UCCX ソリューションの ECDSA 証明書について

目次

概要

このドキュメントでは、楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用のために Cisco Unified Contact Center Express（UCCX）ソリューションを設定する方法について説明します。

前提条件

要件

このドキュメントで説明する設定手順に進む前に、次のアプリケーションのオペレーティング システム（OS）管理ページにアクセスできることを確認してください。

- UCCX
- SocialMiner
- Cisco Unified Communications Manager（CUCM）
- UCCX ソリューション証明書の設定 - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

また、管理者は、エージェントおよびスーパバイザ クライアント PC 上の証明書ストアにもアクセスできる必要があります。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

コモン クライテリア（共通基準、CC）認証の一部として、バージョン 11.0 の ECDSA 証明書が Cisco Unified Communications Manager によって追加されました。 これは UCCX、SocialMiner、MediaSense など、バージョン 11.5 以降のすべての音声オペレーティング システム（VOS）製品に影響します。

楕円曲線デジタル署名アルゴリズムの詳細については、次のページを参照してください。
https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

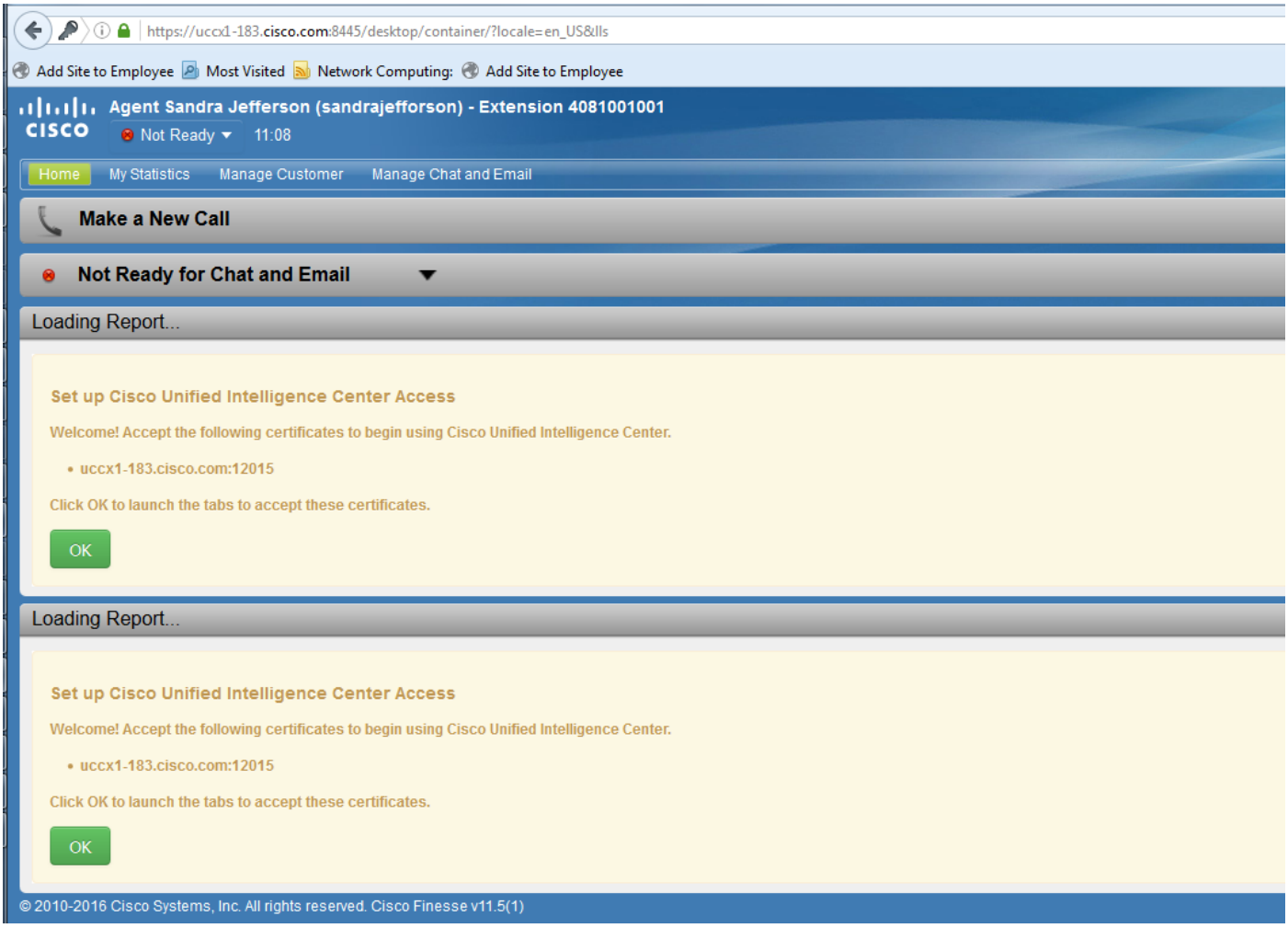
UCCX ソリューションに関しては、11.5 にアップグレードすると、以前のバージョンにはなかった追加の証明書が提供されます。 これは Tomcat-ECDSA 証明書です。

