Collaboration Security for the Enterprise Preferred Architecture 12.0 - ラボ ガイド

最終更新日:2018 年 8 月 15 日

作成者:コラボレーション テクノロジー グループ TME および dCloud コラボレーション チーム

このラボについて

これまでは、Cisco Collaboration へのエンドツーエンドの認証と暗号化の導入は、あまり浸透していませんでした。多くのお客様が、内部ネットワークがセキュアであり、そのために通信のプライバシーは確保されていると考えています。近年、こうした考え方が変化し、追加の防御層として、暗号化を採用する方法を検討するお客様が増えています。また、「VPN レス」アクセス技術の普及に伴い、ファイアウォールの境界を超えて企業のコラボレーション サービスにアクセスするあらゆる端末やクライアントで、シグナリングとメディアのプライバシー要件が標準になっています。

このコラボレーション セキュリティ ラボでは、上記のことを念頭において、セキュリティ機能および、エンド ツー エンドの証明書ベースの認証や、SIP シグナリングおよび RTP メディアの両方に対するメディア暗号化などの機能を有効にするために必要な実践的手順について説明します。範囲は、Cisco Unified Communications Manager、Cisco Unity Connection、Cisco Meeting Server、Cisco Expressway、Cisco Unified Border Element に及びます。

このラボは、Cisco Validated Design(CVD)に文書化されている、Cisco Preferred Architecture for Enterprise Collaboration 12.0 に基づいています。CVD は https://www.cisco.com/c/ja_jp/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd.html で参照できます。

このラボには、以下の 10 モジュールが含まれています。

- モジュール 1:Cisco Unified CM 証明書およびセキュアな LDAP

  このモジュールは、エンタープライズ CA 署名付き Unified CM 証明書(CallManager およびマルチサーバ tomcat 用)と、エンタープライズ LDAP サーバとのセキュアな統合について確認します。

  (コンポーネント:Unified CM、Microsoft 認証局/Active Directory)

- モジュール 2:輸出管理対象となる暗号化機能のスマート ライセンス**(パート B、手順 6 が必要)**

  このモジュールでは、Unified CM 混合モードを有効化するために必要となった、Unified CM 11.5(1) SU3 の新しい暗号化ライセンスについて確認します。また、12.0 コラボレーション システム リリース(CSR)のライセンス導入についても説明します。その中では、輸出規制に対応したライセンス付与の方法と、これまでの Prime License Manager 方式に代わる新しいスマート ライセンス方式についても触れています。

  (コンポーネント:Unified CM、Unity Connection)

- モジュール 3:PCI コンプライアンス対応 TLS 1.2

  このモジュールでは、コラボレーション アプリケーションに対する TLS 1.2 の要件について確認します。TLS について確認し、キャプチャ トレースの確認方法および nmap を使用して TLS のバージョンと暗号化方式を確認する方法について説明します。また、サーバで TLS 1.0/1.1 を無効にする設定についても説明します。

  (コンポーネント:Unified CM/IM and Presence、Unity Connection、Expressway、Cisco Meeting Server、CUBE (vCUBE))

- モジュール 4：ITL リカバリ

  このモジュールでは、トークンレス CTL と ITL が ITL リカバリ キーで署名されるようになった Unified CM 12.0 の新しい動作を確認し、Unified CM とエンドポイント間での信頼の維持に対する効果について説明します。

  （コンポーネント：Unified CM）

- モジュール 5：Jabber エンドポイントの暗号化**（モジュール 6 ～ 10 の前提）**

  このモジュールでは、暗号化されたセキュリティ プロファイルと、オンプレミスの Cisco Jabber® クライアント端末用に LSC 証明書をインストールするための CAPF 登録について説明します。

  （コンポーネント：Unified CM、Jabber®）

- モジュール 6：OAuth2 での更新ログイン フロー

  セキュアなコラボレーション アプリケーション間での OAuth2 の設定について確認します。

  （コンポーネント：Unified CM IM and Presence、Unity Connection、Jabber）

- モジュール 7：Cisco Unified Border Element（CUBE）とのセキュアな統合

  CUBE と Unified CM 間のセキュアな統合の設定について確認します（TLS、証明書）。

  （コンポーネント：Unified CM、CUBE（vCUBE）、Microsoft 認証局）

- モジュール 8：次世代暗号化によるセキュアなボイスメール

  Unity Connection に関する輸出規制対応とスマート ライセンスについて確認し、Unified CM と Unity Connection を統合してセキュアなボイス メッセージングを実現するための次世代暗号化を設定します。

  （コンポーネント：Unified CM、Unity Connection、Jabber、Microsoft 認証局）

- モジュール 9：Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー

  このモジュールでは、Expressway Mobile and Remote Access（MRA）で接続されたリモートのオフプレミス Jabber ユーザのための、エンド ツー エンドで暗号化された通話およびアクセス ポリシーについて確認します。

  （コンポーネント：Unified CM、Expressway、Jabber）

- モジュール 10：Cisco Meeting Server によるセキュアな会議

  即時のアドホック会議用にセキュアなビデオ会議を設定します。

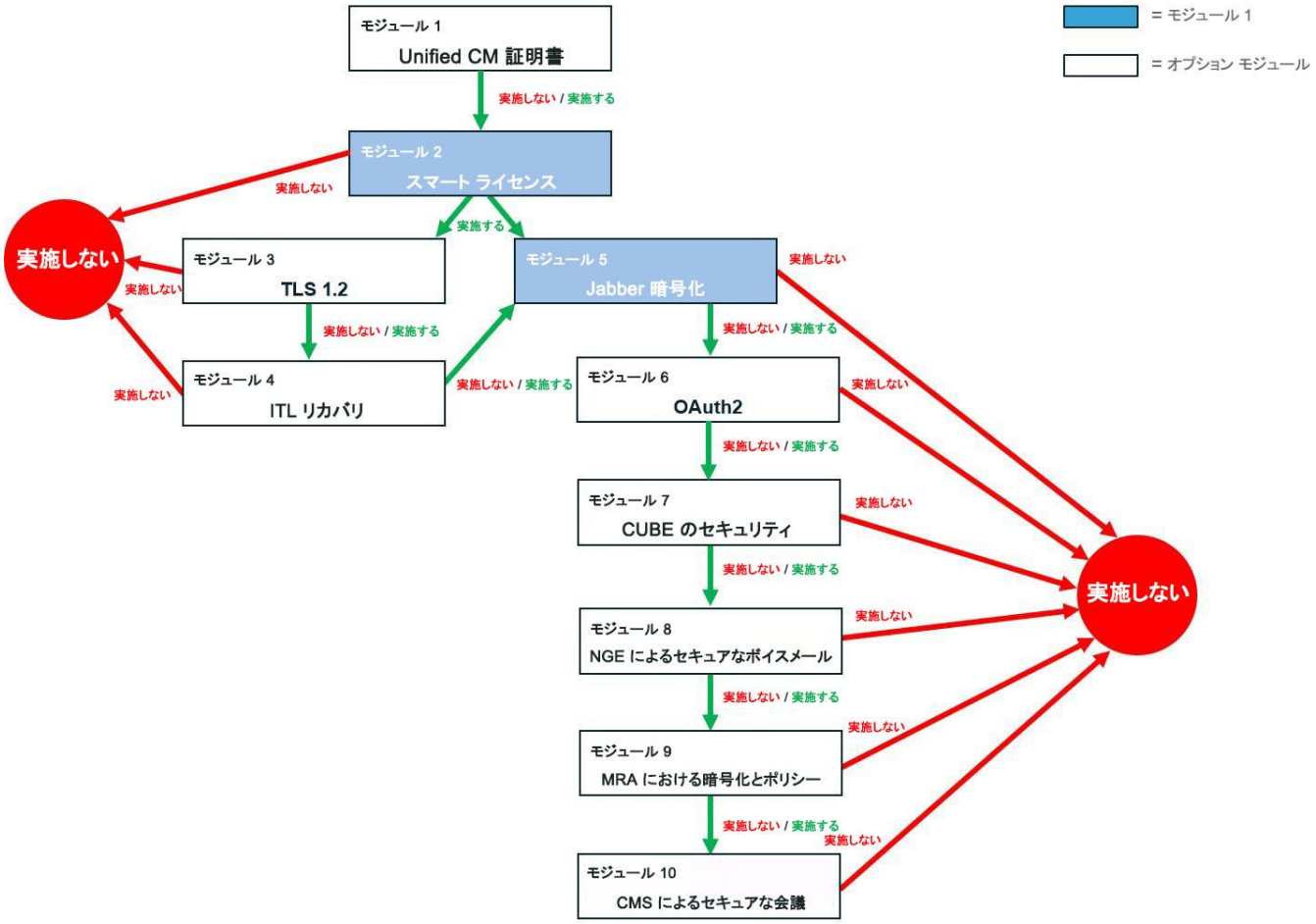
  （コンポーネント：Unified CM、Cisco Meeting Server、Expressway（MRA）、Jabber、Microsoft 認証局）*

  * このモジュール全体を確認するには、モジュール 9（Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー）の最初の 2 セクション（A および B）を完了する必要があります。

このラボは、ユーザがどのモジュールを実施するかを柔軟に選択できるように、できる限りモジュール化しています。ただし、**図 1** の学習マップに示しているように、モジュール間には以下の依存関係があります。

1. どのモジュールを選択する場合でも、モジュール 2（輸出管理対象となる暗号化機能のスマート ライセンス）はすべてのユーザが実施する必要があります。
2. モジュール 2 以外のモジュールはすべて任意です。ただし、モジュール 6 ～ 10 のいずれかを実施する場合は、モジュール 5（Jabber エンドポイントの暗号化）を完了する必要があります。
3. モジュール 9（Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー）の MRA アクセス ポリシーの部分は、モジュール 6（OAuth2 での更新ログイン フロー）が完了していることが前提になります。
4. モジュール 10（Cisco Meeting Server によるセキュアな会議）の、セキュアなアドホック会議の部分は、モジュール 9（Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー）の最初の 2 セクション（A および B）を完了し、アドホック会議への 3 番目の参加者として MRA 接続のリモート Jabber クライアントを有効にしておく必要があります。

図 1. 「エンタープライズ推奨アーキテクチャ向けのコラボレーション セキュリティ ラボ」学習マップ



すべてのモジュールを完了すると、Unified CM 証明書、CAPF 登録、混合モード、エンドポイント セキュリティ プロファイルに関する実践的な知識が得られます。また、最新の Unified CM コラボレーション機能や、輸出規制に対応した Cisco Smart Licensing、OAuth2 認証フレームワーク、PCI コンプライアンス対応 TLS 1.2、モバイル/リモート アクセス コントロール ポリシーを含むセキュリティの導入についても学習できます。Unity Connection ボイスメール、Cisco Meeting Server ビデオ会議、Cisco Unified Border Element 通話をセキュアに統合するための設定に関する知識も得られます。

「エンタープライズ推奨アーキテクチャ向けのコラボレーション セキュリティ」ラボに関するこのガイドには、次のセクションが含まれています。

制限

実稼働環境では、パブリック認証局（CA）の署名付き Expressway-E 証明書を導入するのがベスト プラクティスです。このラボでは、Expressway-E は内部ネットワークにあり、インターネットには接続していません。そのため、エンタープライズ Microsoft CA が Expressway-E 証明書の署名に使用されました。これらは、ラボ/デモの導入をシンプル化し、セッションのキャパシティを最大化するために意図的に導入されたものです。Jabber クライアントは、技術的にはエンタープライズ CA が署名した Expressway-E 証明書を使用できますが、シスコ電話機やビデオ端末を MRA モードで使用する場合は、Expressway-E にサポート対象のパブリック CA が署名した証明書が必要になります。

要件

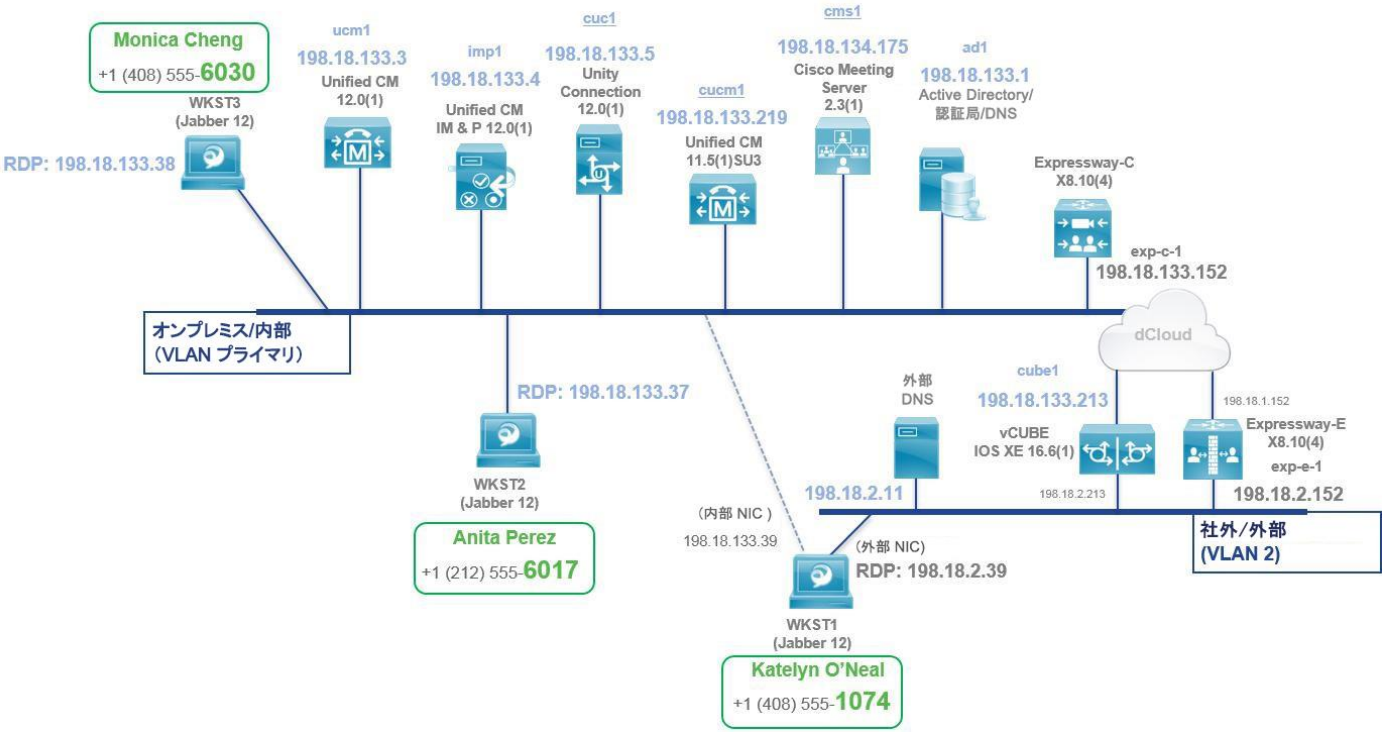
このラボには、ハードウェア要件はありません。

トポロジ

このラボの全体的なトポロジを**図 2** に示します。このトポロジには以下が含まれています。

- コラボレーション アプリケーション（Unified Communications Manager など）や、その他のアプリケーション サーバ（Microsoft Active Directory/認証局/ドメイン ネーム サービス（DNS）など）が存在する、オンプレミスの「内部」ネットワーク。
- インターネットに接続可能な外部の環境を示す、リモートの「外部」ネットワーク。内部のオンプレミス コラボレーション アプリケーションやサービスに到達するためには、このネットワークから Expressway Mobile and Remote Access（MRA）経由で接続できることが必要です。
- 3 台の Windows ワークステーション（2 台はオンプレミスで 1 台はリモート）と、このラボを通してエンドポイントとして使用する Cisco Jabber for Windows。オンプレミスのワークステーションは、このガイドに記載されているすべての設定を実施するために使用します。

図 2. コラボレーション セキュリティ ラボのトポロジ



このラボには、ソリューションの特長や機能を示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、事前定義の管理ユーザ アカウントを使用して任意の設定が可能です。アプリケーション サーバの IP アドレス、およびラボのコンポーネントにアクセスして必要な操作や設定を実施する際に使用する管理アカウントのクレデンシャルについては、以下のサーバおよびアプリケーションのクレデンシャルと詳細情報の表（**表 1**）を参照してください。ラボ演習を完了するためのユーザ名、関連するエンドポイント、割り当てられた電話番号、アカウント クレデンシャルなどのラボ ユーザ情報については、後述の「セッション ユーザ」セクションを参照してください。

表 1. サーバおよびアプリケーションのクレデンシャルと詳細情報

サーバ	説明	ホスト名（FQDN）	IP アドレス	ユーザ名	パスワード
Active Directory、認証局、DNS	Microsoft Windows Server 2008 R2 Standard	ad1.dcloud.cisco.com	198.18.133.1	administrator	C1sco12345
Unified CM	Cisco Unified Communications Manager 12.0(1)	ucm1.dcloud.cisco.com	198.18.133.3	administrator	dCloud123!
Unified CM (11.5)	Cisco Unified Communications Manager 11.5(1)SU3	cucm1.dcloud.cisco.com	198.18.133.219	administrator	dCloud123!
Unified CM IM and Presence	IM and Presence 12.0(1)	imp1.dcloud.cisco.com	198.18.133.4	administrator	dCloud123!
Unity Connection	Unity Connection 12.0(1)	cuc1.dcloud.cisco.com	198.18.133.5	administrator	dCloud123!
Expressway-C	Expressway 8.10(4)	exp-c-1.dcloud.cisco.com	198.18.133.152	admin	dCloud123!
Cisco Meeting Server	Cisco Meeting Server 2.3(1)	cms1.dcloud.cisco.com	198.18.134.175	admin	dCloud123!
Workstation 2	Windows 7 Professional SP1 と Jabber 12.0	wkst2.dcloud.cisco.com	198.18.133.37	aperez	C1sco12345
Workstation 3	Windows 7 Professional SP1 と Jabber 12.0	wkst3.dcloud.cisco.com	198.18.133.38	mcheng	C1sco12345
CUBE	Cisco Unified Border Element、IOS XE 16.6(1)	cube1.dcloud.cisco.com	198.18.133.213（内部、GE 1） 198.18.2.213（外部、GE 2）	admin	dCloud123!

Expressway-E	Expressway 8.10(4)	exp-e-1.dcloud.cisco.com	198.18.1.152 （内部 NIC） 198.18.2.152 （外部 NIC）	admin	dCloud123!
DNS（外部）	Microsoft Windows Server 2008 R2 Standard	ext-dns.dcloud.cisco.com	198.18.2.11	administrator	C1sco12345
Workstation 1	Windows 7 Professional SP1 と Jabber 12.0	wkst1.dcloud.cisco.com	198.18.133.39 （内部 NIC） 198.18.2.39 （外部 NIC）	koneal	C1sco12345

セッション ユーザ

以下の**表 2** には、セッションで使用可能な事前設定済みのユーザについての詳細が記載されています。

表 2. エンド ユーザ情報とクレデンシャル

ユーザ名	ユーザ ID	ユーザ パスワード	エンドポイント端末	企業電話番号	4 桁の内線番号
オンプレミス/内部					
Anita Perez	aperez	C1sco12345	CSFAPEREZ（WKST2 – Jabber）	+1 212 555 6017	6017
Monica Cheng	mcheng	C1sco12345	CSFMCHENG（WKST3 – Jabber）	+1 408 555 6030	6030
リモート/外部					
Katelyn O'Neal	koneal	C1sco12345	CSFKONEAL（WKST1 – Jabber）	+1 408 555 1074	1074

はじめに

デモンストレーションの前に

実際のお客様の前でプレゼンテーションを行う前に、このプロセスを少なくとも 1 回は実施しておくことを強く推奨します。そうすることで、ドキュメントとデモンストレーションの構成に慣れることができます。

お客様向けプレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってデモンストレーションのスケジュールを組み、デモンストレーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る]

注：セッションがアクティブになるまで、最長で 45 分かかることがあります。

2. スタンドアロンのラップトップまたは他の端末からセッションに直接接続します。**Cisco AnyConnect VPN** クライアントをインストールしてアクセスし、Cisco dCloud UI で AnyConnect のクレデンシャルを入力します。[手順を見る]
3. AnyConnect VPN クライアントが接続されたら、使用しているラップトップまたは端末上の **Remote Desktop Protocol（RDP）**クライアントからラボのワークステーションに接続します。[手順を見る] このラボ ガイドに示された適切なワークステーションからすべての操作および設定を実施します。

注：RDP を使用してこのラボの Windows サーバやワークステーションに接続する場合は、ログイン クレデンシャルを入力する際に、ドメイン（DCLOUD\）を指定する必要があります。たとえば、Workstation 2（WKST2）に接続する場合は、最初のログイン時に、ユーザ名として **DCLOUD**aperez を指定します。

モジュール 1　Cisco Unified CM 証明書およびセキュアな LDAP

モジュールの概要

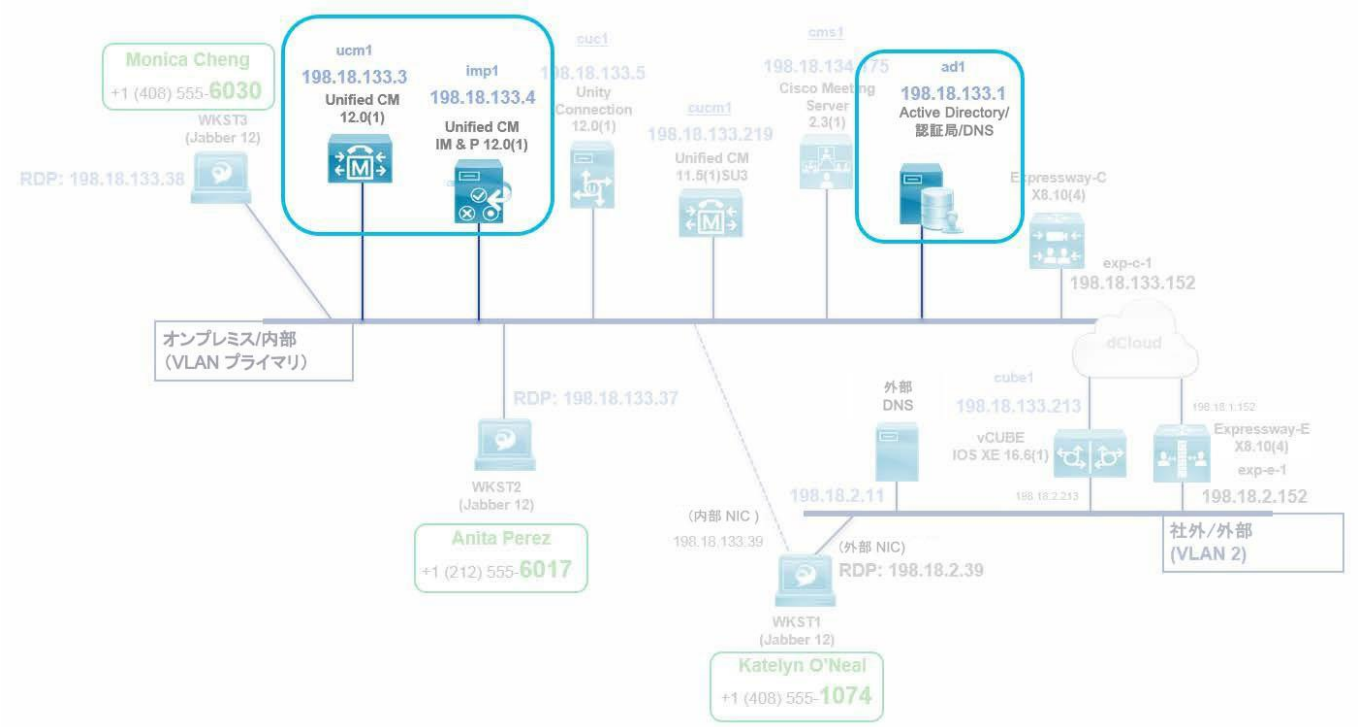
このモジュールでは、Unified CM で以下の 2 つの基本的なタスクを実行します。

A. Unified CM 証明書の調査とタスク

B. セキュアな LDAP のプロビジョニング

次の図 3 は、このモジュールのトポロジと、関連するコンポーネントを示しています。

図 3.　モジュール 1：Cisco Unified CM 証明書およびセキュアな LDAP



A. Unified CM 証明書の調査とタスク

注：このセクションでは、Unified CM 証明書の管理に関する操作を確認します。X.509 デジタル証明書を管理した経験のないユーザにお勧めします。

Unified CM の証明書は、受講者用にすでに署名されています。このセクションを進める場合は、その証明書を再生成して、再度署名することになります。これまでに証明書の管理の経験がある場合は、このセクションをスキップし、セクション B または直接モジュール 2 に進んで構いません。このラボの他のモジュールでも X.509 証明書を管理する機会が何度かあります。

このセクションでは、コラボレーション アプリケーション証明書のベスト プラクティスについて説明します。最初に Unified CM の既存の証明書を確認するところから始めます。次に、tomcat 証明書と CallManager 証明書に対してエンタープライズ CA の署名を得るために、証明書署名要求（CSR）を生成します。署名付き証明書は、Unified CM にアップロードされ、CA 証明書と合わせて、tomcat-trust 信頼ストアと CallManager-trust 信頼ストアにアップロードされます。

1. Unified CM の既存の証明書を確認する

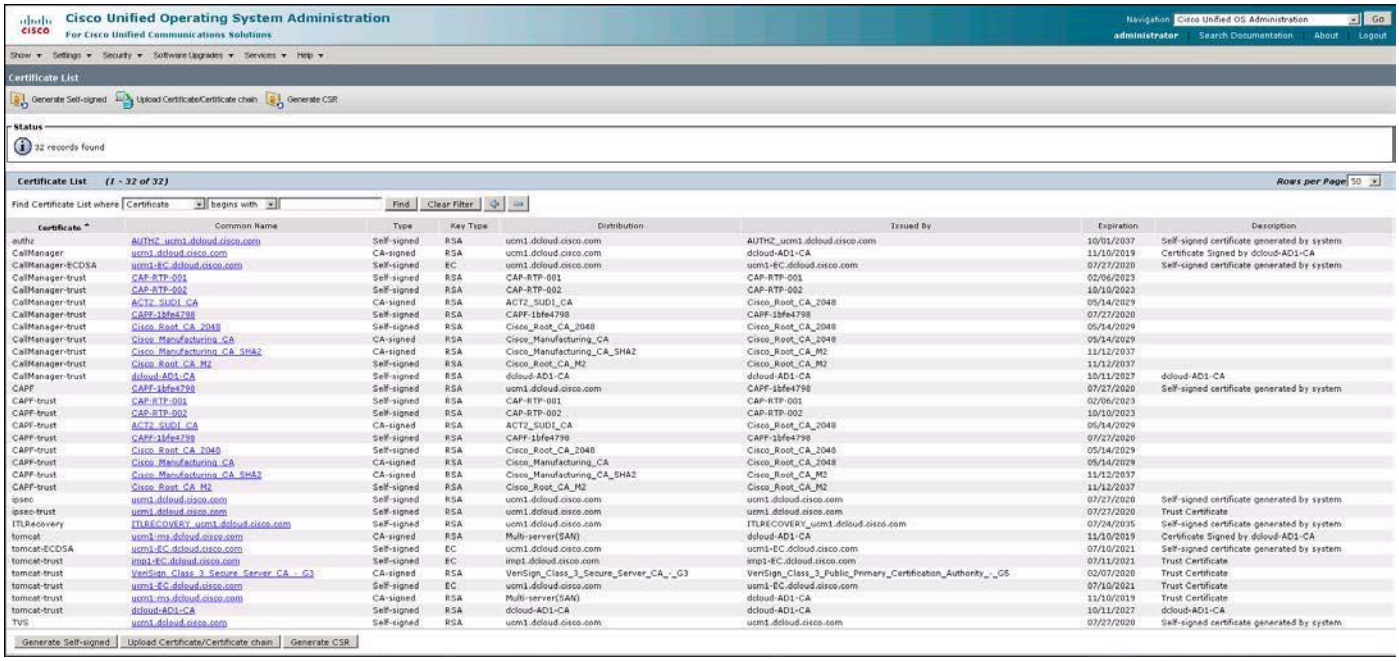
   コラボレーション セキュリティでは、証明書が重要な役割を担っています。Unified CM のさまざまな証明書を見てみましょう。

   WKST3（198.18.133.38、ユーザ名/パスワード：DCLOUD**mcheng/C1sco12345**）に RDP 接続します。Firefox Web ブラウザを起動し、Unified CM オペレーティング システムの管理インターフェイス（https://ucm1.dcloud.cisco.com/cmplatform）に移動します。

   ユーザ名/パスワード：**administrator/dCloud123!** を使用してシステムにログインします。[セキュリティ（Security）] > [証明書の管理（Certificate Management）] の順に選択し、[検索（Find）] をクリックします。

   図 4 に、Unified CM OS 証明書管理インターフェイスと、システム証明書のリストを示します。

   図 4. Unified CM 証明書リスト



   エンタープライズ PA のベスト プラクティスでは、以下のサービスに対して、デフォルトの自己署名証明書ではなく、認証局（CA）で署名された証明書を使用することが推奨されています。

   - tomcat
   - CallManager

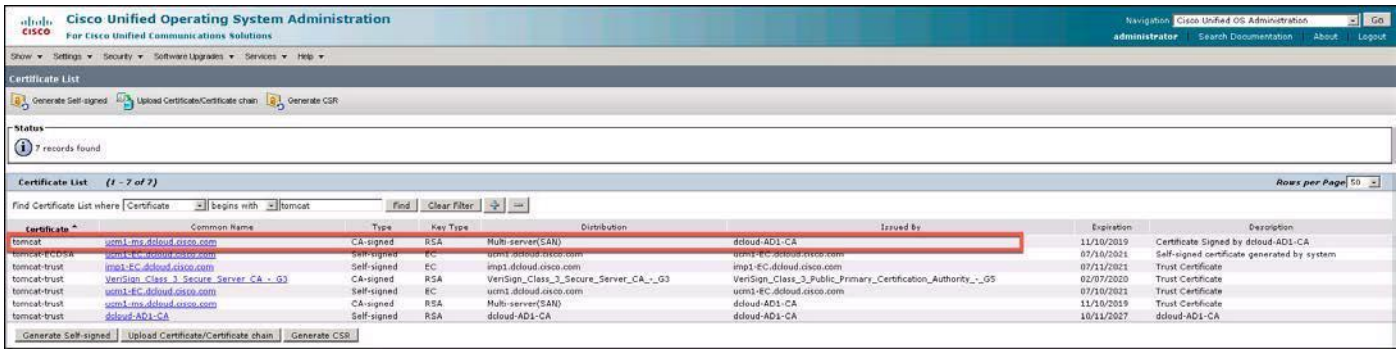
   これらの証明書の署名には、パブリック CA または民間のエンタープライズ CA を使用します。

   注：このラボでは、tomcat と CallManager の証明書は、すでに外部の CA で署名されていますが、今後のセクションのために、CSR を再生成し、新たなエンタープライズ CA 署名付き証明書を取得します。次の手順に進んで、tomcat と CallManager に対して新しい CSR を生成する場合、このモジュールの残りの部分を**完了する必要**があります。または、このモジュールの残りの手順を確認するだけにします。

2. tomcat の証明書署名要求（CSR）を生成する

   証明書リストから **tomcat** で始まる証明書を検索します。図 5 に示すように、tomcat の証明書は、このラボのエンタープライズ CA（dCloud-AD1-CA）ですでに署名されていますが、今回のラボのために、新しく CA 署名付き証明書を再生成します。

