セキュアな接続用の証明書管理

証明書

証明書は、Web 上のクライアントとサーバを認証することにより、ブラウザの通信が安全であることを確保するために使用されます。ユーザは、認証局から証明書を購入でき（CA 署名付き証明書 - 推奨）、または自己署名証明書を使用できます。

自己署名証明書

自己署名証明書（名前が意味するとおり）は、認証局によって署名されるのではなく、そのアイデンティティを証明する同じエンティティによって署名されます。自己署名証明書は、CA 証明書ほど安全であるとはみなされませんが、多くのアプリケーションでデフォルトで使用されています。

CCE 証明書管理ユーティリティ

シスコは、次の証明書管理ユーティリティを提供しています。

シスコ SSL 暗号化ユーティリティ：Web アプリケーションに使用される証明書管理ユーティリティ。

CiscoCertUtil：自己署名証明書および CA 署名付き証明書を作成およびインストールするために使用される証明書管理ユーティリティ。

（注） Unified CCE 証明書モニタリングサービスは、自己署名証明書および CA 署名付き証明書および証明書管理に使用されるキーをモニタします。サービスは、これらの証明書の有効性と有効期限についてシステム管理者に警告します。詳細については、以下にある *Cisco Unified ICM/Contact Center Enterprise* サービスアビリティ ベスト プラクティス ガイドを参照してください。http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

SSL 暗号化ユーティリティ

（注） 現在、このユーティリティには元の名前が付きますが、SSL 暗号化ユーティリティは、TLS で使用するために Web サーバを設定します。

Unified CCE Web サーバは、安全なアクセス（HTTPS）用に設定されています。シスコは、TLS で使用する Web サーバの設定に役立つ SSL 暗号化ユーティリティ（SSLUtil.exe）を提供しています。

（注） SSL 暗号化ユーティリティは、Windows Server 2016 を実行しているサーバでのみサポートされています。

IIS などのオペレーティング システムの機能は、SSL 暗号化ユーティリティで実行される操作を実行することもできます。ただし、シスコユーティリティを使用すると、プロセスが簡単になります。

SSLInstall.exe は、<ICMInstallDrive>\icm\bin フォルダにあります。SSL 暗号化ユーティリティは、セットアップの一部として、スタンドアロンモードで、または自動的に呼び出します。

SSL 暗号化ユーティリティは、実行する操作に関連したログメッセージを生成します。セットアップの一部として実行されると、ログメッセージがセットアップ ログ ファイルに書き込まれます。ユーティリティがスタンドアロンモードの場合、ログメッセージが SSL ユーティリティウィンドウおよび <SystemDrive>\temp\SSLUtil.log ファイルに表示されます。

SSL 暗号化ユーティリティは、次の主要な機能を実行します。

- SSL の設定（SSL Configuration）
- SSL 証明書の管理

SSLTLS は、Windows Server 2016 にインストールされている Unified CCE Web アプリケーションで使用できます。TLS 用のインターネット スクリプト エディタを設定できます。

セットアップ中の TLS のインストール

デフォルトでは、セットアップにより、Unified CCE インターネット スクリプト エディタ アプリケーションで TLS が有効になります。

（注） ユーティリティが開いている間、IIS マネージャを使用して TLS 設定を変更する場合は、SSL 設定ユーティリティを再起動する必要があります。

SSL 設定ユーティリティを使用すると、自己署名証明書の作成と、作成された証明書の IIS へのインストールが容易になります。また、このツールを使用して IIS から証明書を削除することもできます。設定の一部として呼び出された場合、SSL 設定ユーティリティは IIS に TLS ポートを 443 に設定します（空白である場合）。

インターネット スクリプト エディタで TLS を使用するには、インストール中にデフォルト設定を受け入れ、サポートされているサーバが TLS を使用します。

セットアップ中に、ユーティリティは自己署名証明書を生成し、ローカルマシンストアにインポートし、Web サーバにインストールします。仮想ディレクトリが有効になり、256 ビット暗号化を使用する TLS の設定されます。

（注） セットアップ中に、証明書が存在する場合、または Web サーバに既存のサーバ証明書がインストールされている場合は、ログエントリが追加され、変更は適用されません。スタンドアロンモードでユーティリティを使用するか、IIS サービスマネージャを使用して証明書管理を変更します。