これは、次のプレリリース通信にも記載されています。
https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh

エージェント エクスペリエンス

11.5 へのアップグレード後、証明書が自己署名であるか、認証局（CA）により署名されたものであるかに基づいて、エージェントが Finesse デスクトップで証明書を受け入れるように求められることがあります。

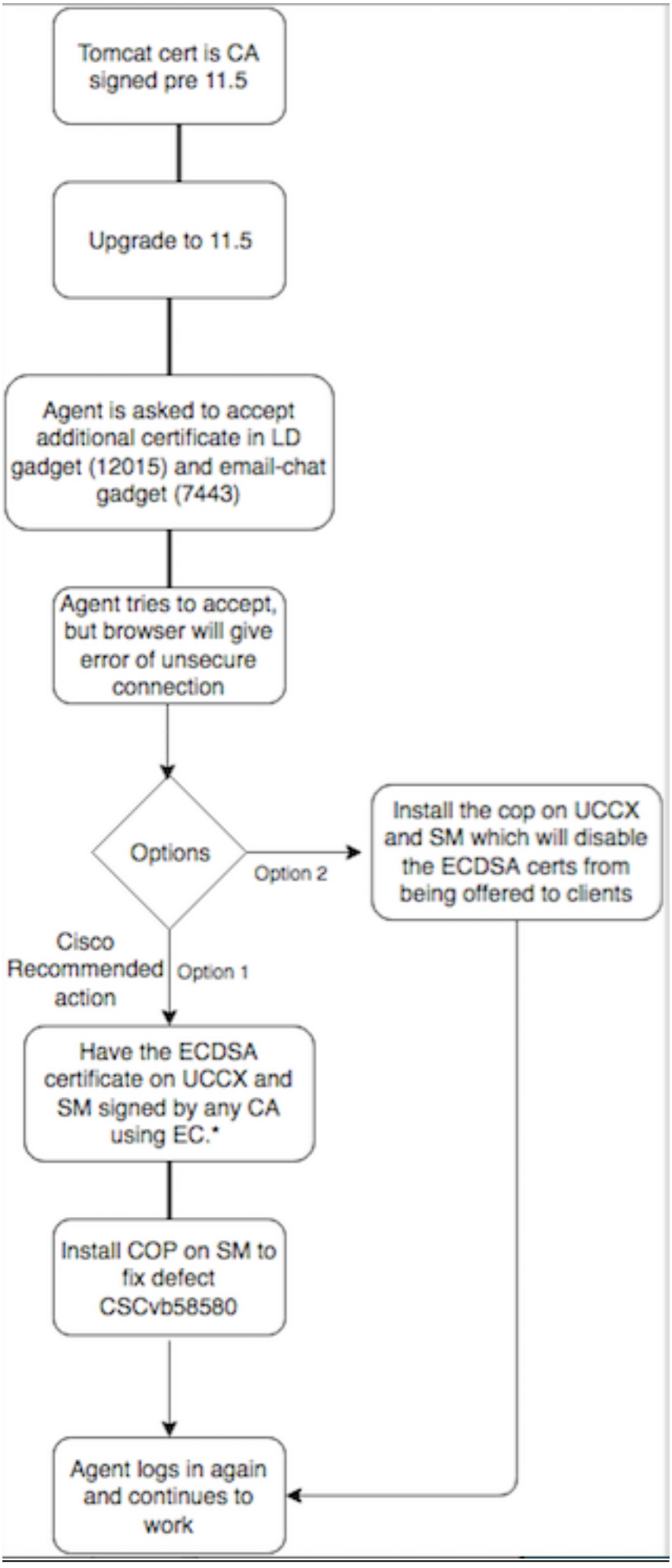
11.5 へのアップグレード後のユーザ エクスペリエンス



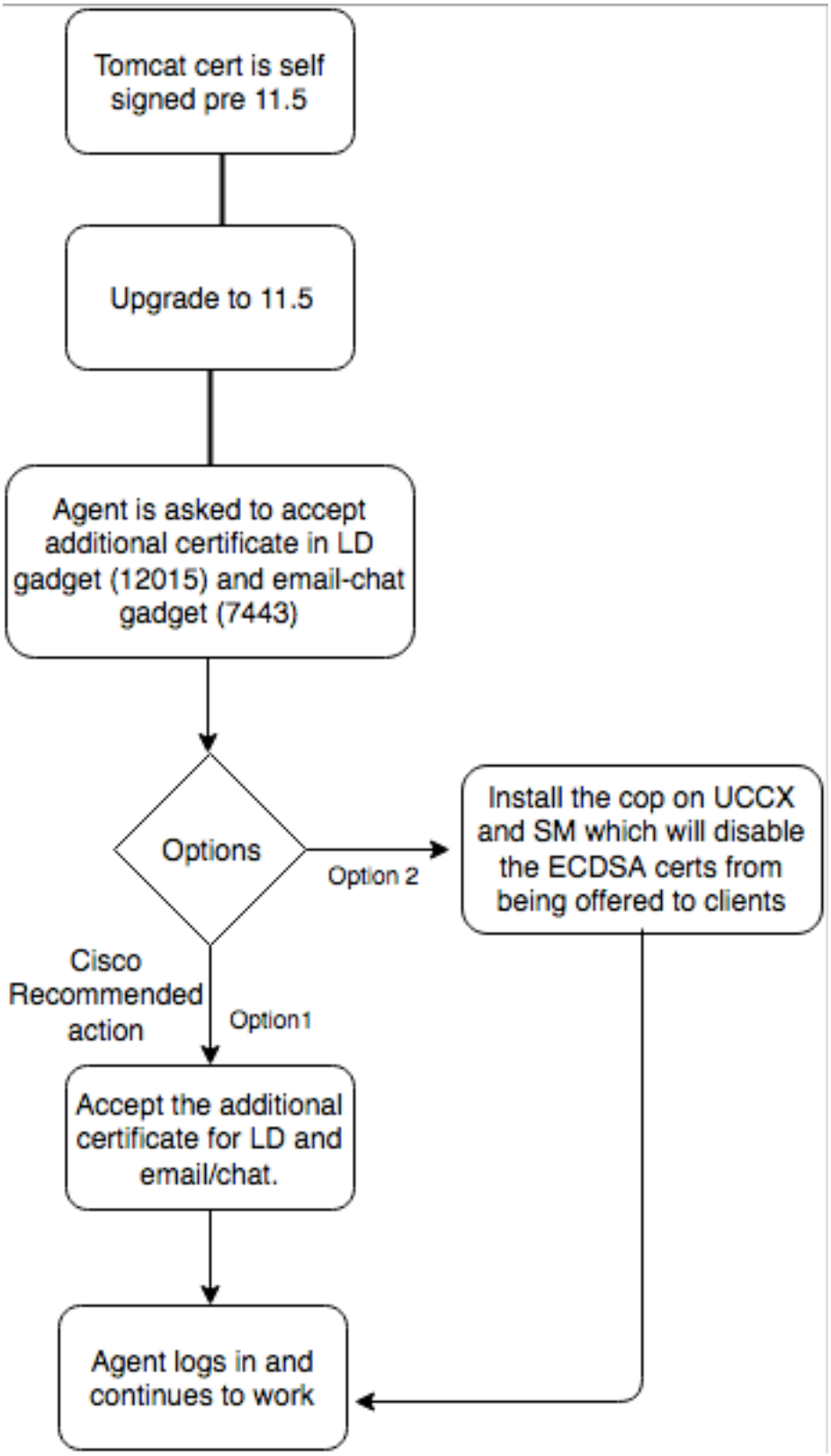
これは、以前は提供されていなかった ECDSA 証明書が Finesse デスクトップで提供されるようになったためです。