図 5. Unified CM の tomcat/tomcat-trust 自己署名証明書

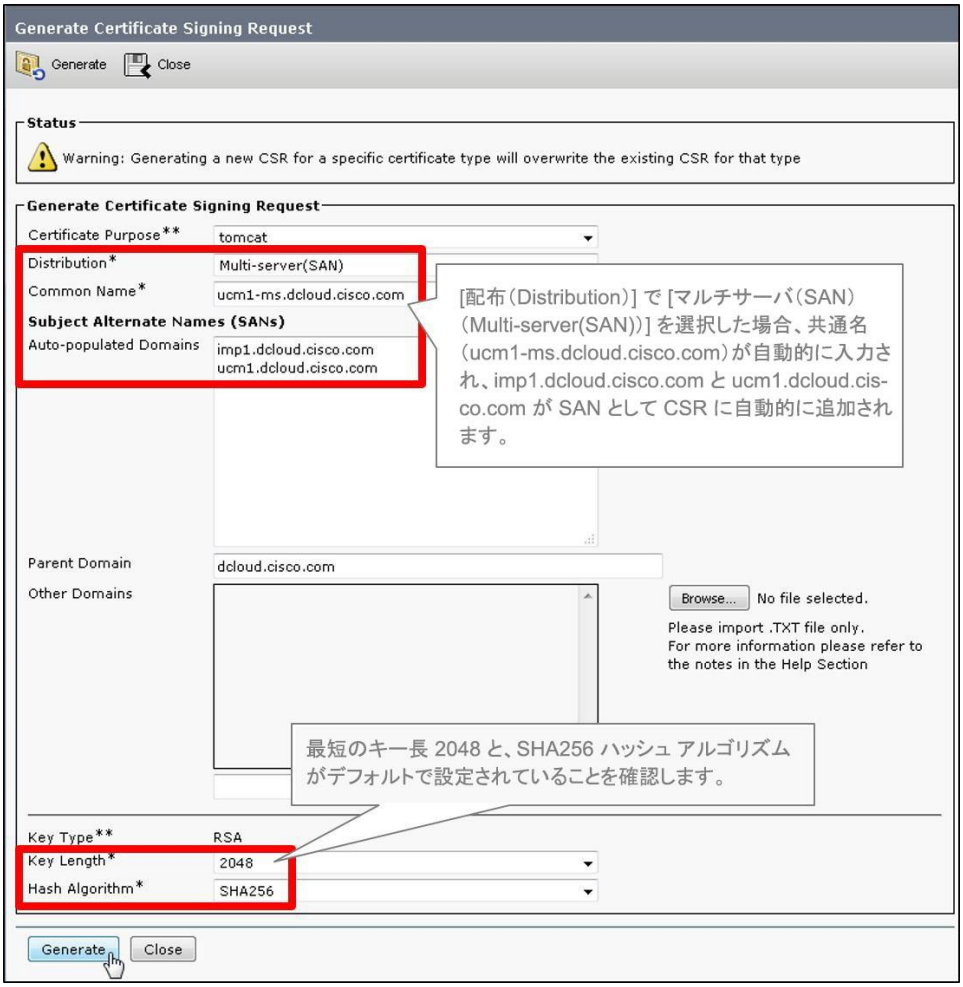


[CSR の生成（Generate CSR）] をクリックします。次のウィンドウの [証明書の用途（Certificate Purpose）] ドロップダウン メニューで **tomcat** が選択されていることを確認します（デフォルト値）。

ここでは、tomcat に対するマルチサーバ SAN の CSR を生成するため、[配布（Distribution）] ドロップダウンから [マルチサーバ（SAN）（Multi-server(SAN)）] を選択します。マルチサーバを選択すると、図 6 に示すように、共通名が **ucm1-ms.dcloud.cisco.com** に変わり、Unified CM ノード（**ucm1.dcloud.cisco.com**）と Unified CM IM and Presence ノード（**imp1.dcloud.cisco.com**）の FQDN が、両方とも SAN として CSR に追加されます。

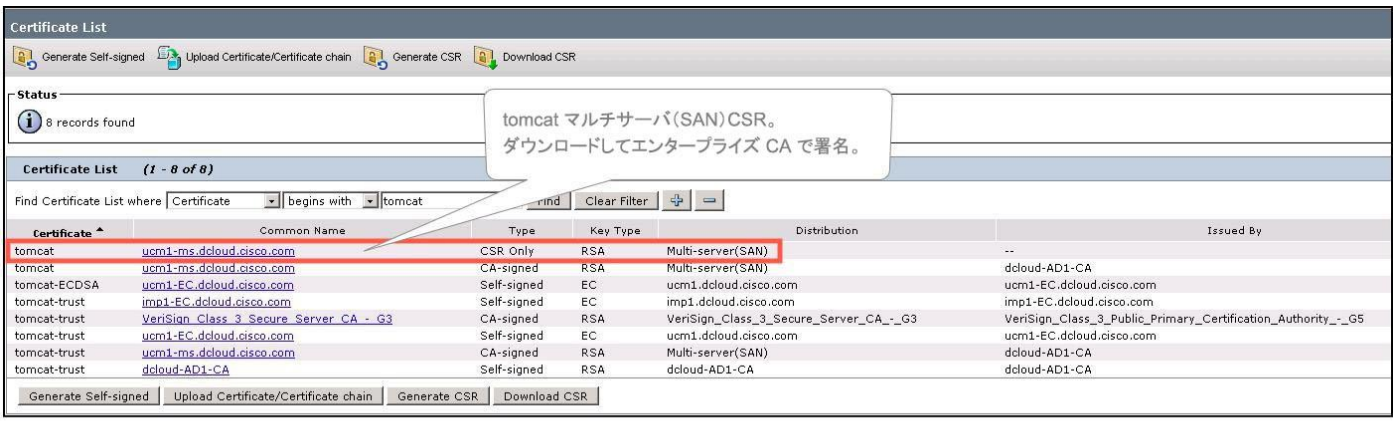
図 6 に示すように、その他すべての値はデフォルトのままにし（長さとハッシュ アルゴリズムはそれぞれ 2048 と SHA256）、[生成（Generate）] をクリックします。

図 6. Unified CM：tomcat マルチサーバ証明書署名要求の生成



CSR が作成されたら、[閉じる（Close）] をクリックします。これで、証明書リストをリロードすると、生成した tomcat CSR が表示されます（図 7 を参照）。

図 7. Unified CM：tomcat CSR



注：証明書リストをリロードするには、必要に応じて [検索（Find）] をクリックします。

マルチサーバ SAN 証明書によって、証明書の署名プロセスが効率化されます。マルチサーバ証明書を利用すれば、同じクラスタ内の複数のノードで、同じ CA 署名付き証明書が使用され、署名して配布しなければならない証明書の数が少なくなります。今回のケースでは、1 つのマルチ SAN CA 署名付き tomcat 証明書（ucm1-ms.dcloud.cisco.com）が、2 つの Unified CM/IM and Presence クラスタノード（Unified CM パブリッシャ/サブスクライバ/TFTP（ucm1.dcloud.cisco.com）と Unified CM IM and Presence パブリッシャ/サブスクライバ（imp1.dcloud.cisco.com））で使用されます。これらの 2 つのノードは、両方の tomcat 接続でマルチサーバ tomcat 証明書を共有します。

次の表 3 は、コラボレーション アプリケーション ノード用の CA 署名付きマルチサーバ SAN 証明書に関するエンタープライズ コラボレーション PA の推奨事項を示しています。

表 3. 推奨される CA 署名付きマルチサーバ SAN 証明書

製品	証明書	留意事項
Unified CM と Unified CM IM and Presence	tomcat	クラスタ内のすべての Unified CM と Unified CM IM and Presence ノードで共有される証明書
Unified CM	CallManager	CallManager サービスを実行するすべての Unified CM クラスタ ノードで共有される証明書
Unified CM IM and Presence	cup-xmpp	すべての Unified CM IM and Presence クラスタ ノードで共有される証明書
Unified CM IM and Presence	cup-xmpp-s2s	すべての Unified CM IM and Presence クラスタ ノードで共有される証明書
Unity Connection	tomcat	両方の Unity Connection クラスタ ノードで共有される証明書

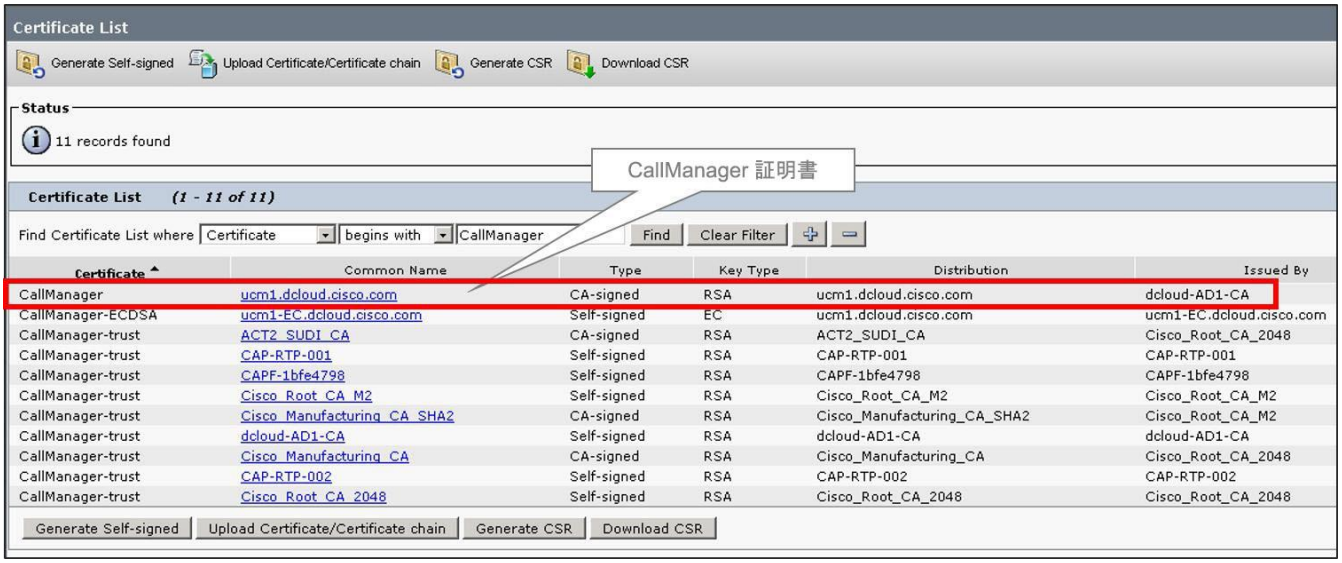
注：マルチサーバ SAN 証明書の CSR が生成され、署名付きマルチサーバ SAN 証明書が関連のパブリッシャ ノードにアップロードされたら、別のノードが今後クラスタに追加された場合、マルチサーバ SAN 証明書を再生成する必要があります（新しいマルチサーバ SAN CSR、新しい署名付きマルチサーバ SAN 証明書）。

ラボのエンタープライズ CA を使用して tomcat CSR に署名する前に、まず CallManager の CSR を生成し、エンタープライズ CA で両方の CSR を合わせて署名しましょう。

3. CallManager CSR を生成する

[証明書リスト（Certificate List）] ページ（[セキュリティ（Security）] > [証明書の管理（Certificate Management）]）で、図 8 に示すように、「**CallManager**」で始まる証明書を検索します。

図 8. Unified CM の CallManager/CallManager-trust 自己署名証明書

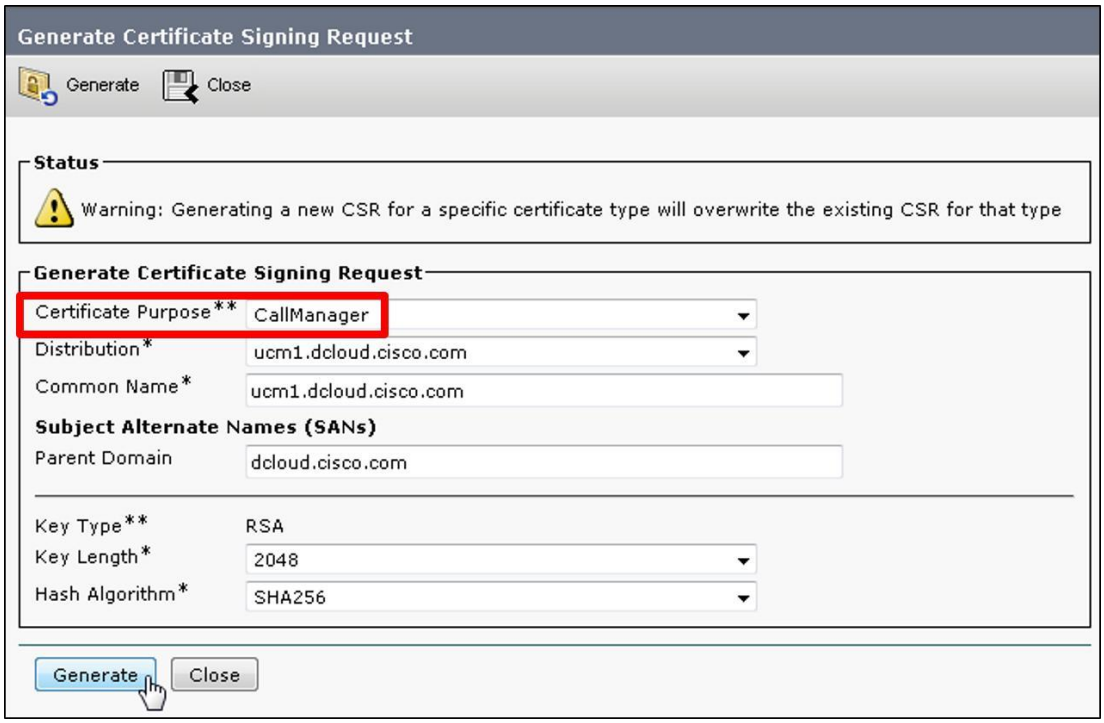


CallManager 証明書は、エンタープライズ CA によってすでに署名されていることに注意してください。今回のラボでは、新しい CA 署名付き証明書を再発行します。

[CSR の生成（Generate CSR）] をクリックします。ここでは、[証明書の用途（Certificate Purpose）] ドロップダウンから [CallManager] を選択します。その他の値はすべてデフォルトのままにし、キー長とハッシュ アルゴリズムが、図 9 に示すようにそれぞれ 2048 と SHA256 に設定されていることを再度確認します。

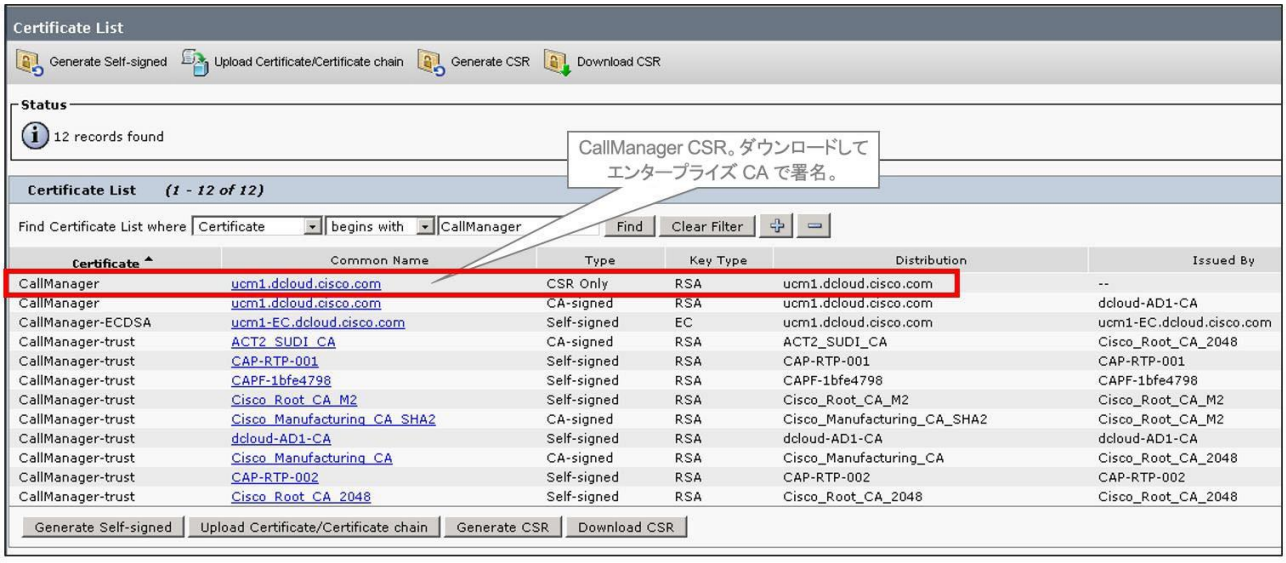
注：ラボの Unified CM クラスタ内には Unified CM ノードが 1 つしかないため、[配布（Distribution）] フィールドではマルチサーバ SAN は使用できません。先に説明したように、複数ノードの Unified CM クラスタでは、マルチサーバ SAN の CSR を生成することが可能です。

図 9. CallManager CSR の生成



[生成（Generate）] をクリックします。CSR が作成されたら、[閉じる（Close）] をクリックします。証明書リストがリロードされ、生成した CallManager CSR が表示されます（図 10 を参照）。

図 10. CallManager CSR

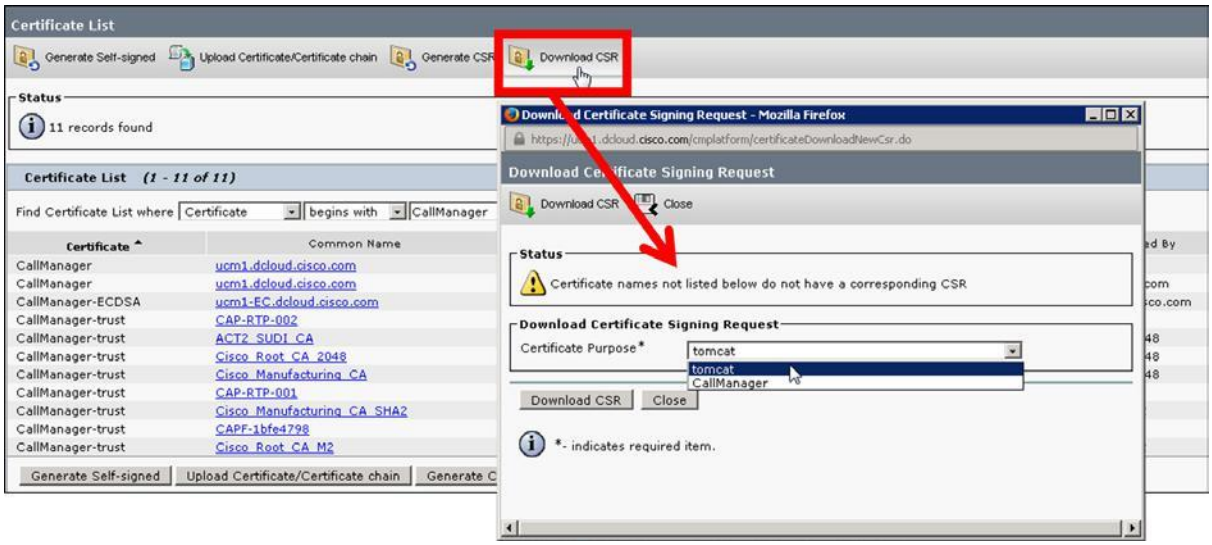


注：証明書リストをリロードするには、必要に応じて [検索（Find）] をクリックします。

4. tomcat CSR をダウンロードする

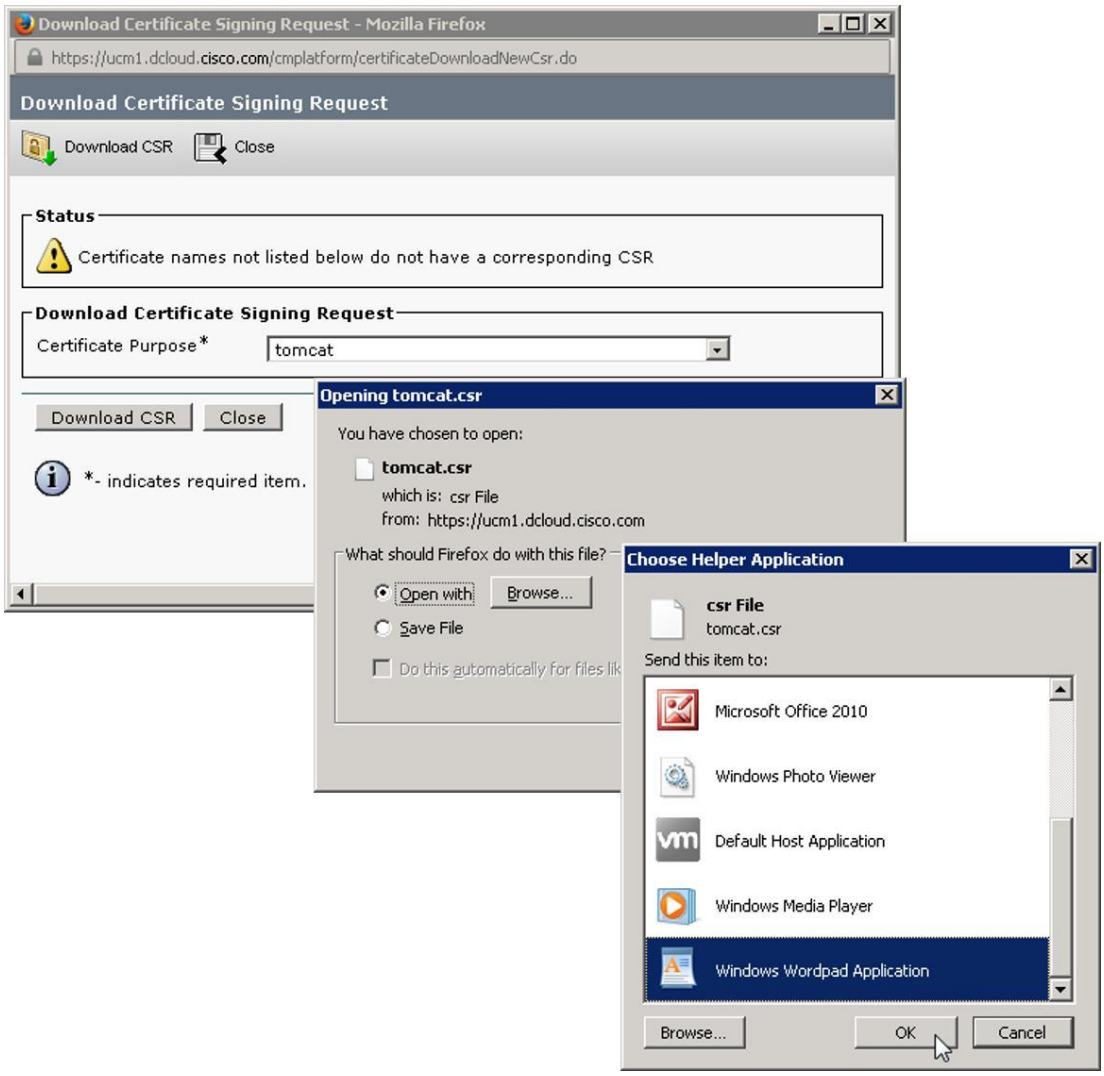
[CSR のダウンロード（Download CSR）] をクリックします。図 11 に示すように、[証明書署名要求のダウンロード（Download Certificate Signing Request）] ウィンドウの [証明書の用途（Certificate Purpose）] ドロップダウンで、[tomcat] が選択されていることを確認します。

図 11. tomcat CSR のダウンロード



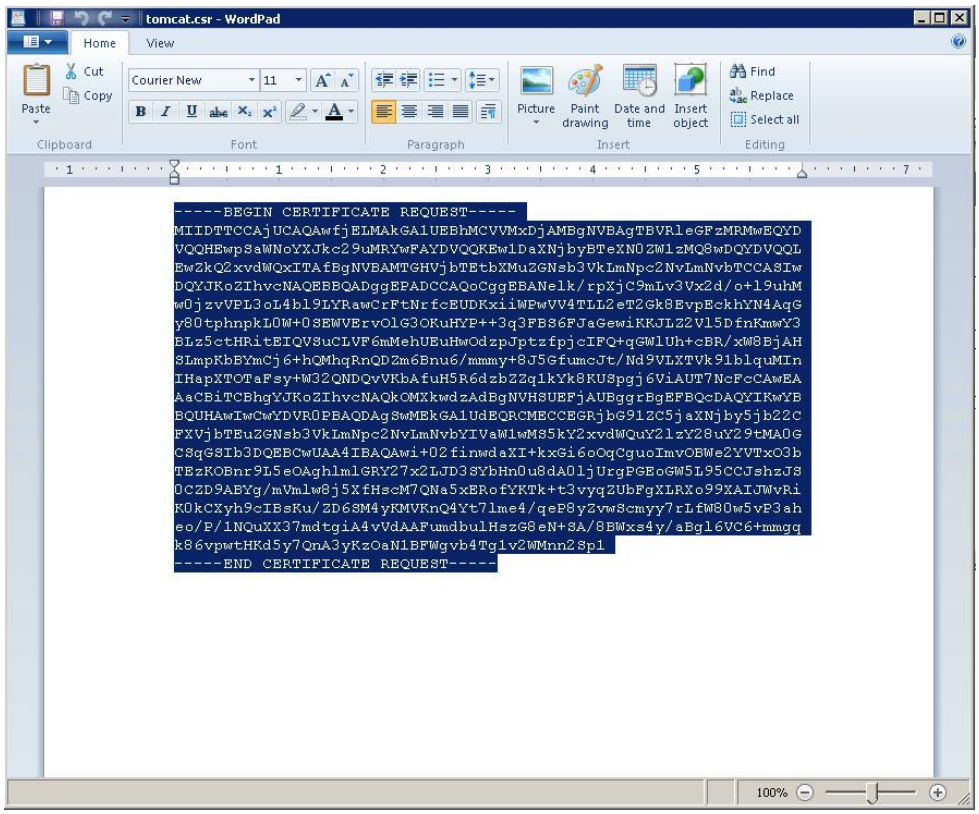
[証明書署名要求のダウンロード（Download Certificate Signing Request）] ウィンドウで、[CSR のダウンロード（Download CSR）] をクリックします。[プログラムから開く（Open with）]/[ファイルの保存（Save File）] ダイアログで、[プログラムから開く（Open with）] を選択します。[参照（Browse）] をクリックします。[Windows ワードパッドアプリケーション（Windows Wordpad Application）]（または [メモ帳（Notepad）] を選択して [OK] をクリックします（図 12 を参照）。

図 12. tomcat CSR をダウンロードして開く



[OK] をクリックして、ワードパッド（またはメモ帳）で CSR を開きます。ファイルが開いたら、ファイルの内容を選択してクリップボードにコピー（Ctrl+C）します。図 13 を参照してください。

図 13. CSR テキストのコピー*



*** 上の図の証明書署名要求文字列は、実際の CSR と異なる場合があります。**

注: CSR ファイルの内容をコピーする際に、ファイルの最後の改行またはスペースはすべて削除します。

[CSR のダウンロード(CSR Download)] ウィンドウを閉じてから次に進みます。

5. エンタープライズ Microsoft 認証局(CA)(ad1.dcloud.cisco.com)を使用し、tomcat 証明書を発行して署名する

   WKST3(198.18.133.38)で Firefox Web ブラウザを使用して、ラボのエンタープライズ Microsoft 認証局(CA)(https://ad1.dcloud.cisco.com/certsrv)にアクセスします。認証を求められたら、ユーザ名/パスワード:**administrator/C1sco12345** を使用してログインします。

[証明書を要求する（Request a Certificate）] をクリックします（図 14 を参照）。

図 14.　エンタープライズ CA で署名付き証明書を要求

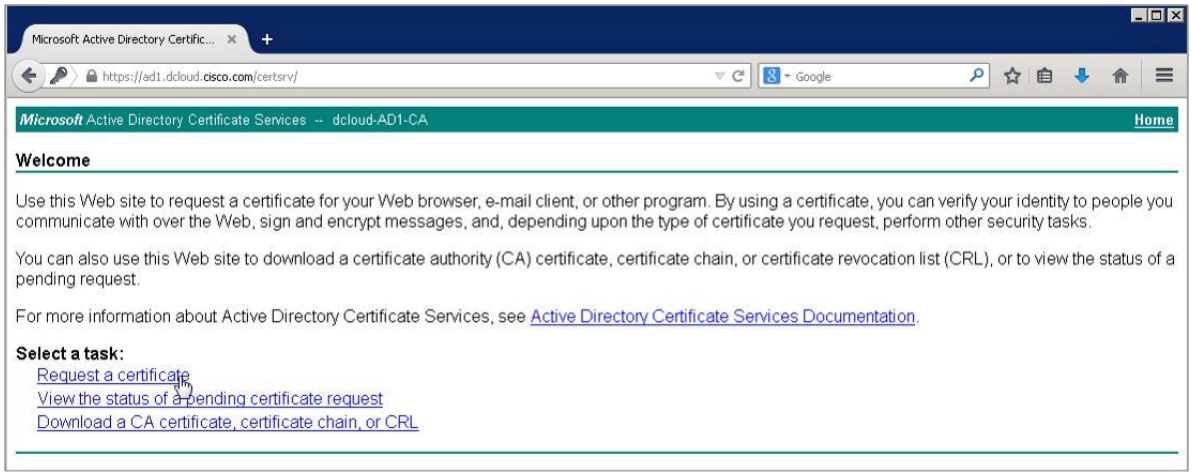
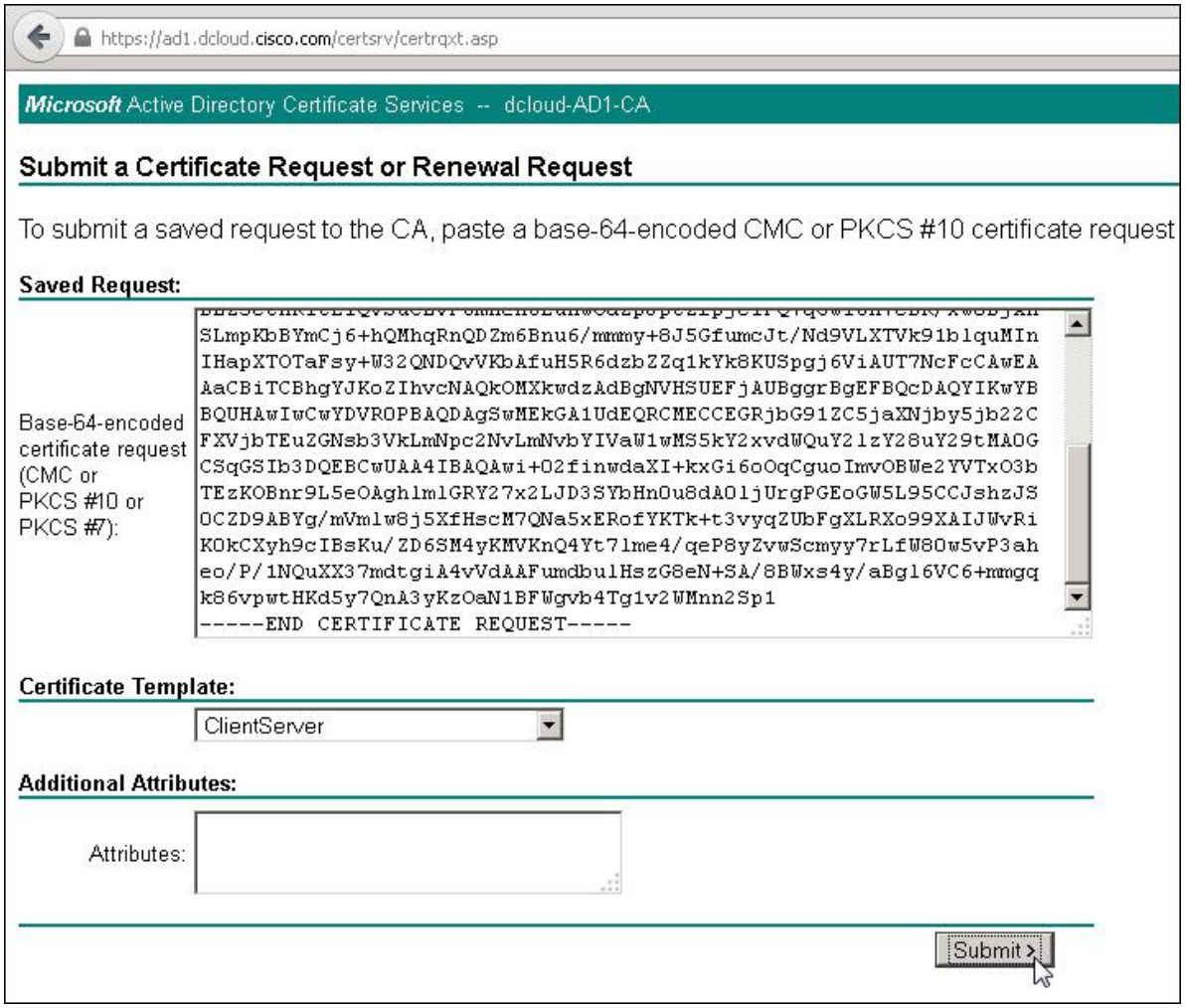


図 15 に示すように、次の画面で、[または詳細証明書要求を送信する（Or, submit an advanced certificate request）] 選択します。

