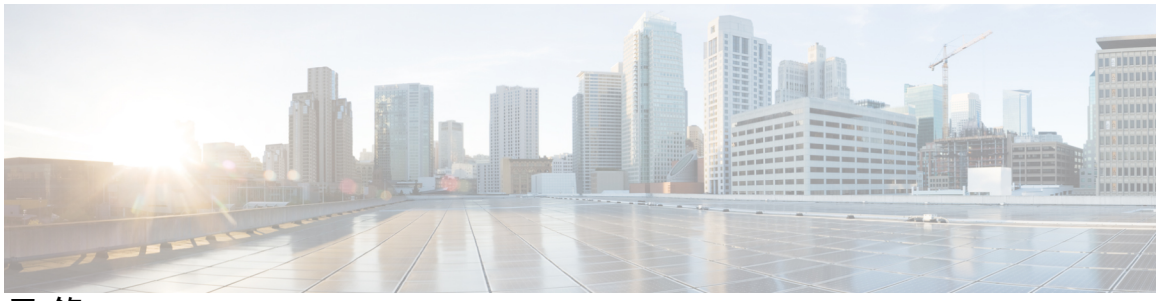
Cisco Jabber 12.9 規劃指南

第一次發佈日期: 2020 年 7 月 9 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



目錄

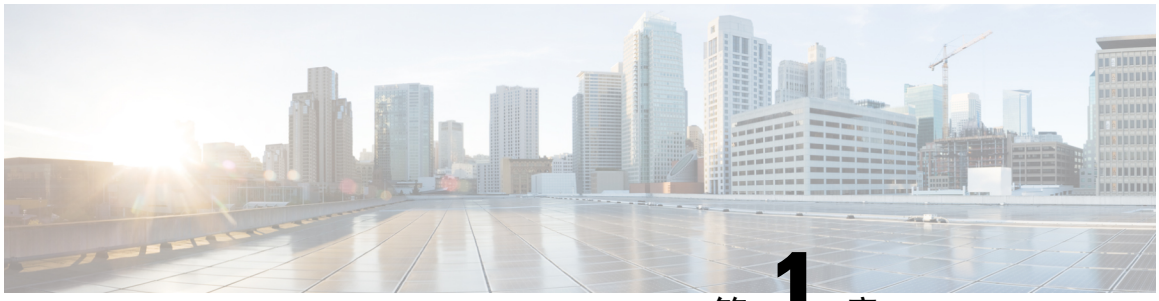
新資訊及變更的資訊

- 新資訊及變更的資訊 ，第 xiii 頁上的

新資訊及變更的資訊

日期	狀態	說明	位置
		初次發佈	
	已更新	已移除對 Android OS 5.x 的支援	Android 版 Cisco Jabber 的硬體需求
	已更新	Mac 現在僅支援 IM 螢幕共用	僅即時訊息螢幕共用
	已更新	不再支援 iOS 12.x	iPhone 和 iPad 版 Cisco Jabber 的硬體需求
	已更新	現在支援 Unified SIP SRST 12.8	可存活性遠端位址電話技術

新資訊及變更的資訊



第 1 章

需求

伺服器需求

以下軟體需求對於此版本中的所有 Cisco Jabber 用戶端都爲通用的：

服務	軟體需求	支援的版本
IM and Presence	Cisco Unified Communications Manager IM and Presence Service	10.5(2) 及更新版本(最低) 11.5(1) SU3 或更新版本(建議使用)
	Cisco Webex Messenger	
電話	Cisco Unified Communications Manager	10.5(2) 及更新版本(最低) 11.5(1) SU3 或更新版本(建議使用)
	Cisco Unified Survivable Remote Site Telephony	Unified SIP SRST 12.8 及更高版本
聯絡人搜尋	LDAP 目錄	符合 LDAP v3 的目錄，例如 Microsoft Active Directory 2008 R2 和 Open LDAP 2.4 或更高版本
語音信箱	Cisco Unity Connection	10.5 及更高版本
多線路	Cisco Unified Contact Center Express	11.6

服務	軟體需求	支援的版本
會議	Cisco Meeting Server	2.2 及更高版本
	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 或更高版本
	雲端 CMR	Cisco Webex Meetings 協作會議室與伺服器
	Cisco Webex Meetings 伺服器	2.8 MR1 及更高版本
	Cisco Webex Meetings 中心	WBS33 及更高版本
遠端存取	Cisco Adaptive Security Appliance 僅Android 版 Cisco Jabber。	8.4 (1) 及更高版本
	Cisco AnyConnect Secure Mobility Client 僅 iPad 及 iPhone 版 Cisco Jabber 與 Android 版 Cisco Jabber 用戶端。	依平台而定
	Cisco Expressway C	X8.10.1 及更新版本
	Cisco Expressway E	X8.10.1 及更高版本。

Cisco Jabber 在啓動過程中使用網域名系統(DNS)伺服器，DNS 伺服器爲 Cisco Jabber 設定所必需的。

作業系統需求

適用於 **Windows** 版 **Cisco Jabber** 的作業系統

您可以在以下作業系統上安裝 Windows 版 Cisco Jabber：

- Microsoft Windows 10 (桌面模式)
- Microsoft Windows 8.1 (桌面模式)
- Microsoft Windows 8 (桌面模式)

Windows 版 Cisco Jabber 不需 Microsoft.NET Framework 或任何 Java 模組。

Windows 10 服務選項

Windows 版 Cisco Jabber 支援以下 Windows 10 服務選項：

- 現有分支(CB)
- 現有業務分支(CBB)
- 長期服務部門(LTSB)-使用此選項，您有責任確保部署任何相關的服務更新。

有關 Windows 10 服務選項的更多資訊，請參閱以下 Microsoft 說明文件：https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx。

附註 預設情況下，Cisco Jabber 將所需檔案安裝到以下目錄：

- %temp%\ Cisco Systems \ Cisco Jabber-Bootstrap.properties 檔案和安裝記錄檔
- %LOCALAPPDATA%\ Cisco \ Unified Communications -記錄檔和臨時遙測資料
- %APPDATA%\ Cisco \ Unified Communications 緩存的組態和帳戶憑證
- 用於 x86 Windows 版%ProgramFiles%\ Cisco Systems \ Cisco Jabber 安裝檔案
- 用於 x64 Windows 版%ProgramFiles(x86)%\ Cisco Systems \ Cisco Jabber 安裝檔案

適用於 Mac 版 Cisco Jabber 的作業系統

您可以在以下作業系統上安裝 Mac 版 Cisco Jabber：

- macOS Catalina 10.15 或更高版本
- macOS Mojave 10.14 或更高版本
- macOS High Sierra 10.13 (或更新版本)

Android 版 Cisco Jabber 的作業系統

有關最新支援的作業系統版本資訊，請參閱 Play 商店。

附註 Android 版 Cisco Jabber 可作爲 32 位應用程式和 64 位應用程式提供。如果您的 Android 裝置具有 64 位作業系統，則可以透過執行 64 位 Jabber 用戶端來獲得更快，更豐富的體驗。

附註 如果 Cisco Jabber 安裝在 Android 6.0 Marshmallow OS 或更高版本上，且保持空閒狀態：

- 與 Cisco Jabber 的網路連線已停用。
- 使用者不會收到任何電話或訊息。

點按**更改設定**並忽略電池最佳化以接聽電話和接收訊息。

適用於 Android 5.x 最新 Jabber 版本的支援

Cisco Jabber 12.8 爲支援執行 Android 5.x 的裝置的最新版本。

下一個 Jabber 版本將終止對所有無法升級到 Android 6.x 的裝置的支援。

iPhone 和 iPad 版 Cisco Jabber 的作業系統

有關最新支援的作業系統版本資訊，請參閱 App Store。

重要須知 Cisco 僅支援目前 App Store 版本的 iPhone 和 iPad 版 Cisco Jabber。任何 Cisco Jabber 版本中發現的瑕疵皆將對照目前的版本評估。

硬體需求

桌面用戶端硬體需求

需求	**Windows 版 Cisco Jabber**	**Mac 版 Cisco Jabber**
已裝 RAM	Microsoft Windows 7 和 Windows 8：2 GB RAM	2-GB RAM
可用實體記憶體	128 MB	1 GB
可用磁碟空間	256 MB	300 MB

需求	Windows 版 Cisco Jabber	Mac 版 Cisco Jabber
CPU 速度與類型	AMD Mobile Sempron 3600+ 2 GHz Intel Core 2 Duo T7400 @ 2。16 GHz	在下列任何 Apple 硬體中安裝 Intel Core 2 Duo 或更新的處理器： • 即時訊息ac Pro • MacBook Pro(包括 Retina 顯示器機型) • MacBook • MacBook Air • iMac • Mac Mini
I/O 連線埠	USB 2.0，適用於 USB 攝影機及音訊裝置。	USB 2.0 適用於 USB 攝影機及音訊裝置

CTI 支援的裝置

要查看 Unified Communications Manager 支援的電腦電話整合(CTI)裝置清單：

1. 在**Cisco統一報告**頁面中自**系統報告**功能表選擇**Unified CM 電話功能清單**。
2. 開啓報告後，自**功能**下拉清單選擇 **CTI 控制**。

Android 版 Cisco Jabber 的硬體需求

Android 裝置的最低需求：

Android 作業系統	CPU	顯示器
6.0 或更高版本	1.5 GHz 雙核 建議使用使用：1.2 GHz 四核或更高	雙向視訊：480p x 800p 或更高。 僅即時訊息：320p x 480p 或更高。

Android 版 Cisco Jabber 在具有以下 OS 版本的裝置中支援完全 UC 模式：

表 *1:* 支援的 *Android* 裝置

裝置	機型	最低 Android OS 版本	備註
BlackBerry	Priv	6.0.1	若 Jabber 已從最近檢視的應用程式清單中移除且裝置已有一段時間保持在閒置狀態，則 Jabber 變爲非活躍狀態。
Fujitsu	Arrows M357	6.0.1	

裝置	機型	最低 Android OS 版本	備註
Google	Nexus 5	6.0	
	Nexus 5X	6.0	
	Nexus 6	6.0	
	Nexus 6P	6.0	如果您有安裝 Android 作業系統 6.x 或 7.0 版的 Google Nexus 6P 裝置，請聯絡您的管理員，以便將您的 Jabber 電話服務設定爲安全性電話服務。否則，您的裝置可能無法回應。 如果您的 Android 作業系統爲 7.1 或更高版本則不需採取任何動作。
	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 通話期間，如果使用者將音訊從行動裝置切換到頭戴式耳機，則可能會出瞬時性的音訊問題。
	Pixel XL	8.0	在 Jabber 通話期間，如果使用者將音訊從行動裝置切換到頭戴式耳機，則可能會出瞬時性的音訊問題。
	Pixel 3	8.0	如果您將附帶的耳機與手機一起使用，則可能會有幾秒鐘的音訊問題。
	Pixel XL	8.0	如果您將附帶的耳機與手機一起使用，則可能會有幾秒鐘的音訊問題。
Honeywell Dolphin	CT50	6.0	
	CT40	7.1.1	
	CT60	7.1.1 和 8.1	我們僅在 Android OS 7.1.1 和 8.1 上支援 CT60。

裝置	機型	最低 Android OS 版本	備註
HTC	10	6.0	
	A9	6.0	
	M8	6.0	
	M9	6.0	
	X9	6.0	
華爲 [1]	Honor 7	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	
	Mate 20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	
LG	G3	6.0	
	G4	6.0	
	G5	6.0	
	G6	7.0	
	V10	6.0	
	V30	8.0	

裝置	機型	最低 Android OS 版本	備註
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	

裝置	機型	最低 Android OS 版本	備註

Samsung	全部	6.0	• 不再支援無法升級到 Android OS 6.x 或更高版本的裝置。
			• 啓用 Jabber 的自動執行選項。
			對於 Android 作業系統 6.x 和更新版本，您可以在 **Smart Manager 應用程式**底下找到自動執行選項。
			• Jabber 在加拿大的 Samsung Galaxy Tab Pro 8.4(機型 T320UEU1AOC1)上會延遲來電通知快顯視窗的顯示速度。
			• Jabber 在失去 Wi-Fi 連線能力時，在 Samsung Xcover 3 上重新連線網路會發生延遲。
			• 搭載晶片組 Exynos 7580 的 Samsung 裝置中有音訊品質的問題。當裝置螢幕關閉時，音訊變得不清楚。以下是裝置清單：
			  • 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	
Son即時訊息	XP8	7.1.1	

裝置	機型	最低 Android OS 版本	備註
Sony Xperia	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z2	6.0	
	Z2 tablet	6.0	
	Z3	6.0	安裝 Android 作業系統 5.0.2 的 Sony Xperia Z3(機型 SO-01G)在進行 Jabber 通話時音訊品質不良。
	Z3 Tablet Compact	6.0	
	Z3+/Z4	6.0	在 Sony Z3+ 及 Z4 上，視訊通話不穩定。視訊通話時嘗試停用自己的影像，否則請僅撥打語音電話。
	Z4 TAB	6.0	
	Z5 Premium 和 Z5	6.0	

裝置	機型	最低 Android OS 版本	備註
小米	4C	6.0	這些裝置上僅可執行 32 位版本。
	MAX	6.0	
	Mi 4	6.0	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Mi 10	10.0	
	Pocophone	8.0	
	Mi Note	6.0	這些裝置上僅可執行 32 位版本。
	Mi Note 2	7.0	
	Mi MIX 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] 由於 EMUI 10 中的更改，當您的裝置鎖定時，來電提示可能不會出現。在 Jabber 中移至**設定值** > **通知**然後選擇**標語**。

Jabber 對 Samsung Knox 的支援

Android 版 Cisco Jabber 支援 Samsung Knox，如下：

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

附註 當您在 Samsung Know 中執行 Android 版 Cisco Jabber 時，Samsung Knox 的安全設計會要求您首先解鎖 Knox。在解鎖 Knox 之前，您無法使用 Jabber 接聽或拒絕來電。

Jabber 支援 Samsung Dex

Android 版 Cisco Jabber 在 Samsung S8，S8 Plus 和 Note 8 中支援 Samsung Dex。

舊版 Android 版 Cisco Jabber 上的支援政策

由於 Android 核心問題，Cisco Jabber 在某些 Android 裝置上無法註冊到 Cisco Unified Communications Manager。爲解決此問題，請嘗試下列方法：

將 Android 核心升級至 3.10 或更高版本。

設定 Cisco Unified Communications Manager 使用混合模式安全性，啓用安全 SIP 通話訊號，並且使用連線埠 5061。如需使用 Cisco CTL Client 設定混合模式的說明，請參閱您版本的 *Cisco Unified Communications Manager* 安全性指南。可以在 Cisco Unified Communications Manager 維護與操作指南中找到安全性指南。此解決辦法適用於下列支援的裝置：

裝置機型	作業系統
HTC M8	Android 作業系統 6.0 或更高版本
HTC M9	Android 作業系統 6.0 或更高版本

裝置機型	作業系統
Sony Xperia Z2	Android 作業系統 6.0 或更高版本及 3.10.49 之前的核心版本。 若裝置的 Android OS 爲 6.0 或更高版本，核心爲 3.10.49 或更高版本，則裝置可支援非安全模式。
Sony Xperia Z2 平板	
Sony Xperia Z3	
Sony Xperia Z3 Tablet Compact	
小米 Mi4	Android 作業系統 6.0 或更高版本
小米 Mi Note	Android 作業系統 6.0 或更高版本
Honeywell Dolphin CT50	Android 作業系統 6.0 或更高版本

支援的藍牙裝置

藍牙裝置	相依性
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，您可能會遇到問題，因爲這些裝置之間有相容性問題。
Jabra Motion	將 Jabra Motion 藍牙耳機升級至韌體版本 3.72 或更高版本。 韌體版本爲 3.72 或更高版本的 Jabra Motion 藍牙耳機可支援 Cisco Jabber 通話控制。
Jabra Wave+	
Jabra Biz 2400	
Jabra Easygo	
Jabra PRO 9470	
Jabra Speak 510	
Jabra Supreme UC	

藍牙裝置	相依性
Jabra Stealth	
Jabra Evolve 65 UC Stereo	
Jawbone ICON for Cisco 藍牙耳機	如果您使用 Samsung Galaxy S4，您可能會遇到問題，因爲這些裝置之間有相容性問題。

藍牙限制：

- 在 Samsung Galaxy SIII 上使用藍牙裝置可能會造成鈴聲和通話音訊失真。
- 如果使用者在 Jabber 通話期間將藍牙耳機斷開後再重新連接則使用者將無法聽到音訊。使用 Android 5.0 之前的 OS 版本的智慧型手機會有這項限制。
- 在作業系統爲 Android 6.0 的 Sony Z4 / LG G4 /裝置中，使用者在開始 Jabber 通話後切換到藍牙耳機時會遇到音訊丟失的情況。此問題的解決方法爲將音訊輸出裝置切換至喇叭然後再切換回藍牙，或爲在進行 Cisco Jabber 通話之前先連接藍牙耳機。

支援的 Android Wear

所有配備 Android 作業系統 5.0 或更新版本及 Google 服務 8.3 或更新版本的 Android Wear 裝置皆可執行 Cisco Jabber。Cisco Jabber 已在以下 Android Wear 裝置上測試過：

- Fossil Gen 3 智能手錶
- Huawei watch
- LG G Watch R
- LG Watch Urbane
- Moto 360
- Moto 360 (第 2 代)
- Samsung Gear Live
- Sony SmartWatch 3

附註 適用於 Android Wear 裝置的 Cisco Jabber 安裝程式與主要的 Jabber APK 檔案爲分開的檔案。將穿戴裝置與行動裝置配對時，使用者可以從 Google Play 商店獲取 Android Wear 安裝程式。

支援的 Chromebook 型號

Chromebook 必須具有 Chrome OS 53 或更高版本。使用者可自 Google Play 商店中將 Android 版 Cisco Jabber 下載到其 Chromebook 中。

- HP Chromebook 13 G1 筆記型電腦
- Google Chromebook Pixel

- Google Chromebook Pixelbook
- Samsung Chromebook Pro
- 華碩 C302

iPhone 和 iPad 版 Cisco Jabber 的硬體需求

iPhone 和 iPad 版 Cisco Jabber 支援執行 iOS 、iOS 13.x 和 iPadOS的以下 Apple 裝置。不支援未升級到這些版本的裝置。

蘋果裝置	版本
iPad	第 5、6 和 7 代
iPad Air	Air 1、Air 2 和 Air 3
iPad Pro	9.7 和 10.5 吋 12.9 吋，第一代、第二代和第三代
iPAD mini	Mini 2、Mini 3、Mini 4 和 Mini 5
iPhone	5s、6、6 Plus、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 上執行的 WatchOS 5。

iPhone 及 iPad 支援下列藍牙耳機：

製造商	型號
Apple	AirPod
Cisco	561, 562
Jabra	BIZ 2400，Easygo，Evolve 65 UC 立體聲，EXTREME 2，Motion [2]，PRO 9470，適用於 Cisco 的 Speak 450，Speak 510，Stealth Supreme UC，Wave +
Jawbone	Jawbone ICON for Cisco 藍牙耳機
Plantronics	Voyager Edge，Voyager Edge UC，Voyager Legend，Voyager Legend UC
Sony Ericsson	MW-600

[2] 支援 Cisco Jabber 通話的藍牙控制。僅韌體版本 3.72 支援此功能。

網路需求

在透過公司 Wi-Fi 網路使用 Cisco Jabber 時，若要獲得最佳使用者體驗，建議您：

- 設計您的 Wi-Fi 網路，以盡可能消除覆蓋範圍的間隙，包括電梯、樓梯和外面走廊之類的區網域。
- 確保所有存取點給行動裝置指定相同的 IP 位址。如果通話期間 IP 位址變更，則通話會中斷。
- 確保所有存取點具有相同的 SSID；如果 SSID 不符，越區切換可能會非常慢。
- 確保所有存取點廣播其 SSID。如果存取點不廣播其 SSID，則行動裝置可能會提示使用者加入其他 Wi-Fi 網路，而這會中斷通話。
- 確保將企業防火牆配置爲允許 NAT 會話遍歷公用工具(STUN)資料包的傳輸。

執行全面的站點調查，盡量減少會影響語音品質的網路問題。我們建議使用您執行以下操作：

- 驗證未重疊的通道組態、存取點覆蓋範圍以及所需的資料和流量速率。
- 消除異常的存取點。
- 識別和減輕潛在干擾來源的影響。

如須更多詳細資訊，請參閱以下說明文件：

- 企業行動化設計指南中的 “VoWLAN 設計建議使用”一節。
- *Cisco Unified* 無線 *IP* 電話 *7925G* 部署指南。
- *IEEE 802.11g* 的容量範圍與部署考量白皮書。
- 適用於您 Cisco Unified Communications ManagerCisco Unified Communications ManagerCisco Unified Communications Manager 版本的解決方案參考網路設計 *(SRND)*。

IPv6 需求：

Cisco Jabber 11.6 完全支援 IPv6，且會在單純的 IPv6 和混合式網路中正常運作，但有一些限制，這些限制列在此章節中。Cisco Collaboration 解決方案目前未能完整支援 IPv6。例如，Cisco VCS Expressway for Mobile and Remote Access 在單純的 IPv6 網路中有一些限制，這種網路必須在行動裝置電信業者網路中部署 NAT64/DNS64。Cisco Unified Communications Manager 與 Cisco Unified Communications Manager IM and Presence 目前不支援單純 IPv6 網路中的 HTTPS。

在 Jabber 中設定此功能的方式爲使用 IP_Mode 參數將通訊協定設爲 IPv4、IPv6 或兩者皆使用。兩者皆使用爲預設設定。 IP_Mode參數可以包含在 Jabber 用戶端組態中(請參閱最新版本的 *Cisco Jabber* 的參數參考指南)，Windows 版引導檔案以及 Mac 和 Mobile 用戶端的 URL 組態。

Jabber 在連線服務時所使用的網路 IP 通訊協定爲由以下因素所決定：

- Jabber 用戶端組態 IP_Mode 參數。
- 用戶端作業系統 IP 功能。

- 伺服器作業系統 IP 功能。
- IPv4 和 IPv6 的 DNS 記錄可用性。
- Cisco Unified Communications Manager 對於 IPv4、IPv6 或這兩者的軟體電話裝置組態的 SIP 設定。軟體電話裝置的 SIP 連線設定必須符合 Jabber IP_Mode 參數設定，才能建立成功的連線。
- 基礎網路 IP 功能。

在 Cisco Unified Communications Manager 上，IP 功能爲由一般伺服器設定和裝置特有的設定所決定。下表列出在給定的各種設定之下所預期的 Jabber 連線，此清單假設 IPv4 和 IPv6 的 DNS 記錄皆已設定。

當用戶端作業系統，伺服器作業系統和 Jabber IP_Mode 參數設定爲“兩者皆使用”時，Jabber 將依據 RFC6555 將 IPv4 或 IPv6 位址用於與伺服器的連線。

用戶端作業系統	伺服器作業系統	Jabber IP_Mode 參數	Jabber 連線結果
僅 IPv4	僅 IPv4	僅 IPv4	IPv4 連線
		僅 IPv6	連線失敗
		皆使用	IPv4 連線
僅 IPv4	僅 IPv6	僅 IPv4	連線失敗
		僅 IPv6	連線失敗
		皆使用	連線失敗
僅 IPv6	僅 IPv4	僅 IPv4	連線失敗
		僅 IPv6	連線失敗
		皆使用	連線失敗
僅 IPv6	僅 IPv6	僅 IPv4	連線失敗
		僅 IPv6	IPv6 連線
		皆使用	IPv6 連線
僅 IPv4	皆使用	僅 IPv4	IPv4 連線
		僅 IPv6	連線失敗
		皆使用	IPv4 連線
僅 IPv6	皆使用	僅 IPv4	連線失敗
		僅 IPv6	IPv6 連線
		皆使用	IPv6 連線

用戶端作業系統	伺服器作業系統	Jabber IP_Mode 參數	Jabber 連線結果
皆使用	僅 IPv4	僅 IPv4	IPv4 連線
		僅 IPv6	連線失敗
		皆使用	IPv4 連線
皆使用	僅 IPv6	僅 IPv4	連線失敗
		僅 IPv6	IPv6 連線
		皆使用	IPv6 連線
皆使用	皆使用	僅 IPv4	IPv4 連線
		僅 IPv6	IPv6 連線
		皆使用	IPv6 連線

在僅 IPv6 模式下使用 Jabber 時，需要 NAT64 / DNS64 才能連線至 IPv4 基礎結構，例如Cisco Webex Messenger服務，用於for Mobile and Remote Access的 Cisco VCS Expressway，以及Cisco Webex Platform 服務。

桌面裝置支援可用於僅 IPv6 的公司處丶所內部署。所有 Jabber 行動裝置必須配置爲兩個堆棧。

如需 IPv6 部署詳細資訊，請參閱《Cisco Collaboration 系統 12.0 版 IPv6 部署指南》。

限制

- HTTPS 連線
  - 在公司處丶所內部署中，Cisco Jabber 僅支援 IPv4 和兩個堆棧模式，以連線至 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service。這些伺服器當前不支援 IPv6 HTTPS 連線。

    Cisco Jabber 可以使用 HTTPS 連線至僅使用 IPv6 模式的語音信箱的 Cisco Unity Connection。

- Cisco Webex Messenger 限制
  - Cisco Webex Messenger 在 IPv6 上不受支援。

- 電話技術限制
  - 當您在 Cisco Unified Communications Manager 上將使用者裝置升級到“兩者皆使用”或僅將 IPv6 升級時，對應的 Jabber 用戶端必須升級到 11.6 或更高版本。
  - 當安裝中包含 IPv4 端點和 IPv6 端點時，建議使用您使用硬體 MTP 在這些裝置之間橋接音訊和視訊。硬體 MTP 與 Cisco IOS 版本 15.5 支援此功能。例如，Cisco 3945 路由器必須執行以下 T-train 現行版本：c3900e-universalk9-mz.SPA.155-2.T2.bin。
  - 目前我們尚無詳細解決方案，以在包括 Jabber 在內的 Cisco 端點中同時支援 IPv4 和 IPv6。Cisco Unified Communications Manager 支援僅 IPv4 和僅 IPv6 的當前功能。需要 MTP 來支援僅 IPv4 端點和僅 IPv6 端點之間的通話，或僅支援 IPv4 或僅 IPv6 閘道之間的通話。

- IPv6 不支援 Jabber 至 Jabber 的通話。

- 檔案傳輸限制
  - 進階檔案傳輸-當爲兩者皆使用配置了用戶端且 Cisco Unified Communications Manager IM and Presence Service 啓用了兩者皆使用時，以下 Cisco Unified Communications Manager IM and Presence Service 版本支援進階檔案傳輸：
    - 10.5.2 SU2
    - 11.0.1 SU2
    - 11.5
  - 人對人檔案傳輸-對於公司處所內的部署，不支援 IPv4 和 IPv6 用戶端之間的人對人檔案傳輸。如果您同時具有 IPv4 和 IPv6 用戶端的網路組態，建議使用您配置進階檔案傳輸。

- Mobile and Remote Access 的限制
  - Cisco VCS Expressway for Mobile and Remote Access 不支援 IPv6。
  - 如果將 Cisco Unified Communications Manager 配置爲進行 IPv6 SIP 連線，則無法使用 Cisco VCS Expressway Mobile and Remote Access 連線至 Cisco Unified Communications Manager 以使用電話服務。

Android 中 IPv6 支援的需求

Android 作業系統需求

Android 5.0 及更高版本

網路需求

- 僅 IPv4 模式(Android 僅接受 IPv4 位址)
- 具有 SLAAC 的兩者皆使用(Android 接受 IPv4 和 IPv6 位址)
- NAT64 或 DNS64(伺服器使用 IPv4 位址，用戶端使用 IPv6 位址)

限制

- DHCPv6 限制
  - Android 裝置不支援 DHCPv6。

- Android OS 限制
  - Android 作業系統不支援僅 IPv6 網路。有關此限制的更多資訊，請參見 Android 開發人員連結。

通訊埠與通訊協定

用戶端使用下表中列出的連線埠和通訊協定。如果您打算在用戶端與伺服器之間部署防火牆，請將防火牆設定爲允許這些連線埠和通訊協定。

	連線埠	應用程式層通訊協定	傳輸層通訊協定	說明
組態				
	6970	HTTP	TCP	連線至 TFTP 伺服器，以下載用戶端組態檔案。
	6972	HTTPS	TCP	連線至 TFTP 伺服器，以安全地下載 Cisco Unified Communications Manager 11.0 及更新版本適用的用戶端組態檔案。
	53	DNS	UDP	主機名稱解析。
	3804	CAPF	TCP	發行公司處丶所內重要憑證 (LSC) 給 IP 電話。此連線埠爲供 Cisco Unified Communications Manager 憑證授權單位proxy 功能 (CAPF) 註冊使用的監聽連線埠。
	8443	HTTPS		Cisco Unified Communications Manager 與 Cisco Unified Communications Manager IM and Presence Service的通訊。
	8191	SOAP	TCP	連線至本機連線埠，以提供簡易物件存取通訊協定 (SOAP) Web 服務。
目錄整合—對於 LDAP 聯絡人解析，將會根據 LDAP 組態使用下列其中一個連線埠。				
	389	LDAP	TCP	LDAP TCP (UDP) 連線至 LDAP 目錄服務。
	3268	LDAP	TCP	連線至全網域編目伺服器，以搜尋聯絡人。
	636	LDAPS	TCP	LDAPS TCP 安全連線至 LDAP 目錄服務。
	3269	LDAPS	TCP	LDAPS TCP 安全連線至全網域編目伺服器。
即時訊息與狀態				

	連線埠	應用程式層通訊協定	傳輸層通訊協定	說明
	443	XMPP	TCP	至 Webex Messenger 服務的 XMPP 流量用戶端僅在雲端部署中透過此連線埠傳送 XMPP。如果連線埠 443 被封鎖，用戶端將後退至連線埠 5222。
	5222	XMPP	TCP	連線至 Cisco Unified Communications Manager IM and Presence Service，以傳送即時訊息和狀態。
	37200	SOCKS5 位元組資料流	TCP	對等檔案傳輸，在內部部署中，用戶端亦使用此連線埠傳送螢幕擷取內容。
	7336	HTTPS	TCP	MFT 檔案傳輸 (僅限內部部署)。
Communication Manager 訊號傳送				
	2748	CTI	TCP	用於進行桌面電話控制的電腦電話語音介面 (CTI)。
	5060	SIP	TCP	提供作業階段啓始通訊協定 (SIP) 通話訊號傳送。
	5061	SIP over TLS	TCP	SIP over TCP 提供安全的 SIP 通話訊號傳送。(在裝置啓用安全 SIP 時使用。)
	30000 到 39999	FECC	UDP	遠端攝影機控制 (FECC)。
	5070 到 6070	BFCP	UDP	二進位發言權控制通訊協定 (BFCP) 提供視訊螢幕共用功能。
語音或視訊媒體交換				
	16384 到 32766	RTP/SRTP	UDP	用於音訊、視訊和 BFCP 視訊桌面共用的 Cisco Unified Communications Manager 媒體連線埠範圍。
	33434 到 33598	RTP/SRTP	UDP	用於音訊和視訊的 Cisco Hybrid Services(Jabber 對 Jabber 通話)媒體連線埠範圍。
	49152 到 65535	RDP	TCP	僅 即時訊息 的桌面共用。僅適用於 Windows 版 Cisco Jabber。
	8000	RTP/SRTP	TCP	使用 Jabber 桌面電話視訊介面，可讓使用者在電腦上透過用戶端來接收傳輸到其桌面電話裝置的視訊。
Unity Connection				

