UCCXソリューション証明書管理ガイド

内容

概要
前提条件
要件
FQDN、DNS、およびドメイン
使用するコンポーネント
背景説明
設定
構成図
署名証明書
署名済みTomcatアプリケーション証明書のインストール
自己署名証明書
ペリフェラルサーバへのインストール
自己署名証明書の再生成
統合とクライアントの設定
UCCX-to-MediaSense
MediaSense-to-Finesse
UCCXからSocialMiner
UCCX AppAdminクライアント証明書
UCCXプラットフォームクライアント証明書
Notification Serviceクライアント証明書
Finesseクライアント証明書
SocialMinerクライアント証明書
CUICクライアント証明書
スクリプトからアクセス可能なサードパーティアプリケーション
確認
トラブルシュート
問題：無効なユーザIDとパスワード
原因
解決方法
問題：CSR SANと証明書SANが一致しない
原因
解決方法
問題：NET::ERR_CERT_COMMON_NAME_INVALID
原因
解決方法
その他の情報
証明書不具合
関連情報

概要

このドキュメントでは、自己署名証明書または署名証明書を使用するために Cisco Unified Contact Center Express（UCCX）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。

- Unified CCX
- SocialMiner
- MediaSense

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

FQDN、DNS、およびドメイン

UCCX設定のすべてのサーバには、ドメインネームシステム(DNS)サーバとドメイン名をインストールする必要があります。また、エージェント、スーパーバイザ、および管理者は、完全修飾ドメイン名(FQDN)を使用してUCCX設定アプリケーションにアクセスする必要があります。

UCCXバージョン10.0+では、インストール時にドメイン名とDNSサーバを入力する必要があります。UCCXバージョン10.0+インストーラによって生成される証明書には、必要に応じてFQDNが含まれています。UCCXバージョン10.0+にアップグレードする前に、DNSサーバとドメインをUCCXクラスタに追加します。

ドメインが初めて変更または入力された場合は、証明書を再生成する必要があります。ドメイン名をサーバー構成に追加した後、すべてのTomcat証明書を再生成してから、ほかのアプリケーションやクライアントブラウザにインストールするか、署名用の証明書署名要求(CSR)を生成します。

使用するコンポーネント

このドキュメントで説明する情報は、次のハードウェアおよびソフトウェアコンポーネントに基づいています。

- UCCX Webサービス
- UCCX通知サービス
- UCCXプラットフォームTomcat
- Cisco Finesse Tomcat
- Cisco Unified Intelligence Center(CUIC)Tomcat
- SocialMiner Tomcat
- MediaSense Webサービス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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、どのようなコマンドについても、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

共存するFinesseとCUICの導入、UCCXとSocialMiner間の電子メールおよびチャットの統合、Finesseを介した証明書の記録、理解、インストールのためのMediaSenseの使用により、証明書の問題をトラブルシューティングする機能が非常に重要になっています。

このドキュメントでは、UCCX設定環境での自己署名証明書と署名付き証明書の両方の使用について説明します。この使用目的は次のとおりです。

- UCCX通知サービス
- UCCX Webサービス
- UCCXスクリプト
- 共存Finesse
- 共存CUIC（ライブデータと履歴レポート）
- MediaSense（Finesseベースの録音およびタギング）
- SocialMiner（チャット）