図 15.　エンタープライズ CA の詳細証明書要求

（前の手順で CSR からコピーした）クリップボードの内容を、[Base-64 でエンコードされた証明書要求（Base-64-encoded certificate request）] フィールドに貼り付けます（Ctrl+V）。図 16 に示すように、[ClientServer] 証明書テンプレートを選択して [送信>（Submit >）] をクリックします。

図 16. 証明書要求の送信*

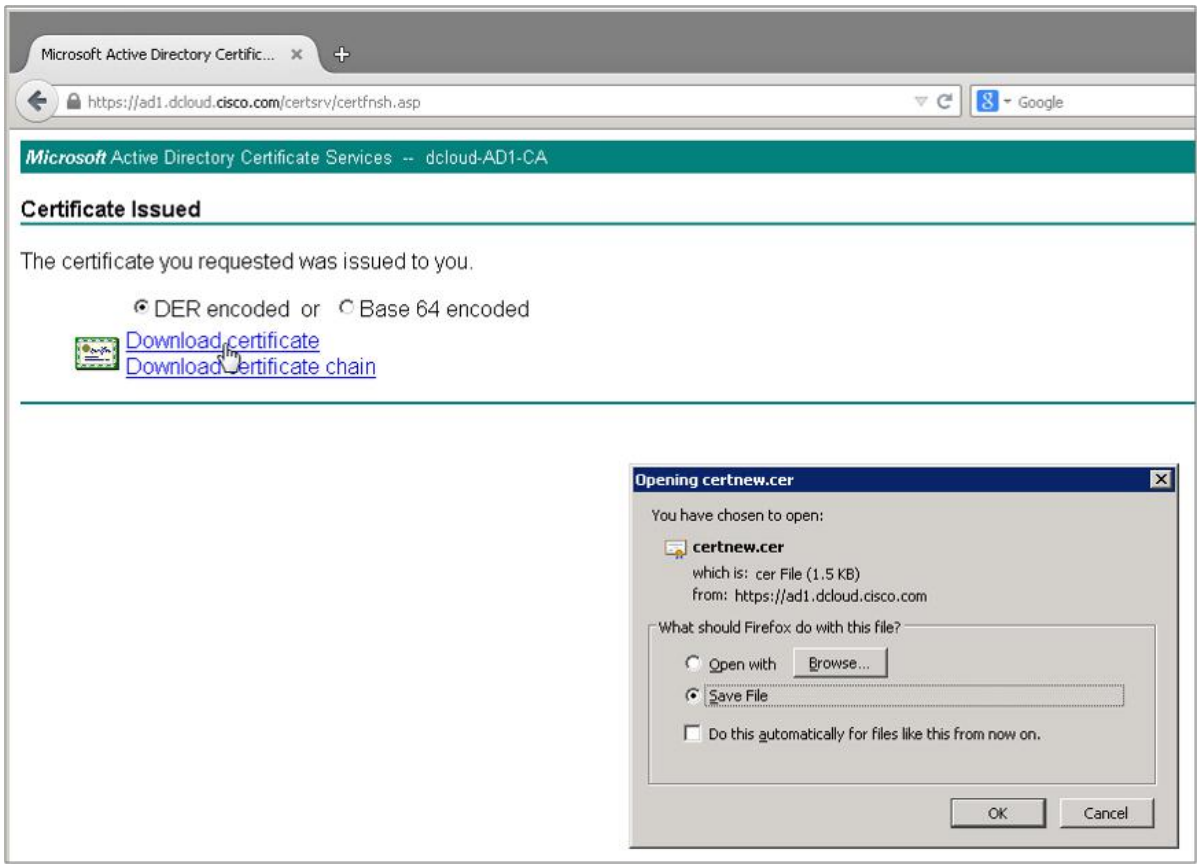


*** 上の図の証明書署名要求文字列は、実際の CSR と異なる場合があります。**

注：ラボのエンタープライズ Microsoft CA の ClientServer 証明書テンプレートは、事前に設定されています。このテンプレートには、ラボのコラボレーション X.509 証明書に必要な拡張キー使用法（EKU）属性（TLS Web サーバ認証と TLS Web クライアント認証）が含まれています。これらの属性を使用した証明書は、相互 TLS（MTLS）接続に使用できます。その場合、クライアント サイドでもサーバ サイドでも接続に証明書の検証が必要です。これによって、特定のトラフィック フローに応じて TLS 接続を設定する際に、アプリケーションがクライアントとしてもサーバとしても機能することができます。

次の画面で [DER でエンコード（DER encoded）]（デフォルト）または [Base 64 でエンコード（Base 64 encoded）] を選択し、[証明書をダウンロード（Download certificate）] をクリックします（図 17 を参照）。

図 17. 署名付き tomcat 証明書の保存



[ファイルの保存（Save File）] を選択して [OK] をクリックし、ファイルをローカル ワークステーションに保存します。ファイルに **tomcat-ms.cer** という名前をつけます。

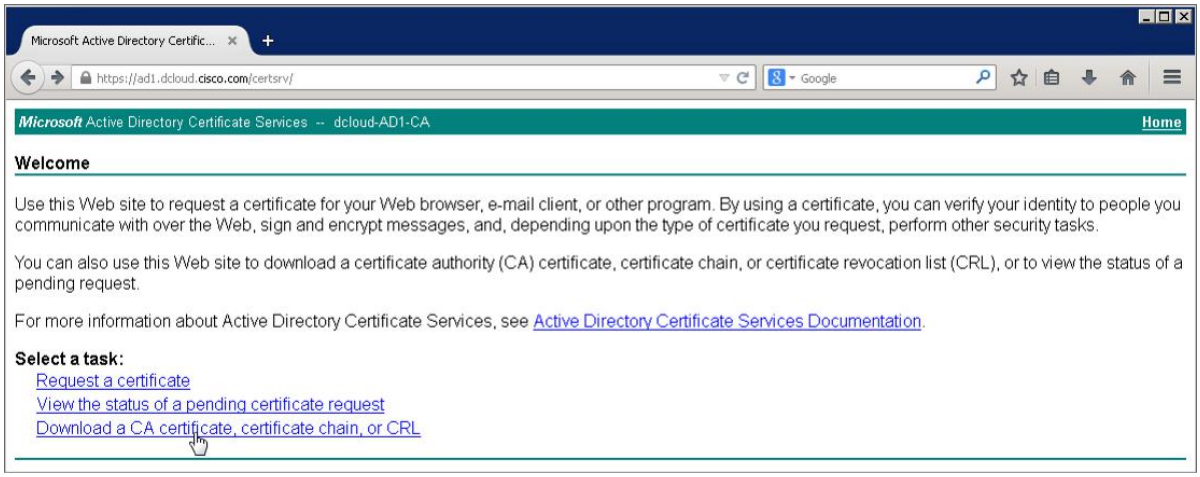
注：上記の手順 4、5 を繰り返して CallManager CSR をダウンロードし、**https://ad1.dcloud.cisco.com/certsrv/** に戻って CSR に署名後、**CallManager.cer** という名前で証明書を保存します。

WKST3 で [CSR のダウンロード（Download CSR）] ウィンドウと**ワードパッド** アプリケーション ウィンドウを閉じてから先に進みます。

6. エンタープライズ CA 証明書をダウンロードする

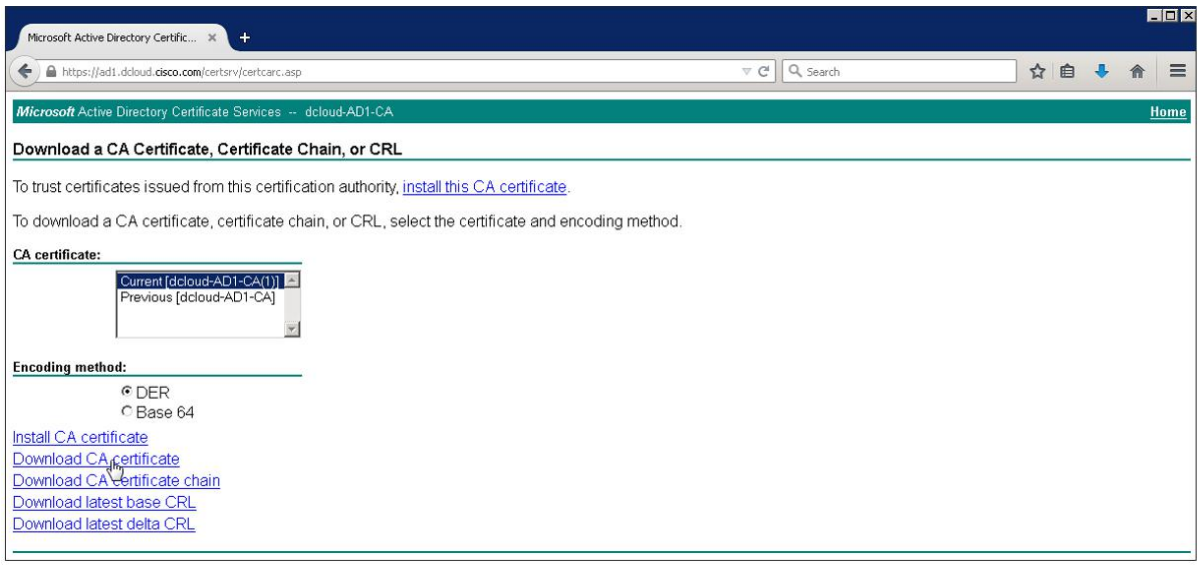
エンタープライズ認証局から離れる前に、https://ad1.dcloud.cisco.com/certsrv/ に戻り（右上隅の [ホーム（Home）] アイコンをクリック）、図 18 に示すように [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

図 18. エンタープライズ CA 証明書のダウンロード（1/2）



次の画面では [現在の[dcloud AD1 CA]（Current [dcloud-AD1-CA]）] がデフォルトで選択されており、[エンコード方式（Encoding method）] には、[DER] がデフォルトで設定されています。[CA 証明書のダウンロード（Download CA certificate）] をクリックします（図 19 を参照）。

図 19. エンタープライズ CA 証明書のダウンロード（2/2）



注：CA 証明書をダウンロードする前に、現在の CA 証明書（[現在の[dcloud-AD1-CA(1)]（Current [dcloud-AD1-CA(1)]）]）が選択されていることを確認してください。これは、前の CA 証明書に代わる新しい CA 証明書です。

[ファイルの保存（Save File）] を選択し、[OK] をクリックします。ファイルに **dCloud_CA_DER.cer** という名前をつけ、[保存（Save）] をクリックしてローカル ワークステーションに保存します。

7. エンタープライズ CA 証明書と署名付き tomcat/CallManager 証明書を Unified CM にアップロードする

これで tomcat と CallManager の証明書が発行・署名されたので、CA 証明書と合わせて Unified CM にアップロードする必要があります。

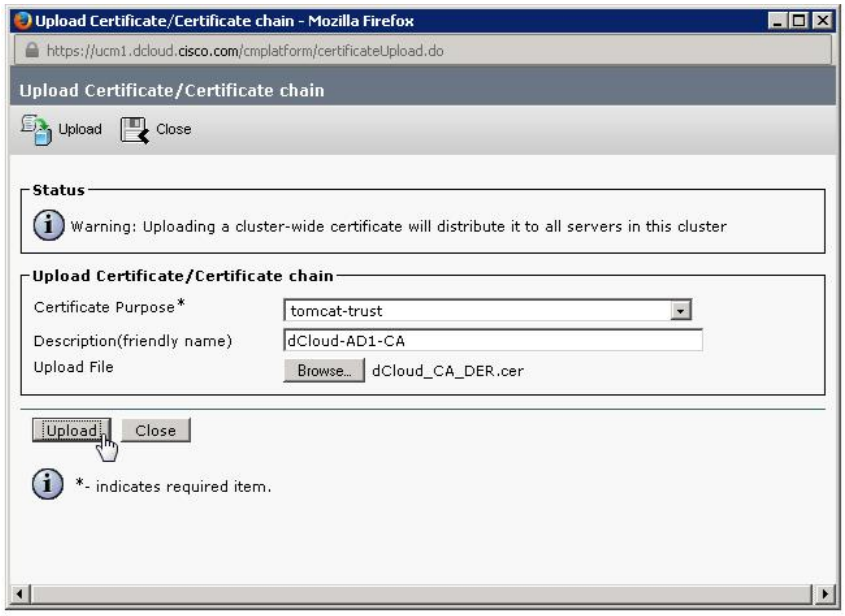
Unified CM オペレーティング システム管理インターフェイス（https://ucm1.dcloud.cisco.com/cmplatform/）に戻り、必要に応じてユーザ名/パスワード：**administrator/dCloud123!** でログインします。

[セキュリティ（Security）] > [証明書管理（Certificate Management）] を選択し、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします（図 20 を参照）。

図 20. CA 証明書、CA 署名付き tomcat/CallManager 証明書のアップロード

まず、エンタープライズ CA 証明書を、tomcat-trust 信頼ストアと CallManager-trust 信頼ストアにアップロードします。[証明書の用途（Certificate Purpose）] ドロップダウンから [tomcat-trust] を選択し、[説明（Description）] フィールドに「dCloud-AD1-CA」と入力します。次に、[参照（Browse）] をクリックして、DER エンコード証明書（C:\Users\mcheng\Downloads に保存してある証明書：**dCloud_CA_DER.cer**）を選択します。[開く（Open）] をクリックします。最後に [アップロード（Upload）] をクリックします（図 21 を参照）。

図 21. tomcat-trust 信頼ストアに CA 証明書をアップロード

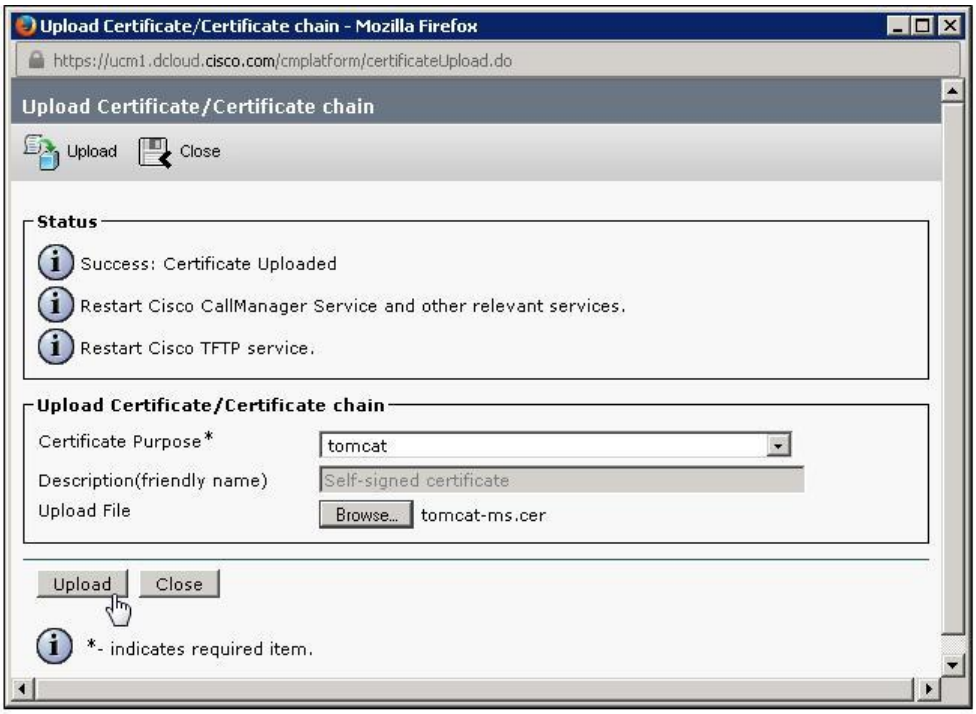


注：Cisco Tomcat サービスの再起動が必要であることを示すメッセージが表示されます。時間を節約するために、このセクションの最後で、CallManager と TFTP サービスと合わせて Cisco Tomcat サービスを再起動します。

CA 証明書が tomcat-trust 信頼ストアに正常にアップロードされたら、上記の手順を繰り返して CallManager-trust 信頼ストアに CA 証明書をアップロードします（[証明書の用途（Certificate Purpose）] ドロップダウンから [CallManager-trust] 選択）。

次に、CA 署名付き tomcat/CallManager 証明書をアップロードします。ここでは、[証明書の用途（Certificate Purpose）] ドロップダウンから [tomcat] を選択します。[参照（Browse）] をクリックし、保存してある証明書 **tomcat-ms.cer**（C:\Users\mcheng\Downloads）を選択します。[開く（Open）] をクリック後、[アップロード（Upload）] をクリックします（図 22 を参照）。

図 22. CA 署名付き tomcat 証明書のアップロード



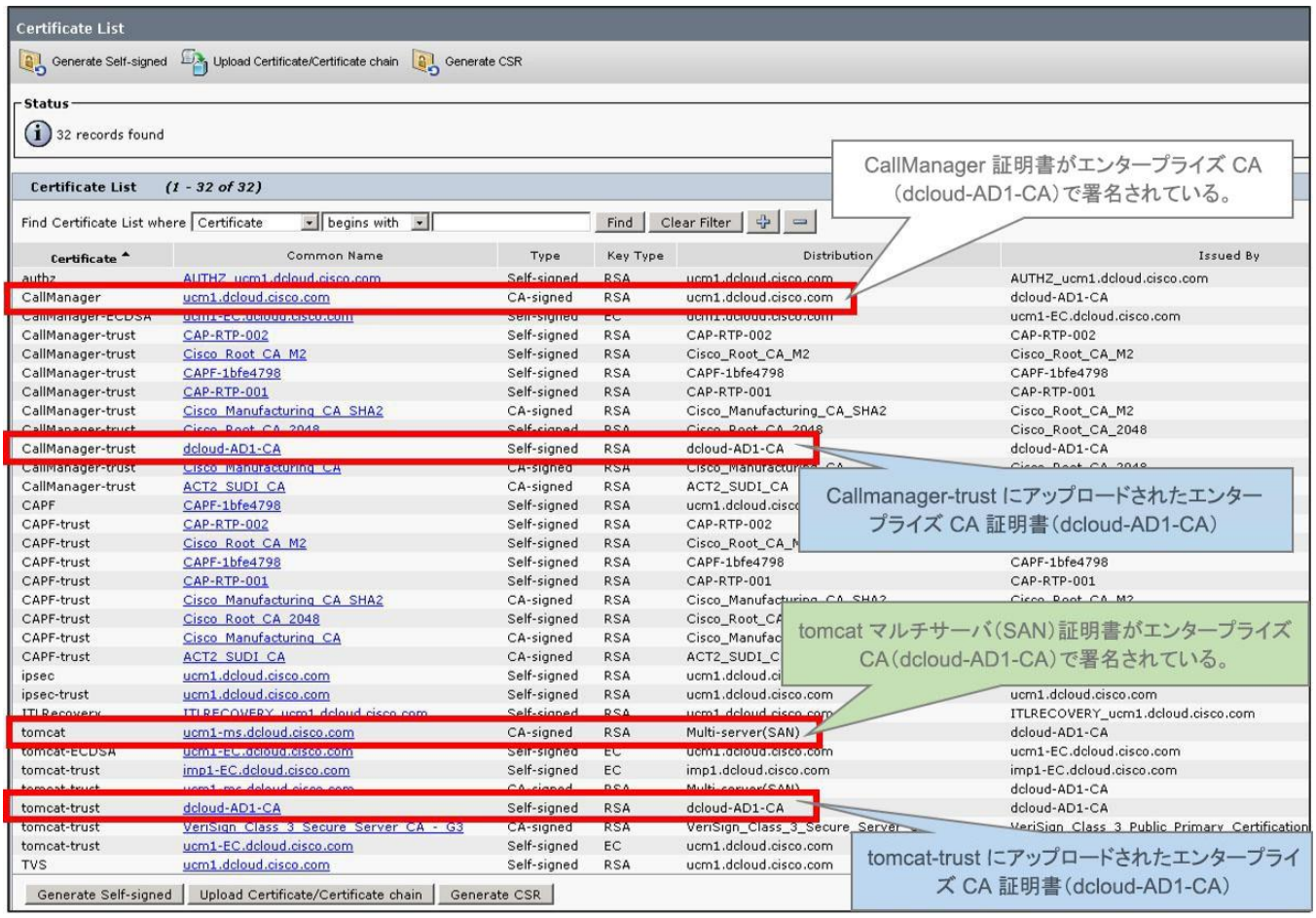
注：このセクションの最後で、Cisco CallManager と Cisco TFTP サービスと合わせて Cisco Tomcat サービスを再起動します。

アップロード ウィンドウのメッセージ（ucm1.dcloud.cisco.com、imp1.dcloud.cisco.com ノードに対する証明書アップロード操作は成功しました）で示されたように、マルチサーバ tomcat 証明書は、クラスタ パブリッシャ ノードからその他すべての該当するクラスタ ノードに自動的にプッシュされます。今回のケースでは、パブリッシャ ノード（ucm1.dcloud.cisco.com）に署名付き tomcat マルチサーバ証明書がアップロードされると、マルチサーバ SAN CSR を生成したときに SAN として追加された Unified CM IM and Presence ノード（imp1.dcloud.cisco.com）に自動的にアップロードされます。tomcat サービスを実行しているクラスタにその他の Unified CM または Unified CM IM and Presence ノードがある場合、それらのノードにも tomcat マルチサーバ証明書が自動的にアップロードされます。これらの他のクラスタ ノードも、CSR を生成した際に SAN ウィンドウに自動的に登録されています。

[証明書の用途（Certificate Purpose）] ドロップダウンから [CallManager] を選択し、上記のプロセスを繰り返して CallManager 証明書をアップロードします。アップロードするファイルとして、**CallManager.cer** を選択します。

[閉じる(Close)] をクリックし、[証明書リスト(Certificate List)] ページ([セキュリティ(Security)] > [証明書の管理(Certificate Management)]) で [次で始まる(begins with)] を空白にして [検索(Find)] をクリックし、証明書を検索します。先ほど署名した CA 署名付き tomcat 証明書と CallManager 証明書が、エンタープライズ CA 証明書と合わせて、tomcat-trust 信頼ストアと CallManager-trust 信頼ストアに表示されることを確認します(図 23 を参照)。tomcat-ms 証明書が tomcat-trust 信頼ストアに自動的にアップロードされていることも確認できます。

図 23. CallManager-trust 信頼ストアと tomcat-trust 信頼ストアにアップロードされた CallManager および tomcat マルチサーバ CA 署名付き証明書と CA 証明書



新しい CA 署名付き証明書と新しい CA 証明書をアップロードしたので、次のセクションに進む前に、Cisco TFTP、Cisco CallManager、Cisco Tomcat の各サービスを再起動する必要があります。

Unified CM サービスアビリティ ポータル(https://ucm1.dcloud.cisco.com/ccmservice/)にアクセスし、ユーザ名/パスワード:**administrator/dCloud123!** でログインします。

[ツール(Tools)] > [コントロールセンター － 機能サービス(Control Center － Feature Services)] に移動し、ドロップダウンから **ucm1.dcloud.cisco.com － CUCM Voice/Video** サーバを選択して [移動(Go)] をクリックします。移動したページで [Cisco TFTP] オプション ボタンをオンにして、[再起動(Restart)] をクリックします([OK] をクリックして再起動を確認)。「TFTP サービスが再起動して「シスコ Tftp サービスの再起動操作が成功しました(Cisco Tftp Service Restart Operation was Successful)」というメッセージが表示されたら、[Cisco CallManager] オプション ボタンをオンにして、[再起動(Restart)] を再度クリックします([OK] をクリックして再起動を確認)。

注: このラボでは CTIManager サービスを再起動する必要はありませんが、通常は再起動する必要があります。

最後に、Unified CM で Cisco Tomcat Service を再起動するために、WKST3(198.18.133.38)の PuTTY を使用して、Unified CM (ucm1.dcloud.cisco.com)コマンドライン インターフェイスに SSH で接続する必要があります。

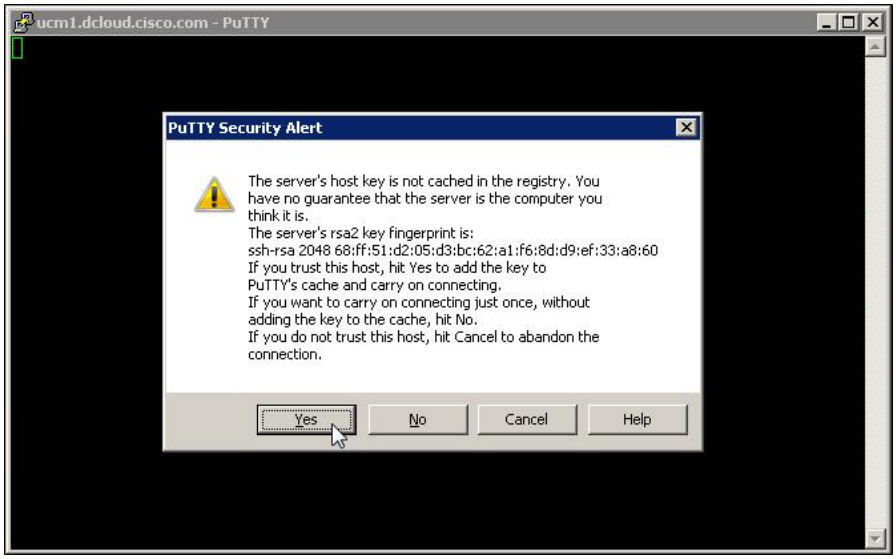
PuTTY アイコンをダブルクリックして 

起動します。[ホスト名（または IP アドレス）（Host Name (or IP Address)）] フィールドに「ucm1.dcloud.cisco.com」と入力します。

[開く（Open）] をクリックします。

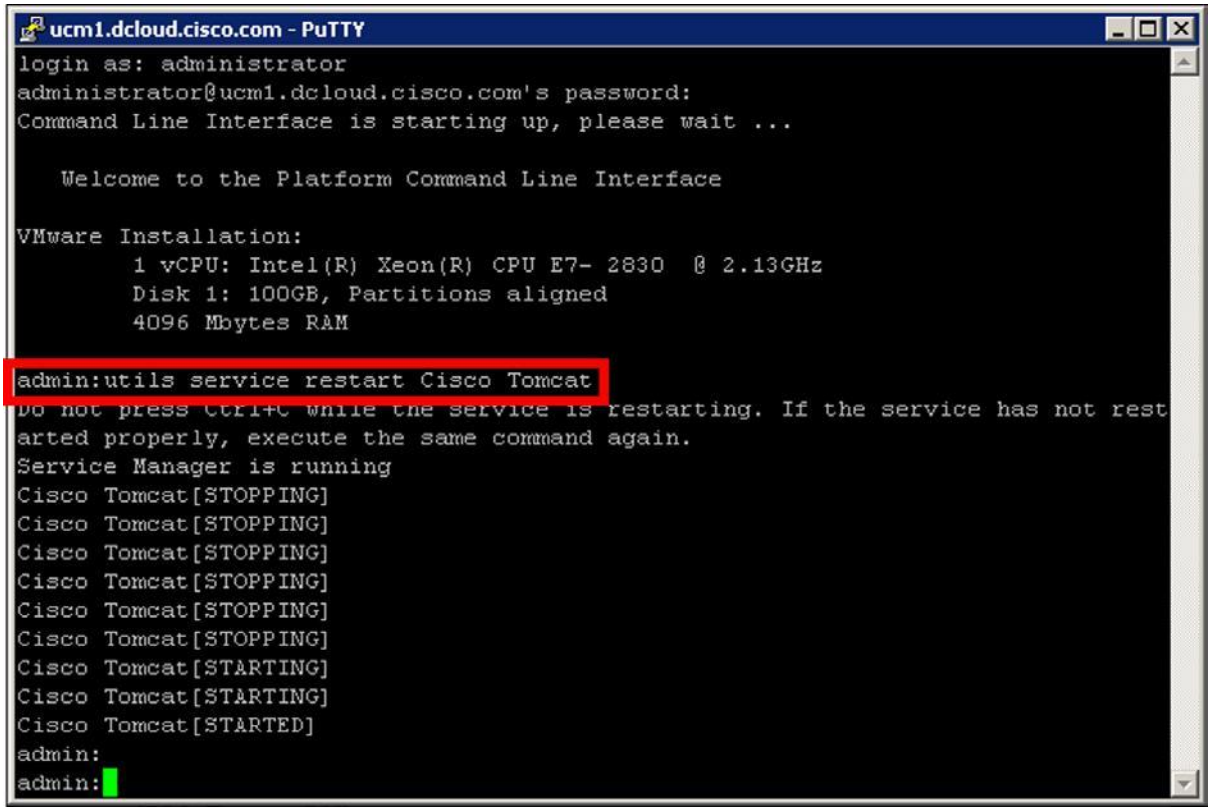
図 24 に示すように、[はい（Yes）] をクリックして ssh-rsa2 キーをキャッシュします。

図 24. Unified CM に SSH 接続する際にキーのキャッシュを確認



ユーザ名/パスワード：**administrator/dCloud123!** でログインした後、コマンド ラインで **utils service restart Cisco Tomcat** コマンドを入力します（図 25 を参照）。Cisco Tomcat サービスが再起動します。図 25 に示すように、サービスが再起動したら、**exit** と入力して、Unified CM への SSH セッションを閉じます。

図 25. Unified CM の Cisco Tomcat サービスを再起動



この時点では、Cisco Tomcat サービスは再起動していますが、完全には動作していない場合があります。ucm1 に接続すると Firefox にエラーが表示される場合は、もう少し待つ必要があります。

8. Unified CM IM and Presence クラスタ ノード（imp1.dcloud.cisco.com）にある既存の証明書を確認する

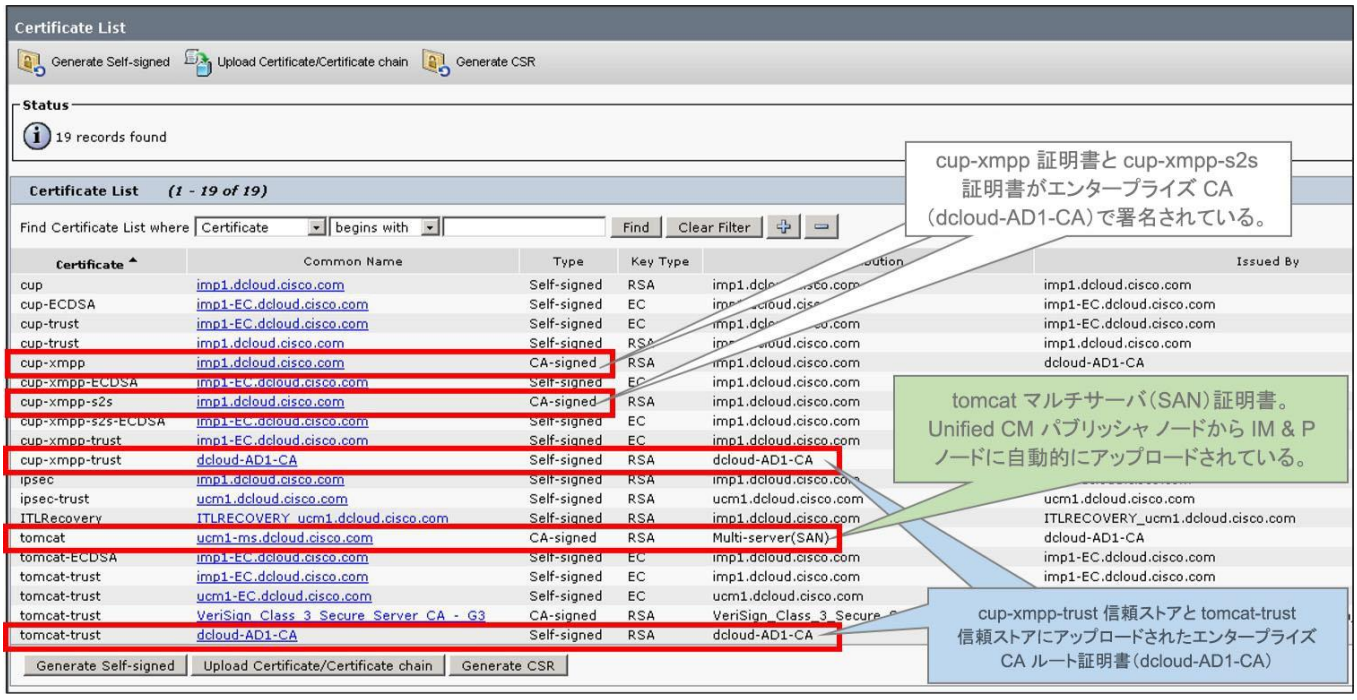
注：この手順では、Unified CM IM and Presence にある証明書を確認するだけです。関連の証明書は受講者用にすでに署名されています。この手順をスキップしても、ラボの残りの部分に影響はありません。