	連線埠	應用程式層通訊協定	傳輸層通訊協定	說明
	7080	HTTP	TCP	用於 Cisco Unity Connection 接收語音留言通知(新留言、留言更新及已刪除的留言)。
	7443	HTTPS	TCP	用於 Cisco Unity Connection 安全地接收語音留言通知(新留言、留言更新及已刪除的留言)。
	443	HTTPS	TCP	連線至 Cisco Unity Connection 以收聽語言信箱。
Cisco Webex Meetings				
	80	HTTP	TCP	連線至 Cisco Webex Meetings Center 以開始會議。
	443	HTTPS	TCP	連線至 Cisco Webex Meetings Center 以開始會議。
	8443	HTTPS	TCP	Cisco Unified Communications Manager 網頁存取，且包括適用於下列項目的連線： • 指定裝置的 Cisco Unified Communications Manager IP 電話 (CCMCIP) 伺服器。 • 用於聯絡人解析的使用者資料服務 (UDS)。
配件管理員				
	8001		TCP	在 Windows 版和 Mac 版 Cisco Jabber 中，Sennheiser 外掛程式會將這個通訊埠用於 Localhost 流量，以進行通話控制。

其他服務和通訊協定適用的連線埠

除了本節所列的連線埠以外，亦請檢閱您部署中的所有通訊協定與服務所需的連線埠。您可以在以下檔案中找到不同伺服器的連線埠與通訊協定需求：

- 對於 Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service，請參閱 *TCP* 與 *UDP* 連線埠使用指南。
- 對於 Cisco Unity Connection，請參閱系統管理指南。
- Cisco Webex Meetings Server 方面請參閱管理指南。
- Cisco Meetings Server 方面請參閱 *Cisco Meeting Server* 版本 *2.6* 和 *2.7*：單一合併式會議伺服器部署。
- Cisco Webex 服務方面請參閱管理指南。
- 對於 Expressway for Mobile and Remote Access，請參閱用於防火牆穿越的 *Cisco Expressway IP* 連線埠使用。
- 如需了解檔案傳輸連線埠的使用，請參閱 *Cisco Unified Communications Manager IM and Presence Service* 的組態和管理。

支援的編解碼器

類型	代碼	轉碼類型	Android 版 Cisco Jabber	iPhone 和 iPad 版 Cisco Jabber	Mac 版 Cisco Jabber	Windows 版 Cisco Jabber
音訊	G.711	A-law	爲 支援普通模式。		是	是
		μ定律/ Mu 定律	爲 支援普通模式。		是	是
	G.722		是		是	是
	G.722.1	24 kb / s 和 32 kb / s	爲 支援普通模式。		是	是
	G.729		不支援 G.729 的可觀看語音留言；但您可使用 G.729 和**撥打語音信箱**功能存取語音留言。		否	否
	G.729a		爲 低頻寬可用性的最低需求。 僅支援低頻寬模式的編解碼器。 支援普通模式。		是	是
	OPUS		是		是	是
視訊	H.264/AVC	基準配置檔	是		是	是
		高配置檔	否		是	是
語音信箱	G.711	A-law	是		是	是
		μ-定律 / Mu-定律(預設)	是		是	是
	GSM 06.10		是		是	是
	PCM linear		是		是	是

如果使用Android 版 Cisco Jabber 或iPhone 和 iPad 版 Cisco Jabber遇到語音品質問題，使用者可以在用戶端設定中開啓或關閉低頻寬模式。

虛擬環境需求

軟體需求

若要部署Windows 版 Cisco Jabber於虛擬環境中，請從以下支援的軟體版本中進行選擇：

軟體	支援的版本
Citrix XenDesktop	7.9, 7.8, 7.6, 7.5, 7.1
Citrix XenApp	7.9 已發佈的應用程式和桌面 7.8 已發佈的應用程式和桌面 7.6 已發佈的應用程式和桌面 7.5 發佈的桌面 6.5 發佈的桌面
VMWare Horizon View	7.0, 6.1, 6.0, 5.3

Softphone 需求

Softphone 通話請使用Jabber Softphone for VDI。

音訊和視訊性能參考

注意 以下資料基於在實驗室環境中的測試。此資料旨在提供有關頻寬使用方面的預期想法。本主題中的內容並不旨在殆盡或反映所有可能會影響頻寬使用情況的 媒體方案。

媒體保證

確保即時媒體在所有網路類型上的品質，好讓您的會議不會因爲媒體品質不良而中斷。媒體保證可以減輕多達 25%的資料包丟失。

Cisco Unified Communications Manager 版本 10.x 或更高版本上的視訊以及 Cisco Unified Communications Manager 版本 11.5 或更高版本上的音訊和視訊均支援媒體保證。

Expressway for Mobile and Remote Access 部署方面，Cisco 媒體保證需要 Cisco Expressway 8.8.1 版或更新版本。

對於輕微到嚴重的網路狀況，Jabber 可以：

- 暫時限制串流的頻寬。
- 重新同步視訊。

- 對封包進行均速傳輸以避免因壅塞造成的不必要的突發封包丟失。
- 透過來自第一個媒體封包的預先 SDP 信令來提供彈性機制。
- 保護封包丟失。
- 避免由於媒體生產過多而造成因擁塞而造成的丟失。
- 改善對低影格率/低位元率串流的保護。
- 支援已驗證和加密的 FEC。

Fastlane 支援

快速通道支援可確保即使在流量較高的情況下，業務相關應用程式在網路上仍爲優先。Jabber 支援語音和視訊流量的快速通道。iOS 10方面，當使用存取點(AP)快速通道功能時，將不再使用在 Cisco Unified Communications Manager 上所配置的 DSCP 值。而不支援快速通道功能的iOS 11 方面Jabber將繼續使用在 Cisco Unified Communications Manager 上配置的 DSCP 值。

不管 Cisco Unified Communications Manager 上的 DSCP 配置如何，如果您的無線 AP 支援快速通道功能，Jabber 都會自動設定以下 DSCP 和使用者優先級(UP)值：

- 對於音訊通話或視訊通話中的音訊部分，DSCP 設定爲 0x2e，UP 設定爲 6。
- 對於視訊通話中的視訊部分，DSCP 設定爲 0x22，UP 設定爲 5。
- 如果您的 AP 不支援或不使用快速通道，則 DSCP 值將自動設定爲 Cisco Unified Communications Manager 指定的值。

先決條件：

- 執行 AireOS 8.3 及更高版本的 WLC
- AP1600 / 2600 系列存取點,AP1700 / 2700 系列存取點,AP3500 系列存取點,AP3600 系列存取點+ 11ac 模塊,WSM,超定位模塊,3602P,AP3700 系列存取點+ WSM,3702P,OEAP600 系列 OfficeExtend 存取點,AP700 系列存取點,AP700W 系列存取點,AP1530 系列存取點,AP1550 系列存取點,AP1570 系列存取點和 AP1040 / 1140/1260 系列存取點
- 執行iOS 11 或更高版本的 iOS 裝置。

Cisco Jabber桌面用戶端的音訊位元率

以下音訊位元率(含 g.711 音訊)適用於 Windows 版 Cisco Jabber 和 Mac 版 Cisco Jabber。

代碼	RTP(千位元/秒)	實際位元率(千位元/秒)	備註
G.722.1	24/32	54/62	高品質壓縮
G.711	64	80	標準未壓縮
G.729a	8	38	低品質壓縮

Cisco Jabber行動用戶端的音訊位元率

下列音訊位元率適用於 iPad 及 iPhone 版 Cisco Jabber 及 Android 版 Cisco Jabber。

代碼	編解碼器位元率(千位元/秒)	使用的網路頻寬(千位元/秒)
g.711	64	80
g.722.1	32	48
g.722.1	24	40
g.729a	8	24

Cisco Jabber桌面用戶端的視訊位元率

以下視訊位元率(含 g.711 音訊)適用於 Windows 版 Cisco Jabber 和 Mac 版 Cisco Jabber。該表未列出所有可能的解析度。

結案回應	畫素	使用 **g.711** 音訊測得的位元率(每秒千比特)
w144p	256 x 144	156
w288p 這爲 Cisco Jabber 呈現視訊的視窗的預設大小。	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

附註 測得的位元率爲實際使用的頻寬(RTP 有效負載+ IP 資料包開銷)。

Android 版 Cisco Jabber 的視訊位元率

視訊	結案回應	頻寬
HD	1280 x 720	1024
VGA	640 x 360	512
CIF	488x211	310

附註 在通話期間傳送和接收高畫質視訊：

- 在 Cisco Unified Communications Manager 中爲高於 1024 kbps 的視訊通話配置最大位元率。
- 在路由器上啓用 DSCP，以高優先等級傳輸視訊 RTP 包。

iPhone 和 iPad 版 Cisco Jabber 的視訊位元率

用戶端以 20 fps 擷取和傳輸。

結案回應	畫素	g.711 音訊的位元率(千位元/秒)
w144p	256 x 144	290%
w288p	512 x 288	340
w360p	640 x 360	415
w720p	1280 x 720	1024

簡報視訊位元率

Cisco Jabber 以 8 fps 捕獲並以 2 – 8 fps 傳輸。

該表中的值不包括音訊。

畫素	估計的線位元率為 2 fps(千位元/秒)	估計的線位元率為 8 fps(千位元/秒)
720 x 480	41	164
704x576	47	188%
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400
1920 x 1080	150-300	500-1000

在 12.5 版中，當您的總視訊頻寬低於 300 kb 時，我們更改了位元率的分配以提高主視訊品質。但該更改還將主視訊的最大位元率設定爲 450 kb / s。

在總視訊頻寬較高的情況下，與早期版本相比，主視訊中的解析度可能會較低。

最大協商之位元率

您可以在 Cisco Unified Communications Manager 中指定最大有效負載位元率**區域組態**視窗。該最大有效負載位元率不包括資料包開銷，因此實際使用的位元率高於您指定的最大有效負載位元率。

下表描述了 Cisco Jabber 如何分配最大有效負載位元率：

桌面共用作業期間	音訊	互動視訊(主視訊)	簡報視訊(桌面共用視訊)
否	Cisco Jabber 使用最大音訊位元率。	Cisco Jabber 使用以下方式分配剩餘的位元率： 最大視訊通話位元率減去音訊位元率。	—
爲	Cisco Jabber 使用最大音訊位元率。	Cisco Jabber 在減去音訊位元率後分配剩餘頻寬的一半。	Cisco Jabber 在減去音訊位元率後分配剩餘頻寬的一半。

音訊	互動視訊(主視訊)
Cisco Jabber 使用最大音訊位元率	Cisco Jabber 使用以下方式分配剩餘的位元率： 最大視訊通話位元率減去音訊位元率。

頻寬

Cisco Unified Communications Manager 上的區域配置可能會限制用戶端可用的頻寬。

您可使用地區來限制某個地區內及現有的地區之間用於音訊和視訊通話的頻寬，其方式爲指定音訊和視訊通話中，與傳輸無關的最大位元速率。如需更多地區配置的資訊，請參閱特定 Cisco Unified Communications Manager 版本的說明文件。

Cisco Jabber 桌面用戶端的頻寬性能期望

Mac 版 Cisco Jabber 分離音訊的位元率，然後在互動視訊和簡報視訊之間平均分配剩餘頻寬。下表提供了有助於您了解每個頻寬應達到的性能的資訊：

上傳速度	音訊	音訊+互動視訊(主視訊)
使用VPN時爲 125 kbps	已達 g.711 的頻寬閾值。 g.729a 和 g.722.1 有足夠的頻寬。	視訊頻寬不足。
使用VPN時爲 384 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w288p(512 x 288)
使用企業網路時爲 384 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w288p(512 x 288)
1000 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w576p(1024 x 576)

上傳速度	音訊	音訊+互動視訊(主視訊)
2000 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w720p30(1280 x 720)

Windows 版 Cisco Jabber 分離音訊的位元率，然後在互動視訊和簡報視訊之間平均分配剩餘頻寬。下表提供了有助於您了解每個頻寬應達到的性能的資訊：

上傳速度	音訊	音訊+互動視訊(主視訊)	音訊+簡報視訊(桌面共用視訊)	音訊+互動視訊+簡報視訊
使用VPN時爲 125 kbps	已達 g.711 的頻寬閾值。 g.729a 和 g.722.1 有足夠的頻寬。 。	視訊頻寬不足。	視訊頻寬不足。	視訊頻寬不足。
使用VPN時爲 384 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w288p(512 x 288)	在 2+ fps 下爲 1280 x 800	在 30 fps 下 w144p(256 x 144)+ 在 2+ fps 下 1280 x 720
使用企業網路時爲 384 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w288p(512 x 288)	在 2+ fps 下爲 1280 x 800	在 30 fps 下 w144p(256 x 144)+ 在 2+ fps 下 1280 x 800
1000 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w576p(1024 x 576)	在 8 fps 下爲 1280 x 800	在 30 fps 下 w288p(512 x 288)+ 在 8 fps 下 1280 x 800
2000 kbps	任何音訊編解碼器皆有足夠頻寬。	在 30 fps 下 w720p30(1280 x 720)	在 8 fps 下爲 1280 x 800	在 30 fps 時 w288p(1024 x 576)+ 在 8 fps 時 1280 x 800

請注意，VPN 會增加有效負載的大小，從而增加頻寬消耗。

Android 版 Cisco Jabber 頻寬的性能期望值

請注意，VPN 會增加有效負載的大小，從而增加頻寬消耗。

上傳速度	音訊	音訊+互動視訊(主視訊)
使用VPN時爲 125 kbps	已達 g.711 的頻寬閾值。視訊頻寬不足。 g.729a 和 g.722.1 有足夠的頻寬。	視訊頻寬不足。

上傳速度	音訊	音訊+互動視訊(主視訊)
256 kbps	任何音訊編解碼器皆有足夠頻寬。	傳輸速率(Tx)—在 15 fps 下爲 256 x 144 接收率(Rx)—30 fps 時爲 256 x 144
使用VPN時爲 384 kbps	任何音訊編解碼器皆有足夠頻寬。	Tx—15 fps 時爲 640 x 360 Rx—30 fps 時爲 640 x 360
使用企業網路時爲 384 kbps	任何音訊編解碼器皆有足夠頻寬。	Tx—15 fps 時爲 640 x 360 Rx—30 fps 時爲 640 x 360

附註 由於裝置限制，Samsung Galaxy SII 和 Samsung Galaxy SIII 裝置無法達到此表中列出的最大解析度。

iPhone 和 iPad 版Cisco Jabber 頻寬的性能期望值

用戶端分離音訊的位元率，然後將剩餘頻寬平均分派給交互式視訊和簡報的視訊。下表提供了有助於您了解每個頻寬應達到的性能的資訊。

請注意，VPN 會增加有效負載的大小，從而增加頻寬消耗。

上傳速度	音訊	音訊+互動視訊(主視訊)
使用VPN時爲 125 kbps	已達 g.711 的頻寬閾值。視訊頻寬不足。 g.729a 和 g.722.1 有足夠的頻寬。	視訊頻寬不足。
290 kbps	任何音訊編解碼器皆有足夠頻寬。	在 20 fps 下爲 256 x144
415 kbps	任何音訊編解碼器皆有足夠頻寬。	在 20 fps 下爲 640 x 360
1024 kbps	任何音訊編解碼器皆有足夠頻寬。	在 20 fps 下爲 1280 x 720

視訊速率調整

Cisco Jabber 使用視訊速率調整來協商最佳視訊品質。視訊速率調整可動態增加或減少視訊位元率吞吐量，以處理可用 IP 路徑頻寬上的即時變化。

Cisco Jabber 使用者應該期望視訊通話在短時間內以較低的解析度開始，然後逐漸擴大到較高的解析度。Cisco Jabber 儲存歷史記錄，以便隨後的視訊通話應以最佳解析度開始。

H.264 配置檔對頻寬的影響

在早期版本中，我們僅支援 H.264 基準配置檔。在版本 12.8 中，我們爲桌面用戶端增添了對 H.264 高配置檔的支援。您不能對 VDI 或行動用戶端使用高配置檔。

高配置檔可以提供相同的視訊品質，使用的頻寬最多減少 10%。或者您可以在相同頻寬下獲得更好的視訊品質。

Jabber 預設爲 H.264 基準配置檔案。要啓用高調，我們 H264HighProfileEnable 參數。

通話管理記錄

通話結束時，Cisco Jabber 會傳送效能和品質資訊至Cisco Unified Communications Manager。Cisco Unified Communications Manager 會使用這些指標來填入 Cisco Unified Communications Manager 通話管理記錄 (CMR)。Cisco Jabber 會傳送音訊與視訊通話的下列資訊：

- 傳送及接收的封包數。
- 傳送及接收的位元組數。
- 遺失的封包數。
- 平均抖動。

用戶端亦會傳送下列視訊特有資訊：

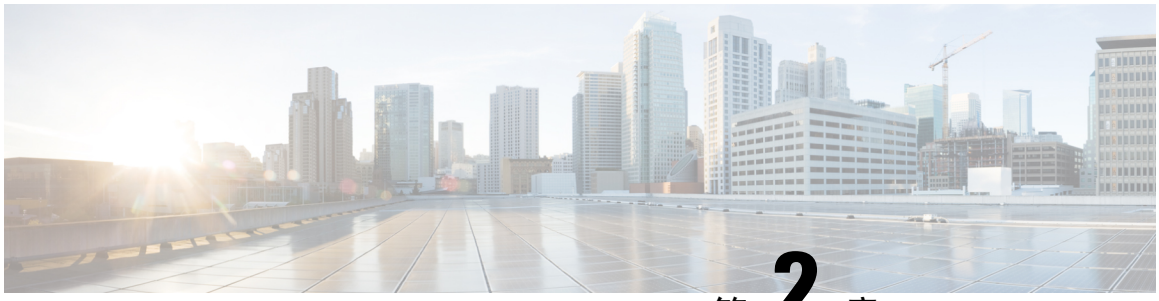
- 編解碼器已傳送和接收。
- 解析度已傳送和接收。
- 影格率已傳送和接收。
- 平均來回時間 (RTT)

用戶端亦會傳送下列音訊特有資訊：

- 隱藏之秒數。
- 嚴重隱藏之秒數

指標會以純文字格式出現在 Cisco Unified Communications Manager CMR 記錄輸出中，而且遙測或分析應用程式可直接讀取或取用此資料。

如需有關設定 Cisco Unified Communications Manager CMR 記錄的詳細資訊，請參閱您的 Cisco Unified Communications Manager 版本適用的詳細通話記錄管理指南中的通話管理記錄一章。



第 2 章

部署案例

公司處所內部署

公司處所內部署爲您設定和管理公司網路上所有服務的部署。

您可以在以下模式下部署Cisco Jabber：

- **完全 UC** —要部署完全 UC 模式請啓用 IM and Presence 功能，提供語音信箱和會議功能，以及爲使用者提供音訊和視訊裝置。
- **僅即時訊息**—要部署僅即時訊息模式，請啓用 IM and Presence 功能。勿爲使用者提供裝置。
- **僅電話模式**—在“僅電話”模式下，使用者的主要身份驗證爲Cisco Unified Communications Manager。要部署僅電話模式，請爲使用者提供具有音訊和視訊功能的裝置。您還可以爲使用者提供其他服務，如語音信箱等。

預設產品模式爲使用者對 IM and Presence 伺服器進行主要身份驗證的模式。

Cisco Unified Communications Manager IM and Presence Service 的公司處所內部署

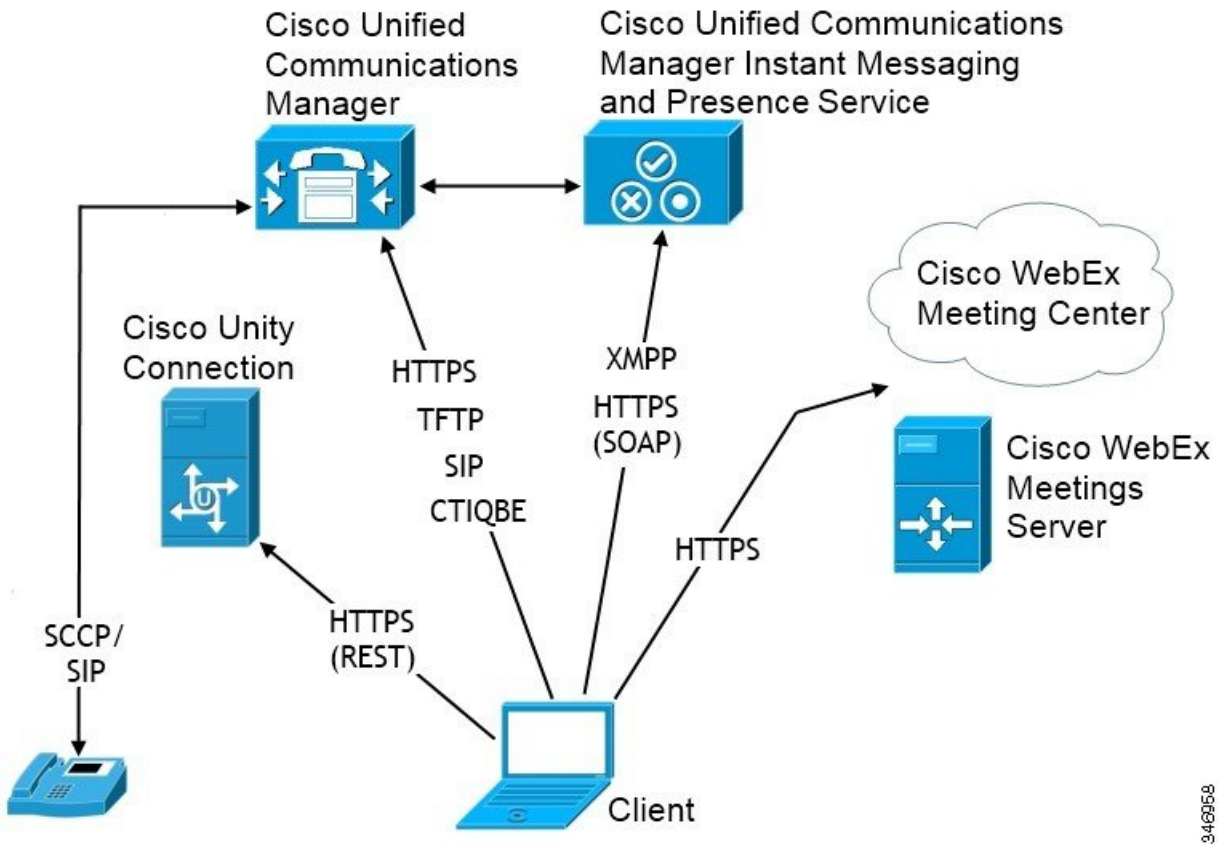
在公司處所內部署中可以使用以下服務：Cisco Unified Communications Manager IM and Presence Service：

- **存在**—透過Cisco Unified Communications Manager IM and Presence Service發佈在線狀態並訂閱其他使用者的在線狀態。

- **即時訊息**—透過Cisco Unified Communications Manager IM and Presence Service傳送和接收即時訊息。
- **檔案傳輸** -透過Cisco Unified Communications Manager IM and Presence Service傳送和接收檔案和螢幕截圖。
- **語音通話** -透過Cisco Unified Communications Manager使用桌面電話裝置或電腦撥出音訊通話。
- **視訊** -透過Cisco Unified Communications Manager進行視訊通話。
- **語音信箱**—透過Cisco Unity Connection傳送和接收語音留言。
- **會議**—與以下之一整合：
  - Cisco Webex Meetings Center-提供主辦會議功能。
  - Cisco Webex Meetings 伺服器-提供公司處所內會議功能。

下圖顯示了Cisco Unified Communications Manager IM and Presence Service與 Jabber 公司處所內部署的體系結構。

圖 *1:* 的公司處所內部署 *Cisco Unified Communications Manager IM and Presence Service*



電腦電話整合。

Windows 版 Cisco Jabber和Mac版Mac 版 Cisco Jabber 支援來自第三方應用程式Cisco Jabber的CTI。

電腦電話整合(CTI)使您可以在撥打，接聽和管理電話時使用電腦處理功能。CTI 應用程式可以使您根據通話者 ID 提供的資訊從資料庫中擷取用戶端資訊，並使您可以使用交互式語音響應(IVR)系統捕獲的資訊。

有關 CTI 的更多資訊，請參閱*Cisco Unified Communications Manager*系統指南適用您版本的 CTI 段落。或者，您可以在 Cisco Developer Network 上看到以下站點，以獲取有關透過Cisco Unified Communications ManagerAPI 建立 CTI 控制應用程式的資訊：

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

電話模式中的公司處所內部署

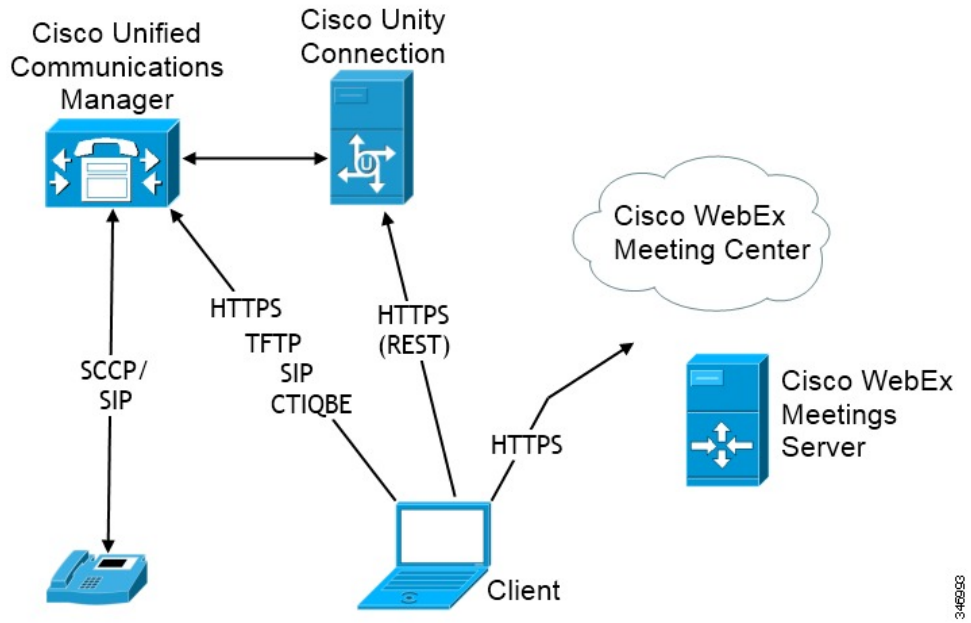
電話模式部署中可以使用以下服務：

- **聯絡人**—僅適用於行動用戶端。Cisco Jabber 從電話的通訊錄更新聯絡人資訊。
- **語音通話** -透過桌面電話裝置或透過在電腦上發出音訊通話Cisco Unified Communications Manager。
- **視訊** -透過Cisco Unity Connection進行視訊通話。
- **語音信箱**—透過Cisco Unity Connection傳送和接收語音留言。
- **會議**—與以下之一整合：
  - **Cisco Webex MeetingsCenter**—提供主辦會議功能。
  - **Cisco Webex Meetings伺服器** -提供公司處所內會議功能。

附註 Android 版 Cisco Jabber和iPhone 和 iPad 版 Cisco Jabber不支援電話模式中的會議。

下圖顯示了電話模式下的公司處所內部署的體系結構。

圖 *2:* 電話模式中的公司處所內部署



Softphone

Softphone 模式從 TFTP 伺服器下載組態檔並以其爲 SIP 註冊的端點執行。用戶端使用 CCMCIP 或 UDS 服務獲取裝置名稱以向 Cisco Unified Communications Manager 註冊。

桌面電話

桌面電話模式建立與 Cisco Unified Communications Manager 的 CTI 連線以控制 IP 電話。用戶端使用 CCMCIP 收集有關與使用者關聯的裝置的資訊，並建立可供用戶端控制的 IP 電話清單。

桌面電話模式下的 Cisco Mac 版 Cisco Jabber 不支援桌面電話視訊。

Extend and Connect

Cisco Unified Communications Manager 的 Extend and Connect 功能讓使用者可以控制諸如公共交換電話網(PSTN)電話和私用分支交換(PBX)裝置之類的裝置上的通話。如需更多地區配置的資訊，請參閱特定 Cisco Unified Communications Manager 版本的說明文件。

我們建議您將 Extend and Connect 功能與 Cisco Unified Communications Manager 9.1 (1)及更高版本一起使用。

