



设置证书验证

- [云部署的证书验证](#)，第 1 页

云部署的证书验证

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

- CAS
- WAPI



注释

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

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

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

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

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

更新配置文件照片 URL

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

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

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



重要事项

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

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

过程

- 步骤 1** 使用Cisco Webex管理工具导出CSV文件格式的用户联系人数据。
- 步骤 2** 在 `userProfilePhotoURL` 字段中，将IP地址替换为Cisco Webex域。
- 步骤 3** 保存CSV文件。
- 步骤 4** 使用Cisco Webex管理工具导入CSV文件。