WKST3（198.18.133.38）で Firefox Web ブラウザを使用して新しいタブを開き、Unified IM and Presence のオペレーティング システム管理インターフェイス（https://imp1.dcloud.cisco.com/cmplatform）に移動します。ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

[セキュリティ（Security）] > [証明書の管理（Certificate Management）] の順に選択し、[検索（Find）] をクリックします。

図 26 に、Unified CM OS 証明書管理インターフェイスと、システム証明書のリストを示します。

図 26. Unified CM IM and Presence 証明書リスト



Cisco Unified CM IM and Presence のセキュリティでは、エンタープライズ コラボレーション PA で示したように、デフォルトの自己署名証明書を使用せず、認証局(CA)が署名した証明書をシステムにインストールすることがベスト プラクティスになります。パブリック CA または民間のエンタープライズ CA によって、次の証明書に署名する必要があります。

- tomcat
- cup-xmpp
- cup-xmpp-s2s

上記の図 26 に示すように、すでに署名した tomcat マルチサーバ証明書が自動的にアップロードされています。さらに、ラボのエンタープライズ CA によって cup-xmpp 証明書がすでに署名され、エンタープライズ CA 証明書(dCloud-AD1-CA)がすでに cup-xmpp および tomcat 信頼ストアにアップロードされています。

前述のように、マルチサーバ SAN 証明書によって証明書の管理がシンプルになります。今回のケースでは、ラボの Unified CM ノードと Unified CM IM and Presence ノードの両方で、同じ CA 署名付き証明書を tomcat 接続に使用しています。

次に、Unified CM の場合と同じ手順を繰り返し、ラボの Unified CM IM and Presence(IM & P)ノードで Cisco Tomcat サービスを再起動します。WKST3(198.18.133.38)で PuTTY を使用して、Unified CM IM and Presence サーバ(imp1.dcloud.cisco.com)のコマンド ライン インターフェイスに SSH でアクセスします。

PuTTY アイコンをダブルクリックして 

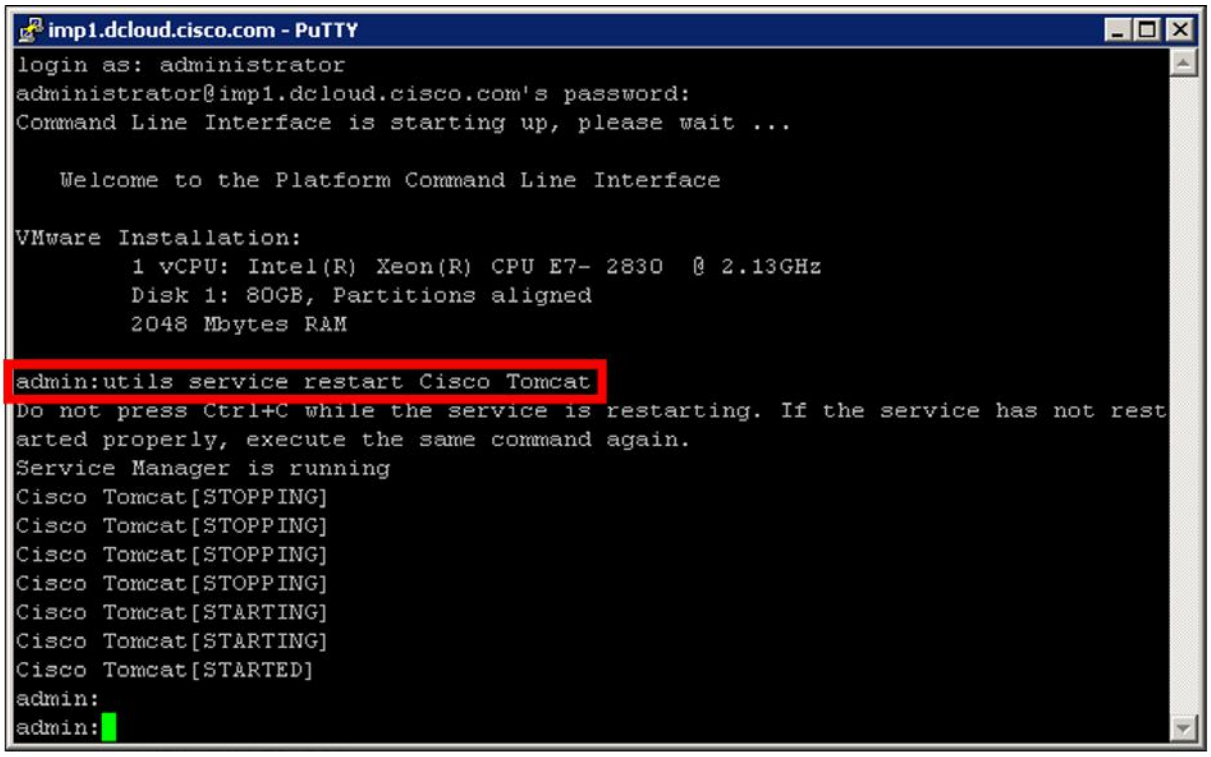
起動します。[ホスト名(または IP アドレス)(Host Name (or IP Address))] フィールドに「**imp1.dcloud.cisco.com**」と入力します。

[開く(Open)] をクリックします。

[はい(Yes)] をクリックして ssh-rsa2 キーをキャッシュします。

ユーザ名/パスワード：**administrator/dCloud123!** でログインした後、コマンド ラインで **utils service restart Cisco Tomcat** コマンドを入力します（図 27 を参照）。Cisco Tomcat サービスが再起動します。図 27 に示すようにサービスが再起動されたら、**exit** と入力して、Unified CM IM and Presence への SSH セッションを閉じます。

図 27. Unified CM IM and Presence の Cisco Tomcat サービスを再起動



注：Cisco Tomcat サービスが再起動して、さまざまな Web 管理インターフェイスが利用できるようになるまでには数分かかる場合があります。

Cisco Tomcat サービスが再起動されたら、CLI で **exit** と入力して SSH セッションを閉じます。

B. セキュアな LDAP のプロビジョニング

これで Unified CM の tomcat と CallManager 証明書の署名を完了し、その証明書およびエンタープライズ CA 証明書を適切な Unified CM 信頼ストア（および使用するブラウザ）にアップロードできました。次に、Unified CM とエンタープライズ LDAP ディレクトリの間のセキュアな接続を確保し、Unified CM と Active Directory（ad1.dcloud.cisco.com）間のトラフィックが、TLS を使用して暗号化されるようにする必要があります。

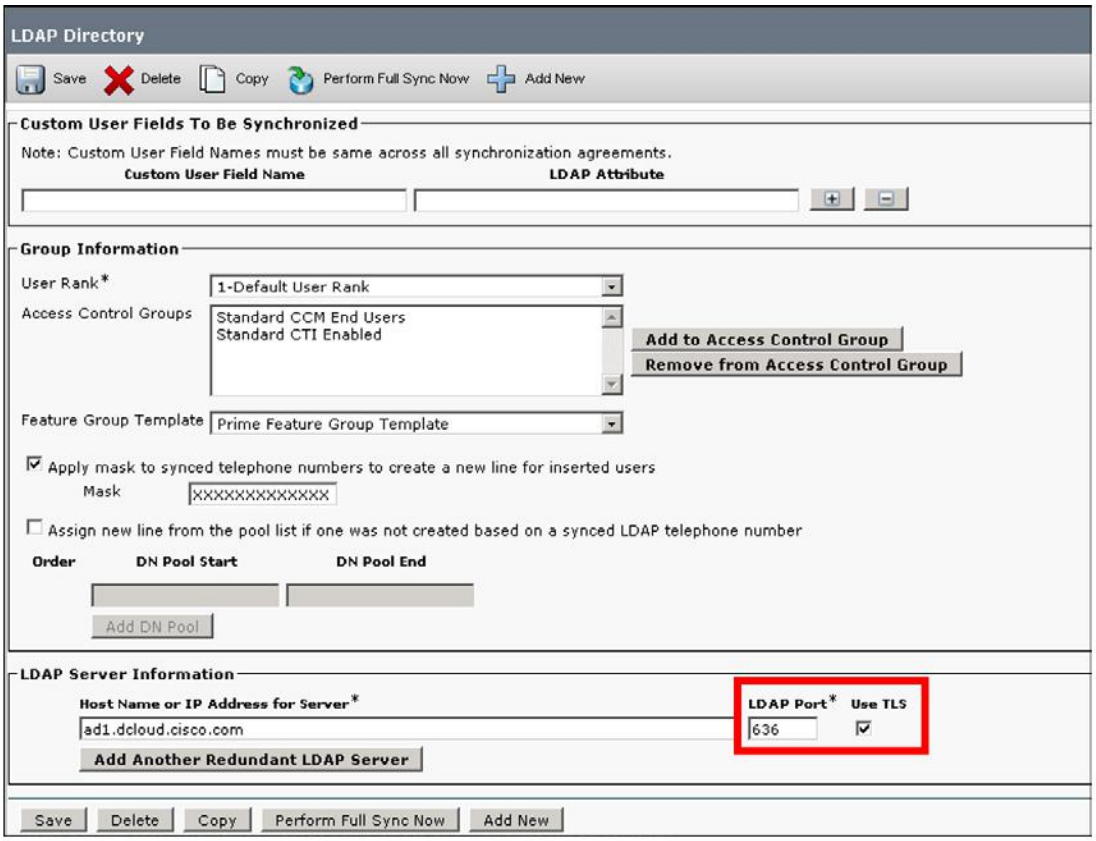
9. Unified CM と LDAP 間のセキュアな接続を設定する

   Unified CM 管理ポータル（https://ucm1.dcloud.cisco.com/ccmadmin/）にアクセスし、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

   HTTP ステータス 404 エラー メッセージが表示された場合、tomcat サービスがまだ完全に再起動していません。数分後に、もう一度やり直してください。

   [システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）] の順に移動し、[検索（Find）] ボタンをクリックして、LDAP ディレクトリ リストを取得します。[Prime LDAP]（LDAP の設定名）をクリックして設定ページを開きます。ページの下部までスクロールし、図 28 に示すように、[TLS を使用（Use TLS）] チェックボックスをオンにし、[LDAP ポート（LDAP Port）] フィールドを、デフォルトの 389 から 636 に変更します。[保存（Save）] をクリック後、[今すぐ完全同期（Perform Full Sync Now）] をクリックします。[OK] をクリックして LDAP 同期警告を確認し、同期を開始します。

図 28. TLS を使用した LDAP ディレクトリ接続の保護



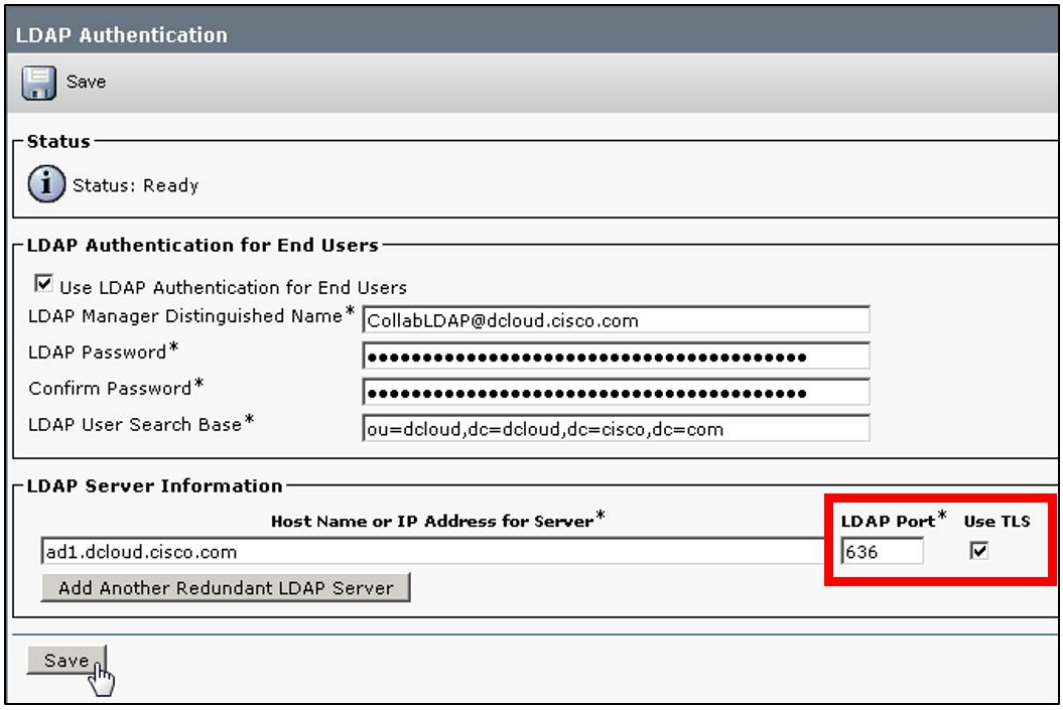
注: 今回のケースでは、Windows の Microsoft Active Directory ドメイン コントローラ（DC）ポートに対して LDAP 同期を実施します。グローバル カタログ（GC）に同期する場合は、LDAP ポート番号は 389 ではなく 3268 になり、セキュアな LDAP ポート番号は 636 ではなく 3269 になります。DC および GC の動作とポート番号に関する詳細については、https://technet.microsoft.com/en-us/library/cc978012.aspx [英語] を参照してください。

これで Unified CM は、LDAP ディレクトリ（ad1.dcloud.cisco.com/198.18.133.1）と安全に通信し、Active Directory の証明書を検証することができます。Active Directory の証明書は、エンタープライズ CA（dCloud-AD1-CA）によって署名され、エンタープライズ証明書が tomcat-trust 信頼ストアにすでにロードされているからです。

注: LDAP ディレクトリの TLS 設定を保存する際にエラーが表示された場合は、システムの tomcat 証明書に問題があることを示しています。前の手順の tomcat マルチサーバ SAN 証明書の操作を再度確認してください。

次に、TLS を使用してセキュアな LDAP 認証を確保するために、[システム（System）] > [LDAP] > [LDAP 認証（LDAP Authentication）] の順に移動して同じ設定を行います。図 29 に示すように、[TLS を使用（Use TLS）] チェックボックスをオンにし、[LDAP ポート（LDAP Port）] フィールドを、デフォルトの 389 から **636** に変更します。[保存（Save）] をクリックします。

図 29. TLS を使用して Unified CM と LDAP ディレクトリ間の認証接続を保護



これで、エンド ユーザが LDAP サーバから認証された際に、Unified CM と LDAP ディレクトリの間の認証トラフィックは暗号化されます。

***** モジュール #1 の終了 *****

モジュール 2　輸出管理対象となる暗号化機能のスマート ライセンス

モジュールの概要

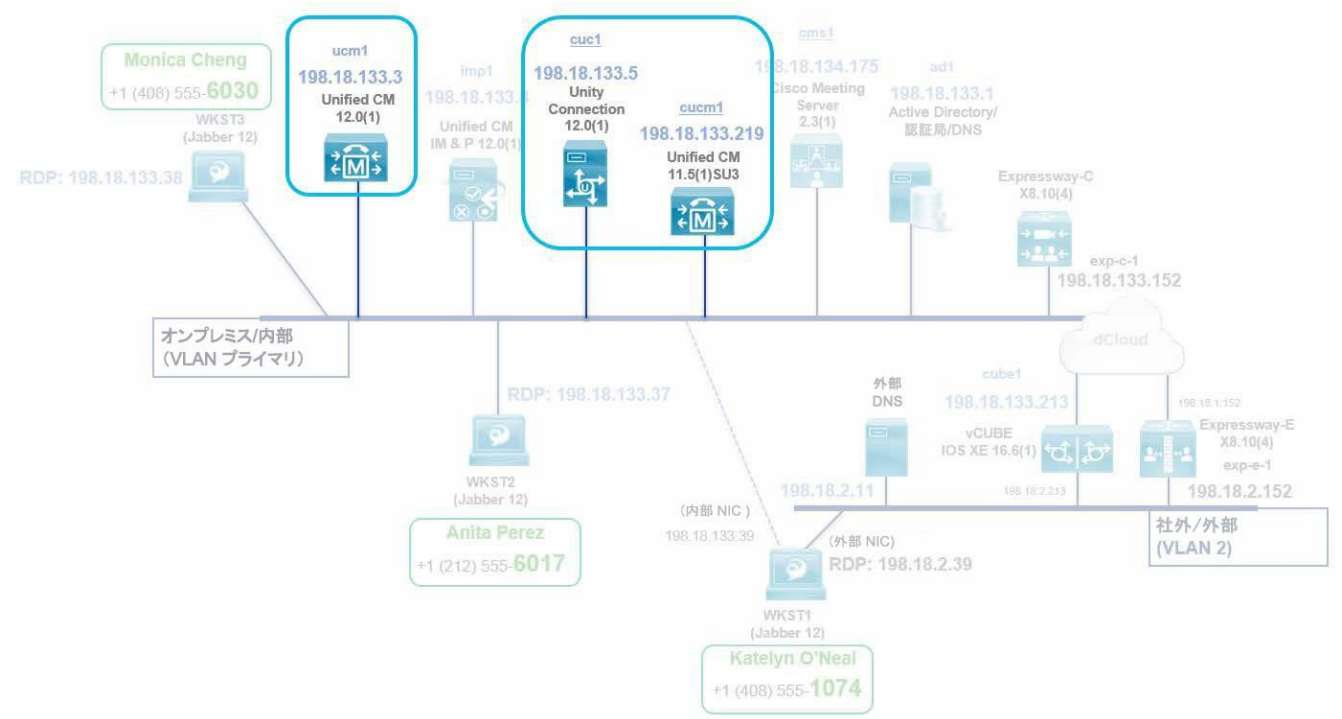
11.5(1) SU3 および 12.0 以降のライセンスに関していくつか変更があります。このモジュールは次の 2 つのセクションに分かれています。

A. Unified CM 11.5(1) SU3 以降の暗号化ライセンス

B. Unified CM および Unity Connection 12.0 の輸出管理機能を許可したスマート ライセンス

次の図 31 では、このモジュールに関連するコンポーネントとトポロジを示しています。

図 31.　モジュール 2：輸出管理対象となる暗号化機能のスマート ライセンスのトポロジ



セクション

注：このモジュールでは、ライセンス操作のほとんどはすでに実施されています。ここでは、必要な操作を示すことが目的です。このラボの次のモジュールに進むために必要なのは、パート B の手順 6 のみです。

A. Unified CM 11.5(1) SU3 用の暗号化ライセンス

Unified CM 用の暗号化ライセンスは、11.5(1) SU3 から導入されています。このリリースでは、混合モードで Cisco Unified Communications Manager を実行するために暗号化ライセンスが必要です。

混合モードの Unified CM クラスタを 11.5(1) SU3 にアップグレードした場合は、アップグレードの直後に、暗号化ライセンスが必要なことを示す警告メッセージがユーザ インターフェイスに表示されます。混合モードで引き続きシステムは稼働しますが、CTL ファイルをアップデートすることはできず、暗号化ライセンスをインストールするか、クラスタのセキュリティ設定を非セキュア モードに戻すまで警告が表示され続けます。シスコでは、できるだけ早く暗号化ライセンスをインストールし、警告が表示されずに混合モードで運用できるようにすることをお勧めします。

アップグレード時に混合モードで実行していなかった場合は、暗号化ライセンスを Cisco Unified Communications Manager に適用して同期が完了するまで、クラスタを混合モードにすることはできません。暗号化ライセンスは無料で発注できます。詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/11_5_1/SU3/cucm_b_release-notes-cucm-imp-1151su3/cucm_b_release-notes-cucm-imp-1151su3_chapter_01.html#reference_B203B3DDDC4F060BB3661BEB0D34E9E4

このセクションでは、11.5(1) SU3 が稼働している **cucm1（ucm1 ではない）**を使用し、次の手順を実施します。

1. 暗号化ライセンスがない状態で、混合モードを有効にしようとします。これは失敗します。
2. Cisco Prime License Manager（PLM）に暗号化ライセンスをインストールします。
3. 混合モードを有効にします。今度は成功します。

注：Unity Connection 11.5(1) SU3 でも暗号化ライセンスが導入されています。このラボでは説明しませんが、手順は Unified CM 11.5(1) SU3 と同様です。Unity Connection の詳細については、Cisco Unity Connection リリース 11.x のセキュリティ ガイド（https://www.cisco.com/c/ja_jp/support/unified-communications/unity-connection/products-user-guide-list.html）を参照してください。

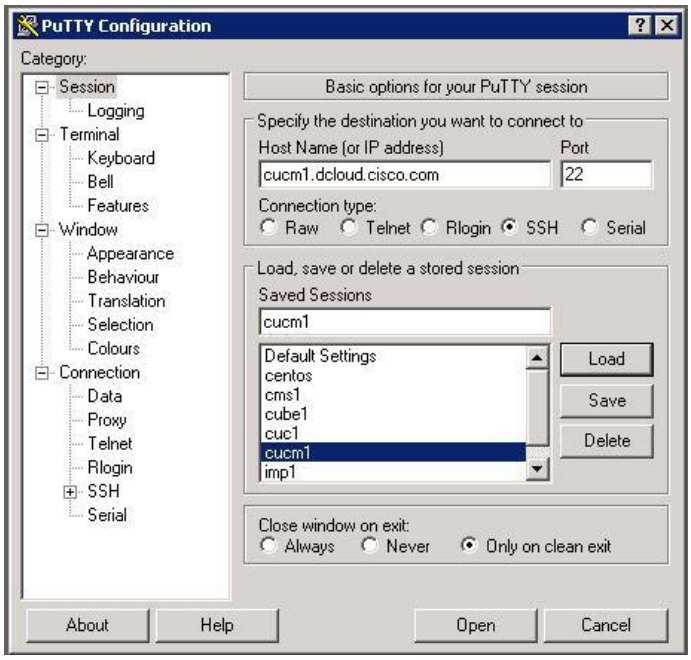
1. 暗号化ライセンスがない状態で混合モードを有効にする

   WKST3（198.18.133.38、ユーザ名/パスワード：**DCLOUD\mcheng/C1sco12345**）に RDP 接続します。

   PuTTY アイコン  をダブルクリックして起動します。[ホスト名（または IP アドレス）（Host Name (or IP Address)）] フィールドに **cucm1.dcloud.cisco.com** と入力するか、リストにあればそこから選択して、**cucm1.dcloud.cisco.com** に接続します。[開く（Open）] をクリックします（図 32 を参照）。

注：これは 11.5(1) SU3 を実行中の **cucm1.dcloud.cisco.com** です。12.0(1) が実行されている ucm1.dcloud.cisco.com ではありません。

図 32. PuTTY：cucm1 に SSH で接続



セキュリティ アラート ウィンドウが表示されたら、図 33 に示すように、[はい（Yes）] をクリックして ssh-rsa2 キーをキャッシュします。

図 33. Unified CM に SSH 接続する際にキーのキャッシュを確認

ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

CLI で **utils ctl set-cluster mixed-mode** コマンドを入力し、クラスタを混合モードに移行させます。プロンプトが表示されたら、「**y**」を入力して Enter を押し、続行することを確認します。PLM に暗号化ライセンスがないため、このコマンドは失敗します。図 34 を参照してください。

注：Y と入力しても、Y が画面に表示されない場合があります。その場合は、Y を入力した後にそのまま Enter を押してください。動作しない場合は、もう一度やり直してください。図 34 に示すように、最終的にコマンドは終了します。

図 34. Unified CM 11.5(1) SU3：暗号化ライセンスがないため混合モード クラスタでコマンドが失敗

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to c
ontinue? (y/n):

Command cannot be executed because this Unified Communications Manager cluster is unable to obtain an Encryption License.
 Please ensure an Encryption License is installed on the Prime License Manager this cluster is associated to and this UCM
 cluster has been synchronized.

Note: PLM must be upgraded to the latest version that supports the Encryption License.