帶有聯絡人部署的電話模式

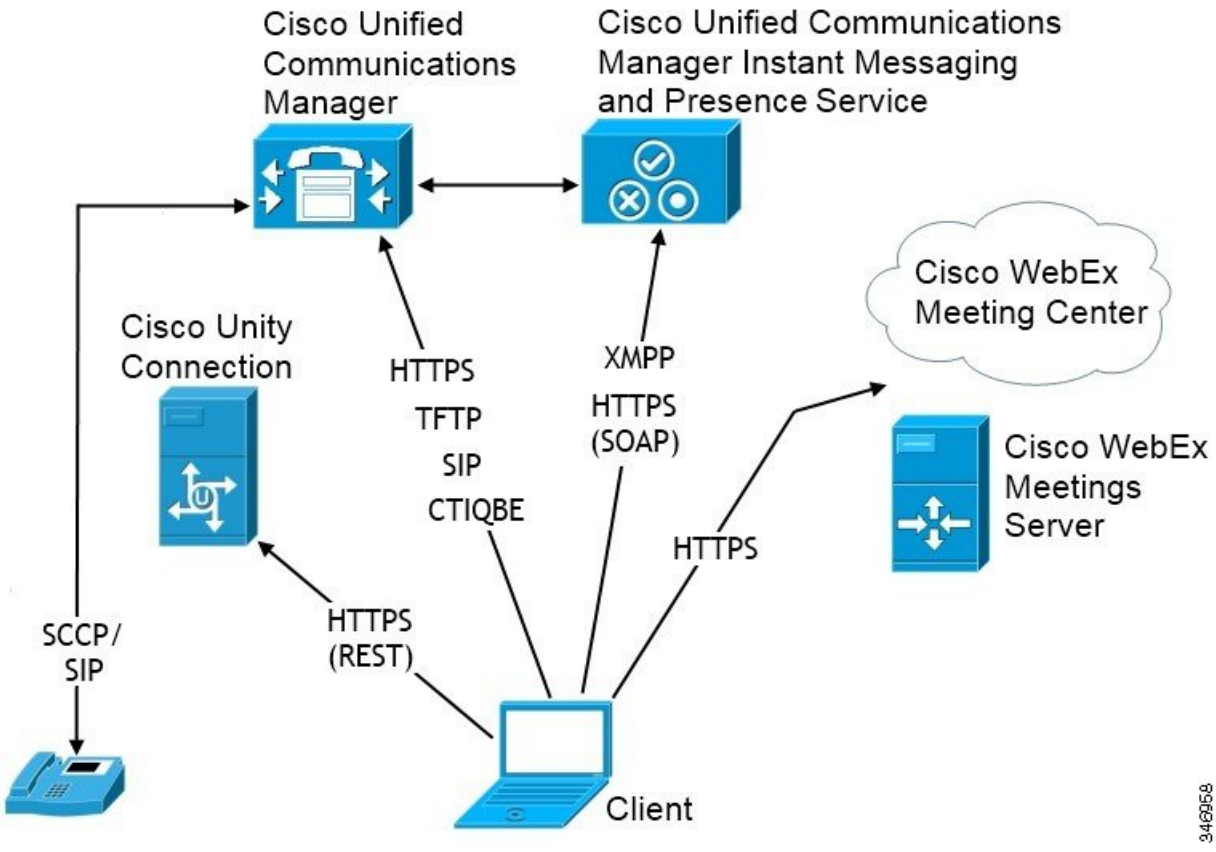
在部署聯絡人的電話模式下，可以使用以下服務：

- **聯絡人**—透過Cisco Unified Communications Manager IM and Presence Service的聯絡人資訊。
- **存在**—透過Cisco Unified Communications Manager IM and Presence Service發佈在線狀態並訂閱其他使用者的在線狀態。

- **語音通話** -透過Cisco Unified Communications Manager使用桌面電話裝置或電腦撥出音訊通話。
- **視訊** -透過Cisco Unified Communications Manager進行視訊通話。
- **語音信箱**—透過Cisco Unity Connection傳送和接收語音留言。
- **會議**—與以下之一整合：
  - Cisco Webex Meetings Center-提供主辦會議功能。
  - Cisco Webex Meetings 伺服器-提供公司處所內會議功能。

下圖顯示了Cisco Unified Communications Manager IM and Presence Service與 Jabber 公司處所內部署的體系結構。

圖 *3:* 帶有聯絡人部署的電話模式



雲端型部署

雲端型的部署使用Cisco Webex託管服務。

使用 Cisco Webex 執行雲端型部署模型時，您可以使用 Cisco Webex管理工具來管理和監控雲端型部署。您無需爲使用者設定服務配置檔。

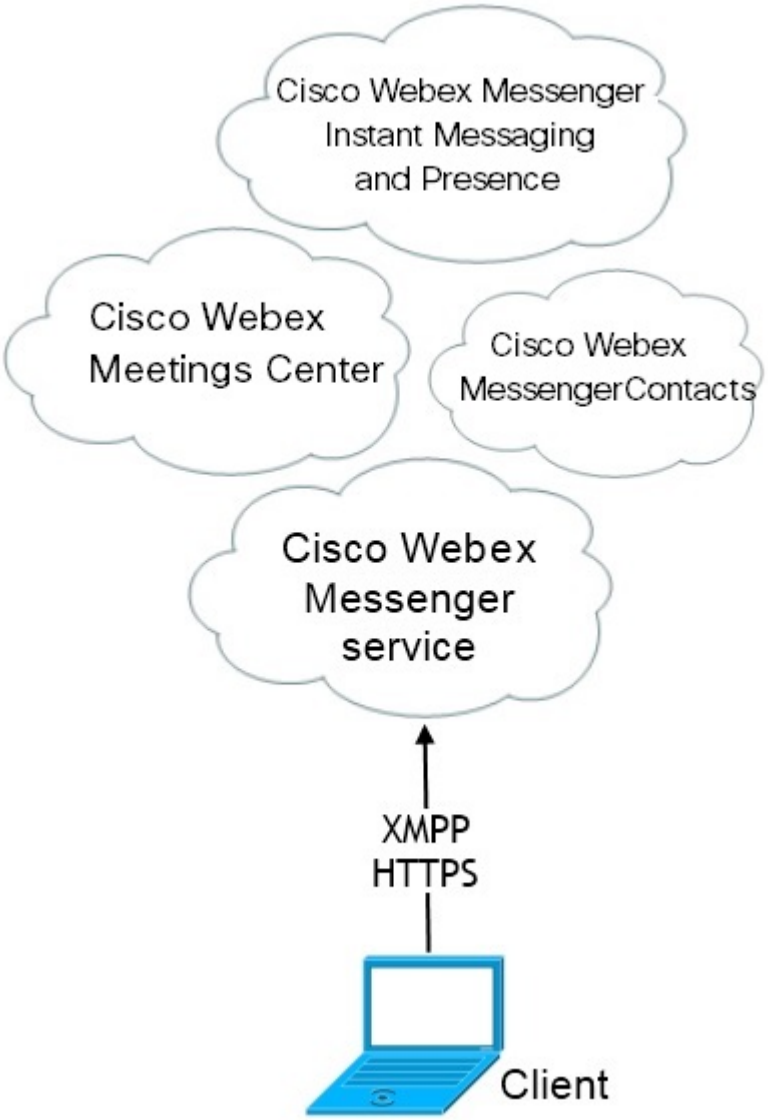
Cisco Webex Platform 服務的雲端和混合部署，您可以使用 Cisco Control Hub 管理和監控您的部署。

使用 Cisco Webex Messenger 進行雲端型部署

使用 Webex Messenger 的雲端型的部署中可以使用以下服務：

- **聯絡人來源**—Cisco Webex Messenger提供聯絡人解析。
- **在線狀態**- Cisco Webex Messenger允許使用者發佈其在線狀態並查看其他使用者的在線狀態。
- **即時訊息**—Cisco Webex Messenger允許使用者傳送和接收即時訊息。
- **會議**—Cisco Webex Meetings Center 提供主辦會議功能。

下圖顯示了雲端型部署的體系結構。

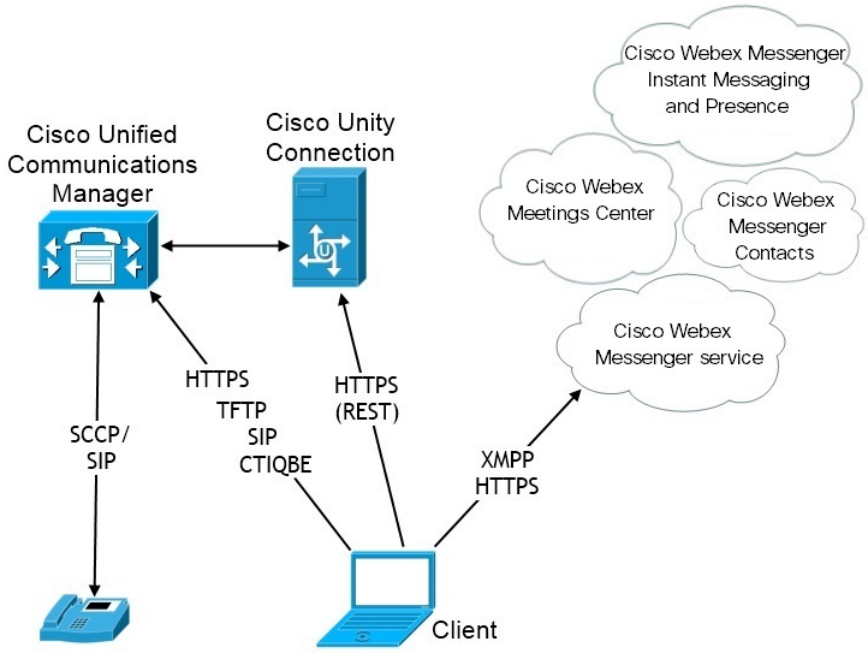


以 Cisco Webex Messaging Service 進行混合雲端型部署

在使用 Webex Messenger Service 的雲端型混合部署中可以使用以下服務：

- **聯絡人來源**—Cisco Webex Messenger服務提供聯絡人解析。
- **在線狀態**- Cisco Webex Messenger服務允許使用者發佈其在線狀態並查看其他使用者的在線狀態。
- **即時訊息**—Cisco Webex Messenger服務允許使用者傳送和接收即時訊息。
- **語音** -透過Cisco Unified Communications Manager使用桌面電話裝置或電腦撥出音訊通話。
- **視訊** -透過Cisco Unified Communications Manager進行視訊通話。
- **會議**—Cisco Webex Meetings Center 提供主辦會議功能。
- **語音信箱**—透過Cisco Unity Connection傳送和接收語音留言。

下圖顯示了混合雲端型部署的體系結構。



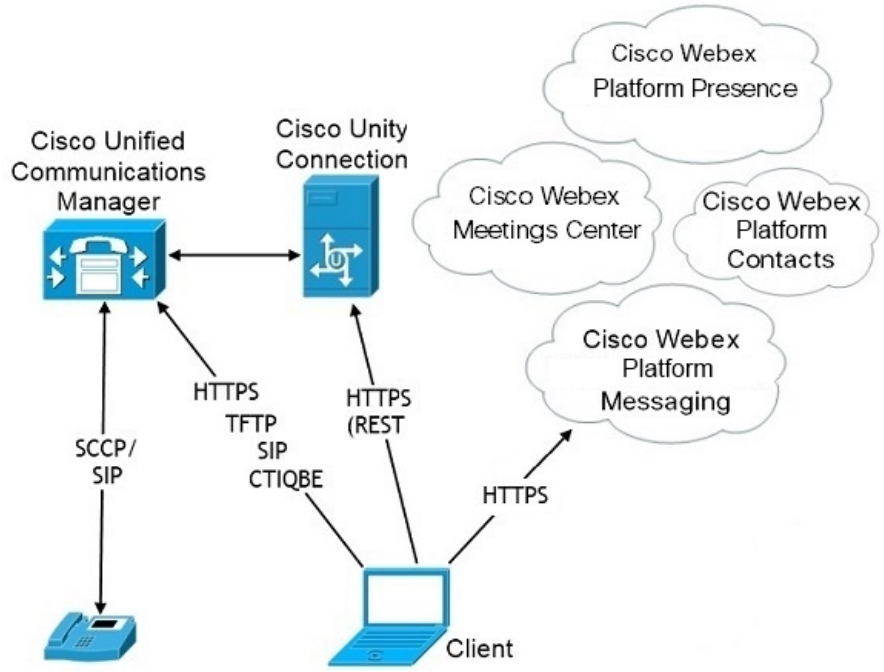
混合雲端型的部署 Cisco Webex Platform 服務

Jabber 的混合雲端型部署中可使用以下 Jabber 團隊訊息傳遞模式服務：Cisco Webex Platform 服務：

- 聯絡人來源—Cisco Webex Platform 服務提供聯絡人。
- 在線狀態- Cisco Webex Platform 服務允許使用者發佈其在線狀態並查看其他使用者的在線狀態。
- 訊息傳遞-Cisco Webex Platform 服務允許使用者傳送和接收訊息。

- 音訊-使用 Cisco UC Manager 透過桌面電話裝置或電腦進行音訊通話。
- 視訊-使用 Cisco UC Manager 進行視訊通話。
- 會議-Webex Meetings Center 提供了託管會議功能。
- 語音郵件-透過 Cisco Unity Connection 傳送和接收語音訊息。

下圖顯示了Cisco Webex Platform 服務與 Jabber 混合雲端型部署的體系結構。



Jabber 團隊訊息傳遞模式中的聯絡人

登入流程

在 Webex Control Hub 中啓用團隊訊息傳遞模式時，必須遷移使用者的聯絡人。

此登入流程概述了遷移使用者聯絡人的過程。該流程從使用者登入到其當前 Jabber 部署開始。您啓用 Jabber 團隊訊息傳遞模式，然後遷移其聯絡人。

1. 使用者已登入到其當前的 Jabber 部署，該部署連線至 Cisco UC Manager IM&P 或 Cisco Webex Messenger。
2. 管理員在 Webex Control Hub 中更改組態以啓用 Jabber 團隊訊息傳遞模式及可選的聯絡人遷移和 Jabber 通話。
3. 第二天，使用者登入到其當前的 Jabber 部署。在五分鐘內，Jabber 執行Service Discovery過程，檢測到該使用者有存在Cisco Webex Platform 服務的部署。
4. Jabber 提示使用者登出 Jabber，並顯示“檢測到配置更改”訊息。
5. 使用者再次重新登入，這次向Cisco Webex Platform 服務進行身份驗證。

6. 如果啓用了聯絡人遷移，則會出現一條訊息，提示使用者獲取其 Jabber 聯絡人。如果他們點選“確定”，則 Jabber 將獲取聯絡人名單緩存並將其上傳到Cisco Webex Platform 服務。如果使用者選擇**取消**，則 Jabber 不會遷移其聯絡人名單，他們以後可以分別搜尋和新增他們的聯絡人。

   聯絡人遷移期間，Jabber 僅遷移已啓用Cisco Webex Platform 服務的聯絡人。Jabber 不會在Cisco Webex Platform 服務中儲存自訂聯絡人並且無法將其新增到使用者的聯絡人名單中。

7. Jabber 連線至Cisco Webex Platform 服務後會連線至 Cisco UC Manager 以下載服務配置檔。如果在Cisco Webex Platform 服務 和 UC Manager 都啓用了 SSO 然後具有不同 IdP，或僅在一個啓用 SSO，則會提示使用者輸入憑證。但若兩個 SSO 都使用相同的 IdP，則無需登入。

Jabber 團隊訊息傳遞模式和聯絡人遷移的部署注意事項

貴Cisco Webex Platform 服務 組織必須具有與服務網域相同的網域。若爲不同的網域，則使用者無法進行聯絡人遷移。

在虛擬環境中部署

您可以在虛擬環境中部署Windows 版 Cisco Jabber。

虛擬環境中支援以下功能：

- 與其他Cisco Jabber 用戶端分享即時訊息與狀態
- 桌面電話控制
- 語音信箱
- 與 Microsoft Outlook 2007、2010 和 2013 進行狀態整合
- 行動及遠端存取 (MRA)

虛擬環境和漫遊配置檔案

在虛擬環境中，使用者並非總爲存取同一虛擬桌面。爲了保證一致的使用者體驗，每次啓動用戶端時都必須可以存取這些檔案。Cisco Jabber將使用者資料儲存在以下位置：

- `C:\Users\`*`username`*`\AppData\Local\Cisco\Unified Communications\Jabber\CSF`
  - **聯絡人**—聯絡人緩存檔案
  - **歷史**—通話和聊天記錄
  - **照片緩存** -在本地緩存目錄照片
- `C:\Users\`*`username`*`\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`
  - **設定檔** -維護使用者組態檔案並儲存組態儲存緩存
  - **認證**—儲存加密的使用者名稱密碼檔案

由於檔案加密和解密已連結到 Windows 使用者設定檔，因此請確保可存取以下資料夾：

- 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

附註 在非持續虛擬部署基礎架構(VDI)模式下使用 Cisco Jabber 時，不支援 Cisco Jabber 憑證緩存。

如果需要，可以透過將檔案和資料夾新增到排除清單中以排除在同步之外。要同步排除檔案夾中的子檔案夾，請將子檔案夾新增到包含清單中。

要保留個人使用者設定，請執行以下操作：

- 請勿排除以下目錄：
  - AppData \ Local \ Cisco
  - AppData\Local\JabberWerxCPP
  - AppData\Roaming\Cisco
  - AppData\Roaming\JabberWerxCPP
- 使用以下專用的配置檔管理解決方案：
  - **Citrix 配置檔案管理**—爲 Citrix 環境提供配置檔解決方案。在具有隨機託管的虛擬桌面分配的部署中，Citrix 配置檔案管理在其安裝的系統和使用者儲存之間同步每個使用者的整個配置檔案。
  - **VMware View Persona 管理**—保留使用者配置檔並將其與遠端配置檔儲存庫動態同步。VMware View Persona Management 不需要配置 Windows 漫遊配置檔，並且可以在 VMware Horizon View 使用者配置檔的管理中繞過 Windows Active Directory。Persona Management 增強了現有漫遊配置檔案的功能。

部署適用於 VDI 的 Jabber Softphone

要在具有通話功能的虛擬環境中部署 Jabber，您需要爲虛擬桌面基礎結構部署 Jabber Softphone。

部署 Jabber Softphone for VDI 的工作流程取決於您爲在公司處所內還爲混合環境中進行部署，並遵循 Jabber 部署工作流程直到應用程式安裝，此時，您將遵循 Jabber Softphone 進行 VDI 部署和安裝工作流程。

要獲取 Jabber Softphone for VDI 的公司處丶所內部署工作流程，請參閱 Cisco Jabber 公司處所內部署中部署和安裝工作流程區段中的完整的 *UC* 部署工作流程。

要獲取Jabber Softphone for VDI 的混合部署工作流程，請參閱Cisco Jabber 的雲端和混合部署中雲端和混合部署的工作流程區段中的使用 *Webex Messenger* 的混合部署工作流程。

企業行動化管理部署

Jabber 支援以兩個 SDK 爲基礎的用戶端之企業行動化管理 (EMM) 部署：

- Cisco Jabber for Intune
- Cisco Jabber for BlackBerry

您的組織可以部署這些用戶端，以在允許「自帶裝置」的部署中實施在行動裝置上使用 Jabber 的政策。例如，這些政策可以：

- 防止使用不安全的越獄或已 Root 裝置。
- 強制執行最低操作系統和應用程式版本。
- 防止使用者在 Jabber 中複製數據並將其粘貼到另一個應用程式中。

使用新的 EMM 類型參數來控制使用者可以登入的 Jabber 用戶端。

記住 這些用戶端會遵循延遲的發佈週期。用戶端的發佈要晚於相應的 Android 版 Jabber 和 iPhone 和 iPad 版 Jabber。

EMM 和 Jabber for Intune

在部署中使用 Jabber for Intune 用戶端時，管理員將在 Microsoft Azure 中配置管理政策。使用者從 App Store 或 Google Play 商店下載新的用戶端。當使用者執行新用戶端時，它將與管理員建立的政策同步。

注意 Jabber for Intune 在 iOS 平台上不支援 Apple 推送通知 (APN)。將 Jabber 放在背景執行時，iOS 裝置可能會收不到聊天訊息和通話。

附註 對於 Android 裝置，使用者首先要安裝 Intune 公司入口網站。然後，他們要透過入口網站執行用戶端。

設定 Jabber for Intune 的一般過程如下：

1. 建立一個新的 Azure AD 租使用者。
2. 建立新的 AD 使用者或同步本機 AD 使用者。
3. 建立一個 Office 365 群組或一個安全群組並新增您的使用者。
4. 將 Jabber for Intune 用戶端新增到 Microsoft Intune。

5. 在 Microsoft Intune 中建立和部署政策。
6. 使用者登入到用戶端並同步以接收您的政策。

有關這些步驟的詳細資訊，請參閱 Microsoft 的文件。

下表列出了我們在 Cisco Jabber 應用程式保護原則中所支援的 Microsoft Intune 限制：

限制	Android	iPhone 和 iPad
將資料傳送到其他應用程式	是	是
儲存組織資料的副本	是	是
剪下，複製和粘貼到其他應用程式	是	是
螢幕擷圖	是	不適用
最大PIN 輸入次數	是	是
離線寬限期	是	是
最低應用程式版本	是	是
在越獄或root的裝置上使用	是	是
最低裝置作業系統版本	是	是
最低補丁版本	是	不適用
工作(或學校)帳戶憑證以進行存取	是	是
重新檢查存取需求	是	是

EMM 和 Jabber for BlackBerry

在部署中使用 Jabber for BlackBerry Client 時，管理員將在 BlackBerry Unified Endpoint Management (UEM) 中配置管理政策。使用者從 App Store 或 Google Play 商店下載新的用戶端。Jabber for BlackBerry 正等待 BlackBerry 認證，尚未在 BlackBerry Marketplace 中提供。

重要須知 由於用戶端正在等待BlackBerry認證，因此我們必須向您的組織申請存取權限。如要取得存取權限，請與我們聯絡 (jabber-mobile-mam@cisco.com)，並提供 BlackBerry UEM 伺服器所提供的客戶組織 ID。

新用戶端已整合 BlackBerry Dynamics SDK，可以直接從 BlackBerry UEM 取得政策。用戶端會繞過 BlackBerry Dynamics 進行連接和儲存。BlackBerry Dynamics SDK 不支援 FIPS 設定。

您的聊天、語音和視訊流量會繞過 BlackBerry 基礎結構。當用戶端不屬於內部部署，便會要求透過 Cisco Expressway 進行所有流量的行動電話和遠程存取。

注意 Jabber for BlackBerry 在 iOS 平台上不支援 Apple 推送通知 (APN)。將 Jabber 放在背景執行時，iOS 裝置可能會收不到聊天訊息和通話。

附註 Android 必須執行 Android 6.0 或更高版本才能使用 Jabber for BlackBerry。

iOS 必須執行 iOS 11.0 或更高版本才能使用 Jabber for BlackBerry。

對於 BlackBerry Dynamics，您的管理員可以設定政策來控制 BlackBerry 用戶端對 Jabber 的使用方法。

設定 Jabber for BlackBerry 的一般過程如下：

1. 在 UEM 中建立伺服器。
2. 將 Jabber for BlackBerry 用戶端新增到 BlackBerry Dynamics 中。
3. 在 BlackBerry Dynamics 中建立或匯入使用者。

附註 對於 Android 使用者，您可以選擇在 BlackBerry Dynamics 中產生存取密鑰。

4. 在 UEM 中建立和部署政策。請注意這些設定在 Jabber for BlackBerry 應用程式配置上的行爲：
   - 如果啓用可選的 DLP 政策，則 BlackBerry 會要求：
     - 使用 BlackBerry Works 發送電子郵件。
     - 使用 BlackBerry Access 在 iOS 裝置中進行 SSO 驗證。在 iOS 的 Expressway 和 Unified Communications Manager 啓用**使用本機瀏覽器**。然後，將 **ciscojabber** 方案新增至 BlackBerry UEM 中的 BlackBerry 存取政策。
   - 該清單顯示了 Jabber MAM 參數，這些參數對於在 Jabber for BlackBerry 部署中的應用程式配置進行設定非常有用。參閱部署指南的適用於 *Android*、*iPhone* 和 *iPad* 的 *Cisco Jabber* 之 *URL* 配置部分，了解有關這些參數的更多詳細資訊：

MAM 參數	**iOS 可支援**	**Android 可支援**
伺服領域	是	是
VOICE_SERVICES_DOMAIN	是	—
ServiceDiscoveryExcludedServices	是	—
ServicesDomainSsoEmailPrompt	是	—
InvalidCertificateBehavior	是	—
Telephony_Enabled	是	—

MAM 參數	iOS 可支援	Android 可支援
AllowUrlProvisioning	是	—
IP_MODE	是	—

5. 使用者登入用戶端。

有關這些步驟的詳細資訊，請參閱 BlackBerry 的文件。

下表列出了我們在 Cisco Jabber 應用程式保護原則中所支援的 BlackBerry 限制：

群組	功能	Android	iPhone 和 iPad
IT 政策	在沒有網路連線的情況下清除裝置	是	是
啓用	允許的版本	是	是
BlackBerry Dynamics	密碼	是	是
	數據洩漏防護-不允許將數據從 BlackBerry Dynamics 應用程式複製到非 BlackBerry Dynamics 應用程式	是	是
	數據洩漏防護-不允許將數據從非 BlackBerry Dynamics 應用程式複製到 BlackBerry Dynamics 應用程式	是	是
	數據洩漏防護-不允許在 Android 和 Windows 10 裝置上擷取螢幕截圖	是	不適用
	數據洩漏防護-不允許在 iOS 裝置上進行螢幕錄影和共用	不適用	是
	數據洩漏防護-不允許在 iOS 裝置上使用自訂鍵盤	不適用	是
企業管理代理設定檔	允許收集個人應用程式的資訊	是	是
合規設定檔	已 Root 作業系統或認證失敗	是	是
	安裝了受限制的作業系統版本	是	是
	未安裝所需級別的安全修補程序	是	不適用

Jabber for BlackBerry 的 IdP 連線

在適用於 Android，iPhone 和 iPad 的 Jabber 部署中，用戶端會連接到 DMZ 中的身分識別提供者 (IdP) 代理。然後，代理會將請求傳遞到內部防火牆後的 IdP 伺服器。

在 Jabber for BlackBerry 中，您有一條備用路徑。如果您在 BlackBerry UEM 中啓用了 DLP 政策，則 iOS 裝置上的用戶端可以安全地直接經過通道傳輸到 IdP 伺服器。要使用此設定，請按以下方式配置部署：

- 在 iOS 的 Expressway 和 Unified CM 啓用**使用本機瀏覽器**。
- 將 **ciscojabber** 方案新增至 BlackBerry UEM 中的 BlackBerry 存取政策。

Android 作業系統的 Jabber for BlackBerry 一律會連接到 SSO 的 IdP 代理。

如果您的部署僅包含執行 iOS 的裝置，則 DMZ 中不需要 IdP 代理。但是，如果您的部署包含任執行 Android OS 的裝置，則需要 IdP 代理。

遠端存取

貴組織使用者可能需要自公司網路外部的位置存取其工作。您可以使用一種Cisco的遠端存取產品以提供使用者的存取權限。

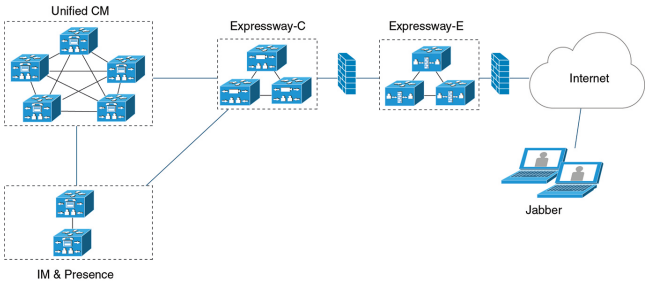
Jabber 未經任何第三方 VPN 用戶端的測試或驗證。

Expressway for Mobile and Remote Access

與Cisco Unified Communications Manager使用的 Expressway for Mobile and Remote Access 允許使用者從公司防火牆外部存取其協作工具，而無需使用VPN。使用 Cisco Collaboration 閘道，用戶端可以從遠端位置(如公共 Wi-Fi 網路或行動資料網路)安全地連線至公司網路。

圖 *4:* 用戶端如何連線至 *Expressway for Mobile and Remote Access*

下圖說明了Expressway for Mobile and Remote Access 環境的體系結構。



首次使用 Expressway for Mobile and Remote Access 登入至 Jabber

適用於行動用戶端的 Cisco Jabber。

使用者可以使用 Expressway for Mobile and Remote Access 首次登入到用戶端，以從公司防火牆外部連線至服務。但爲，在以下情況下，最初爲在公司網路上登入的：

- 如果語音服務網域與其他服務網域不同，則使用者必須位於公司網路內才能從 `jabber-config.xml` 檔案中獲取正確的語音服務網域。對於混合部署，管理員可以配置 VoiceServicesDomain參數，請參閱最新版本 *Cisco Jabber* 的參數參考指南。在這種情況下，使用者不需登入公司網路。
- 如果 Cisco Jabber 必須完成 CAPF 註冊過程，則使用安全或混合模式叢集時需要此過程。

如果使用者透過 Expressway for Mobile and Remote Access 環境使用安全電話，則我們不支援在公共網路上的首次登入。如果組態爲具有加密的 TFTP 的安全配置檔而配置，則首次的登入必須爲公司處所內以允許 CAPF 註冊。沒有 Cisco Unified Communications Manager，Expressway for Mobile and Remote Access 以及 Cisco Jabber 增強功能，即無法支援在公共網路上的首次登入。但我們有支援：

- 加密的 TFTP，於公司處所內首次登入。
- 未加密的 TFTP，可以 Expressway for Mobile and Remote Access 或於公司處所內首次登入。

支援的服務

下表總結了用戶端以 Expressway for Mobile and Remote Access 遠端連線至 Cisco Unified Communications Manager 時所支援的服務和功能。

***表 2: Expressway for Mobile and Remote Access* 支援的服務摘要**

服務	支援	不支援
目錄		
UDS 目錄搜尋	X	
LDAP 目錄搜尋		X
目錄照片解析度	X *在 Cisco Expressway-C 上使用 HTTP 白名單	
網域內聯合	X *聯絡人搜尋支援取決於聯絡人 ID 的格式。如需更多資訊，請參閱下方附註。	
網域間聯合	X	
即時訊息與狀態		
內部部署	X	
雲端	X	
訊息	X	
多人聊天	X	
持續聊天	X	
高可用性：公司處所內部署	X	

服務	支援	不支援
檔案傳輸：公司處所內部署	X 使用 Cisco Unified Communications Manager IM and Presence Service 10.5 (2)或更高版本的檔案傳輸可用的進階選項，請參閱以下附註。	
檔案傳輸：雲端部署	X	
視訊螢幕共用 - BFCP	X(行動用戶端的 Cisco Jabber 僅支援 BFCP 接收。)	
僅即時訊息螢幕共用		x
音訊或視訊		
音訊及視訊通話：	X Cisco Unified Communications Manager 9.1 (2) 及更高版本	
桌面電話控制模式(CTI)(僅限桌面用戶端)		X
Extend and connect(僅限桌面用戶端)		X
遠端桌面控制(僅桌面用戶端)		X
安靜狀態監控和通話錄音		X
透過 Office 撥號-反向(僅限行動用戶端)	X	X
作業階段永久性		X
早期媒體		X
存取 Self Care Portal		X
優美的註冊	X * 適用於 Android 版 Cisco Jabber。 Android 版 Jabber 支援從 Cisco Unified Communications Manager 版本 10.5.(2) 10000-1 透過 Expressway for Mobile and Remote Access 優美的註冊。	

服務	支援	不支援
共用線路	X 先決條件： • 將 Cisco Expressway 升級至 X8.9.1 或更新版本 • 將 Cisco Unified Communications Manager 升級至 11.5 SU (2) 或更新版本	
語音信箱		
Visual Voicemail	X *在 Cisco Expressway-C 上使用 HTTP 白名單	
Cisco Webex Meetings		
內部部署	X	X
雲端	X	
Cisco Webex 螢幕共用(僅桌面用戶端)	X	
安裝(桌面用戶端)		
安裝程式更新	X *在 Cisco Expressway-C 上使用 HTTP 白名單	X Mac 版 Cisco Jabber 不支援
自訂		
建立自訂 HTML 標籤		X
增強的 911 提示	X * 爲確保在公司網路之外執行的所有 Jabber 用戶端都能正確呈現該網頁，該網頁必須爲靜態 HTML 頁面，因爲指令碼和連結標記不爲 E911 通知 URL 參數所支援。如需詳細資訊，請參閱 *Cisco Jabber* 適用的參數參考指南。	
安全性		
媒體 ICE 協議	X	
端對端加密	X	X