スタンドアロンモードでの暗号化ユーティリティ

スタンドアロンモードでは、SSL 設定ユーティリティによって、ローカルマシンにインストールされている Unified ICM インスタンスのリストが表示されます。インスタンスを選択すると、ユーティリティにインストールされている Web アプリケーションとその SSL 設定が表示されます。その後、Web アプリケーションの SSL 設定を変更できます。

SSL 設定ユーティリティを使用すると、自己署名証明書の作成と、作成された証明書の IIS へのインストールが容易になります。また、このツールを使用して IIS から証明書を削除することもできます。設定の一部として呼び出された場合、SSL 設定ユーティリティは IIS に TLS ポートを 443 に設定します（空白である場合）。

CiscoCertUtil ユーティリティ

CiscoCertUtil ユーティリティを使用すると、CCE マシン上の証明書を管理し、システムがコンポーネントをまたがって処理する PII を保護できます。

TLS が有効なコンポーネントは、このユーティリティを使用して証明書をセットアップします。CCEのセットアップでは、このユーティリティを使用して証明書を生成し、インストールします。

CiscoCertUtil ユーティリティ：

- 自己署名証明書を生成します。
- 証明書署名要求（CSR）を生成します。
- パーソナルフォルダの下にあるローカルマシンの証明書ストアにリモート証明書をインストールします。
- パーソナルフォルダの下にあるローカルマシンの証明書ストアから証明書を削除します。
- 自己署名証明書を PEM 形式（X509 内線）で生成します。
- ファイル名 *host.key* を使用して対応するキーを生成します。
- 証明書を検証しません。
- 実行する操作に関連するログファイルを作成しません。エラーが発生すると、エラーログがコンソールに表示されます。
- Windows Server を実行しているサーバでサポートされています。

（注） CiscoCertユーティリティを使用すると、自己署名証明書のみをインストールまたは削除できます。

CiscoCert ユーティリティの使用

CiscoCertUtil *[/generateCert]|[/generateCSR]|[/generateCert /f]|[/remove <cert_name>]|[/install <cert_file>]| [/list]|[/help]|* コマンドを使用します。

ここで、

1. */list* は、信頼されたルートの下のローカルマシンストアに存在する証明書のリストを表示します。
2. */generateCert* は、ファイル名 *host.pem* とファイル名 *host.key* のキーを使用して自己署名証明書を生成します。自己署名証明書は`C:\icm\ssl\certs`に、キーは`C:\icm\ssl\keys`にコピーされます。キーが存在する場合は、同じキーを使用して自己署名証明書 *host.pem* を生成します。2048 ビットの RSA キー長が使用されます。

   /generateCert コマンドは *host.key* と *host.pem* を上書きしません。既存の自己署名証明書を上書きするには、*/generateCert /f* コマンドを使用します。このコマンドは、すでにシステムで使用可能な場合、*host.key* と *host.pem* を上書きします。

（注） CCEのインストール中は、自己署名証明書がすでに生成されます。新しい証明書を生成する必要がある場合にのみ */generateCert* コマンドを使用する必要があります。たとえば、証明書のキーが侵害された場合や、自己署名証明書の有効期限が切れた場合に、証明書を生成する必要がある場合があります。

3. */generateCSR* は、ファイル名 *host.csr* と、ファイル名 *host.key*（秘密キー）を持つキーを使用してCSRを生成します。その後、*host.csr* は認証局に送信され、デジタルID証明書を取得します。キーが存在する場合、*host.csr* の生成に同じキーが使用されます。
4. */remove* <*certificate_name*> は、証明書 <*cert_name*> をパーソナルフォルダの下のローカルマシンの証明書ストアから削除します。コマンドの実行に失敗すると、エラーメッセージが表示されます。存在する証明書のリストを表示するには、*/list* コマンドを使用します。
5. */install* <*cert_file_path*> は、<*cert_file_path*> の下で説明されている証明書をパーソナルフォルダの下のローカルマシン証明書ストアにインストールします。コマンドの実行に失敗すると、エラーメッセージが表示されます。

   このコマンドの例を示します。

   ```
   CiscoCertUtil /install c:\icm\ssl\certs\host.pem.
   ```
6. */help* は、コマンドの使用方法を表示します。

