用于 Cisco Jabber 14.0 的 Webex Messenger 部署

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

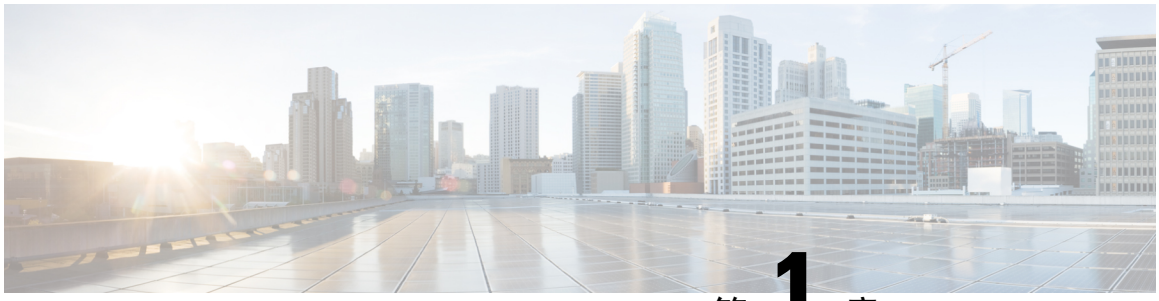
目录

更改历史记录

新信息及变更内容

日期	参数	变更说明	部分
2021 年 3 月		首次发布	

更改历史记录



第 1 章

Jabber 概述

本指南的目的

本指南包含部署和安装 Cisco Jabber 所需的以下基于任务的信息：

- 配置和安装工作流程，其中概述了用于配置和安装云或混合部署的流程。
- 如何配置与 Cisco Jabber 客户端交互的各种服务，例如 IM and Presence Service、语音和视频通信、可视语音邮件和会议。
- 如何配置目录集成、证书验证和服务发现。
- 如何安装客户端。

在部署和安装 Cisco Jabber 之前，请参阅 *Cisco Jabber* 规划指南 (https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html)，以确定最适合您企业需求的部署选项。

关于 Cisco Jabber

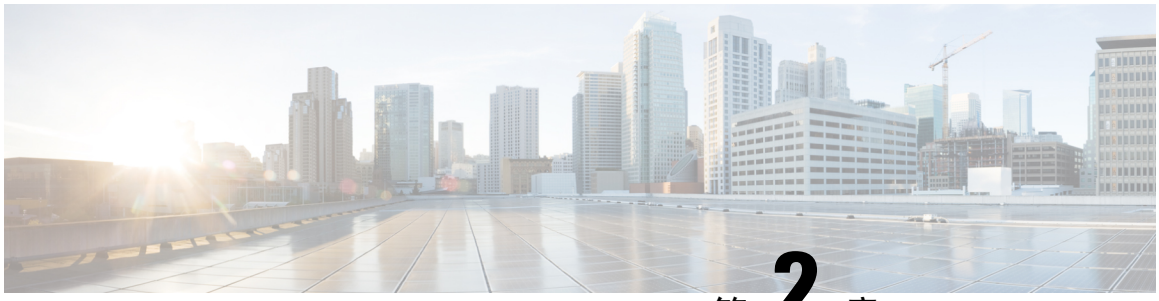
Cisco Jabber 是一套统一通信应用程序，可让您在任何位置与您的联系人无缝交互。Cisco Jabber 提供即时消息、在线状态、音频和视频呼叫、语音邮件和会议服务。

Cisco Jabber 产品系列中的应用程序包括：

- Cisco Jabber Windows 版本
- Cisco Jabber Mac 版本
- Cisco Jabber iPhone 和 iPad 版本
- Cisco Jabber Android 版本

- Cisco Jabber VDI 软终端

有关 Cisco Jabber 产品套件的详细信息，请参阅 https://www.cisco.com/go/jabber 或 https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html。



第 2 章

云和混合部署工作流程

使用 Cisco Webex Messenger 的云部署工作流程

过程

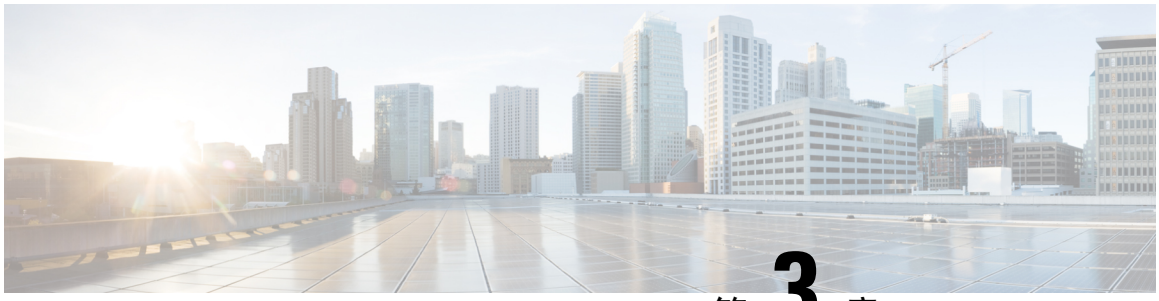
	命令或操作	目的
步骤 1	配置策略， 第 5 页	
步骤 2	为云部署创建用户， 第 15 页	
步骤 3	设置证书验证， 第 53 页	
步骤 4	配置客户端， 第 55 页	
步骤 5	部署 Cisco Jabber 应用程序和 Jabber VDI 软终端， 第 67 页	

使用 Webex Messenger 的混合部署工作流程

过程

	命令或操作	目的
步骤 1	配置策略， 第 5 页	
步骤 2	配置群集， 第 11 页	
步骤 3	在 Unified Communications Manager 上创建用户， 第 23 页	
步骤 4	配置软终端， 第 37 页	

	命令或操作	目的
步骤 5	配置桌面电话控制， 第 29 页	
步骤 6	配置扩展与连接， 第 47 页	
步骤 7	配置远程访问的服务发现， 第 51 页	
步骤 8	设置证书验证， 第 53 页	
步骤 9	配置客户端， 第 55 页	
步骤 10	部署 Cisco Jabber 应用程序和 Jabber VDI 软终端， 第 67 页	
步骤 11	Remote Access， 第 111 页	



第 3 章

配置策略

添加策略

过程

步骤 1 选择**策略编辑器**选项卡。
策略列表显示在**策略**屏幕的左侧，**操作列表**显示在右侧。

步骤 2 在**策略列表**下，选择**添加**。
新策略将出现在现有策略列表的顶部。

步骤 3 为策略输入唯一名称。

下一步做什么

要为此策略添加操作，请参阅：将操作添加到策略， 第 5 页

将操作添加到策略

过程

步骤 1 选择**策略编辑器**选项卡。
策略列表显示在**策略编辑器**屏幕的左侧，**操作列表**显示在右侧。

步骤 2 在**策略名称**下，选择要为其添加操作的策略。

步骤 3 要添加操作，请在屏幕右侧的**操作列表**中选择**添加**。

此时将显示**操作编辑器**屏幕。

步骤 4 从**操作标记名称**列表中选择一项策略操作。

步骤 5 选择**保存**。

步骤 6 重复步骤 3-5，直到为所有策略都分配了操作。

策略操作 Cisco Webex

默认情况下，新部署 Cisco Webex 的组织将授予所有用户全部功能。

注释 默认情况下，不会启用端到端加密策略。组织管理员可以启用此策略。当需要对所有用户或特定用户组禁用特定功能时，管理员可以创建策略。

无法对使用第三方 XMPP IM 应用程序的用户实施策略操作。

不超过十个 VoIP 会议参与者可以同时连接到同一 VoIP 会议。

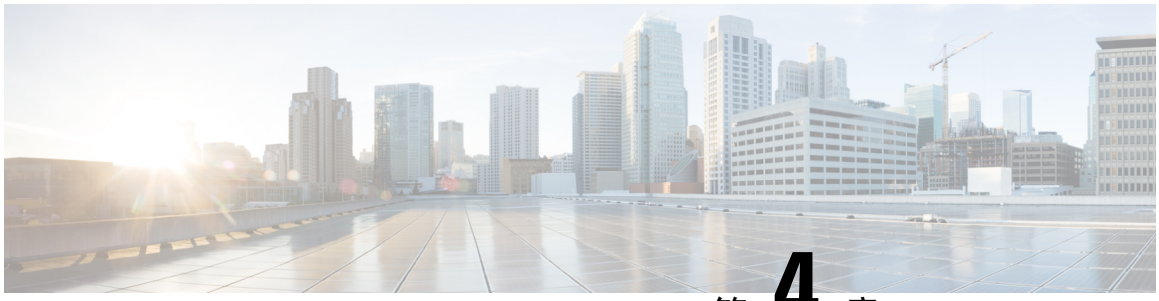
外部用户是指不属于 Cisco Webex 组织的用户。他们仍可使用 Cisco Webex 与属于 Cisco Webex 组织的用户进行通信。

策略操作	说明	影响	默认值
外部文件传输	控制 IM 会话中组织用户与组织外部用户之间的文件传输。	**禁用**—停止组织用户与外部用户之间的所有文件传输。这包括至少有一个外部用户的多方 IM 会话。	**启用**
内部文件传输	控制 IM 会话中组织内用户之间的文件传输。	**禁用**—停止所有内部文件传输。 **启用**—组织内的所有用户都可以与内部用户交换文件。	**启用**
外部 IM	控制组织内部用户与组织外部用户之间的 IM 会话。	**禁用**—停止组织内部用户和组织外部用户之间的所有 IM 会话。这将停止所有从属服务，如语音、视频和 VoIP。	**启用**

策略操作	说明	影响	默认值
外部 VoIP	控制 IM 会话中组织内部用户与组织外部用户之间的 VoIP 通信	**禁用** — 停止 IM 会话中组织内部用户与组织外部用户之间的所有 VoIP 通信。但是，诸如基于文本的 IM 会话和文件传输等其他服务仍可用	**启用**
内部 VoIP	控制 IM 会话中组织内部用户之间的 VoIP 通信。	**禁用** — 停止 IM 会话中组织内部用户之间的所有 VoIP 通信。但是，诸如基于文本的 IM 会话和文件传输等其他服务仍可用。 **启用** — 组织内部所有用户都可以在 IM 会话中使用 VoIP 通信。	**启用**
外部视频	控制 IM 会话中组织内部用户与组织外部用户之间的视频服务	**禁用** — 停止 IM 会话中组织内部用户和组织外部用户之间的所有视频服务。但是，诸如基于文本的 IM 会话和文件传输等其他服务仍可用。	**启用**
内部视频	控制 IM 会话中组织内部用户之间的视频服务。	**禁用** — 停止 IM 会话中组织内部用户之间的所有视频服务。但是，诸如基于文本的 IM 会话和文件传输等其他服务仍可用。 **启用** — 组织内部所有用户都可以在 IM 会话中使用视频通信。	**启用**
本地存档	控制用户是否能本地存档 IM 文本消息。		**启用**

策略操作	说明	影响	默认值
外部桌面共享	控制组织内部用户是否能与组织外部用户共享其桌面。	**禁用**—禁止组织内部用户与组织外部用户共享其（本地）桌面。 **启用**—用户可以与组织外部用户共享其（本地）桌面。	**启用**
内部桌面共享	控制组织内部用户是否能与组织内的其他用户共享其桌面。	**禁用**—组织内部用户无法与组织内的其他用户共享其桌面。 **启用**—用户可以与组织内的其他用户共享其桌面。	**启用**
支持 IM 的端到端加密	指定是否支持 IM 会话的端对端加密。	**启用** — 支持 IM 会话的端到端加密。 登录的用户不支持端到端加密。	**禁用**
不支持对 IM 进行编码	控制启用了端到端加密的应用程序是否可以启动与未启用端到端加密的应用程序或不支持端对端加密的第三方应用程序的 IM 会话。	**禁用**—禁止启用了端到端加密的应用程序启动与未启用端到端加密的应用程序或第三方应用程序的 IM 会话。 **启用**—协商的加密级别是第三方支持的最高级别。	**启用**
内部IM（包括已列入白名单的域）	控制组织内部用户与白名单中特定域之间的IM通信。	**禁用**—禁止组织内部用户成为白名单中指定域内的 IM 用户。但是，域中的用户可以彼此发起IM。此外，还会禁用其他相关服务，例如VoIP、视频和文件传输。	**启用**
上传小组件			**启用**

策略操作	说明	影响	默认值
允许用户编辑配置文件	控制是否能限制用户编辑其配置文件信息。	**禁用**—禁止用户编辑其配置文件信息。 此策略操作会影响**配置**选项卡中**配置文件设置**屏幕中的设置。	**启用**
允许用户编辑配置文件视图设置	控制是否能限制用户组更改其用户配置文件视图设置。	**禁用**—禁止用户更改其用户配置文件视图设置。 此策略操作影响**配置**选项卡**配置文件设置**屏幕中的**允许用户更改其配置文件视图设置**复选框。 **允许用户更改其配置文件视图设置**复选框不会影响，即使已选中。	**启用**
内部屏幕截图	控制用户是否能向组织内部用户发送屏幕截图。	**禁用**—阻止组织内部用户在组织内发送屏幕截图。	**启用**
外部屏幕截图	控制用户是否能向组织外部用户发送屏幕截图。	**禁用**—阻止组织内部用户将屏幕截图发送到组织外部。	**启用**
发送内部广播消息	控制用户是否能向组织内部用户发送广播消息。	**禁用**—阻止组织内部用户在组织内发送广播消息。	**启用**
发送外部广播消息	控制用户是否能向组织外部用户发送广播消息。	**禁用**—阻止组织内部用户向组织外部发送广播消息。	**启用**
允许用户向目录组发送广播	控制用户是否能向组织内的某个目录组发送广播消息。	**禁用**—阻止组织内部用户向组织内的某个目录组发送广播消息。	**启用**
高清视频	当外部视频或内部视频策略启用时，控制是否将计算机上的高清视频功能用于计算机呼叫	**禁用**—禁止将所有计算机的高清视频用于计算机呼叫。	**启用**



第 4 章

配置群集

配置可视语音邮件

过程

步骤 1 要配置可视语音邮件，请选择 **配置选项卡** > **统一通信**。
统一通信窗口将会打开。

步骤 2 选择**语音邮件**，打开 **CUCI 可视语音邮件默认设置**屏幕。

Unity connection 客户应在“”语音邮件服务器“”和“邮件存储服务器”字段中输入 Unity connection 服务器 IP 地址或 DNS 名称。建议所有其他设置均保留默认值。

步骤 3 要启用可视语音邮件，请选择**启用可视语音邮件**。

步骤 4 如果要手动输入可视语音邮件设置，请选择**允许用户手动输入设置**。

步骤 5 请输入以下信息：

- **语音邮件**服务器：Cisco Webex 应用程序在检索语音邮件时应与之通信的可视语音邮件服务器的名称。
- **语音邮件**协议：用于与可视语音邮件服务器通信的协议。您可以选择 HTTPS 或 HTTP。
- **语音邮件端口**：与可视语音邮件服务器关联的端口。

不支持以下邮件存储参数选项。Cisco Webex 管理工具需要值，请输入 `10.0.0.0` 作为邮件存储服务器，其余字段保留默认值。

- **邮件存储服务器**：邮件存储服务器的名称。
- **邮件存储协议**：邮件存储服务器使用的协议。您可以选择 TLS 或 Plain。
- **邮件存储端口**：与邮件存储服务器关联的端口。

- **IMAP 空闲过期时间**：经过多长时间（分钟）后服务器停止自动检查语音邮件功能。
- **邮件存储收件箱文件夹名称**：在邮件存储服务器上配置的收件箱文件夹名称。
- **邮件存储垃圾桶文件夹名称**：在邮件存储服务器上配置的垃圾桶文件夹名称（通常为“已删除项目”文件夹）。

步骤 6 选择**保存**。

配置 Cisco Unified Communications Manager 集成

过程

步骤 1 选择**配置选项卡** > **其他服务** > **统一通信**。

步骤 2 选择**群集**选项卡，然后选择**添加**。

步骤 3 选择**启用 Cisco UC Manager 与 Messenger 服务客户端集成**。

步骤 4 选择**允许用户手动输入设置**，用户可以在基本模式下更改主服务器值，或在高级模式下更改 TFTP/CTI/CCMCIP 服务器值。

注释 启用此选项后，用户输入的设置将覆盖为 Cisco Webex 组织指定的 Cisco Unified Communications Manager 默认或全局设置。

步骤 5 在 **Cisco Unified Communications Manager 服务器设置**下，选择：

- **基本服务器设置**：为 Cisco Unified Communications Manager 服务器输入基本设置。
- **高级服务器设置**：为 Cisco Unified Communications Manager 服务器输入详细设置。

注释 服务器配置选项的更改基于“基本”或“高级”选项。

步骤 6 为**基本服务器设置**输入以下值：

- **主服务器**：输入 Cisco Unified Communications Manager 主服务器的 IP 地址。此服务器配置有 TFTP、CTI 和 CCMCIP 设置。
- **备用服务器**：输入 Cisco Unified Communications Manager 备用服务器的 IP 地址。此服务器配置有 TFTP、CTI 和 CCMCIP 设置，并在 Unified Communications Manager 主服务器发生故障时提供故障转移支持。

步骤 7 如果选择了**高级服务器设置**，则请指定 TFTP（简单文件传输协议）、CTI（计算机电话集成）和 CCMCIP（Cisco Unified Communications Manager IP 电话）服务器的每项设置。

步骤 8 输入以下每个服务器的 IP 地址：

注释　您最多可以为一个 TFTP 服务器指定两个备份服务器，为 CTI 和 CCMCIP 服务器指定一个备份服务器。输入每个备份服务器输入的相应 IP 地址。

- **TFTP 服务器**
- **CTI 服务器**
- **CCMCIP 服务器** — 这是 Cisco Unified Communications Manager (UDS) 服务器的地址。

列出的服务器必须位于用户的主群集中。

步骤 9　在**语音邮件引导号码**框中，输入 Cisco Unified Communications 服务器中的语音留言服务号码。

组织管理员通常会为整个 Cisco Webex 组织提供默认的语音留言服务号码。但是，您可以选择**允许用户手动输入设置**复选框，以使群集的用户能够覆盖此默认语音留言服务号码。

步骤 10　选择**语音邮件**。

步骤 11　选择**启用可视语音邮件**。

此处输入的可视语音邮件设置仅适用于属于此群集的用户。

步骤 12　在**群集**选项卡中，选择**此群集的特定语音邮件服务器**以指定语音邮件服务器（与为整个组织提供的语音邮件服务器设置不同）。

步骤 13　选择**允许用户手动输入设置**以允许用户为此群集手动输入可视语音邮件设置。

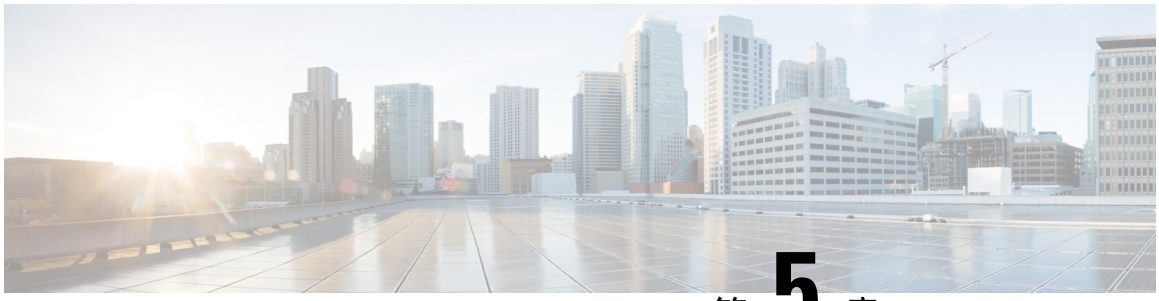
步骤 14　请输入以下信息：

语音邮件服务器	输入语音邮件服务的 IP 地址中或 FQDN
语音邮件协议	选择 HTTP 或 HTTPS。
语音邮件端口	输入端口号

邮件存储服务器信息不受支持，Cisco Webex 管理工具需要此字段的值，请输入`10.0.0.0`。“邮件存储协议”、“端口”和 "IMAP 空闲过期时间" 字段不受支持，请勿删除这些字段中的默认值。