服務	支援	不支援
CAPF 註冊		X
單一登入 (SSO)	X	
Advanced Encryption Standard (AES) 256 和 TLS1.2。	X * 適用於 Android 版 Cisco Jabber。 僅公司 Wi-Fi 支援高級加密	
故障排除(僅限桌面用戶端)		
產生問題報告	X	
上傳問題報告		X
高可用性(容錯移轉)		
音訊和視訊服務		X
語音信箱服務		X
IM and Presence Service	X	
聯絡人搜尋	X	
聯絡人解析	X	
組態管理		
快速登入	X	
驗證及授權		
SSO Jabber 使用者的 O-Auth 支援	X	

目錄

當用戶端使用 Expressway for Mobile and Remote Access 連線至服務時，它支援具有以下限制的目錄整合。

- LDAP 聯絡人解析-在公司防火牆之外，用戶端無法使用 LDAP 進行聯絡人解析，需改用 UDS 進行聯絡人解析。

  當使用者位於公司防火牆內時，用戶端可以使用 UDS 或 LDAP 進行聯絡人解析。如果您在公司防火牆內部署 LDAP，Cisco建議您將 LDAP 目錄伺服器與 Cisco Unified Communications Manager 同步，以允許用戶端於使用者在公司防火牆之外時與 UDS 連線。

- 目錄照片解析度—爲確保用戶端可以下載聯絡人照片，您必須將託管聯絡人照片的伺服器新增到 Cisco Expressway-C 伺服器的白名單中。要將伺服器新增到 Cisco Expressway-C 白名單，請使用 **HTTP 伺服器允許**設定。有關更多資訊，請參閱相關的 Cisco Expressway 說明文件。

- 網域內聯合—部署網域內聯合且用戶端自防火牆外部與 Expressway for Mobile and Remote Access 連線時，僅當聯絡人 ID 使用以下格式之一時才支援聯絡人搜尋：
  - sAMAccountName @ domain
  - UserPrincipleName(UPN)@domain
  - EmailAddress @ domain
  - employeeNumber @ domain
  - 電話號碼@網域
- 使用 XMPP 的網域間聯合-Expressway for Mobile and Remote Access不會啓用 XMPP 網域間聯合本身。如果已在 Cisco Unified Communications Manager IM and Presence 中啓用了 XMPP 網域間聯合，則透過 Expressway for Mobile and Remote Access連線的 Cisco Jabber 用戶端可以使用 XMPP 網域間聯合。

即時訊息與狀態

當用戶端使用 Expressway for Mobile and Remote Access 連線至服務時會支援即時訊息傳遞和狀態，但存在以下限制：

檔案傳輸對於桌面和行動用戶端具有以下限制：

- 對於Cisco Webex雲端部署支援檔案傳輸。
- 對於使用 Cisco Unified Communications IM and Presence Service 10.5 (2)或更高版本的公司處所內部署支援**託管檔案傳輸**的選擇，但不支援**點對點**選項。
- 對於使用 Cisco Unified Communications Manager IM and Presence Service 10.0 (1)或更早版本的公司處所內部署不支援檔案傳輸。
- 對於具有不受限的 Cisco Unified Communications Manager IM and Presence 伺服器的 Expressway for Mobile and Remote Access部署不支援託管檔案傳輸。

音訊及視訊通話：

當用戶端使用 Expressway for Mobile and Remote Access 連線至服務時會支援音訊和視訊通話，但存在以下限制：

- Cisco Unified Communications Manager—Expressway for Mobile and Remote Access 透過 Cisco Unified Communications Manager 9.1.2 及更高版本支援視訊和語音通話。
- 桌面電話控制模式(CTI)(僅桌面用戶端)—用戶端不支援桌面電話控制模式(CTI)，包括分機行動性。
- Extend and connect(僅桌面用戶端)— 用戶端不能用於：
  - 在辦公室的非 Cisco IP 電話撥打及接聽電話。
  - 執行通話中控制，例如在家庭電話，酒店電話或辦公室中的 Cisco IP 電話上保留和恢復通話。

- 會話持久性—發生網路過渡時，用戶端無法從音訊和視訊通話掉線中恢復。例如，如果使用者在辦公室內發起 Cisco Jabber 通話，然後走出建築物並失去 Wi-Fi 連線，則該通話會隨著用戶端切換爲使用 Expressway for Mobile and Remote Access而掉線。
- Early Media—Early Media 允許用戶端在建立連線之前在端點之間交換資料。例如，如果使用者撥打給不同組織的一方而該方拒絕或未接聽電話，則 Early Media 確保使用者聽到忙碌音或被轉接到語音信箱。

  使用 Expressway for Mobile and Remote Access時，如果對方拒絕或不接聽電話，則使用者不會聽到忙碌音，在通話終止之前則是會聽到大約一分鐘的靜音。
- Self care portal 存取(僅桌面用戶端)-防火牆外的使用者無法存取 Cisco Unified Communications Manager Self Care Portal。不能從外部存取 Cisco Unified Communications Manager 使用者頁面。

  Cisco Expressway-E 將用戶端和防火牆內部的 Unified Communications 服務之間的所有通訊以 proxy 傳送。但 Cisco Expressway-E 不會將不屬於 Cisco Jabber 應用程式的瀏覽器存取的服務以 proxy傳送。

語音信箱

當用戶端使用 Expressway for Mobile and Remote Access 連線至服務時將支援語音郵件服務。

附註 爲了確保用戶端可以存取語音郵件服務，您必須將語音郵件伺服器新增到 Cisco Expressway-C 伺服器的白名單中。要將伺服器新增到 Cisco Expressway-C 白名單，請使用 **HTTP 伺服器允許**設定。有關更多資訊，請參閱相關的 Cisco Expressway 說明文件。

安裝

Mac 版 Cisco Jabber—當用戶端使用 Expressway for Mobile and Remote Access 連線至服務時不支援安裝程式更新。

Windows 版 Cisco Jabber—當用戶端使用 Expressway for Mobile and Remote Access 連線至服務時支援安裝程式更新。

附註 爲確保用戶端可以下載安裝程式更新，您必須將託管安裝程式更新的伺服器新增到Cisco Expressway-C 伺服器的白名單。要將伺服器新增到 Cisco Expressway-C 白名單，請使用 **HTTP 伺服器允許**設定。有關更多資訊，請參閱相關的 Cisco Expressway 說明文件。

安全性

當用戶端使用 Expressway for Mobile and Remote Access連線至服務時支援具有以下限制的大多數安全性功能。

- 初始CAPF 註冊—認證頒發機構proxy功能(CAPF)註冊爲在 Cisco Unified Communications Manager 發佈伺服器上執行的安全性服務，該服務向 Cisco Jabber(或其他用戶端)頒發認證。要成功註冊 CAPF，用戶端必須從防火牆內部或使用 VPN 進行連線。

- 端到端加密-當使用者透過 Expressway for Mobile and Remote Access 連線並參與通話時：
  - 始終在 Cisco Expressway-C 與使用 Expressway for Mobile and Remote Access 向 Cisco Unified Communications Manager 註冊的裝置之間的通話路徑上對媒體進行加密。
  - 如果未使用加密安全模式配置 Cisco Jabber 或內部裝置，則在 Cisco Expressway-C 與公司處所內註冊到 Cisco Unified Communications Manager 的裝置之間的通話路徑上不會對媒體進行加密。
  - 如果同時將 Cisco Jabber 和內部裝置配置了 Encypted 安全模式，則 Expressway-C 與在公司處所內註冊到 Cisco Unified Communications Manager 的裝置之間的通話路徑上的媒體將被加密。
  - 如果 Cisco Jabber 用戶端始終透過 Expressway for Mobile and Remote Access連線，則不需要 CAPF 註冊即可實現端到端加密，但仍必須將 Cisco Jabber 裝置配置爲加密安全模式，且必須啓用 Cisco Unified Communications Manager 以支援混合模式。
  - 您可以在 Expressway-C 或 Expressway-E 伺服器上配置 ICE 直通支援，以確保在公司網路外部時，透過 Jabber 傳送的媒體被加密。有關如何設定的更多資訊，請參閱*Mobile and Remote Access through Expressway*的部署指南

疑難排解

僅 Windows 版 Cisco Jabber 問題報告上傳—桌面用戶端使用 Expressway for Mobile and Remote Access 連線至服務時無法傳送問題報告，因爲用戶端會透過 HTTPS 將問題報告上傳到指定的內部伺服器。

要避開此問題，使用者可以將報告儲存在公司處所內，並以其他方式傳送報告。

高可用性(容錯移轉)

高可用性意味著，如果用戶端無法連線至主伺服器，則它將故障轉移到輔助伺服器而服務中斷的極少或完全沒有中斷。與 Expressway for Mobile and Remote Access 支援的高可用性相關的，高可用性是指將特定服務的伺服器故障轉移到如 IM and Presence 的輔助伺服器。

Expressway for Mobile and Remote Access的某些服務不支援高可用性。這意味著，如果使用者從公司網路外部連線至用戶端，且即時訊息傳遞和在線狀態伺服器進行故障轉移，則這些服務將繼續正常執行。但若音訊和視訊伺服器或語音郵件伺服器進行故障轉移，則這些服務將不起作用，因爲相關伺服器不支援高可用性。

Cisco AnyConnect 的部署

Cisco AnyConnect 爲指伺服器-用戶端基礎結構，使用戶端能夠從遠端位置(例如 Wi-Fi 網路或行動資料網路)安全地連線至公司網路。

Cisco AnyConnect 環境包括以下組件：

- Cisco Adaptive Security Appliance -提供一項服務以保護遠端存取。
- Cisco AnyConnect 安全行動化用戶端-從使用者裝置建立到 Cisco Adaptive Security Appliance 的安全連線。

本部分提供與 Cisco AnyConnect 安全行動用戶端一起部署 Cisco Adaptive Security Appliance(ASA)時應考慮的資訊。Cisco AnyConnect 爲 Android 版 Cisco Jabber 和 iPhone 和 iPad 版 Cisco Jabber 特定的所支援的 VPN。如果您使用不支援的 VPN 用戶端，請確定您使用相關的第三方文件安裝與配置該 VPN 用戶端。

使用執行 Android 作業系統 4.4.x 的 Samsung 裝置，請使用 Samsung AnyConnect 4.0.01128 版或更新版本。對於 Android 作業系統 5.0 以上的版本，您必須使用高於 4.0.01287 版的 Cisco AnyConnect 軟體版本。

Cisco AnyConnect 爲遠端使用者提供到 Cisco 5500 系列 ASA 的安全 IPsec(IKEv2)或 SSL VPN 連線。可以從 ASA 或使用企業軟體部署系統將 Cisco AnyConnect 部署到遠端使用者。從 ASA 部署時，遠端使用者透過在配置爲接受無用戶端 SSL VPN 連線的 ASA 瀏覽器中輸入 IP 位址或 DNS 名稱，來建立與 ASA 的初始 SSL 連線。然後，ASA 在瀏覽器視窗中顯示一個登入螢幕，如果使用者滿足登入和身份驗證的需求，它將下載與電腦作業系統相符的用戶端。下載後，用戶端將自行安裝和配置並建立與 ASA 的 IPsec(IKEv2)或 SSL 連線。

有關 Cisco Adaptive Security Appliance和 Cisco AnyConnect 安全行動化用戶端需求的資訊，請參閱軟體需求主題。

相關主題

瀏覽 Cisco ASA 系列說明文件
Cisco AnyConnect Secure Mobility Client

單一登入部署

您可以使用安全聲明標記語言(SAML)單一登入(SSO)啓用服務。SAML SSO 可以在公司處所內、雲端或混合部署中使用。

以下步驟描述了貴組織使用者啓動Cisco Jabber用戶端後 SAML SSO 的登入流程：

1. 使用者啓動Cisco Jabber用戶端。如果將身份提供者(IdP)配置爲提示使用者使用 Web 表單登入，則該表單將顯示在用戶端中。
2. Cisco Jabber用戶端向其連線的服務傳送授權請求，例如Cisco Webex Messenger服務、Cisco Unified Communications Manager、Cisco Unity Connection。
3. 該服務重新導向用戶端以從 IdP 請求身份驗證。
4. IdP 請求憑證。可以透過以下方法之一提供憑證：
   - 基於表單的身份驗證，其中包含使用者名稱和密碼欄位。
   - 整合 Windows 身份驗證(IWA)的 Kerberos(僅 Windows)
   - 智能卡身份驗證(僅 Windows)
   - 基本的 HTTP 身份驗證方法，用戶端在發出 HTTP 請求時會提供使用者名稱和密碼。
5. IdP 向瀏覽器或其他身份驗證方法提供 cookie。IdP 使用 SAML 對身份進行身份驗證，這使服務可以向用戶端提供令牌。
6. 用戶端使用令牌進行身份驗證以登入到服務。

驗證方法

身份驗證機制會影響使用者的登入方式。例如，如果您使用 Kerberos，則用戶端不會提示使用者輸入憑證，因爲貴組織使用者已經提供了身份驗證以存取桌面。

使用者工作階段

使用者登入會議，這爲他們提供了預定的使用期限Cisco Jabber服務。要控制會話的持續時間，可以配置 Cookie 和令牌逾時參數。

以適當的時間配置 IdP 超時參數，確保將不會提示使用者登入。例如，當 Jabber 使用者切換至外部 Wi-Fi，正在漫遊，其筆記本電腦進入休眠狀態，或因閒置筆記本電腦進入休眠狀態時。如果 IdP 會話仍處於活躍狀態，則使用者恢復連線後不需登入。

當會話到期且 Jabber 無法悄悄更新時，由於需要使用者的輸入，將提示使用者重新進行身份驗證。當授權 cookie 不再有效時，可能會發生這種情況。

如果使用 Kerberos 或智能卡，除非智能卡需要 PIN，否則無需任何操作即可重新認證。不會中斷語音郵件，來電或即時訊息等服務。

單一登入需求

SAML 2.0

您必須使用 SAML 2.0 爲使用 Cisco Unified Communications Manager 服務的 Cisco Jabber 用戶端啓用單一登入(SSO)。SAML 2.0 與 SAML 1.1 不相容。您必須選擇使用 SAML 2.0 標準的 IdP。支援的身份提供程序已經過測試，符合 SAML 2.0 的需求，可用於納入 SSO。

支援的身份提供商

IdP 必須符合安全斷言標記語言(SAML)。用戶端支援以下身份提供者：

- Ping Federate 6.10.0.4
- Microsoft Active Directory 聯盟服務 (ADFS) 2.0
- 開放式存取管理器(OpenAM)10.1

附註 確保您將全球持續性 cookie 配置爲與 OpenAM 一起使用。

配置 IdP 時，配置的設定會影響您登入用戶端的方式。某些參數(例如 Cookie 的類型(持久性或會話)或身份驗證機制(Kerberos 或 Web 表單))確定必須多久進行一次身份驗證。

Cookie

要啓用與瀏覽器的 cookie 共用，必須使用持久性 cookie 而不爲作業期間 cookie。持續性 Cookie 會提示使用者一次在用戶端或使用 Internet Explorer 的任何其他桌面應用程式中輸入憑證。作業期間 Cookie 要求使用者每次啓動用戶端時都輸入其憑證。您將持續性 cookie 配置爲 IdP 上的設定。如果您將 Open Access Manager 用作 IdP，則必須配置全球持續性 Cookie(而不爲領域特定的持續性 Cookie)。

當使用者使用 SSO 憑證成功登入到 iPhone 和 iPad 版 Cisco Jabber 時，預設情況下 cookie 被儲存在 iOS 鑰匙串中。如果 cookie 在 iOS 鑰匙串中，則使用者無需輸入下次登入的登入憑證，除非 cookie 在登入期間過期。在以下情況下將從 iOS 鑰匙串中刪除 cookie：

- 手動登出 Cisco Jabber
- Cisco Jabber 已重設
- 重啓 iOS 裝置後
- Cisco Jabber 手動關閉

如果 iOS 系統在後台停止用於 iPhone 和 iPad 版 Cisco Jabber，則 Cisco Jabber 允許使用者自動登入而無需輸入密碼。

所需的瀏覽器

要在瀏覽器和用戶端之間共用身份驗證 cookie(由 IdP 發出)，必須將以下瀏覽器之一指定爲預設瀏覽器：

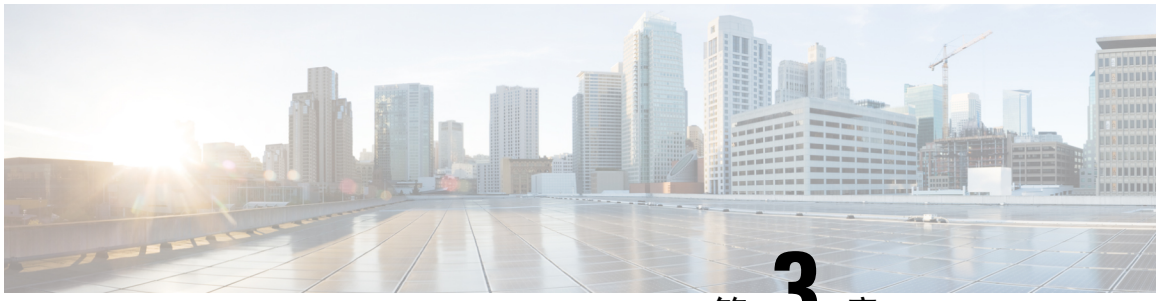
產品	所需的瀏覽器
Windows 版 Cisco Jabber	網際網路 Explorer
Mac 版 Cisco Jabber	Safari
iPhone 和 iPad 版 Cisco Jabber	Safari
Android 版 Cisco Jabber	Chrome 或 Internet Explorer

附註 當將 SSO 與 Android 版 Cisco Jabber 一起使用時，嵌入式瀏覽器無法與外部瀏覽器共用 cookie。

單丨登入和遠端存取

對於使用 Expressway Mobile and Remote Access 從公司防火牆外部提供其憑證的使用者，單點登入具有以下限制：

- 單點登入(SSO)在 Cisco Expressway 8.5 和 Cisco Unified Communications Manager 版本 10.5.2 或更高版本中可用。您必須同時在兩者上啓用或禁用 SSO。
- 您不能在安全電話上的 Expressway for Mobile and Remote Access使用 SSO。
- 使用的身份提供者必須具有相同的內部和外部 URL。如果 URL 不同，則在公司防火牆的內部和外部之間進行切換時，可能會提示使用者重新登入。



第 3 章

使用者管理

Jabber ID

Cisco Jabber 使用 Jabber ID 來識別聯絡人來源中的聯絡人資訊。

使用使用者 ID 和在線狀態網域建立預設的 Jabber ID。

例如，Adam McKenzie 的使用者 ID 爲`amckenzie`，網域名爲 `example.com` 而 Jabber ID 爲 `amckenzie@example.com`。

下列爲 Cisco Jabber 使用者 ID/電子郵件地址中支援的字元：

- 大寫字元(A 到 Z)
- 小寫字元(a 到 z)
- 數字 (0-9)
- 句點 (.)
- 連字型大小 (-)
- 底線 (_)
- 波浪符號 (~)
- 井號(#)

當填充聯絡人名單時，用戶端將使用 Jabber ID 搜尋聯絡人來源，以解析聯絡人並顯示名字，姓氏和任何其他聯絡人資訊。

即時訊息位址方案

當網域位於相同的在線狀態體系結構(例如，example-us.com 和 example-uk.com 中的使用者)時，Cisco Jabber 10.6 及更高版本支援用於公司處所內部署的多個在線狀態網域體系結構模型。Cisco Jabber 使用 Cisco Unified Communications Manager IM and Presence 10.x 或更高版本以支援彈性的即時訊息位址方案。即時訊息位址方案即爲標識 Cisco Jabber 使用者的 Jabber ID。

爲了支援多網域模型，部署的所有組件都需要以下版本：

- Cisco Unified Communications IM and Presence 伺服器節點和通話控制節點版本 10.x 或更高版本。
- 在 Windows，Mac，IOS 和 Android 10.6 或更高版本上執行的所有用戶端。

僅可在以下的多網域架構情況下部署 Cisco Jabber：

- Cisco Jabber 10.6 或更高版本在貴組織中以新安裝部署給所有系統(Windows，Mac，IOS 、和 Android [包括如 DX系列的 Android IP 電話])上的所有使用者。
- 於在線狀態伺服器上進行任何網域或即時訊息位址更改之前，所有系統(Windows，Mac，IOS 、和 Android [包括如 DX系列的 Android IP 電話])方面的使用者 Cisco Jabber 均已升級到版本 10.6 或更高版本。

“進階在線狀態設定”中可用 即時訊息位址方案爲：

- UserID @ [預設網域]
- 目錄 URI

UserID @ [預設網域]

使用者 ID 欄位對映到 LDAP 欄位。這爲預設的即時訊息位址方案。

例如，使用者 Anita Perez 擁有一個帳戶名 aperez，而“使用者 ID”欄位對映到 sAMAccountName LDAP 欄位。使用的位址方案爲 aperez@example.com。

目錄 URI

目錄 URI 對映到**郵件**或 **msRTCSIP-primaryuseraddress** LDAP 欄位。此選項提供獨立於用於身份驗證的使用者 ID 的方案。

例如，使用者 Anita Perez 的帳戶名爲 aperez，郵件欄位爲 Anita.Perez@domain.com，使用的位址方案爲 Anita.Perez@domain.com。

使用 Jabber ID 的Service Discovery

Service Discovery採用以下格式輸入的 Jabber ID `[userid] @ [domain.com]` 預設情況下，提取Jabber ID 的 `domain.com` 部分以發現可用的服務。對於存在網域與Service Discovery網域不同的部署，可以在安裝期間包括Service Discovery網域資訊，如下所示：

- 在 Windows 版 Cisco Jabber 中，透過使用 `SERVICES_DOMAIN` 命令行參數以包括網域的資訊。
- 在 Mac 版 Cisco Jabber，Android 版 Cisco Jabber 或 iPhone 和 iPad 版 Cisco Jabber 中，可以使用 URL 組態中所使用的`ServicesDomain` 參數設定Service Discovery的網域。

.

SIP URI

SIP URI 與每個使用者相關聯。SIP URI 可以爲電子郵件位址、即時訊息位址、UPN。

使用 Cisco Unified Communications Manager 中的“目錄 URI”欄位配置 SIP URI。這些爲可用的選項：

- mail
- msRTCSIP-pr即時訊息aryuseraddress

使用者可以透過輸入 SIP URI 搜尋聯絡人並撥打給聯絡人。

LDAP 使用者 ID

從目錄來源同步到 Cisco Unified Communications Manager 時，將從目錄中的屬性填充使用者 ID。含有使用者 ID 的預設屬性爲 `sAMAccountName`。

聯合身份驗證的使用者 ID 規劃

對於聯合身份驗證，Cisco Jabber 需要每個使用者的聯絡人 ID 或使用者 ID 以在聯絡人搜尋期間解析聯絡人。

在 SipUri 參數中設定使用者 ID 的屬性。預設值爲 `msRTCSIP-PrimaryUserAddress`. 如果您要從使用者 ID 中刪除前綴，則可以在 UriPrefix 參數中設定一個值，請參閱最新版本的 *Cisco Jabber* 的參數參考指南。

使用者聯絡人照片的 proxy 位址

Cisco Jabber 存取照片伺服器以擷取聯絡人照片。如果您的網路組態含 Web proxy，則需確保 Cisco Jabber 可以存取 Photo Server。

驗證及授權

Cisco Unified Communications Manager LDP 身份驗證

LDAP 身份驗證在 Cisco Unified Communications Manager 上配置爲透過目錄伺服器進行身份驗證。

當使用者登入用戶端時，在線狀態伺服器會將身份驗證路由到 Cisco Unified Communications Manager。Cisco Unified Communications Manager 即會將該身份驗證proxy到目錄伺服器。

Cisco Webex Messenger 登入驗證

Cisco Webex Messenger身份驗證使用Cisco Webex管理工具。

當使用者登入到用戶端時，資訊將傳送到Cisco Webex Messenger並將身份驗證令牌傳送回用戶端。

單一登入驗證

使用身份提供程序(IdP)和服務配置單點登入身份驗證。

當使用者登入到用戶端時，資訊將傳送到 IdP，一旦憑證被接受，身份驗證令牌即傳送回 Cisco Jabber。

iPhone 和 iPad 版 Cisco Jabber 的基於認證的身份驗證

Cisco Jabber 透過用戶端憑證在 IdP 伺服器上進行身份驗證。此憑證驗證讓使用者無需輸入使用者憑證即可登入伺服器。用戶端使用 Safari 的 framework 來實現此功能。

需求

- 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 8.9 和更新版本。
- 爲 Cisco Unified Communications 基礎架構啓用 SSO
- 所有伺服器認證皆爲 CA 簽署，包括 Cisco Unified Communications Manager，IM and Presence Service，Cisco Unity Connection 和 IdP 伺服器。如果 iOS 裝置確實使用了 OS 的可信授權，請在安裝 Cisco Jabber 應用程式之前安裝 CA 憑證。
- 在 Cisco Unified Communications Manager 中爲 SSO 配置本機瀏覽器(嵌入式 Safari)。有關更多資訊，請參閱“基於認證的 SSO 身份驗證”部分。*Cisco Jabber* 的公司處所內部署。
- 在 Expressway for Mobile and Remote Access 伺服器中爲 SSO 配置本機瀏覽器(嵌入式 Safari)。有關更多資訊，請參閱《Cisco Expressway 安裝指南》https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html。

您可以透過 EMM 解決方案在 iOS 裝置上部署 Cisco 認證。

建議使用—Cisco建議使用 EMM 解決方案在 iOS 裝置上部署認證。

Android 版 Cisco Jabber 的基於認證的身份驗證

Cisco Jabber 使用用戶端憑證登入單一登入伺服器(Webex Messenger和公司處所內)。

需求

- Android 作業系統 5.0 或更高版本
- 單一登入已啓用
- Mobile and Remote Access(MRA)和非 MRA 部署模式支援 Jabber 用戶端。
- Jabber 始終在 Android 7.0 及更高版本上顯示無效認證的通知，即使在 Android OS 上已安裝的自訂 CA 簽署認證亦爲如此。搭配 Android 7.0 的應用程式僅信任系統提供的認證，而不再信任使用者新增的認證頒發機構。

認證部署

Cisco建議使用 EMM 解決方案在 Android 裝置上部署認證。

語音信箱驗證

使用者需要在 Cisco Unity Connection 上存在。Cisco Unity Connection 支援多種身份驗證類型。如果 Cisco Unified Communications Manager 和 Cisco Unity Connection 使用相同的身份驗證，則我們建議使用將 Cisco Jabber 配置爲使用相同的憑證。

OAuth

您可以將 Cisco Jabber 設定爲使用 OAuth 協議授權使用者對服務的存取權限。如果使用者登入到啓用 OAuth 的環境，則無需在使用者每次登入時都輸入憑證。倘若伺服器未啓用 OAuth，則 Jabber 可能無法正常執行。

如果您使用的爲 Cisco Unified Communications Manager 12.5 或更高版本則仍可啓用 SIP OAuth，它允許 Jabber 向 SIP 驗證，從而允許 Jabber 透過 TLS 連線至 SIP 服務，亦允許 Jabber 透過安全連線(sRTP)傳送媒體。SIP OAuth 意味著不再需要 CAPF 註冊才能啓用安全的 SIP 和媒體。

先決條件：

- 如果要正常執行，必須在所有這些組件上開啓 OAuth 重新整理令牌
- Cisco Unified Communications Manager，Cisco Unified Communications Manager 即時訊息和狀態和 Cisco Unity Connection 必須爲 11.5(SU3)或 12.0 版本。
- Cisco Expressway for Mobile and Remote Access X8.10 或更高版本
- SIP OAuth：Mobile and Remote Access 的啓用代碼登入功能需要具備 Cisco Unified Communications Manager 12.5(1) SU1 或更高版本以及 Cisco Expressway X12.5 或更高版本才可使用。

在配置 OAuth 之前，請檢查您擁有的部署類型：

- 如果您具有公司處所內身份驗證部署，則不需要 IdP 伺服器，且 Cisco Unified Communications Manager 負責身份驗證。
- 您可以在配置或不配置 SSO 的情況下設定 OAuth。如果您使用的爲 SSO，請確保已爲所有服務啓用了 SSO。如果您具有啓用 SSO 的部署，請部署一台 IdP 伺服器然後由 IdP 伺服器負責身份驗證。

您可以爲使用者的以下服務啓用 OAuth：

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

預設情況下，在這些伺服器上停用 OAuth。要在這些伺服器上啓用 OAuth：

- Cisco Unified Communications Manager 和 Cisco Unity Connection 伺服器方面，請移至**企業參數配置** > **具有重新整理登入流程的 OAuth**。
- Cisco Expressway-C 方面請移至**組態 Unified Communication** > **配置由 OAuth 令牌授權並重新整理**。

在這些伺服器中的任何一個上啓用或禁用 OAuth 時，Jabber 都會在組態重新獲取間隔內對其進行標識，並讓使用者登出後再登入 Jabber。

登出之期間，Jabber會刪除儲存在緩存中的使用者憑證，然後讓使用者以常規的登入流程登入，Jabber於此流程中先獲取所有配置資訊後再讓使用者存取 Jabber 服務。

未在 Cisco Unified Communications Manager 中設定電話

1. 移至**Cisco Unified Communications Manager 管理** > **系統** > **企業參數** > **SSO 組態**
2. 設定 **O-Auth 存取令牌到期計時器(分鐘)**爲理想的值。
3. 設定 **O-Auth 存取令牌重新整理計時器(天)**爲理想的值。
4. 按一下「**儲存**」按鈕。

要在 Cisco Expressway 上配置 OAuth：

1. 移至**組態** > **Unified Communications** > **組態** > **MRA 存取控制**。
2. 設定 **O-Auth 公司處所內身份驗證**爲**開啟**。

在 Cisco Unity 上配置 OAuth：

1. 移至 **AuthZ 伺服器**然後選擇**新增**。
2. 在所有欄位中輸入詳細資訊，然後選擇**忽略認證錯誤**。
3. 按一下**儲存**。

限制

Jabber 觸發自動入侵防護

情況：

- 您的 Expressway for Mobile and Remote Access配置爲透過 OAuth 令牌(帶有或不帶有 Refresh 令牌)進行授權。
- Jabber 使用者的存取令牌已過期。

