirectoryUriPrefix	所有客户端	注销
SwapDisplayNameOrder	所有客户端	注销
PresenceDomain	所有客户端	注销
Support_SSL_Encoding	所有客户端	注销
Support_No_Encoding	所有客户端	注销
IM_Logging_Enabled	所有客户端	注销
IGS_CUP_ENABLESECURE	所有客户端	注销
DISALLOW_FILE_TRANSFER_ON_MOBILE	所有客户端	注销
Persistent_Chat_Enabled	桌面客户端	注销
Persistent_Chat_Mobile_Enabled	移动客户端	注销
Disable_MultiDevice_Message	所有客户端	注销
Location_Enabled/Location_Matching_Mode	所有客户端	注销
IP_MODE	所有客户端	注销
Telephony_Enabled	所有客户端	注销
Voicemail_Enabled	所有客户端	注销
EnableLoadAddressBook	移动客户端	注销
ShowRecentsTab	仅 Jabber Windows	注销
IM_Enabled	所有客户端	注销
Disallow-jaibreak-device	移动客户端	注销
EnableChats	仅 Jabber Windows	注销



第 8 章

屏幕共享

屏幕共享

屏幕共享有四种类型：

- Cisco Webex share
- BFCP 共享
- 仅 IM 共享
- 升级到会议并共享

Cisco Webex 屏幕共享

适用于云部署的 Cisco Jabber 桌面客户端版本。

对于云部署，如果“BFCP”和“仅 IM”屏幕共享选项不可用，在选择联系人后自动选择 Cisco Webex 屏幕共享。

您可以使用以下方法之一启动 Cisco Webex 屏幕共享：

- 右击中心窗口中的联系人，然后从菜单选项中选择 **共享屏幕..**。
- 在中心窗口中选择一个联系人，然后单击**设置**菜单。选择 **通信** 并从菜单选项中选择 **共享屏幕 ……**
- “BFCP”和“仅 IM”屏幕共享选项不可用时，请在对话窗口的菜单项中选择 …… > **共享屏幕**。

BFCP 屏幕共享

适用于 Cisco Jabber 桌面客户端，而用于移动客户端的 Cisco Jabber 只能接收 BFCP 屏幕共享。

二进制层控制协议 (BFCP) 屏幕共享由 Cisco Unified Communications Manager 控制。Cisco Unified Communications Manager 会处理用户使用视频桌面共享功能时传输的 BFCP 包。在呼叫时选择……> **共享屏幕** 以启动 BFCP 屏幕共享。

此功能不支持远程屏幕控制。

如果在软终端设备上启用了**信任的中继点**或**媒体终结点**，则不支持使用 BFCP 的视频桌面共享。

注释 在 Jabber Windows 版本中，按**屏幕共享**按钮默认会启动 BFCP 屏幕共享。如果基于 BFCP 的共享不可用，按该按钮会启动仅 IM 屏幕共享（如可能）。

仅 IM 屏幕共享

适用于 Cisco Jabber Windows 版本。

仅 IM 屏幕共享是基于远程桌面协议 (RDP) 的一对一客户端到客户端屏幕共享。EnableP2PDesktopShare 参数控制仅 IM 屏幕共享是否可用。PreferP2PDesktopShare 参数控制 Jabber 偏好视频共享还是仅 IM 屏幕共享。

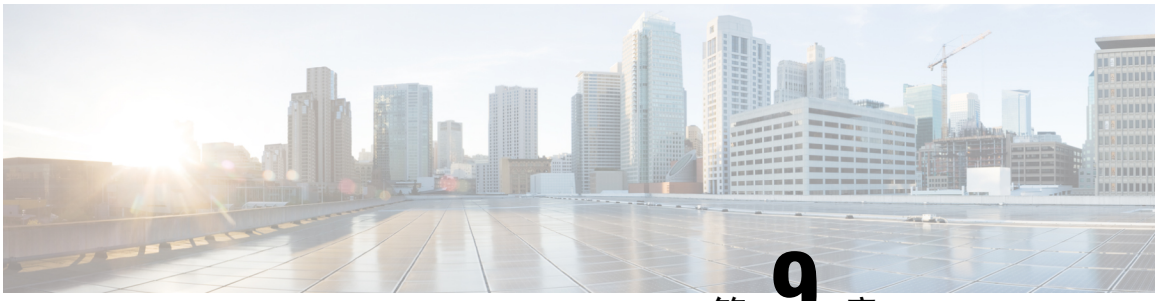
如果您的部署允许仅 IM 屏幕共享，请在聊天窗口中选择 **...** > **共享屏幕** 以启动屏幕共享。

RDP 默认需要端口 3389。仅即时消息屏幕共享默认端口范围为 49152 – 65535 TCP 和 UDP。您可以使用 SharePortRangeStart 和 SharePortRangeSize 参数来限制端口范围。

升级到会议并共享

适用于所有 Cisco Jabber 客户端。

您可以升级到即时 Cisco Webex Meetings 并使用 Cisco Webex Meetings 控件共享屏幕。



第 9 章

域间联合

域间联合可使企业域中的Cisco Jabber用户可以与另一个域中的用户共享可用性，并相互发送即时消息。

- Cisco Jabber 用户必须手动输入另一个域的联系人。
- Cisco Jabber 支持与以下各项的联合：
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP 基于标准的环境，如 Google Talk