（注） *remove* コマンドが失敗した場合は、*list* コマンドを使用して、削除しようとした証明書がローカルマシンの証明書ストアに存在するかどうかを確認します。

転送中の安全な PII

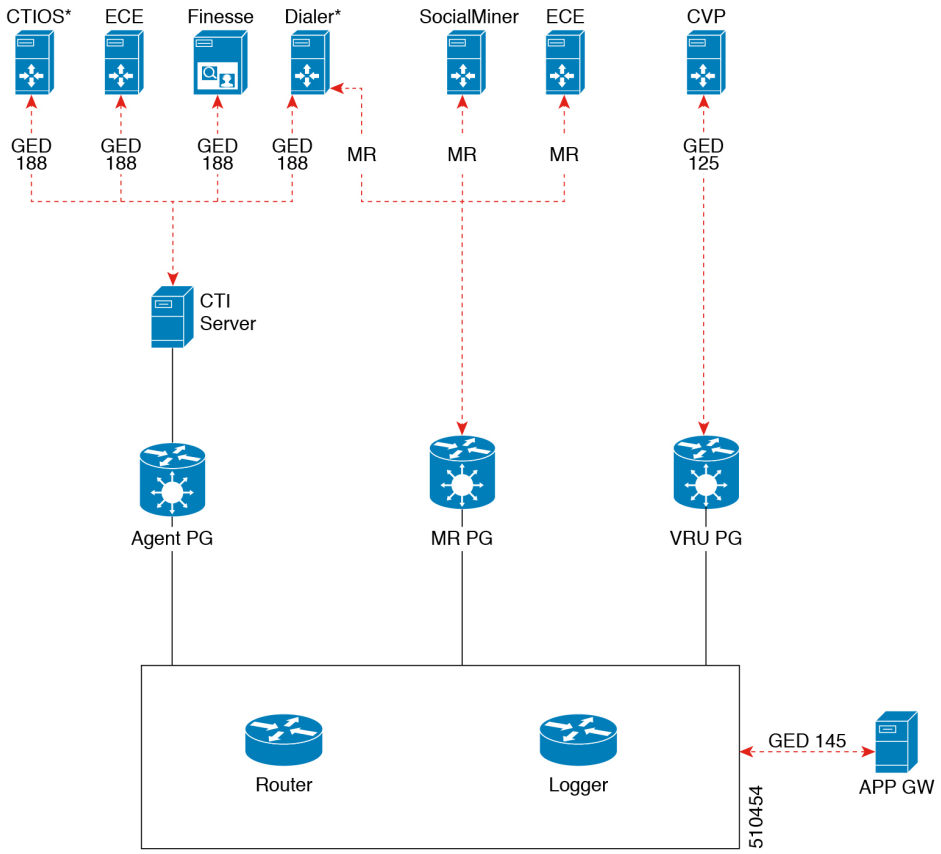
Contact Center Enterprise ソリューションは、クレジットカード情報、PIN、その他の機密情報を含む顧客の機密性の高い個人識別情報（PII）を処理します。このような機密情報はECC変数でシステム全体に送信され、利用される可能性があります。

GED 188、GED 125、GED 145、およびMR carry PIIなどのトランスポートチャネルは、攻撃を受けやすいです。したがって、PIIを移送するトランスポートチャネルを確保し、いかなる脅威からでも保護する必要があります。

PIIの確保は、規制のセキュリティ コンプライアンスにも準拠している必要があります。CCEソリューションは、TLSプロトコルを使用して、PIIをサポートするトランスポートチャネルのセキュリティを有効にします。

（注） セントラルコントローラとPG間の通信チャネルは安全ではありません。エンドツーエンドのソリューションのセキュリティについては、IPSecネットワーク分離ゾーンを使用します。

図 *1:* セキュリティで保護された接続の例



次の表に、セキュアな接続、サーバからクライアントへの対応マトリクス、および使用されるプロトコルの導入例を示します。

使用例	サーバ	サポート対象クライアント	[プロトコル（**Protocol**）]
セキュアなセルフサービス通信：セルフサービス通信を保護するために、CVP および VRU PG でのセキュアな接続を有効にします。	CVP	VRU PG	GED 125