Jabber 執行以下操作之一：

- 從桌面休眠狀態恢復
- 恢復網路連線
- 登出幾個小時後嘗試快速登入

行爲：

- 一些 Jabber 模組嘗試使用過期的存取令牌在 Expressway-E 上進行授權。
- Expressway-E 正確地拒絕了這些請求。
- 如果來自特定 Jabber 用戶端的請求超過五個，則 Expressway-E 會封鎖該 IP 位址十分鐘(預設情況下)。

徵狀：

受影響的 Jabber 用戶端的 IP 位址將增添到 Expressway-E 的“封鎖的位址”清單中的 HTTP proxy授權失敗類別中，在**系統** > **保護** > **自動檢測** > **封鎖的位址**可以看到。。

因應措施：

您可以透過兩種方法來解決此問題；可以提高該特定類別的偵測閾值，亦可以爲受影響的用戶端建立豁免。我們在此描述閾值選項，因爲豁免在您的環境中可能不實用。

1. 移至**系統** > **保護** > **自動偵測** > **組態**。
2. 請點選 **HTTP proxy授權失敗**。
3. 將**引發程度**從 5 更改爲 10。10 必須足以承受呈現過期令牌的 Jabber 模組。
4. 儲存配置，此配置會立即生效。
5. 解除封鎖任何受影響的用戶端。

多個資來源登入

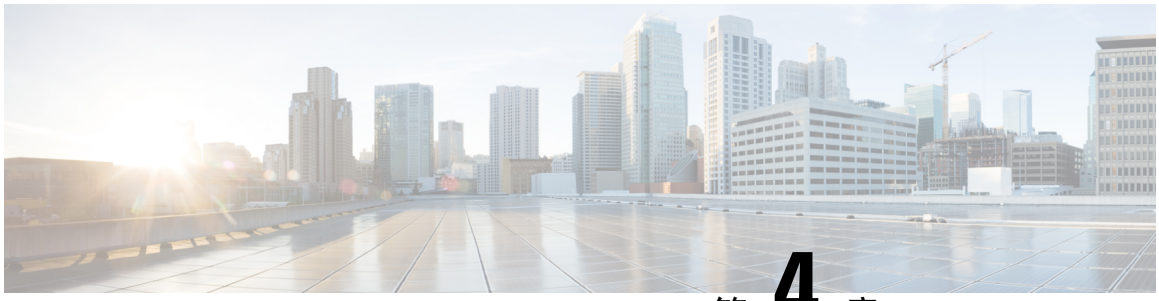
使用者登入系統時，所有Cisco Jabber用戶端都會向以下中央IM and Presence Service節點之一註冊。此節點會追蹤可用性，聯絡人名單及 IM and Presence Service環境的其他方面。

- 公司處所內部署： Cisco Unified Communications Manager IM and Presence Service.
- 雲端部署：Cisco Webex。

此 IM and Presence 服務節點按以下順序追蹤與每個唯一網路使用者關聯的所有註冊用戶端：

1. 當 2 個使用者起始一個新的即時訊息對話時，第一則傳入的訊息會廣播至接收使用者的所有已註冊的用戶端。
2. IM and Presence Service 節點會等候其中一個已註冊用戶端的第一個回應。
3. 第一個回應的用戶端即會收到其餘傳入的訊息，直到使用者開始由其他已註冊用戶端回應。
4. 然後節點重新路由後續訊息給這個新用戶端。

附註 如果使用者登入到多個裝置時沒有作用中的資源，則最高優先在線狀態等級的用戶端爲最優先。如果所有裝置上的在線狀態優先等級皆相同，則使用者最近所登入的用戶端爲最優先。



第 4 章

Service Discovery

用戶端如何連線到服務

要連線至服務，Cisco Jabber 需要以下資訊：

- 身份驗證來源，使得使用者可以登入到用戶端。
- 定位服務

您可以透過以下方法將該資訊提供給用戶端：

URL 組態

向使用者傳送其管理員的電子郵件。電子郵件中包含一個 URL，它將配置Service Discovery所需的網域。

Service Discovery

用戶端自動找到並連線至服務。

手動連線設定

使用者在用戶端使用者介面中手動輸入連線設定。

Cisco Webex Platform 服務 探索

Cisco Jabber 傳送 HTTPS 請求到Cisco Webex Platform 服務以檢查爲否爲使用者啓用了團隊訊息傳遞模式。如果爲使用者啓用了團隊訊息傳遞，則 Jabber 繼續檢查可用的公司處所內服務。

Cisco Webex Messenger Service Discovery

Cisco Jabber 將雲端 HTTP 請求傳送到 CAS URL 以Cisco Webex Messenger服務。Cisco Jabber 透過以下方式對使用者進行身份驗證Cisco Webex Messenger服務並連線至可用服務。

服務於Cisco Webex管理工具配置。

Cisco 叢集間查詢服務

在含有多個叢集的環境中，您將配置叢集間尋找服務 (ILS)。ILS 可讓用戶端找到使用者主叢集及進行 Service Discovery。

Expressway for Mobile and Remote Access Discovery

Expressway for Mobile and Remote Access 使遠端使用者可以存取服務。

用戶端向名稱伺服器查詢 SRV 記錄。用戶端以 `_collab-edge` SRV 記錄透過 Expressway for Mobile and Remote Access 連線至內部網路並進行 Service discovery。

名稱伺服器返回 `_collab-edge` SRV 記錄且用戶端獲取 Cisco Expressway-E 伺服器的位置。Cisco Expressway-E 伺服器即向用戶端提供內部名稱伺服器的查詢結果，須包括 `_cisco-uds` SRV 記錄，用戶端然後自 Cisco Unified Communications Manager 擷取服務配置檔。

建議使用的連線模式

爲用戶端提供連線至服務所需的資訊時，應使用的方法取決於部署類型，伺服器版本和產品模式。下表重點介紹了各種部署方法以及如何向用戶端提供必要的資訊。

表 *3:* 的公司處所內部署 *Windows* 版 *Cisco Jabber*

產品模式	伺服器版本	發現方法	非 **DNS SRV** 記錄方法
完全 UC(預設模式)	版本 9.1.2 及更高版本： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	針對 `_cisco-uds .<domain>`的 DNS SRV 請求	使用以下安裝程式開關和值： • `AUTHENTICATOR=CUP` • `CUP_ADDRESS =` <在線狀態伺服器位址>

產品模式	伺服器版本	發現方法	非 **DNS SRV** 記錄方法
僅即時訊息(預設模式)	版本 9 及更高版本： Cisco Unified Communications Manager IM and Presence Service	針對 _cisco-uds .<domain>的 DNS SRV 請求	使用以下安裝程式開關和值： • AUTHENTICATOR=CUP • CUP_ADDRESS = <在線狀態伺服器位址>
電話模式	版本 9 及更高版本： Cisco Unified Communications Manager	針對 _cisco-uds .<domain>的 DNS SRV 請求	使用以下安裝程式開關和值： • AUTHENTICATOR=CUCM • TFTP = <CUCM_位址> • CCMCIP = <CUCM_位址> • PRODUCT_MODE=phone_mode 使用這種部署方法不支援高可用性。

Cisco Unified Communications Manager 版本 9.x 及更早版本-如果啓用 Cisco Extension Mobility，則 Cisco Extension Mobility服務必須在用於 CCMCIP 的 Cisco Unified Communications Manager 節點上啓動。如需 Cisco Extension Mobility 的資訊，請參閱特定 Cisco Unified Communications Manager 版本的功能與服務指南。

附註 Cisco Jabber9.6 版和更高版本仍可以使用 _cuplogin DNS SRV 請求發現完整的 Unified Communications 和僅IM服務，但如果存在 _cisco-uds 請求則 _cisco-uds 將具有優先權。

如果希望使用者在首次全新安裝期間繞過電子郵件螢幕，請使用 SERVICES_DOMAIN 安裝程式開關指定 DNS 記錄所在的網域的值。

表 *4:* 的公司處所內部署 *Mac* 版 *Cisco Jabber*

產品模式	伺服器版本	發現方法
完全 UC(預設模式)	版本 9 及更高版本： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	針對 _cisco-uds .<domain>的 DNS SRV 請求

表 *5: Android* 版 *Cisco Jabber*和 *iPhone* 和 *iPad* 版 *Cisco Jabber*的公司處所內部署

產品模式	伺服器版本	發現方法
完全 UC(預設模式)	版本 9 及更高版本： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	針對 `_cisco-uds .<domain>`和 `_cuplogin .<domain>`的 DNS SRV 請求
僅即時訊息(預設模式)	版本 9 及更高版本： Cisco Unified Communications Manager IM and Presence Service	針對 `_cisco-uds .<domain>`和 `_cuplogin .<domain>`的 DNS SRV 請求
電話模式	版本 9 及更高版本： Cisco Unified Communications Manager	針對 `_cisco-uds .<domain>`的 DNS SRV 請求

附註 Cisco Unified Communications Manager版本 9 和更高版本仍可以使用 `_cuplogin` DNS SRV 請求發現完整的 Unified Communications 和僅IM服務，但如果存在 `_cisco-uds` 請求則 _cisco-uds 將具有優先權。

表 *6:* 混合雲端型的部署

伺服器版本	連線方式
Cisco Webex Messenger	針對 `https://loginp.Webexconnect.com/cas/FederatedSSO?org=<domain>`的 HTTPS 請求
Cisco Webex Platform 服務	針對 `atlas-a.wbx2.com`的 HTTPS 請求

表 *7:* 雲端型部署

部署類型	連線方式
啓用單一登入 (SSO)	Cisco Webex 管理工具 設定 SSO_ORG_DOMAIN 參數的引導檔案。
未啓用 SSO	Cisco Webex 管理工具

驗證的來源

身份驗證的來源或身份驗證工具使得使用者可以登入到用戶端。

三種可能的身份驗證來源如下：

- Cisco Unified Communications Manager IM and Presence一僅在完整 UC 或 即時訊息中進行公司處所內部署。
- 以 Cisco Unified Communications Manager - 電話模式中的公司處所內部署
- Cisco Webex Messenger 服務-雲端型或混合雲端型的部署。
- Cisco Webex Platform 服務-雲端型或混合雲端型的部署。

用戶端如何尋找到服務

以下步驟描述了用戶端如何使用 SRV 記錄尋找服務：

1. 用戶端的主機或裝置獲得網路連線。

   當用戶端的主機電腦建立網路連線時，亦會從 DHCP 設定中獲取網域名系統(DNS)名稱伺服器的位址。

2. 使用者在首次登入期間使用以下方法之一發現服務：
   - 手動-使用者開始Cisco Jabber然後在歡迎畫面上輸入類似電子郵件的位址。
   - URL 組態-URL 組態允許使用者點選連結以交叉啓動Cisco Jabber而無需手動輸入電子郵件。
   - 使用 EMM 進行行動配置-作爲 URL 組態的替代方法，您可以使用 Android 版 Cisco Jabber 上的 Android for Work 搭配企業行動性管理(EMM)，或 iPhone 和 iPad 版 Cisco Jabber 上的 Apple 託管應用程式組態兩個方式配置 Cisco Jabber。您需要在 EMM 控制台中配置用於建立 URL 組態連結的相同參數。

   要建立 URL 組態連結，請包括以下內容：
   - ServicesDomain-Cisco Jabber用於Service Discovery 的網域。
   - VoiceServicesDomain-對於混合部署，Cisco Jabber用於擷取 DNS SRV 記錄的網域可能不同於用於發現 DNS SRV 記錄的 ServicesDomain Cisco Jabber網域。
   - ServiceDiscoveryExcludedServices-在某些部署方案中，服務可以從Service Discovery過程中排除。這些值可以爲以下各項的組合：
     - Webex
     - CUCM

附註 包括所有三個參數時，不會發生Service Discovery，且會提示使用者手動輸入連線設定。

用以下格式建立組態 URL：

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

範例：

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

使用電子郵件或網站向使用者提供連結。

附註 如果您的組織使用支援交叉啓動專有協議或自訂連結的郵件應用程式，則可以使用電子郵件將連結提供給使用者，否則應使用網站將連結提供給使用者。

3. 用戶端從 DHCP 設定中獲取 DNS 名稱伺服器的位址。
4. 用戶端向中央身份驗證服務(CAS)URL 發出 HTTP 查詢，用於Cisco Webex Messenger服務。

   該查詢使用戶端可以確定網域爲否爲有效Cisco Webex網域。
5. 用戶端依照優先順序查詢名稱伺服器，尋找下列 SRV 記錄：
   - `_cisco-uds`
   - `_collab-edge`

附註 用戶端緩存 DNS 查詢的結果以在後續的啓動時載入。

附註 用戶端緩存 DNS 查詢的結果以在後續的啓動時載入。

以下是 _collab-edge SRV 記錄的範例：

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

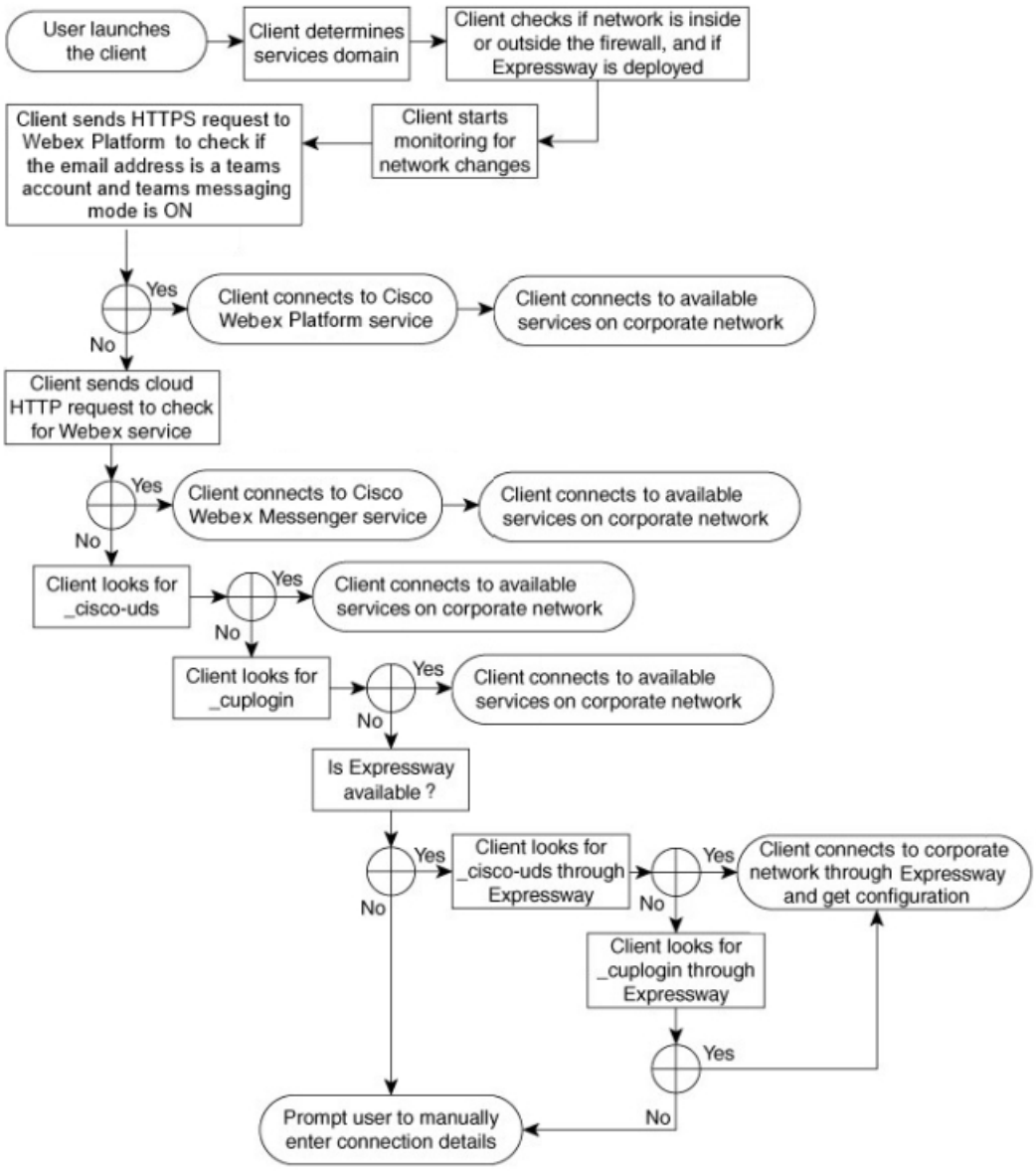
方法 1：搜尋服務

我們建議使用您使用此方法使得 Cisco Jabber 偵測到使用者可以使用哪些服務和功能。搜尋服務意味著用戶端使用 DNS 服務(SRV)記錄來確定用戶端可以使用哪些服務。

用戶端如何發現可用服務

下圖顯示了用戶端用於連線至服務的流程。

圖 *5: Service Discovery*的登入流程



爲了發現可用的服務，用戶端執行以下操作：

1. 檢查網路爲在防火牆內部還爲外部，以及爲否部署了 Expressway for Mobile and Remote Access。用戶端將查詢傳送到名稱伺服器以獲取 DNS 服務(SRV)記錄。
2. 開始監視網路的更改。

   當部署 Expressway for Mobile and Remote Access 時，用戶端會監視網路，以確保在防火牆內部或外部網路發生更改時，用戶端都可以重新連線。
3. 向Cisco Webex Platform 服務發出多個 HTTPS 請求以確定 Jabber 爲否進入團隊訊息傳遞模式。該請求將檢查使用者的電子郵件位址，以查看爲否已在 Webex Control Hub 中爲使用者啓用了團隊訊息傳遞。
4. 向 Cisco Webex Messenger服務的 CAS URL 發出 HTTP 查詢。

   該查詢使用戶端可以確定網域爲否爲有效Cisco Webex網域。

   部署 Expressway for Mobile and Remote Access 後，用戶端將連線至Cisco Webex Messenger服務並使用 Expressway for Mobile and Remote Access 以連線至 Cisco Unified Communications Manager。用戶端首次啓動時，使用者將看到“電話服務連線錯誤”，且必須在用戶端選項螢幕中輸入其憑證，隨後的啓動將使用緩存的資訊。
5. 查詢名稱伺服器以獲取 DNS 服務(SRV)記錄，除非該記錄存在於上一個查詢的緩存中。

   該查詢使用戶端能夠執行以下操作：

   - 確定哪些服務可用。
   - 確定它爲否可以透過 Expressway for Mobile and Remote Access 連線至公司網路。

用戶端對 Cisco Webex Messenger Service 發出 HTTP 查詢

除了在名稱伺服器中查詢 SRV 記錄以尋找可用服務之外，Cisco Jabber將 HTTP 查詢傳送到 CAS URL Cisco Webex Messenger服務。透過此請求，用戶端可以確定雲端型的部署，並對使用者進行Cisco Webex Messenger服務的身份驗證。

當用戶端從使用者那裡獲得服務網域時，它將該網域附加到以下 HTTP 查詢：

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

例如，如果用戶端得到 `example.com` 作爲來自使用者的服務網域，會發出以下查詢：

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

該查詢返回一個 XML 回應，用戶端使用該回應確定服務網域爲否爲有效Cisco Webex網域。

如果用戶端確定服務網域爲有效的Cisco Webex網域，會提示使用者輸入他們的Cisco Webex憑證。然後用戶端即向Cisco Webex Messenger服務驗證，並擷取於Cisco Webex組織管理員配置的組態和 UC 服務。

如果用戶端確定服務網域不爲有效Cisco Webex網域，會將名稱伺服器的查詢結果用以尋找可用服務。

當用戶端將 HTTP 請求傳送到 CAS URL 時，它將使用已配置的系統proxy。

有關更多資訊，請參見*Cisco Jabber* 部署和安裝指南配置*proxy*設定的區段。

用戶端查詢名稱伺服器

用戶端端查詢名稱伺服器時將向名稱伺服器發送個別的同時請求，以獲取 SRV 記錄。

用戶端按以下順序請求以下 SRV 記錄：

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

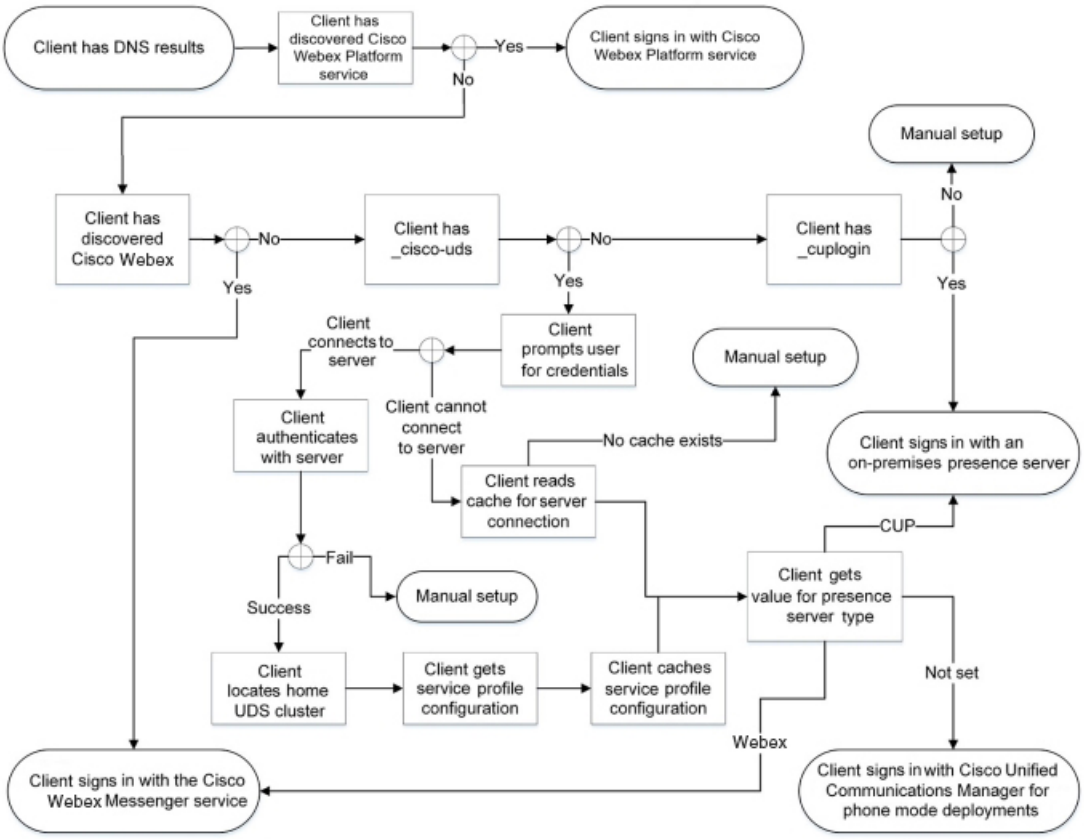
若名稱伺服器返回：

- `_cisco-uds` -用戶端偵測到其已在公司網路內部並連線至 Cisco Unified Communications Manager。
- `_collab-edge` -用戶端嘗試透過 Expressway for Mobile and Remote Access 連線至內部網路並發現服務。
- 沒有 SRV 記錄-用戶端提示使用者手動輸入設定和登入詳細資訊。

用戶端連線至內部服務

下圖顯示了用戶端如何連線至內部服務：

圖 *6:* 用戶端連線至內部服務



連線內部服務時，目標爲確定身份驗證工具，將使用者登入並連線至可用服務。

使用者在登入畫面透過以下服務之一進行身份驗證：

- Cisco Webex Platform 服務-雲端或混合部署。
- Cisco Webex Messenger 服務-雲端或混合部署。
- Cisco Unified Communications Manager-電話模式中的內部部署

用戶端連線至它發現的任何服務，具體取決於部署。

1. 如果用戶端發現使用者已啓用團隊訊息傳遞模式，則用戶端將執行以下操作：
    1. 確定Cisco Webex Platform 服務爲身份驗證的主要來源。
    2. 自動連線至Cisco Webex 平台服務。
    3. 提示使用者輸入憑證。
2. 若用戶端發現 CAS URL 尋找爲指示Cisco Webex使用者，用戶端將執行以下操作：
    1. 確定Cisco Webex Messenger服務爲身份驗證的主要來源。
    2. 自動連線至Cisco Webex Messenger服務。
    3. 提示使用者輸入憑證。
    4. 擷取用戶端和服務組態。
3. 若用戶端發現 `_cisco-uds` SRV 記錄，用戶端執行以下操作：

    提示使用者提供用於進行身份驗證的憑證Cisco Unified Communications Manager。

    1. 找到使用者的主叢集。

        定位主叢集使用戶端可以自動獲取使用者的裝置清單並向Cisco Unified Communications Manager進行註冊。

        在含有多個Cisco Unified Communications Manager叢集的環境中，您需設定叢集間尋找服務(ILS)。ILS 可讓用戶端尋找使用者主叢集及探索服務。

重要須知 請參閱 *Cisco Unified Communications Manager* 功能和服務指南適當的版本了解如何配置 ILS。

    2. 擷取服務配置檔。

        服務配置檔向用戶端提供身份驗證工具以及用戶端和 UC 服務配置。

        用戶端根據即時訊息和狀態配置檔中“產品類型”欄位的值確定身份驗證者，如下所示：

        - Cisco Unified Communications Manager-Cisco Unified Presence 或Cisco Unified Communications Manager IM and Presence Service爲驗證工具。
        - Webex(即時訊息和狀態)—Cisco Webex Messenger服務爲驗證工具。

附註 從此版本開始，用戶端除了發出SRV記錄查詢外，還會發出HTTP查詢。透過 HTTP 查詢，用戶端可以確定爲否應向Cisco Webex Messenger服務進行驗證。

HTTP查詢導致用戶端連線至Cisco Webex Messenger雲端型部署中的服務。若用戶端已經使用 CAS 尋找來發現 Webex 服務則設定**產品類別**欄位的值爲Webex不起作用。

- 未設定-如果服務配置檔案不包含 IM and Presence Service 組態，則身份驗證工具爲Cisco Unified Communications Manager。

3. 登入至身份驗證工具。

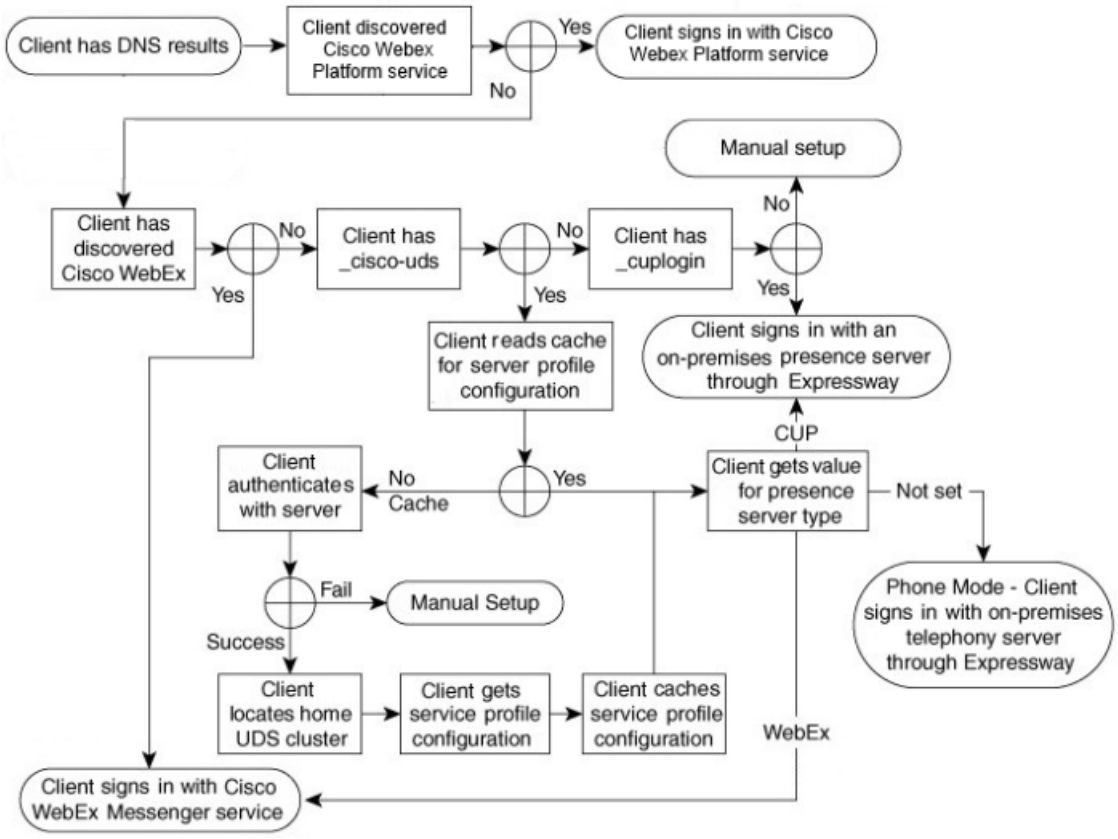
   用戶端登入後，可以確定產品模式。

用戶端透過 Mobile and Remote Access through Expressway 連線

如果名稱伺服器返回 `_collab-edge` SRV 記錄，用戶端將嘗試透過 Expressway for Mobile and Remote Access 連線至內部伺服器。

下圖顯示了當用戶端透過 Expressway for Mobile and Remote Access 連線至網路時，用戶端如何連線至內部服務：

圖 *7:* 用戶端透過 ***Mobile and Remote Access through Expressway*** 連線



當名稱伺服器返回 `_collab-edge` SRV 記錄，用戶端會獲取 Cisco Expressway-E 伺服器的位置，Cisco Expressway-E 伺服器即向用戶端提供內部名稱伺服器的查詢結果。