邮件存储收件箱文件夹名称	在邮件存储服务器上配置的收件箱文件夹名称
邮件存储垃圾桶文件夹名称	在邮件存储服务器上配置的“垃圾桶”或“已删除项目”文件夹的名称

步骤 15　选择**保存**。



第 5 章

为云部署创建用户

“创建用户”工作流程

Cisco Webex 管理工具提供多种为组织创建用户的方式。

过程

	命令或操作	目的
步骤 1	使用以下方法之一在 Cisco Webex 管理工具中创建用户： • 您可以使用 Cisco Webex 管理工具逐个添加用户。 创建新用户， 第 16 页 • 您可以生成电子邮件邀请，让用户自行注册 Cisco Webex 帐户。 用户设置信息， 第 16 页 • 创建并导入一个列有用户信息的 CSV 文件。 创建并导入 CSV 文件， 第 17 页	
步骤 2	将用户分配到策略组。 将用户分配给策略， 第 21 页	

创建新用户

过程

步骤 1 要创建新用户或管理员，请选择**用户选项卡** > **添加**。

步骤 2 在每个字段中输入信息。默认角色为“用户”（非管理员）。

注释 用户名是企业电子邮箱。您无法编辑用户名。

步骤 3 （可选）选择**策略组分配**选项卡，为用户分配策略组。

步骤 4 如果对 Cisco Webex Messenger 组织启用“IM 存档”，**添加用户**对话框中将显示**存档 IM** 复选框。要记录此用户的 IM 以进行存档，请选中**存档 IM** 复选框。

步骤 5 要更改端点，请从下拉列表中选择不同的端点。
若选择**默认**，将为用户分配 **IM 存档**屏幕中预配置为默认端点的端点。

步骤 6 要将此用户分配到升级站点，请从**升级站点**下拉列表中选择一个站点。

步骤 7 如果您 Cisco Webex Messenger 组织支持 Cisco Unified Communications，则“添加用户”对话框中将显示“统一通信”选项卡。选择**统一通信**选项卡以查看可用于 Cisco Unified Communications 的设置。

步骤 8 在**群集**下，选择要将此用户添加到的相应 Cisco Unified Communications 群集。

步骤 9 如果您 Cisco Webex Messenger 组织支持 Cisco Webex 会议中心集成，则会显示“添加用户”对话框。若要为用户分配组织管理员角色，请选中**组织管理员**复选框。

注释
- 如果您在**会议**页面中创建新用户时已启用了**自动启用会议帐户**，则默认会选中**会议帐户**复选框。在这种情况下，您无法取消选中“会议帐户”复选框。
- 选中**会议帐户**复选框时，表示为此用户创建相应的 Cisco Webex 会议中心帐户。

步骤 10 选择**保存**。

新用户将收到一封基于 Cisco Webex Messenger 管理工具中“欢迎电子邮件”模板的欢迎电子邮件。

步骤 11 重复前面的步骤以继续添加新用户。

用户设置信息

用户设置包括指定用户部署信息（例如注册），以及创建用户配置文件时的必填字段。您在此处进行的设置会影响 Cisco Webex Messenger 组织中设置的用户。例如，如果您在此处将特定的字段设置为必填，则在创建用户配置文件时，用户必须填写这些字段。

Cisco Webex Messenger 当未启用 SAML 或目录集成时，客户可以启用自助注册。在这种情况下，组织管理员无需指定注册 URL。未启用注册时，客户可以指定自定义网页。尝试使用与客户所在域匹

配的电子邮件地址注册的任何用户都将重定向到“自定义”网页。客户可以使用此网页显示创建新 Cisco Webex Messenger 帐户所需的内部流程的相关信息。

例如：

□□□ Cisco Webex Messenger □□□□□□□□□□□ ithelpdesk@mycompany.com □□□ +1 800 555 5555□

输入用户设置信息

过程

步骤 1 要输入用户配置信息，请在**配置**选项卡下选中**系统设置** > **用户设置**。

步骤 2 要允许用户通过 Cisco Jabber 应用程序自助注册帐户，请选择**允许用户使用注册页面**Cisco Webex**自助注册**。

“自助注册”页面的 URL 为 www.webex.com/go/wc。Cisco Webex Messenger 组织管理员通常会提供此 URL。

注释 如果未选中“允许用户使用 Cisco Webex 注册页面自助注册”，将会显示“自助注册 URL”字段和“自定义消息”框。在这种情况下，您需要输入“自定义用户注册”页面的 URL。

步骤 3 在**自定义注册 URL**字段中，输入自定义自助注册页面的 URL。

如果不输入自定义 URL，将会显示以下自助注册页面（默认）URL：www.webex.com/go/wc。

步骤 4 在**自定义**消息框中，输入自定义自助注册页的说明。

步骤 5 若要在每次用户使用“自助注册”页面注册时通过电子邮件通知组织管理员，请选择**当用户使用 Cisco Webex 注册页面自助注册时向管理员发送通知**。

步骤 6 在**设置用户简档的必填字段**下，选择每次创建或查看用户配置文件时强制显示的字段。在您每次执行以下操作时总是会显示这些：

- 创建新用户
- 更改现有用户简档
- 从 CSV 文件导入用户

步骤 7 选择**保存**。

创建并导入 CSV 文件

您可以轻松地将大量用户通过逗号分隔值 (CSV)文件导入到您 Cisco Webex Messenger 的组织中。同样，您也可以将用户导出为 CSV 文件。导入是一种非常有用的方式，可以轻松地向您的组织添加大量用户，从而节省手动添加每个用户的工作量。

导入完成后，发起导入的组织管理员将收到关于导入状态的电子邮件。该电子邮件将说明导入是成功、失败还是被终止。

CSV 文件导入后，用户会显示在**用户**选项卡中。

CSV 字段

注意：无法使用 CSV 导入过程创建组织管理员和用户管理员。

在将用户导入 Cisco Webex 之前，CSV 文件中应包含以下字段（无任特定顺序）。有些字段是必填字段，必须在这些字段中输入信息，而有些字段是选填字段。

注意：如果不想在字段中输入信息，您可以输入字符“-”，然后将其作为空白字段导入到数据库中。您只能为选填字段执行此操作。如果在必填字段中输入“-”，则会在导入时报告错误。请勿使用值 N/A。

字段名称	说明
employeeID	必填（仅在已启用 *SSO* 时）输入用户的 ID。
displayName	选填输入用户的显示名称。
firstName	必填输入用户的名字。
lastName	必填输入用户的姓氏。
邮件	必填输入用户的电子邮件地址。
userName	必填以 user@email.com 格式输入用户的用户名。
jobTitle	选填输入用户的职务或称号。
address1	选填输入用户地址的第一行。组织管理员可以配置此字段，使其成为用户必填字段。
address2	选填输入用户地址的第二行。组织管理员可以配置此字段，使其成为用户必填字段。
城市	选填输入用户居住的城市。组织管理员可以配置此字段，使其成为用户必填字段。
state	选填输入用户居住的州/省。组织管理员可以配置此字段，使其成为用户必填字段。
zipCode	选填输入用户的邮政编码。组织管理员可以配置此字段，使其成为用户必填字段。

字段名称	说明
ISOcountry	选填输入用户居住的国家/地区代码（两个字母），例如 IN、US、CN。有关详细信息，请参阅 http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm。组织管理员可以配置此字段，使其成为用户必填字段。
phoneBusinessISOCountry	选填输入用户办公电话号码的国家/地区代码，例如 IN、US、CN。组织管理员可以配置此字段，使其成为用户必填字段。
phoneBusinessNumber	选填输入用户的办公电话号码。组织管理员可以配置此字段，使其成为用户必填字段。
phoneMobileISOCountry	选填输入用户手机号码的国家/地区代码，例如 IN、US、CN。组织管理员可以配置此字段，使其成为用户必填字段。
phoneMobileNumber	选填输入用户的手机号码。组织管理员可以配置此字段，使其成为用户必填字段。
传真	选填输入用户的传真号码。
PolicyGroupName	选填输入用户所属的默认策略组。
userProfilePhotoURL	选填输入可访问用户简档图片的 URL。
activeConnect	选填指示用户在 Cisco Webex 中状态是否为**活跃**输入**是**表示**活跃**状态，输入**否**表示**不活跃**状态。
中心	选填用于分配（是）或移除（否）Cisco Jabber 应用程序用户的中心帐户。仅可指定一个中心。
storageAllocated	选填输入分配给用户的存储空间 (MB)。 此值必须为一个数值
CUCMClusterName	选填输入用户所属的 Cisco Unified Communications Manager 群集名称。
businessUnit	选填输入用户所在的业务部门或部门。组织管理员可以配置此字段，使其成为用户必填字段。
IMLoggingEnable	选填指示是否对此用户启用 IM 记录。输入 **True** 表示**已启用**，输入 **False** 表示**已禁用**。
endpointName	选填输入为记录 IM 而配置的端点名称。

字段名称	说明
autoUpgradeSiteName	选填输入升级站点名称。

注释 您可以使用以制表符或逗号分隔的CSV文件。确保您的CSV文件以UTF-8或UTF16-LE格式编码。

选择 UTF-8 作为编码格式

过程

步骤 1 在 Microsoft Excel 中选择**文件 > 另存为**。

步骤 2 在**另存为**对话框中，选择**工具和 Web 选项**。

步骤 3 在 **Web 选项**对话框中，选择**编码**选项卡。

步骤 4 在**将此文档另存为**列表中，选择 **UTF-8**。

步骤 5 选择**确定**，返回**另存为**对话框。

步骤 6 从**另存为类型**列表中，选择 **CSV（逗号分隔）(*.csv)**。

步骤 7 在**文件名**字段中，输入 CSV 文件的名称，然后选择**保存**。

导入和导出用户

过程

步骤 1 要从 CSV 文件导入用户，请在 Cisco Webex Messenger 管理工具中，选择**用户选项卡 > 更多操作 > 导入/导出**。

步骤 2 选择**浏览**，然后选择包含您要导入的用户列表的 CSV 文件。

步骤 3 选择**导入**以开始导入过程。

步骤 4 要导出用户，请在**导入/导出用户**对话框中选择**导出**。

进度消息指示导出过程的进度。

步骤 5 要查看包含导出用户的 CSV 文件，请选择导出消息的时间戳。
此时将显示确认提示。该消息类似于以下示例：上次导出时间：`2009-06-24 09:02:01`。

步骤 6 选择**打开**以查看包含您的 Messenger 组织用户的 CSV 文件。或者，选择**保存**以将 CSV 文件保存到本地计算机。

将用户分配给策略

过程

步骤 1 要将用户分配到策略组，请选择**用户**选项卡。

步骤 2 如果要为新用户分配策略组，请选择**添加**以首先创建新用户。

步骤 3 如果要为现有用户分配策略组，请搜索该用户。

步骤 4 在搜索结果中，双击相应的用户名称以打开**编辑用户**对话框。

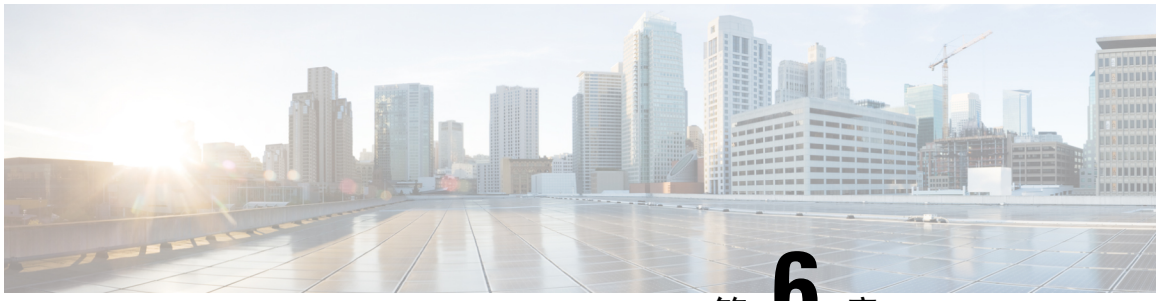
步骤 5 选择**策略组分配**选项卡以打开 **策略组分配**对话框。

步骤 6 在**搜索**字段中，输入要搜索并分配给此用户的策略组的至少一个字母。

步骤 7 选择**搜索**。

步骤 8 在**搜索结果**窗口中，选择相应的策略组，然后选择**分配**以将策略分配给此用户。

步骤 9 选择"保存" 以保存策略组分配，然后返回"用户" 选项卡。



第 6 章

在 Unified Communications Manager 上创建用户

启用同步

要确保目录服务器中的联系人数据复制到 Cisco Unified Communications Manager，必须与目录服务器同步。您必须启用同步，然后才能与目录服务器同步。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**系统** > **LDAP** > **LDAP 系统**。

LDAP 系统配置窗口将会打开。

步骤 3 找到 **LDAP 系统信息**部分。

步骤 4 选择从 **LDAP 服务器启用同步**。

步骤 5 从 **LDAP 服务器类型**下拉列表中，选择您从中同步数据的目录服务器类型。

下一步做什么

为用户 ID 指定 LDAP 属性。

为用户 ID 指定 LDAP 属性

您从目录源同步到 Cisco Unified Communications Manager 时，您可以从目录属性填充用户 ID。保存用户 ID 的默认属性为 sAMAccountName。

过程

步骤 1 在 **LDAP 系统配置**窗口中找到**用户 ID 的 LDAP 属性**下拉列表。

步骤 2 根据需要为用户 ID 指定属性，然后选择**保存**。

重要事项 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。

指定目录 URI 的 LDAP 属性

在 Cisco Unified Communications Manager 版本 9.0 (1) 和更高版本中，您可以从目录中的属性填充目录 URI。

开始之前

启用同步。

过程

步骤 1 选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 选择相应的 LDAP 目录，或选择**新增**以添加 LDAP 目录。

步骤 3 找到**要同步的标准用户字段**部分。

步骤 4 从**目录 URI** 下拉列表中选择以下 LDAP 属性之一：

- **msRTCSIP-primaryuseraddress** — 使用 Microsoft Lync 或 Microsoft OCS 时，此属性将填充到 AD 中。这是默认属性。
- **mail**

步骤 5 选择保存。

执行同步

在添加目录服务器和指定所需的参数之后，您可以同步 Cisco Unified Communications Manager 和目录服务器。

过程

步骤 1 选择系统 > LDAP > LDAP 目录。

步骤 2 选择新增。

LDAP 目录窗口将会打开。

步骤 3 在 LDAP 目录窗口中指定所需的详细信息。

有关您可以指定的值和格式的详细信息，请参阅《Cisco Unified Communications Manager 管理指南》。

步骤 4 创建 LDAP 目录同步计划，以确保您的信息定期同步。

步骤 5 选择保存。

步骤 6 选择立即执行完全同步。

注释 完成同步过程所需的时间取决于在您目录中存在的用户数。如果您同步有成千上万个用户的大目录，则此过程需要一些时间。

目录服务器中的用户数据会与 Cisco Unified Communications Manager 数据库同步。Cisco Unified Communications Manager 然后会同步用户数据与在线状态服务器数据库。

分配角色和组

对于所有部署类型，将用户分配到标准 CCM 最终用户组。

过程

步骤 1 打开 Cisco Unified CM 管理界面。

步骤 2 选择用户管理 > 最终用户。
查找并列出用户窗口将会打开。

步骤 3 从列表中查找并选择用户。

最终用户配置窗口将会打开。

步骤 4 找到**权限信息**部分。

步骤 5 选择**添加至访问控制组**。
查找并列出访问控制组对话框将会打开。

步骤 6 为用户选择访问控制组。

您至少应该将用户分配到以下访问控制组：

- **标准 CCM 最终用户**
- **启用标准 CTI** — 此选项用于桌面电话控制。

如果您为用户配置安全电话功能，则不要将用户分配到**标准 CTI 安全连接**组。

某些电话型号需要其他控制组，如下所示：

- 对于 Cisco Unified IP Phone 9900、8900、8800 或 DX 系列，选择**标准 CTI 允许控制支持已连接转接和会议的电话**。
- 对于 Cisco Unified IP Phone 6900 系列，选择**标准 CTI 允许控制支持跳转模式的电话**。

步骤 7 选择**添加选定项**。
查找并列出访问控制组窗口将会关闭。

步骤 8 在**最终用户配置**窗口中选择**保存**。

认证选项

在客户端中启用 SAML SSO

开始之前

- 在 Cisco Unity Connection 版本 10.5 上启用 SSO — 有关对此服务启用 SAML SSO 的详细信息，请参阅 在 *Cisco Unity Connection* 中管理 *SAML SSO*。
- 对 Cisco Webex Messenger 服务启用 SSO 以支持 Cisco Unified Communications 应用程序和 Cisco Unity Connection。

  有关对此服务启用 SAML SSO 的详细信息，请参阅*Cisco Webex Messenger*管理员指南中的“单点登录”。

过程

步骤 1 在所有服务器上部署证书，以便 Web 浏览器能够验证证书，否则用户将收到关于无效证书的警告消息。有关证书验证的详细信息，请参阅证书验证。

步骤 2 确保客户端中已启用 SAML SSO 服务发现。客户端使用标准服务发现在客户端中启用 SAML SSO。通过使用以下配置参数启用服务发现：ServicesDomain、VoiceServicesDomain 和 ServiceDiscoveryExcludedServices。有关如何启用服务发现的详细信息，请参阅为*Remote Access*配置服务发现。

步骤 3 定义会话的持续时间。

会话由Cookie和令牌值组成。Cookie的持续时间通常比标记长。Cookie的生存期在标识提供商中定义，并且令牌的持续时间在服务中定义。

步骤 4 启用 SSO 后，所有 Cisco Jabber 用户默认使用 SSO 登录。管理员可为每个用户更改此设置，以便某些用户不使用 SSO，而是使用其 Cisco Jabber 用户名和密码登录。要为 Cisco Jabber 用户禁用 SSO，请将 SSO_Enabled 参数的值设置为 FALSE。

如果您已将 Cisco Jabber 配置为不要求用户提供电子邮件地址，则其第一次登录到 Cisco Jabber 时可能是非 SSO 登录。在某些部署中，参数 ServicesDomainSsoEmailPrompt 需要设置为 ON。这可确保 Cisco Jabber 具有执行第一次 SSO 登录所需的信息。如果用户之前登录到 Cisco Jabber，则不需要此提示，因为需要提供必要的信息。

有关将 SSO 与 Unified CM 集成（以便 Webex Teams 用户能够使用一组凭证进行登录）的详细信息，请参阅 *Cisco Unified Communications* 应用程序的 *SAML SSO* 部署指南。

通过 LDAP 服务器验证身份

如果要启用 LDAP 验证，请执行此程序，以便根据公司 LDAP 目录中分配的密码对最终用户密码进行验证。LDAP 验证使得系统管理员能够为最终用户分配一个适用于所有公司应用程序的密码。此配置仅适用于最终用户密码，不适用于最终用户 PIN或应用程序用户密码。当用户登录到客户端时，在线状态服务会将身份验证路由到 Cisco Unified Communications Manager。Cisco Unified Communications Manager 随后会将该验证发送到目录服务器。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

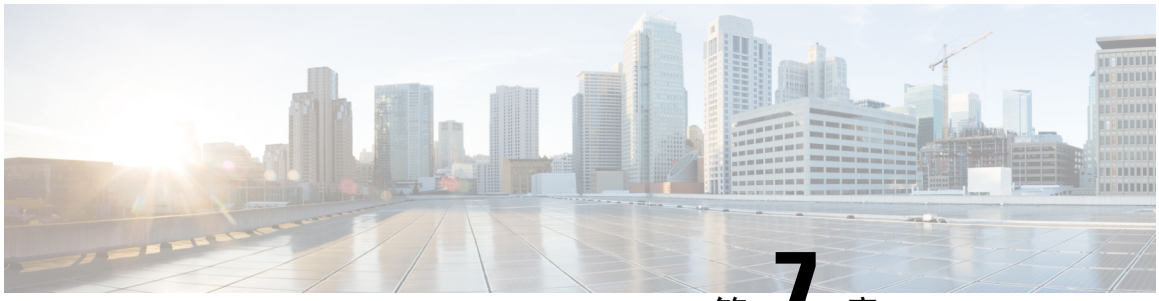
步骤 2 选择 **系统** > **LDAP** > **LDAP 身份验证**。

