証明書検証に関する Jabber の完全な手引きガイド

目次

概要

このドキュメントは、複数のシスコ リソースを Cisco Jabber で証明書を検証するためのすべての要件を満たすために使用される統合された完全な操作ガイドにまとめたものです。 これが必要となるのは、サーバとのセキュアな接続を確立するために Cisco Jabber で証明書検証を使用する必要があるためです。 この要件は、ユーザ環境に必要となる場合がある多くの変更を伴います。

> **注:** このガイドは、オンプレミス展開専用です。 現在、クラウド サービス展開がパブリック証明書認証局（CA）で照合されるため、それらの展開に必要な変更はありません。

この変更によって Jabber クライアントが受ける影響

証明書検証を実行するすべてのクライアントを次の表に示します。

表 1

デスクトップ クライアント	モバイル クライアントとタブレット クライア
Jabber for Macintosh バージョン 9.2（2013 年 9 月）	Jabber for iPhone バージョン 9.5（2013 年 1 ）

Jabber for Microsoft (MS) Windows バージョン 9.2.5（2013 年 9 月）	Jabber for iPhone and iPad バージョン 9.6（ 年 11 月） Jabber for Android バージョン 9.6（2013 年 ）

これは Jabber 環境にどういう意味を持つか?

表 1 に記載されているクライアントのインストールまたはアップグレード時に、セキュアな接続にサーバでの必須の証明書検証が使用されます。 基本的に、Jabber クライアントがセキュアな接続を使用しようとすると、サーバは Cisco Jabber に証明書を提示します。 その後、Cisco Jabber は、デバイスの証明書ストアでそれらの証明書の照合を試みます。 クライアントが証明書を検証できない場合、証明書を受け入れて企業の信頼ストアに保存するかを確認するよう求められます。

どの証明書が必要であるか?

オンプレミス サーバと、セキュアな接続を確立するために Cisco Jabber に提示する証明書の一覧を次に示します。

表 2

サーバ	証明書
Cisco Unified Presence	HTTP（Tomcat） XMPP
Cisco Unified Communications Manager IM and Presence	HTTP（Tomcat） XMPP
Cisco Unified Communications Manager	HTTP（Tomcat）
Cisco Unity Connection	HTTP（Tomcat）
Cisco WebEx Meetings Server	HTTP（Tomcat）

以下に注意すべき事項を一部紹介します。

- 証明書署名プロセスを開始する前に、Cisco Unified Presence（CUP）または Cisco Unified Communications Manager（CUCM）IM and Presence に対して最新のサービス更新（SU）を適用します。
- 必要な証明書は、すべてのサーバ バージョンに適用されます。 たとえば、CUP バージョン 8.x および CUCM IM and Presence バージョン 9.x 以降は、Extensible Messaging and Presence Protocol（XMPP）および HTTP の証明書をクライアントに提示します。
- クラスタ、サブスクライバおよびパブリッシャの各ノードは、Tomcat サービスを実行し、HTTP の証明書でクライアントを提示できます。 クラスタ内の各ノードの証明書に署名します。
- クライアントと CUCM 間のセッションの開始プロトコル（SIP）シグナリングセキュアにするには、Certification Authority Proxy Function（CAPF）登録を使用します。

証明書検証に使用できる方法

現在、証明書検証にいくつかの方法を使用できます。

方法 1： すべての証明書のポップアップに対して [Accept] をクリックします。 小規模環境においては、この方法が最も理想的なソリューションであると考えられます。 [Accept] をクリックすると、デバイスの企業の信頼ストアに証明書が保存されます。 証明書が企業の信頼ストアに保存された後は、そのローカル デバイスで Jabber クライアントにログインする際に証明書を要求されることがなくなります。

方法 2： 必要な証明書（**表 2**）を個々のサーバからダウンロードし（デフォルトでは、自己署名証明書）、ユーザ デバイスの企業の信頼ストアにインストールします。 証明書署名でプライベート CA あるいはパブリック CA へのアクセス権がない環境おいては、この方法が最も理想的なソリューションであると考えられます。

これらの証明書をユーザにプッシュする方法はいくつかありますが、簡単な方法の 1 つとして、Microsoft Windows レジストリを使用する方法があります。

1. 1 台のマシンから、Jabber に提示されるすべての証明書を企業信頼ストアに受け入れます。
2. 証明書が存在することを確認するには、**Certmgr.msc コマンド**を入力し、[EnterpriseTrust] > [Certificates] に移動します。
3. **run** コマンドを使用して **regedit** を開き、[HKCU] > [Software] > [Microsoft] > [SystemCertificates] > [trust] > [Certificates] に移動します。
4. 右クリックし、レジストリの Certificates フォルダを **.reg** ファイルとしてエクスポートします。
5. グループ ポリシー オブジェクト（GPO）（またはその他の適切な方法で）を使用してこのファイルをすべてのユーザにプッシュします。

これで、Jabber 向けの Enterprise Trust Certificate のインストールが完了し、これ以降はユーザに対してプロンプトは表示されなくなります。