使用例	サーバ	サポート対象クライアント	[プロトコル（Protocol）]
セキュアなアウトバウンドコール：アウトバウンドコールを保護するために、CTI サーバ、ダイヤラ、およびメディアルーティング PG でセキュアな接続を有効にします。	CTI サーバ	ダイヤラ	GED 188
	ダイヤラ	MR PG	メディアルーティングプロトコル
セキュアなエージェントデスクトップ通信：Cisco Finesse サーバおよび CTI OS との通信を保護するために、CTI サーバでの混在モード接続を有効にします。次に、必要に応じ、Cisco Finesse サーバまたは CTI OS でセキュアな接続を有効にします。	CTI サーバ	Cisco Finesse	GED 188
		CTI OS	
セキュアなサードパーティとの統合：CCE とサードパーティの統合を保護するために、アプリケーションゲートウェイ サーバとクライアントでのセキュアな接続を有効にします。	アプリケーションゲートウェイ サーバ	アプリケーションゲートウェイ クライアント	GED 145

使用例	サーバ	サポート対象クライアント	[プロトコル（Protocol）]
セキュアなマルチチャネル通信：マルチチャネル通信を保護するために、以下の間のセキュアな接続を有効にします。 • ECE（サービスサーバ）と MR PG（クライアント） • CTI サーバと ECE（クライアント）	ECE	MR PG	メディアルーティングプロトコル
	Customer Collaboration Platform		
	CTI サーバ	ECE	GED 188

サーバとクライアント間のセキュアな接続を確立するには、次のいずれかのセキュリティ証明書を使用して相互認証を作成する必要があります。

- 自己署名証明書
- サードパーティー CA 署名付き証明書

たとえば、CTI サーバとダイヤラ間で自己署名証明書を交換してセキュアな接続を確立する場合は、次の手順を実行する必要があります。

1. CTI サーバで利用可能な自己署名証明書をコピーしてダイヤラにインストールします。有効な証明書をまだ利用できない場合は、新しい証明書を生成する必要があります。詳細については、自己署名証明書の管理 （10 ページ）を参照してください。
2. 同様に、ダイヤラで利用可能な自己署名証明書を CTI サーバにコピーしてインストールします。

（注） クライアントとサーバが同じマシン上にある場合は、マシンで利用可能なセキュリティ証明書を、サーバまたはクライアントによって信頼されているストアに 1 度置く必要があります。証明書を信頼されているストアに 2 度目に配置しようとすると失敗します。詳細については、CiscoCertUtil ユーティリティ （3 ページ）を参照してください。

3. 次に、それぞれのインターフェイスで **[セキュアな接続を有効にする（Enable Secured Connection）]** チェックボックスをオンにする必要があります。この場合は、**[アウトバウンドオプション ダイヤラのプロパティ（Outbound Option Dialer Properties）]** 画面の **[CTI サーバコンポーネントのプロパティ（CTI Server Component Properties）]** 画面で **[セキュアな接続を有効にする（Enable Secured Connection）]** チェックボックスをオンにする必要があります。

詳細については、次のガイドを参照してください。

- Cisco Unified Contact Center Enterprise インストールおよびアップグレード ガイド at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- Unified Contact Center Enterprise アウトバウンド オプション ガイド at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

（注） 証明書を交換し、ソリューションのA側とB側の両方で個別にセキュアな接続を確立します。

（注） 証明書の追加、削除、更新など、証明書で新しいタスクを実行する場合は、必ずサービスを再起動して新しい接続を確立してください。

同様に、表「セキュア接続についてのサーバとクライアント間マトリクス」に記載された他のサーバとクライアント間でセキュアな接続を確立することもできます。

他のコンポーネント間のセキュアな接続については、次のガイドを参照してください。

- CVP と VRU PG 間のセキュアな接続については、http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html にある 『*Configuration Guide for Cisco Unified Customer Voice Portal*』 を参照してください。
- ダイヤラとのセキュアな接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html にある *Unified Contact Center Enterprise* アウトバウンド オプション ガイド を参照してください。
- CTI サーバと Cisco Finesse 間のセキュアな接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html にある Finesse の証明書の管理 （11 ページ） と を参照してください。
- CTI サーバと CTI OS 間のセキュアな接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html にある Cisco Unified ICM CTI OS システム マネージャ ガイド を参照してください。
- アプリケーション ゲートウェイ サーバとクライアント間のセキュアな接続については、次にある Cisco Unified ICM/Contact Center Enterprise コンフィギュレーション ガイド を参照してください。https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
- セキュアなマルチチャネル接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html にある Cisco Unified ICM/Contact Center Enterprise コンフィギュレーション ガイド を参照してください。