步骤 3 选择**为最终用户使用 LDAP 身份验证**。

步骤 4 根据需要指定 LDAP 凭证和用户搜索库。

有关 **LDAP 身份验证**的详细信息，请参阅 *Cisco Unified Communications Manager* 管理指南。

步骤 5 选择**保存**。



第 7 章

配置桌面电话控制

先决条件

Cisco CTIManager 服务必须在 Cisco Unified Communications Manager 群集中运行。

配置桌面电话控制任务流

过程

	命令或操作	目的
步骤 1	启用 CTI 设备， 第 30 页	允许 Cisco Jabber 桌面客户端控制用户的桌面电话。
步骤 2	配置桌面电话视频， 第 30 页.	让用户通过客户端接收那些传输到其计算机上桌面电话设备的视频。
步骤 3	启用视频速率调整， 第 31 页	客户端通过视频速率调整来协调最佳视频质量。
步骤 4	配置用户关联， 第 33 页	将用户与设备关联并将用户分配到访问控制组。
步骤 5	重置设备， 第 34 页	在配置用户关联后，您必须重置设备。

启用 CTI 设备

如果您希望 Cisco Jabber desktop 客户端能够控制用户的桌面电话，则必须在为用户创建设备时选择**允许从 CTI 控制设备**选项。

过程

步骤 1 在 Cisco Unified CM 管理中，单击**设备** > **电话**，搜索电话。

步骤 2 在**设备信息**部分，选择**允许从 CTI 控制设备**。

步骤 3 单击**保存**。

配置桌面电话视频

借助桌面电话视频功能，您能够在笔记本电脑上接收视频视频信号，在桌面电话上接收音频信号。通过计算机端口将计算机物理连接到桌面电话，以便客户端建立与 Jabber 客户端的连接。此功能不能通过无线方式连接到您的桌面电话。

注释 如果您同时建立了无线连接和有线连接，则应配置 Microsoft Windows，以使无线连接的优先级低于有线连接。参阅 Microsoft 的 用于互联网协议路由的 *Automatic Metric* 功能的说明，了解更多信息。

首先，从 Cisco.com 下载并安装 Jabber 桌面电话视频服务界面。Jabber 桌面电话视频服务接口提供 Cisco 探索协议 (CDP) 驱动程序。CDP 允许客户端：

- 发现桌面电话。
- 使用 CAST 协议建立并维护与桌面电话的连接。

桌面电话视频注意事项

在设置桌面电话视频功能前，请查看以下注意事项和限制：

- 您不能使用 CAST 协议连接多个视频设备。使用此功能时，您无法使用带有内置摄像头的桌面电话。如果您的桌面电话有本地 USB 摄像头，请在使用此功能之前将其删除。
- 该功能不适用于不支持 CTI 的设备。
- 您不能同时使用基于 BFCP 协议的视频屏幕共享和桌面电话视频功能。
- 对于使用 SCCP 的端点来说，无法仅接收视频。SCCP 端点必须既发送视频，又接收视频。在 SCCP 端点不发送视频信号的情况下，将会导致仅限音频的呼叫。
- 7900 系列电话必须将 SCCP 用于桌面电话视频功能。7900 系列电话不能将 SIP 用于桌面电话视频功能。

- 如果通过桌面电话设备上的键盘发起呼叫，该呼叫在开始时将作为桌面电话设备上的音频呼叫。之后，Jabber会将此呼叫升级为视频呼叫。因此，您不能对那些不支持升级的设备（例如H.323端点）进行视频呼叫。要在不支持升级的设备上使用此功能，请从 Jabber 客户端开始呼叫。
- 使用固件版本 SCCP45.9-2-1S 的 Cisco Unified IP 电话存在兼容性问题。将固件升级到版本 SCCP45.9-3-1 以使用此功能。
- 某些防病毒或防火墙应用程序（例如 Symantec EndPoint Protection）会阻止传入的 CDP 包。这种情况会禁用桌面电话视频。请配置您的防病毒或防火墙应用程序，使其允许传入的CDP包。

  有关此问题的更多详细信息，请参阅以下Symantec技术文档：*Cisco IP Phone* 版本 *7970* 和 *Cisco Unified Video Advantage* 被网络威胁保护功能阻止。
- 请勿在 Cisco Unified Communications Manager (Unified CM) 的 SIP 干线配置中选中**需要媒体终结点**复选框。该设置将禁用桌面电话视频。

过程

步骤 1 将计算机物理连接到桌面电话上的计算机端口。

步骤 2 在 Unified CM 中启用用于视频的桌面电话。

步骤 3 在您的计算机上安装 Jabber 桌面电话视频服务接口。

桌面电话视频故障诊断

如果您遇到一个错误，指示桌面电话视频功能不可用或桌面电话设备未知，则执行以下操作：

1. 确保在Cisco Unified Communications Manager 中启用用于视频的桌面电话设备。
2. 重置物理桌面电话。
3. 退出客户端。
4. 在安装客户端的计算机上运行 services.msc。
5. 从 Windows 任务管理器的“服务”选项卡重新启动 Jabber 桌面电话视频服务接口。
6. 重新启动客户端。

启用视频速率调整

客户端通过视频速率调整来协调最佳视频质量。视频速率调整会根据网络状况动态提高和降低视频质量。

要使用视频速率调整，您必须在 Cisco Unified Communications Manager 上启用实时传输控制协议 (RTCP)。

注释 默认情况下，在软终端设备上启用 RTCP。不过，您必须在桌面电话设备上启用 RTCP。

在常用电话配置文件中启用 RTCP

您可以在常用电话配置文件中启用 RTCP，以便在使用配置文件的所有设备上启用视频速率调整。

注释 RTCP 是 Jabber 电话服务的有机组成部分。即使禁用，Jabber 仍将继续发送 RTCP 数据包。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **设备设置** > **通用电话配置文件**。

查找并列出常用通用电话配置文件窗口将会打开。

步骤 3 在**查找通用电话配置文件位置**字段中指定适当的过滤器，然后选择**查找**以检索配置文件列表。

步骤 4 从列表中选择适当的配置文件。

通用电话配置文件配置窗口将会打开。

步骤 5 找到**产品特定配置布局**部分。

步骤 6 从 **RTCP** 下拉列表中选择**启用**。

步骤 7 选择**保存**。

在设备配置中启用 RTCP

您可以在特定的设备配置而不是常用电话配置文件中启用 RTCP。特定的设备配置会替代您在常用电话配置文件中指定的任何设置。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **电话**。

查找并列出电话窗口将会打开。

步骤 3 在**查找电话位置**字段中指定适当的过滤器，然后选择**查找**以检索电话列表。

步骤 4 从列表中选择适当的电话。

电话配置窗口将会打开。

步骤 5 找到**产品特定配置布局**部分。

步骤 6 从 **RTCP** 下拉列表中选择**启用**。

步骤 7 选择**保存**。

配置用户关联

当您将用户与设备关联时，应该将该设备提供给用户。

开始之前

创建和配置 Cisco Jabber 设备。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**用户管理** > **最终用户**。

查找并列出用户窗口将会打开。

步骤 3 在**查找用户位置**字段中指定适当的过滤器，然后选择**查找**以检索用户列表。

步骤 4 从列表中选择适当的用户。

最终用户配置窗口将会打开。

步骤 5 找到**服务设置**部分。

步骤 6 从 **UC 服务配置文件**下拉列表中为用户选择相应的服务配置文件。

步骤 7 找到**设备信息**部分。

步骤 8 选择**设备关联**。

用户设备关联窗口将会打开。

步骤 9 选择您要与用户关联的设备。Jabber 仅支持每种设备类型关联一个软终端。例如，只有一个 TCT、BOT、CSF 和 TAB 设备可以与用户关联。

步骤 10 选择**保存选定项/更改**。

步骤 11 选择**用户管理** > **最终用户**，并返回到**查找并列出用户**窗口。

步骤 12 从列表中查找并选择相同的用户。

最终用户配置窗口将会打开。

步骤 13 找到**权限信息**部分。

步骤 14 选择**添加至访问控制组**。

查找并列出访问控制组对话框将会打开。

步骤 15 选择您要将用户分配到的访问控制组。

您至少应该将用户分配到以下访问控制组：

- **标准 CCM 最终用户**
- **已启用标准 CTI**

记住　　如果您为用户提供安全电话功能，请不要将用户分配到**标准 CTI 安全连接**组。

某些电话型号需要其他控制组，如下所示：

- 对于 Cisco Unified IP Phone 9900、8900、8800 或 DX 系列，选择**标准 CTI 允许控制支持已连接转接和会议的电话**。
- 对于 Cisco Unified IP Phone 6900 系列，选择**标准 CTI 允许控制支持跳转模式的电话**。

步骤 16 选择**添加选定项**。

查找并列出访问控制组窗口将会关闭。

步骤 17 在**最终用户配置**窗口中选择**保存**。

重置设备

在创建将用户与设备关联之后，您应该重置这些设备。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **电话**。

查找并列出电话窗口将会打开。

步骤 3 在**查找电话位置**字段中指定适当的过滤器，然后选择**查找**以检索设备列表。

步骤 4 从列表中选择适当的设备。

电话配置窗口将会打开。

步骤 5 找到**关联信息**部分。

步骤 6 选择适当的目录号码配置。

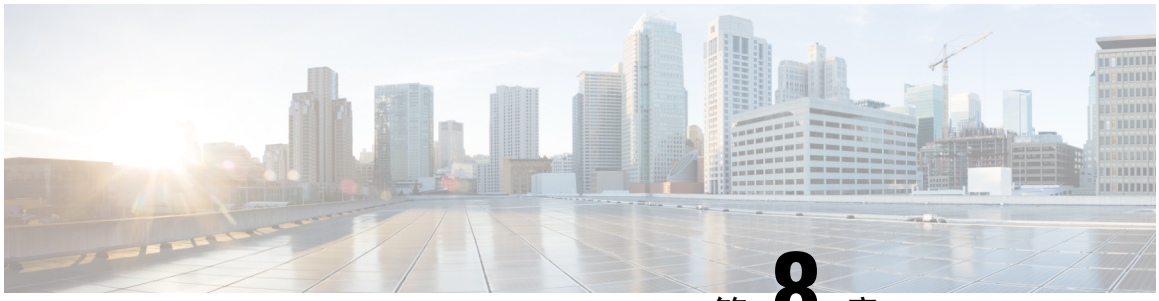
目录号码配置窗口将会打开。

步骤 7 选择**重置**。

设备重置对话框将会打开。

步骤 8 选择**重置**。

步骤 9 选择**关闭**以关闭**设备重置**对话框。



第 8 章

配置软终端

创建软终端工作流程

过程

	命令或操作	目的
步骤 1	创建和配置 Cisco Jabber 设备， 第 37 页	为访问 Cisco Jabber 的每位用户至少创建一个设备。生成要为用户提供的身份验证字符串。
步骤 2	将目录号码添加到设备， 第 41 页	对于您创建的每个设备，添加一个目录号码。
步骤 3	将用户与设备关联， 第 41 页	将用户与设备关联。
步骤 4	创建移动 SIP 配置文件， 第 42 页.	如果您使用 Cisco Unified Communications Manager 版本 9 并打算为移动客户端配置设备，请完成此任务。
步骤 5	配置电话安全性配置文件， 第 44 页	完成此任务可为所有设备设置安全电话功能。

创建和配置 Cisco Jabber 设备

为访问 Cisco Jabber 的每位用户至少创建一个设备。一个用户可以有多个设备。

注释 用户只有在使用软终端 (CSF) 设备呼叫时才可以从会议呼叫中删除参与者。

开始之前

- 安装 COP 文件。
- 创建 SIP 配置文件（如果您有 Cisco Unified Communications Manager 版本 9 或更早版本），并且计划为移动客户端配置设备。
- 如果打算为所有设备设置安全电话功能，则创建电话安全性配置文件。
- 如果您使用 CAPF 注册，对于 Cisco Unified Communications Manager 版本 10 或更高版本，请确保**证书颁发机构到端点**的思科证书权限代理功能（CAPF）服务参数值为 **Cisco Certificate Authority Proxy Function**。这是 Cisco Jabber 支持的唯一选项。有关 CAPF 服务参数配置的信息，请参阅 Cisco Unified Communications Manager 安全指南中的更新 *CAPF* 服务参数主题。
- 在为 Cisco Jabber 移动版用户创建 TCT 设备、BOT 设备或 TAB 设备之前，需指定组织的顶级域名以支持 Cisco Jabber 与 Cisco Unified Communications Manager 之间的注册。在 Unified CM 管理界面中，选择**系统** > **企业参数**。在“群集范围域配置”部分中，输入组织的顶级域名。例如 cisco.com。此顶级域名由 Jabber 在注册电话时用作 Cisco Unified Communications Manager 服务器的 DNS 域。例如，CUCMServer1@cisco.com。

过程

步骤 1 登录 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **电话**。
查找并列出电话窗口将会打开。

步骤 3 选择**新增**。

步骤 4 从**电话类型**下拉列表中，选择适用于所配置设备类型的选项，然后选择**下一步**。

对于 Jabber 用户，虽然您可以为每位用户创建多个设备，但只能为每个用户创建一种设备类型。例如，您可以创建一个平板设备和一个 CSF 设备，但不能创建两种 CSF 设备。

- **Cisco Unified Client Services Framework** — 若要为 Cisco Jabber Mac 版本或 Cisco Jabber Windows 版本创建 CSF 设备，请选择此选项。
- **Cisco Dual Mode for iPhone** — 若要为 iPhone 创建 TCT 设备，请选择此选项。
- **Cisco Jabber 平板电脑版本** — 若要为 iPad 或 Android 平板电脑或 Chromebook 创建 TAB 设备，请选择此选项。
- **Cisco 双模 Android 版本** — 若要为 Android 设备创建 BOT 设备，请选择此选项。

步骤 5 从**所有者用户 ID** 下拉列表中，选择您要为其创建设备的用户。

对于电话模式部署中的 **Cisco Unified Client Services Framework** 选项，请确保选择该**用户**。

步骤 6 在**设备名称**字段中，使用适用的格式指定设备名称：

如果您选择	所需格式
Cisco Unified Client Services Framework	• 有效字符：a – z、A – Z、0 – 9。 • 不超过 15 个字符。
Cisco Dual Mode for iPhone	• 设备名称必须以 *TCT* 开头。 例如，您为用户 Tanya Adams 创建 TCT 设备，则输入 **TCTTADAMS**。 • 必须为大写。 • 有效字符：A – Z、0 – 9、句点 (.)、下划线 (_)、连字符 (-)。 • 不超过 15 个字符。
Cisco Jabber 平板电脑版	• 设备名称必须以 *TAB* 开头。 例如，您为用户 Tanya Adams 创建 TAB 设备，则输入 **TABTADAMS**。 • 必须为大写。 • 有效字符：A – Z、0 – 9、句点 (.)、下划线 (_)、连字符 (-)。 • 不超过 15 个字符。
适用于 **Android** 的 **Cisco** 双模	• 设备名称必须以 *BOT* 开头。 例如，您为用户 Tanya Adams 创建 BOT 设备，则输入 **BOTTADAMS**。 • 必须为大写。 • 有效字符：A – Z、0 – 9、句点 (.)、下划线 (_)、连字符 (-)。 • 不超过 15 个字符。

步骤 7 如果您使用 CAPF 注册，请完成以下步骤以生成身份验证字符串：

1. 用户可以使用您提供的身份验证字符串来访问其设备并安全地注册到 Cisco Unified Communications Manager，导航到**证书权限代理功能 (CAPF) 信息**部分。
2. 在**证书操作**下拉列表中，选择**安装/升级**。
3. 从**身份验证模式**下拉列表中，选择**按身份验证字符串**或**按空字符串**。不支持为 JVDI 和 Jabber Windows 版本的 CSF 设备使用**按空字符串** CAPF 身份验证模式。这会导致 Jabber 注册 Cisco Unified Communications Manager 失败。

4. 单击**生成字符串**。身份验证字符串会自动填充字符串值。这是您将为最终用户提供的字符串。
5. 在**密钥大小（位）**下拉列表中，选择您在电话安全性配置文件中设置的相同密钥大小。
6. 在**操作完成时间**字段中，指定验证字符串的到期值或使用默认值。
7. 如果您使用的是组配置文件，请在**桌面客户端设置**的**思科支持字段**中指定。Cisco Jabber 不会使用**桌面客户端设置**中提供的任何其他设置。

步骤 8 选择**保存**。

步骤 9 单击**应用配置**。

下一步做什么

将目录号码添加到设备。

为用户提供验证字符串

如果您使用 CAPF 注册配置安全电话，则必须为用户提供身份验证字符串。用户必须在客户端界面中指定身份验证字符串，才能访问其设备，并安全地注册 Cisco Unified Communications Manager。

用户在客户端界面中输入验证字符串之后，CAPF 注册过程才开始。

注释 完成注册过程所需的时间可能因用户计算机或移动设备以及 Cisco Unified Communications Manager 的当前负荷而异。客户端完成 CAPF 注册过程可能最多需要一分钟。

如果出现以下情况，客户端会显示错误：

- 用户输入不正确的验证字符串。

  用户可以尝试再次输入验证字符串，以完成 CAPF 注册。不过，如果用户继续输入不正确的验证字符串，即使字符串是正确的，客户端也可能会拒绝用户输入的任何字符串。在此情况下，您必须在用户设备上生成新的身份验证字符串，然后将其提供给用户。

- 在**操作完成时间**字段中设置的到期时间之前，用户没有输入身份验证字符串。

  在此情况下，您必须在用户设备上生成新的身份验证字符串。然后，用户必须在到期时间之前输入该身份验证字符串。

重要事项 在 Cisco Unified Communications Manager 中配置最终用户时，必须将其添加到以下用户组：

- **标准 CCM 最终用户**
- **标准 CTI 已启用**

用户不得属于“标准 CTI 安全连接”用户组。

将目录号码添加到设备

在创建和配置每个设备后，您必须为设备添加一个目录号码。本主题提供有关使用**设备** > **电话**菜单选项添加目录号码的说明。

开始之前

创建设备。

过程

步骤 1 在**电话配置**窗口中找到**关联信息**部分。
步骤 2 单击**添加新目录号码**。
步骤 3 在**目录号码**字段中指定目录号码。
步骤 4 在**与线路关联的用户**部分中，单击**关联最终用户**。
步骤 5 在**查找用户位置**字段中指定适当的过滤器，然后选择**查找**。
步骤 6 从显示的列表中选择相应用户，然后单击**添加选定用户**。
步骤 7 根据需要指定所有其他必需的配置设置。
步骤 8 选择**应用配置**。
步骤 9 选择**保存**。

将用户与设备关联

仅限 Cisco Unified Communications Manager版本 9.x：当客户端尝试检索用户的服务配置文件时，将首先从 Cisco Unified Communications Manager 获取设备配置文件。然后，客户端可以使用设备配置来获取您为用户应用的服务配置文件。

例如，您可以为 Adam McKenzie 配置名称为 `CSFAKenzi` 的 CSF 设备。当 Adam 登录时，客户端将从 Cisco Unified Communications Manager 检索 `CSFAKenzi.cnf.xml`。然后，客户端会在 `CSFAKenzi.cnf.xml` 中查找以下内容：

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

因此，如果您使用 Cisco Unified Communications Manager 版本 9.x，则应执行以下操作，以确保客户端能够成功检索您要为用户应用的服务配置文件：

- 将用户与设备关联。
- 将设备配置中的**用户所有者 ID** 字段设置为相应用户。如果未设置此值，客户端将检索默认服务配置文件。

开始之前

注释 如果您打算为这些用户使用不同的服务配置文件，请勿将 CSF 与多个用户关联。

过程

步骤 1 将用户与设备关联。

a) 打开 **Unified CM 管理**界面。
b) 选择**用户管理** > **最终用户**。
c) 查找并选择相应用户。
最终用户配置窗口将会打开。
d) 在**设备信息**部分，点击**设备关联**。
e) 根据需要将用户与设备关联。
f) 返回到**最终用户配置**窗口，然后选择**保存**。