方法 3： パブリック CA またはプライベート CA（**表 2**）が必要なすべての証明書に署名します。シスコは、この方法を推奨します。 この方法では、証明書署名要求（CSR）が証明書ごとに生成され、署名され、さらにサーバに再アップロードされ、ユーザ デバイスの Trusted Root Certificate Authorities ストアにインポートされている必要があります。 詳細については、このドキュメントの「**CSR の生成**」と「**証明書をユーザ デバイスの証明書ストアにインポートする方法** 」のセクションを参照してください。

> **注:** パブリック CA の場合、ルート証明書がクライアントの信頼ストアに存在している必要があります。

特定の形式に準拠するように、パブリック CA には通常、CSR が必要であることに留意しておくことが重要です。 たとえば、パブリック CA は、次のような CSR を受け入れる場合があります。

- Base 64 エンコードである
- @&! などの文字を [Organization] や [Organizational Unit (OU)] などのフィールドに含めない。
- サーバの公開キーで特定のビット長を使用する。

同様に、複数ノードから CSR を送信すると、パブリック CA は、すべての CSR で情報の整合性がとれていることを必要とする場合があります。

CSR の問題を回避するために、CSR を送信するパブリック CA からの形式の要件を確認します。 次に、サーバを構成する際に、入力する情報がパブリック CA が要求する形式に適合していることを保証します。

発生する可能性がある要件を次に示します。

FQDN ごとに 1 つの証明書: いくつかのパブリック CA は完全修飾ドメイン名（FQDN）ごとに 1 つの証明書にのみ署名します。

たとえば、単一の CUCM IM and Presence ノードの HTTP 証明書と XMPP 証明書に署名するには、それぞれの CSR を別々のパブリック CA に送信する必要があります。

証明書が自己署名または CA 署名付きであるかどうかの確認

> **注:** この例は、CUCM バージョン 8.x 向けです。 プロセスは、サーバによって異なる場合があります。

1. Cisco Unified OS Administration に移動します。
2. [Security] > [Certificate Management] を選択します。
3. Tomcat-Trust Certificate .pem ファイルを見つけてクリックします。
4. [Download]、[Save] の順にクリックします。
5. そのファイルに移動し、.cer 拡張子を付けてその名前を変更します。
6. このファイルを開いて表示します（MS Windows のユーザ）。
7. [Issued by] フィールドを確認します。 これが [Issued to] フィールドに一致する場合、証明書は自己署名です（例を参照）。

例： 自己署名とプライベート CA 署名付き証明書

自己署名プライベート CA 署名付き

CSR の生成

> **注:** この例は、CUCM バージョン 8.x 向けです。 プロセスは、サーバによって異なる場合があります。

1. Cisco Unified OS Administration に移動します。
2. [Security] > [Certificate Management] を選択します。
3. [Generate CSR] をクリックし、ドロップダウン リストから [Tomcat] を選択します。
4. [Generate CSR] をクリックし、[Close] をクリックします。
5. [Download CSR] をクリックし、ドロップダウン リストから [Tomcat] を選択します。
6. [Download CSR] をクリックし、ファイルを保存します。
7. プライベート CA サーバまたはパブリック CA によって署名される .csr ファイルを送信します。
   注: この CSR ファイルの作成後、プロセスは環境によって異なります。
8. サーバに発行された新しい署名付き証明書を再アップロードするには、[Security] > [Certificate Management] の順に選択し、Upload Certificate/Certificate Chain] をクリックします。

証明書をユーザ デバイスの証明書ストアにインポートする方法

どのサーバ証明書でも、ユーザ デバイスの信頼ストアで、関連するルート証明書を提示しておくようにします。 Cisco Jabber は、サーバが信頼ストアのルート証明書に対して提示する証明書を検証します。

MS Windows ce rtificate ストアへのインポート ルート証明:

- プライベート CA などの信頼ストアにない証明書が CA によって署名される場合。その場合は、プライベート CA 証明書を Trusted Root Certification Authorities ストアにインポートする必要があります。
- 証明書には自己署名します。 その場合は、自己署名証明書を企業の信頼ストアにインポートする必要があります。

MS Windows ce rtificate ストアに適切なメソッド輸入 証明書を、使用できます (以下を参照) :

- 個別に証明書をインポートするために、[Certificate Import Wizard] を使用します。
- MS Windows Server で CertMgr.exe コマンドライン ツールを使用してユーザに証明書を展開します （ このオプションでは、MS 管理コンソールの CertMgr.msc ではなく、Certificate Manager ツールの CertMgr.exe を使用する必要があります ）。
- Microsoft Windows Server で GPO を使用してユーザに証明書をデプロイします。

注: 証明書のインポートに関する詳細については、適切な MS のドキュメントを参照してください。

証明書のサーバ識別情報

署名プロセスの一部として、CA は証明書のサーバ識別情報を指定します。 クライアントがその証明書を検証する場合、次のことを確認します。

- 信頼できる機関が証明書を発行している。
- 証明書を提示するサーバの識別情報は、証明書に明記されたサーバの識別情報と一致します。

注: パブリック CA は、通常、サーバの識別情報として、IP アドレスではなく、FQDN を必要とします。

ID フィールド

クライアントは、ID の一致に関して、サーバ証明書の次の ID フィールドを確認します。

XMPP 証明書

- SubjectAltName\OtherName\xmppAddr
- SubjectAltName\OtherName\srvName
- SubjectAltName\dnsNames
- Subject CN