- セキュアな接続のポートの詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html にある Cisco Unified Contact Center Enterprise Solutions ポート使用状況ガイド を参照してください。

証明書とキーの場所

証明書、中間証明書、信頼できる証明書、およびキーをそれぞれのマシンの次のディレクトリに保存します。

証明書とキー	ディレクトリ
証明書	C:\icm\ssl\certs
中間証明書と信頼できる証明書	C:\icm\ssl\trust-certs 信頼できる証明書はこの場所に保存され、ここから Microsoft Windows ストアにインストールされます。
オプション キー（Keys）	C:\icm\ssl\keys

証明書を生成してインストールする手順については、このセクションで説明します。

自己署名証明書の管理

インターフェイス-サーバ-クライアント関係の範囲内でサーバとして定義されているマシン上の指定されたフォルダに、自己署名証明書を生成してコピーするには、次の手順を使用します。

/generateCert /generateCert /f および **generateCSR** のコマンドについては、CiscoCertUtil ユーティリティ （3 ページ） のコマンドの説明を参照してください。

Windows オペレーティングシステム上で実行されているシステムの証明書の管理

Windows オペレーティングシステム上で実行されているシステムの証明書を管理するには、次の手順を参照してください。

クライアントマシンへのサーバ証明書のインストール

手順

ステップ 1 サーバマシンで、以下のコマンドを使用して証明書を生成します：*<Install_Dir>:\icm\bin>CiscoCertUtil /generateCert*。このコマンドは、PEM 形式の証明書を生成し、このパス `C:\icm\ssl\certs` にコピーします。

有効な自己署名証明書がすでに利用可能な場合は、ステップ2に進みます。詳細については、CiscoCertUtil ユーティリティ （3 ページ） にある */generateCert* セクションを参照してください。

ステップ 2 パス `c:\icm\ssl\certs` に移動します。

ステップ 3 **host.pem** を クライアントマシンの一時的な場所にコピーします。

ステップ 4 クライアントマシン上で、次のコマンドを使用して、信頼された証明書ストアにこの証明書ファイルをインストールします：*CiscoCertUtil /install c:\icm\ssl\certs\host.pem*。証明書ファイルがクライアントマシンの信頼された証明書ストアに既に存在している場合は、新しい証明書ファイルをインストールする前に、この既存の証明書ファイルを削除します。

ステップ 5 証明書ファイルが正常にインストールされたことを確認するには、*CiscoCertUtil /list* コマンドを実行します。次に、サーバホスト名が `LOCAL_MACHINE/ROOT` の下にリストされたかを確認します。

サーバへのクライアント証明書のインストール

手順

ステップ 1 クライアントシステムで、以下のコマンドを使用して証明書を生成します：*<Install_Dir>:\icm\bin>CiscoCertUtil /generateCert*。このコマンドは、PEM 形式の証明書を生成し、このパス `C:\icm\ssl\certs` にコピーします。

有効な自己署名証明書がすでに利用可能な場合は、ステップ2に進みます。詳細については、CiscoCertUtil ユーティリティ （3 ページ） にある */generateCert* セクションを参照してください。

ステップ 2 `c:\icm\ssl\certs` に移動します。

ステップ 3 **host.pem** をサーバの一時的な場所にコピーします。

ステップ 4 サーバ上で、次のコマンドを使用して、信頼された証明書ストアにこの証明書ファイルをインストールします：*CiscoCertUtil /install c:\icm\ssl\certs\host.pem*。証明書ファイルがサーバの信頼された証明書ストアに既に存在している場合は、新しい証明書ファイルをインストールする前に、この既存の証明書ファイルを削除します。

ステップ 5 証明書ファイルが正常にインストールされたことを確認するには、*CiscoCertUtil /list* コマンドを実行します。次に、クライアントホスト名が `LOCAL_MACHINE/ROOT` の下にリストされたかを確認します。