步骤 2 在设备配置中设置**用户所有者 ID** 字段。

a) 选择**设备** > **电话**。
b) 查找并选择相应设备。
电话配置窗口将会打开。
c) 找到**设备信息**部分。
d) 选择**用户**作为**所有者**字段的值。
e) 从**所有者用户 ID**字段中选择相应的用户 ID。
f) 选择**保存**。

创建移动 SIP 配置文件

仅当您使用 Cisco Unified Communication Manager 版本 9 并为移动客户端配置设备时，才需要执行此程序。使用为桌面客户端提供的默认 SIP 配置文件。为移动客户端创建和配置设备之前，您必须创

建 SIP 配置文件，以允许 Cisco Jabber 在其于后台运行时与 Cisco Unified Communication Manager 保持连接。

如果使用 Cisco Unified Communication Manager 版本 10，则在为移动客户端创建和配置设备时，选择默认配置文件**移动设备标准 SIP 配置文件**。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **设备设置** > **SIP 配置文件**。

查找并列出 SIP 配置文件窗口将会打开。

步骤 3 执行以下操作之一以新建 SIP 配置文件：

- 查找默认的 SIP 配置文件，并创建您可以编辑的副本。
- 选择**新增**以创建新的 SIP 配置文件。

步骤 4 在新的 SIP 配置文件中，设置以下值：

- **计时器注册增量** = 120
- **计时器注册过期** = 720
- **计时器保持活动过期** = 720
- **计时器预订过期** = 21600
- **计时器预订增量** = 15

步骤 5 选择**保存**。

设置系统 SIP 参数

如果您连接到低带宽网络并且发现很难在移动设备上接听来电，则可以设置系统 SIP 参数以改善这种情况。增大“SIP 双模警报计时器”值，以确保对 Cisco Jabber 分机的呼叫不会过早路由到移动网络电话号码。

开始之前

此配置仅适用于移动客户端。

Cisco Jabber 必须运行才能接收工作呼叫。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**系统** > **服务参数**。

步骤 3 选择节点。

步骤 4 选择 **Cisco CallManager**（活动）服务。

步骤 5 滚动到**群集范围参数**（**系统 - 移动**）部分。

步骤 6 将 **SIP 双模警报计时器**的值增大到 10000 毫秒。

步骤 7 选择**保存**。

注释 如果在增大“SIP 双模警报计时器”的值后，Cisco Jabber 收到的来电仍会被终止并使用“移动连接”转移，则您可以 500 毫秒为单位重新增大 SIP 双模式警报计时器的值。

配置电话安全性配置文件

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。

开始之前

- 使用 Cisco CTL 客户端配置 Cisco Unified Communications Manager 安全模式。至少要选择混合模式安全。

  有关如何使用 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。

- 对于会议呼叫，确保会议桥支持安全电话功能。如果会议桥不支持安全电话功能，则向该会议桥呼叫不安全。同样，所有参与方的客户端都必须支持通用加密算法，以便在电话会议中加密媒体。

- 如果您的部署使用 Unified Communications Manager 12.5 或更高版本，我们建议将 SIP OAuth 与 Cisco Jabber 配合使用。详细信息，请参阅《*Cisco Unified Communications Manager* 功能配置指南》 (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html) 中的 SIP OAuth 章节。

过程

步骤 1 在 **Cisco Unified Communications Manager** 中，选择**系统** > **安全性** > **电话安全性配置文件**。

步骤 2 选择**新增**。

步骤 3 从**电话类型**下拉列表中，选择适用于所配置设备类型的选项，然后选择**下一步**。

- **Cisco Unified 客户端服务框架** — 若要为 Cisco Jabber Mac 版本或 Cisco Jabber Windows 版本创建 CSF 设备，请选择此选项。
- **Cisco 双模 iPhone 版本**—选择此选项以创建 IPHONE 的 TFT 设备。
- **Cisco Jabber 平板电脑版本** — 若要为 iPad 或 Android 平板电脑或 Chromebook 创建 TAB 设备，请选择此选项。
- **Cisco 双模 Android 版本** — 若要为 Android 设备创建 BOT 设备，请选择此选项。
- **CTI 远程设备** — 若要创建 CTI 远程设备，请选择此选项。

  CTI 远程设备是通过用户的远程目标进行监视和呼叫控制的虚拟设备。

步骤 4 在**电话安全性配置文件配置**窗口的**姓名**字段中，为电话安全性配置文件指定名称。

步骤 5 对于**设备安全模式**，请选择以下选项之一：

- **已验证** — SIP 连接通过使用 NULL-SHA 加密的 TLS 实现。
- **已加密** — SIP 连接通过使用 AES 128/SHA 加密的 TLS实现。客户端使用安全实时传输协议 (SRTP) 提供加密的媒体流。

步骤 6 对于**传输类型**，保留 **TLS** 的默认值。

步骤 7 选中 **TFTP 加密**复选框，以加密 TFTP 服务器上的设备配置文件。

注释 对于 TCT/BOT/平板电脑设备，请勿在此处选中“TFTP 加密配置”复选框。对于身份验证模式，请选择“按身份验证字符串”或“空字符串”。

步骤 8 对于**身份验证模式**，请选择**按身份验证字符串**或**按空字符串**。

注释 不支持为 JVDI 和 Jabber Windows 版本的 CSF 设备使用**按空字符串** CAPF 身份验证模式。这会导致 Jabber 注册 Cisco Unified Communications Manager 失败。

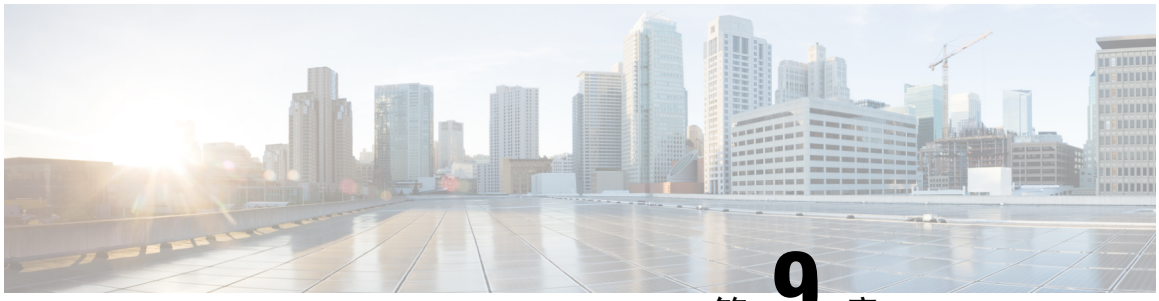
步骤 9 对于**密钥长度（位）**，为证书选择适当的密钥长度。密钥大小是指客户端在 CAPF 注册过程中生成的公钥和私人密钥的位长度。

Cisco Jabber 客户端已使用 1024 位长密钥的身份验证字符串测试过。Cisco Jabber 客户端生成 2048 位长密钥比生成 1024 位长密钥需要的时间长。因此，如果您选择 2048，则需要更长的时间完成 CAPF 注册过程。

步骤 10 对于**SIP 电话端口**，保留默认值。

您在此字段中指定的端口只有在您选择**非安全**作为**设备安全模式**的值时才会生效。

步骤 11 单击**保存**。



第 9 章

配置扩展与连接

配置扩展和连接工作流程

过程

	命令或操作	目的
步骤 1	启用用户移动功能， 第 47 页	启动用户移动功能，您就能够以 CTI 远程设备所有者的身份分配用户。
步骤 2	创建 CTI 远程设备， 第 48 页	创建 CTI 远程设备，这些虚拟设备就能通过用户的远程目标进行监视和呼叫控制。
步骤 3	添加远程目标， 第 49 页	（可选）如果您计划为用户提供专用 CTI 远程设备，就应该通过 Cisco Unified Communications Manager 添加远程目标。

启用用户移动功能

此任务仅适用于桌面客户端。

您必须启用用户移动功能才能提供 CTI 远程设备。如果您不为用户启动移动功能，就无法作为 CTI 远程设备的所有者分配这些用户。

开始之前

此任务仅在以下情况下适用：

- 您计划将 Cisco Jabber Mac 版本或 Cisco Jabber Windows 版本用户分配到 CTI 远程设备。
- 您使用 Cisco Unified Communication Manager 版本 9.x 和更高版本。

过程

步骤 1 选择**用户管理** > **最终用户**。

查找并列出用户窗口将会打开。

步骤 2 在**查找用户位置**字段中指定适当的过滤器，然后选择**查找**以检索用户列表。

步骤 3 从列表中选择用户。

最终用户配置窗口将会打开。

步骤 4 找到**移动功能信息**部分。

步骤 5 选择**启用移动功能**。

步骤 6 选择**保存**。

创建 CTI 远程设备

CTI 远程设备是通过用户的远程目标进行监视和呼叫控制的虚拟设备。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **电话**。

查找并列出电话窗口将会打开。

步骤 3 选择**新增**。

步骤 4 从**电话类型**下拉列表中选择 **CTI 远程设备**，然后选择**下一步**。

电话配置窗口将会打开。

步骤 5 从**所有者用户 ID**下拉列表中选择适当的用户 ID。

注释　只有您为其启用了移动功能的用户才会出现在**所有者用户 ID**下拉列表中。有关详细信息，请参阅在客户端中启用 *SAML SSO*。

Cisco Unified Communications Manager会使用用户 ID 和 **CTIRD**前缀填写**设备名称**字段；例如，**CTIRDusername**

步骤 6 根据需要编辑**设备名称**字段中的默认值。

步骤 7 确保从**协议特定信息部分**的**重新路由呼叫搜索空间**下拉列表中选择适当的选项。

重新路由呼叫搜索空间下拉列表定义用于重新路由的呼叫搜索空间，并确保用户可从 CTI 远程设备发送和接收呼叫。

步骤 8 按需要在**电话配置**窗口中指定所有其他配置设置。

有关详细信息，请参阅 Cisco Unified Communications Manager 系统配置指南文档中的 *CTI* 远程设备设置主题。

步骤 9 选择**保存**。

关联目录号码和添加远程目标的字段在**电话配置**窗口中即变成可用。

添加远程目标

远程目标代表用户可用的 CTI 可控制设备。

如果您计划为用户提供专用 CTI 远程设备，就应该通过**Cisco Unified CM管理** 界面添加远程目标。此任务可确保用户能够在启动客户端时自动控制他们的电话和发出呼叫。

如果您计划为用户提供 CTI 远程设备以及软终端设备和桌面电话设备，就不应该通过 **Cisco Unified CM 管理**界面添加远程目标。用户可以通过客户端界面输入远程目标。

注释

- 您应该为每位用户只创建一个远程目标。不要为一位用户添加两个或更多个远程目标。
- Cisco Unified Communications Manager 不会验证它能否路由您通过 **Cisco Unified CM 管理**界面添加的远程目标。因此，您必须确保 Cisco Unified Communications Manager 可以路由您添加的远程目标。
- Cisco Unified Communications Manager 会自动将应用程序拨号规则应用到 CTI 远程设备的所有远程目标号码。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**设备** > **电话**。

查找并列出电话窗口将会打开。

步骤 3 在**查找电话位置**字段中指定适当的过滤器，然后选择**查找**以检索电话列表。

步骤 4 从列表中选择 CTI 远程设备。

电话配置窗口将会打开。

步骤 5 找到**关联的远程目标**部分。

步骤 6 选择**添加新的远程目标**。

远程目标信息窗口将会打开。

步骤 7 在**名称**字段中指定 JabberRD。

限制 您必须在 **名称**字段中指定 JabberRD。客户端只使用 JabberRD 远程目标。如果您指定除 JabberRD 以外的名称，用户无法访问该远程目标。

当用户通过客户端界面添加远程目标时，客户端会自动设置 JabberRD 名称。

步骤 8 在**目标号码**字段中输入目标号码。

步骤 9 根据需要指定所有其他值。

步骤 10 选择**保存**。

下一步做什么

完成以下步骤以验证远程目标，并将配置应用到 CTI 远程设备：

1. 重复以上步骤，为 CTI 设备打开**电话配置**窗口。
2. 找到**关联的远程目标**部分。
3. 验证远程目标是否可用。
4. 选择**应用配置**。

注释 **电话配置**窗口中的**设备信息**部分包含**活动的远程目标**字段。

当用户在客户端中选择远程目标时，它会显示为**活动的远程目标**的值。

如果是以下情况，**无**会显示为**活动的远程目标**的值：

- 用户没有在客户端中选择远程目标。
- 用户退出或没有登录客户端。

第 10 章

配置远程访问的服务发现

服务发现要求

服务发现允许客户端自动在您的企业网络上检测和查找服务。移动设备和Remote Access的 Expressway 可使您访问企业网络上的服务。您应满足以下要求，以使客户端能够通过移动设备和Remote Access 的 Expressway 进行连接，然后发现服务：

- DNS 要求
- 证书要求
- 测试外部 SRV `_collab-edge`。

DNS 要求

通过Remote Access实现服务发现的 DNS 要求包括：

- 在外部 DNS 服务器上配置 `_collab-edge` DNS SRV 记录。
- 在内部名称服务器上配置`_cisco-uds` DNS SRV 记录。
- 或者，对于 IM 和在线状态服务器和语音服务器的具有不同域的基于云的混合部署，可以配置语音服务域来找到具有 `_collab-edge` 记录的 DNS 服务器。

证书要求

在您配置远程访问之前，请下载 Cisco VCS Expressway 和 Cisco Expressway-E 服务器证书。服务器证书用于 HTTP 和 XMPP。

有关配置 Cisco VCS Expressway 证书的详细信息，请参阅《Cisco vcs Expressway 上的配置证书》 。

测试 _collab-edge SRV 记录

过程

步骤 1 打开命令提示符。

步骤 2 输入**nslookup**。
将显示默认的 DNS 服务器和地址。确认这是预期的 DNS 服务器。

步骤 3 输入 **set type=SRV**。

步骤 4 输入每个 SRV 记录的名称。

例如 `_collab-edge.exampledomain`

- 显示服务器和地址 — 可以访问 SRV 记录。
- 显示 `_collab-edge.exampledomain`：不存在的域 — 您的 SRV 记录存在问题。

第 11 章

设置证书验证

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。

更新配置文件照片 URL

在基于云的部署中，当您添加或导入用户时，Cisco Webex为配置文件照片分配唯一的URL。当Cisco Jabber 解析联系信息时，将通过照片所在处的 URL 从Cisco Webex检索配置文件照片。

配置文件照片URL 使用HTTP 安全（`https://server_name/`）并向客户端出示证书。如果URL 中的服务器名称为：

- 包含Cisco Webex域的完全限定域名 (FQDN) — 客户端可以根据Cisco Webex证书来验证托管配置文件照片的 web 服务器。
- IP 地址 — 客户端无法根据Cisco Webex证书验证托管配置文件照片的 web 服务器。在这种情况下，客户端在配置文件照片 URL 中查找具有 IP 地址的联系人时，会提示用户接受证书。

重要事项

- 我们建议您更新包含 IP 地址作为服务器名称的所有配置文件照片 URL。将 IP 地址替换为包含 Cisco Webex域的 FQDN，以确保客户端不会提示用户接受证书。
- 更新照片时，照片可能需要 24 小时才能在客户端中刷新。

以下步骤介绍如何更新配置文件照片 URL。有关详细说明，请参阅相应的文档。Cisco Webex

过程

步骤 1 使用Cisco Webex管理工具导出 CSV 文件格式的用户联系人数据。

步骤 2 在 **userProfilePhotoURL** 字段中，将 IP 地址替换为Cisco Webex域。

步骤 3 保存 CSV 文件。

步骤 4 使用Cisco Webex管理工具导入 CSV 文件。

第 12 章

配置客户端

客户端配置工作流

过程

	命令或操作	目的
步骤 1	客户端配置简介	
步骤 2	在 *Unified CM* 中设置客户端配置参数（最高优先级）或创建和托管客户端配置文件	
步骤 3	在电话配置中为桌面客户端设置参数	
步骤 4	在电话配置中为移动客户端设置参数	
步骤 5	配置代理设置—可选	

客户端配置简介

Cisco Jabber 可以从以下来源检索配置设置：

- 客户端配置 — 您可以设置用户登录时应用的客户端配置参数，方法是：
  - 使用 Unified CM 设置客户端配置参数。

- 使用包含配置参数的 XML 编辑器创建 XML 文件。然后，您可将 XML 文件托管在 TFTP 服务器上。

- Cisco Webex管理工具 — 您可以使用Cisco Webex管理工具配置一些客户端设置。

  您可以将 `jabber-config.xml` 客户端配置文件上传到Cisco Webex管理工具中。您可以为Cisco Webex Messenger管理工具中的组应用不同的配置文件。成功连接到Cisco Webex Messenger后，客户端会下载 XML 文件并应用这些配置。

  客户端将按以下顺序使用配置设置：

  1. Cisco Webex Messenger管理工具中的设置
  2. 来自Cisco Webex Messenger管理工具的 `jabber-config.xml` 文件中的设置。

     注释 组配置文件设置优先于Cisco Webex Messenger管理工具中的配置文件。

  3. 来自 TFTP 服务器的 `jabber-config.xml` 文件中的设置。

  如果与配置设置有任何冲突，Cisco Webex管理工具中设置的设置将优先于此配置文件。

在 Unified CM 中设置客户端配置参数

对于基于云的部署，使用Cisco Webex管理工具配置客户端。不过，您可以选择设置客户端配置参数以配置客户端，使其设置不会在Cisco Webex管理工具中使用。

对于 Cisco Jabber iPhone 和 iPad 版本以及 Cisco Jabber Android 版本，您必须设置以下参数：

- 内部部署的目录集成。
- 混合云部署的语音邮件服务凭证。

注释 在大多数环境中，Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本不需要任何配置即可连接到服务。只有当您需要自定义内容（例如自动更新、问题报告或用户策略和选项）时，才应设置客户端配置参数。

过程

步骤 1 定义 Jabber 配置参数， 第 57 页

步骤 2 分配 Jabber 客户端配置到服务配置文件， 第 57 页

定义 Jabber 配置参数

通过 Unified CM，您可以添加、搜索、显示和维护有关 UC 服务（包括 Jabber 客户端配置）的信息。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**用户管理** > **用户设置** > **UC 服务**。

步骤 3 选择**新增**。

步骤 4 选择 **Jabber 客户端配置 (jabber-config.xml)** 作为 **UC 服务类型**。

步骤 5 选择**下一步**。

步骤 6 在 **UC 服务信息**部分输入名称，请参阅"Unified CM 帮助"了解更多要求。

步骤 7 在 **Jabber 配置参数**部分输入参数，了解参数相关信息，请参阅最新版本的《*Cisco Jabber* 参数参考指南》。

步骤 8 选择**保存**。

分配 Jabber 客户端配置到服务配置文件

通过 Unified CM，您可以通过服务配置文件为用户分配 Jabber 客户端配置。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**用户管理** > **用户设置** > **服务配置文件**。

步骤 3 选择**新增**或选择要为其分配 Jabber 客户端配置的现有服务配置文件。

步骤 4 在 **Jabber 客户端配置 (jabber-config.xml) 配置文件**部分选择要应用到配置文件的配置的名称。

步骤 5 选择**保存**。

创建并托管客户端配置文件

使用Cisco Webex管理工具配置客户端。不过，您可以选择设置 TFTP 服务器以配置客户端，其设置在Cisco Webex管理工具中不可用。

对于 Cisco Jabber iPhone 和 iPad 版本和 Cisco Jabber Android 版本，您必须创建一个全局配置文件来设置：

- 内部部署的目录集成。

- 混合云部署的语音邮件服务凭证。

注释 在大多数环境中，Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本不需要任何配置即可连接到服务。只有当您需要自定义内容（例如自动更新、问题报告或用户策略和选项）时，才创建配置文件。

开始之前

注意以下配置文件要求：

- 配置文件名区分大小写。在文件名中使用小写字母以避免出现错误，并确保客户端可以从TFTP服务器检索文件。
- 对配置文件使用 UTF-8 编码。
- 客户端无法读取无有效 XML 结构的配置文件。检查关闭元素的配置文件结构以及正确的元素嵌套。
- 仅在配置文件中使用有效的 XML 字符实体参考。例如，使用 `&` 而不是 `&`。如果您的 XML 包含无效字符，客户端就无法解析配置文件。