附註 Cisco Expressway-C 伺服器尋找內部 SRV 記錄，並將記錄提供給 Cisco Expressway-E 伺服器。

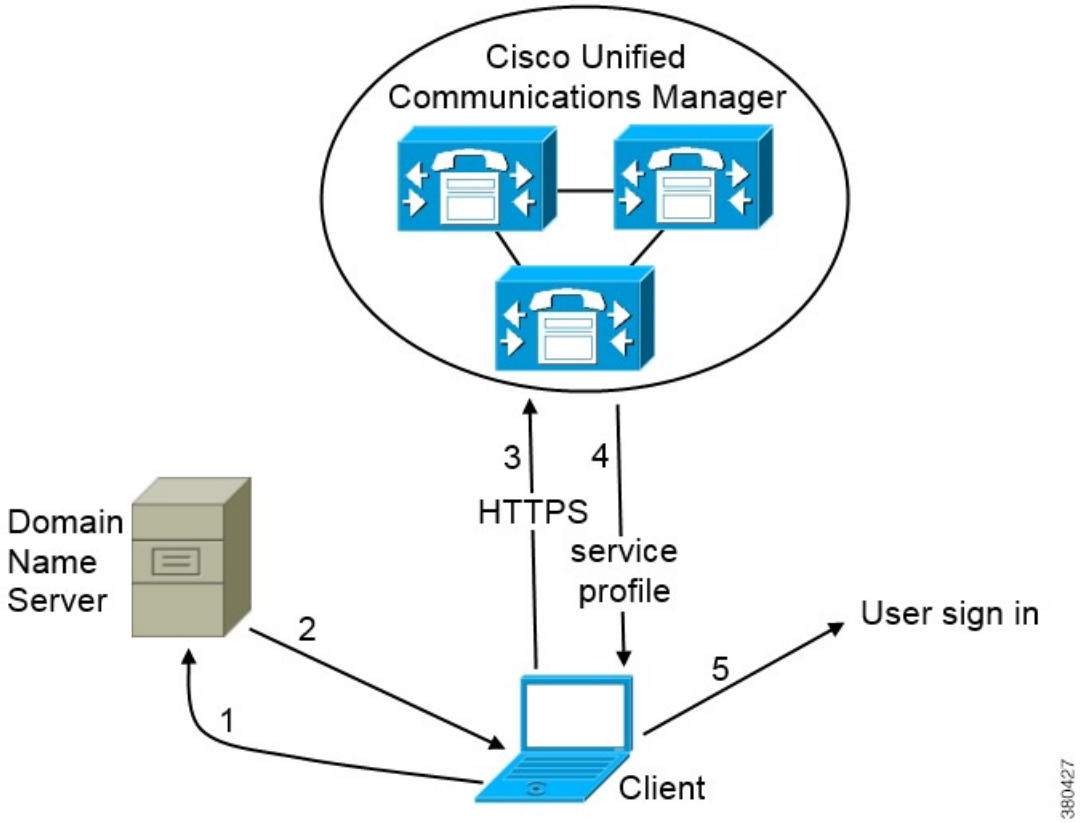
用戶端獲得內部 SRV 記錄後即自Cisco Unified Communications Manager中擷取服務配置檔案，記錄需有包括 `_cisco-uds` 記錄，服務配置檔即會向用戶端提供使用者的主叢集和組態，主叢集爲身份驗證的主要來源。

Cisco UDS SRV 記錄

在使用Cisco Unified Communications Manager版本 9 及更高版本的部署中，用戶端可以透過以下方式自動發現服務和配置 `_cisco-uds` SRV 記錄。

下圖顯示了用戶端如何使用 `_cisco-uds` SRV 記錄。

圖 *8: UDS SRV* 記錄登入流程



1. 用戶端向名稱伺服器查詢 SRV 記錄。
2. 網域名伺服器返回 `_cisco-uds` SRV 記錄。
3. 用戶端找到使用者的主叢集。

   結果，用戶端可以爲使用者檢索裝置配置並自動註冊電話服務。

重要須知

在含有多個Cisco Unified Communications Manager叢集的環境中，您需設定叢集間尋找服務 (ILS)。ILS 可讓用戶端找到使用者主叢集及進行 Service Discovery。

如果未配置 ILS，則必須手動配置遠端集群資訊，類似於 跨叢集的行動化內線 (EMCC)遠端集群設定。如需遠端叢集組態的詳細資訊，請參閱 *Cisco Unified Communications Manager* 功能與服務指南。

4. 用戶端擷取使用者的服務配置檔。

   使用者的服務配置檔包含 UC 服務和用戶端組態的位址和設定。

   用戶端亦從服務配置檔中確定身份驗證工具。
5. 用戶端將使用者登入到身份驗證工具。

以下是 `_cisco uds` SRV 記錄的範例：

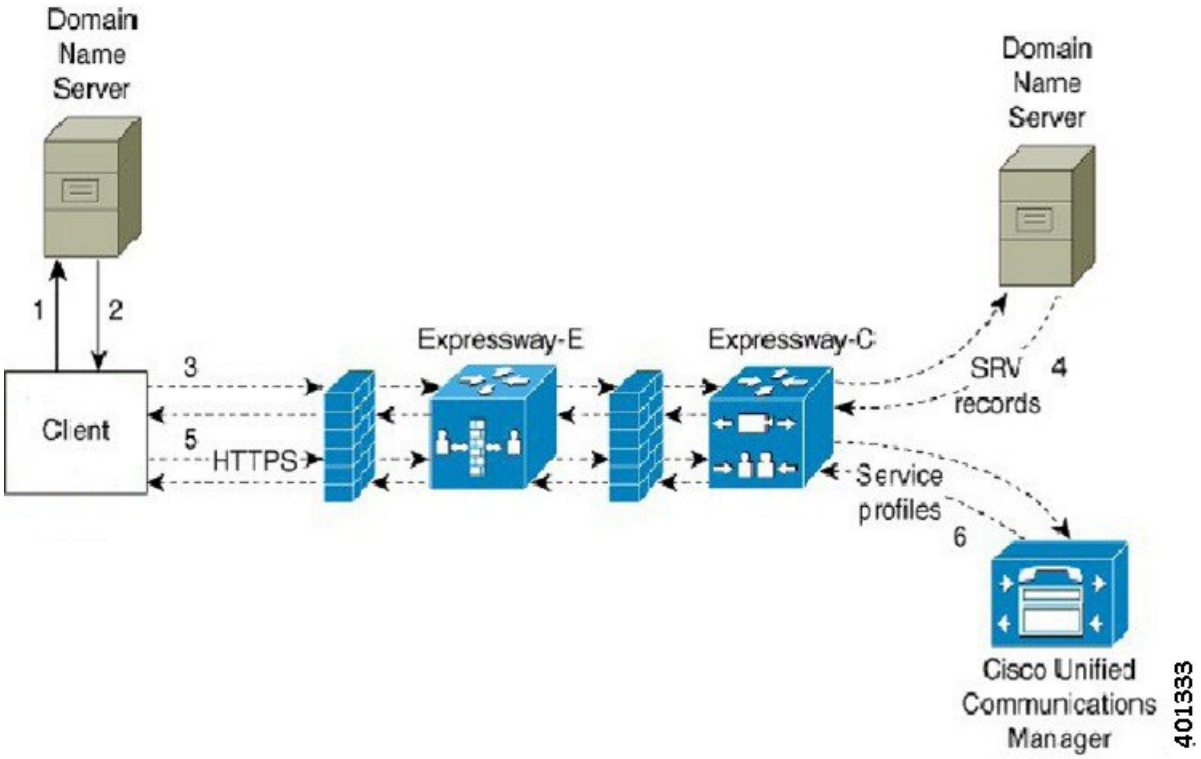
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 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 記錄

Cisco Jabber可以嘗試透過 Expressway for Mobile and Remote Access 連線至內部伺服器，以透過以下方式發現服務 `_collab-edge` SRV 記錄。

下圖顯示了用戶端如何使用 `_collab-edge` SRV 記錄。

圖 *9: Collaboration Edge*記錄登入流程



1. 用戶端向外部網域名伺服器查詢 SRV 記錄。
2. 名稱伺服器返回 `_collab-edge` SRV 記錄，不返回 `_cuplogin` 或 `_cisco-uds` SRV 記錄。

結果爲Cisco Jabber可以找到 Cisco Expressway-E 伺服器。

3. 用戶端從內部網域名伺服器請求內部 SRV 記錄(透過 Expressway)。

   這些 SRV 記錄必須包括 `_cisco-uds` SRV 記錄。

4. 用戶端(透過 Expressway)獲取內部 SRV 記錄。

   結果爲用戶端可以找到Cisco Unified Communications Manager伺服器。

5. 用戶端從Cisco Unified Communications Manager中請求服務配置檔(透過 Expressway)。

6. 用戶端從Cisco Unified Communications Manager中擷取服務配置檔(透過 Expressway)。

   服務配置檔案包含使用者的主叢集，身份驗證的主要來源和用戶端配置。

DNS 組態

用戶端如何使用 DNS

Cisco Jabber 使用網域名伺服器執行以下操作：

- 確定用戶端是在公司網路內部還爲外部。
- 自動發現公司網路內的公司處所內伺服器。
- 在公開網際網路上找到 Expressway for Mobile and Remote Access的存取點。

附註 Android 作業系統限制：使用 DNS 服務的 Android OS 4.4.2 和 5.0 僅能解析網域名，而不能解析主機名。

有關更多資訊，請參閱 Android 開發人員連結。

用戶端如何找到名稱伺服器

Cisco Jabber從以下位置尋找 DNS 記錄：

- 公司網路內的內部名稱伺服器。
- 公共網際網路上的外部名稱伺服器。

當用戶端的主機或裝置建立網路連線時，主機或裝置亦會從DHCP設定中獲取DNS名稱伺服器的位址。根據網路連線，該名稱伺服器可能位於公司網路內部或外部。

Cisco Jabber 查詢主機或裝置從 DHCP 設定獲取的名稱伺服器。

用戶端如何獲取服務網域

用戶端以不同的方式發現服務網域。

新安裝：

- 使用者在用戶端使用者介面中以 `username@example.com` 格式輸入位址。
- 使用者點選含有服務網域的組態 URL。此選項僅在以下版本的用戶端中可用：
  - Android 版 Cisco Jabber 9.6 或更新版本
  - Mac 版 Cisco Jabber 9.6 或更新版本
  - iPhone 和 iPad 版 Cisco Jabber 9.6.1 或更新版本
- 用戶端在引導檔案中使用安裝開關。此選項僅在以下版本的用戶端中可用：
  - Windows 版 Cisco Jabber 9.6 或更新版本

現有安裝：

- 用戶端使用緩存的組態。
- 使用者在用戶端使用者介面中手動輸入位址。

在混合部署中，透過中央身份驗證服務(CAS)尋找發現Cisco Webex網域所需的網域可能會與部署 DNS 記錄的網域不同。在這種情況下，您將 ServicesDomain 設定爲用於發現Cisco Webex的網域並將 VoiceServicesDomain 設定爲部署 DNS 記錄的網域。語音服務網域的配置如下：

- 用戶端在配置檔案中使用 VoiceServicesDomain 參數。此選項在支援以下功能的用戶端中可用：`jabber-config.xml` 檔案。
- 使用者點選含有 VoiceServicesDomain 的組態 URL。以下用戶端中提供了此選項：
  - Android 版 Cisco Jabber 9.6 或更新版本
  - Mac 版 Cisco Jabber 9.6 或更新版本
  - iPhone 和 iPad 版 Cisco Jabber 9.6.1 或更新版本
- 用戶端在引導檔案中使用 Voice_Services_Domain 安裝開關。此選項僅在以下版本的用戶端中可用：
  - Windows 版 Cisco Jabber 9.6 或更新版本

Cisco Jabber 獲得服務網域後，它將查詢配置到用戶端電腦或裝置的名稱伺服器。

網域名稱系統設計

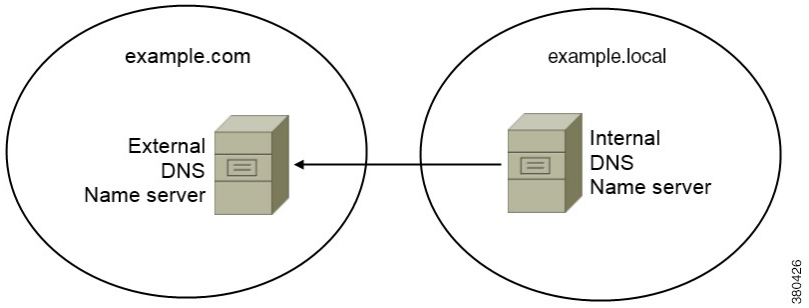
部署 DNS 服務(SRV)記錄的位置取決於 DNS 命名空間的設計。通常，有兩種 DNS 設計：

- 公司網路內部和外部爲個別的網域名。
- 公司網路內部和外部皆爲相同的網域名。

個別網域的設計

下圖顯示了個別網域的設計：

圖 *10:* 個別網域的設計



個別網域的設計的一個示例爲您的組織向網際網路名稱授權機構註冊下列的外部網域：`example.com`。

您的公司亦使用下列的內部網域之一：

- 外部網域的子網域，例如`example.local`。
- 例如，與外部網域不同的網域，`exampledomain.com`。

個別網域的設計具有下列特性：

- 內部名稱伺服器具有包含內部網域資來源記錄的區域。內部名稱伺服器對內部網域具有權威性。
- 當 DNS 用戶端查詢外部網域時，內部名稱伺服器會將請求轉到外部名稱伺服器。
- 外部名稱伺服器具有一個包含組織外部網域的資來源記錄的區域。外部名稱伺服器對該網域具有權威性。
- 外部名稱伺服器可以將請求轉到其他外部名稱伺服器，但外部名稱伺服器無法將請求轉到內部名稱伺服器。

在個別網域結構中部署 *SRV* 記錄

在個別的名稱設計中，有兩個網域，一個內部網域和一個外部網域。用戶端會查詢服務網域中的SRV記錄。內部名稱伺服器必須爲服務網域提供記錄。但在個別的名稱設計中，內部名稱伺服器上可能不存在服務網域的區域。

如果內部名稱伺服器當前不提供服務網域，則可以：

- 在服務網域的內部區域內部署記錄。
- 在內部名稱伺服器上的精確子網域區域內部署記錄。

以內部區域作爲服務網域

如果內部名稱伺服器上尚沒有服務網域的區域則可以建立一個。此方法使內部名稱伺服器對服務網域具有權威性。因爲是權威的，所以內部名稱伺服器不會將查詢轉發到任何其他名稱伺服器。

此方法會更改整個網域的轉發關係，並有可能破壞您的內部DNS結構。如果無法爲服務網域建立內部區域，則可以在內部名稱伺服器上建立精確的子網域區域。

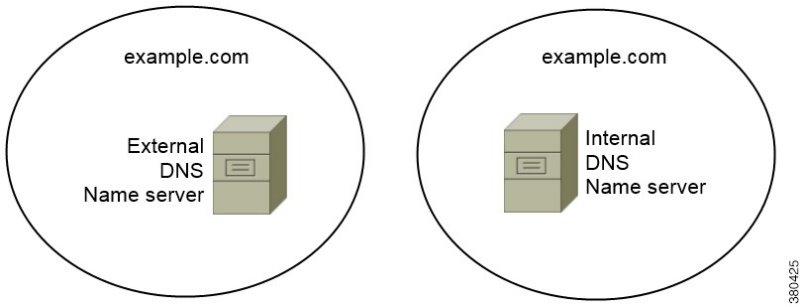
同一網域的設計

同一網域設計的一個示例爲您的組織註冊 `example.com` 爲具有網際網路名稱授權的外部網域。您的組織亦會使用 `example.com` 作爲內部網域的名稱。

單一網域，分左右腦

下圖顯示了具有裂腦網域設計的單個網域。

圖 *11*: 單一網域，分左右腦



兩個 DNS 區域代表單一網域：內部名稱伺服器中的一個 DNS 區域和外部名稱伺服器中的一個 DNS 區域。

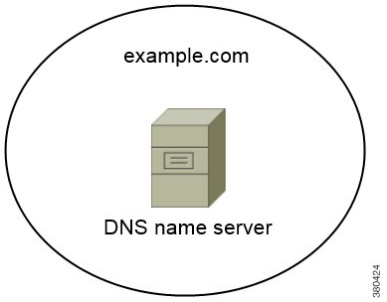
內部名稱伺服器和外部名稱伺服器皆對單一網域具有權威性，但服務不同的主機群。

- 公司網路內部的主機僅存取內部名稱伺服器。
- 公共網際網路上的主機僅存取外部名稱伺服器。
- 在企業網路和公共網際網路之間移動的主機在不同時間會存取不同的名稱伺服器。

單一網域，不分左右腦

下圖顯示了具不分左右腦網域設計的單一網域。

圖 *12*: 單一網域，不分左右腦



在此單一網域不分左右腦設計中，內部和外部主機由一組名稱伺服器提供服務並且可以存取相同的 DNS 資訊。

重要須知 這種設計並不常見，因爲它向潛在的攻擊者公開了有關內部網路的更多資訊。

方法 2：自訂

您可以使用安裝參數，URL 組態或企業行動管理自訂Service Discovery。

Service Discovery 自訂

Windows 版 Cisco Jabber 的自訂安裝

Windows 版 Cisco Jabber 提供了 MSI 安裝軟體包，您可以透過以下方式使用該軟體包：

- 使用命令行-您可以在命令行視窗中指定參數來設定安裝屬性。

  如果您打算安裝多個實例，請選擇此選項。

- 手動執行 MSI-在用戶端工作站的檔案系統上手動執行 MSI，然後在啓動用戶端時指定連線屬性。

  如果您打算安裝單個實例以進行測試或評估，請選擇此選項。

- 建立自訂安裝程式-開啓預設安裝包，指定所需的安裝屬性，然後儲存自訂安裝包。

  如果您計畫分配具有相同安裝屬性的安裝軟體包，請選取此選項。

- 使用群組原則進行部署-將用戶端安裝在同一網域中的多台電腦上。

安裝開關：Windows 版 Cisco Jabber

安裝時Cisco Jabber，您可以指定身份驗證工具和伺服器位址。安裝程式會將這些詳細資訊儲存到引導檔案中。使用者首次啓動用戶端時，用戶端將讀取引導檔案。如果部署了Service Discovery，則引導檔案將優先。

在尚未部署Service Discovery 且您不希望使用者手動指定其連線設定的情況下，引導檔案爲Service Discovery提供了一種後備機制。

用戶端僅在初始啓動時讀取引導檔案。初始啓動後，用戶端將緩存伺服器位址和配置，然後在後續啓動時從緩存中載入。

我們建議您不要在使用Cisco Unified Communications Manager 9.x 及更高版本的公司處所內部署中使用引導檔案，而應使用Service Discovery。

Mac版、iPhone 和 iPad 版、 Android 版 Cisco Jabber 的自訂安裝

您可以使用 URL 組態爲 Mac 或行動用戶端建立 Cisco Jabber 的自訂安裝。行動用戶端方面您還可以使用企業行動性管理。這些自訂安裝取決於啓用服務的安裝參數。

URL 組態

要使使用者無需手動輸入Service Discovery資訊即可啓動 Cisco Jabber，請向使用者提供配置 URL 連結以安裝用戶端。

透過直接將連結傳送給使用者或透過將連結發佈到網站來向使用者提供配置 URL 連結。

使用 EMM 進行行動配置

您可以在Android 版 Cisco Jabber 和iPhone 和 iPad 版 Cisco Jabber 上使用企業行動性管理(EMM)配置 Cisco Jabber。有關設定 EMM 的更多資訊，請參閱 EMM 供應商爲管理員提供的指示。

如果希望 Jabber 僅在受管理的裝置上執行，則可以部署基於認證的身份驗證，並透過 EMM 註冊用戶端憑證。

有關如何部署 EMM 的更多資訊，請參見*Cisco Jabber* 的公司處所內部署或適用於 *Cisco Jabber* 的雲和混合部署中的部署 *Cisco Jabber* 的應用程式

方法 3：手動安裝

進階選項爲使用者可以在登入畫面中手動連線至服務。

高可用性

即時訊息和在線狀態的高可用性

高可用性爲指子叢集中存在多個節點以提供即時訊息傳遞和狀態服務的故障轉移功能的環境。如果子叢集中的一個節點不可用則語音和視訊故障轉移到子叢集中的另一節點。這樣，高可用性可確保 Cisco Jabber 即時訊息傳遞和狀態服務的可靠連續性。

LDAP 支援高可用性。使用 UDS 聯絡人來源時不支援高可用性。

Cisco Jabber 透過以下伺服器支援高可用性：

Cisco Unified Communications Manager IM and Presence Service 版本 9.0 或更高

使用以下 Cisco Unified Communications Manager IM and Presence Service說明文件獲取有關高可用性的更多資訊。

Cisco Unified Communications Manager IM and Presence Service 的組態和管理

高可用性用戶端登入配置檔

對高可用性進行故障排除

故障轉移期間保留中的活動通話

如果 Cisco Unified Communications Manager 的主實例發生故障轉移到輔助實例，則您將無法保留進行中的通話。

用戶端中的高可用性

故障轉移期間的用戶端行為

如果在伺服器上配置了高可用性，則在主伺服器故障轉移到輔助伺服器後，用戶端將暫時失去在線狀態，最多一分鐘。配置重新登入參數以定義用戶端在嘗試重新登入伺服器之前等候多長時間。

配置組態參數

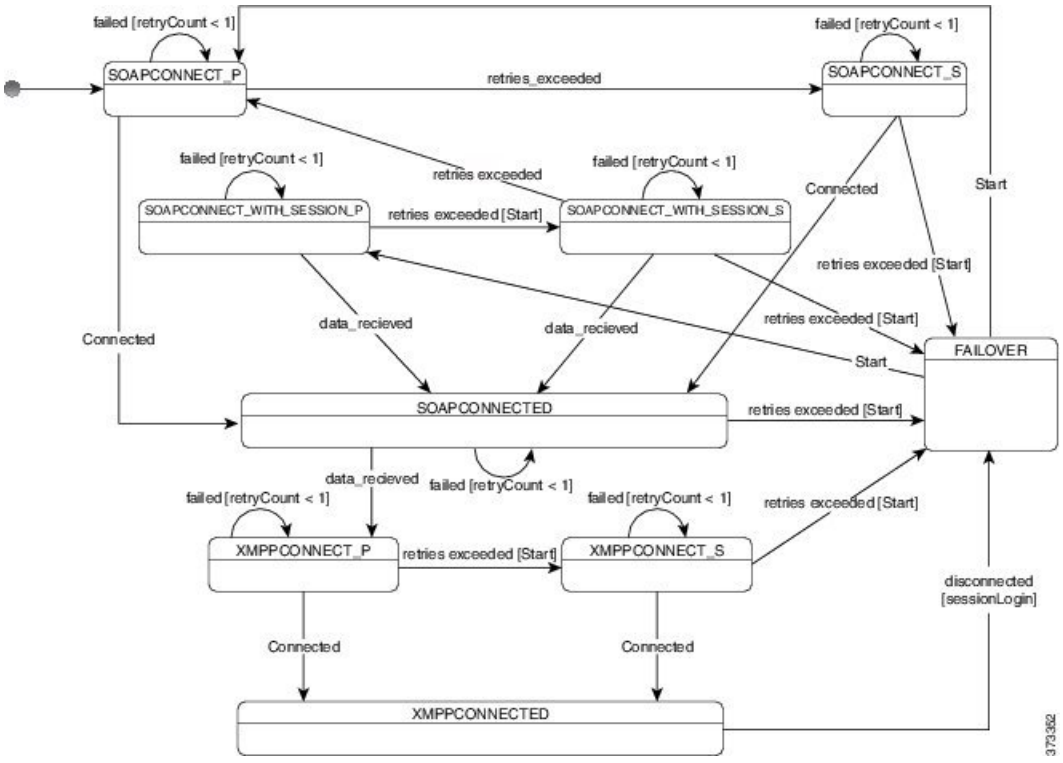
在 Cisco Unified Communications Manager IM and Presence Service中，您可以配置 Cisco Jabber 在嘗試重新登入到伺服器之前等候的最多和最少秒數。在伺服器上，您可以在以下欄位中指定重新登入參數：

- 用戶端重新登入下限
- 用戶端重新登入上限

故障轉移期間的用戶端行為

下圖顯示了故障轉移期間 Cisco Unified Communications Manager IM and Presence Service 時用戶端的行爲。

圖 *13:* 故障轉移期間的用戶端行為



1. 當用戶端自其伺服器斷開連線時，用戶端將從 XMPPCONNECTED 狀態變爲 FAILOVER 狀態。

2. 在 FAILOVER 狀態中，用戶端嘗試透過嘗試 SOAPCONNECT_SESSION_P(作爲主伺服器)來達到 SOAPCONNECTED 狀態，如果失敗，則嘗試透過 SOAPCONNECT_SESSION_S(作爲輔助伺服器)。
   - 如果無法獲得 SOAPCONNECT_SESSION_P 或 SOAPCONNECT_SESSION_S，則用戶端將重新進入 FAILOVER 狀態。
   - 用戶端從 FAILOVER 狀態嘗試達到 SOAPCONNECT_P 狀態，如果失敗，則嘗試達到 SOAPCONNECT_S 狀態。
   - 如果用戶端無法達到 SOAPCONNECT_P 或 SOAPCONNECT_S 狀態，則在使用者啓動登入嘗試之前，用戶端不會再嘗試與 IM & P 伺服器的任何自動連線。
3. 用戶端自 SOAPCONNECT_SESSION_P，SOAPCONNECT_SESSION_S，SOAPCONNECT_P 或 SOAPCONNECT_S 狀態擷取其當前的主要輔助 XMPP 伺服器位址。此位址會在故障轉移期間更改。
4. 用戶端從 SOAPCONNECTED 狀態嘗試透過嘗試連線至 XMPPCONNECT_P 狀態來達到 XMPPCONNECTED 狀態，如果失敗，則嘗試 XMPPCONNECT_S 狀態。
   - 如果用戶端無法達到 XMPPCONNECT_P 或 XMPPCONNECT_S 狀態，則在使用者啓動登入嘗試之前，用戶端不會再嘗試與 IM & P 伺服器的任何自動連線。
5. 用戶端處於 XMPPCONNECTED 狀態後便具有 IM & P 功能。

語音及視訊的高可用性

如果子叢集中的一個節點不可用則語音和視訊故障轉移到子叢集中的另一節點。

預設情況下，軟體電話裝置或桌面電話最多需要 120 秒才能向另一個節點註冊。如果此逾時時間過長，請調整您節點的 SIP 站 KeepAlive 間隔的服務參數。 SIP 站 KeepAlive 間隔服務參數在 Cisco Unified Communications Manager上修改所有電話裝置。調整時間間隔之前，請先分析對Cisco Unified Communications Manager伺服器的影響。

要配置節點的服務參數，請在Cisco Unified Communications Manager管理選擇**系統** > **服務參數**。

對於使用非DNS SRV記錄方法的電話模式部署，語音和視訊無法進行故障轉移，因爲僅指定了一個 Cisco Unified Communications Manager 節點。

持續聊天的高可用性

持續聊天具有高可用性支援。在容錯移轉期間，系統可能會提示使用者無法傳送訊息。當節點容錯移轉後，使用者會自動重新加入聊天室，而且再度可以傳送訊息。

聯絡人搜尋和聯絡人解析的高可用性

Cisco Unified Communications Manager 使用者資料服務(UDS)提供了用於聯絡人搜尋和聯絡人解析的高可用性。如果主 UDS 伺服器不可用，則 Jabber 會自動故障轉移到第二個 UDS 伺服器或第三個 UDS 伺服器(如果已配置)。

語音信箱的高可用性

若有設定次要語音信箱伺服器，則當主要伺服器無法使用或無法連線時所有用戶端會自動容錯移轉至次要語音信箱伺服器。

可存活性遠端位址電話技術

適用於 Windows 版 Cisco Jabber 和 Mac 版 Cisco Jabber。

當Cisco Unified Communications Manager應用程式無法存取或 WAN 斷開，請使用 Cisco Unified Survivable Remote Site Telephony (SRST) 爲遠程使用者保留基本電話服務。當連接斷開時，用戶端將會無法轉移到遠程站點上的本地路由器。

附註 支援 SRST 12.8 和更高版本。

SRST提供基本的通話控制，當系統處於容錯移轉狀態時，僅啓用開始、結束、保留、恢復、靜音、取消靜音和雙音調多頻 (DTMF) 訊號。

容錯移轉期間下列服務不可用：

- 視訊
- 通話中功能 (轉移、iDivert、通話駐留、會議、發送至行動電話)
- 經由辦公室撥號 (DVO)
- 即時會議
- 二進位發言權控制通訊協定 (BFCP) 共用

有關配置 SRST 的詳細說明，請參閱*Cisco Unified Communications Manager* 管理指南。

組態之優先等級

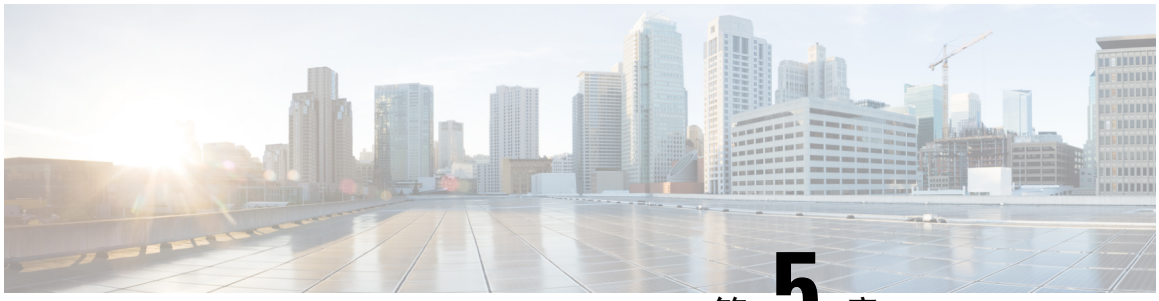
當服務配置檔和組態檔同時存在時，下表說明哪個參數值優先。

服務配置檔	組態檔	哪個參數值優先?
參數值已設定	參數值已設定	服務配置檔
參數值已設定	參數值爲空白	服務配置檔
參數值爲空白	參數值已設定	組態檔
參數值爲空白	參數值爲空白	服務配置檔空白(預設)值

使用 Cisco 支援欄位的群組配置

群組組態檔適用於一個子集的使用者。如果爲使用者提供 CSF 裝置，則可以在裝置組態中**Cisco 支援欄位**指定群組組態檔的檔名。如果使用者沒有CSF裝置，則可以在安裝期間使用TFTP_FILE_NAME參數爲每個群組設定不同的組態檔名。

TCT 和 BOT 上的 COP 檔案 14122 版本或更高支援群組配置。



第 5 章

聯絡人來源

什麼為聯絡人來源？

聯絡人來源爲使用者資料的集合。當使用者在Cisco Jabber用戶端中搜尋聯絡人或新增聯絡人時，將從聯絡人來源讀取聯絡人資訊。

Cisco Jabber從聯絡人來源檢索資訊以填充聯絡人名單，更新用戶端以及其他顯示聯絡人資訊的區域中的聯絡人卡片。當用戶端接收到任何傳入通訊(例如即時訊息或語音/視訊通話)時，聯絡人來源將用於解析聯絡人資訊。

聯絡人來源伺服器

附註 所有 Jabber 用戶端都支援用於目錄整合的 LDAPv3 標準。任何支援此標準的目錄伺服器都與這些用戶端相容。

您可以與Cisco Jabber一起使用以下聯絡人來源伺服器：

- 適用於 Windows Server 2012 R2 的 Active Directory 網域服務
- 適用於 Windows Server 2008 R2 的 Active Directory 網域服務
- Cisco Unified Communications Manager使用者資料伺服器(UDS)。Cisco Jabber使用Cisco Unified Communications Manager 10.5 版或更高版本支援 UDS。
- OpenLDAP
- Active Directory 輕量型目錄服務 (AD LDS) 或 Active Directory 應用程式模式 (ADAM)