次のタスク

証明書のインストール後、対応するサービスを再起動します。

Finesse の証明書の管理

Finesse サーバのセキュリティ証明書管理については、次の手順を参照してください。

Finesse サーバからの証明書のエクスポート

セキュリティ証明書を Finesse サーバからエクスポートするには、次の手順を使用します。

手順

ステップ 1 Finesse サーバの Cisco Unified Operating System の管理ページにログインします。

Finesse サーバ（`http://FQDN of Finesse server:8443/cmplatform`）の FQDN パスを使用してログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 Tomcat証明書のリストが表示されるかどうかに基づいて、次のいずれかの手順を実行します。

- Tomcat 証明書がリストされていない場合は、次の項目を実行します。
  - [新規作成（Generate New）] をクリックします。
  - 証明書の作成が完了したら、VOS サーバを再起動します。
  - この手順を再度行います。
- Tomcat 証明書がリストされている場合は、次の項目を実行します。
  - 証明書をクリックして選択します。[.pemファイルのダウンロード（Download .pem file）] をクリックして、ファイルをデスクトップに保存します。
  - 選択した証明書に、サーバのホスト名が含まれていることを確認します。

次のタスク

すべての Finesse サーバノードで、次の手順を実行します。

Finesse サーバへの証明書のインポート

セキュリティ証明書を Finesse サーバにインポートするには、次の手順を使用します。

手順

ステップ 1 Finesse サーバの Cisco Unified Operating System の管理ページにログインします。

Finesse サーバ（`http://FQDN of Finesse server:8443/cmplatform`）の FQDN パスを使用してログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 3 [Upload Certificate] をクリックします。

ステップ 4 **[証明書の名前（Certificate Name）] > [tomcat-trust]** を選択します。

ステップ 5 **[参照（Browse）]**をクリックします。

.pem ファイル拡張子を使用して、CTI サーバ証明書の場所を参照します。

ステップ 6 ファイルを選択し、[ファイルのアップロード（Upload File）] をクリックします。

次のタスク

残りのロードされていない証明書について、ステップ 3 ～ 6 を繰り返します。

すべての証明書をアップロードした後、Finesse Tomcat アプリケーションを再起動します。

サードパーティ CA 署名付き証明書の生成とコピー

相互認証にサードパーティ認証局（CA）の署名付き証明書を使用している場合は、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html にある『*Cisco Unified Contact Center Enterprise* インストレーションおよびアップグレードガイド』の「*CA* 証明書」の「CA 証明書」のセクションを参照してください。

Customer Collaboration Platform

Customer Collaboration Platformアプリケーションアクセスの制御

デフォルトでは、 Customer Collaboration Platform管理ユーザインターフェースへのアクセスは制限されています。管理者は、クライアントの IP アドレスを許可してアクセス権を提供し、許可リストからクライアントの IP を削除してアクセス権を取り消すことができます。許可リストを変更する場合は、Cisco Tomcat を再起動する必要があります。

（注） IP アドレス範囲とサブネットマスクはサポートされていません。

utils whitelist admin_ui list

このコマンドは、許可されている IP アドレスをすべて表示します。このリストは、着信要求の送信元を承認するために使用されます。

構文

utils whitelist admin_ui list

例

```
admin: utils whitelist admin_ui list Admin UI whitelist is: 10.232.20.31
10.232.20.32 10.232.20.33 10.232.20.34
```

utils whitelist admin_ui add

このコマンドは, 指定された IP アドレスをアドレスの許可リストに追加します。

構文

utils whitelist admin_ui add

例

```
admin:utils whitelist admin_ui add 10.232.20.33 Successfully added IP:
10.232.20.33 to the whitelist Restart Cisco Tomcat for the changes to take
effect
```

utils whitelist admin_ui delete

このコマンドは、指定された IP アドレスを許可リストから削除します。

構文

utils whitelist admin_ui delete

例

```
admin:utils whitelist admin_ui delete 10.232.20.34 Successfully deleted IP:
10.232.20.34 from the whitelist Restart Cisco Tomcat for the changes to take
effect
```