HTTP 証明書

- SubjectAltName\dnsNames
- Subject CN

注: [Subject CN] フィールドには、左端の文字（たとえば、*.cisco.com）としてワイルドカード（*）を含めることができます。 CUCM、CUP、および Cisco Unity Connection サーバでは、ワイルドカードの証明書をサポートしていない場合があります（改善 Cisco Bug ID CSCta14114 を参照）。

ID の不一致の防止

Jabber クライアントが IP アドレスでサーバに接続し、サーバ証明書が FQDN でサーバを識別しようとすると、クライアントは信頼できるサーバを識別できないため、ユーザに指定するよう要求されます。 したがって、サーバ証明書が FQDN でサーバを識別する場合、サーバの多くの場所の FQDN としてサーバ名を指定します。

表 3 は、IP アドレスまたは FQDN であるかどうかにかかわらず、証明書に表示されるサーバ名を指定する必要があるすべての場所を示します。

表 3

server	**場所（設定は証明書と一致する必要があります）**
Cisco Jabber クライアント	ログイン サーバ アドレス（クライアントによって異なり、通常は [Settings] の下にある）
	**すべてのノード名（[System] > [Cluster Topology]）
	*?注意: これを FQDN に変更した場合、DNS を介してこれを解決でバが起動状態であることを確認してください。
	TFTP サーバ（[Application] > [Cisco] > [Jabber] > [Settings]）
CUP（バージョン 8.x 以前）	プライマリとセカンダリの Cisco Call Manager Cisco IP Phone（CCMCIP）（[Application] > [Cisco Jabber] > [CCMCIP Prof
	ボイスメールのホスト名（[Application] > [Cisco Jabber] > [Voicema
	メールストア名（[Application] > [Cisco] > [Jabber] > [Mailstore]）
	会議のホスト名（[Application] > [Cisco Jabber] > [Conferencing Server]）（Meeting Place 専用）
	XMPP ドメイン（「**クライアントへの XMPP ドメインの提供**」セク）
	**すべてのノード名（[System] > [Cluster Topology]）
	*?注意: これを FQDN に変更した場合、DNS を介してこれを解決でバが起動状態であることを確認してください。
CUCM IM and Presence（バージョン 9.x 以降）	TFTP サーバ（[Application] > [Legacy Clients] > [Settings]）
	プライマリとセカンダリの CCMCIP（[Application] > [Legacy Client Profile]）
	XMPP ドメイン（「**クライアントへの XMPP ドメインの提供**」セク）
CUCM（バージョン8.x 以前）	サーバ名（[System] > [Server]）
	サーバ名（[System] > [Server]）
CUCM（バージョン 9.x 以降）	IM and Presence Server サーバ（[User Management] > [User Setting Service] > [IM and Presence]）
	ボイスメールのホスト名（[User Management] > [User Settings] > [Voicemail]）
	メールストア名（[User Management] > [User Settings] > [UC Servic [Mailstore]）

Cisco Unity Connection（すべてのバージョン）	会議のホスト名（[User Management] > [User Settings] > [UC Servic [Conferencing]）（Meeting Place のみ） **変更不要**

クライアントへの XMPP ドメインの提供

クライアントは、FQDN ではなく XMPP ドメインを使用して、XMPP 証明書を識別します。 XMPP の証明書は ID フィールドに XMPP ドメインを含める必要があります。

クライアントがプレゼンス サーバに接続しようとすると、プレゼンス サーバはクライアントに XMPP ドメインを提供します。 その際に、クライアントは XMPP 証明書に対するプレゼンス サーバの識別情報を検証します。

プレゼンス サーバがクライアントに XMPP のドメインを提供することを確認するには、次の手順を実行します。

1. プレゼンス サーバの管理インターフェイス（[Cisco Unified CM IM and Presence Administration] インターフェイスまたは [Cisco Unified Presence Administration] インターフェイス）を開きます。
2. [System] > [Security] > [Settings] に移動します。
3. [XMPP Certificate Settings] セクションを検索します。
4. [Domain name for XMPP Server-to-Server Certificate Subject Alternative Name] フィールドにプレゼンス サーバのドメインを指定します。
5. [Use Domain Name for XMPP Certificate Subject Alternative Name] チェックボックスをオンにします。
6. [Save] をクリックします。
7. この変更を保存した後、サーバで **cup-xmpp** 証明書を再生成する必要があります。
8. 変更を有効にするには、**XCP Router** を再起動します。

注意： XCP Router の再起動はサービスに影響を与えます。

これで、証明書検証が完了しました。

関連情報

- Cisco Jabber 9.2.5 のリリース ノート
- Cisco Jabber： 必須の証明書検証テクニカルノート
- テクニカルサポートとドキュメント - Cisco Systems