手順

CA 署名付き証明書のアップグレード前手順


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

自己署名証明書のアップグレード前手順



設定

この証明書で推奨されるベスト プラクティス

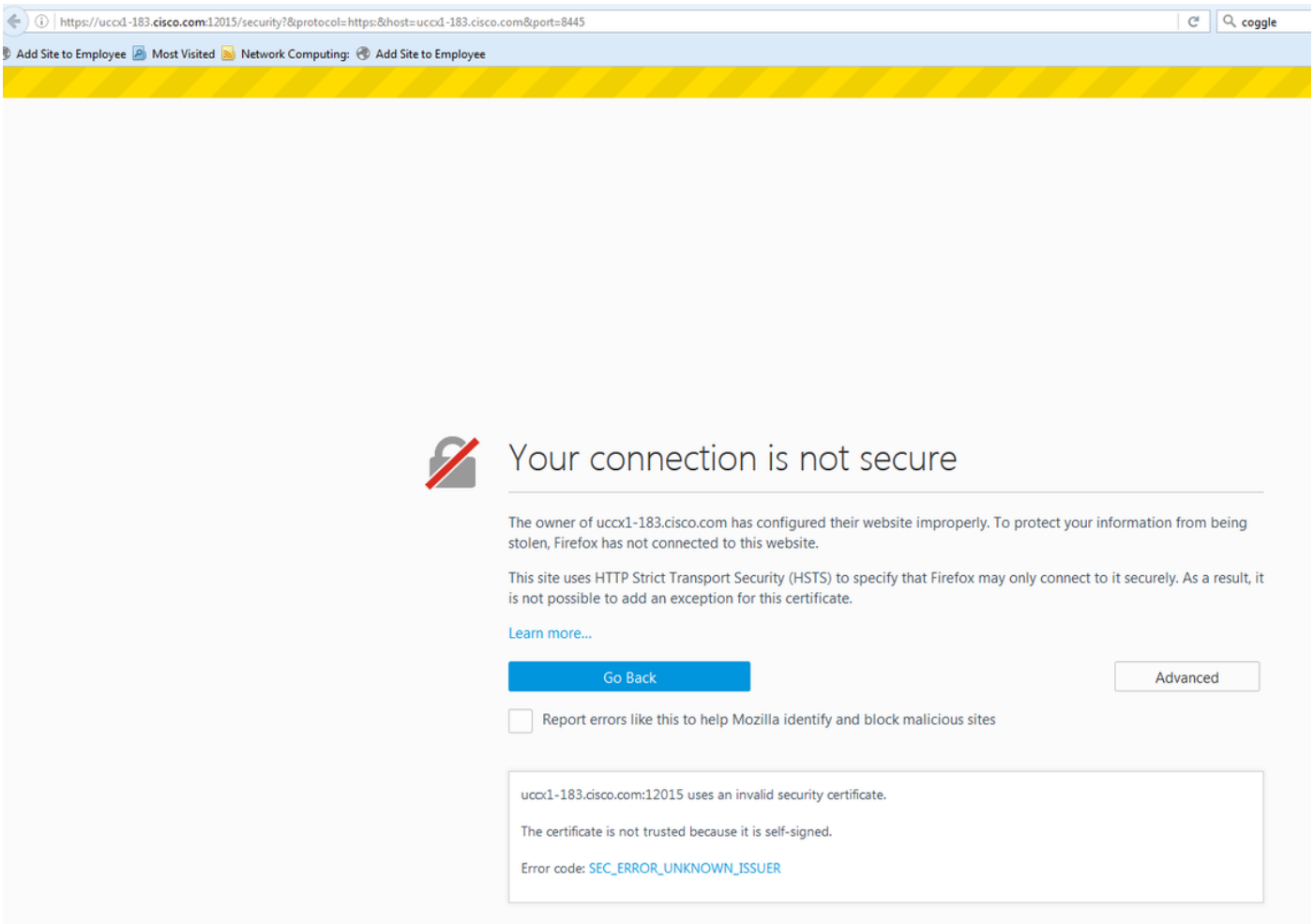
UCCX および SocialMiner の署名付き証明書

CA 署名証明書を使用する場合、他の証明書とともにこの ECDSA 証明書も認証局（CA）によって署名される必要があります。

> **注:** CA が RSA を使用してこの ECDSA 証明書に署名した場合、この証明書はクライアントに表示されません。 セキュリティを強化するには、ECDSA 証明書をクライアントに提示することをベスト プラクティスとして推奨します。