CA 署名付き証明書の取得

サインインするごとに、ブラウザがサーバによって提示された証明書を検証します。証明書が信頼されたルート認証局（CA）によって署名されていない場合、ブラウザは通常、ユーザが明示的に許可するまで接続を許可しません。これを回避するには、CAによって署名されたルート証明書を取得し、Customer Collaboration Platform の上にインストールする必要があります。

Unified OS の管理の証明書管理ユーティリティを使用して、これを行います。

[管理（Administration）] タブ > [プラットフォーム管理（Platform Administration）] から Unified OS の管理を開きます。

証明書を取得する方法

1. **セキュリティ > 証明書管理 > CSRの生成**を選択します。
2. 生成が成功したら、**[CSR のダウンロード（Download CSR）]** をクリックします。
3. CSR を使用して、認証局（CA）から署名付きのアプリケーション証明書と CA ルート証明書を取得します。

証明書をアップロードする方法

1. 証明書を受け取った場合は、**[管理（Administration）]> [プラットフォーム管理（Platform Administration）]** から Unified OS 管理を開きます。
2. **[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [証明書のアップロード（Upload Certificate）]** を選択します。
3. [Certificate Name] リストから、証明書の名前を選択します。
4. ルート証明書をアップロードします。
    1. [アップロード（Upload）] ダイアログボックスで、ドロップダウンリストから **tomcat trust** を選択します。
    2. ファイルを参照し、**[開く（Open）]** をクリックします。
    3. [ファイルのアップロード（Upload File）] をクリックします。
5. アプリケーション証明書をアップロードします。
    1. [アップロード（Upload）] ダイアログボックスで、ドロップダウンリストから **tomcat** を選択します。
    2. [ルート証明書（Root Certificate）] テキストボックスに CA ルートの名前を入力します。
    3. ファイルを参照し、**[開く（Open）]** をクリックします。
    4. **[ファイルのアップロード（Upload File）]** をクリックします。

CA 署名付き証明書の詳細については、Unified OS の管理のオンラインヘルプのセキュリティに関するトピックを参照してください。

証明書のアップロード後

1. Customer Collaboration Platform からログアウトします。
2. XMPP サービスを再起動します。（SSH から Customer Collaboration Platform を選択して、コマンド *admin:utils service restart Customer Collaboration Platform XMPP Server*）をコマンドライン インターフェイスに入力します。

3. tomcat を再起動します。（SSH から Customer Collaboration Platform を選択して、コマンド *admin:utils service restart Cisco Tomcat)*をコマンド ライン インターフェイスに入力します。
4. Customer Collaboration Platform にログインします。

自己署名証明書の取得

ブラウザは、自己署名証明書をさまざまな方法で処理します。以下のセクションでは、Customer Collaboration Platform でサポートされているブラウザで自己署名証明書を処理する方法について説明します。

Internet Explorer と自己署名証明書

Windows マシンで IE ブラウザを使用する場合は、DNS サーバが正しく設定されていることを確認して、完全修飾Customer Collaboration Platformホスト名をCustomer Collaboration Platformアドレスで解決 できます。信頼できる認証局（Verisign など）の署名付き証明書を使用します。

自己署名証明書（Customer Collaboration Platform でインストールされている場合）を使用する場合は、ログインのごとに証明書の警告が表示されるのを避けるために、次の手順に従います。

- [スタート（Start）] メニューで IE を右クリックし、[管理者として実行（Run as Administrator）] を選択します。
- アドレスバーに Customer Collaboration Platform サーバ の URL を入力します。
- セキュリティ警告が表示されたら、[**このサイトの閲覧を続行する（推奨されません）（Continue to this website (not recommended)**）] をクリックします。
- アドレスバーが赤色に変わると、アドレスバーの横に証明書エラーが表示されます。証明書エラーを選択します。
- ポップアップの下部にある **[証明書を表示（View certificates）]** を選択します。証明書ダイアログが開きます。
- [全般（General）] タブで、 **[証明書のインストール（Install Certificate）]** を選択します。に移動します。
- 証明書のエクスポートウィザードが起動します。[Next] をクリックします。
- 証明書の保存場所を確認するプロンプトが表示されたら、**[証明書をすべて次のストアに配置する（Place all certificates in the following store）]** を選択し、**[参照（Browse）]** をクリックして、**[信頼されたルート証明機関（Trusted Root Certification Authorities）]** を選択します。
- **[OK]** をクリックし、**[次へ（Next）]** をクリック して **[完了（Finish）]** をクリックして、証明書インポートウィザードを完了します。
- 証明書 の インポートを求めるプロンプトが表示されたら、**[はい（Yes）]** をクリックします。