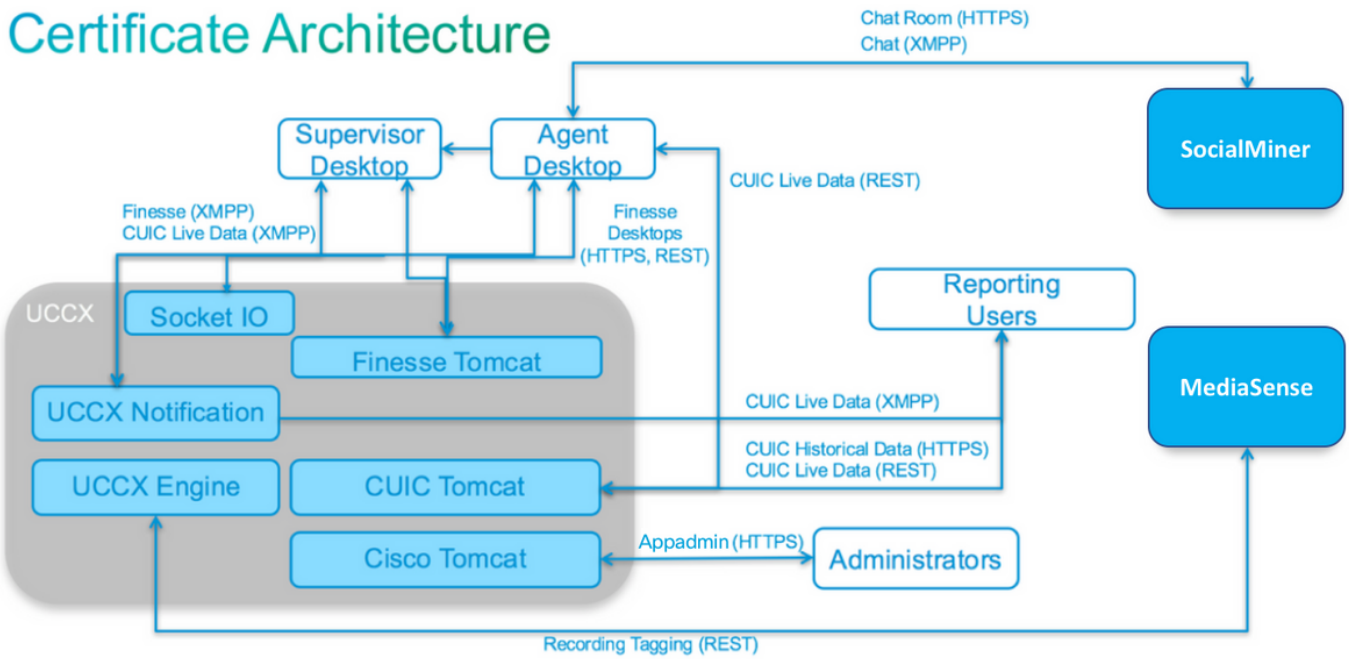
証明書（署名済みまたは自己署名済み）は、UCCX設定のアプリケーション（サーバ）と、エージェントおよびスーパーバイザクライアントのデスクトップの両方にインストールする必要があります。

Unified Communications Operating System(UCOS)10.5では、クラスタ内の各ノードの個々の証明書に署名しなくてもクラスタに対して単一のCSRを生成できるように、マルチサーバ証明書が追加されました。このタイプの証明書は、UCCX、MediaSense、およびSocialMinerでは明示的にサポートされていません。

設定

このセクションでは、自己署名証明書および署名証明書を使用するようにUCCXを設定する方法について説明します。

構成図



UCCX 11.0で有効なUCCXソリューションアーキテクチャ。HTTPS通信図。

署名証明書

UCCX設定の証明書管理に推奨される方法は、署名付き証明書を活用することです。これらの証明書は、内部の認証局(CA)または既知のサードパーティCAによって署名できます。

Mozilla FirefoxやInternet Explorerなどの主要なブラウザでは、よく知られたサードパーティCAのルート証明書がデフォルトでインストールされます。これらのCAによって署名されたUCCX設定アプリケーションの証明書は、ブラウザにすでにインストールされているルート証明書で証明書チェーンが終了するため、デフォルトで信頼されます。

内部CAのルート証明書は、グループポリシーまたはその他の現在の設定を通じて、クライアントブラウザにプレインストールされている場合もあります。

クライアントのブラウザでCAのルート証明書を使用できるかどうかと、事前にインストールしておく必要がある場合は、UCCX設定アプリケーションの証明書を、よく知られたサードパーティCAで署名するか、内部CAで署名するかを選択できます。

署名済みTomcatアプリケーション証明書のインストール

UCCXパブリッシャおよびサブスクライバ、SocialMiner、MediaSenseパブリッシャおよびサブスクライバ管理アプリケーションの各ノードについて、次の手順を実行します。

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] 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] を選択し、[Download CSR] をクリックします。

前述のように、新しいCSRをサードパーティCAに送信するか、内部CAで署名します。このプロ

セスでは、次の署名付き証明書が生成されます。

- CAのルート証明書
- UCCXパブリッシャアプリケーション証明書
- UCCXサブスクライバアプリケーション証明書
- SocialMinerアプリケーション証明書
- MediaSenseパブリッシャアプリケーション証明書
- MediaSenseサブスクライバアプリケーション証明書