> **注:** SocialMiner 上の ECDSA 証明書が RSA を使用して CA によって署名された場合、電子メールおよびチャットで問題が発生します。 この問題は障害 CSCvb58580 に記載されており、COP ファイルが提供されています。 この COP は、ECDSA 証明書がクライアントに提示されないようにします。 RSA のみで ECDSA 証明書に署名できる CA を使用している場合は、この証明書を使用しないでください。COP を使用すると、ECDSA 証明書が提示されず、RSA のみの環境になります。

CA 署名付き証明書を使用しており、アップグレード後に ECDSA 証明書が署名/アップロードされない場合、追加の証明書を受け入れるよう求めるメッセージがエージェントに表示されます。 エージェントが [OK] をクリックすると、Web サイトにリダイレクトされます。 しかし ECDSA 証明書は自己署名であり、他の Web 証明書は CA 署名付きであるため、ブラウザ側のセキュリティ対策が原因でこの操作は失敗します。 この通信はセキュリティ上のリスクと見なされます。



バージョン 11.5 で UCCX および SocialMiner にアップグレードした後、UCCX パブリッシャとサブスクライバおよび SocialMiner の各ノードで次の手順を実行してください。

1. [OS Administration] ページを選択し、[Security] > [Certificate Management] を選択します。

2. [Generate CSR] をクリックします。

3. [Certificate List] ドロップダウン リストから、証明書名として [tomcat-ECDSA] を選択し、[Generate CSR] をクリックします。

4. [Security] > [Certificate Management] を選択し、[Download CSR] を選択します。

5. ポップアップ ウィンドウで、ドロップダウン リストから [tomcat-ECDSA] を選択し、[Download CSR] をクリックします。

新しい CSR をサードパーティ CA に送信するか、EC 証明書に署名する内部 CA でこれに署名します。 これにより、次の署名付き証明書が生成されます。

- CA のルート証明書（アプリケーション証明書と EC 証明書に同じ CA を使用する場合は、この手順をスキップできます）
- UCCX パブリッシャ ECDSA 署名付き証明書
- UCCX サブスクライバ ECDSA 署名付き証明書
- SocialMiner ECDSA 署名付き証明書

注: パブリッシャ（UCCX）にルート証明書および中間証明書をアップロードすると、それが自動的にサブスクライバに複製されます。 すべてのアプリケーション証明書が同じ証明書チェーンで署名される場合は、コンフィギュレーション内の他の非パブリッシャ サーバにルート証明書や中間証明書をアップロードする必要はありません。 また、同じ CA が EC 証明書に署名し、UCCX アプリケーション証明書の設定時にアップロードが済んでいる場合は、ルート証明書のアップロードを省略できます。

ノードにルート証明書および EC 証明書をアップロードするには、各アプリケーション サーバで次の手順を実行してください。

1. [OS Administration] ページを選択し、[Security] > [Certificate Management] を選択します。

2. [Upload Certificate] をクリックします。

3. ルート証明書をアップロードし、証明書タイプとして [tomcat-trust] を選択します。

4. [Upload File] をクリックします。

5. [Upload Certificate] をクリックします。

6. アプリケーション証明書をアップロードし、証明書タイプとして [tomcat-ECDSA] を選択します。

7. [Upload File] をクリックします。

   注: 下位 CA が証明書に署名する場合、ルート証明書の代わりに、下位 CA のルート証明書を *tomcat-trust* 証明書としてアップロードします。 中間証明書が発行される場合、アプリケーション証明書に加えて、この証明書を *tomcat-trust* ストアにアップロードします。 また、同じ CA が EC 証明書に署名し、UCCX アプリケーション証明書の設定時にアップロードが済んでいる場合には、ルート証明書のアップロードを省略できます。
8. 完了したら、次のアプリケーションを再起動します。