admin:
```

2. Cisco Prime License Manager（PLM）に暗号化ライセンスをインストールする

次の手順では、暗号化ライセンスのライセンス要求を生成し、暗号化ライセンスを PLM にインストールします。このラボでは、手動履行モードを使用します。全体としては、次の手順を実行する必要があります。

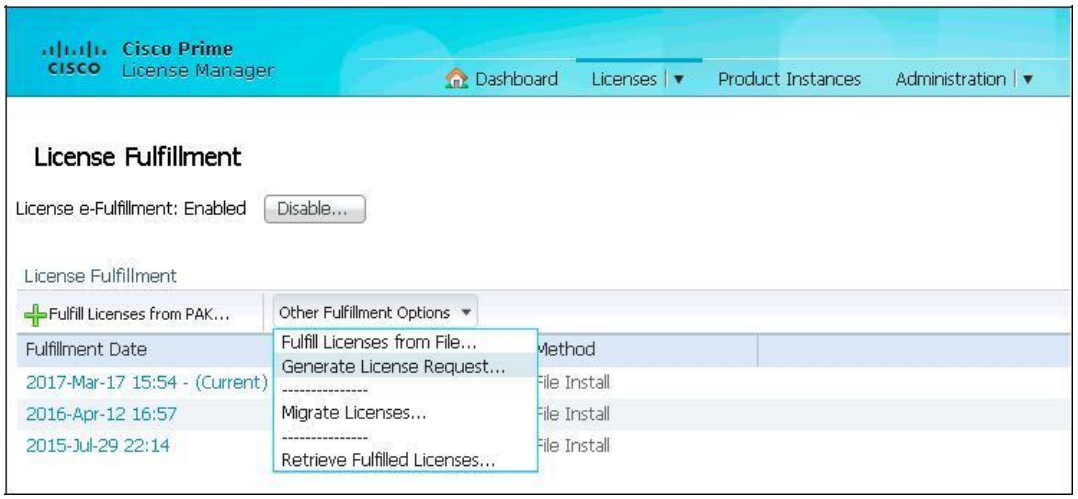
1. ENC PAK ライセンス ファイルを取得する。
2. PLM でライセンス要求を生成する。
3. [製品ライセンス登録（Product License Registration）] ページで PAK 情報とライセンス要求情報を入力してライセンス ファイルを取得する。
4. PLM で新しい暗号化ライセンス ファイルをインストールする。

WKST3（198.18.133.38、ユーザ名/パスワード：DCLOUD**mcheng/C1sco12345**）に RDP 接続します。WKST3 で Firefox Web ブラウザを起動し、**cucm1**（https://cucm1.dcloud.cisco.com）の FQDN を入力します。[Cisco Prime License Manager] をクリックし、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

注：このラボでは、手順と関連のスクリーンショットを提示するだけです。ライセンス要求の生成とライセンス ファイルの取得に関する手順は**実施しません**。ライセンス ファイルはすでに生成され、受講者のポッド ワークステーションにダウンロードされています。次に必要な手順が記載されている、図 42 の次の注まで以降の手順をスキップできます。

[ライセンス（Licenses）] > [履行（Fulfillment）] に移動します。このページでは、図 35 に示すように、[その他の履行オプション（Other Fulfillment Options）] > [ライセンス要求の生成...（Generate License Request...）] を選択します。

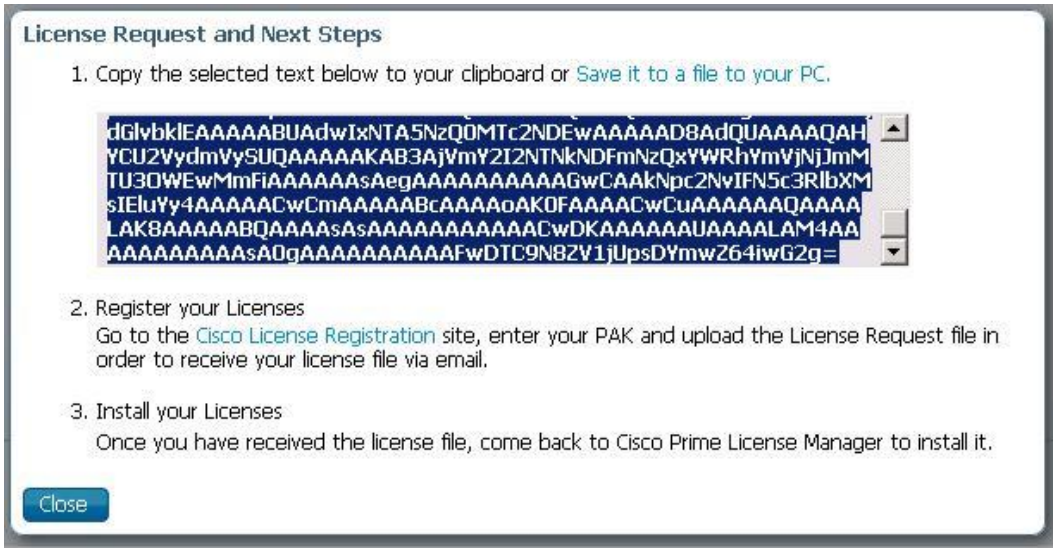
図 35. Prime License Manager：ライセンス要求の生成*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

この操作を完了する場合は、図 36 に示すように、選択したテキストをクリップボードにコピー（Ctrl+C）します。

図 36. Prime License Manager：ライセンス要求のコピー*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

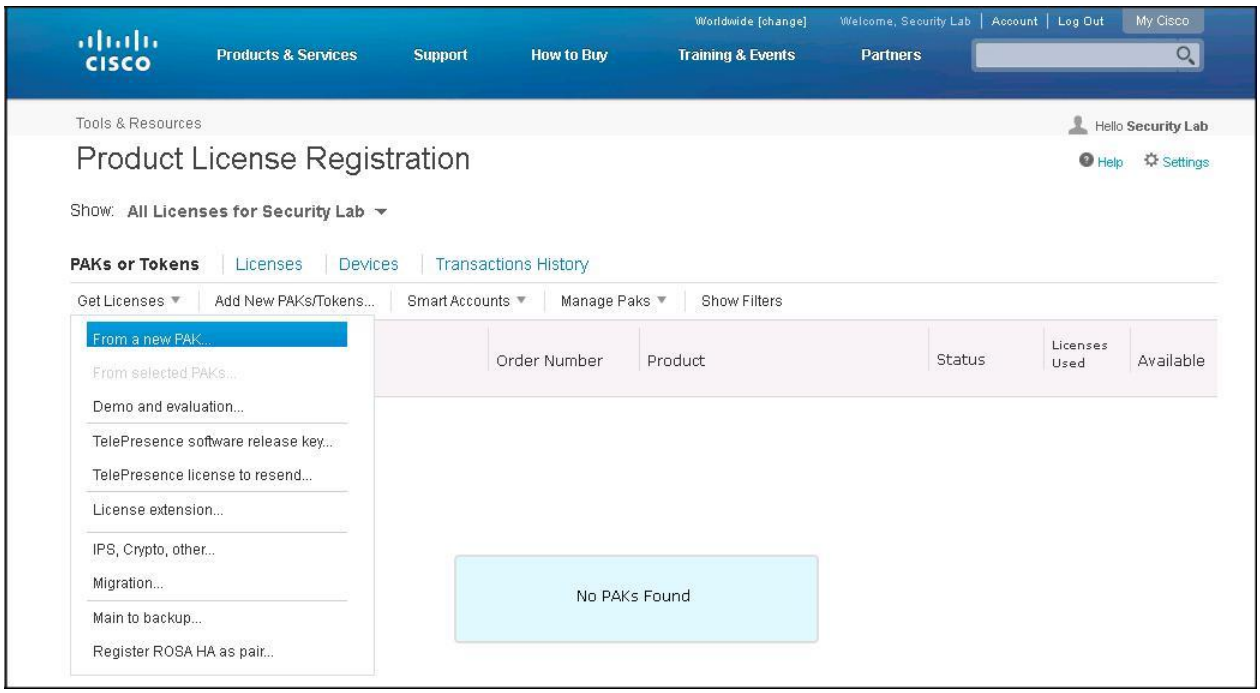
次に、[シスコライセンス登録（Cisco License Registration）] リンクをクリックします。ブラウザで新しいタブが開きます。**実際の導入では、この Web サイトで操作を続行してライセンス要求を生成します。このラボではすでに実行されています。**

注：サーバがインターネットにアクセスできる場合、[ファイルからライセンスを履行（Fulfill Licenses from File）] オプションの代わりに、[PAK からライセンスを履行（Fulfill Licenses from PAK）] オプションを選択することもできます。

[ライセンスの登録（License Registration）] サイトでは、最初にいくつかのお知らせウィンドウを閉じる必要があります。その後、[セキュリティラボのすべてのライセンス（All Licenses for Security Lab）] をクリックします。

図 37 に示すように、[ライセンスの取得（Get Licenses）] > [新しい PAK から...（From a new PAK...）] をクリックします。

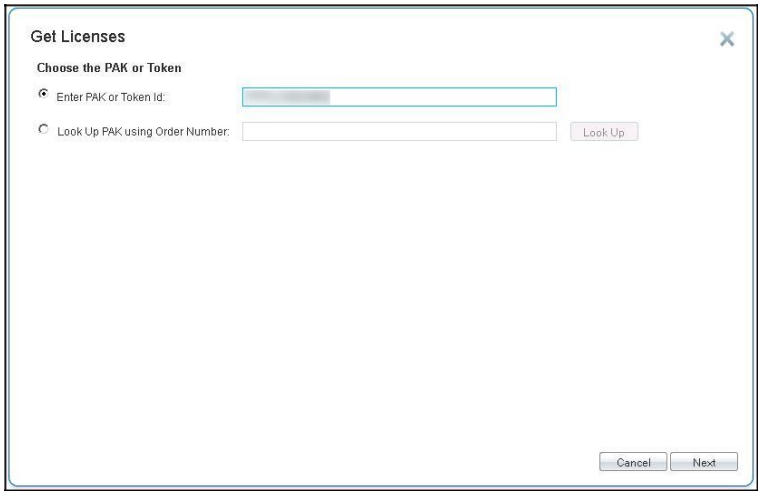
図 37. 新しい PAK からライセンスを取得*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

PAK を入力して [Next（次へ）] をクリックします。このラボでは、PAK またはトークン ID を提供しないため、この手順を実施することはできません。図 38 ～ 42 を参照してください。手順に関する画面を示しています。

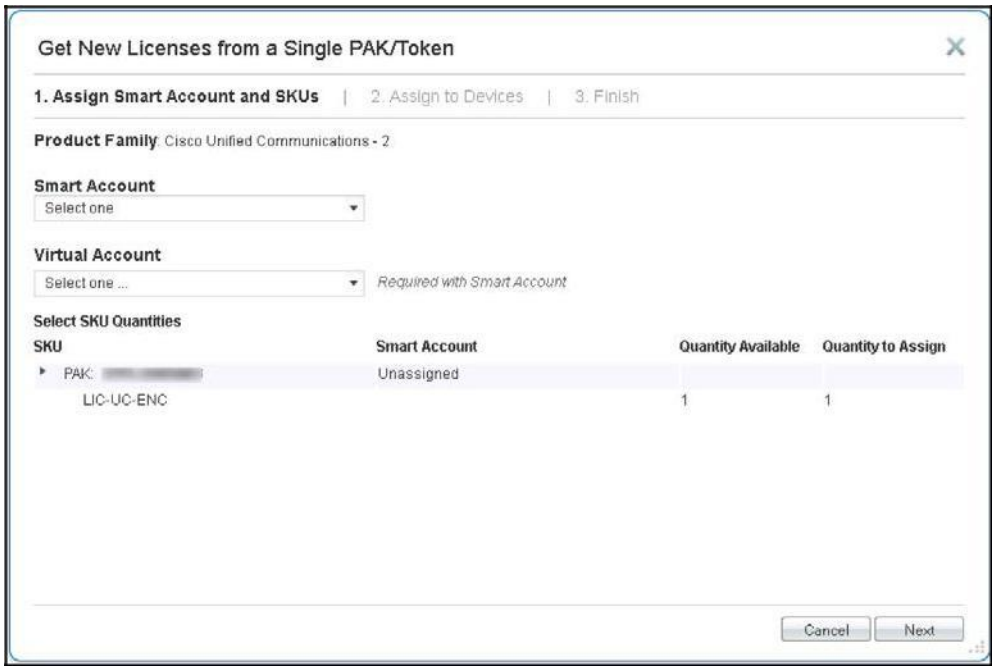
図 38. 製品ライセンス登録用に PAK を入力する*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

[次へ（Next）] をクリックします。

図 39. LIC-UC-ENC に割り当てられていない PAK の表示*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

[次へ（Next）] をクリックします。

PLM から提供されるライセンス要求の内容を貼り付けます（図 40 を参照）。

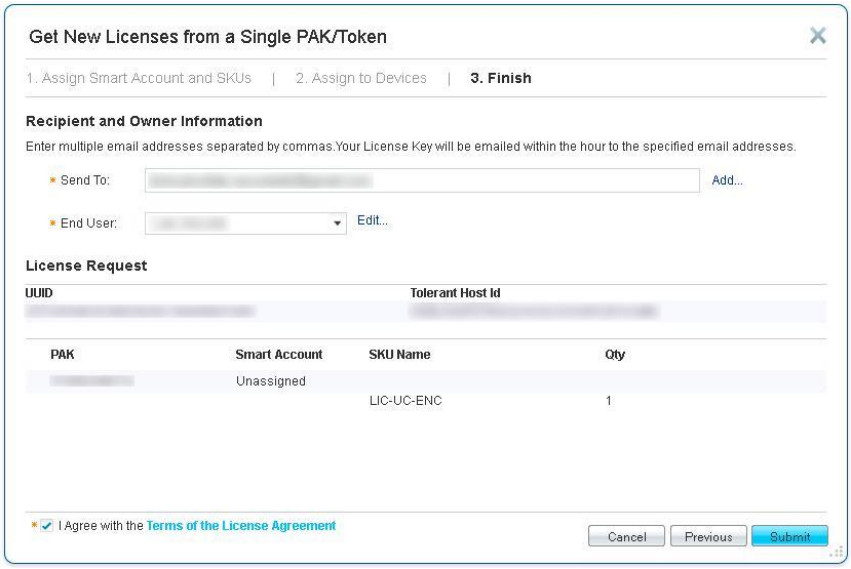
図 40. ライセンス要求の内容を貼り付けて新しいライセンスに関する操作を完了する*

* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

[次へ（Next）] をクリックします。

図 41 に示すように、次の画面に表示される情報が正しいことを確認します。確認したら、[ライセンス契約書の条項に同意します（I Agree with the Terms of the License Agreement）] チェックボックスをオンにして [送信（Submit）] をクリックします。

図 41. ライセンス契約書に同意する*

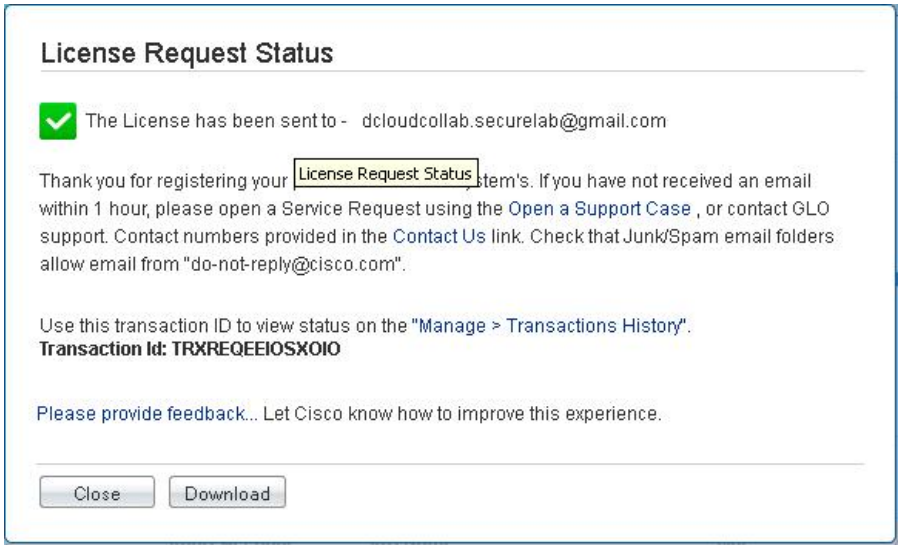


* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

[送信（Submit）] をクリックします。図 42 に示すように、ライセンス要求のステータス画面に戻ります。

[ダウンロード（Download）] をクリックしてデスクトップにライセンス ファイルをダウンロードします。

図 42. ライセンス要求に対する応答とステータス画面*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

繰り返しになりますが、このラボではライセンス ファイルはすでに生成されています。ライセンス ファイルは、WKST3（198.18.133.38、ユーザ名/パスワード：**DCLOUD\mcheng/C1sco12345**）の **Download** フォルダにダウンロードされています。ライセンス ファイルは、受講者に便利なように、WKST2（198.18.133.37）にもダウンロードされています。

注：上記の手順では、ライセンス要求を生成してライセンス ファイルを取得するための手順と関連のスクリーンショットを示しています。ライセンス ファイルはすでに生成され、受講者のポッド ワークステーションにダウンロードされています。ここで PLM に移動し、既存のライセンスをアップロードします。

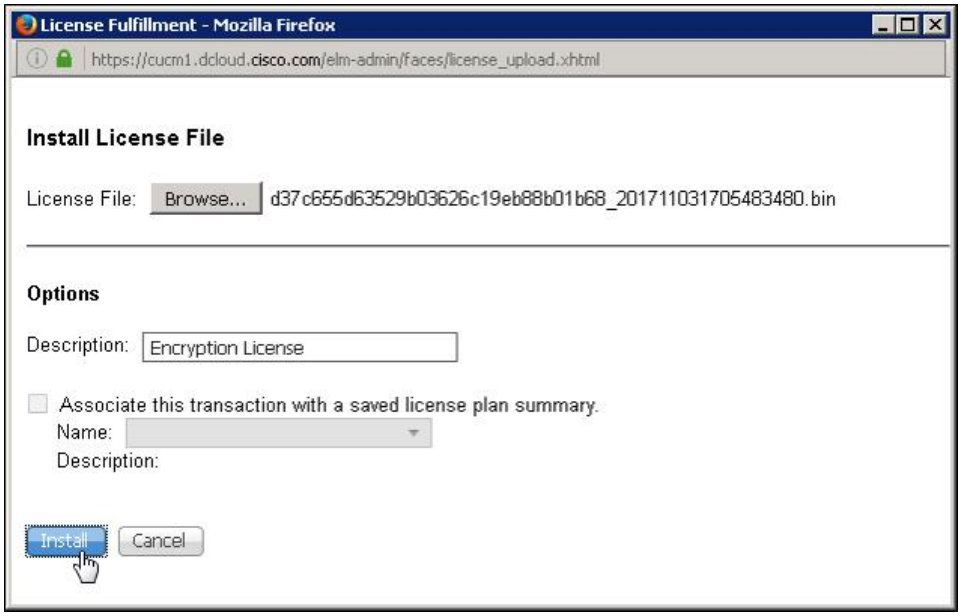
PLM（https://cucm1.dcloud.cisco.com/elm-admin、ユーザ名/パスワード：**administrator/dCloud123!**）に戻ります。

[ライセンス（Licenses）] > [履行（Fulfillment）] に移動します。このページで、[その他の履行オプション（Other Fulfillment Options）] > [ファイルからライセンスの履行...（Fulfill licenses from File...）] を選択します。

図 43 に示すように、[参照...（Browse...）] をクリックして、ライセンス ファイルを選択します。今回のケースでは、Download フォルダにある、**d37c655d63529b03626c19eb88b01b68_201711031705483480.bin** というファイルを選択します。[開く（Open）] をクリックします。

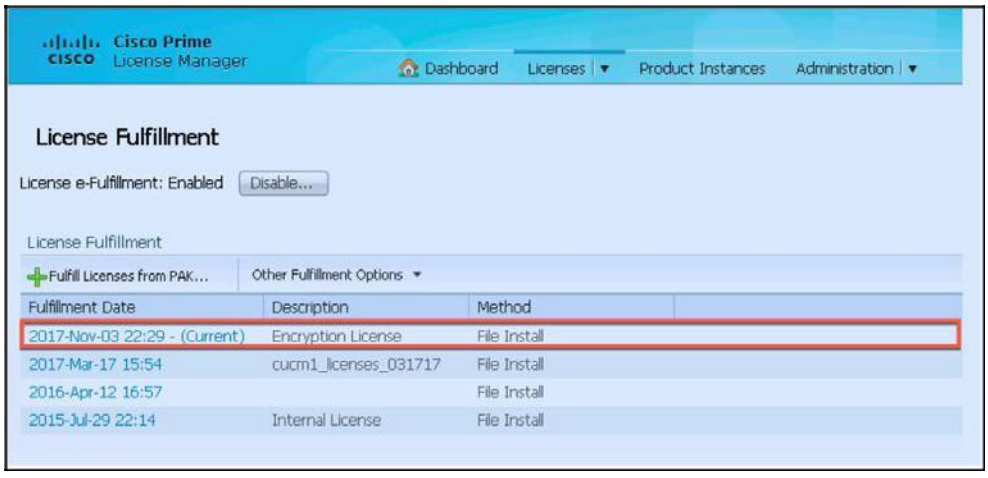
ライセンス ファイルの説明を入力し（「暗号化ライセンス」など）、[インストール（Install）] をクリックします（図 43 を参照）。

図 43. Prime License Manager：ライセンスの履行



ウィンドウを閉じ、PLM に戻ります。暗号化ライセンスが表示されます（以下の図 44 を参照）。

図 44. Prime License Manager：暗号化ライセンスの履行の確認

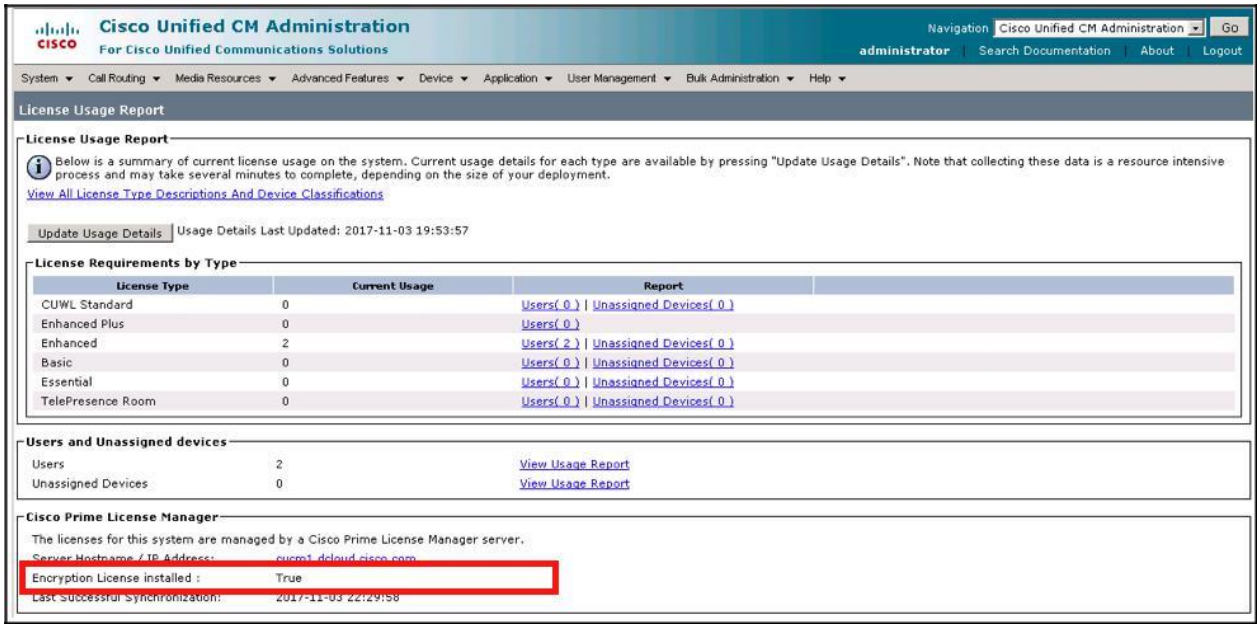


通常は、[製品インスタンス（Product Instances）] タブで [今すぐ同期（Synchronize Now）] クリックして、PLM のライセンスを同期します。今回のケースでは、PLM は cucm1.dcloud.cisco.com と共存しているため必要ありません。

ここで、Unified CM にライセンスが正しくインストールされていることを確認します。

Unified CM の管理インターフェイス（https://cucm1.dcloud.cisco.com/ccmadmin）にログインします（ユーザ名/パスワード：**administrator/dCloud123!**）。[システム（System）] > [ライセンス（Licensing）] > [ライセンス使用状況レポート（License Usage Report）] に移動します。図 45 に示すように、[暗号化ライセンスがインストール済み（Encryption License installed）] フィールドに [はい（True）] が表示されていることを確認します。

図 45. 暗号化ライセンスが Unified CM に正常にインストールされていることの確認



これで、暗号化ライセンスが正常にインストールされました。

3. Unified CM 11.5(1) SU3 で混合モードを有効にする

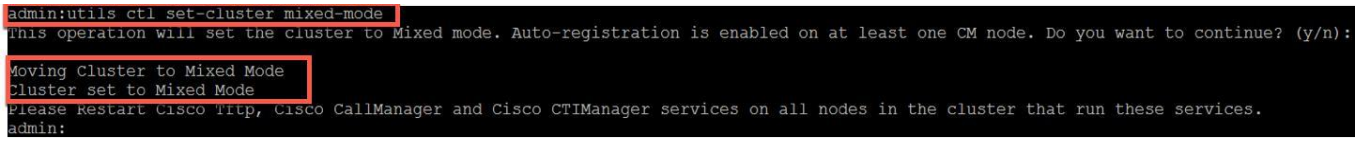
ここで、**cucm1**.dcloud.cisco.com の混合モードを有効にします。

PuTTY を開き、まだ接続していない場合は、SSH で cucm1.dcloud.cisco.com に接続します。ユーザ名/パスワードは、**administrator/dCloud123!** です。

CLI で **utils ctl set-cluster mixed-mode** コマンドを入力して Enter を押し、クラスタを混合モードに移行させます。プロンプトが表示されたら、「**Y**」を入力して Enter を押し、続行することを確認します（図 46 を参照）。

注：Y と入力しても、Y が画面に表示されない場合があります。その場合は、Y を入力した後にそのまま Enter を押してください。動作しない場合は、もう一度やり直してください。図 46 に示すように、最終的にコマンドは終了します。

図 46. cucm1.dcloud.cisco.com の混合モードを有効にする



cucm1.dcloud.cisco.com クラスタで混合モードが有効になりました。今回は、PLM に暗号化ライセンスがインストールされているため成功しました。

TFTP、CTIManager、CallManager サービスを再起動する必要もありますが、ラボでは cucm1.dcloud.cisco.com でこれらのサービスは使用しないため、今回は必要ありません。

注: 同様に、Unity Connection 11.5(1) SU3 およびそれ以降の SU でも、Unity Connection で暗号化モードを有効にするには暗号化ライセンスが必要です。

これには、Unified CM 11.5(1) SU3 用の暗号化ライセンスに関する手順も含まれています。

B. Unified CM および Unity Connection 12.0 の輸出管理機能を許可したスマート ライセンス

注: このモジュールの残りの Unified CM の作業は、12.0(1) バージョン：**ucm1.dcloud.cisco.com**（198.18.133.3）で実施します。

Cisco Unified Communications Manager リリース 12.0(1) 以降のリリースでは、Prime License Manager は、Cisco Smart Software Manager に代わります。Cisco Prime License Manager は、リリース 12.0(1) から使用されず、ログイン前の [インストール済みアプリケーション（Installed Applications）] 画面にも表示されなくなります。シスコ スマート ソフトウェア ライセンシングを使用することで、端末が自己登録してライセンスの使用状況を報告するため、製品アクティベーション キー（PAK）が不要になり、お客様は簡単にライセンスを購入、展開、および管理することができます。

Unified CM と IM and Presence は、https://software.cisco.com でホストされている Cisco Smart Software Manager（SSM）に、HTTPS の直接接続または Web プロキシ経由で直接登録できます。セキュリティ上の理由によりインターネットに直接接続してインストール ベースを管理したくない場合は、Smart Software Manager サテライトをお客様のオンプレミス環境にインストールすることができます。Smart Software Manager サテライトでは Cisco Smart Software Manager の機能のサブセットが提供され、製品の登録やライセンス使用状況のレポートができます。サテライトは定期的に Cisco Smart Software Manager と同期され、最新のライセンス使用状況が反映されます。

インストール後、Cisco Unified Communications Manager は、90 日間評価期間として実行されます。評価期間が終われば、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されるまで、Cisco Unified Communications Manager では、新規ユーザや新規端末の追加ができなくなります。

詳細については、次の URL から Unified CM 12.0(1) リリース ノートを参照してください。
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/12_0_1/cucm_b_release-notes-for-cucm-imp-1201/cucm_b_release-notes-for-cucm-imp-1201_chapter_00.html#reference_01133E095CB51F07C0B854928E817A7A

このラボでは、リリース 12.0 を実行している ucm1.dcloud.cisco.com および cuc1.dcloud.cisco.com を使用します。全体的には、次のタスクを実施します。

1. Unified CM が Cisco Smart Software Manager に登録される前に Unified CM の登録ステータスを確認する。
2. Unified CM で混合モードを有効にできないことを確認する。
3. Unity Connection で同じ操作を実施する。
4. Unified CM および Unity Connection で輸出管理機能を有効にし、登録トークンを作成する。
5. Unified CM と Unity Connection を Cisco Smart Software Manager に登録する方法、ステータスを確認する方法、スマート ソフトウェア ライセンシングのページを操作する方法を習得する。
6. CLI でライセンス ステータスを確認後、Unified CM で混合モードを有効にし、Unity Connection で暗号化を有効にする。

注: 今回のラボでは、**このモジュールを効率化するために、12.0 システムでのライセンス登録はすでに完了しています**。上記の各手順を確認していきますが、手順 1 ～ 5 はすでに完了しています。これらの手順については、内容を説明し、関連するスクリーンショットでプロセスを示しますが、タスク自体は**実施しません**。ここから、次に必要な手順のパート B、手順 6 までスキップできます。

手順 1 ～ 5 を再度実施する場合、システムの応答は、このラボ ガイドとは異なり、輸出管理機能が許可されたライセンスの状態に戻るまでに少し時間がかかります。

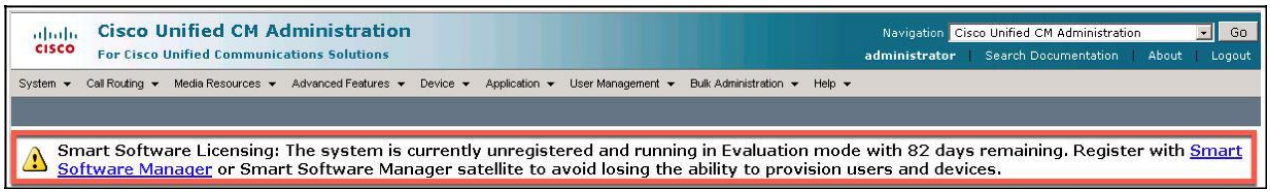
1. Unified CM が Cisco Smart Software Manager に登録される前に Unified CM の登録ステータスを確認する

注:これは手順の確認だけで実施しません。システムにはすでにライセンスが付与されています。

ここで、Unified CM が Smart Software Manager に登録される前に Unified CM の登録ステータスを確認します。

Unified CM が Cisco Smart Software Manager に登録される前に、Unified CM 管理ポータルに移動した場合、Unified CM クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに**登録されていない**ことを示す警告メッセージが表示されます(図 47 を参照)。

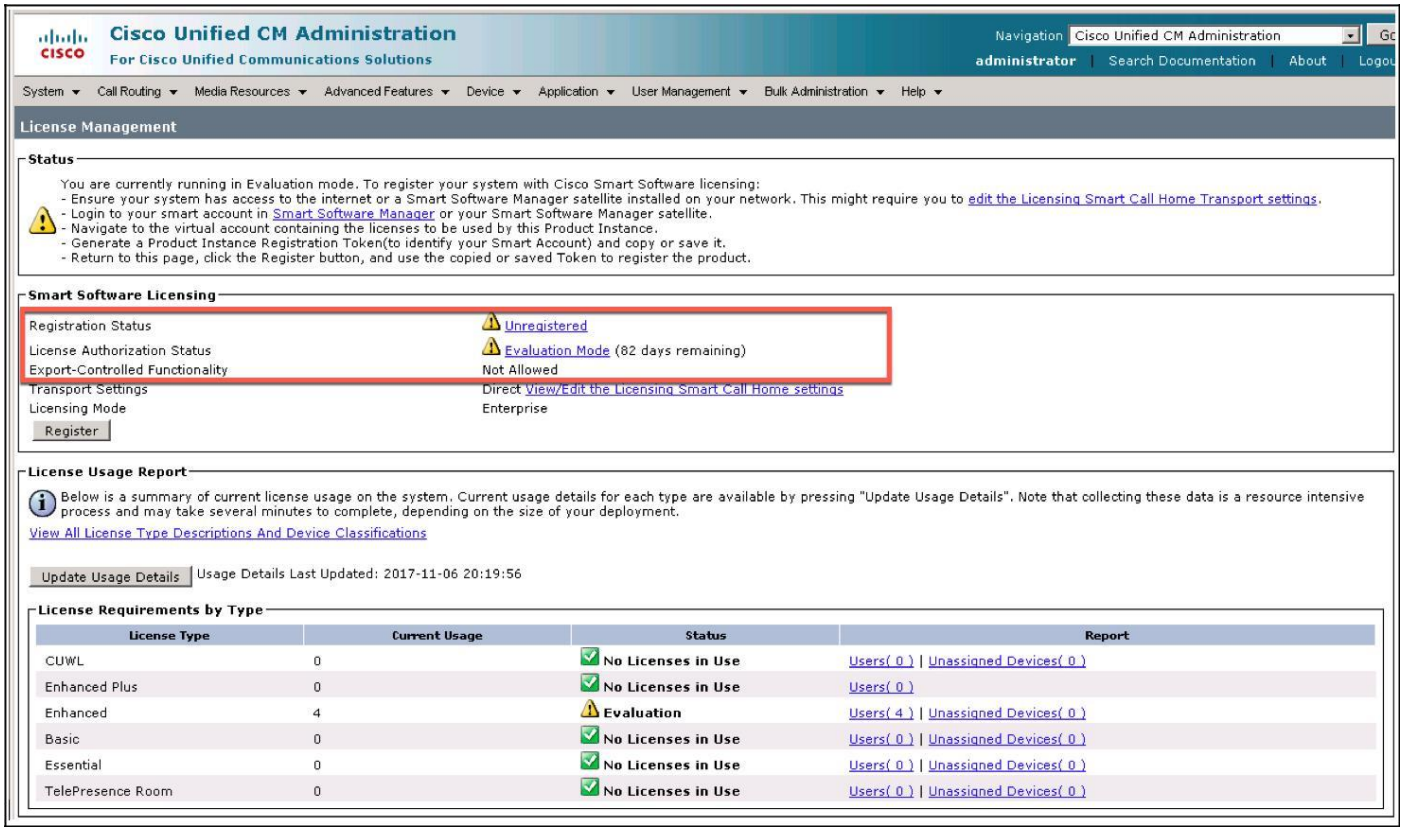
図 47. 警告メッセージ:Unified CM が Cisco Smart Software Manager に登録されていない*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

図 48 に示すように、[システム(System)] > [ライセンス(Licensing)] > [ライセンス管理(License Management)] に移動すれば、Unified CM がシスコ スマート ソフトウェア ライセンシングに登録されていないことがわかります。[登録ステータス(Registration Status)] に [未登録(Unregistered)] と表示され、[輸出管理機能(Export-Controlled Functionality)] が [未許可(Not Allowed)] となっていることを確認します。

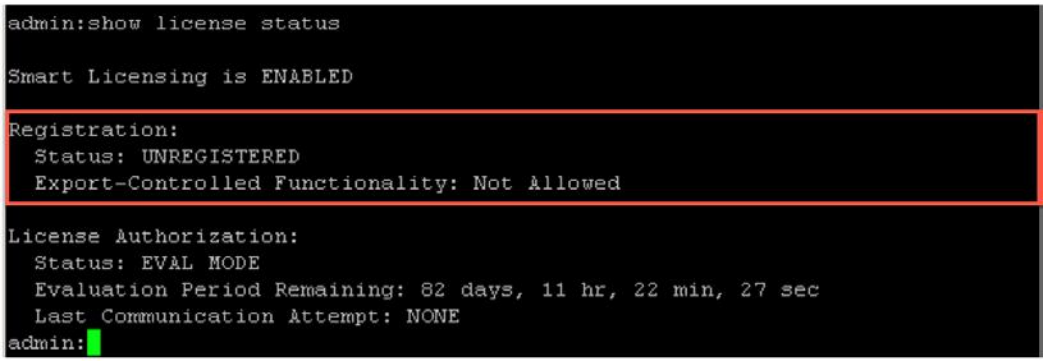
図 48. ライセンス管理の設定 – Unified CM のステータス:未登録*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

SSH で Unified CM の CLI に接続し、**show license status** コマンドを発行してライセンスのステータスを確認した場合、図 49 に示すように、[ステータス（Status）] は [未登録（UNREGISTERED）]、[輸出管理機能（Export-Controlled Functionality）] は [未許可（Not Allowed）] と表示されます。

図 49. Unified CM 12.0(1)：Show License Status - 未登録*



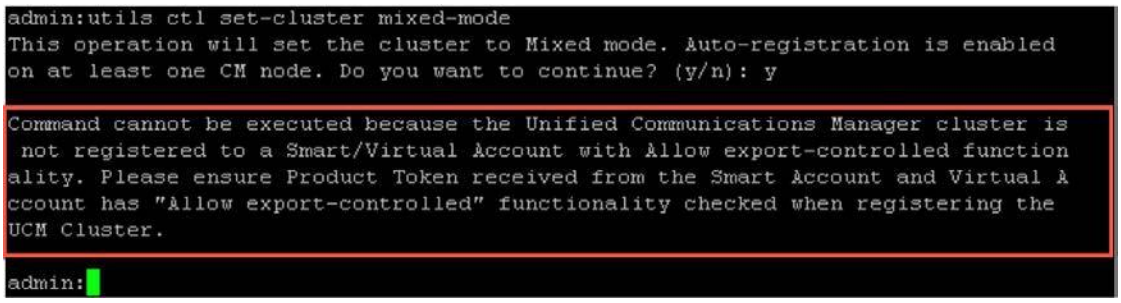
* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

2. Unified CM で混合モードを有効にできないことを確認する

注：これは手順の確認だけで実施しません。システムにはすでにライセンスが付与されています。

図 50 に示されているように、**utils ctl set-cluster mixed-mode** コマンドを発行して Unified CM で混合モードを有効にしようとすると、このコマンドは失敗します。Unified CM で混合モードを有効にするには、輸出管理機能が許可された有効なトークンが必要だからです。システムは、Cisco Smart Software Manager にまだ登録されていないので、必要なトークンがありません。