  要验证您的配置文件，请在 Microsoft Internet Explorer 中打开该文件。

  - 如果 Internet Explorer 显示整个 XML 结构，则您的配置文件是有效的。
  - 如果 Internet Explorer 仅显示部分 XML 结构，则您的配置文件可能包含无效字符或实体。

过程

	命令或操作	目的
步骤 1	指定 TFTP 服务器地址，第 58 页	指定您的TFTP服务器地址，以便客户端可以访问您的配置文件。
步骤 2	创建全局配置，第 59 页	为您部署中的用户配置客户端。
步骤 3	创建组配置，第 60 页	将不同的配置应用到不同的用户组。
步骤 4	托管配置文件，第 61 页	将配置文件托管在任何 TFTP 服务器上。
步骤 5	重新启动您的 TFTP 服务器，第 61 页	重新启动TFTP服务器，方可访问配置文件。

指定 TFTP 服务器地址

客户端从 TFTP 服务器获取配置文件。

过程

	命令或操作	目的
步骤 1	指定您的TFTP服务器地址，以便客户端可以访问您的配置文件。	注意 如果 Cisco Jabber 从 DNS 查询获取 _cisco-uds 记录，它可以自动找到用户的主群集。因此，客户端还可以查找 Cisco Unified Communications Manager TFTP 服务。 如果您部署 _cisco-uds SRV 记录，则无需指定您的 TFTP 服务器地址。

在电话模式中指定 TFTP 服务器

过程

	命令或操作	目的
步骤 1	如果您在电话模式中部署客户端，则可按照以下方式提供 TFTP 服务器的地址： • 在启动客户端时，用户手动输入TFTP服务器地址。 • 您可以在安装期间使用 TFTP 参数指定 TFTP 服务器地址。	

创建全局配置

在登录过程中，客户端会从您的 TFTP 服务器下载全局配置文件。为您部署中的所有用户配置客户端。

开始之前

如果您的配置文件结构无效，客户端将无法读取您设置的值。有关详细信息，请参阅本章中的XML示例。

过程

步骤 1 使用任何文本编辑器创建名为 jabber-config.xml 的文件。

- 在文件名中使用小写字母。

- 使用 UTF-8 编码。

步骤 2 在 `jabber-config.xml` 中定义所需配置参数。

步骤 3 在 TFTP 服务器中托管组配置文件。

如果您的环境有多个 TFTP 服务器，则必须确保所有 TFTP 服务器上的配置文件都相同。

创建组配置

组配置文件适用于用户的子集，并且在 Cisco Jabber 桌面版本（CSF 设备）和 Cisco Jabber 移动设备版本上均受到支持。组配置文件的优先级高于全局配置文件。

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。

开始之前

如果您的配置文件结构无效，客户端将无法读取您设置的值。有关详细信息，请参阅本章中的XML示例。

过程

步骤 1 使用任何文本编辑器创建 XML 组配置文件。

组配置文件可以有任何适当的名称，例如 `jabber-groupa-config.xml`。

步骤 2 在组配置文件中定义需要的配置参数。

步骤 3 将组配置文件添加到适用的 CSF 设备。

a) 打开 **Cisco Unified CM 管理**界面。
b) 选择**设备** > **电话**。
c) 查找并选择组配置所应用的适当 CSF 设备。
d) 在**电话配置**窗口中，浏览到**产品特定配置布局** > **桌面客户端设置**。
e) 在 **Cisco 支持字段**字段中，输入 `configurationfile=`*`group_configuration_file_name.xml`*。例如，输入 `configurationfile=groupa-config.xml`。

注释 如果您在除默认目录以外位置的TFTP服务器上托管组配置文件，就必须指定路径和文件名，例如 `configurationfile=/customFolder/groupa-config.xml`。

请勿添加多个组配置文件。客户端仅使用 **Cisco 支持字段**字段中的第一个组配置。

f) 选择**保存**。

步骤 4 在 TFTP 服务器中托管组配置文件。

托管配置文件

您可将配置文件托管在任何 TFTP 服务器上，使其成为配置文件的主机。但是，我们建议将配置文件托管在设备配置文件所在的 Cisco Unified Communications Manager TFTP 服务器上。

过程

步骤 1 打开 Cisco Unified Communications Manager 上的 **Cisco Unified 操作系统管理** 界面。

步骤 2 选择**软件升级** > **TFTP 文件管理**。

步骤 3 选择**上传文件**。

步骤 4 在**上传文件**部分中选择**浏览**。

步骤 5 在文件系统中选择配置文件。

步骤 6 请勿在**上传文件**部分的**目录**文本框中指定任何值。

您应将**目录**文本框留空，以使配置文件处在 TFTP 服务器的默认目录中。

步骤 7 选择**上传文件**。

重新启动您的 TFTP 服务器

您必须先重新启动 TFTP 服务器，客户端方可访问配置文件。

过程

步骤 1 打开 Cisco Unified Communications Manager 上的 **Cisco Unified 功能配置**界面。

步骤 2 选择**工具** > **控制中心 - 功能服务**。

步骤 3 从 **CM 服务**部分中选择 **Cisco Tftp**。

步骤 4 选择**重新启动**。

此时会显示一个窗口，提示您确认重新启动。

步骤 5 单击**确定**。

将会显示 **Cisco Tftp 服务重新启动操作成功**状态。

步骤 6 选择**刷新**以确保 **Cisco Tftp** 服务成功启动。

下一步做什么

要验证您的 TFTP 服务器是否提供配置文件，请在任何浏览器中打开该配置文件。通常，您可访问位于以下 URL 地址的全局配置文件：
`http://tftp_server_address:6970/jabber-config.xml`

配置文件

有关 *jabber-config* 配置文件结构、组元素、参数和示例的详细信息，请参阅《Cisco Jabber 参数参考指南》。

在电话配置中为桌面客户端设置参数

客户端可以从 Cisco Unified Communications Manager 上的以下位置检索电话配置中的配置设置：

企业电话配置

适用于整个群集。

注释 对于仅具有 IM and Presence Service 功能（仅 IM）的用户，您必须在**企业电话配置**窗口中设置电话配置参数。

通用电话配置文件配置

适用于设备组，并且优先于群集配置。

Cisco Unified 客户端服务框架 (CSF) 电话配置

适用于各 CSF 桌面设备，并且优先于组配置。

电话配置中的参数

下表列出了您可以在电话配置的**产品特定配置布局**部分设置的配置参数，并从客户端配置文件映射对应的参数：

桌面客户端设置配置	说明
视频呼叫	启用或禁用视频功能。 **启用（默认值）** 用户可以发送和接收视频通话。 **禁用** 用户无法发送或接收视频呼叫。 **限制** 此参数仅适用于 CSF 设备配置。
要在文件传输中屏蔽的文件类型	限制用户传输特定的文件类型。 将文件扩展名设置为值，例如 `.exe`。 使用分号分隔多个值，例如 `.exe;.msi;.rar;.zip`

桌面客户端设置配置	说明
自动在电话控制中启动	当客户端第一次启动时，可为用户设置电话类型。在初始启动后，用户可以更改电话类型。然后，客户端保存用户首选项，并在后续启动时使用。 **启用** 使用桌面电话设备进行呼叫。 **禁用（默认值）** 使用软终端 (CSF) 设备进行呼叫。
Jabber Windows 版本软件更新服务器 URL	指定包含客户端更新信息的 XML 文件的 URL。客户端使用此 URL 从您的 Web 服务器检索 XML 文件。 在基于混合云的部署中，您应该使用Cisco Webex管理工具配置自动更新。
问题报告服务器 **URL**	指定可让用户提交问题报告的自定义脚本的 URL。

在电话配置中为移动客户端设置参数

客户端可以从 Cisco Unified Communications Manager 上的以下位置检索电话配置中的配置设置：

- Cisco iPhone 版双模 (TCT) 配置 — 适用于各个 TCT 设备，并且优先于组配置。
- Cisco Jabber 平板电脑版 (TAB) 配置 — 适用于各个 TAB 设备，并且优先于组配置。

电话配置中的参数

下表列出了您可以在电话配置的**产品特定配置布局**部分设置的配置参数，并从客户端配置文件映射对应的参数：

参数	说明
按需 VPN URL	用于启动按需 VPN 的 URL。 **注释** 仅适用于 iOS。
预设 Wi-fi 网络	输入您的组织批准的 Wi-Fi 网络的 SSID。使用正斜线 (/) 分隔 SSID。如果连接到其中一个输入的 Wi-fi 网络，则设备不会连接到安全连接。
默认铃声	将默认铃声设置为**正常**或**响亮**。

参数	说明
视频功能	启用或禁用视频功能。 • 已启用（默认）—用户可以发送和接收视频呼叫。 • 已禁用 — 用户无法发送或接收视频呼叫。
通过办公室拨号 注释　仅限 TCT 和 BOT 设备。	启用或禁用 Dial via Office。 • 已启用 — 用户可以使用 dial via office。 • 已禁用（默认）— 用户无法使用 dial via office。

代理设置的可选配置

您的客户端可能会使用代理设置连接到服务。

对这些 HTTP 请求使用代理时，以下限制适用：

- 不支持代理身份认证。
- 支持绕过列表中的通配符。
- Cisco Jabber 支持使用 HTTP 连接的 HTTP 请求的代理，但使用 HTTPS 连接时不支持代理。
- 不支持 Web 代理自动发现 (WAPD)，必须禁用。

如有必要，请按照以下适用于您的客户端类型的步骤配置代理设置。

配置 Cisco Jabber Windows 版本的代理设置

在 Internet 属性的局域网 (LAN) 设置中配置 Windows 代理设置。

过程

步骤 1 选择**连接**选项卡，然后选择**局域网设置**。

步骤 2 使用以下选项之一配置代理：

- 要使用自动配置，请指定 `.pac` 文件 URL。
- 对于代理服务器，指定一个明确的代理地址。

配置 Cisco Jabber Mac 版本的代理设置

在**系统首选项**中配置 Mac 的代理设置。

过程

步骤 1 选择**系统首选项** > **网络**

步骤 2 从列表中选择您的网络服务，然后选择**高级** > **代理**。

步骤 3 使用以下选项之一配置代理：

- 要使用自动配置，请指定 `.pac` 文件 URL。
- 对于代理服务器，指定一个明确的代理地址。

配置 Cisco Jabber iPhone 和 iPad 版本的代理设置

使用以下方法之一在 iOS 设备的 Wi-fi 设置中配置代理设置：

过程

步骤 1 选择 **Wi-Fi** > **HTTP 代理** > **自动**并指定 `.pac` 文件 URL 作为自动配置脚本。

步骤 2 选择 **Wi-Fi** > **HTTP 代理** > **手动**并指定明确的代理地址。

配置 Cisco Jabber Android 版本的代理设置

过程

使用以下方法之一在 Android 设备的 Wi-fi 设置中配置代理设置：

- 在**Wi-Fi** > **修改网络** > **显示高级选项** > **代理设置** > **自动**选项卡中，将 .pac 文件 URL 指定为自动配置脚本。

  注释 此方法仅适用于安装了 Android OS 5.0 及更高版本的设备和 Cisco DX 系列设备。

- 在**Wi-Fi 网络** > **修改网络** > **显示高级选项** > **代理设置** > **自动**选项卡中，指定明确的代理地址。

第 13 章

部署 Cisco Jabber 应用程序和 Jabber VDI 软终端

附件管理器

附件管理器

Jabber 桌面客户端使用配件管理器来启用与头戴式耳机等配件的交互。配件管理器是一个组件，为配件设备供应商提供 Unified Communication 控制 API。

部分 Cisco 头戴式耳机和其他第三方设备使用这些 API 从设备将音频静音、应答呼叫和结束呼叫。第三方供应商编写了应用程序加载的插件。标准头戴式耳机使用 API 来连接扬声器和麦克风支持。

仅特定设备与附件管理器交互以进行呼叫控制。请联系设备供应商，获取更多信息。配件管理器不支持桌面电话。

附件管理器功能默认启用，通过启用附件管理器参数配置。您可以使用 BlockAccessoriesManager 参数，禁用来自第三方供应商的特定配件管理器插件。

注释 如果在 `jabber-config.xml` 中将 EnableAccessoriesManager 设置为 false，部分头戴式耳机上的呼叫控制按钮将不起作用。

客户端安装程序包括来自供应商的第三方插件。它们安装在 `/Library/Cisco/Jabber/Accessories/` 文件夹中。

支持的第三方供应商：

- Logitech
- Sennheiser
- Jabra
- Plantronics

下载 Cisco Jabber 客户端

如果需要，您可以使用该客户端操作系统上的签名工具将您自己的客户签名添加到 Jabber 安装程序或 Cisco 动态库中。

注释 对于 Cisco Jabber Mac 版本，安装程序包含产品安装程序文件。在添加到安装程序之前，使用终端工具从安装程序提取 `pkg` 文件，并对 `pkg` 文件签名。

过程

从适用的来源下载客户端。

- 访问Cisco 软件中心以下载Cisco Jabber Mac 版本和Cisco Jabber Windows 版本客户端。
- 对于 Cisco Jabber Android 版本，请从 Google Play 中下载应用程序。
- 对于 Cisco Jabber iPhone 和 iPad 版本，从 App store 下载应用程序。

安装 Cisco Jabber Windows 版本

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

安装选项	说明
使用命令行，第 69 页	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，第 85 页	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。

安装选项	说明
创建自定义安装程序，第 85 页	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。
使用组策略进行部署，第 89 页	在同一域中的多个计算机上安装客户端。

开始之前

您必须以本地管理权限登录。

使用命令行

在命令行窗口中指定安装参数。

过程

步骤 1 打开命令行窗口。

步骤 2 输入以下命令：

```
msiexec.exe /i CiscoJabberSetup.msi
```

步骤 3 以“参数=值”配对的形式指定命令行参数。

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

步骤 4 运行命令以安装 Cisco Jabber Windows 版本。

示例安装命令

查看用于安装 Cisco Jabber Windows 版本的命令示例。

Cisco Unified Communications Manager 版本 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

其中：

CLEAR=1 — 删除任何现有引导程序文件。

/quiet — 指定无提示安装。

相关主题

命令行参数，第 70 页
语言的 LCID，第 83 页

命令行参数

查看在安装 Cisco Jabber Windows 版本时可以指定的命令行参数。

相关主题

示例安装命令，第 69 页
语言的 LCID，第 83 页

替代参数

下表说明您必须指定来替代以前所安装的任何现有引导程序文件的参数：

参数	值	说明
CLEAR	1	指定客户端是否替代以前所安装的任何现有引导程序文件。 客户端会将您在安装期间设置的参数和值保存到引导程序文件中。然后，客户端在启动时从引导程序文件加载设置。

如果您指定 CLEAR，在安装期间会发生以下情况：

1. 客户端会删除任何现有的引导程序文件。
2. 客户端会创建新的引导程序文件。

如果您不指定 CLEAR，在安装期间客户端会检查现有的引导程序文件。

- 如果引导程序文件不存在，在安装期间客户端会创建引导程序文件。
- 如果引导程序文件存在，客户端不会替代该引导程序文件，并保留现有设置。

注释 如果您要重新安装 Cisco Jabber Windows 版本，则应考虑以下事项：

- 客户端不保留现有引导程序文件中的设置。如果您指定CLEAR，则还必须根据需要指定所有其他安装参数。
- 客户端不会将您的安装参数保存到现有的引导程序文件。如果您要更改安装参数的值，或指定其他安装参数，就必须指定 CLEAR 覆盖现有的设置。

要替代现有的引导程序文件，请按如下在命令行中指定CLEAR：

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

模式类型参数

下表说明您用来指定产品模式的命令行参数：

参数	值	说明
PRODUCT_MODE	Phone_Mode	指定客户端的产品模式。您可以设置以下值： • 电话模式 — Cisco Unified Communications Manager 是身份验证器。 选择此值，向用户提供音频设备作为基本功能。

何时设置产品模式

在电话模式部署中，Cisco Unified Communications Manager 是身份验证器。客户端获取身份验证器后，确定产品模式为电话模式。但是，由于客户端在首次启动时始终以默认产品模式启动，因此用户在登录后必须重新启动客户端以进入电话模式。

注释 Cisco Unified Communications Manager，9.x 和更高版本 — 在安装过程中不应设置 PRODUCT_MODE。客户端从服务配置文件获取身份验证器。在用户登录后，客户端需要重新启动以进入电话模式。

更改产品模式

要更改产品模式，您必须更改客户端的身份验证器。然后，客户端可以通过身份验证器确定产品模式。

安装后更改产品模式的方法具体取决于您的部署。

注释 在所有部署中，用户都可以在“高级设置”窗口中手动设置身份验证器。

在这种情况下，您必须指示用户在“高级设置”窗口中更改身份验证器以更改产品模式。即使是先卸载然后重新安装客户端，您也不能覆盖手动设置。

使用 Cisco Unified Communications Manager 版本 9.x 和更高版本更改产品模式

要使用 Cisco Unified Communications Manager 9.x 版和更高版本更改产品模式，请在服务配置文件中更改身份验证器。

过程

步骤 1 在服务配置文件中更改相应用户的身份验证器。

更改默认模式 > 电话模式

不要为用户提供 IM and Presence Service。

如果服务配置文件不包含 IM and Presence Service 配置，则身份验证器就是 Cisco Unified Communications Manager。

更改电话模式 > 默认模式

为用户提供 IM and Presence Service。

如果在 IM and Presence 配置文件中将**产品类型**字段的值设置为：

- **Unified CM (IM and Presence)**，则身份验证器是 Cisco Unified Communications Manager IM and Presence Service。
- Webex**(IM and Presence)**，则身份验证器是Cisco Webex Messenger服务。

步骤 2 指示用户注销，然后重新登录。

当用户登录到客户端时，客户端会检索服务配置文件中的更改，并将用户登录到身份验证器。然后，客户端确定产品模式并提示用户重新启动客户端。

用户重新启动客户端后，将完成产品模式更改。

验证参数

下表说明您可以设置的命令行参数，用于指定验证来源：

参数	值	说明
AUTHENTICATOR	Webex	指定客户端的身份验证来源。如果服务发现失败，使用此值。将以下各项设置为值： • Webex—Cisco Webex Messenger 服务。基于云或基于混合云的部署。
CUP_ADDRESS	IP 地址 主机名 FQDN	指定 Cisco Unified Communications Manager IM and Presence Service 的地址。设置以下一项作为值： • 主机名 (*hostname*) • IP 地址 (*123.45.254.1*) • FQDN (*hostname.domain.com*)

参数	值	说明
TFTP	IP 地址 主机名 FQDN	指定 TFTP 服务器的地址。设置以下一项作为值： • 主机名 (*hostname*) • IP 地址 (*123.45.254.1*) • FQDN (*hostname.domain.com*) 如果您将 Cisco Unified Communications Manager 设置为身份验证器，请指定此参数。 如果您部署： • 在电话模式中，请指定托管客户端配置的TFTP服务器的地址。 • 在默认模式下，您可以指定托管设备配置的 Cisco Unified Communications Manager TFTP 服务的地址。
CTI	IP 地址 主机名 FQDN	设定 CTI 服务器的地址。 在以下情况下指定此参数： • 您将 Cisco Unified Communications Manager 设置为验证器。 • 用户有桌面电话设备，且需要 CTI 服务器。
CCMCIP	IP 地址 主机名 FQDN	设定 CCMCIP 服务器的地址。 在以下情况下指定此参数： • 您将 Cisco Unified Communications Manager 设置为验证器。 • CCMCIP 服务器的地址与 TFTP 服务器地址不相同。 如果两个地址相同，客户端可以使用 TFTP 服务器地址查找 CCMCIP 服务器。
SERVICES_DOMAIN	域	设置用于服务发现的 DNS SRV 记录所在域的值。 如果您希望客户端使用安装程序设置或手动配置来获取此信息，则此参数可设置为不包含 DNS SRV 记录的域。如果未指定此参数并且服务发现失败，则用户会收到服务域信息提示。