為什麼需要聯絡人來源？

Cisco Jabber 透過以下方式使用聯絡人來源：

- 使用者搜尋聯絡人-用戶端獲取輸入的資訊並在聯絡人來源中搜尋。從聯絡人來源中擷取資訊，而用戶端將顯示可用於與聯絡人進行互動的方法。
- 用戶端收到傳入通知-用戶端將從傳入通知中獲取資訊，並以聯絡人來源中的聯絡人解析 URI，編號，JabberID。用戶端將在警報中顯示聯絡人詳細資訊。

何時配置聯絡人來源伺服器

附註 在註冊到 Active Directory 網域的工作站上安裝 Cisco Jabber。在這種環境下，您無需配置 Cisco Jabber 即可連線至目錄。用戶端自動發現目錄並連線至該網域中的全球目錄伺服器。

如果您計劃使用以下服務之一作爲聯絡人來源，請配置 Cisco Jabber 以連線至目錄服務：

- Active Directory 服務
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight 目錄服務
- Active Directory 應用程式模式

您可以選擇將目錄整合配置爲：

- 更改預設屬性對映。
- 調整目錄查詢設定。
- 指定用戶端如何擷取聯絡人照片。
- 執行網域內聯合。

Cisco目錄整合 聯絡人來源選項

在公司處所內部署中，用戶端需要以下聯絡人來源之一來解析目錄尋找中的使用者資訊：

- 輕型目錄存取協議(LDAP)-如果您有公司目錄，則可以使用以下基於 LDAP 的聯絡人來源選項將目錄配置爲聯絡人來源：
  - Cisco目錄整合(CDI)-使用此聯絡人方式選項來部署所有用戶端。
- Cisco Unified Communications Manager 使用者資料服務(UDS)-如果您沒有公司目錄，或者您的部署中包含使用 Expressway Mobile and Remote Access 連線的使用者，則可以使用此選項。

輕量型目錄存取通訊協定

Cisco目錄整合如何與 LDAP 配合使用

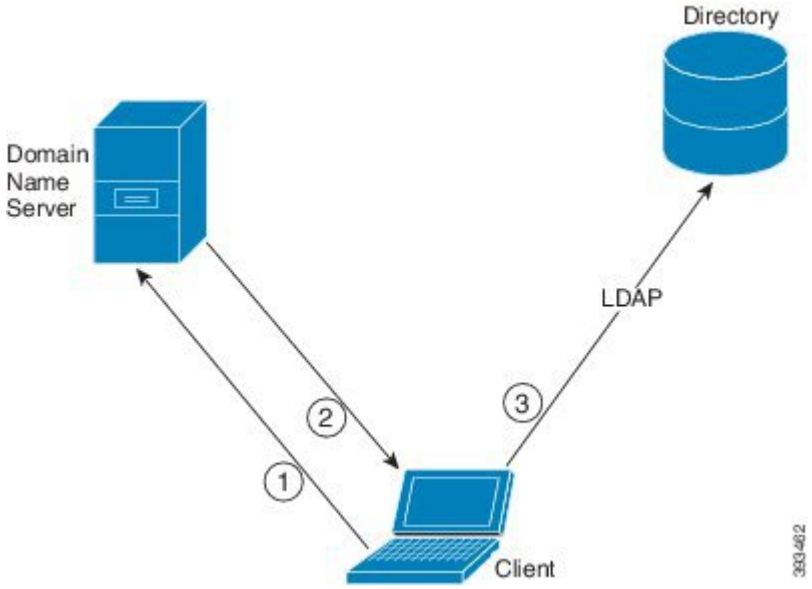
CDI 使用Service Discovery來確定 LDAP 伺服器。

以下爲使用 CDI 進行公司處丶所內部署的預設設定：

- Cisco Jabber 與 Active Directory 整合爲聯絡人來源。
- Cisco Jabber 會自動發現並連線至全球目錄。

自動 Service Discovery- 建議使用

我們建議使用您使用Service Discovery來自動連線全球目錄(GC)伺服器或 LDAP 伺服器並對其進行身份驗證。如果要自訂部署，請查看提供 LDAP 伺服器資訊的選項以及可用的身份驗證選項。Jabber 首先將 DNS 查詢傳送到 GC 網域以發現 GC 伺服器。若無發現 GC 伺服器，則 Jabber 會將 DNS 查詢傳送到 LDAP 網域以發現 LDAP 伺服器。



如果有可用的 GC，則用戶端將執行以下操作：

1. 從工作站獲取 DNS 網域，並尋找 GC 的 SRV 記錄。
2. 自 SRV 記錄中擷取 GC 的位址。
3. 使用登入使用者的憑證連線至 GC。

使用 GC 網域進行 discovery

Jabber 嘗試透過 DNS SRV 查詢發現 GC 伺服器。首先，Jabber 獲得 GC 網域：

1. 如果有的話，Jabber 使用 DNSFORESTNAME 環境變數爲 GC 網域。
2. 若 DNSFORESTNAME 不可用，Jabber 會檢查以下爲否爲 GC 網域：
   - 在 Windows 上，Jabber 會調用 Windows `DsGetDcName` API 以獲取 `DnsForestName`。
   - 在非 Windows 平台上，Jabber 自 `jabber-config.xml`讀取 LdapDNSForestDomain 。

Jabber 獲取 GC 網域後，它將傳送 DNS SRV 查詢以獲取 GC 伺服器位址：

- 在 Windows 上，Jabber 透過 Windows `DsGetSiteName` API 檢查`SiteName`爲否可用：
  - 若`SiteName`存在，Jabber 傳送出 DNS SRV 查詢：`_gc._tcp.SiteName._sites.GCDomain` 以獲取 GC 伺服器位址。
  - 如果`SiteName`不存在或 `_gc._tcp.SiteName._sites.GCDomain` 沒有返回 SRV 記錄，Jabber 傳送出 DNS SRV 查詢：`_gc._tcp.GCDomain` 以獲取 GC 伺服器位址。
- 在非 Windows 平台上，Jabber 傳送 DNS SRV 查詢：`_gc._tcp.GCDomain` 以獲取 GC 伺服器位址。

使用 LDAP 網域進行 discovery

如果 Jabber 無法發現 GC 伺服器，則它將嘗試發現 LDAP 網域：

1. 如果有的話，Jabber 使用 DNSFORESTNAME 環境變數爲 LDAP 網域。
2. 若 USERDNSDOMAIN 無法使用，Jabber 自 `jabber-config.xml`讀取 LdapUserDomain 。
3. 如果 LdapUserDomain 不可用，Jabber 以使用者登入時使用的電子郵件網域爲 LDAP 網域。

Jabber 獲取 LDAP 網域後，它將傳送 DNS SRV 查詢以獲取 LDAP 伺服器位址：

- 在 Windows 上，Jabber 透過 Windows `DsGetSiteName` API檢查`SiteName`爲否可用。
  - 如果網站名稱存在，Jabber 發出 DNS SRV 查詢，`_ldap._tcp.SiteName.sites.LdapDomain` 以獲取 LDAP 伺服器位址。
  - 如果`SiteName`不存在或 `_ldap._tcp.SiteName.sites.LdapDomain` 沒有返回 SRV 記錄，Jabber 傳送出 DNS SRV 查詢：`_ldap._tcp.LdapDomain` ，以獲取 LDAP 伺服器位址。
- 在非 Windows 平台上，Jabber 傳送 DNS SRV 查詢：`_ldap._tcp.LdapDomain` 以獲取 LDAP 伺服器位址。

Jabber 連線至 LDAP 伺服器後，它將讀取 LDAP 伺服器的`SupportedSaslMechanisms`屬性指定要使用的身份驗證機制的清單和順序。

手動配置 LDAP 服務

手動配置 LDAP 服務

1. 您可以配置 PrimaryServerName 參數，用於定義供 Jabber 連線的特定 LDAP 伺服器。
2. 您可以配置 `jabber-config.xml` 檔案中的 LdapSupportedMechanism參數以覆蓋 supportedSaslMechanisms屬性中的清單。

   聯絡人服務和 LDAP 伺服器必須支援所有這些機制。請使用空格來區隔各個值。

   - GSSAPI – Kerberos v5
   - EXTERNAL – 外部 SASL
   - PLAIN(預設) – 簡單 LDAP 綁定，匿名爲簡單綁定的子集。

   範例：

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

3. 如有必要，配置 LdapUserDomain 參數以設定 Jabber 用於與 LDAP 伺服器進行身份驗證的網域。例如：

   ```
   CUCMUsername@LdapUserDomain
   ```

LDAP 注意事項

Cisco 目錄整合 (CDI) 取代基本目錄整合 (BDI) 和進階目錄整合 (EDI)參數。CDI 參數適用於所有用戶端。

Cisco Jabber 部署案例

方案 1：若您為 11.8 的 Jabber 新手

我們建議使用您使用Service Discovery來自動連線 LDAP 伺服器並進行身份驗證。如果要自訂部署，請查看提供 LDAP 伺服器資訊的選項以及可用的身份驗證選項。

方案 2：若要自 EDI 組態升級到 11.8

如果您的配置僅使用 EDI 參數，則 Jabber 將讀取 EDI 參數並將其用於您的目錄來源整合，我們仍然建議使用您升級 EDI 參數並將其替換爲等效的 CDI 參數。

方案 3：若要自 BDI 組態升級到 11.8

如果您的配置僅使用 BDI 參數，則必須將 BDI 參數更新爲等效的 CDI 參數。例如，BDIPrimaryServerName的話您需要將參數替換爲 PrimaryServerName。 BDIEnableTLS 被替換爲UseSSL參數。

方案 4：若要自 EDI / BDI 混合組態升級到 11.8

如果您的配置同時使用 EDI 和 BDI，則必須檢查 BDI 配置，因爲 Jabber 在連線至 LDAP 伺服器時將使用 EDI 參數。

目錄參數

下表列出了 BDI 和 EDI 參數，指示 CDI 參數名稱或其不適用於 Jabber 11.8 或更高版本。

BDI 參數	EDI 參數	CDI 參數
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL
-	UseSecureConnection	-

BDI 參數	EDI 參數	CDI 參數
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BDIBaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards
-	MinimumCharacterQuery	MinimumCharacterQuery
BDI SearchBase1	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
BDI PhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName
BDIFirstname	firstName	firstName

BDI 參數	EDI 參數	CDI 參數
BDILLastname	lastName	lastName
BDIEmailAddress	EmailAddress	EmailAddress
BDISipUri	SipUri	SipUri
BDI PhotoSource	PhotoSource	PhotoSource
BDI BusinessPhone	BDIBusinessPhone	BDIBusinessPhone
BDI MobilePhone	MobilePhone	MobilePhone
BDIHomePhone	HomePhone	HomePhone
BDI OtherPhone	OtherPhone	OtherPhone
BDIDirectoryUri	DirectoryUri	DirectoryUri
BDITitle	Title	Title
BDICompanyName	CompanyName	CompanyName
BDIUserAccountName	UserAccountName	BDIUserAccountName
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

使用者資料服務(UDS)爲 Cisco Unified Communications Manager 上的 REST 介面，可提供聯絡人解析。

在以下情況下，UDS 用於聯絡人解析：

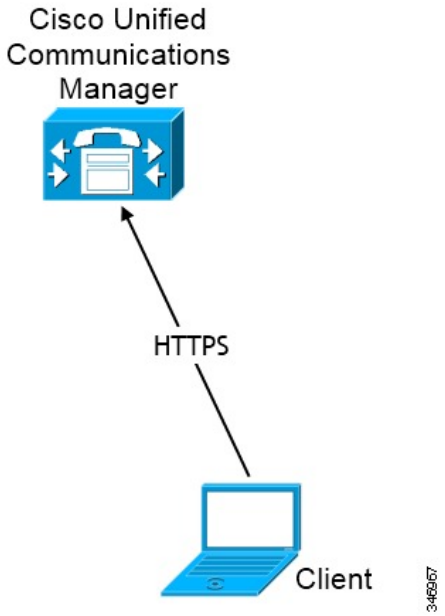
- 如果您設定 DirectoryServerType 參數以在用戶端配置檔案中使用 UDS 的值。

  透過此配置，用戶端在公司防火牆之內或之外時都可以使用 UDS 進行聯絡人解析。

- Expressway for Mobile and Remote Access 部署

  使用此配置，當用戶端位於公司防火牆之外時，用戶端會自動使用 UDS 進行聯絡人解析。

您將會自目錄伺服器將聯絡人資料同步到 Cisco Unified Communications Manager 中。然後，Cisco Jabber 會自動從 UDS 擷取該聯絡人資料。



具有多個叢集的聯絡人解析

要使用多個 Cisco Unified Communications Manager 叢集解析聯絡人，請將公司目錄中的所有使用者同步到各個叢集。在適當的叢集上提供這些使用者的子集。

假設您的組織有 40,000 個使用者，北美有 20,000 位使用者，20,000 個使用者居住在歐洲，您的組織在北美及歐洲皆有以下 Cisco Unified Communications Manager 叢集：

- `cucm-cluster-na`北美
- `cucm-cluster-eu` 歐洲

在此示例中，將所有 40,000 個使用者同步到兩個叢集。配置 20,000 個北美使用者於 `cucm-cluster-na`，歐洲的 20,000 個使用者配置於 `cucm-cluster-eu`。

當歐洲使用者致電北美使用者時，Cisco Jabber 將自`cucm-cluster-na`爲歐洲的使用者擷取聯絡資料。

當北美使用者致電歐洲使用者時，Cisco Jabber 會自`cucm-cluster-eu`爲北美的使用者擷取聯絡資料。

延伸的 UDS 聯絡人來源

將聯絡人搜尋從 UDS 擴展到您的 LDAP 伺服器。在 Cisco Unified Communications Manager 11.5 (1) 或更高版本中，您可以配置 Jabber 爲否搜尋 LDAP 伺服器。

LDAP 先決條件

Cisco Jabber 使用各種屬性搜尋聯絡人來源，預設情況下並不索引所有這些屬性。爲了確保高效率的搜尋，須對 Cisco Jabber 使用的屬性進行索引。

如果使用預設屬性對映，請確保會在 LDAP 伺服器上對以下屬性進行索引：

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-Pr即時訊息aryUserAddress

LDAP 服務帳號

在 Unified Communications Manager 版本 12.5 (1) SU2 中，Unified CM 新增了對在服務設定檔中安全傳遞加密LDAP認證的支援。此更新會確保一律以加密格式儲存和發送密碼，以保護對目錄的存取。此更改包括以下過程中的加密：

- 目錄存取驗證
- 用戶端設定檔下載
- BAT 匯入/匯出
- 升級

如需更多詳細資訊，請參閱 *Cisco Unified Communications Manager* 和 *IM and Presence* 服務 *12.5(1)SU2* 版的版本資訊。

在具有此 Unified CM 版本或更高版本的 Jabber 12.8 中，我們透過在驗證最終使用者之後將 LDAP 認證作爲使用者設定檔的一部分下載來利用此功能。

要將 Jabber 連線至 LDAP 伺服器，您必須定義 LDAP 如何驗證 Jabber 使用者：

- 預設選項爲 Jabber 使用 Kerberos 或用戶端憑證(SASL 外部)自動連線至聯絡人來源伺服器。我們建議使用此選項，因爲它爲最安全的。
- 如果您在服務配置檔或 `jabber-config.xml` 檔案定義憑證，憑證將始終優先於預設選項。
- 如果您配置 LdapSupportedMechanisms 參數使用 PLAIN 值，但不配置目錄配置檔案的使用者名稱或密碼，則使用者可以直接將其目錄憑證輸入到用戶端中。
- 否則，如果您連接到服務設定檔中的安全連接埠，則可以定義 Jabber 如何連接到聯絡來源伺服器。您可以透過在以下選項中指定 Cisco Unified Communications Manager 認證來定義 `jabber-config.xml` 檔案中的 LDAP_UseCredentialsFrom 參數。
- 如果之前選項不可用，請使用服務配置檔或 `jabber-config.xml` 檔案。此選項最不安全。Jabber 使用帳號以於聯絡人來源伺服器進行身份驗證。我們建議使用此帳號對目錄具有唯讀的存取權限且最好爲一組熟悉的公開憑證。在這種情況下，所有 Jabber 使用者都使用這些憑證進行搜尋。

附註 從 Cisco Unified Communications Manager 12.0 版本開始，您不能在服務配置檔中配置使用者名稱和密碼。Jabber 使用者可以選擇使用目錄服務驗證自己。使用者首次登入 Jabber 時會收到通知。若他們第一次沒有驗證自己，則當他們嘗試存取聯絡人名單時會收到警示。

Jabber ID 屬性對映

使用者 ID 的 LDAP 屬性爲 sAMAccountName。此爲預設屬性。

如果使用者 ID 的屬性不爲 sAMAccountName 且您在 Cisco Unified Communications Manager IM and Presence Service中使用預設即時訊息位址方案，則必須在用戶端配置檔案中將屬性指定爲參數值，如下方所示：

CDI 參數爲 UserAccountName。<UserAccountName>屬性名稱</ UserAccountName>

如果未在配置中指定屬性且該屬性不爲 sAMAccountName ，用戶端無法解析您目錄中的聯絡人，結果使用者無法獲得在線狀態亦無法傳送或接收即時訊息。

搜尋 Jabber ID

Cisco Jabber 使用 Jabber ID 在目錄中搜尋聯絡人資訊。有一些選項可以最佳化目錄中的搜尋：

- **搜尋基礎**—預設情況下，用戶端從目錄樹的根目錄開始搜尋。您可以使用搜尋基礎來指定其他搜尋開始或將搜尋限制爲特定的群組。例如，貴組織一子集使用者僅具有即時訊息傳遞功能。將這些使用者包括在 OU 中，然後將其指定爲搜尋基礎。
- **基礎篩選**—指定目錄子項名稱僅用於在查詢目錄時擷取使用者物件以外的物件。
- **預測搜尋篩選**—您可以定義多個逗號分隔的值來過濾搜尋查詢。預設值爲 ANR(歧義名稱解析。)

有關這些選項的更多資訊，請參見 *Cisco Jabber* 的參數參考指南。

本地聯絡人來源

Cisco Jabber 能夠存取和搜尋本地聯絡人來源。這些本地聯絡人來源包括：

- Windows 版 Cisco Jabber可以存取 Microsoft Outlook 中儲存的本地聯絡人。
- Windows 版 Cisco Jabber(從版本 11.1 起)可以存取 IBM Notes 中儲存的本地聯絡人。
- Mac 版 Cisco Jabber，Android 版 Cisco Jabber 和iPhone 和 iPad 版 Cisco Jabber 可存取本地通訊錄聯絡人。

自訂聯絡人來源

所有用戶端的 Cisco Jabber 爲使用者提供了匯入自訂聯絡人至其用戶端的功能。

聯絡人緩存

Cisco Jabber建立公司處所內緩存。除其他事項外，緩存還儲存使用者的聯絡人名單。當使用者在其聯絡人名單中搜尋某人時，Jabber 會在開始目錄搜尋之前在公司處所內緩存中搜尋配對的項目。

如果使用者搜尋不在其聯絡人名單中的某人，則 Jabber 首先搜尋公司處所內緩存，然後搜尋公司目錄。如果使用者隨後與該聯絡人開始聊天或通話，則 Jabber 會將聯絡人新增到公司處所內緩存中。

公司處所內緩存資訊將在 24 小時後過期。

解決重複的聯絡人

Jabber 中的聯絡人可以來自不同的來源。Jabber 可以在多個聯絡人來源中找到同一聯絡人的相同結果，這種情況下，Jabber 會確定哪些記錄與同一個人相符並合併該位聯絡人的所有資料。爲了確定聯絡人來源中的一個記錄爲否與聯絡人相同，Jabber 會依以下的順序尋找欄位：

1. **Jabber ID(JID)**—如果記錄具有 JID，則 Jabber 依此作記錄上的對比。Jabber 不會依郵件或電話號碼欄位再進一步比對。
2. **郵件**—如果記錄中有一郵件欄位，則Jabber依此作記錄上的對比。Jabber不會依電話號碼欄位再進一步比對。
3. **Jabber ID(JID)**—如果記錄有一電話號碼，則 Jabber 依此作記錄上的對比。

當 Jabber 比對記錄並確定那些紀錄爲同一個人時將合併聯絡人的資料爲一項。

撥號計劃對映

您可以配置撥號計劃對映，以確保 Cisco Unified Communications Manager 上的撥號規則與目錄上的撥號規則相符。

應用程式撥號規則

應用程式撥號規則會自動在使用者撥打的電話號碼中新增或刪除數字。應用程式撥號規則處理使用者從用戶端撥號的號碼。

例如，撥號規則會在 7 位數電話號碼的前面自動加上數字 9，以提供外線的存取。

目錄查詢撥號規則

目錄尋找撥號規則將發話者識別號碼轉換爲用戶端可在目錄中查閱的號碼。目錄查詢規則根據最初的數字和號碼的長度指定要變換的號碼。

例如，您可以建立目錄查詢規則來從 10 位數電話中自動移除區碼及 2 位數首碼。 `4089023139` 轉換爲 `23139`爲這種規則的一個例子。

Cisco Unified Communications Manager UDS - Mobile and Remote Access

當 Cisco Jabber 使用 Expressway for Mobile and Remote Access 連線時，Cisco Unified Communication Manager UDS 爲所使用的聯絡人來源。如果在公司防火牆內部署 LDAP，我們建議使用您將 LDAP 目錄伺服器與 Cisco Unified Communications Manager 同步，以允許使用者在公司防火牆之外時用戶端與 UDS 連線。

雲端聯絡人來源

Cisco Webex 聯絡人來源

Cloud 部署中的聯絡人資料在Cisco Webex Messenger管理工具中或透過使用者更新配置。可以使用Cisco Webex Messenger管理工具匯入聯絡人資料。有關更多資訊，請參閱Cisco Webex Messenger管理指南中的使用者管理的區段。

聯絡人照片格式和尺寸

爲了使用Cisco Jabber達到最佳效果，您的聯絡人照片應具有特定的格式和尺寸。查看支援的格式和最佳尺寸。了解用戶端對照片進行的調整。

聯絡人照片格式

Cisco Jabber 支援以下目錄中聯絡人照片的格式：

- jpg
- PNG
- BMP

重要須知 Cisco Jabber 不會進行任何修改來增強 GIF 格式的聯絡人照片的呈現。因此，GIF 格式的聯絡人照片可能會不正確呈現或品質低於最佳品質。爲了獲得最佳品質，聯絡人照片請使用 PNG 格式。

聯絡人照片尺寸

提示 聯絡人照片的最佳尺寸爲 128 畫素 x 128 畫素，長寬比爲 1：1。

128 畫素 x 128 畫素爲 Microsoft Outlook 中本地聯絡人照片的最大允許尺寸。

下表列出了中聯絡人照片的不同尺寸Cisco Jabber。

位置	尺寸
音訊通話視窗	128 x 128 畫素
邀請和提醒，例如： • 來電視窗 • 會議提醒視窗	64 x 64 畫素
聯絡人名單，例如： • 聯絡人名單 • 參加者名冊 • 通話歷史記錄 • 語音信箱留言	32 畫素 x 32 畫素

聯絡人照片調整

Cisco Jabber 會如下調整聯絡人照片：

- 調整大小-如果目錄中的聯絡人照片小於或大於 128 畫素 x 128 畫素，則用戶端會自動調整照片的大小。例如，您目錄中的聯絡人照片爲 64 x 64 畫素。當 Cisco Jabber 從您的目錄擷取聯絡人照片時會將照片的大小調整爲 128 畫素 x 128 畫素。

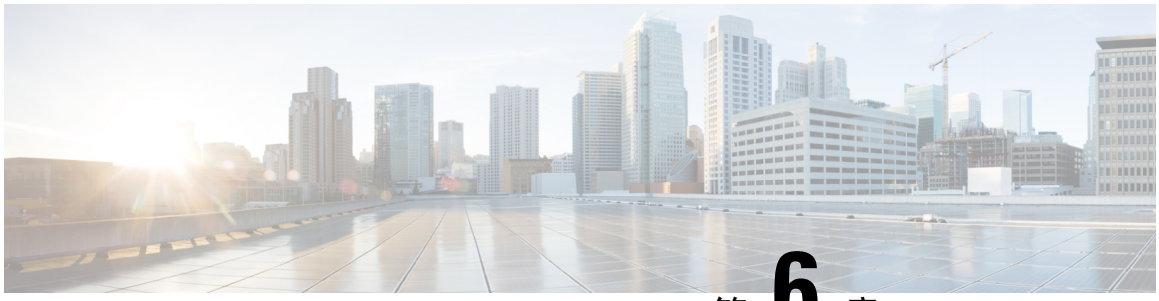
  提示 調整聯絡人照片的大小可能會導致較差的解析度，故請使用 128 畫素 x 128 畫素的聯絡人照片，以使用戶端不會自動調整它們的大小。

- 裁剪-Cisco Jabber 自動將非方形聯絡人照片裁剪爲方形長寬比，或者將寬高與高寬相同的長寬比爲 1：1。
- 縱向-如果目錄中的聯絡人照片具有縱向，則用戶端從頂部裁切 30%，從底部裁切 70%。

  例如，如果您目錄中的聯絡人照片的寬度爲 100 畫素，高度爲 200 畫素，則 Cisco Jabber 需要在高度上裁剪 100 畫素以實現 1：1 的長寬比。在這種情況下，用戶端從照片頂部裁剪 30 個畫素，從照片底部裁剪 70 個畫素。

- 橫向-如果目錄中的聯絡人照片具有橫向，則用戶端在兩側各裁切 50%。

  例如，如果您目錄中的聯絡人照片的寬度爲 200 畫素，高度爲 100 畫素，則 Cisco Jabber 需要在寬度上裁剪 100 畫素以實現 1：1 的長寬比。在這種情況下，用戶端從照片的右側裁剪 50 個畫素，從照片的左側裁剪 50 個畫素。



第 6 章

安全性及認證

加密

檔案傳輸和螢幕截圖的合規和原則管控

如果使用 Cisco Unified Communications Manager IM and Presence 10.5 (2)或更高版本上的“託管檔案傳輸”選項傳送檔案傳輸和螢幕截圖，則可以將檔案傳送到遵從性伺服器以進行審核和原則實施。

如需合規詳細資訊，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence Service* 的即時訊息合規。

有關配置檔案傳輸和螢幕截圖的更多資訊，請參閱《*Cisco Unified Communications Manager IM and Presence* 部署和安裝指南》。

即時訊息加密

Cisco Jabber使用傳輸層安全性(TLS)來保護用戶端和伺服器之間網路上的可擴展訊息傳遞和狀態協議(XMPP)通信。Cisco Jabber加密點對點即時訊息。

公司處所內加密

下表總結了公司處所內部署中即時訊息加密的詳細資訊。

連線	通訊協定	協商認證	預期之加密演算法
用戶端至伺服器	TLS v1.2 上的 XMPP	X.509 公鑰基礎結構認證	AES 256 位

伺服器和用戶端協商

以下伺服器使用 X.509 公鑰基礎結構(PKI)認證與 Cisco Jabber 協商 TLS 加密，並具有以下內容：

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

伺服器和用戶端協商 TLS 加密後，用戶端和伺服器皆將產生並交換會話密鑰以加密即時訊息傳遞流量。

下表列出了 Cisco Unified Communications Manager IM and Presence Service的 PKI 認證密鑰長度。

版本	金鑰長度
Cisco Unified Communications Manager IM and Presence Service 版本 9.0.1 或更高	2048 位

XMPP 加密

Cisco Unified Communications Manager IM and Presence Service使用 256 位長度的會話密鑰，這些密鑰用 AES 算法加密，以保護 Cisco Jabber 和在線狀態伺服器之間的即時訊息通信。

如果對伺服器節點之間的流量需求更高的安全性，則可以在 Cisco Unified Communications Manager IM and Presence Service上配置 XMPP 安全性設定。有關安全設定的更多資訊，請參見以下內容：

- Cisco Unified Communications Manager IM and Presence Service—*IM and Presence* 上的安全性配置

即時訊息記錄

您可以記錄和存檔即時訊息，以符合法規準則。要記錄即時訊息，您可以配置外部資料庫或與第三方合規性伺服器整合。Cisco Unified Communications Manager IM and Presence Service不加密您在外部資料庫或第三方合規性伺服器中登入的即時訊息。您必須適當地配置外部資料庫或第三方合規性伺服器，以保護您記錄的即時訊息。

有關合規性的更多資訊，請參見以下內容：

- Cisco Unified Communications Manager IM and Presence Service—*IM and Presence Service* 的即時訊息合規

有關加密級別和密碼算法(包括對稱密鑰算法(例如 AES)或公共密鑰算法(例如 RSA))的更多資訊，請在此連結https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html參閱下一代加密。

有關 X.509 公鑰基礎結構認證的更多資訊，請參閱此連結https://www.ietf.org/rfc/rfc2459.txt上的 網際網路 *X.509* 公鑰基礎結構認證和 *CRL* 配置檔文件。

雲端型加密

下表總結了在雲端型的部署中即時訊息加密的詳細資訊：

連線	通訊協定	協商認證	預期之加密演算法
用戶端至伺服器	TLS 中的 XMPP	X.509 公鑰基礎結構認證	AES 128 位
用戶端至用戶端	TLS 中的 XMPP	X.509 公鑰基礎結構認證	AES 256 位

伺服器和用戶端協商

以下伺服器與Cisco Webex Messenger服務使用 X.509 公鑰基礎結構(PKI)認證，與Cisco Jabber協商 TLS 加密 。

伺服器和用戶端協商 TLS 加密後，用戶端和伺服器皆將產生並交換會話密鑰以加密即時訊息傳遞流量。

XMPP 加密

Cisco Webex Messenger服務使用透過 AES 算法加密的 128 位會話密鑰來保護Cisco Jabber和Cisco Webex Messenger服務之間的即時訊息流量。

您可以選擇啓用 256 位用戶端到用戶端 AES 加密，以保護用戶端之間的流量。

即時訊息記錄

Cisco Webex Messenger服務可以記錄即時訊息，但不會以加密格式將即時訊息存檔。然而Cisco Webex Messenger服務使用嚴格的資料中心安全性(包括 SAE-16 和 ISO-27001 審核)來保護其所記錄的即時訊息。

Cisco Webex Messenger如果啓用 AES 256 位用戶端到用戶端加密，則服務無法記錄即時訊息。

有關加密級別和密碼算法(包括對稱密鑰算法(例如 AES)或公共密鑰算法(例如 RSA))的更多資訊，請在此連結https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html參閱下一代加密。

有關 X.509 公鑰基礎結構認證的更多資訊，請參閱此連結https://www.ietf.org/rfc/rfc2459.txt上的 網際網路 *X.509* 公鑰基礎結構認證和 *CRL* 配置檔文件。