• ブラウザを閉じて再起動して Customer Collaboration Platform にアクセスします。

Firefox と自己署名証明書

Firefox のセキュリティモデルの変更により、Firefox 上の Customer Collaboration Platform Web アプリケーションを使用するために許可される必要がある、追加の自己署名証明書があります。

新しくインストールされた Firefox ブラウザ（任意のバージョン）を使用して Customer Collaboration Platform サーバにアクセスすると、Firefox は Customer Collaboration Platform が最初に使用するメインポート（ポート 443）への接続を試行します。接続できない場合は、自己署名証明書を許可するプロンプトがユーザに表示されます。

（注） ポップアップがブロックされている場合は、手動で証明書ページを起動する手順が示されます。また、証明書を許可する前に証明書ウィンドウを閉じると、ページが自動的に再起動します。

- 要求された場合は、**[リスクについて理解しました（I Understand the Risks）]** をクリックし、**[例外の追加（Add Exception）]** をクリックします。
- [セキュリティ例外の確認（Confirm Security Exception）] をクリックします。

次に、Firefox はポート 7443（セキュアな XMPP ポート）への接続を試行します。Firefox では、このポートを使用するために2番目の自己署名証明書を許可する必要があります。Customer Collaboration Platform の画面には、このプロセス中は「接続の確認中....」と表示されます。

「接続の確認中..」の画面が数秒間表示された場合、**[続行（Continue）]**をクリックして Firefox 証明書の許可画面に進みます（前述のとおり）。

[リスクについて理解しました（I Understand the Risks）] をクリックして、**[例外の追加（Add Exception）]**、**[セキュリティ例外の確認（Confirm Security Exception）]** を再度クリックします。

ユーザは、新しい Firefox ブラウザと自己署名証明書を初めて使用する場合にのみ、このプロセスを実行する必要があります。証明書が正しく設定されると、「接続の確認中...」の画面が表示されない場合があります（あるいは、少しの間表示され、Customer Collaboration Platform のログイン画面に進みます）。

Google Chrome と自己署名証明書

Google Chrome ブラウザを使用して Customer Collaboration Platform のサーバにアクセスすると、ポート 7443 を使用してプライベートなセキュア接続の確立が試行されます。

- Chrome でサーバの IP アドレスを入力すると、ブラウザに**「接続はプライベートではありません」**という接続の警告メッセージが表示されます。セキュアな接続を続行するには、**[詳細設定（Advanced）]** をクリックします。

- **[<サーバ IP アドレス>に進む（Proceed to <Server IP Address>）]** をクリックします。次に、Chrome はポート 7443（セキュアな XMPP ポート）への接続を試行します。
- ブラウザに**「接続の確認中」**が表示されます。[続行（Continue）] をクリックして進みます。別の Chrome タブが開き、接続に関する別の警告メッセージが表示されます。
- **[詳細設定（Advanced）]** をクリックします。
- **[<サーバ IP アドレス> に進む（Proceed to <Server IP Address>）]** をクリックすると、Customer Collaboration Platform のログインページが表示されます。

（注） ユーザは、新しい Chrome ブラウザと自己署名証明書を初めて使用する場合にのみ、このプロセスを実行する必要があります。

Transport Layer Security（TLS）の要件

Contact Center Enterprise のソリューションは、Transport Layer Security（TLS）を使用します。TLS のサポートを設定する方法の詳細については、お使いのブラウザのマニュアルを参照してください。サポートされる TLS バージョンについては、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある Contact Center Enterprise 互換性マトリクスを参照してください。

（注） 以前のバージョンのクライアントとの後方互換性を確保するために、Microsoft の手順に従って、Unified CCE Windows システムを以前のバージョンの TLS にダウングレードすることができます。

TLS のサポートを構成せずにセキュリティ強化を適用すると、お使いのブラウザが Web サーバに接続できません。ページが利用できない、または Web サイトに技術的な問題が発生しているというエラーメッセージが表示されます。