参数	值	说明
VOICE_SERVICES_DOMAIN	域	在混合部署中，Webex通过 CAS 查找发现所需的域可以不同于 DNS 记录部署所在的域。如果是这种情况，请将SERVICES_DOMAIN设置为用于发现的域Webex（或让用户输入电子邮件地址），并将VOICE_SERVICES_DOMAIN 设置为部署 DNS 记录的域。如果指定了此设置，客户端将使用 VOICE_SERVICES_DOMAIN 的值来查找以下 DNS 记录，以便进行服务发现和边缘检测： • `_cisco-uds` • `_cuplogin` • `_collab-edge` 此设置是可选的，如果未指定，则会在 SERVICES_DOMAIN 中获取的服务域、用户输入的电子邮件地址，或缓存的用户配置中查询 DNS 记录。
EXCLUDED_SERVICES	以下一项或多项： • Webex • CUCM	列出您希望 Jabber 从服务发现中排除的服务。例如，假设您已使用Webex试用并且您的公司域已注册Webex。但您希望 Jabber 通过 CUCM 服务器进行身份验证，而不是通过Webex。在这种情况下，设置： • EXCLUDED_SERVICES= WEBEX 可能的值包括 CUCM、 Webex 如果排除所有服务，您需要使用手动配置或引导程序配置来配置 Jabber 客户端。
UPN_DISCOVERY_ENABLED	true false	允许您定义客户端是否在发现服务时使用 Windows 会话的用户主体名称 (UPN) 获取用户的用户 ID 和域。 • true（默认值）— UPN 用于查找用户的用户 ID 和域，在服务发现期间使用。只有从 UPN 发现的用户可以登录到客户端。 • false — UPN 不用于查找用户的用户 ID 和域。系统将提示用户输入凭证以查找用于服务发现的域。 安装命令示例：`msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED= false`

TFTP 服务器地址

Cisco Jabber Windows 版本从 TFTP 服务器检索两个不同的配置文件：

- 您所创建的客户端配置文件。
- 位于 Cisco Unified Communications Manager TFTP 服务上的设备配置文件（如果您为用户提供设备）。

为了尽量减少工作量，您应在 Cisco Unified Communications Manager TFTP 服务上托管客户端配置文件。之后，您会拥有一个适用于所有配置文件的 TFTP 服务器地址，并可根据需要指定该地址。

然而，您可以在与设备配置文件不同的 TFTP 服务器上托管您的客户端配置文件。在此情况下，您拥有两个不同的TFTP服务器地址：一个是托管设备配置的TFTP服务器的地址，另一个是托管客户端配置文件的 TFTP 服务器的地址。

默认部署

本节介绍您如何在具有在网状态服务器的部署中处理两个不同的 TFTP 服务器地址。

您应执行以下操作：

1. 在“在网状态”服务器上指定托管客户端配置的 TFTP 服务器的地址。
2. 在安装期间，使用 TFTP 参数指定 Cisco Unified Communications Manager TFTP 服务的地址。

当客户端首次启动时，它会：

1. 从引导程序文件检索 Cisco Unified Communications Manager TFTP 服务的地址。
2. 从 Cisco Unified Communications Manager TFTP 服务获取设备配置。
3. 连接到在网状态服务器。
4. 在“在网状态”服务器上指定托管客户端配置的 TFTP 服务器的地址。
5. 从 TFTP 服务器获取客户端配置。

电话模式部署

本节介绍您如何在电话模式部署中处理两个不同的 TFTP 服务器地址。

您应执行以下操作：

1. 在安装期间，使用 TFTP 参数指定托管客户端配置的 TFTP 服务器的地址。
2. 使用以下参数，在您的客户端配置文件中指定托管设备配置的TFTP服务器的地址：TftpServer1。
3. 在 TFTP 服务器上托管客户端配置文件。

当客户端首次启动时，它会：

1. 从引导程序文件中检索 TFTP 服务器的地址。
2. 从 TFTP 服务器获取客户端配置。

3. 从客户端配置检索 Cisco Unified Communications Manager TFTP 服务的地址。
4. 从 Cisco Unified Communications Manager TFTP 服务获取设备配置。

通用安装参数

下表介绍某些通用命令行参数：

参数	值	说明
AUTOMATIC_SIGN_IN	true false	指定当用户安装客户端时，是否选中**在 Cisco Jabber 启动时登录**复选框。 • true — 当用户安装客户端时，选中**在 Cisco Jabber 启动时登录**复选框。 • false（默认值）— 当用户安装客户端时，不选中 **在 Cisco Jabber 启动时登录**复选框。
CC_MODE	true false	指定 Jabber 是否在 Common Criteria 模式下运行。 默认值为 false。
CLICK2X	禁用 Click2Call	禁止使用 Cisco Jabber 的一键操作功能。 如果您在安装期间指定此参数，客户端不会在操作系统中注册一键操作功能的处理程序。此参数可阻止客户端在安装期间写入 Microsoft Windows 注册表。 您必须重新安装客户端并省略此参数，从而在安装后通过客户端启用一键操作功能。 **浏览器中的 Click2Call 功能**—Click2X 参数现在可以使用新添加的 Click2Call 参数配置。这仅可以启用浏览器中的单击呼叫功能并禁用 Click2X 功能。
DIAGNOSTICSTOOLENABLED	true false	指定 Cisco Jabber 诊断工具是否可用于 Cisco Jabber Windows 版本。 • true（默认值）— 用户可以通过按下 Ctrl + Shift + D 显示 Cisco Jabber 诊断工具。 • flase — 用户不能使用 Cisco Jabber 诊断工具。

参数	值	说明
ENABLE_DPI_AWARE	true false	启用DPI感知功能。DPI感知功能允许Cisco Jabber自动调整文本和图像的显示，以适应不同的屏幕大小。 • true（默认值）— • 在 Windows 8.1 和 Windows 10 上，Cisco Jabber 会在每台显示器上调整为不同的 DPI 设置。 • 在 Windows 7 和 Windows 8 上，Cisco Jabber 将根据系统 DPI 设置显示。 • flase — 不启用 DPI 感知功能。 默认启用 DPI 感知功能。要禁用 DPI 感知功能，请使用以下命令：`msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false` **注释** 如果您使用命令行安装 Cisco Jabber，请记住包含 CLEAR = 1 参数。如果不使用命令行安装 Cisco Jabber，则必须手动删除 jabber-bootstrap.properties 文件。
ENABLE_PRT	true false	• true（默认值）—在客户端的**帮助**菜单中启用了**报告问题**菜单项。 • false — 从客户端的**帮助**菜单中删除了 Jabber 菜单项选项**报告问题**。 如果将此参数设置为 false，用户仍可手动使用**开始菜单** > **Cisco Jabber** 目录或“程序”文件目录并手动启动“问题报告”工具。如果用户手动创建PRT，并且此参数值设置为 false，则从 PRT 创建的 zip 文件没有任何内容。

参数	值	说明
ENABLE_PRT_ENCRYPTION	true false	启用问题报告加密。您必须使用 PRT_CERTIFICATE_NAME 参数配置此参数。 • true—Jabber 客户端发送的 PRT 文件是加密的。 • false（默认值）—Jabber 客户端发送的 PRT 文件未加密。 PRT 加密要求使用公钥对/私钥对来加密和解密 Cisco Jabber 问题报告。
FIPS_MODE	true false	指定 Cisco Jabber 是否处于 FIPS 模式。 Cisco Jabber 可以在未启用 FIPS 的操作系统上处于 FIPS 模式。只有与非 Windows API 之间的连接处于 FIPS 模式。 如果不包含此设置，Cisco Jabber 将根据操作系统确定 FIPS 模式。
FORGOT_PASSWORD_URL	URL	指定用户可在其中重置遗失或忘记的密码的 URL 地址。 此参数为可选，但建议使用。 **注释** 在基于云的部署中，您可以使用 Cisco Webex管理工具指定忘记的密码 URL。不过，在用户登录之前，客户端不能检索此忘记的密码 URL。
FORWARD_VOICEMAIL	true false	在“语音留言”选项卡中启用语音邮件转发。 • true（默认值）—用户可以将语音邮件转发到联系人。 • false — 语音邮件转发未启用。

参数	值	说明
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	指定无效证书的客户端行为。 • RejectAndNotify — 显示警告对话框，客户端不会加载。 • PromptPerSession — 显示警告对话框，用户可以接受或拒绝无效的证书。 对于 FIPS 模式中的无效证书，此参数将被忽略，客户端会显示一条警告消息，而不会加载。
IP_Mode	仅 IPv4 仅 IPv6 两个堆栈	指定 Jabber 客户端使用的网络 IP 协议。 • 仅 IPv4 — Jabber 将仅尝试进行 IPv4 连接。 • 仅 IPv6 — Jabber 将仅尝试进行 IPv6 连接。 • 两个堆栈（默认）— Jabber 可以与 IPv4 或 IPv6 连接。 **注释** 仅 IPv6 支持仅适用于桌面设备内部部署。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《思科协作系统版本的 IPv6 部署指南》。 决定 Jabber 所使用网络 IP 协议的因素有很多，有关详细信息，请参阅 《规划指南》中的“IPv6 要求”部分。

参数	值	说明
LANGUAGE	LCID（十进制数）	定义 Cisco Jabber Windows 版本所用语言的区域设置 ID (LCID)（十进制数）。此值必须是与支持的语言对应的 LCID（十进制数）。 例如，您可以指定以下项目之一： • 1033 指定英语。 • 1036 指定法语。 有关您可以指定的语言的完整列表，请参阅 *LCID* 的语言主题。 此参数为可选。 如果不指定值，Cisco Jabber Windows 版本会检查 UseSystemLanguage 参数的值。如果 UseSystemLanguage 参数设置为 true，则使用与操作系统相同的语言。如果 UseSystemLanguage 参数设置为 false 或未定义，则客户端默认使用当前用户的区域语言。 区域语言在以下位置设置：**控制面板** > **区域和语言** > **更改日期、时间或号码格式** > **格式选项卡** > **格式下拉列表**。
LOCATION_MODE	已启用 已禁用 ENABLEDNOPROMPT	指定是否已启用位置功能，以及在检测到新位置时是否通知用户。 • 已启用（默认值）—已开启位置功能。检测到新位置时通知用户。 • 已禁用 — 已关闭位置功能。检测到新位置时，不会通知用户。 • ENABLEDNOPROMPT — 已开启位置功能。检测到新位置时，不会通知用户。

参数	值	说明
LOG_DIRECTORY	本地文件系统中的绝对路径	定义客户端写入日志文件的目录。 使用引号以防路径中存在空格字符，如下例所示： `"C:\my_directory\Log Directory"` 您指定的路径不能包含 Windows 无效字符。 默认值为 `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`
LOGIN_RESOURCE	WBX MUT	控制用户登录到多个客户端实例。 默认情况下，用户可以同时登录到多个 Cisco Jabber 实例。设置以下值之一来更改默认行为： • WBX — 用户可以一次登录到一个 Cisco Jabber Windows 版本实例。 Cisco Jabber Windows 版本将 `wbxconnect` 后缀附加到用户的 JID。用户无法登录到使用 `wbxconnect` 后缀的任何其他 Cisco Jabber 客户端。 • MUT — 用户每次只能登录到一个 Cisco Jabber Windows 版本实例，但可以同时登录到其他 Cisco Jabber 客户端。 每个 Cisco Jabber Windows 版本实例均会为用户 JID 添加一个唯一的后缀。
PRT_CERTIFICATE_NAME	证书名称	使用企业信任或信任的根证书颁发机构证书存储库中的公钥指定证书的名称。证书公钥用于加密 Jabber 问题报告。您必须使用 ENABLE_PRT_ENCRYPTION 参数配置此参数。
RESET_JABBER	1	重置用户的本地和漫游配置文件数据。 以下这些文件夹已删除： • `%appdata%\Cisco\Unified Communications\Jabber` • `%localappdata%\Cisco\Unified Communications\Jabber`

参数	值	说明
SSO_EMAIL_PROMPT	开启 关闭	指定是否为用户显示确定其主群集的电子邮件提示。 为使 ServicesDomainSsoEmailPrompt 定义的电子邮件提示生效，安装程序要求如下： • SSO_EMAIL_PROMPT=ON • UPN_DISCOVERY_ENABLED = False • VOICE_SERVICES_DOMAIN=<domain_name> • SERVICES_DOMAIN=<domain_name> 示例：msiexec.exe /i CiscoJabberSetup.msi SSO_EMAIL_PROMPT=ON UPN_DISCOVERY_ENABLED=False VOICE_SERVICES_DOMAIN=example.cisco.com SERVICES_DOMAIN=example.cisco.com CLEAR=1
Telemetry_Enabled	true false	指定是否收集分析数据。默认值为 true。 为改善您的体验和产品性能，Cisco Jabber 可能会收集非个人识别使用和性能数据并发送给 Cisco。Cisco 使用聚合数据了解 Jabber 客户端的使用方式及其执行方式的趋势。 有关 Cisco Jabber 收集和不收集的分析数据的完整详情，请参见 Cisco 在线隐私策略的 Cisco Jabber 补充，网址为：https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html。
TFTP_FILE_NAME	文件名	指定组配置文件的唯一名称。 您可以指定非限定或全限定文件名作为值。您指定的文件名（作为此参数的值）会替代 TFTP 服务器上的任何其他配置文件。 此参数为可选。 记住 在 Cisco Unified Communications Manager 的 CSF 设备配置的 **Cisco 支持字段**中，您可以指定组配置文件。

参数	值	说明
UXModel	现代 传统	适用于 Cisco Jabber 桌面客户端版本。 Jabber 默认为所有部署中的现代设计。但 Webex Messenger 部署也支持传统设计。Jabber 组消息模式仅支持现代设计。 如果您希望采用 Webex Messenger 部署启动传统设计，请使用 UXModel 参数。允许的值包括： • 现代（默认值）—Jabber 启动现代设计。 • 传统—Jabber 启动传统设计。 每个用户都可以在 Jabber 中设置个人首选项，这将优先于此参数。

语言的 LCID

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

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
丹麦语——丹麦	X	X	X	1030
荷兰语——荷兰	X	X	X	1043
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

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
斯洛文尼亚语——斯洛文尼亚	X	X		1060
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

相关主题

示例安装命令，第 69 页
命令行参数，第 70 页

手动运行 MSI

您可以手动运行安装程序，以安装单个客户端实例，并在“高级设置”窗口中指定连接设置。

过程

步骤 1 启动 `CiscoJabberSetup.msi`。

安装程序会打开窗口，指导您进行安装。

步骤 2 按照以下步骤完成安装过程。

步骤 3 启动 Cisco Jabber Windows 版本。

步骤 4 选择**手动设置和登录**。

“高级设置”窗口将会打开。

步骤 5 指定连接设置属性的值。

步骤 6 选择**保存**。

创建自定义安装程序

您可以转换默认的安装软件包，以创建自定义安装程序。

注释 您使用 Microsoft Orca 创建自定义安装程序。Microsoft Orca 作为适用于 Windows 7 和 .NET Framework 4 的 Microsoft Windows SDK 的一部分提供。

从microsoft 网站下载并安装适用于 Windows 7 和 .NET Framework 4 的 Microsoft Windows SDK。

过程

	命令或操作	目的
步骤 1	获取默认的转换文件， 第 86 页	您必须有默认的转换文件，才能使用 Microsoft Orca 修改安装软件包。
步骤 2	创建自定义转换文件， 第 86 页	转换文件包含您应用到安装程序的安装属性。
步骤 3	转换安装程序， 第 87 页	应用转换文件以自定义安装程序。

获取默认的转换文件

您必须有默认的转换文件，才能使用 Microsoft Orca 修改安装软件包。

过程

步骤 1 从软件下载页下载 Cisco Jabber 管理软件包。

步骤 2 将 `CiscoJabberProperties.msi` 从 Cisco Jabber 管理软件包复制到您的文件系统。

下一步做什么

创建自定义转换文件， 第 86 页

创建自定义转换文件

要创建自定义安装程序，您可以使用转换文件。转换文件包含您应用到安装程序的安装属性。

默认的转换文件可让您在转换安装程序时指定属性的值。如果您在创建一个自定义安装程序，就应该使用默认的转换文件。

您可以有选择性地创建自定义转换文件。您为自定义转换文件中的属性指定值，然后将其应用到安装程序。

如果您需要使用不同属性值的多个自定义安装程序，请创建自定义转换文件。例如，创建一个将默认语言设置成法语的转换文件，和另一个将默认语言设置成西班牙语的转换文件。然后，您可以将每个转换文件单独应用到安装软件包。结果是您创建了两个安装程序，每种语言一个安装程序。

开始之前

获取默认的转换文件，第 86 页

过程

步骤 1 启动 Microsoft Orca。

步骤 2 打开 `CiscoJabberSetup .msi`，然后应用 `CiscoJabberProperties`。

步骤 3 指定适当安装程序属性的值。

步骤 4 生成并保存转换文件。

a) 选择**转换** > **生成转换**。

b) 在文件系统中选择保存转换文件的位置。

c) 指定转换文件的名称，然后选择**保存**。

您创建的转换文件会保存为 *`file_name`*`.mst`。您可以应用此转换文件以修改 `CiscoJabberSetup.msi` 的属性。

下一步做什么

转换安装程序，第 87 页

转换安装程序

应用转换文件以自定义安装程序。

注释 应用转换文件将更改 `CiscoJabberSetup.msi` 的数字签名。尝试修改或重命名 `CiscoJabberSetup.msi` 将彻底删除该签名。

开始之前

创建自定义转换文件，第 86 页

过程

步骤 1 启动 Microsoft Orca。

步骤 2 在 Microsoft Orca 中打开 `CiscoJabberSetup.msi`。

a) 选择**文件** > **打开**。

b) 浏览到您的文件系统上 `CiscoJabberSetup.msi` 的位置。

c) 选择 `CiscoJabberSetup.msi`，然后选择**打开**。

安装软件包将在 Microsoft Orca 中打开。安装程序的表格列表将在**表格**窗格中打开。

步骤 3 必需： 移除除 1033（英语）之外的所有语言代码。

限制 您必须从自定义安装程序中移除除 1033（英语）之外的所有语言代码。

Microsoft Orca 不会在自定义安装程序中保留任何语言文件，但默认值 1033 除外。如果不从自定义安装程序中移除所有语言代码，您将无法在英语之外的任何操作系统上运行安装程序。

a) 选择**查看** > **摘要信息**。

编辑摘要信息窗口将会显示。

b) 找到**语言**字段。
c) 移除除 1033 之外的所有语言代码。
d) 单击**确定**。

英语已设置为您的自定义安装程序的语言。

步骤 4 应用转换文件。

a) 选择**转换** > **应用转换**。
b) 浏览到您的文件系统上的转换文件的位置。
c) 选择转换文件，然后选择**打开**。

步骤 5 在**表格**窗格中的表格列表中选择**属性**。

`CiscoJabberSetup.msi` 的属性列表将在应用程序窗口的右窗格中打开。

步骤 6 指定所需属性的值。

提示 值区分大小写。请确保您输入的值与本文档中的值相匹配。

提示 将 CLEAR 属性的值设为 `1` 以覆盖以前安装中的任何现有引导程序文件。如果不覆盖现有的引导程序文件，则您在自定义安装程序中设置的值不会生效。

步骤 7 删除任何不需要的属性。

删除任何未设置的属性非常重要，否则设置的属性不会生效。逐一删除每个不需要的属性。

a) 右键单击要删除的属性。
b) 选择**删除行**。
c) 在 Microsoft Orca 提示您继续时选择**确定**。

步骤 8 必需： 启用您的自定义安装程序以保存嵌入的流。

a) 选择**工具** > **选项**。
b) 选择**数据库**选项卡。
c) 选择在**‘另存为’期间复制嵌入的流**。
d) 选择**应用**，然后选择**确定**。