Cisco SocialMinerCisco UCCX パブリッシャとサブスクライバ

UCCX および SocialMiner の自己署名証明書

自己署名証明書を UCCX または SocialMiner で使用している場合、チャット - 電子メール ガジェットおよびライブ データ ガジェットで示される証明書の警告を受け入れるようにエージェントに通知する必要があります。

クライアント マシンに自己署名証明書をインストールするには、グループ ポリシーまたはパッケージ マネージャを使用するか、各エージェント PC のブラウザで個別に証明書をインストールします。

Internet Explorer の場合、[Trusted Root Certification Authorities] ストアに、クライアント側の自己署名証明書をインストールします。

Mozilla Firefox の場合は、次の手順を実行します：

1. [Tools] > [Options] に移動します。
2. [Advanced] タブをクリックします。
3. [View Certificate] をクリックします。
4. [Servers] タブを選択します。
5. [Add Exception] をクリックします。

1. **注:** あるいは、証明書をインストールするためのセキュリティ例外を追加することもできます（これは上記のプロセスと同等です）。 これは、クライアントで 1 回のみ行う設定です。

よく寄せられる質問（FAQ）

CA 署名付き証明書を持っていますが、EC CA で署名される必要のある ECDSA 証明書を使用したいと考えています。 CA 署名付き証明書が使用可能になるのを待っている間、ライブデータを起動させる必要があります。 どうすればよいですか。

この追加の証明書に署名したり、エージェントでこの追加の証明書を受け入れたりすることを希望していません。 どうすればよいですか。

ECDSA 証明書をブラウザに提示することが推奨されていますが、オプションでこれを無効にすることもできます。 COP ファイルを UCCX および SocialMiner にインストールすると、RSA 証明書のみがクライアントに提示されるようになります。 ECDSA 証明書はまだキーストアに残りますが、クライアントには提示されません。

この COP を使用して ECDSA 証明書のクライアントへの提示を無効にした場合、再び有効にすることはできますか。

可能です。ロールバック COP が提供されています。 これを適用すると、この証明書に署名してサーバにアップロードできるようになります。

すべての証明書が ECDSA になる予定ですか。

現時点ではそうではありませんが、将来的には VOS プラットフォームのセキュリティ更新が行われます。

どのような場合に UCCX COP をインストールすべきですか。

- 自己署名証明書を使用していて、追加の証明書をエージェントに受け入れさせないようにする場合
- CA によって署名された追加の証明書を取得できない場合

どのような場合に SM COP をインストールしますか。

- 自己署名証明書を使用していて、追加の証明書をエージェントに受け入れさせないようにする場合
- CA によって署名された追加の証明書を取得できない場合
- RSA のみを使って ECDSA 証明書に署名できる CA を使用している場合

各 Web サーバ サーバ インスタンスでデフォルトで提供される証明書は何ですか。

証明書の組み合わせ/Web サーバ	11.5 へのアップグレード後のデフォルトのエージェント エクスペリエンス (COP なしの場合)	UCCX Tomcat	Open Unifi 知サ
自己署名 Tomcat、自己署名 Tomcat-ECDSA	エージェントは、ライブ データ ガジェットおよびチャット - 電子メール ガジェットで証明書を受け入れるように求められます。	自己署名	自己署
RSA CA により署名された Tomcat、RSA CA により署名された Tomcat-ECDSA	エージェントは Finesse およびライブ データを使用できますが、電子メール - チャット ガジェットはロードされず、SocialMiner Web ページもロードされません。*	RSA	RSA
RSA CA により署名された Tomcat、EC CA により署名された Tomcat-ECDSA	エージェントは Finesse でライブ データとチャット - 電子メールの両方を使用できます。*	RSA	RSA
RSA CA により署名された Tomcat、自己署名 Tomcat-ECDSA	エージェントは、ライブ データ ガジェットおよびチャット - 電子メール ガジェットで追加の証明書を受け入れるように求められます。 ライブ データ ガジェットからの証明書の受け入れは失敗し、電子メール - チャット ガジェットからの証明書の受け入れは成功します。*	RSA	RSA

関連情報

- UCCX ECDSA COP - https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822
- SocialMiner ECDSA COP - https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=

11.5(1)&softwareid=283812550&sortparam=

- UCCX 証明書の情報 - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html