用戶端至用戶端加密

預設情況下，用戶端與用戶端之間的即時訊息傳遞流量Cisco Webex Messenger服務爲安全的。您可以選擇在Cisco Webex管理工具指定原則以保護用戶端之間的即時訊息傳遞流量。

以下原則指定即時訊息的用戶端到用戶端加密：

- **支援即時訊息的 AES 編碼** -傳送用戶端使用 AES 256 位算法加密即時訊息。接收端用戶端解密即時訊息。
- **不支援即時訊息編碼** -用戶端可以與其他不支援加密的用戶端之間收發即時訊息。

下表描述了可以使用這些政策設定的不同組合。

政策組合	用戶端至用戶端加密	當遠端用戶端支援 **AES** 加密時	當遠端用戶端不支援 **AES** 加密時
支援即時訊息的 AES 編碼 = false **支援即時訊息的無編碼** = true	否	Cisco Jabber 傳送未加密的即時訊息。 Cisco Jabber 不協商密鑰交換。結果，其他用戶端不傳送Cisco Jabber加密的即時訊息。	Cisco Jabber 傳送和接收未加密的即時訊息。
支援即時訊息的 AES 編碼 = true **支援即時訊息的無編碼** = true	爲	Cisco Jabber 傳送和接收加密的即時訊息。 Cisco Jabber 顯示一個圖示，顯示即時訊息已加密。	Cisco Jabber 傳送未加密的即時訊息。 Cisco Jabber 接收未加密的即時訊息。
支援即時訊息的 AES 編碼 = true **支援即時訊息的無編碼** = true	爲	Cisco Jabber 傳送和接收加密的即時訊息。 Cisco Jabber 顯示一個圖示，顯示即時訊息已加密。	Cisco Jabber 不向遠端用戶端傳送或接收即時訊息。 Cisco Jabber 當使用者嘗試向遠端用戶端傳送即時訊息時，顯示錯誤訊息。

附註 Cisco Jabber不支援透過多人聊天的用戶端到用戶端的加密。Cisco Jabber僅對點對點聊天使用用戶端到用戶端加密。

有關加密和Cisco Webex原則，請參閱Cisco Webex文件中的關於加密級別。\

加密圖示

查看用戶端顯示的圖標以指示加密級別。

用戶端至伺服器加密的鎖定圖示

在公司處所內和雲端型的部署中，Cisco Jabber 皆會顯示以下圖示來指示用戶端至伺服器的加密：

用戶端至用戶端加密的鎖定圖示

在雲端型的部署中，Cisco Jabber 顯示以下圖標指示用戶端至用戶端的加密：

本地聊天記錄

在參與者關閉聊天視窗之後直到參與者登出之前，聊天記錄都會保留下來。如果您不想在參與者關閉聊天視窗後保留聊天記錄，請設定 Disable_IM_History 參數爲 true。該參數適用於除僅即時訊息使用者之外的所有用戶端。

Mac 版 Cisco Jabber 的公司處所內部署，如果在Mac 版 Cisco Jabber 的 **聊天偏好設定**視窗中選擇**將聊天檔案儲存到：**選項 ，聊天記錄儲存在本地的 Mac 檔案系統且可以使用 Spotlight 搜尋。

啓用公司處所內聊天歷史記錄時，Cisco Jabber 不會加密存檔的即時訊息。

對於桌面用戶端，您可以透過將存檔儲存到以下目錄來限制對聊天記錄的存取：

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

行動用戶端無法存取聊天記錄檔案。

語音和視訊加密

您可以選取爲所有裝置設定電話安全性功能。安全電話功能提供安全的 SIP 信令，安全的媒體串流和加密的裝置組態檔案。

如果爲使用者啓用安全電話功能，則與 Cisco Unified Communications Manager 的裝置連線爲安全的。但僅當兩個裝置皆有安全連線時，與其他裝置之間的通話始爲安全。

安全媒體的身份驗證方法

使用 SIP oAuth 可以在令牌型的身份驗證中啓用安全媒體。您可以爲 Jabber 的公司處所、雲端和混合部署的安全性驗證設定 SIP oAuth 而非 CAPF 註冊。

SIP 認證
在您的 Cisco Unified Communications Manager 設定上完成一次。它可以確保您的 SIP 通信(包括 RTP 媒體)爲安全的。

CAPF 註冊
啓用 CAPF 註冊的工作流程如下：

- 建立和配置 Jabber 裝置
- 驗證字串
- 配置電話安全性配置檔

PIE ASLR 支援

Android、iPhone 和 iPad 版 Cisco Jabber 支援位置不相關可執行位址空間佈局隨機化(PIE ASLR)。

聯邦資訊處理標準

聯邦資訊處理標準 (FIPS) 140-2：用於認可密碼編譯模組的美國和加拿大政府電腦安全標準。這些加密模組包括一組硬體，軟體和韌體，它們實現了批准的安全性功能，並包含在加密邊界內。

FIPS需求用戶端使用的所有加密，密鑰交換，數字簽署以及散列和隨機數產生功能都必須符合FIPS 140.2 對加密模組安全性的需求。

FIPS模式使用戶端可以更嚴格地管理認證。如果服務的認證過期且尚未重新輸入憑證，則處於FIPS模式的使用者可能會在用戶端中看到認證錯誤。使用者還可以在其 Hub 視窗中看到 FIPS 圖示，以指示用戶端正在 FIPS 模式下執行。

啟用 Windows 版 Cisco Jabber FIPS

Windows 版 Cisco Jabber 支援兩種啓用 FIPS 的方法：

- 已啓用作業系統-Windows 作業系統處於 FIPS 模式。
- Cisco Jabber 引導檔案設定-配置 FIPS_MODE 安裝程式開關。在未啓用 FIPS 的作業系統上，Cisco Jabber 可以處於 FIPS 模式。在這種情況下，僅有與非 Windows API 的連線處於 FIPS 模式。

表 8: Windows 版 Cisco Jabber FIPS 的設定

平台模式	引導檔案設定	Cisco Jabber 用戶端設定
已啓用 FIPS	已啓用 FIPS	FIPS 已啓用-引導檔案設定。
已啓用 FIPS	FIPS 已停用	FIPS 停用-引導檔案設定。
已啓用 FIPS	無任何設定	FIPS 已啓用-平台設定。
FIPS 已停用	已啓用 FIPS	FIPS 已啓用-引導檔案設定。
FIPS 已停用	FIPS 已停用	FIPS 停用-引導檔案設定。
FIPS 已停用	無任何設定	FIPS 已停用-平台設定。

附註 在 SSL 連線期間，Jabber 語音信箱服務僅接受 HTTP 請求的 TLS 版本 TLS 1.2 **https://164.62.224.15/vmrest/version 已啟用 FIPS** 。

啟用行動用戶端版 Cisco Jabber FIPS

要爲行動用戶端的 Cisco Jabber 啓用 FIPS，請在企業行動性管理(EMM)中將 FIPS_MODE 參數設定爲 TRUE。

重要須知

- 啓用FIPS將使得使用者無法接受不受信任的認證。在這種情況下，使用者可能無法使用某些服務。認證信任清單(CTL)或ITL檔案不適用於此處。伺服器的認證必須正確簽署，或者必須使用戶端透過側面載入來信任伺服器的認證。
- FIPS 強制執行 TLS1.2，因此停用了較舊的協議。
- 適用於行動用戶端的 Cisco Jabber 不支援平台模式。

通用標準

資訊技術安全評估通用標準爲一組用於評估IT產品安全屬性的國際標準所組成。您可以在符合通用標準認證需求的模式下執行 Cisco Jabber。必須爲每個用戶端啓用此模式以執行。

要在啓用了通用標準的環境中執行 Jabber，請執行以下操作：

- Windows 版 Jabber：將 CC_MODE 安裝參數設定爲 TRUE。
- Android 版 Jabber 和 iPhone 及 iPad 的 Jabber：在企業行動性管理(EMM)中將 CC_MODE 參數設定爲 TRUE。
- RSA 密鑰長度必須至少爲 2048 位。要配置 RSA 密鑰長度，請在 *Cisco Jabber 12.5* 的公司處、所內部署指南中閱讀有關如何建立和配置 *Cisco Jabber* 裝置。

有關如何設定Jabber以在通用標準模式下執行的更多資訊，請閱讀有關如何部署*Cisco Jabber*應用程式在裡面 *Cisco Jabber 12.5* 的公司處、所內部署指南。

安全 LDAP

安全 LDAP 通訊爲透過 SSL / TLS 的 LDAP

LDAPS 透過 SSL / TLS 連線啓動 LDAP 連線，開啓 SSL 會話，然後開始使用 LDAP 協定，會需要個別的通訊埠 636 或全球目錄通訊埠 3269。

經身份驗證的 UDS 聯絡人搜尋

在 Cisco Unified Communications Manager 中爲 UDS 聯絡人搜尋啓用身份驗證而 Cisco Jabber 提供憑證以與 UDS 進行身份驗證以進行聯絡人搜尋。

認證

認證驗證

認證驗證過程

作業系統Cisco Jabber對服務進行身份驗證時，在上執行可驗證伺服器認證。嘗試建立安全連線時，服務會呈現Cisco Jabber與認證。作業系統會根據用戶端裝置的公司處所內認證儲存區中的內容來驗證顯示的認證。如果認證不在認證儲存區中，則該認證被視爲不可信任而Cisco Jabber提示使用者接受或拒絕該認證。

如果使用者接受認證，Cisco Jabber連線至服務並將認證儲存在裝置的認證儲存區或鑰匙串中。如果使用者拒絕認證，Cisco Jabber無法連線至服務而認證不儲存到裝置的認證儲存區或鑰匙串中。

如果認證在裝置的公司處所內認證儲存中，Cisco Jabber將信任認證。Cisco Jabber將連線至服務而不會提示使用者接受或拒絕認證。

Cisco Jabber 可以根據組織中部署的內容對多種服務進行身份驗證。必須爲每個服務產生一個認證籤名請求(CSR)。某些公共認證頒發機構不接受每個完全合格的網域名(FQDN)有多於一個 CSR，這意味著可能需要將每個服務的 CSR 傳送到個別的公共認證頒發機構。

確保在服務配置檔案中爲每個服務指定 FQDN 而非 IP 位址或主機名。

已簽署的認證

該認證可以是自我簽署的，亦可以是受信任的根認證授權單位 (CA) 簽署的。

- CA 簽署的認證(推薦使用)-不提示使用者，因爲您本身在裝置上安裝認證的。CA 簽署的認證可以由私有 CA 或公共 CA 簽署。由公共 CA 簽署的許多認證都儲存在裝置的認證儲存區或鑰匙串中。使用 Android 7.0 或更高版本的裝置僅能識別 CA 簽署的認證。
- 自簽署認證-認證由提供認證的服務簽署，並且始終提示使用者接受或拒絕認證。

認證驗證選項

在設定認證驗證之前，您必須決定如何驗證認證：

- 您要部署的爲公司處所內部署還是雲端型部署的認證；
- 您使用何種方法簽署認證；
- 如果要部署 CA 簽署的認證，要使用的爲 公共 CA 還是私有 CA；
- 您需要爲哪些服務獲得認證；

公司處所內伺服器所需的認證

公司處所內伺服器提供以下認證，以與Cisco Jabber建立安全連線：

伺服器	憑證
Cisco Unified Communications Manager IM and Presence Service	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP(Tomcat)和CallManager認證(用於安全電話的安全 SIP 通話信令)
Cisco Unity Connection	HTTP (Tomcat)
Cisco Webex Meetings 伺服器	HTTP (Tomcat)
Cisco VCS Expressway Cisco Expressway-E	伺服器認證(用於HTTP，XMPP和SIP通話信令)

重要注意事項

- 安全聲明標記語言(SAML)單一登入(SSO)和身份提供者(IdP)需要 X.509 認證。
- 在開始認證簽署過程之前您應套用Cisco Unified Communications Manager IM and Presence Service最新的服務更新(SU)。
- 所需的認證適用於所有伺服器版本。
- 每個叢集節點，訂閱者和發佈者都執行一個Tomcat服務，且可以向用戶端提供 HTTP 認證。

  您應該計劃爲叢集中的每個節點簽署認證。
- 確保用戶端和用戶端之間的 SIP 信令安全Cisco Unified Communications Manager，則應使用認證頒發機構proxy功能(CAPF)註冊。

認證簽署請求格式及需求

公共認證頒發機構(CA)通常需求認證籤名請求(CSR)符合特定格式。例如，公共CA可能僅接受具有以下需求的 CSR：

- 爲 Base64 編碼的。
- 在**組織**、**OU** 或其他欄位中無包含某些字元，例如 `@&!` 等。
- 在伺服器的公鑰中使用特定的位長。

如果您從多個節點遞交 CSR，則公共 CA 可能要求所有 CSR 中的資訊皆爲一致。

若要防止CSR出現問題，您應檢閱計畫向其送出CSR的公共CA的格式需求。然後，您應確保在設定伺服器時輸入的資訊符合公共 CA 需要的格式。

每個 FQDN 一張認證——一些公共 CA 在每個完全限定的網域名(FQDN)中僅簽署一個認證。

例如，爲簽署單個Cisco Unified Communications Manager IM and Presence Service節點 HTTP 和 XMPP 認證，您可能需要將每個 CSR 遞交到不同的公共 CA。

吊銷伺服器

如果無法使用吊銷伺服器，則 Cisco Jabber 無法連線至 Cisco Unified Communications Manager 伺服器。另外，如果認證頒發機構(CA)吊銷認證，則 Cisco Jabber 不允許使用者連線至該伺服器。

不會向使用者通知以下結果：

- 認證不包含吊銷資訊。
- 無法連線 NTP 伺服器

要驗證認證，認證中必須包含 HTTP URL。**CDP** 或**AIA**可提供吊銷資訊的可連線伺服器的欄位。

爲確保在獲得由 CA 頒發的認證時對您的認證有進行驗證，您必須滿足以下需求之一：

- 確保 **CRL 分發點**(CDP)欄位包含指向吊銷伺服器上的認證吊銷清單(CRL)的 HTTP URL。
- 確保**授權資訊存取**(AIA)欄位包含在線認證狀態協議(OCSP)伺服器的 HTTP URL。

認證中的伺服器身份

作爲簽署過程的一部分，CA 在認證中指定伺服器身份。當用戶端驗證該認證時，它將檢查以下內容：

- 受信任的機構已頒發認證。
- 提供認證的伺服器的身份與認證中指定的伺服器的身份相符。

附註 公共 CA 通常需求使用完全限定的網域名(FQDN)作爲伺服器身份而非 IP 位址。

標識符欄位

用戶端檢查伺服器認證中的以下標識符欄位爲否存在身份相符：

- XMPP 認證
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - 主題 `CN`
- HTTP 認證
  - `SubjectAltName\dnsNames`
  - 主題 `CN`

提示 主題 CN 欄位可以包含通配符(*)作爲最左邊的字元，例如， *.cisco.com。

防止身份不相符

如果使用者嘗試使用IP位址或主機名連線至伺服器，且伺服器認證使用FQDN標識伺服器，則用戶端無法將伺服器標識爲受信任並將提示使用者。

如果伺服器認證使用 FQDN 標識伺服器，則應計劃在伺服器上的許多位置將每個伺服器名稱指定爲FQDN。有關更多資訊，請參閱對技術說明進行故障排除的防止身份不相符區段。

多伺服器 SAN 的認證

如果您使用多伺服器SAN，則每個tomcat認證的叢集及每個XMPP認證的叢集僅需上載一次認證即可。如果不使用多伺服器 SAN，則必須將認證上載到每個 Cisco Unified Communications Manager 節點的服務。

雲端部署的認證驗證

Cisco Webex Messenger和Cisco Webex Meetings Center 預設向用戶端提供以下認證：

- CAS
- WAPI

附註 Cisco Webex 認證由信任的認證頒發機構 (CA) 簽署。Cisco Jabber 會驗證這些認證，以與雲端型的服務建立安全連線。

Cisco Jabber驗證從Cisco Webex Messenger接收的以下 XMPP 認證。如果這些認證未包含在您的作業系統中，則必須提供。

- VeriSign 3 類公共主要認證頒發機構-G5-此認證儲存在“受信任的根認證頒發機構”中
- VeriSign 3 類安全伺服器 CA-G3-此認證可驗證Webex Messenger伺服器身份並儲存在中間認證頒發機構中。
- AddTrust 外部 CA 根
- GoDaddy 2 類認證頒發機構根認證

有關適用於Windows版Cisco Jabber的根認證的更多資訊，請參閱https://www.identrust.co.uk/certificates/trustid/install-nes36.html。

有關Mac 版 Cisco Jabber 的根認證的更多資訊，請參閱https://support.apple.com。

多租戶託管協作解決方案的伺服器名稱指示支援

Cisco Jabber 透過多租戶託管協作解決方案在 Mobile and Remote Access(MRA)部署中支援伺服器名稱指示(SNI)。

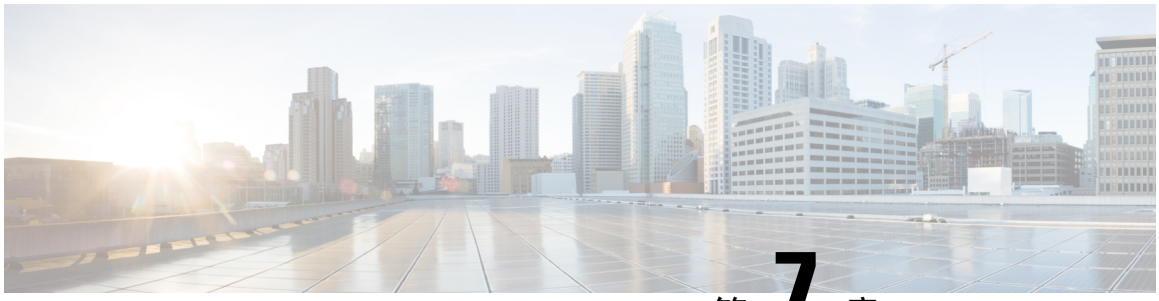
Cisco Jabber 使用 SNI 將網域資訊傳送到 Expressway。Expressway 尋找認證儲存以尋找包含網域資訊的認證，並將認證返還至 Cisco Jabber 進行驗證。

有關多租戶部署的更多資訊，請參閱Cisco Hosted Collaboration Solution，版本 11.5《多租戶 Expressway 配置指南》中的具網域認證的端點服務的 *Service Discovery*和無網域認證的 *Jabber Service Discovery* 段落。

防毒排除

若您部署防毒軟體，則在防毒排除清單中納入下列資料夾位置：

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



第 7 章

組態管理

快速登入

此功能讓Cisco Jabber現在能夠同時登入所有服務，而非稍早使用的依序登入程序，每項服務獨立連線至各自的伺服器並根據快取資料對您進行授權。這可讓您快速且動態地完成登入程序。但此功能僅有在您第二次登入 Jabber 時才會開始生效。

您可以透過在所有用戶端使用 STARTUP_AUTHENTICATION_REQUIRED 參數來設定快速登入功能，但行動用戶端方面您必須同時配置 STARTUP_AUTHENTICATION_REQUIRED 和 CachePasswordMobile 參數。如需有關設定此功能的詳細資訊，請參閱 *Cisco Jabber* 適用的參數參考指南。

配置重新獲取 -快速登入不會在每次登入或登出時同步地擷取伺服器端的設定。與以前的Jabber版本一樣，這僅會在首次登入期間發生。

對於後續的登入，系統會在例如登入後的 1 到 5 分鐘內、登入後的 7 到 9 個小時內或貴司使用者進行手動重新整理以獲取新的組態時，傳送請求以從伺服器獲取新的組態。

您可以配置 ConfigRefetchInterval 參數以每隔 7 或 8 小時從伺服器獲取一次組態。如需有關設定這些參數的詳細資訊，請參閱 *Cisco Jabber* 版本或更新適用的參數參考指南 。

動態配置更改操作

在 Jabber 11.9 中，組件和服務會動態響應組態更改。您會收到以下提示，提示您在以下的情況下登出或重設Jabber：

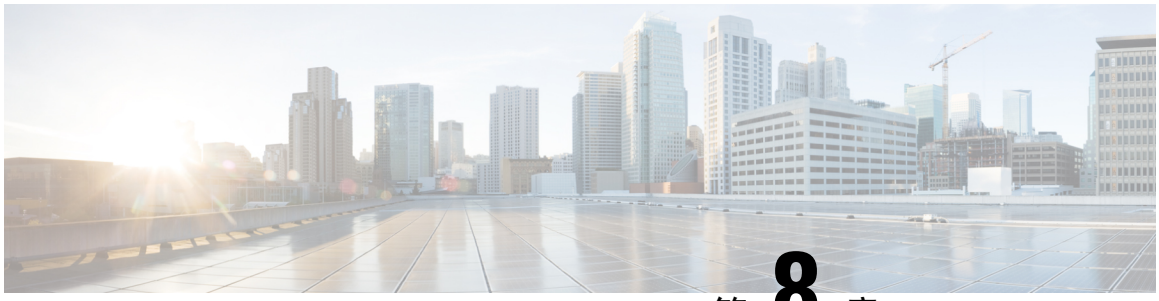
重設 Jabber—如果更改了主要服務，您將收到一條提示訊息，提示您重設 Jabber。例如，如果 IM & Presence 和電話技術帳號更改爲僅電話帳號，則 Jabber 將需要重設。

登出 Jabber —如果下表中列出的組態密鑰有任何更改，Jabber 將提示使用者登出並再登入以使用新組態。

- **Windows**—您將收到有關組態已更改的彈出通知。您可以忽略該通知，亦可以登出並登入以使用新組態。

- **行動用戶端**—Jabber 自動登出。然後您會收到一個彈出通知，指出組態已更改。請點選**確定**以接受組態的更改以自動登入 Jabber。

按鍵名稱	平台	登出
RemoteAccess	所有用戶端	登出
Meetings_Enabled	所有用戶端	登出
DirectoryServerType	所有用戶端	登出
DirectoryUri	所有用戶端	登出
UseSipUriToResolveContacts	所有用戶端	登出
SipUri	所有用戶端	登出
UriPrefix	所有用戶端	登出
DirectoryUriPrefix	所有用戶端	登出
SwapDisplayNameOrder	所有用戶端	登出
PresenceDomain	所有用戶端	登出
Support_SSL_Encoding	所有用戶端	登出
Support_No_Encoding	所有用戶端	登出
IM_Logging_Enabled	所有用戶端	登出
IGS_CUP_ENABLESECURE	所有用戶端	登出
DISALLOW_FILE_TRANSFER_ON_MOBILE	所有用戶端	登出
Persistent_Chat_Enabled	桌面用戶端	登出
Persistent_Chat_Mobile_Enabled	行動用戶端	登出
Disable_MultiDevice_Message	所有用戶端	登出
Location_Enabled / Location_Matching_Mode	所有用戶端	登出
IP_MODE	所有用戶端	登出
Telephony_Enabled	所有用戶端	登出
Voicemail_Enabled	所有用戶端	登出
EnableLoadAddressBook	行動用戶端	登出
ShowRecentsTab	僅 Windows 版 Jabber	登出
IM_Enabled	所有用戶端	登出
Disallow-jaibreak-device	行動用戶端	登出
EnableChats	僅 Windows 版 Jabber	登出



第 8 章

螢幕共用

螢幕共用

螢幕共用有四種類型：

- Cisco Webex Share
- BFCP 共用
- 僅即時訊息共用
- 升級爲會議並共用

Cisco Webex 螢幕共用

適用於雲端部屬中桌面用戶端 Cisco Jabber。

雲端部署中，如果“BFCP”和“僅即時訊息”螢幕共用選項不可用，則選擇聯絡人後會自動選擇 Cisco Webex“螢幕共用”。

您可以使用以下方法之一開始Cisco Webex螢幕共用：

- 右鍵點選 Hub 視窗中的聯絡人，然後在功能表選項中選擇**分享畫面...**。
- 在 Hub 視窗中選擇一個聯絡人，然後點選**設定值**功能表。選擇**通訊**然後在功能表選項中選擇**分享畫面...**。
- 如果“BFCP”和“僅即時訊息”螢幕共用選項不可用，則在對話視窗中選擇**在功能表選項中選擇...** > **分享畫面**。

BFCP 螢幕共用

適用於 Cisco Jabber 的桌面用戶端，行動用戶端的 Cisco Jabber 僅能接收 BFCP 螢幕共用。

二進制發言權控制協議(BFCP)螢幕共用由 Cisco Unified Communications Manager 控制。使用視訊桌面共用功能時，Cisco Unified Communications Manager 處理使用者傳輸的 BFCP 資料包。通話時選擇 **...** > **分享畫面**啓動 BFCP 螢幕共用。

此功能不支援遠端螢幕控制。

如果在軟體電話裝置上啓用**可信任中繼點**或**媒體終止點**則不支援使用 BFCP 的視訊桌面共用。

附註 在 Windows 版 Jabber 中，**螢幕分享**按鈕預設會啓動 BFCP 螢幕共用。如果基於 BFCP 的共用不可用，則該按鈕將啓動僅即時訊息的螢幕共用。

僅即時訊息螢幕共用

適用於 Windows 版 Cisco Jabber。

僅即時訊息的螢幕共用爲使用 RDP 的一對一螢幕共用。 EnableP2PDesktopShare 參數控制僅即時訊息的螢幕共用是否可用。PreferP2PDesktopShare參數控制 Jabber 爲偏好視訊共用或僅即時訊息的螢幕共用。

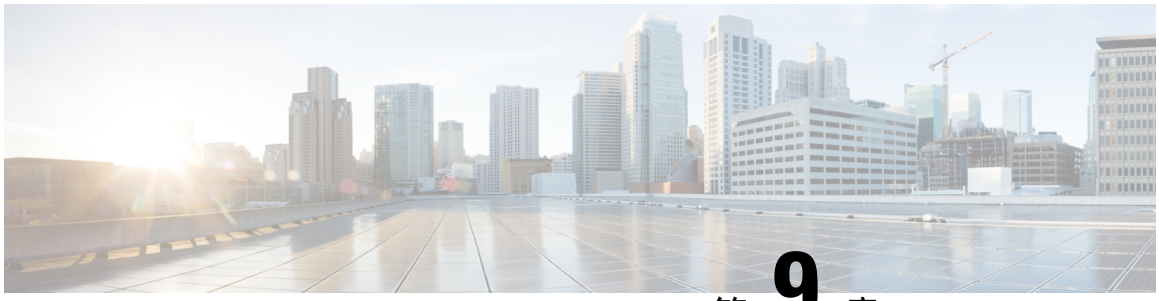
如果您的部署允許僅即時訊息的螢幕共用，請選擇 **在聊天視窗中...** > **分享畫面**開始螢幕共用。

預設情況下，RDP 要求通訊埠 3389 爲開啓。對於僅即時訊息的螢幕共用，Jabber的預設通訊埠範圍爲 49152 – 65535。您可以使用 SharePortRangeStart 和 SharePortRangeSize 參數以限制通訊埠範圍。

升級為會議並共用

適用於所有用戶端的 Cisco Jabber。

您可以升級至即時的Cisco Webex Meetings並使用Cisco Webex Meetings控制共用螢幕。



第 9 章

聯合

網域間聯合

網域間聯合使企業網域中的Cisco Jabber使用者可以共用在線狀態並與另一個網域中的使用者傳送即時訊息。

- Cisco Jabber 使用者必須手動輸入來自另一個網域的聯絡人。
- Cisco Jabber 透過以下方式支援聯合：
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP 標準化環境如 Google Talk 等

  附註 Expressway for Mobile and Remote Access 本身並不會啓用 XMPP 網域間聯合。如果已在 Cisco Unified Communications Manager IM and Presence 中啓用了 XMPP 網域間聯合，則透過 Expressway for Mobile and Remote Access 連線的 Cisco Jabber 用戶端可以使用 XMPP 網域間聯合。
  - AOL Instant Messenger

在 Cisco Unified Communications Manager IM and Presence Service 配置 Cisco Jabber 的網域間聯合。有關更多資訊，請參見適當的伺服器說明文件。

網域內聯合

網域內聯合使同一個網域內的使用者可以共用線上狀態並在 Cisco Unified Communications Manager IM and Presence Service與 Microsoft Office Communications Server、Microsoft Live Communications Server 或其他在線狀態伺服器之間傳送即時訊息。

網域內聯合允許您將使用者從其他在線狀態伺服器遷移到 Cisco Unified Communications Manager IM and Presence Service。因此，您需要在在線狀態伺服器上爲 Cisco Jabber 配置網域內聯合。如需更多資訊，請參閱：

- Cisco Unified Communications Manager IM and Presence Service: *Cisco Unified Communications Manager IM and Presence Service* 用於已分區網域內聯合

附錄 A

Jabber 所支援的語言

支援的語言

下表列出了以下語言的區域設定標識符(LCID)或語言標識符(LangID)：Cisco Jabber用戶端的支援。

支援的語言	Windows 版 Cisco Jabber	Mac 版 Cisco Jabber	iPad 及 iPhone 版 Cisco Jabber 、Android 版 Cisco Jabber。	LCID /語言 ID
阿拉伯文 (沙烏地阿拉伯)	X		X	1025
保加利亞語-保加利亞	X	X		1026
加泰羅尼亞語-西班牙	X	X		1027
中文(簡體)- 中國	X	X	X	2052
中文(繁體)- 台灣	X	X	X	1028
克羅埃西亞語-克羅埃西亞	X	X	X	1050
捷克語 - 捷克共和國	X	X		1029
丹麥文 - 丹麥	X	X	X	1030
荷蘭文 - 荷蘭	X	X	X	1043
英文 - 美國	X	X	X	1028

Jabber 所支援的語言

支援的語言	Windows 版 Cisco Jabber	Mac 版 Cisco Jabber	iPad 及 iPhone 版 Cisco Jabber、Android 版 Cisco Jabber。	LCID /語言 ID
芬蘭文 - 芬蘭	X	X		1035
法文 - 法國	X	X	X	1036
德文 - 德國	X	X	X	1031
希臘文 - 希臘	X	X		1032
希伯來語-以色列	X			1037
匈牙利文-匈牙利	X	X	X	1038
義大利文 - 義大利	X	X	X	1040
日文 - 日本	X	X	X	1041
韓文-韓國	X	X	X	1042
挪威文-挪威	X	X		2068
波蘭文- 波蘭	X	X		1045
葡萄牙文-巴西	X	X	X	1046
葡萄牙語 - 葡萄牙	X	X		2070
羅馬尼亞文 - 羅馬尼亞	X	X	X	1048
俄文 - 俄羅斯	X	X	X	1049
塞爾維亞文	X	X		1050
斯洛伐克文-斯洛伐克文	X	X	X	1051
斯洛維尼亞語-斯洛維尼亞	X	X		1060
西班牙語-西班牙(現代式)	X	X	X	3082
瑞典文 - 瑞典	X	X	X	5149
泰文 - 泰國	X	X		1054
土耳其文	X	X	X	1055