注：CSRの**Distribution**フィールドは、サーバのFQDNのままにしておきます。

注：「マルチサーバ(SAN)」証明書は、11.6リリース以降のUCCXでサポートされています。ただし、SANにはUCCXノード1とノード2のみを含める必要があります。SocialMinerなどの他のサーバは、UCCXのSANに含めないでください。

注：UCCXは、1024ビットと2048ビットの証明書キー長のみをサポートします。

ルート証明書とアプリケーション証明書をノードに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ます。

注：パブリッシャ（UCCXまたはMediaSense）にルート証明書と中間証明書をアップロードする場合は、サブスクライバに自動的に複製されます。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。

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] 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。*
8. 完了したら、次のアプリケーションを再起動します。 Cisco MediaSenseパブリッシャおよびサブスクライバCisco SocialMinerCisco UCCX パブリッシャとサブスクライバ

注：UCCX、MediaSense、およびSocialMiner 11.5以降を使用する場合、tomcat-ECDSAという名前の新しい証明書があります。署名済みのtomcat-ECDSA証明書をサーバにアップロードする場合は、tomcat証明書ではなく、tomcat-ECDSA証明書としてアプリケーション証明書をアップロードします。ECDSAの詳細については、ECDSA証明書を理解して設定するためのリンクの「関連情報」セクションを参照してください。

自己署名証明書

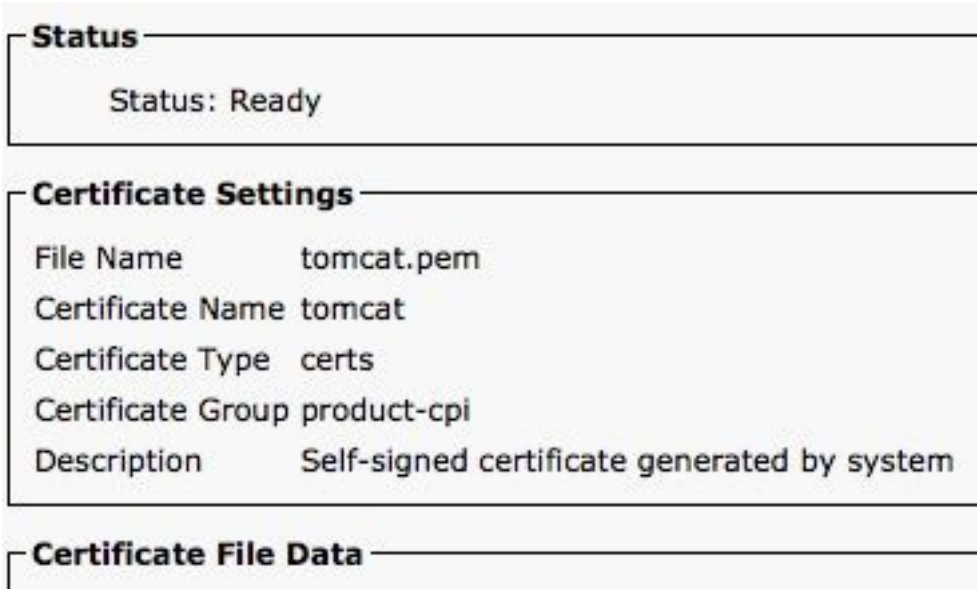
ペリフェラルサーバへのインストール

UCCX設定で使用されるすべての証明書は、設定アプリケーションにプリインストールされ、自己署名されます。これらの自己署名証明書は、クライアントブラウザまたは別の設定アプリケーションに提示される場合は、暗黙的に信頼されません。UCCX設定のすべての証明書に署名することが推奨されますが、プリインストールされた自己署名証明書を使用できます。

アプリケーションの関係ごとに、適切な証明書をダウンロードし、アプリケーションにアップロードする必要があります。証明書を取得してアップロードするには、次の手順を実行します。

1. アプリケーションの[OS Administration] ページにアクセスし、[Security] > [Certificate Management] を選択します。

2. 該当する証明書.pemファイルをクリックし、[Download] を選択します。



3. 適切なアプリケーションに証明書をアップロードするには、[OS Administration] ページに移動し、[Security] > [Certificate Management] を選択します。
4. [Upload Certificate / Certificate Chain] をクリックします。