步骤 9 保存您的自定义安装程序。

a) 选择**文件** > **将转换数据另存为**。
b) 在您的文件系统上选择用于保存安装程序的位置。

c) 指定安装程序的名称，然后选择**保存**。

安装程序属性

以下是您可以在自定义安装程序中修改的属性：

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

这些属性与安装参数对应，并有相同的值。

使用组策略进行部署

在 Microsoft Windows Server 上安装使用 Microsoft Group Policy Management Console (GPMC) 的 Cisco Jabber Windows 版本。

注释 要安装使用组策略的 Cisco Jabber Windows 版本，则您计划部署 Cisco Jabber Windows 版本的所有计算机或用户都必须在相同域内。

过程

	命令或操作	目的
步骤 1	设置语言代码，第 90 页	只有在以任何方式修改 MSI 时，才必须使用此程序并将“语言”字段设置为 1033。
步骤 2	使用组策略部署客户端，第 91 页	部署使用组策略的 Cisco Jabber Windows 版本。

设置语言代码

在组策略部署方案中，如果使用Cisco提供的准确MSI文件，则无需更改安装语言。在这些情况下，将根据 Windows用户区域设置（格式）确定安装语言。只有在以任何方式修改MSI时，才必须使用此程序并将“语言”字段设置为 1033。

有关 Jabber 客户端支持的语言的区域设置标识符 (LCID) 或语言标识符 (LangID) 的列表，请参阅语言的 LCID，第 83 页。

过程

步骤 1 启动 Microsoft Orca。

Microsoft Orca 作为适用于 Windows 7 和 .NET Framework 4 的 Microsoft Windows SDK 的一部分提供，您可以从 Microsoft 网站下载。

步骤 2 打开 `CiscoJabberSetup.msi`。

a) 选择**文件** > **打开**。
b) 浏览到您的文件系统上 `CiscoJabberSetup.msi` 的位置。
c) 选择 `CiscoJabberSetup.msi`，然后选择**打开**。

步骤 3 选择**查看** > **摘要信息**。

步骤 4 找到**语言**字段。

步骤 5 将**语言**字段设置为 1033。

步骤 6 单击**确定**。

步骤 7 必需： 启用您的自定义安装程序以保存嵌入的流。

a) 选择**工具** > **选项**。
b) 选择**数据库**选项卡。
c) 选择在‘**另存为**’期间**复制嵌入的流**。
d) 选择**应用**，然后选择**确定**。

步骤 8 保存您的自定义安装程序。

a) 选择**文件** > **将转换数据另存为**。
b) 在您的文件系统上选择用于保存安装程序的位置。

c) 指定安装程序的名称，然后选择**保存**。

下一步做什么

使用组策略部署客户端 ， 第 91 页

使用组策略部署客户端

完成此任务中的步骤，以使用组策略部署 Cisco Jabber Windows 版本。

开始之前

设置语言代码 ， 第 90 页

过程

步骤 1 将安装软件包复制到软件分发点进行部署。

您计划部署 Cisco Jabber Windows 版本的所有计算机或用户，必须能够访问分发点中的安装软件包。

步骤 2 选择**开始** > **运行**，然后输入以下命令：

```
GPMC.msc
```

组策略管理控制台将会打开。

步骤 3 创建新的组策略对象。

a) 在左窗格中右键单击适当的域。

b) 选择**在这个域中创建 GPO 并在此处链接**。

新建 GPO 窗口将会打开。

c) 在**名称**字段中输入组策略对象的名称。

d) 保留默认值，或从**源 Starter GPO** 下拉列表中选择适当的选项，然后选择**确定**。

新的组策略会显示在域的组策略列表中。

步骤 4 设置您的部署范围。

a) 在左窗格中的域下面，选择组策略对象。

组策略对象会显示在右窗格中。

b) 在**范围**选项卡的**安全筛选**部分，选择**添加**。

选择用户、计算机或组窗口将会打开。

c) 指定您要部署Cisco Jabber Windows 版本的计算机和用户。

步骤 5 指定安装软件包。

a) 在左窗格中右键单击组策略对象，然后选择**编辑**。

组策略管理编辑器将会打开。

b) 选择**计算机配置**，然后选择**策略** > **软件设置**。
c) 右键单击**软件安装**，然后选择**新建** > **软件包**。
d) 在**文件名**旁边输入安装软件包的位置，例如 `\\server\software_distribution`。

重要事项 您必须输入通用命名约定 (UNC) 路径，作为安装软件包的位置。如果您不输入 UNC 路径，组策略就无法部署 Cisco Jabber Windows 版本。

e) 选择安装软件包，然后选择**打开**。
f) 在**部署软件**对话框中，选择**已分配**，然后再选择**确定**。

在下次计算机启动时，组策略即会在每台计算机上安装 Cisco Jabber Windows 版本。

配置 Windows 版本自动更新

要启用自动更新，您可以创建包含最新版本信息的 XML 文件，包括 HTTP 服务器中安装软件包的 URL。当用户登录、从休眠模式恢复计算机，或从**帮助**菜单执行手动更新请求时，客户端会检索 XML 文件。

注释 如果对即时消息Cisco Webex Messenger和在网状态功能使用此服务，则应使用Cisco Webex管理工具配置自动更新。

XML 文件结构

用于自动更新的 XML 文件有以下结构：

```
<JabberUpdate>
          <App name=”JabberWin”>
               <LatestBuildNum>12345</LatestBuildNum>
               <LatestVersion>11.8.x</LatestVersion>
               <Mandatory>true</Mandatory>
               <Message>
                  <![CDATA[<b>This new version of Cisco Jabber lets you do the
                  following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
                  more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
               </Message>
               <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>

          </App>
        </JabberUpdate>
```

开始之前

- 安装并配置 HTTP 服务器以托管 XML 文件和安装软件包。
- 确保用户有在工作站中安装软件更新的权限。

如果用户在工作站中没有管理权限，Microsoft Windows 会停止更新安装。您必须以管理权限登录才能完成安装。

过程

步骤 1 在 HTTP 服务器上托管更新安装程序。

步骤 2 使用任何文本编辑器创建更新 XML 文件。

步骤 3 按如下方式在 XML 中指定值：

- 名称— 指定以下 ID 作为应用程序元素的名称属性的值：
  - JabberWin — 更新适用于 Cisco Jabber Windows 版本。
- `LatestBuildNum` — 更新的内部版本号。
- `LatestVersion` — 更新的版本号。
- 必填—（仅限 Windows 客户端）True 或 False。确定在提示时用户是否必须升级其客户端版本。
- `Message` — 以下格式的 HTML：

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL` — HTTP 服务器中的安装软件包 URL。
- `AllowUpdatesViaExpressway`—（仅限 Windows 客户端）。False（默认值）或 True。确定 Jabber 在通过移动设备和Remote Access的 Expressway 连接到公司网络时，是否可以执行自动更新。

  如果您的更新 XML 文件托管在公共 web 服务器上，请将此参数设置为“flase”。否则，更新文件会告诉 Jabber 它托管在必须通过手机和Remote Access的 Expressway 访问的内部服务器上。

步骤 4 保存并关闭您的更新 XML 文件。

步骤 5 在 HTTP 服务器上托管您的更新 XML 文件。

步骤 6 在配置文件中指定更新 XML 文件的 URL 作为 UpdateUrl 参数的值。

卸载 Cisco Jabber Windows 版本

您可以使用命令行或 Microsoft Windows 控制面板来卸载 Cisco Jabber Windows 版本。本文档说明了如何使用命令行卸载 Cisco Jabber Windows 版本。

使用安装程序

如果安装程序在文件系统中可用，请使用它删除 Cisco Jabber Windows 版本。

过程

步骤 1 打开命令行窗口。

步骤 2 输入以下命令：

```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```

例如，

```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```

其中 `/quiet` 指定无提示卸载。

该命令将从计算机中删除 Cisco Jabber Windows 版本。

使用产品代码

如果安装程序在文件系统中不可用，请使用产品代码删除 Cisco Jabber Windows 版本。

过程

步骤 1 查找产品代码。

a) 打开 Microsoft Windows 注册表编辑器。
b) 找到以下注册表项：`HKEY_CLASSES_ROOT\Installer\Products`
c) 选择**编辑** > **查找**。
d) 在**查找**窗口的**查找目标**文本框中输入 Cisco Jabber，然后选择**查找下一个**。
e) 查找 **ProductIcon** 项的值。

产品代码是 **ProductIcon** 项的值，例如 `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`。

注释 产品代码因不同的 Cisco Jabber Windows 版本版本而有变化。

步骤 2 打开命令行窗口。

步骤 3 输入以下命令：

```
msiexec.exe /x product_code
```

例如，

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

其中 `/quiet` 指定无提示卸载。

该命令将从计算机中删除 Cisco Jabber Windows 版本。

安装 Cisco Jabber Mac 版本

Cisco Jabber Mac 版本的安装程序

安装客户端

您可以选择使用以下方法之一安装客户端：

- 为用户提供安装程序以手动安装应用程序。该客户端安装在应用程序文件夹中。需要删除客户端的旧版本。
- 为用户配置自动更新，安装程序会无提示更新应用程序。

  对于自动更新，始终会将客户端添加到应用程序文件夹中。

  - 如果客户端存在于不同的文件夹或应用程序文件夹的子文件夹中，则会在该文件夹中创建一个链接，以便在“应用程序”文件夹中运行客户端。
  - 如果用户之前重命名了客户端，则安装程序将重命名新客户端以进行匹配。

系统会提示用户输入与安装其他 OS X 安装程序类似的系统凭证。

静默安装— 若要静默安装客户端，请在终端工具中使用以下 Mac OS X 命令：

```
sudo installer -pkg /path_to/Install_Cisco-Jabber-Mac.pkg -target /
```

有关安装程序命令的详细信息，请参阅 Mac 上的安装程序手动页。

配置

为您的用户提供配置信息以登录到客户端。选择下列操作之一：

- 为您的用户提供包含可选服务器信息的配置 URL。有关详细信息，请参阅 *Cisco Jabber Mac* 版本的 *URL* 配置部分。
- 为您的用户提供服务器信息以手动连接。有关详细信息，请参阅手动连接设置部分。
- 使用服务发现。有关详细信息，请参阅服务发现部分。

手动运行安装程序

您可以手动运行安装程序，以安装单个客户端实例，并在**首选项**设置中指定连接设置。

开始之前

删除客户端的任何旧版本。

过程

步骤 1 启动 `jabber-mac.pkg`。
安装程序会打开窗口，指导您进行安装。

步骤 2 按照以下步骤完成安装过程。
安装程序会提示用户输入系统凭证。

步骤 3 使用配置 URL 或直接运行客户端以启动客户端。
输入用户凭证。

Cisco Jabber Mac 版本的 URL 配置

要让用户在不手动输入服务发现信息的情况下启动Cisco Jabber，请创建一个配置 URL 并将其分发给用户。

您可以直接通过电子邮件将配置 URL 链接发送给用户，也可以发布指向网站的链接。

您可以在 URL 中包含和指定以下参数：

- ServicesDomain — 必要。每个配置 URL 必须包括Cisco Jabber服务发现所需的 IM and Presence 服务器的域。
- ServiceDiscoveryExcludedServices — 可选。您可以从服务发现过程中排除以下任何服务：
  - Webex— 当您设置此值时，客户端会：
    - 不执行 CAS 查找
    - 查找：
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM — 设置此值时，客户端会：
    - 不查找 `_cisco-uds`
    - 查找：
      - `_cuplogin`
      - `_collab-edge`
  - CUP — 当您设置此值时，客户端会：
    - 不查找 `_cuplogin`

- 查找：
  - _cisco-uds
  - _collab-edge

您可以指定多个逗号分隔的值以排除多项服务。

如果要排除全部三项服务，客户端将不会执行服务发现，并提示用户手动输入连接设置。

- ServicesDomainSsoEmailPrompt — 可选。指定是否为用户显示用于确定其主群集的电子邮件提示。
  - 开启
  - 关闭
- EnablePRTEncryption — 可选。指定是否加密 PRT 文件。适用于 Cisco Jabber Mac 版本。
  - true
  - false
- PRTCertificateName — 可选。指定证书的名称。适用于 Cisco Jabber Mac 版本。
- InvalidCertificateBehavior — 可选。指定无效证书的客户端行为。
  - RejectAndNotify — 显示警告对话框，客户端不会加载。
  - PromptPerSession — 显示警告对话框，用户可以接受或拒绝无效的证书。
- Telephony_Enabled — 指定用户是否具有电话功能。默认值为 true。
  - True
  - False
- DiagnosticsToolEnabled — 指定诊断工具在客户端中是否可用。默认值为 true。
  - True
  - False

按以下格式创建配置 URL：

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

注释 该参数区分大小写。

示例

- ciscojabber://provisionServicesDomain = cisco.com
- ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com
- ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX
- ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP
- ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF

配置 Mac 版自动更新

要启用自动更新，您可以创建包含最新版本信息的 XML 文件，包括 HTTP 服务器中安装软件包的 URL。当用户登录、从休眠模式恢复计算机，或从**帮助**菜单执行手动更新请求时，客户端会检索 XML 文件。

注释 如果对即时消息Cisco Webex Messenger和在网状态功能使用此服务，则应使用Cisco Webex管理工具配置自动更新。

XML 文件结构

以下是用于自动更新的示例 XML 文件：

```
<JabberUpdate>
<App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>
</App>
</JabberUpdate>
```

示例 XML 文件 2

以下是用于 Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本自动更新的 XML 文件示例：

```
<JabberUpdate>
 <App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
```

```
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>

 </App>
 <App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2
  </li></ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
  </DownloadURL>
</App>
</JabberUpdate>
```

开始之前

安装并配置 HTTP 服务器以托管 XML 文件和安装软件包。

注释 配置 Web 服务器以转义特殊字符，从而确保 DSA 签名成功。例如，Microsoft IIS 上的选项是：**允许双空格**。

过程

步骤 1 在 HTTP 服务器上托管更新安装程序。

步骤 2 使用任何文本编辑器创建更新 XML 文件。

步骤 3 按如下方式在 XML 中指定值：

- 名称— 指定以下 ID 作为应用程序元素的名称属性的值：
  - JabberWin — 更新适用于 Cisco Jabber Windows 版本。
  - JabberMac — 更新适用于 Cisco Jabber Mac 版本。
- `LatestBuildNum` — 更新的内部版本号。
- `LatestVersion` — 更新的版本号。
- `Mandatory`— True 或 False。确定在提示时用户是否必须升级其客户端版本。
- `Message` — 以下格式的 HTML：

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL` — HTTP 服务器中的安装软件包 URL。

  对于 Cisco Jabber Mac 版本，URL 文件必须采用以下格式：

  ```
  Install_Cisco-Jabber-Mac-version-size-dsaSignature.zip
  ```

步骤 4 保存并关闭您的更新 XML 文件。

步骤 5 在 HTTP 服务器上托管您的更新 XML 文件。

步骤 6 在配置文件中指定更新 XML 文件的 URL 作为 UpdateUrl 参数的值。

安装 Cisco Jabber 移动客户端

过程

步骤 1 要安装 Cisco Jabber Android 版本，请从移动设备上的 App Store 下载应用程序。

步骤 2 要安装 Cisco Jabber iPhone 和 iPad 版本，请从移动设备上的 App Store 下载应用程序。

Cisco Jabber Android、iPhone 和 iPad 版本的 URL 配置

要让用户在不手动输入服务发现信息的情况下启动Cisco Jabber，请创建一个配置 URL 并将其分发给用户。

您可以直接通过电子邮件将配置 URL 链接发送给用户，也可以发布指向网站的链接。

您可以在 URL 中包含和指定以下参数：

- ServicesDomain — 必要。每个配置 URL 必须包括Cisco Jabber服务发现所需的 IM and Presence 服务器的域。
- ServiceDiscoveryExcludedServices — 可选。您可以从服务发现过程中排除以下任何服务：
  - Webex— 当您设置此值时，客户端会：
    - 不执行 CAS 查找
    - 查找：
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM — 设置此值时，客户端会：
    - 不查找 `_cisco-uds`
    - 查找：
      - `_cuplogin`
      - `_collab-edge`

- CUP — 当您设置此值时，客户端会：
  - 不查找 _cuplogin
  - 查找：
    - _cisco-uds
    - _collab-edge

  您可以指定多个逗号分隔的值以排除多项服务。

  如果要排除全部三项服务，客户端将不会执行服务发现，并提示用户手动输入连接设置。
- ServicesDomainSsoEmailPrompt — 可选。指定是否为用户显示用于确定其主群集的电子邮件提示。
  - 开启
  - 关闭
- InvalidCertificateBehavior — 可选。指定无效证书的客户端行为。
  - RejectAndNotify — 显示警告对话框，客户端不会加载。
  - PromptPerSession — 显示警告对话框，用户可以接受或拒绝无效的证书。
- PRTCertificateUrl — 使用信任根证书存储库中的公共密钥指定证书的名称。适用于 Cisco Jabber 移动客户端。
- Telephony_Enabled — 指定用户是否具有电话功能。默认值为 true。
  - True
  - False
- ForceLaunchBrowser — 用于强制用户使用外部浏览器。适用于 Cisco Jabber 移动客户端。
  - True
  - False

注释 ForceLaunchBrowser 用于客户端证书部署，适用于使用 Android 5.0 以下操作系统的设备。

按以下格式创建配置 URL：

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

注释 该参数区分大小写。

示例

- `ciscojabber://provisionServicesDomain = cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

使用企业移动性管理的移动配置

通过 AppConfig 标准进行企业移动性管理 (EMM)

在使用企业移动性管理 (EMM) 之前，请确保：

- EMM 供应商支持使用 Android for Work 或 Apple 托管的应用配置。
- 该 Android 设备的操作系统为 5.0 或更高版本。

要允许用户启动 Cisco Jabber Android 版本或者 Cisco Jabber iPhone 和 iPad 版本，可以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。

您可以将 Cisco Jabber iPhone 和 iPad 版本配置为从 Microsoft Exchange Server 导入的本地联系人的默认拨号器。使用**Exchange ActiveSync** 配置配置文件，并在 MDM 配置文件的**默认音频呼叫应用程序**字段中输入值 `com.cisco.jabberIM`。

使用 EMM 时，在 EMM 应用程序中将 AllowUrlProvisioning 参数设置为 False 以禁用 URL 配置。有关配置参数的详细信息，请参阅 *AllowUrlProvisioning* 参数部分。

通过应用程序封装进行 EMM

另外一种 EMM 方法是应用程序封装。您可以使用供应商应用程序封装工具来封装 Jabber，并应用策略来限制用户可以在 Jabber 中执行的操作。然后，可以将封装的 Jabber 分发给用户。升级到新版本的 Jabber 后必须重复封装操作。

我们要求您签署一项双向协议，以将应用程序封装与 Cisco Jabber 结合使用。请发送邮件至 jabber-mobile-mam@cisco.com 与我们联系以了解详情。

通过 SDK 集成进行 EMM

在版本 12.8 中，我们新增了对于 Microsoft Intune 和 BlackBerry Dynamics 的支持作为另外一种 EMM 方法。我们使用 Microsoft 和 BlackBerry SDK 创建了可通过 App Store 和 Google Play Store 获取的新客户端：

- Jabber Intune 版本
- Jabber BlackBerry 版本

借助这些解决方案，您可以在门户中创建自己的管理策略。当用户使用新客户端登录时，客户端将与门户同步并应用您的策略。

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

限制	Android	iPhone 和 iPad
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。当客户端不在本地时，它需要通过 Cisco Expressway 对所有流量进行移动和远程访问。

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

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

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

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

Jabber BlackBerry 版本的一般设置流程如下：

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

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

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

字段	iOS 支持	Android 支持
禁用交叉启动 Webex Meetings [1]	是	是
服务域	是	是
语音服务域	是	是
服务发现排除的服务	是	是
服务域 SSO 电子邮件提示	是	是
无效的证书行为	是	是
已启用电话	是	是
允许 Url 预配置	是	是
IP 模式	是	是

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

5. 用户登录到客户端。

有关这些步骤的详细信息，请参阅 BlackBerry 文档。

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

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

Jabber BlackBerry 版本中的 IdP 连接

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

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

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

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

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

iOS 上的应用程序传输安全性

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，只要满足相同的要求即可。

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。

适用于 MDM 部署的有用参数

EMM 供应商可能允许您在“应用程序配置”设置中设置不同的值类型，但 Jabber 仅读取字符串值类型。对于 EMM，您可能会发现以下参数很有用。有关这些参数的更多详情，请参阅 *Cisco Jabber Android*、*iPhone* 和 *iPad* 版本的 *URL* 配置部分：