図 50. Unified CM 12.0(1)：暗号化ライセンスがないため混合モードを有効化するクラスタ コマンドが失敗*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

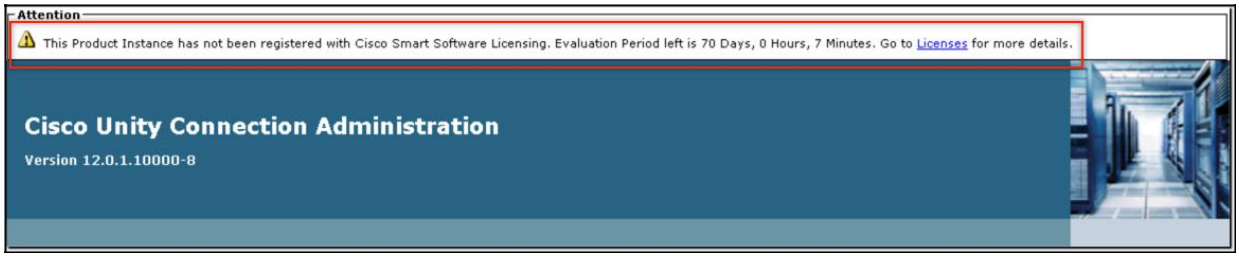
3. Unity Connection で同じ操作を実行する

注：これは手順の確認だけで実施しません。システムにはすでにライセンスが付与されています。

Unity Connection に対して同じ手順を繰り返します。

Smart Licensing Manager に登録する前に Unity Connection の管理インターフェイスにログインした場合、図 51 に示すように、「この製品インスタンスは Cisco Smart Software Licensing に登録されていません（This Product Instance has not been registered with Cisco Smart Software Licensing）」というメッセージが表示され、スマート ライセンスがまだ有効になっていないことがわかります。

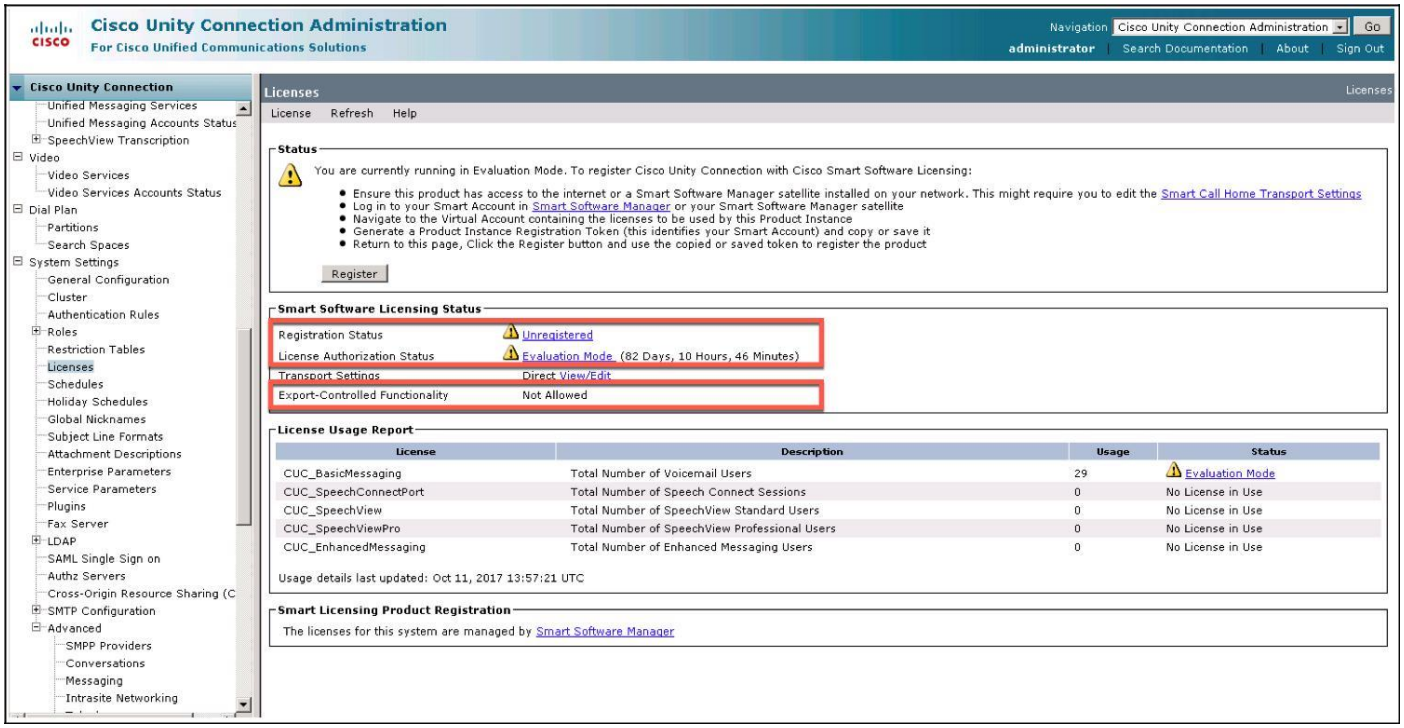
図 51. 警告メッセージ - Unity Connection が Cisco Smart Software Manager に登録されていない*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

[システム設定（System Settings）] > [ライセンス（Licenses）] に移動した場合、図 52 に示すように、登録ステータスは [未登録（Unregistered）] で、[輸出管理機能（Export-Controlled Functionality）] は [未許可（Not Allowed）] になっていることがわかります。

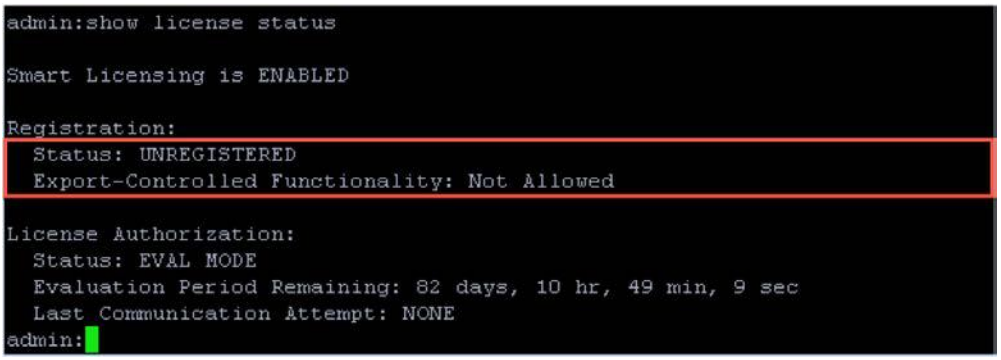
図 52. ライセンス管理の設定 – Unity Connection のステータス：未登録*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

SSH で Unity Connection の CLI に接続し、**show license status** コマンドを発行した場合、図 53 に示すように、サーバがシスコ スマート ソフトウェア ライセンシングに登録されていないことがわかります。

図 53. Unity Connection 12.0(1)：Show License Status - 未登録*



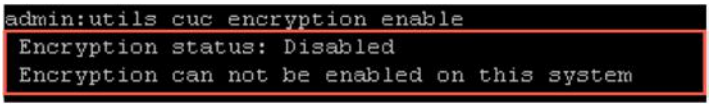
* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

Unity Connection 12.0(1) 以降の評価モードでは、暗号化はデフォルトで無効になっています。そのため、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに製品が登録されるまで、輸出管理機能を許可するトークンを使用してボイス メール アカウントへのアクセスを暗号化することはできません。

注：Unity Connection で暗号化を有効にすることができるのは、米国の輸出規制対象ソフトウェアを使用して Unity Connection をインストールしている場合**のみ**です。米国の輸出規制対象外のソフトウェアを使用する場合は、暗号化を有効にすることはできません。

図 54 に示すように、**utils cuc encryption enable** コマンドを使用して暗号化を有効にしようとすると、このコマンドは失敗します。Unity Connection が、輸出管理機能を許可した状態で Cisco Smart Software Manager に登録されていないからです。

図 54. Unity Connection 12.0(1)：暗号化ライセンスがないため暗号化を有効にするコマンドが失敗*



** ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、このメッセージは表示されません。*

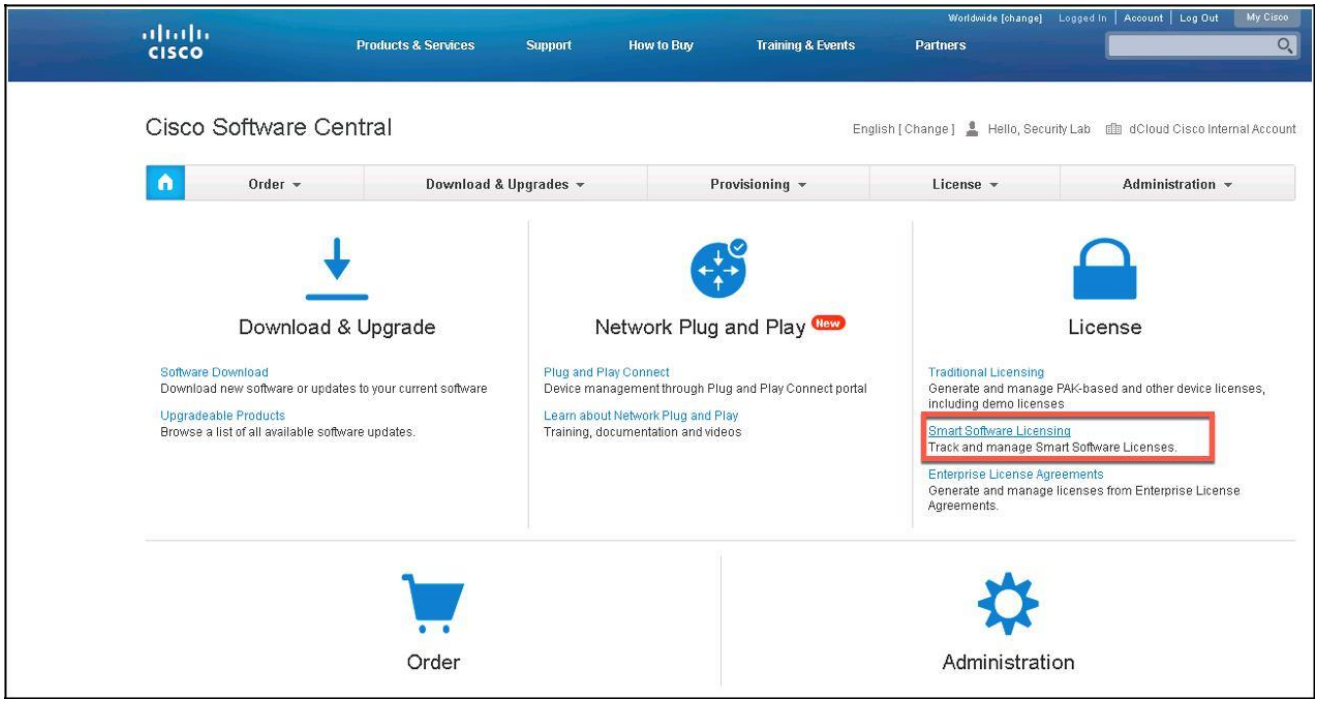
4. Unified CM および Unity Connection で輸出管理機能を有効にし、登録トークンを作成する

注：これは手順の確認だけで実施しません。このシステムにはライセンスがすでに付与されているため、登録トークンは必要ありません。

この時点で、Unified CM および Unity Connection 用のトークンを作成して、両サーバを Cisco Smart Software Manager に登録する必要があります。https://software.cisco.com にアクセスして自分の Cisco.com ユーザ名とパスワードでログインし、特定の組織のライセンスを管理します。

[スマートソフトウェアライセンシング（Smart Software Licensing）] をクリックします（図 55 を参照）。

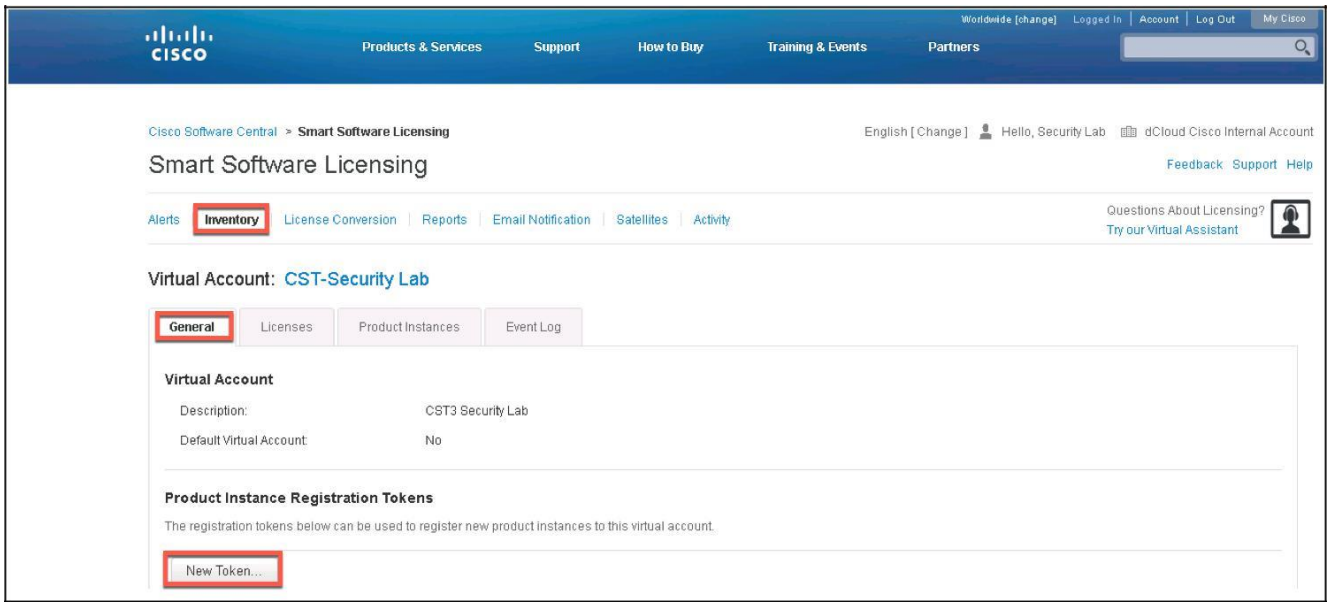
図 55. Cisco Software Central（https://software.cisco.com）：スマート ソフトウェア ライセンシングへのアクセス*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

次に、[インベントリ（Inventory）] タブをクリックします。バーチャルアカウントの [一般（General）] タブが表示されます。[新規トークン...（New Token...）] ボタンをクリックします（図 56 を参照）。

図 56. スマート ソフトウェア ライセンシング：バーチャルアカウントのインベントリおよび登録トークンの生成*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

図 57 に示すように、[登録トークンの生成（Create Registration Token）] ポップアップ ウィンドウで以下の内容の要求を実行します。

a. [説明（Description）]：POD-1-CUCM

b. [期限が切れるまでの期間（Expire After）]：1 日

c. [このトークンを使用して登録した製品で輸出管理機能を許可（Allow export-controlled functionality on the products registered with this token）]：オンこれをオンにすると、Unified CM で混合モードを有効化できます。

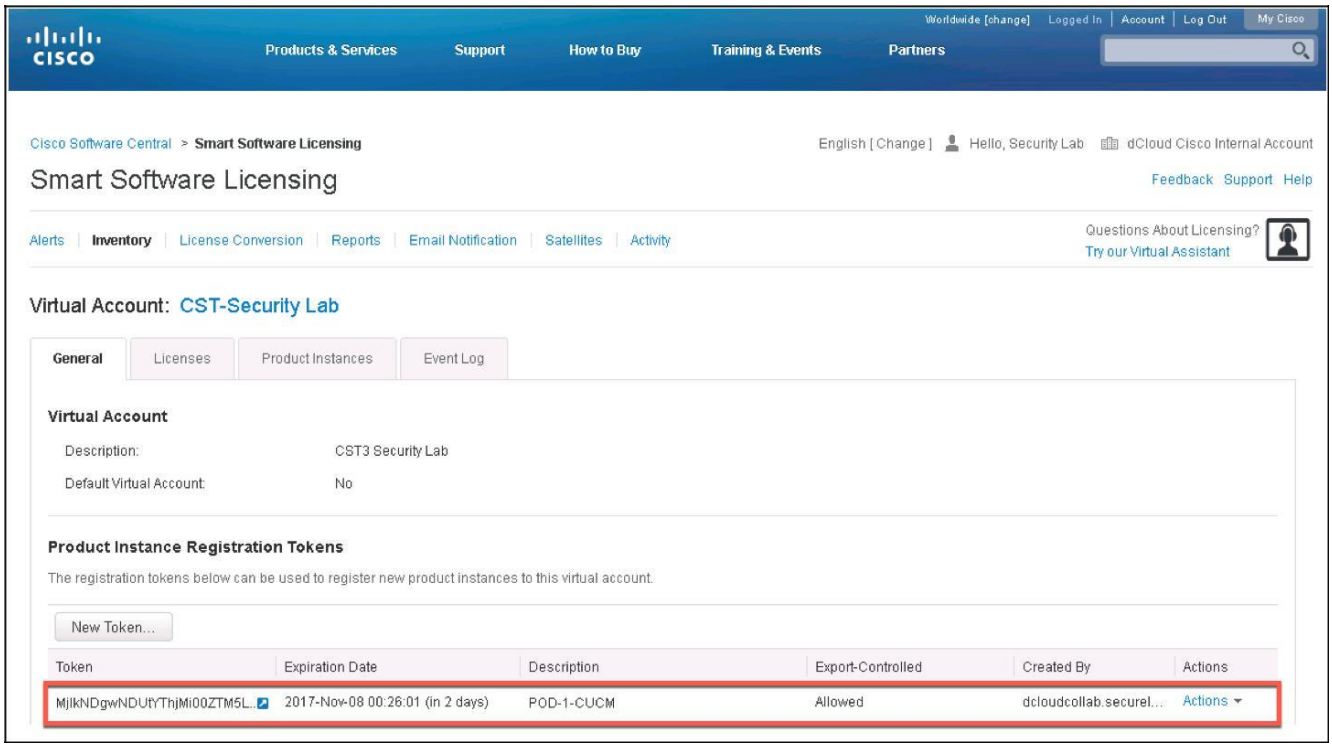
図 57. スマート ソフトウェア ライセンシング：Unified CM 用の登録トークンの作成*

* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

[トークンの作成（Create Token）] をクリックします。

[製品インスタンス登録トークン（Product Instance Registration Tokens）] に、新しく作成した**トークン**が表示されます（図 58 を参照）。

図 58. スマート ソフトウェア ライセンシング：新たに作成された Unified CM 登録トークン*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

Unity Connection のトークンを作成するために、同じ手順を完了します。

[新規トークン（New Token...）] をクリックします。

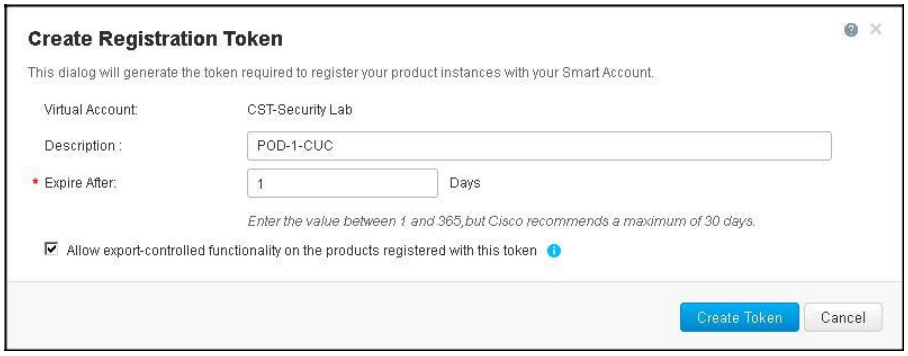
[登録トークンの作成（Create Registration Token）] ポップアップ ウィンドウで以下の内容の要求を実行します（図 59 を参照）。

a. [説明（Description）]：POD-1-CUC

b. [期限が切れるまでの期間（Expire After）]：1 日

c. [このトークンを使用して登録した製品で輸出管理機能を許可（Allow export-controlled functionality on the products registered with this token）]：オンこれをオンにすると、Unity Connection で混合モードを有効化できます。

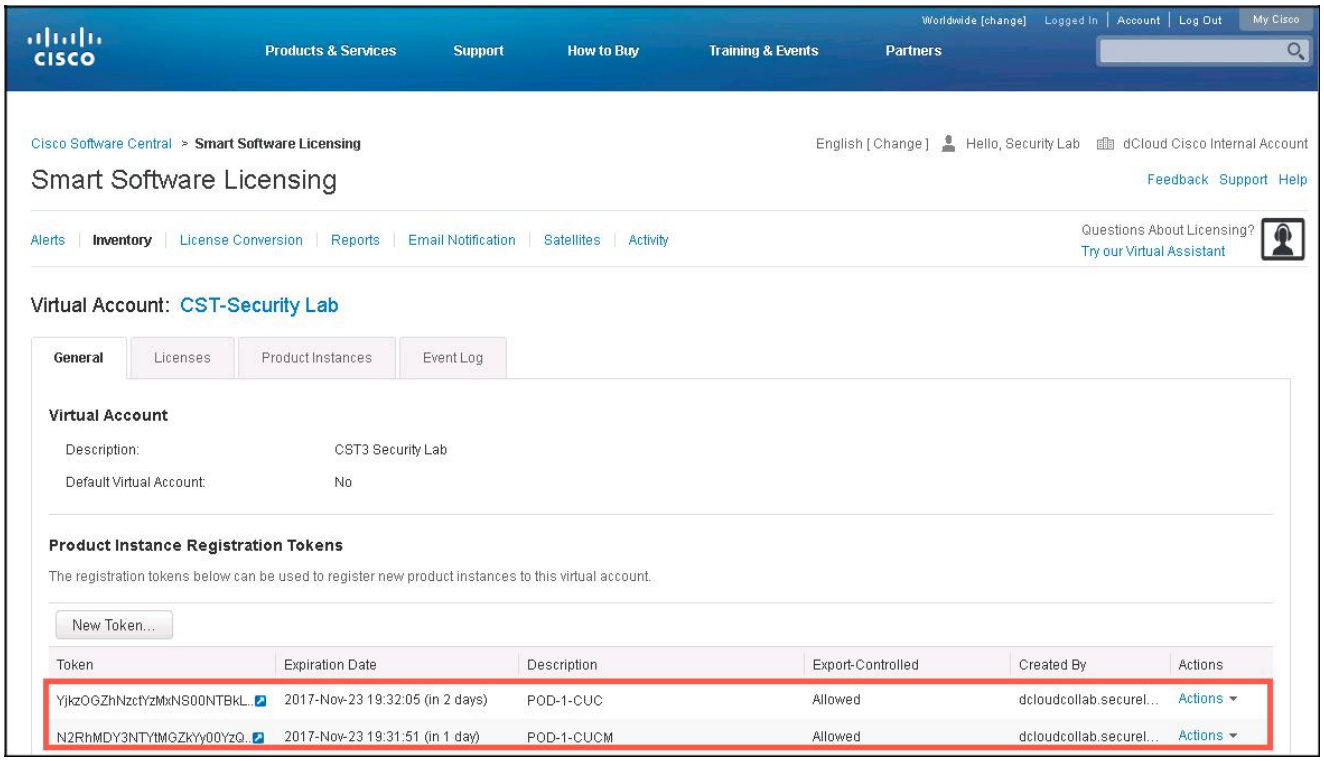
図 59. スマート ソフトウェア ライセンシング：Unity Connection 用の登録トークンの作成*



ここでは図を示しているだけです。ライセンスはすでに付与されていますので、この手順は実施しません。

[製品インスタンス登録トークン（Product Instance Registration Tokens）] に、新しく作成した**トークン**が表示されます（図 60 を参照）。

図 60. スマート ソフトウェア ライセンシング：新たに作成された Unity Connection 登録トークン*



ここでは図を示しているだけです。ライセンスはすでに付与されていますので、この手順は実施しません。

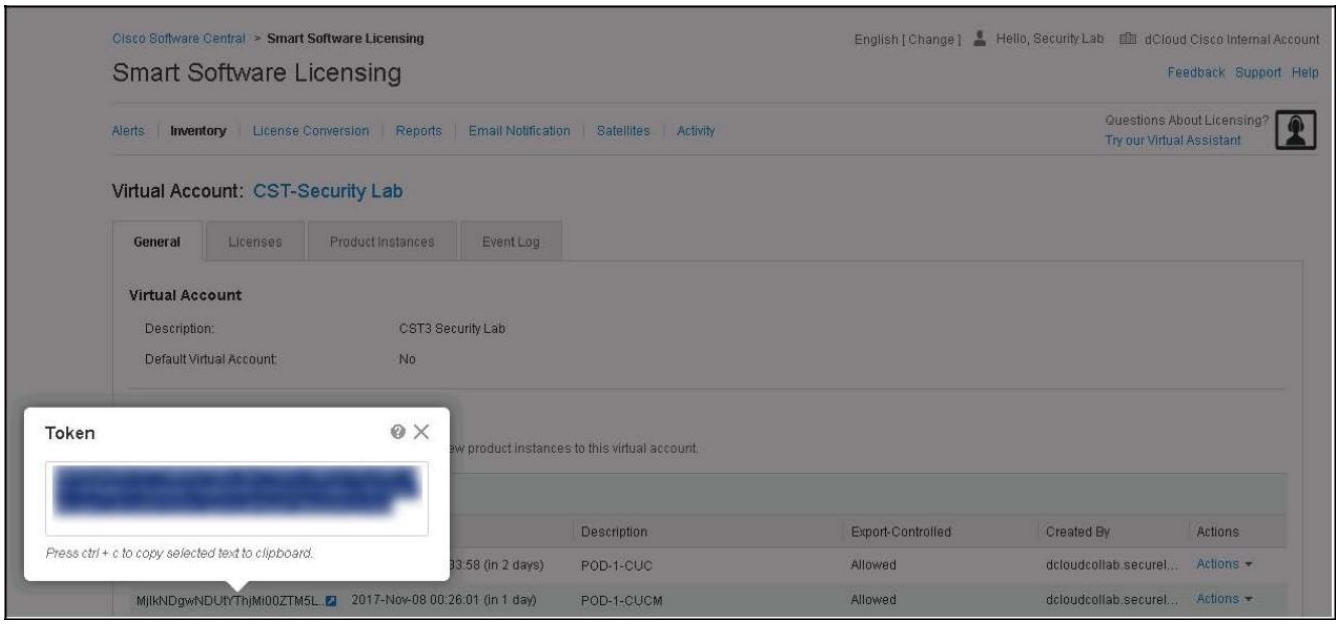
5. Unified CM と Unity Connection を Cisco Smart Software Manager に登録する方法、ステータスを確認する方法、スマート ソフトウェア ライセンシングのページを操作する方法を習得する

注: これは手順の確認だけで実施しません。システムにはすでにライセンスが付与されています。

この手順では、Unified CM および Unity Connection を Cisco Smart Software Manager に登録する方法を確認します。

Cisco Smart Software Manager に接続した際に、図 61 に示すように、Unified CM（POD-1-CUCM）のトークン ID をクリックし、Ctrl + C を押してトークンをクリップボードにコピーします。

図 61. スマート ソフトウェア ライセンシング：Unified CM 登録トークンをコピー*



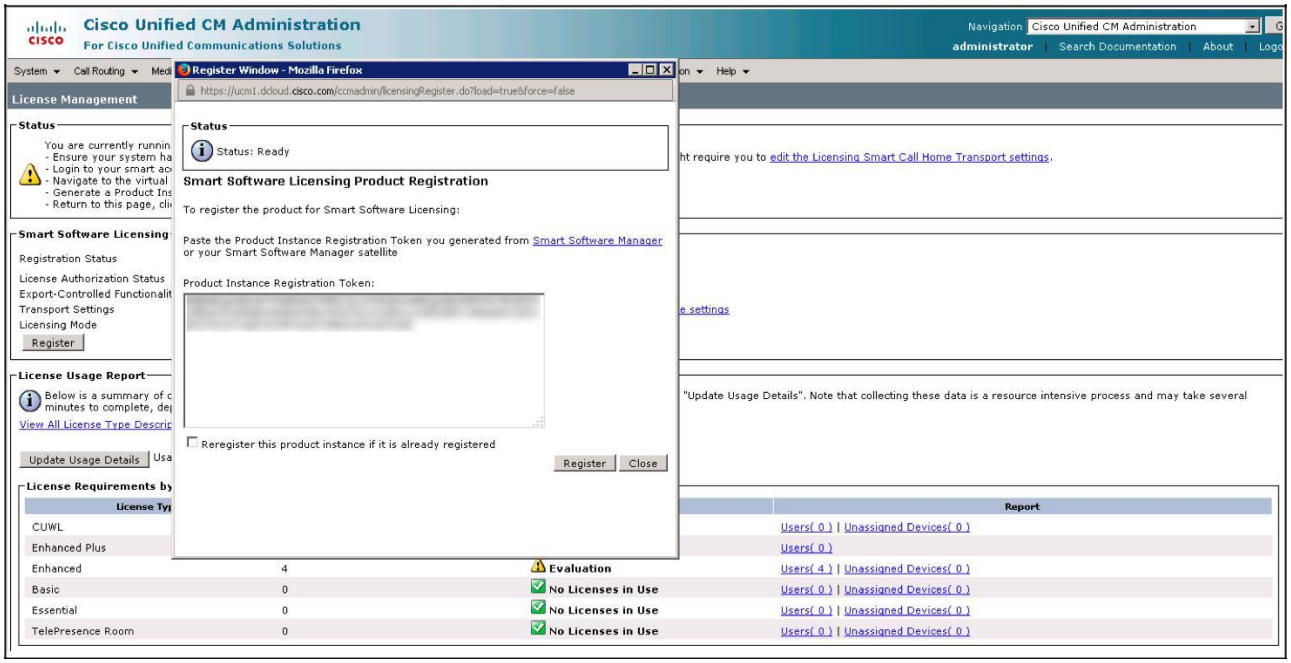
** ここでは図を示しているだけです。ライセンスはすでに付与されていますので、この手順は実施しません。*

Unified CM の管理インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin/）に戻ります。

[ライセンス管理ページ（License Management）] ページ（[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）] の順に移動）で、[登録（Register）] をクリックし、[製品インスタンスの登録トークン（Product Instance Registration Token）] フィールドにトークンを貼り付けます（図 62 を参照）。

注: システムにはすでにライセンスが付与されているため、このタスクは実行しません。

図 62　スマート ソフトウェア ライセンシング：登録トークンを利用した Unified CM 製品インスタンスの登録*

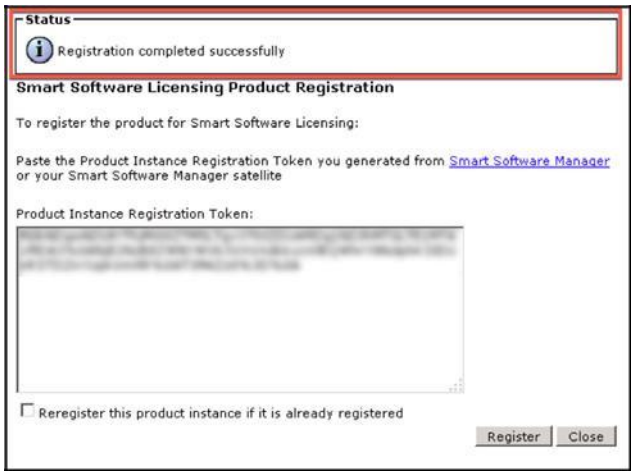


** ここでは図を示しているだけです。ライセンスはすでに付与されていますので、この手順は実施しません。*

[登録（Register）] をクリックします。

図 63 に示すように、「登録が正常に完了しました（Registration completed successfully）」というメッセージがウィンドウの上部に表示されます。

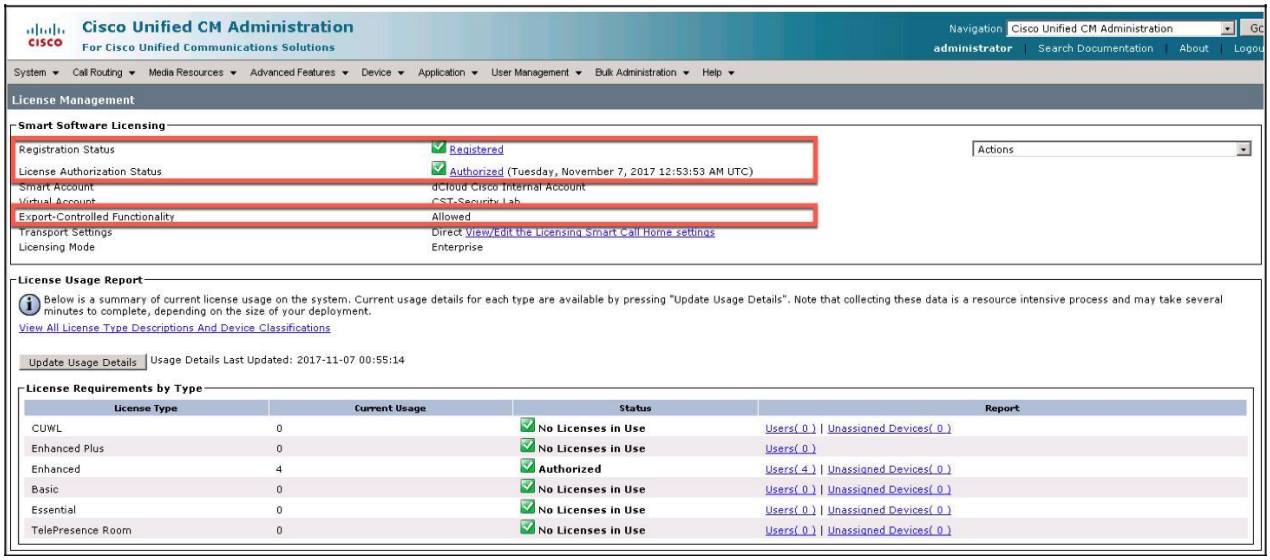
図 63　スマート ソフトウェア ライセンシング：登録が正常に完了*



** ここでは図を示しているだけです。ライセンスはすでに付与されていますので、この手順は実施しません。*

図 64 に示すように、[ライセンス管理（License Management）] ページの登録ステータスは、[登録済み（Registered）] に変わり、[輸出管理機能（Export-Controlled Functionality）] は、[許可（Allowed）] となっています。

図 64　ライセンス管理の設定 – Unified CM：登録済みおよび承認済みステータス、輸出管理機能許可済み*



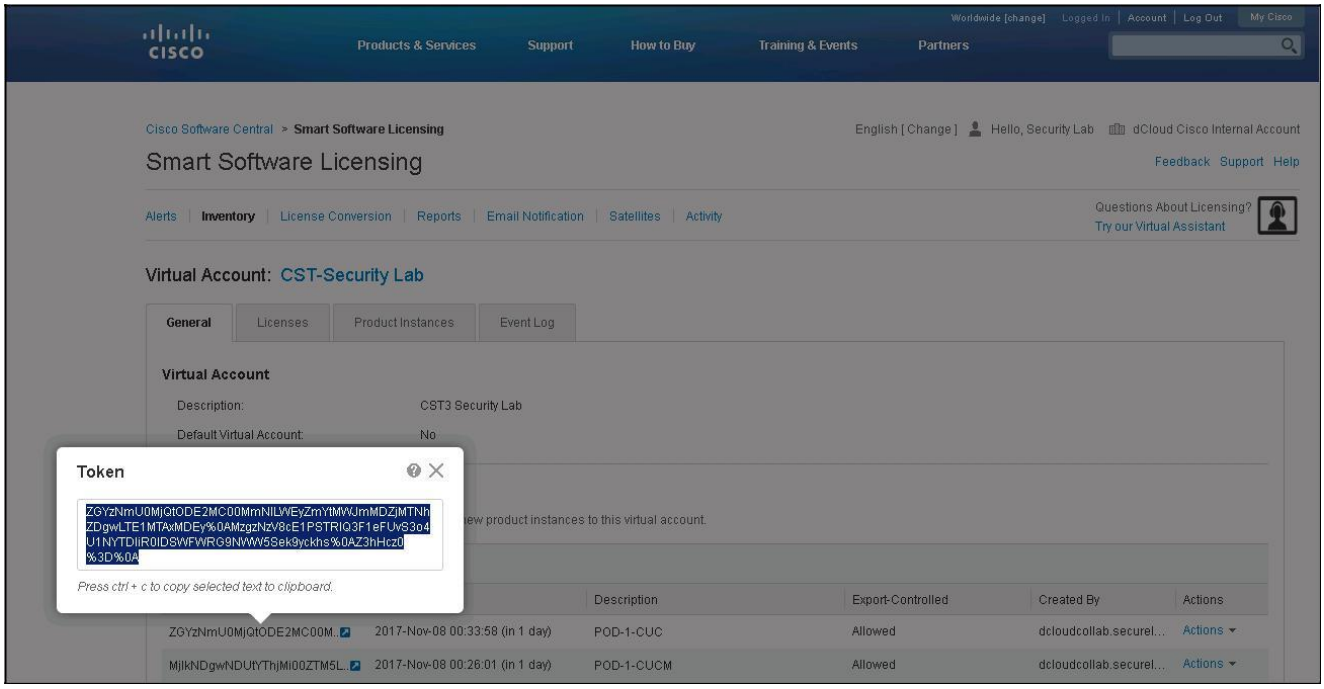
* ここでは図を示しているだけです。システムにはすでにライセンスが付与されています。

ここで同じ手順を繰り返して、Unity Connection のライセンスも付与します。

注：システムにはすでにライセンスが付与されているため、このタスクは実行しません。

最初に、[Cisco Smart Software Manager] ページ（https://software.cisco.com/）で、Unity Connection（POD-1-CUC）のトークン ID をクリックし、Ctrl + C を押してクリップボードにコピーして、トークンを取得します（図 65 を参照）。

図 65　スマート ソフトウェア ライセンシング：Unity Connection の登録トークンをコピー*

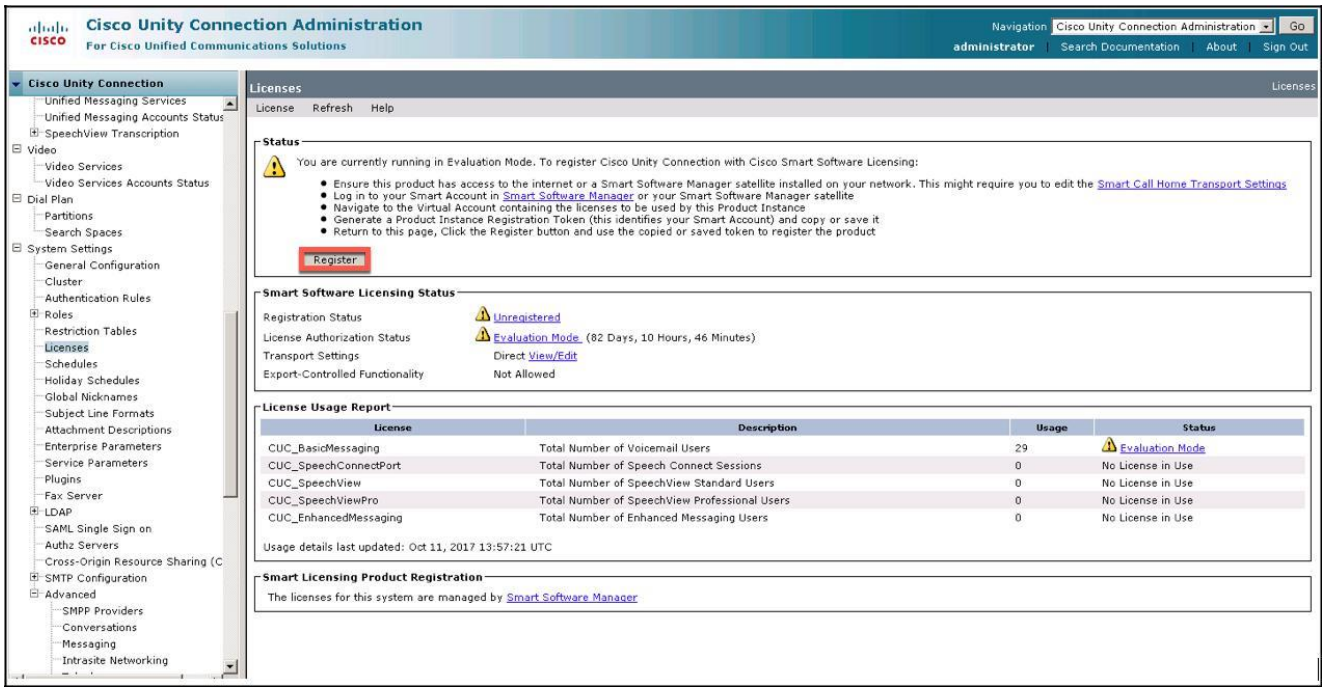


* ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。

次に、Unity Connection システム（https://cuc1.dcloud.cisco.com/cuadmin）にアクセスしてログインします。

左側のパネルで、[システム設定（System Setting）] > [ライセンス（Licenses）] の順に移動します。[登録（Register）] をクリックします（図 66 を参照）。

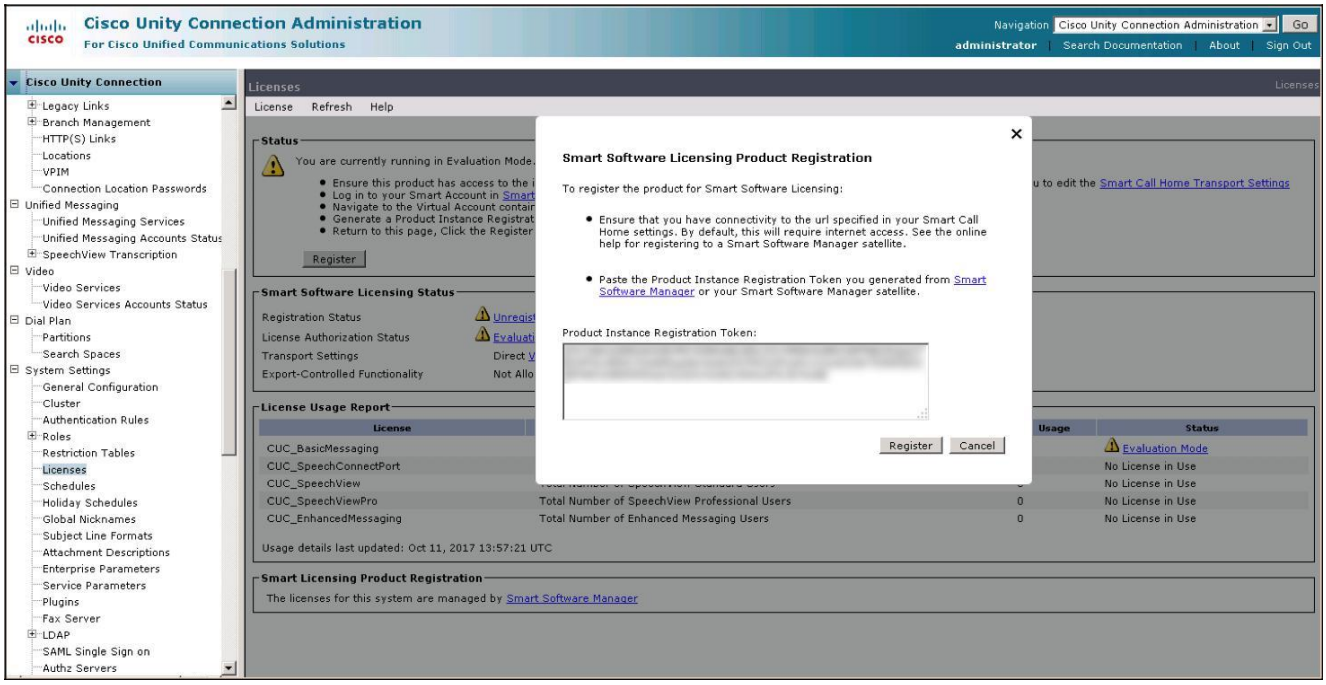
図 66　ライセンス管理の設定 – Unity Connection：輸出管理機能が許可されておらず、未登録 *



** ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。*

次に、図 67 に示すように、[ライセンストークン ID（License Token ID）] フィールドにトークンを貼り付けてから [登録（Register）] をクリックします。

図 67　スマート ソフトウェア ライセンシング：登録トークンを利用した Unity Connect 製品インスタンスの登録*



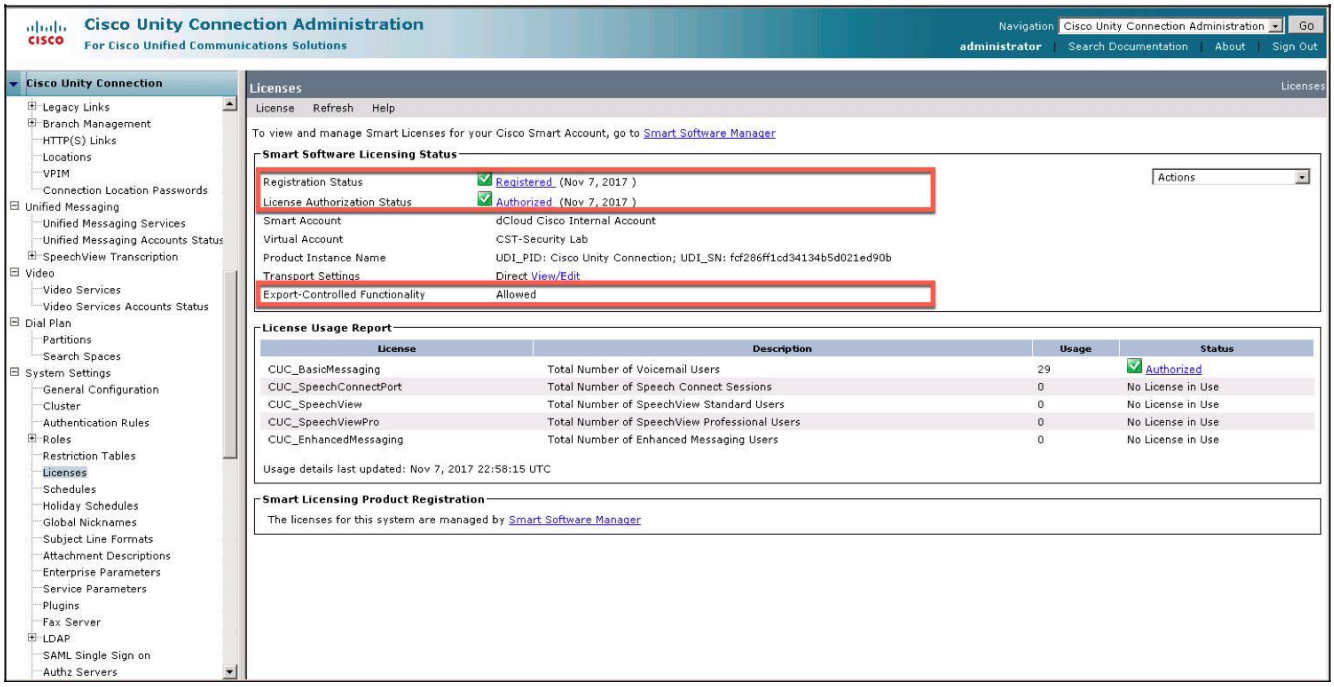
** ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。*

登録が成功した場合は、図 68 のようなメッセージが表示されます。

図 68　Unity Connection のスマート ライセンス登録成功を示すポップアップ

[ライセンス（Licenses）] ページが更新されたら、[スマートライセンスクライアントステータス（Smart License Client Status）] が[登録済み（Registered）] に変わり、[輸出管理機能（Export-Controlled Functionality）] が[許可（Allowed）] になっていることがわかります（図 69 を参照）。

図 69　ライセンス管理の設定 – Unity Connection：登録済みおよび承認済みステータス、輸出管理機能許可済み*



* ここでは図を示しているだけです。この手順はすでに実行されていますので、ここでは実施しません。

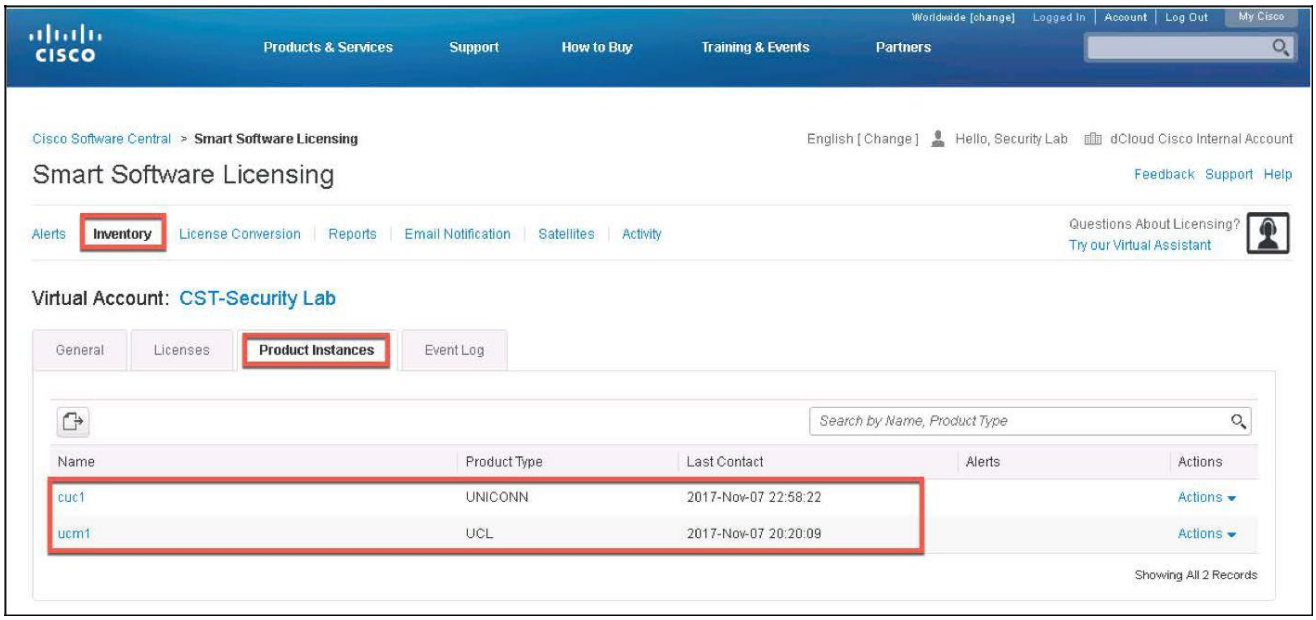
次に、スマート ソフトウェア ライセンシング ポータル（https://software.cisco.com/）での検証に進みます。

スマート ソフトウェア ライセンシング ポータル（https://software.cisco.com/）に戻り、必要に応じて、Cisco.com ユーザ名とパスワードで再度ログインします。

[インベントリ（Inventory）] タブをクリックします。

次に、[製品インスタンス（Product Instances）] タブをクリックして、Cisco Communications Manager（**ucm1**）と Cisco Unity Connection（**cuc1**）がそのページに表示されていることを確認します（図 70 を参照）。

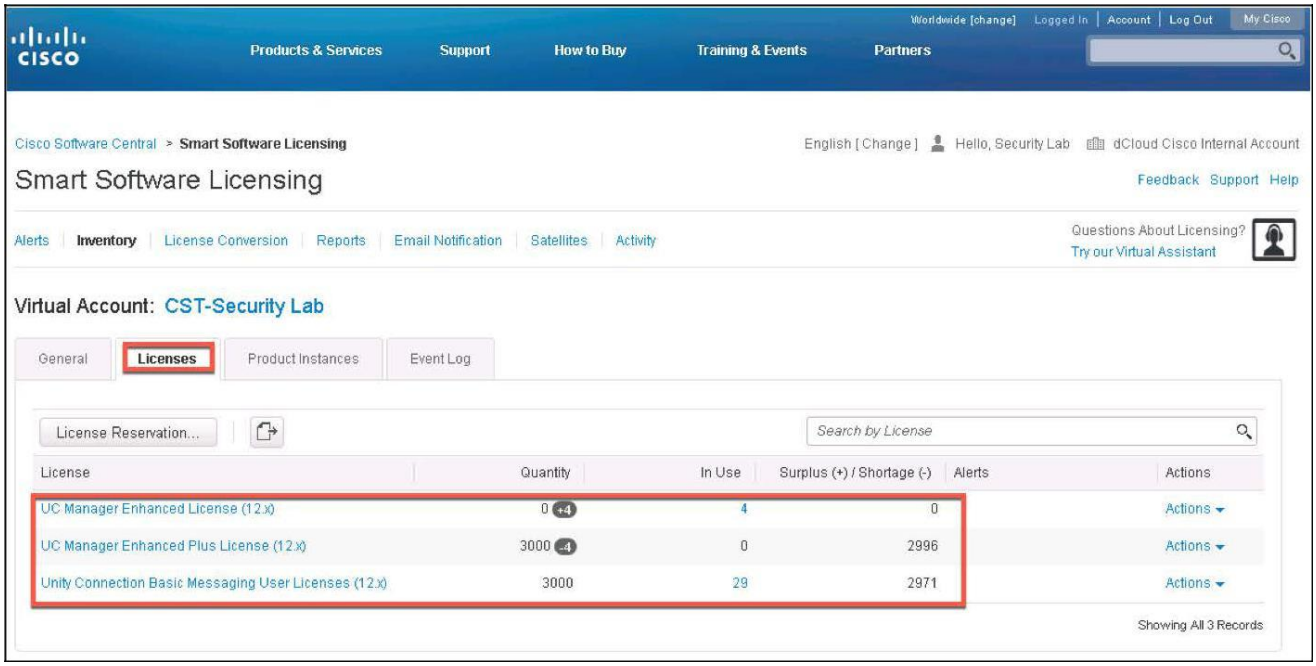
図 70　スマート ソフトウェア ライセンシング：Unified CM（ucm1）と Unity Connection（cuc1）製品インスタンスを確認*



** ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。*

次に[ライセンス（Licenses）] タブをクリックし、現在のライセンス使用状況を確認します（図 71 を参照）。

図 71　スマート ソフトウェア ライセンシング：ライセンスの数量と使用状況を確認*

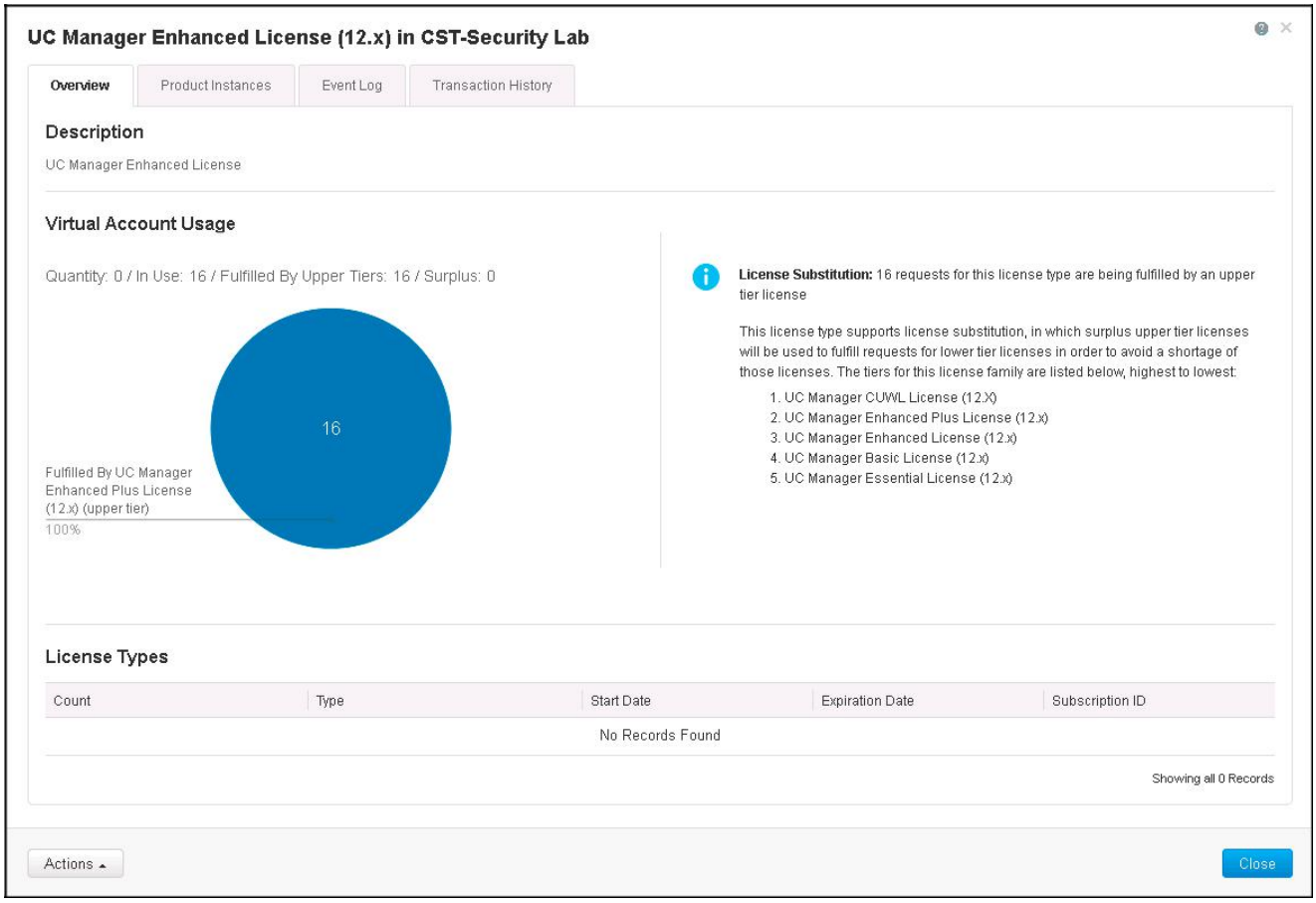


** ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。*

次に、[UC Manager 機能拡張ライセンス（12.x）（UC Manager Enhancement License (12.x)）] をクリックします。

図 72 に示すようなポップアップ ウィンドウが開きます。

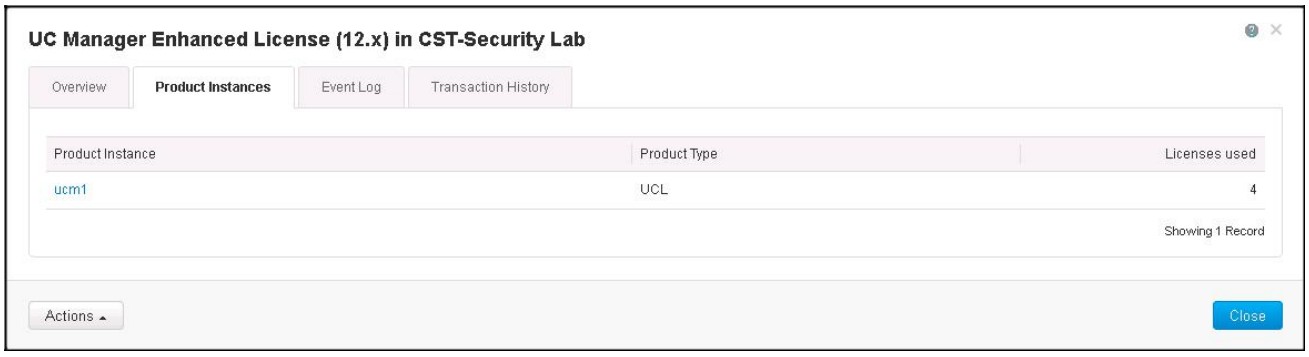
図 72　UC Manager 機能拡張ライセンスの概要*



ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。

図 73 に示すように、[製品インスタンス（Product Instances）] をクリックして、ライセンスを使用している特定の製品インスタンスを表示します。

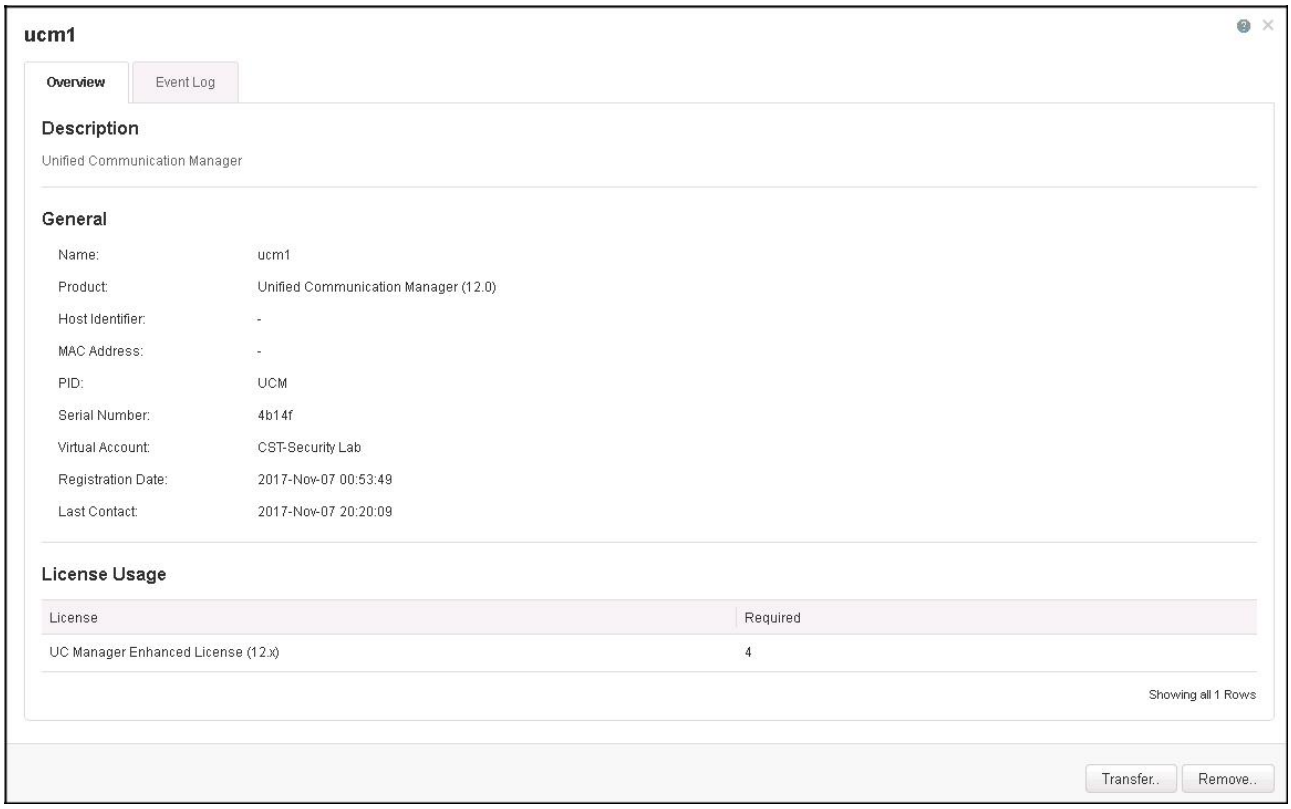
図 73　UC Manager 機能拡張ライセンスを使用している製品インスタンス*



ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。

[ucm1] という名前の製品インスタンスをクリックします。図 74 に示すように、クリックした特定の製品インスタンスに関するライセンスの使用状況などの情報を確認できます。

図 74　ucm1 で UC Manager 機能拡張ライセンスを使用している製品インスタンスの概要*



** ここでは図を示しているだけです。このシステムにはライセンスがすでに付与されていますので、この操作は実行しません。*

6. CLI でライセンス ステータスを確認後、Unified CM で混合モードを有効にし、Unity Connection で暗号化を有効にする

注:このラボを続行するには、この手順を完了する必要があります。

ここでは、CLI でステータスを確認し、Unified CM の混合モードを有効にします。

まだ接続していない場合、PuTTY を使用して SSH で ucm1.dcoud.cisco.com に接続します（ユーザ名/パスワード: **administrator/dCloud123!**）。

show license status コマンドを実行します。

図 75 に示すように、Unified CM が登録され、[輸出管理機能（Export-Controlled Functionality）] が [許可（Allowed）] になっていることを確認します。

図 75　Unified CM 12.0(1)：Show License Status - 登録済み、輸出管理機能許可済み