5. 完了したら、次のサーバを再起動します。

   Cisco MediaSenseパブリッシャおよびサブスクライバCisco SocialMinerCisco UCCX パブリッシャとサブスクライバ

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。

自己署名証明書の再生成

自己署名証明書の期限が切れた場合は、自己署名証明書を再生成し、「**ペリフェラルサーバへのインストール**」の設定手順を再度実行する必要があります。

1. アプリケーションへのアクセス **OS Administration** ページと選択 **Security > Certificate Management**.
2. 該当する証明書をクリックし、[Regenerate] を選択します。
3. 証明書が再生成されたサーバを再起動する必要があります。
4. アプリケーションの関係ごとに、適切な証明書をダウンロードし、「**ペリフェラルサーバへのインストール**」の設定手順に従ってアプリケーションにアップロードする必要があります。

統合とクライアントの設定

UCCX-to-MediaSense

UCCXは、次の2つの目的のためにMediaSense WebサービスのRESTアプリケーションプログラミングインターフェイス(API)を消費します。

- Cisco Unified Communications Manager(CUCM)で呼び出される新しい録音の通知に登録します。
- UCCXエージェントの録音にエージェントおよびコンタクトサービスキュー(CSQ)情報のタグを付ける。

UCCXは、MediaSense管理ノードのREST APIを消費します。MediaSenseクラスタには最大2つまで存在します。UCCXは、REST APIを介してMediaSense拡張ノードに接続しません。両方のUCCXノードがMediaSense REST APIを使用する必要があるため、両方のUCCXノードに2つのMediaSense Tomcat証明書をインストールします。

MediaSenseサーバの署名付きまたは自己署名証明書チェーンをUCCX *tomcat-trust*キーストアにアップロードします。

MediaSense-to-Finesse

MediaSenseは、FinesseのMediaSense検索および再生ガジェットのエージェントを認証するために、Finesse WebサービスREST APIを使用します。

検索および再生ガジェットのFinesse XMLレイアウトで設定されたMediaSenseサーバは、Finesse REST APIを使用する必要があります。そのため、このMediaSenseノードに2つのUCCX Tomcat証明書をインストールします。

UCCXサーバの署名付きまたは自己署名付き証明書チェーンをMediaSense *tomcat-trust*キーストアにアップロードします。

UCCXからSocialMiner

UCCXは、電子メールの連絡先と設定を管理するためにSocialMiner RESTおよび通知APIを消費します。両方のUCCXノードがSocialMiner REST APIを使用し、SocialMiner通知サービスによって通知される必要があるため、両方のUCCXノードにSocialMiner Tomcat証明書をインストールします。

SocialMinerサーバの署名付きまたは自己署名証明書チェーンをUCCX *tomcat-trust*キーストアにアップロードします。

UCCX AppAdminクライアント証明書

UCCX AppAdminクライアント証明書は、UCCXシステムの管理に使用されます。UCCX管理者用のUCCX AppAdmin証明書をインストールするには、クライアントPCで各UCCXノードの**https://<UCCX FQDN>/appadmin/main**に移動し、ブラウザを使用して証明書をインストールします。

UCCXプラットフォームクライアント証明書

UCCX Webサービスは、クライアントブラウザへのチャット連絡先の配信に使用されます。UCCXエージェントおよびスーパーバイザのUCCXプラットフォーム証明書をインストールするには、クライアントPCで、各UCCXノードの**https://<UCCX FQDN>/appadmin/main**に移動し、ブラウザを使用して証明書をインストールします。

Notification Serviceクライアント証明書

CCX通知サービスは、Finesse、UCCX、およびCUICで使用され、Extensible Messaging and Presence Protocol(XMPP)経由でクライアントデスクトップにリアルタイム情報を送信します。これは、リアルタイムのFinesse通信およびCUICライブデータに使用されます。

ライブデータを使用するエージェントやスーパーバイザ、またはレポートユーザのPCに通知サービスのクライアント証明書をインストールするには、各UCCXノードの**https://<UCCX FQDN>:7443/** に移動し、ブラウザを介して証明書をインストールします。

Finesseクライアント証明書

Finesseクライアント証明書は、デスクトップと共存するFinesseサーバ間のREST API通信の目的でFinesse Tomcatインスタンスに接続するために、Finesseデスクトップによって使用されます。

エージェントとスーパーバイザのFinesse証明書をインストールするには、クライアントPCで各UCCXノードの**https://<UCCX FQDN>:8445/**に移動し、ブラウザプロンプトから証明書をインストールします。

