安全和证书

加密

文件传输和屏幕捕获的合规性和策略控制

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

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

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

即时消息加密

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

内部加密

下表概述了内部部署中即时消息加密的详细信息。

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

服务器与客户端协商

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

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

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

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

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

XMPP 加密

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

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

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

即时消息记录

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

有关合规性的详细信息，请参阅以下内容：

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

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

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

基于云加密

下表概述了基于云部署中即时消息加密的详细信息：

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

服务器与客户端协商

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

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

XMPP 加密

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

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

即时消息记录

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

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

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

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

客户端至客户端加密

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

以下策略可指定即时消息的客户端对客户端加密：

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

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

下表说明您可以使用这些策略设置的不同组合：

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

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

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

加密图标

查看客户端显示以指示加密级别的图标。

客户端到服务器加密的锁定图标

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

客户端至客户端加密的锁定图标

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

本地聊天历史记录

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

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

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

对于桌面客户端，可以通过将存档保存到以下目录来限制对聊天历史的访问：

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

对于移动客户端，无法访问聊天历史文件。

语音和视频加密

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

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

安全媒体的验证方法

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

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

CAPF 注册
启用 CAPF 注册的工作流程如下：

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

PIE ASLR 支持

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

联邦信息处理标准

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

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

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

为 Cisco Jabber Windows 版本启用 FIPS

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

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

表 *1:* 适用于 *FIPS* 的 *Cisco Jabber Windows* 版本设置

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

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

已针对用于移动客户端的 Cisco Jabber 启用 FIPS

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

重要事项

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

通用标准

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

要在通过 Common Criteria 启用的环境中运行 Jabber：

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

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

安全 LDAP

安全 LDAP 通信是 LDAP over SSL/TLS

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

已验证的 UDS 联系人搜索

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

证书

证书验证

证书验证过程

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

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

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

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

确保在服务配置文件中为每项服务指定 FQDN，而不是 IP 地址或主机名。

已签名证书

证书可由证书颁发机构 (CA) 签名，也可自签。

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

证书验证选项

在设置证书验证之前，必须确定您希望验证证书的方式：

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

- 您需要为其获取证书的服务。

内部服务器所需证书

内部服务器提供以下证书以与 Cisco Jabber 建立安全连接：

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

重要说明

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

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

证书签名请求格式和要求

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

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

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

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

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

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

吊销服务器

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

系统不会通知用户以下结果：

- 证书不包含吊销信息。
- 无法访问吊销服务器。

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

为确保您在获得 CA 颁发的证书时验证您的证书，您必须满足以下要求之一：

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

证书中的服务器身份

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

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

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

标识符字段

客户端在服务器证书中检查标识匹配的以下标识符字段：

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

- HTTP 证书
  - SubjectAltName\dnsNames
  - Subject CN

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

防止标识不匹配

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

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

多服务器 SAN 证书

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

云部署的证书验证

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

- CAS
- WAPI

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

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

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

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

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

多租户托管协作解决方案的服务器名称指示支持

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

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

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

防病毒排除

如果您部署了防病毒软件，请在防病毒排除列表中包含以下文件夹位置：

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