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser

- FIPS_MODE
- CC_MODE
- LastLoadedUserProfile
- AllowUrlProvisioning

  使用 EMM 时，在 EMM 应用程序中将 AllowUrlProvisioning 参数设置为 **`False`** 以禁用 URL 配置。有关配置参数的详细信息，请参阅主题 *AllowUrlProvisioning* 参数。
- IP_Mode
- AllowTeamsUseEmbeddedSafari — 仅适用于 Cisco Jabber iPhone 和 iPad 版本
- AutoLoginUserName
- AutoLoginUserPassword

以下各节讨论了部分参数在 MDM 部署中的使用。

AllowUrlProvisioning 参数

将用户从 URL 配置迁移到 EMM 时使用此参数。

将以下值应用到此参数：

- true（默认值）— 使用 URL 配置执行引导程序配置
- false — 不使用 URL 配置执行引导程序配置

  示例：`<AllowURLProvisioning>*false*</AllowURLProvisioning>`

AutoLoginUserName

适用于 Cisco Jabber iPhone 和 iPad 版本。

在 EMM 中，定义移动设备上的用户名。此参数必须与 AutoLoginUserPassword 参数和 ServicesDomain 参数一起使用。通过这些参数，您可以在输入用户的登录详细信息后安装 Jabber 应用程序。

AutoLoginUserPassword

适用于 Cisco Jabber iPhone 和 iPad 版本。

在 EMM 中，定义移动设备上的密码。此参数必须与 AutoLoginUserName 参数和 ServicesDomain 参数一起使用。通过这些参数，您可以在输入用户的登录详细信息后安装 Jabber 应用程序。

CC_MODE 参数

使用此参数可在使用 EMM 的 Cisco Jabber 移动客户端上启用或禁用 Common Criteria 模式。

- *true* — 以 Common Criteria 模式运行 Cisco Jabber。
- *false*（默认值）— 不以 Common Criteria 模式运行 Cisco Jabber。

  示例：`<CC_MODE>*true*</CC_MODE>`

注释 要启用 CC_MODE，RSA 密钥大小必须至少为 2048 位。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* 的本地部署指南》中有关如何部署 *Cisco Jabber* 应用程序的详细信息。

FIPS_MODE 参数

使用此参数可在使用 EMM 的 Cisco Jabber 移动客户端上启用或禁用 FIPS 模式。

- *true* — 以 FIPS 模式运行 Cisco Jabber。
- *false* — 不以 FIPS 模式运行 Cisco Jabber。

  示例：`<FIPS_MODE>false</FIPS_MODE>`

安装 Jabber VDI 软终端

过程

步骤 1 完成部署 Jabber 的工作流程。

步骤 2 要安装 Cisco Jabber VDI 软终端，请按照适用于您安装的客户端的《Cisco Jabber VDI 软终端部署和安装指南》中的说明操作。

第 14 章

Remote Access

服务发现要求工作流程

过程

	命令或操作	目的
步骤 1	服务发现要求， 第 51 页	
步骤 2	DNS 要求， 第 51 页	
步骤 3	证书要求， 第 51 页	
步骤 4	测试 _collab-edge SRV 记录， 第 112 页	

服务发现要求

服务发现允许客户端自动在您的企业网络上检测和查找服务。移动设备和Remote Access的 Expressway 可使您访问企业网络上的服务。您应满足以下要求，以使客户端能够通过移动设备和Remote Access 的 Expressway 进行连接，然后发现服务：

- DNS 要求
- 证书要求
- 测试外部 SRV `_collab-edge`。

DNS 要求

通过Remote Access实现服务发现的 DNS 要求包括：

- 在外部 DNS 服务器上配置 `_collab-edge` DNS SRV 记录。
- 在内部名称服务器上配置`_cisco-uds` DNS SRV 记录。
- 或者，对于 IM 和在线状态服务器和语音服务器的具有不同域的基于云的混合部署，可以配置语音服务域来找到具有 `_collab-edge` 记录的 DNS 服务器。

证书要求

在您配置远程访问之前，请下载 Cisco VCS Expressway 和 Cisco Expressway-E 服务器证书。服务器证书用于 HTTP 和 XMPP。

有关配置 Cisco VCS Expressway 证书的详细信息，请参阅《Cisco vcs Expressway 上的配置证书》。

测试 _collab-edge SRV 记录

测试 SRV 记录

在创建 SRV 记录后，测试以确认是否可以访问这些记录。

提示 如果您偏好基于 web 的选项，您也可以使用协作解决方案分析器站点上的 SRV 检查工具。

过程

步骤 1 打开命令提示符。

步骤 2 输入**nslookup**。

将显示默认的 DNS 服务器和地址。确认这是预期的 DNS 服务器。

步骤 3 输入 **set type=SRV**。

步骤 4 输入每个 SRV 记录的名称。

例如，`_cisco-uds._tcp.exampledomain`

- 显示服务器和地址 — 可以访问 SRV 记录。
- 显示 `_cisco-uds_tcp.exampledomain`：不存在的域 — 您的 SRV 记录存在问题。

Cisco Anyconnect 部署工作流程

过程

	命令或操作	目的
步骤 1	应用配置文件， 第 113 页	
步骤 2	自动进行 VPN 连接， 第 114 页	
步骤 3	AnyConnect 文档参考， 第 117 页	
步骤 4	会话参数， 第 117 页	

Cisco AnyConnect 部署

应用配置文件

将 Cisco AnyConnect 安全移动客户端下载到其设备后，ASA 必须为应用程序提供配置文件。

Cisco AnyConnect 安全移动客户端的配置文件包括 VPN 策略信息，例如公司 ASA VPN 网关、连接协议（IPSec 或 SSL）以及按需策略。

您可以通过以下方式之一为 Cisco Jabber iPhone 和 iPad 版本配置应用程序配置文件：

ASDM

我们建议您在 ASA 设备管理器 (ASDM) 上使用配置文件编辑器定义 Cisco AnyConnect 安全移动客户端的 VPN 配置文件。

使用此方法时，VPN 配置文件会在客户端首次建立 VPN 连接后自动下载到 Cisco AnyConnect 安全移动客户端。您可以对所有设备和 OS 类型使用此方法，也可以在 ASA 上集中管理 VPN 配置文件。

有关详细信息，请参阅您相应版本的《*Cisco AnyConnect* 安全移动客户端管理员指南》中的创建和编辑 *AnyConnect* 配置文件主题。

iPCU

您可以使用通过 iPhone 配置实用程序 (iPCU) 创建的 Apple 配置文件来配置 iOS 设备。Apple 配置文件是一种 XML 文件，包含设备安全策略、VPN 配置信息、Wi-Fi、邮件和日历设置等信息。

高级步骤如下所示：

1. 使用 iPCU 创建 Apple 配置文件。

   有关详细信息，请参阅 iPCU 的文档。

2. 将 XML 配置文件导出为 .mobileconfig 文件。

3. 将 .mobileconfig 文件通过电子邮件发送给用户。

   用户打开文件后，将 AnyConnect VPN 配置文件和其他配置文件设置安装到客户端应用程序。

MDM

您可以使用通过第三方移动设备管理 (MDM) 软件创建的 Apple 配置文件来配置 iOS 设备。Apple 配置文件是一种 XML 文件，包含设备安全策略、VPN 配置信息、Wi-Fi、邮件和日历设置等信息。

高级步骤如下所示：

1. 使用 MDM 创建 Apple 配置文件。

   有关使用 MDM 的信息，请参阅 Apple 文档。

2. 将 Apple 配置文件推送到注册的设备。

要为 Cisco Jabber Android 版本配置应用程序配置文件，请使用 ASA 设备管理器 (ASDM) 上的配置文件编辑器定义 Cisco AnyConnect 安全移动客户端的 VPN 配置文件。VPN 配置文件会在客户端首次建立 VPN 连接后自动下载到 Cisco AnyConnect 安全移动客户端。您可以对所有设备和 OS 类型使用此方法，也可以在 ASA 上集中管理 VPN 配置文件。有关详细信息，请参阅您相应版本的《*Cisco AnyConnect* 安全移动客户端管理员指南》中的创建和编辑 *AnyConnect* 配置文件主题。

自动进行 VPN 连接

当用户从公司 Wi-Fi 网络之外打开 Cisco Jabber 时，Cisco Jabber 需要 VPN 连接才能访问 Cisco UC 应用程序服务器。您可以将系统设置为允许 Cisco AnyConnect 安全移动客户端在后台自动建立 VPN 连接，从而确保为用户提供无缝连接体验。

注释 6023即使 VPN 设置为自动连接，VPN 也不会在移动设备和Remote Access Expressway 之前启动，因为后者优先级较高。

设置受信任的网络连接

受信任网络检测功能可根据用户位置自动执行 VPN 连接，从而提升用户体验。当用户在公司 Wi-Fi 网络内部时，Cisco Jabber 可以直接接通 Cisco UC 基础设施。当用户离开公司 Wi-Fi 网络时，Cisco Jabber 会自动检测到位于受信任的网络之外。在这种情况下，Cisco AnyConnect Secure 移动客户端将发起 VPN，以确保连接到 UC 基础设施。

注释 受信任的网络检测功能与基于证书和基于密码的验证相配合。但是，基于证书的身份验证可提供最高程度的无缝式用户体验。

过程

步骤 1 使用 ASDM 打开 Cisco AnyConnect 客户端配置文件。

步骤 2 列出客户端处于企业 Wi-Fi 网络内时接口可能收到的受信任 DNS 服务器和受信任 DNS 域名后缀。Cisco AnyConnect 客户端将对当前接口 DNS 服务器和域名后缀与配置文件中的设置进行比较。

注释 您必须指定所有 DNS 服务器，以确保受信任网络检测功能正常工作。如果您同时设置 TrustedDNSDomains 和 TrustedDNSServers，会话必须将要定义的两种设置同时匹配到受信任网络。

有关设置受信任网络检测的详细步骤，请参阅您对应版本的《*Cisco AnyConnect* 安全移动客户端管理员指南》中，配置 *AnyConnect* 功能（版本 2.5）或配置 *VPN* 访问（版本 3.0 或 3.1）一章中，受信任网络检测一节。

设置按需连接 VPN

Apple iOS 按需连接功能通过基于用户域自动进行 VPN 连接提升了用户体验。

当用户在公司 Wi-Fi 网络内部时，Cisco Jabber 可以直接接通 cisco UC 基础设施。当用户离开公司 Wi-Fi 网络时，Cisco AnyConnect 会自动检测是否已连接到您在 AnyConnect 客户端配置文件中指定的域。如果是这样，应用程序将发起 VPN 连接，以确保连接到 UC 基础设施。设备上的所有应用程序（包括 Cisco Jabber）均可以利用此功能。

注释 按需连接仅支持通过证书进行身份验证的连接。

此功能提供以下选项：

- **始终连接** — Apple iOS 始终尝试与该列表中的域建立 VPN 连接。
- **视需要连接** — Apple iOS 只有在无法利用 DNS 解析地址时才尝试与该列表中的域建立 VPN 连接。
- **始终连接** — Apple iOS 始终尝试与该列表中的域建立 VPN 连接。

注意 Apple 计划在不久的将来删除“始终连接”选项。在删除“始终连接”选项后，用户可以选择“视需要连接”选项。在某些情况下，Cisco Jabber 用户在使用“视需要连接”选项时可能会出现问题。例如，如果 Cisco Unified Communications Manager 的主机名可在公司网络之外进行解析，则 iOS 将不会触发 VPN 连接。用户可以通过在发起呼叫之前手动启动 Cisco AnyConnect 安全移动客户端解决此问题。

过程

步骤 1 使用 ASDM 配置文件编辑器、iPCU 或 MDM 软件打开 AnyConnect 客户端配置文件。

步骤 2 在 AnyConnect 客户端配置文件中，在“视需要连接”部分，输入可按需连接的域列表。

域列表可以包含通配符选项（例如，cucm.cisco.com、cisco.com 和 *.webex.com）。

在 Cisco Unified Communications Manager 上设置自动 VPN 访问

开始之前

- 必须将移动设备设置为通过基于证书的身份验证按需连接到 VPN。如需有关设置 VPN 连接的帮助，请联系您的 VPN 客户端和头端提供商。
- 有关 Cisco AnyConnect 安全移动客户端和 Cisco 自适应安全设备的要求，请参阅软件要求主题。
- 有关设置 Cisco AnyConnect 的信息，请参阅《*Cisco AnyConnect VPN* 客户端维护和操作指南》。

过程

步骤 1 确定将引导客户端按需启动 VPN 的 URL。

a) 使用以下方法之一确定引导客户端按需启动 VPN 的 URL。

- 视需要连接
  - 配置 Cisco Unified Communications Manager 通过域名（不是 IP 地址）访问，并确保此域名无法在防火墙外部解析。
  - 将此域名包含在 Cisco AnyConnect 客户端连接的按需连接域名列表中的“视需要连接”列表中。
- 始终连接
  - 将步骤 4 中的参数设置为不存在的域名。当用户在防火墙内部或外部时，不存在的域名会导致 DNS 查询失败。
  - 将此域名包含在 Cisco AnyConnect 客户端连接的按需连接域名列表中的“始终连接”列表中。

    URL 必须仅包含域名。不要包含协议或路径（例如，使用“cm8ondemand.company.com”而不是 “https://cm8ondemand.company.com/vpn”。

b) 在 Cisco AnyConnect 中输入 URL，并验证此域上的 DNS 查询是否失败。

步骤 2 打开 **Cisco Unified CM 管理**界面。

步骤 3 导航到用户的设备页面。

步骤 4 在**产品特定配置布局**部分的**按需 VPN URL** 字段中，输入您在步骤 1 中为 Cisco AnyConnect 确定和使用的 URL。

URL 只能是域名，不能是协议或路径。

步骤 5 选择**保存**。

当 Cisco Jabber 打开时，它会向 URL 发起 DNS 查询。如果此 URL 与您在此过程中定义的按需域名列表条目（例如，cisco.com）匹配，Cisco Jabber 将间接发起 AnyConnect VPN 连接。

下一步做什么

- 测试此功能。
  - 在 iOS 设备的互联网浏览器中输入 URL，然后验证是否自动启动 VPN。您应在状态栏中看到一个 VPN 图标。
  - 验证 iOS 设备是否可以使用 VPN 连接到公司网络。例如，在公司内联网上访问网页。如果 iOS 设备无法连接，请联系您的 VPN 技术提供商。
  - 与您的 IT 部门核实，您的 VPN 不会限制访问某些类型的流量（例如，管理员是否将系统设置为只允许电子邮件和日历流量）。
- 验证您将客户端设置为直接连接到公司网络。

AnyConnect 文档参考

有关 AnyConnect 要求和部署的详细信息，请参阅您对应版本的文档，网址如下：https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

会话参数

您可以配置 ASA 会话参数来改善安全连接的性能。为了实现最佳的用户体验，您应配置以下 ASA 会话参数：

- 数据包传输层安全 (DTLS) — DTLS 是一个 SSL 协议，它提供了可防止延迟和数据丢失的数据路径。
- 自动重连 — 自动重连或会话保持，允许 Cisco AnyConnect 安全移动客户端从会话终端中恢复，并重新建立会话。
- 会话保持 — 该参数允许 VPN 会话从服务中断中恢复，并重新建立连接。
- 空闲超时 — 空闲超时定义了一个时间段，如果在这段时间内没有任何通信活动，ASA 将会终止安全连接。
- 失效对端检测 (DTD) — DTD 确保 ASA 和 Cisco AnyConnect 安全移动客户端能够快速检测失败的连接。

设置 ASA 会话参数

我们建议您按照以下方式设置 ASA 会话参数，以优化 Cisco AnyConnect 安全移动客户端的最终用户体验。

过程

步骤 1 设置 Cisco AnyConnect 以使用 DTLS。

有关详细信息，请参阅《*Cisco AnyConnect VPN* 客户端管理员指南 》（版本 2.0）中， 使用 *ASDM* 配置 *AnyConnect* 功能一章中，通过 *AnyConnect (SSL)* 连接启用数据报传输层安全 *(DTLS)* 主题。

步骤 2 设置会话保持（自动重连）。

a) 使用 ASDM 打开 VPN 客户端配置文件。

b) 将**自动重新连接行为**参数设置为**恢复后重新连接**。

有关详细信息，请参阅您对应版本的《*Cisco AnyConnect* 安全移动客户端管理员指南》中，配置 *AnyConnect* 功能（版本 2.5）或配置 *VPN* 访问 （版本 3.0 或 3.1）一章中的配置自动重连主题。

步骤 3 设置空闲超时值。

a) 创建针对具体 Cisco Jabber 客户端的组策略。

b) 将“空闲超时”的值设置为 30 分钟。

有关详细信息，请参阅您对应版本的《*Cisco ASA 5580* 自适应安全设备命令参考》的 *vpn* 空闲超时部分。

步骤 4 设置失效对端检测 (DPD)。

a) 禁用服务器端 DPD。

b) 启用客户端 DPD。

有关详细信息，请参阅《*Cisco ASA 5500* 系列配置指南》，配置 *VPN*一章中启用和调整失效对端检测主题（使用 CLI、8.4 和 8.6）。

第 15 章

故障诊断

更新 Cisco Jabber 域的 SSO 证书

此过程适用于云或混合部署。使用此程序为您的 Cisco Jabber 域上传更新的单点登录 (SSO) 证书。

注释 仅支持采用 1024、2048 或 4096 加密位和 RC4-MD5 算法的证书。

开始之前

证书必须为 .CER 或 .CRT 文件格式。

过程

步骤 1 登录Webex组织管理工具，地址https://www.webex.com/go/connectadmin。

步骤 2 在加载管理工具后，单击**配置**选项卡。

步骤 3 在左侧导航栏中，单击**安全设置**。

步骤 4 单击**组织证书管理**链接。
将显示之前导入的 x.509 证书。

步骤 5 在**别名**字段中，输入您的公司的Cisco Webex组织。

步骤 6 单击**浏览**导航到 x.509 证书。
证书必须为 .CER 或 .CRT 文件格式。

步骤 7 单击**导入**以导入证书。
如果证书不符合为 x.509 证书指定的格式，将会显示错误。

步骤 8 单击**关闭**两次，返回到 **SSO 相关选项**屏幕。

步骤 9 单击**保存**以保存联合 Web 单点登录配置详细信息。

Cisco Jabber 诊断工具

Windows 和 Mac

Cisco Jabber 诊断工具提供以下功能的配置和诊断信息：

- 服务发现
- Cisco Webex
- Cisco Unified Communications Manager 摘要
- Cisco Unified Communications Manager 配置
- 语音邮件
- 证书验证
- Active Directory
- DNS 记录

要访问 Cisco Jabber 诊断工具窗口，用户必须将中央窗口置于焦点，然后输入 **Ctrl + Shift + D**。用户可以通过单击**重新加载**按钮更新数据。用户还可以单击**保存**按钮，将信息保存到 HTML 文件。

默认情况下，Cisco Jabber 诊断工具可用。要禁用此工具，必须将 DIAGNOSTICS_TOOL_ENABLED 安装参数设置为 FALSE。有关此安装参数的详细信息，请参阅 *Cisco Jabber* 内部部署或 *Cisco Jabber* 云和混合部署，具体取决于您的设置。

Android、iPhone 和 iPad

如果用户无法登录到 Cisco Jabber，或者您的 Cisco Jabber IM 和电话服务未连接，可以使用**诊断错误**选项检查问题原因。

用户可以在**登录**页或在连接到 Cisco Jabber 服务时收到的警告通知中点击**诊断错误**选项。然后，Cisco Jabber 会验证：

- 是否存在任何网络问题
- 是否可访问 Cisco Jabber 服务器
- 是否可以重新连接 Cisco Jabber

如果其中任何一项检查失败，Cisco Jabber 会显示一份错误报告，并在其中给出可能的解决方案。如果问题仍然存在，则可能会发送问题报告。