Finesse管理者用のFinesse証明書をインストールするには、クライアントPCで各UCCXノードの**https://<UCCX FQDN>:8445/cfadmin**に移動し、ブラウザプロンプトから証明書をインストールします。

SocialMinerクライアント証明書

SocialMiner Tomcat証明書がクライアントマシンにインストールされている必要があります。エージェントがチャット要求を受け入れると、チャットガジェットはチャットルームを表すURLにリダイレクトされます。このチャットルームはSocialMinerサーバによってホストされ、顧客またはチャットの連絡先が含まれます。

ブラウザにSocialMiner証明書をインストールするには、クライアントPCで**https://<SocialMiner FQDN>/**に移動し、ブラウザプロンプトから証明書をインストールします。

CUICクライアント証明書

CUIC Tomcat証明書は、履歴レポートまたはライブデータレポートにCUIC Webインターフェイスを使用するエージェント、スーパーバイザ、およびレポートユーザのために、CUIC Webページ内またはデスクトップのガジェット内でクライアントマシンにインストールする必要があります。

ブラウザにCUIC Tomcat証明書をインストールするには、クライアントPCで**https://<UCCX FQDN>:8444/**に移動し、ブラウザプロンプトから証明書をインストールします。

CUICライブデータ証明書（11.x以降）

CUICは、バックエンドのライブデータにSocket IOサービスを使用します。この証明書は、ライブデータのCUIC Webインターフェイスを使用するエージェント、スーパーバイザ、およびレポートユーザ、またはFinesse内のライブデータガジェットを使用するユーザのクライアントマシンにインストールする必要があります。

ブラウザにソケットIO証明書をインストールするには、クライアントPCで**https://<UCCX FQDN>:12015/**に移動し、ブラウザプロンプトから証明書をインストールします。

スクリプトからアクセス可能なサードパーティアプリケーション

UCCXスクリプトがサードパーティサーバ上の安全な場所にアクセスするように設計されている場合(たとえば、*Get URL Document*ステップからHTTPS URLに、または*Make Rest Call*からHTTPS REST URLにアクセスする場合など)、サードパーティサービスの署名付きまたは自己署名証明書チェーンをUCCX *tomcat-trust*キーストアにアップロードします。この証明書を取得するには、UCCX **OS Administration**ページにアクセスし、**Upload Certificate**を選択します。

UCCXエンジンは、スクリプトの手順を使用して安全な場所にアクセスするサードパーティアプリケーションからプラットフォームTomcatキーストアにサードパーティ証明書チェーンが提示されたときに、これらの証明書チェーンを検索するように設定されています。

デフォルトではTomcatキーストアにはルート証明書が含まれていないため、証明書チェーン全体をプラットフォームTomcatキーストアにアップロードする必要があります。このキーストアには[OS Administration] ページからアクセスできます。

これらの操作が完了したら、Cisco UCCXエンジンを再起動します。

確認

すべての証明書が正しくインストールされていることを確認するには、このセクションで説明する機能をテストします。証明書エラーが表示されず、すべての機能が正しく機能する場合、証明書は正しくインストールされます。

- Finesseを設定して、ワークフローを介してエージェントを自動的に記録します。エージェントがコールを処理した後、MediaSense Search and Playアプリケーションを使用してコールを検索します。MediaSenseの録音メタデータにエージェント、CSQ、およびチームタグがコールに関連付けられていることを確認します。
- SocialMinerでエージェントWebチャットを設定します。Webフォームからチャットコンタクトを挿入します。エージェントがチャットの連絡先を受け入れるバナーを受信し、チャットの連絡先を受け入れるとチャットフォームが正しくロードされ、エージェントがチャットメッセージを受信および送信できることを確認します。
- Finesse経由でエージェントにログインを試みます。証明書の警告が表示されず、Webページに証明書のブラウザへのインストールを求めるプロンプトが表示されないことを確認します。エージェントが状態を正しく変更でき、UCCXへの新しいコールがエージェントに正しく表示されることを確認します。
- エージェントおよびスーパーバイザのFinesseデスクトップレイアウトでライブデータガジェットを設定したら、エージェント、スーパーバイザ、およびレポートユーザにログインします。ライブデータガジェットが正しく読み込まれ、初期データがガジェットに入力され、基になるデータが変更されたときにデータが更新されることを確認します。
- ブラウザから両方のUCCXノードのAppAdmin URLに接続してみます。ログインページでプロンプトが表示されたときに証明書の警告が表示されないことを確認します。