  注释 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。
  - AOL Instant Messenger

在 Cisco Unified Communications Manager IM and Presence Service 上配置适用于 Cisco Jabber 的域间联合。有关详情，请参阅适当的服务器文档。

- 域内联合，第 123 页
- 用于联合的用户 ID 规划，第 124 页

域内联合

域内联合可使同一域中的用户能够在Cisco Unified Communications Manager IM and Presence Service、Microsoft Office Communications Server、Microsoft Live Communications Server 或另一个在线状态服务器之间共享可用性和发送即时消息。

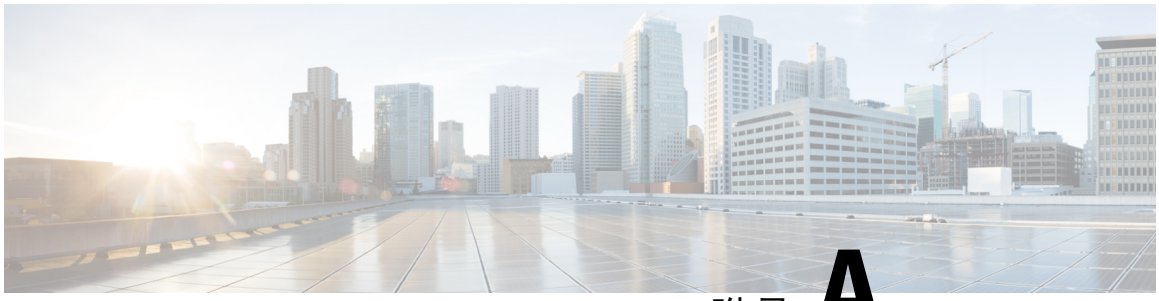
域内联合允许您将用户从不同的在线状态服务器迁移至 Cisco Unified Communications Manager IM and Presence Service。因此，您可以在在线状态服务器上为 Cisco Jabber 配置域内联合。有关详情，请参阅：

- Cisco Unified Communications Manager IM and Presence Service：*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的分区域内联合

用于联合的用户 ID 规划

对于联合，Cisco Jabber 需要每个用户的联系人 ID 或用户 ID，以便在联系人搜索期间解析联系人。

在 SipUri 参数中设置用户 ID 的属性。默认值为 `msRTCSIP-PrimaryUserAddress`。如果存在要从您的用户 ID 中删除的某个前缀，您可以在 UriPrefix 参数中设置一个值，请参阅《*Cisco Jabber* 的参数参考指南》的最新版本。



附录 A

Jabber 支持的语言：

支持的语言

下表列出了Cisco Jabber客户端所支持语言的区域设置标识符（LCID）或语言标识符（LangID）。

支持的语言	Cisco Jabber Windows 版本	Cisco Jabber Mac 版本	适用于 Cisco Jabber Android 版本， Cisco Jabber iPhone 和 iPad 版本	LCID/LangID
阿拉伯语——沙特阿拉伯	X		X	1025
保加利亚语——保加利亚	X	X		1026
加泰罗尼亚语——西班牙	X	X		1027
中文（简体）——中国	X	X	X	2052
中文（繁体）——台湾	X	X	X	1028
克罗地亚语——克罗地亚	X	X	X	1050
捷克语——捷克共和国	X	X		1029
丹麦语——丹麦	X	X	X	1030
荷兰语——荷兰	X	X	X	1043

Jabber 支持的语言：

支持的语言	Cisco Jabber Windows 版本	Cisco Jabber Mac 版本	适用于 Cisco Jabber Android 版本，Cisco Jabber iPhone 和 iPad 版本	LCID/LangID
英语 ——美国	X	X	X	1033
芬兰语——芬兰	X	X		1035
法语——法国	X	X	X	1036
德语——德国	X	X	X	1031
希腊语——希腊	X	X		1032
希伯来语——以色列	X			1037
匈牙利语——匈牙利	X	X	X	1038
意大利语——意大利	X	X	X	1040
日语——日本	X	X	X	1041
朝鲜语——朝鲜	X	X	X	1042
挪威语——挪威	X	X		2068
波兰语——波兰	X	X		1045
葡萄牙语——巴西	X	X	X	1046
葡萄牙语——葡萄牙	X	X		2070
罗马尼亚语——罗马尼亚	X	X	X	1048
俄语——俄罗斯	X	X	X	1049
塞尔维亚语	X	X		1050
斯洛伐克语——斯洛伐克	X	X	X	1051
斯洛文尼亚语——斯洛文尼亚	X	X		1060

支持的语言	Cisco Jabber Windows 版本	Cisco Jabber Mac 版本	适用于 Cisco Jabber Android 版本，Cisco Jabber iPhone 和 iPad 版本	LCID/LangID
西班牙语——西班牙（现代排序）	X	X	X	3082
瑞典语——瑞典	X	X	X	5149
泰国语——泰国	X	X		1054
土耳其语	X	X	X	1055

Jabber 支持的语言：