```
admin:show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: dCloud Cisco Internal Account
  Virtual Account: CST-Security Lab
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Nov 7 00:53:50 2017 UTC
  Last Renewal Attempt: SUCCEEDED on Nov 7 00:53:50 2017 UTC
  Next Renewal Attempt: May 6 00:53:50 2018 UTC
  Registration Expires: Nov 7 00:47:49 2018 UTC

License Authorization:
  Status: AUTHORIZED on Nov 7 20:20:09 2017 UTC
  Last Communication Attempt: SUCCEEDED on Nov 7 20:20:09 2017 UTC
  Next Communication Attempt: Dec 7 20:20:09 2017 UTC
  Communication Deadline: Feb 5 20:14:09 2018 UTC
admin:
```

次に、**utils ctl set-cluster mixed-mode** コマンドを発行して、Unified CM で混合モードを有効にします。今回は成功し、図 76 に示すように、クラスタが混合モードに設定されていることを確認できます。

注：Y と入力しても、Y が画面に表示されない場合があります。その場合は、Y を入力した後にそのまま Enter を押してください。動作しない場合は、もう一度やり直してください。図 76 に示すように、最終的にコマンドは終了します。

図 76　Unified CM 12.0(1)：クラスタの混合モード設定が成功

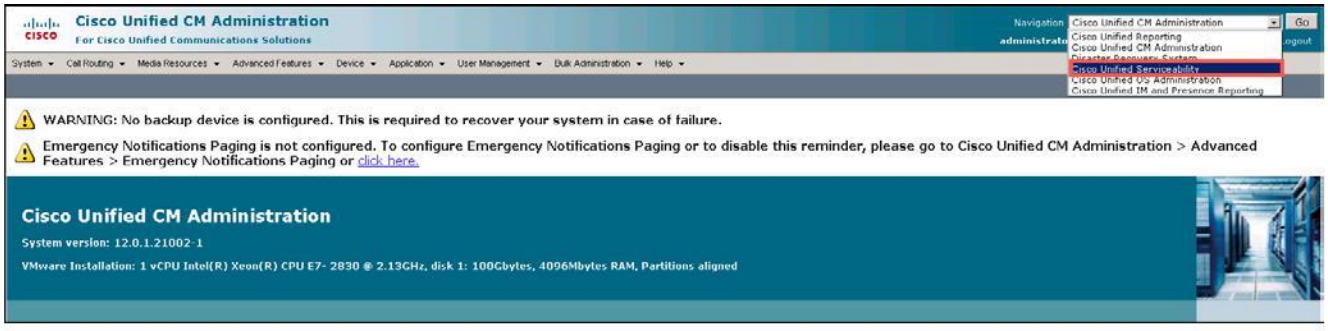
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled
on at least one CM node. Do you want to continue? (y/n): y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all th
e nodes in the cluster that run these services.

admin:
```