トラブルシュート

問題：無効なユーザIDとパスワード

UCCX Finesseエージェントが「**Invalid User ID/Password**」エラーでログインできません。

原因

Unified CCXが例外「SSLHandshakeException」をスローし、Unified CMとの接続を確立できません。

解決方法

- Unified CM Tomcat証明書が期限切れでないことを確認します。
- Unified CMにアップロードした証明書に、クリティカルとしてマークされた次のいずれかの拡張機能があることを確認します。
  X509v3キー使用法(OID - 2.5.29.15)
  X509v3基本制約(OID - 2.5.29.19)
  他の内線をクリティカルとしてマークすると、Unified CM証明書の検証が失敗するため、Unified CCXとUnified CM間の通信が失敗します。

問題：CSR SANと証明書SANが一致しない

CA署名付き証明書をアップロードすると、「CSR SAN and Certificate SAN does not match」エ

ラーが表示されます。

原因

CAは、証明書のサブジェクト代替名(SAN)フィールドに別の親ドメインを追加している可能性があります。デフォルトでは、CSRには次のSANがあります。

SubjectAltName [
  example.com(dNSName)
  hostname.example.com(dNSName)
]

CAは、別のSANが証明書に追加された証明書を返すことがあります。
www.hostname.example.com にアクセスしてください。この場合、証明書には追加のSANが含まれます。

SubjectAltName [
  example.com(dNSName)
  hostname.example.com(dNSName)

  www.hostname.example.com(dNSName)
]

これにより、SANミスマッチエラーが発生します。

解決方法

UCCXの[Generate Certificate Signing Request]ページの[Subject Alternate Name (SANs)]セクションで、[Parent Domain]フィールドが空のCSRを生成します。この方法では、CSRがSAN属性を使用して生成されず、CAがSANをフォーマットできるため、証明書をUCCXにアップロードするときにSAN属性が一致しません。[Parent Domain]フィールドのデフォルトはUCCXサーバのドメインであるため、CSRの設定が構成されている間は値を明示的に削除する必要があります。

問題：NET::ERR_CERT_COMMON_NAME_INVALID

UCCX、MediaSense、またはSocialMinerのいずれかのWebページにアクセスすると、エラーメッセージが表示されます。

「接続はプライベートではありません。

攻撃者は、<Server_FQDN>から情報（パスワード、メッセージ、クレジットカードなど）を盗もうとしている可能性があります。NET::ERR_CERT_COMMON_NAME_INVALID

このサーバーは<Server_FQDN>であることを証明できませんでした。そのセキュリティ証明書は[missing_subjectAltName]から取得されます。これは、設定ミスや攻撃者が接続を傍受したことが原因である可能性があります。

原因

Chromeバージョン58では新しいセキュリティ機能が導入され、Webサイトの共通名(CN)が

SANとしても含まれていない場合に、そのWebサイトの証明書がセキュリティで保護されていないことが報告されました。

解決方法

- [Advanced] > [Proceed to <Server_FQDN> (unsafe)] に移動してサイトに進み、証明書エラーを受け入れることができます。
- CA署名付き証明書を使用すると、このエラーを完全に回避できます。CSRを生成すると、サーバのFQDNがSANとして含まれます。CAはCSRに署名できます。署名された証明書をサーバにアップロードすると、サーバの証明書のSANフィールドにFQDNが設定されるため、エラーは表示されません。

その他の情報

「Chrome 58での廃止と削除」の「証明書でのcommonName照合のサポートを削除する」セクションを参照してください。

証明書不具合

- Cisco Bug ID CSCvb46250 - UCCX:Tomcat ECDSA証明書がFinesseライブデータに与える影響
- Cisco Bug ID CSCvb58580:RSA CAによって署名されたtomcatとtomcat-ECDSAの両方を使用してSocialMinerにログインできない
- Cisco Bug ID CSCvd56174 - UCCX:SSLHandshakeExceptionが原因のFinesseエージェントログイン障害
- Cisco Bug ID CSCuv89545 - Finesse Logjamの脆弱性

関連情報

- UCCXソリューションでのECDSA証明書について
- SHA 256によるUCCXのサポート
- UCCX の署名済み証明書と自己署名証明書の設定例
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。