混合モードを有効化した際のメッセージに示されているように、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ページから CallManager サービスを再起動する必要があります（図 77 を参照）。このラボでは CTI を使用しないため、CTIManager を再起動する必要はありません。

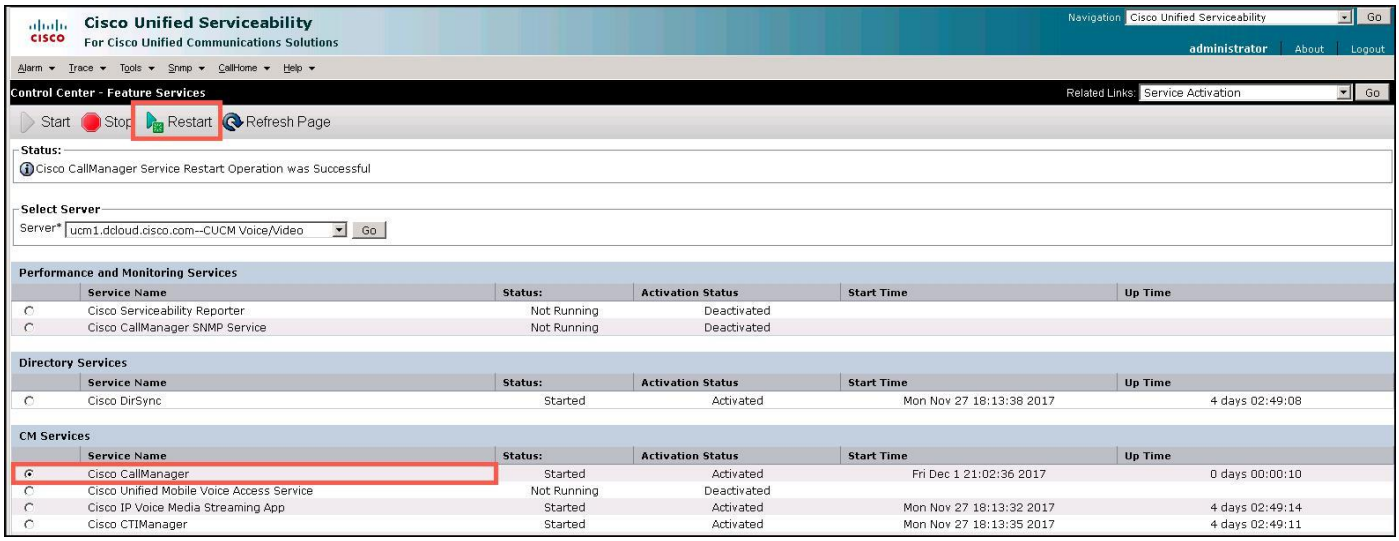
図 77　Unified CM サービスアビリティ インターフェイスの操作



[ツール（Tools）] > [コントロール センター － 機能サービス（Control Center － Feature Services）] に移動し、[サーバ（Server）] ドロップダウン メニューから [ucm1.dcloud.cisco.com--CUCM Voice/Video] を選択して、[移動（Go）] をクリックします。

次に図 78 に示すように、[Cisco CallManager] の横にあるオプション ボタンをオンにし、[再起動（Restart）] ボタンをクリックします。

図 78　Unified CM：Cisco CallManager サービスの再起動

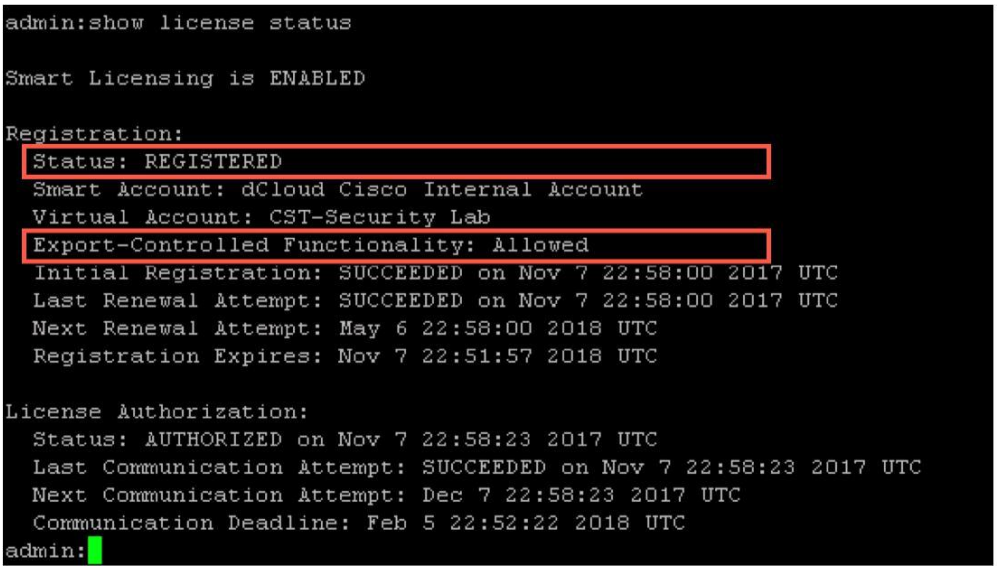


次のステップでは、CLI を通じてステータスを確認し、Unity Connection での暗号化を有効にします。

まだ接続していない場合は、PuTTY を使用して Unity Connection cuc1 に SSH 接続します（ユーザ名/パスワード：**administrator/dCloud123!**）。

show license status コマンドを実行します。図 79 に示すように、[ステータス（Status）] が [登録済み(REGISTERED)] で、[輸出管理機能（Export-Controlled Functionality）] が [許可（Allowed）] であることを確認します。

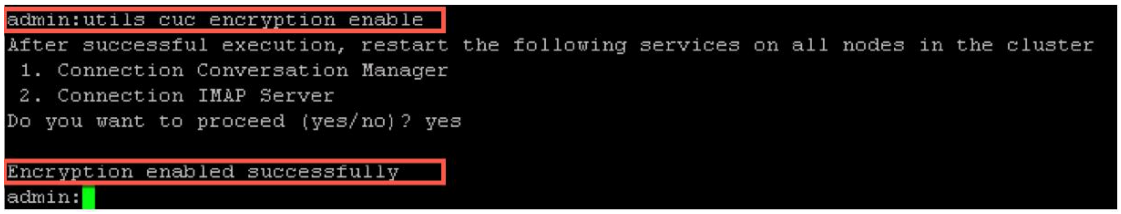
図 79　Unity Connection 12.0(1)：ライセンス ステータスの表示 － 登録および輸出管理機能の許可



次に、Unity Connection で暗号化を有効にします。

Cisco Unity Connection Restricted バージョンで暗号化を有効にするために、Unity Connection 12.0(1) では新しい CLI コマンド **utils cuc encryption enable** が導入されています。このコマンドは図 80 に示すように実行します。暗号化が有効になったことがわかります。それは、Unity Connection が Cisco Smart Software Manager に登録され、[輸出管理機能（Export-Controlled Functionality）] が [許可（Allowed）] に設定されたことによります。

図 80　Unity Connection 12.0(1)：暗号化が有効化される



通常はここで Connection Conversation Manager と Connection IMAP Server を再起動しますが、このモジュールではそれらのサービスを使用しないため、この時点で再起動する必要はありません。それらはモジュール 8（次世代暗号化によるセキュアなボイスメール）で再起動します。

[輸出管理機能（Export-Controlled Functionality）] を [許可（Allowed）] に設定し、Unified CM を混合モードにし、Unity Connection で暗号化を有効にしたので、Unified CM と Unity Connection が Cisco Smart Software Manager に登録されました。

これで、このモジュールは終了です。

***** モジュール #2 の終了 *****

モジュール 3. PCI コンプライアンスのための TLS 1.2

モジュールの概要

このモジュールでは、TLS 接続用にネゴシエートされたバージョンと、TLS バージョン 1.2 の要件を示します。このモジュールは、次の 6 つのセクションに分割されています。

A. デフォルト設定とスニファ トレースの監視により Unified CM Web インターフェイスで TLS バージョンを確認する

B. ブラウザが TLS 1.0 に対応し、スニファ トレースを監視する際に TLS のバージョンを確認する

C. NMAP を使用して、Web および SIP インターフェイスで許可される TLS のバージョンと暗号を確認する

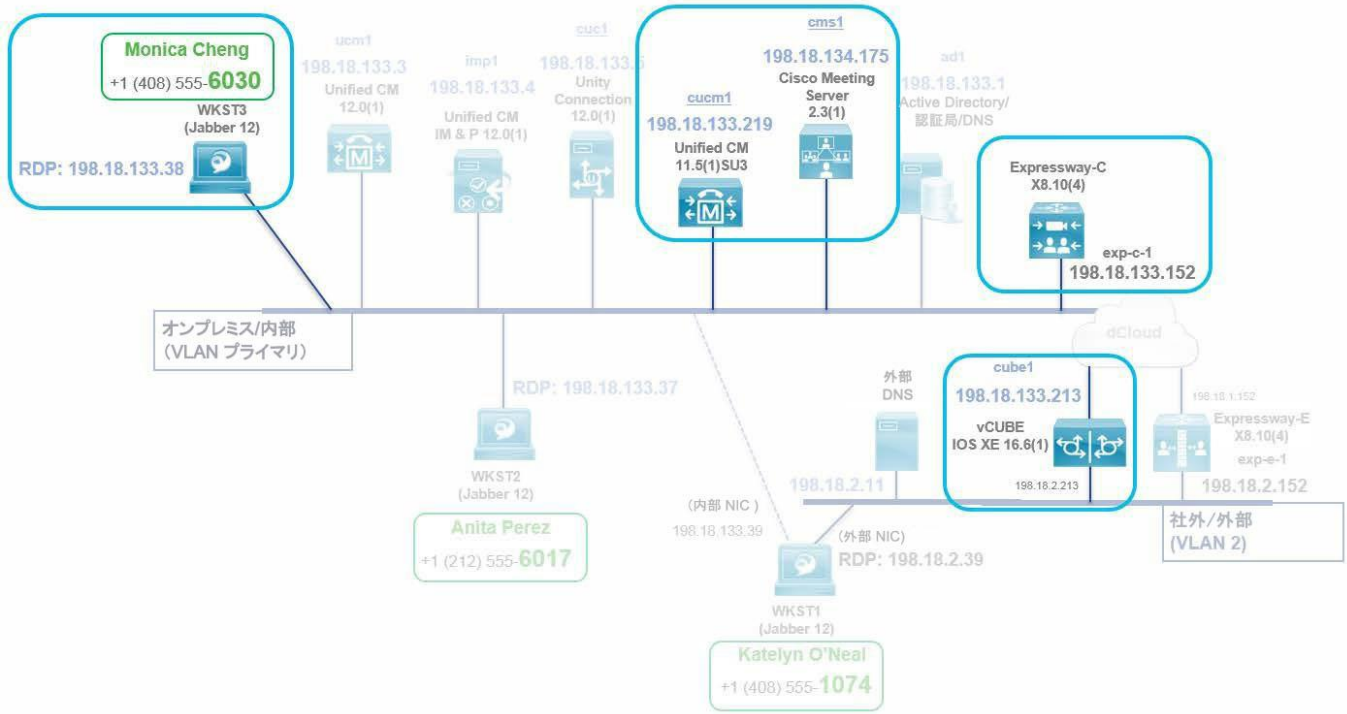
D. TLS 1.0 および 1.1 の無効化

E. ブラウザ専用の TLS 1.0 に対応している場合、TLS 接続が拒否されることを確認する

F. 他のアプリケーションで TLS 1.0 と 1.1 を無効にする方法

図 81 に、このモジュールで使用するトポロジおよび関連するコンポーネントを示します。

図 81　モジュール 3：PCI コンプライアンス トポロジのための TLS 1.2



手順

A. デフォルト設定とスニファ トレースの監視により Unified CM Web インターフェイスで TLS バージョンを確認する

ここで実行する手順の概要は次のとおりです。

1. Unified CM Web インターフェイスでデフォルトで使用する TLS バージョンを確認します。TLS 1.2 はネゴシエートが必要です。
2. スニファ トレースでの TLS ハンドシェイクを監視します。

WKST3（198.18.133.38、ユーザ名/パスワード：**DCLOUD\mcheng/C1sco12345**）に RDP 接続します。

ラボを開始する前に、PuTTY のすべてのインスタンスを終了（すべての SSH 接続を終了）します。

Unified CM 管理インターフェイス（https://cucm1.dcloud.cisco.com/ccmadmin）に接続します。

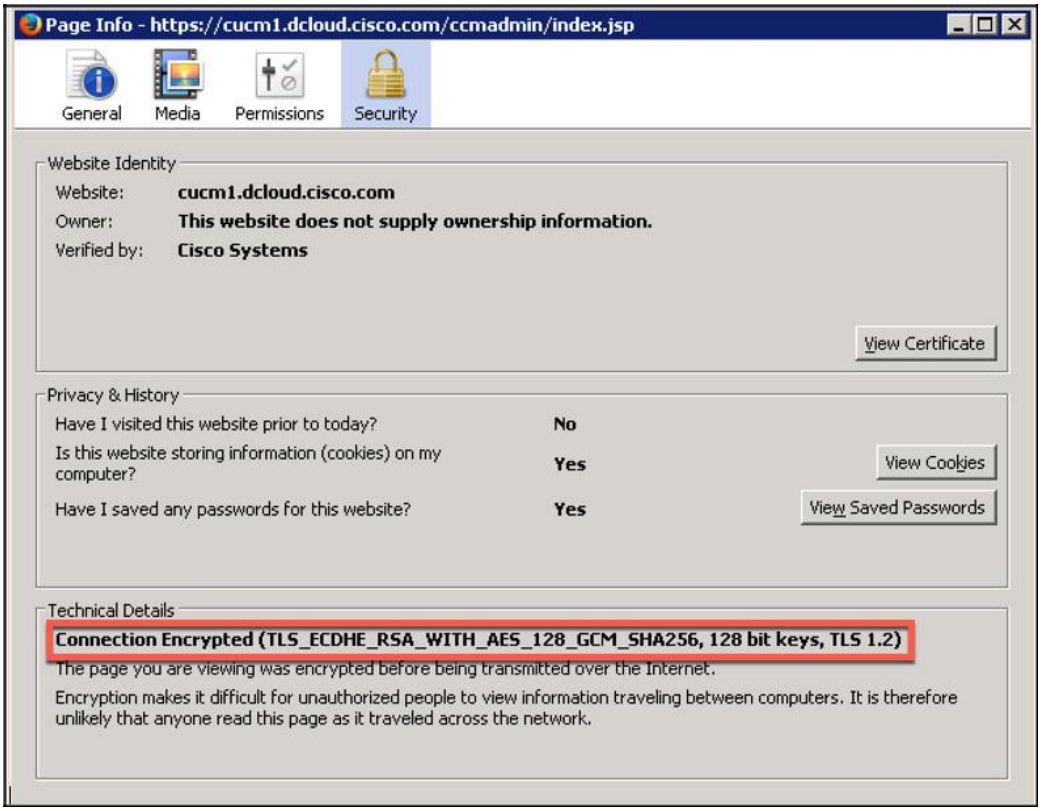
注：これは 11.5(1) SU3 を実行中の **cucm1.dcloud.cisco.com** です。12.0(1) を実行中の ucm1.dcloud.cisco.com< ではありません。

Firefox バーのロック アイコンをクリックします。ポップアップ ウィンドウで、**cucm1.dcloud.cisco.com** の横の矢印をクリックします。次に [詳細情報（More Information…）] をクリックします（図 82 を参照）。

図 82　Firefox でのセキュリティ情報の取得

ウィンドウの下部には、ネゴシエートされた TLS のバージョンが表示されます。この例では、図 83 に示すように TLS 1.2 になっています。

図 83　Web ページの詳細情報 – 技術詳細情報に TLS 1.2 と表示

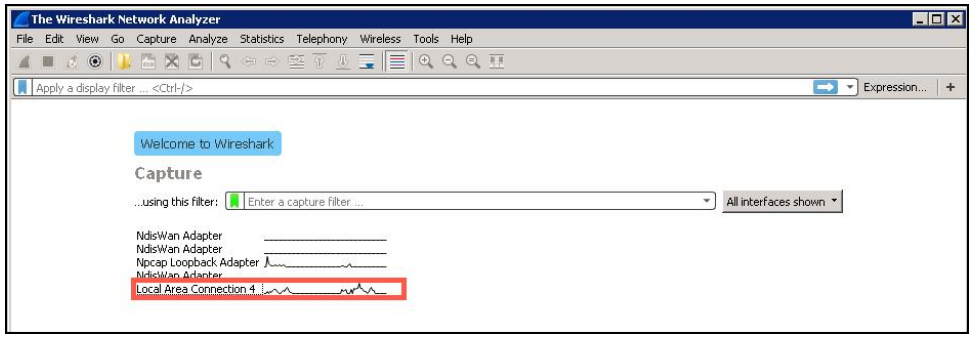


このウィンドウは、TLS 1.2 がネゴシエートされたことを示しています。デフォルトで、Unified CM の Web サーバ インターフェイスでは TLS 1.0、1.1、1.2、さらに Firefox ブラウザがサポートされています。ブラウザでは、最も強力なバージョンである TLS 1.2 が最初に提示されています。Unified CM でサポートされているため、TLS 1.2 がネゴシエートされます。

次に、TLS バージョンがネゴシエートされているスニファ トレースを見てみましょう。

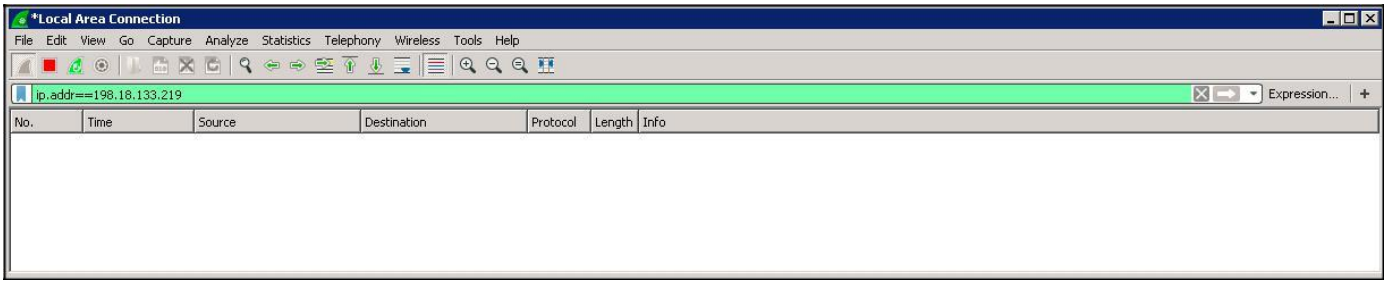
Windows ワークステーションのタスクバーの  アイコンをクリックして、Wireshark を開きます。Wireshark のソフトウェア更新オファーが表示された場合は、[このバージョンをスキップ（Skip this version）] をクリックして破棄します。図 84 に示すように、[ローカルエリア接続 X（Local Area Connection X）] （X は空白または任意の数字）をダブルクリックします。

図 84　Wireshark でネットワーク インターフェイスを選択



フィルタバーに「**ip.addr==198.18.133.219**」と入力し、Enter を押します。パケットは表示されません（図 85 を参照）。

図 85　フィルタ処理によって Wireshark 内のパケットを制限



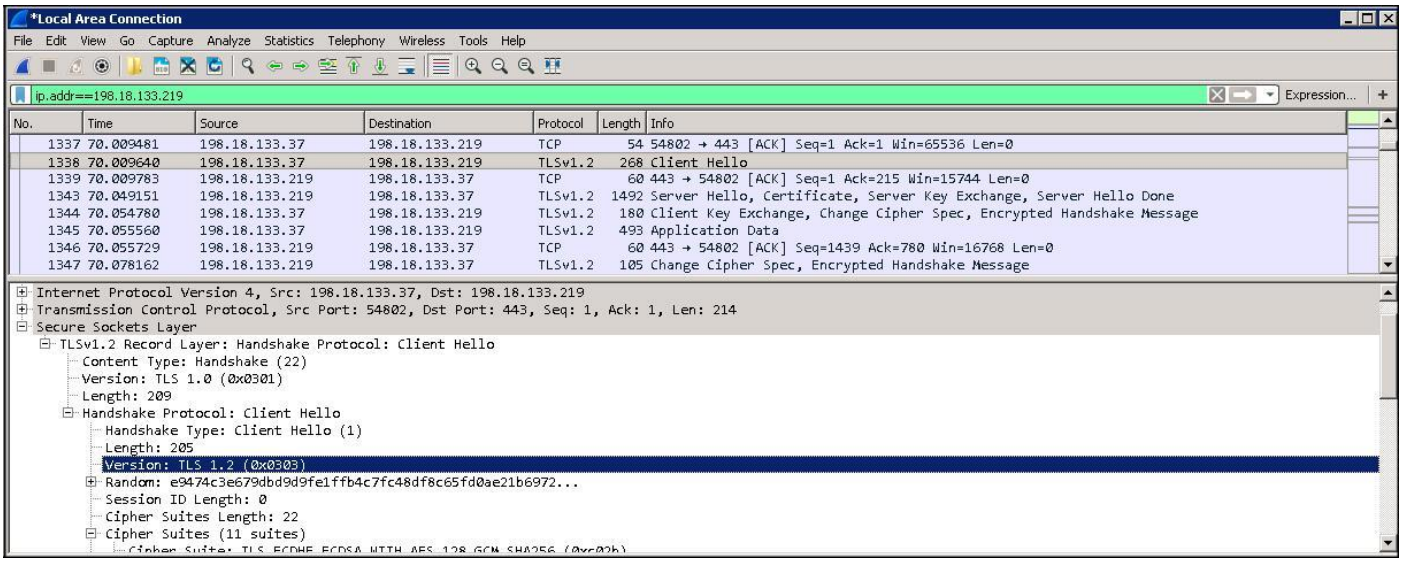
新しいタブを開き、cucm1（https://cucm1.dcloud.cisco.com/ccmadmin）の Unified CM 管理インターフェイスに移動します。

Wireshark に戻り、停止ボタン  を押してキャプチャを停止します。

パケットの中から [Client Hello] パケットを探し、パケットの説明のフィールドを展開します。[セキュアソケットレイヤ（Secure Socket Layer）] > [TLSv1.2 レコードレイヤ: ハンドシェイクプロトコル: Client Hello（TLSv1.2 Record Layer: Handshake Protocol: Client Hello）] > [ハンドシェイクプロトコル: Client Hello（Handshake Protocol: Client Hello）] の下に、TLS のバージョンが表示されます。図 86 に示すように、[バージョン: TLS 1.2 (0x303)（Version: TLS 1.2 (0x303)）] と表示されます。これは、Unified CM との接続を開始する際に、ブラウザでは TLS 1.2 が使用されることを意味します。

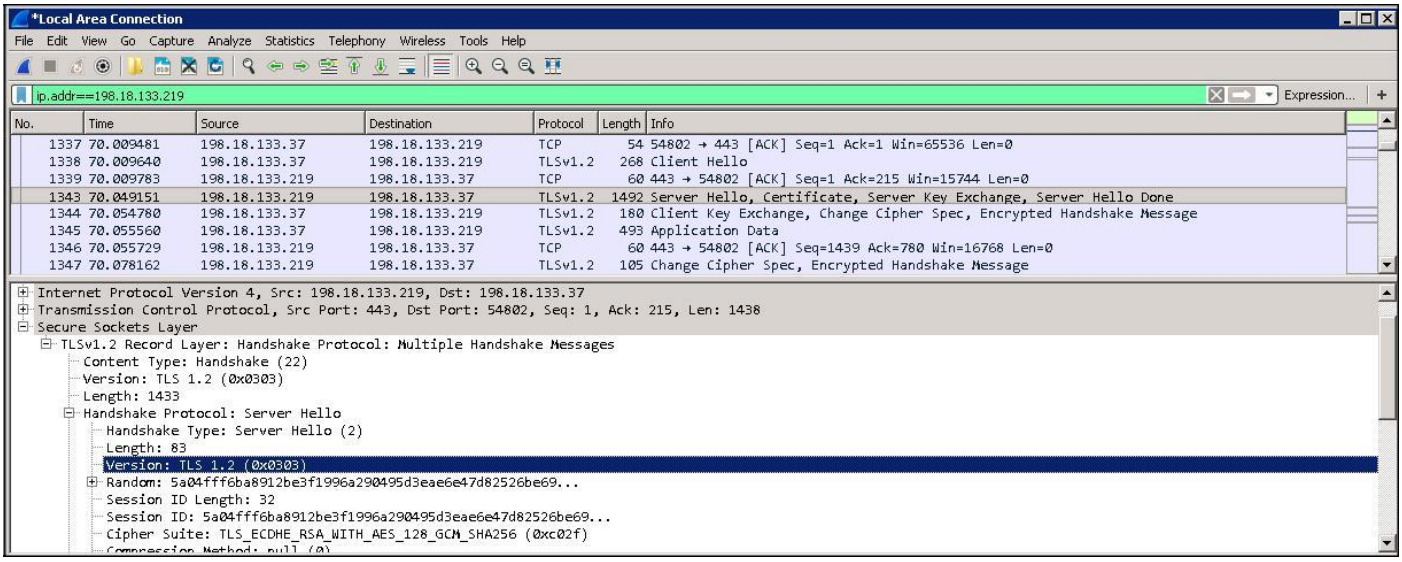
注: [セキュアソケットレイヤ（Secure Socket Layer）] > [TLSv1.2 レコードレイヤ: ハンドシェイクプロトコル: Client Hello（TLSv1.2 Record Layer: Handshake Protocol: Client Hello）] > [ハンドシェイクプロトコル: Client Hello（Handshake Protocol: Client Hello）] の下に、TLS のバージョンが TLS 1.0 であると表示されます。これは接続に実際に使用される TLS バージョンではなく、そのヘッダーの TLS バージョンです。実際には、[Client Hello] > [ハンドシェイクプロトコル：Client Hello（Handshake Protocol: Client Hello）] の下にある 2 番目の TLS バージョンを使用します。

図 86　TLS ハンドシェイクの Client Hello – TLS 1.2



下方向にスクロールし、[Server Hello, Certificate] パケットを見つけます。パケットの説明のフィールドを展開します。[セキュアソケットレイヤ（Secure Socket Layer）] > [TLSv1.2 レコードレイヤ: ハンドシェイクプロトコル: Client Hello（TLSv1.2 Record Layer: Handshake Protocol: Server Hello）] > [ハンドシェイクプロトコル: Client Hello（Handshake Protocol: Server Hello）] の下に、TLS のバージョンが表示されます。これは [バージョン: TLS 1.2 (0x303)（Version: TLS 1.2 (0x303)）] と表示されます（図 87 を参照）。これは、サーバである Unified CM が TLS 1.2 のオファーを承認し、TLS 接続で TLS 1.2 が使用されることを意味します。

図 87　TLS ハンドシェイクの Server Hello – TLS 1.2

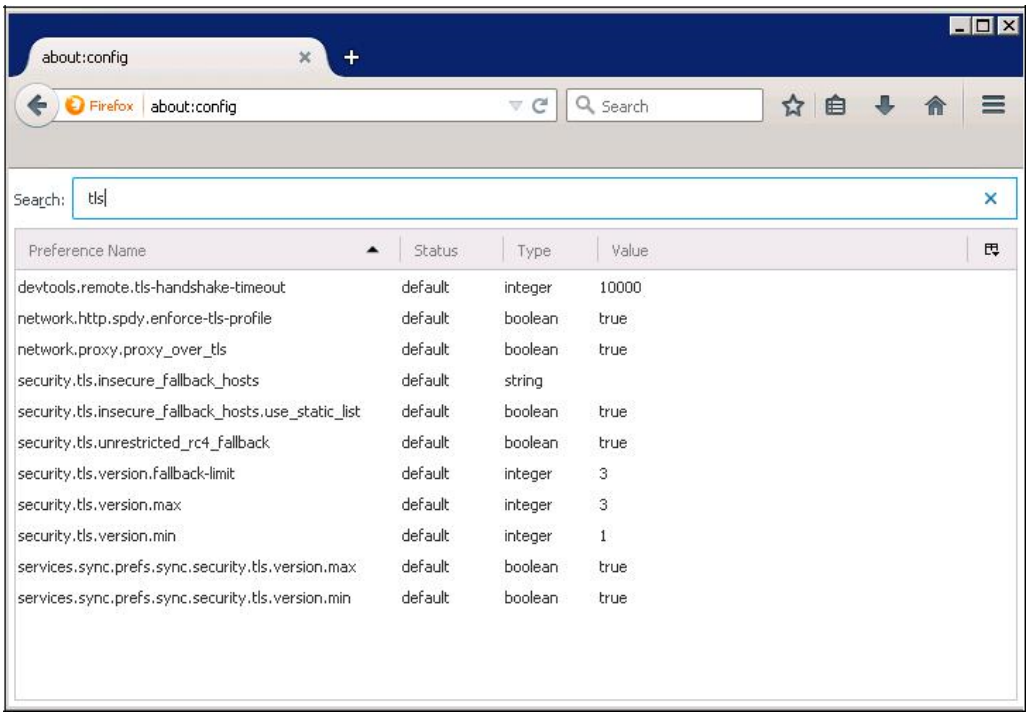


これは良好な状態です。デフォルトでは、TLS 1.2 がネゴシエートされます。

B. ブラウザが TLS 1.0 に対応し、スニファトレースを監視する際に、Unified CM Web インターフェイスの TLS のバージョンを確認する

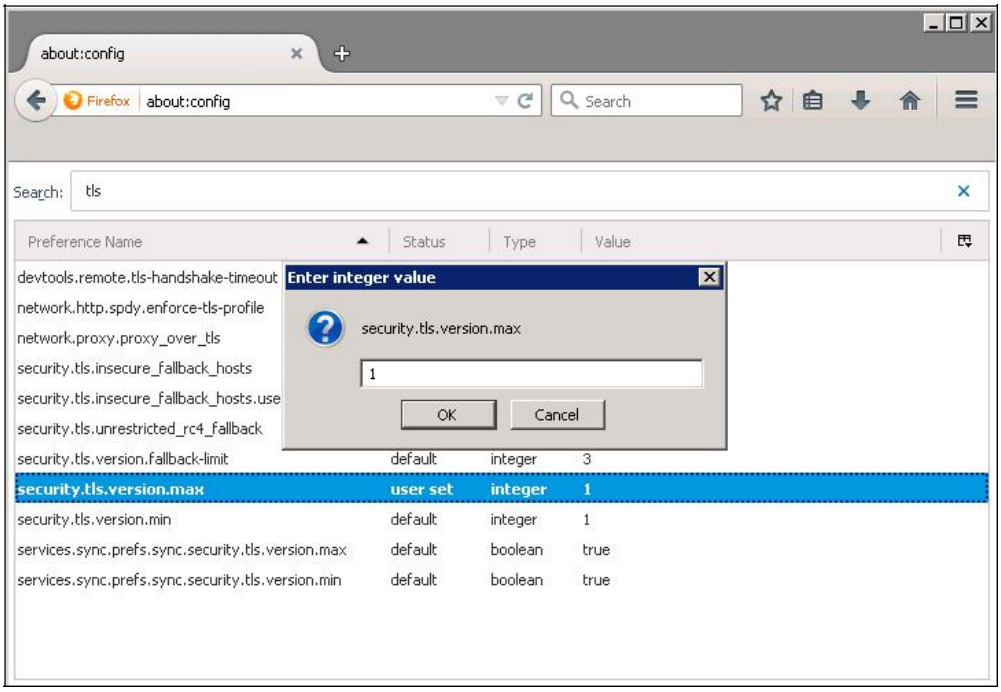
次に、TLS ハンドシェイクでブラウザが TLS 1.0 をサポートしている場合を見てみましょう。Firefox, で新しいタブを開きます（たとえば + タブをクリック）。アドレスバーに「**about:config**」と入力し、警告メッセージを読み、[リスクを理解しました（I Understand the Risks）] をクリックして承認します。図 88 に示すように、[検索（Search）] ボックスに「**tls**」と入力します。

図 88　Firefox での TLS バージョンの設定



security.tls.version.max をダブルクリックし、「**1**」と入力します。提供される TLS の最大バージョンは TLS 1.0 になります。[OK] をクリックします（図 89 を参照）。

図 89　Firefox での TLS バージョン 1 の設定



Firefox で cucm1 に接続しているタブを閉じます。

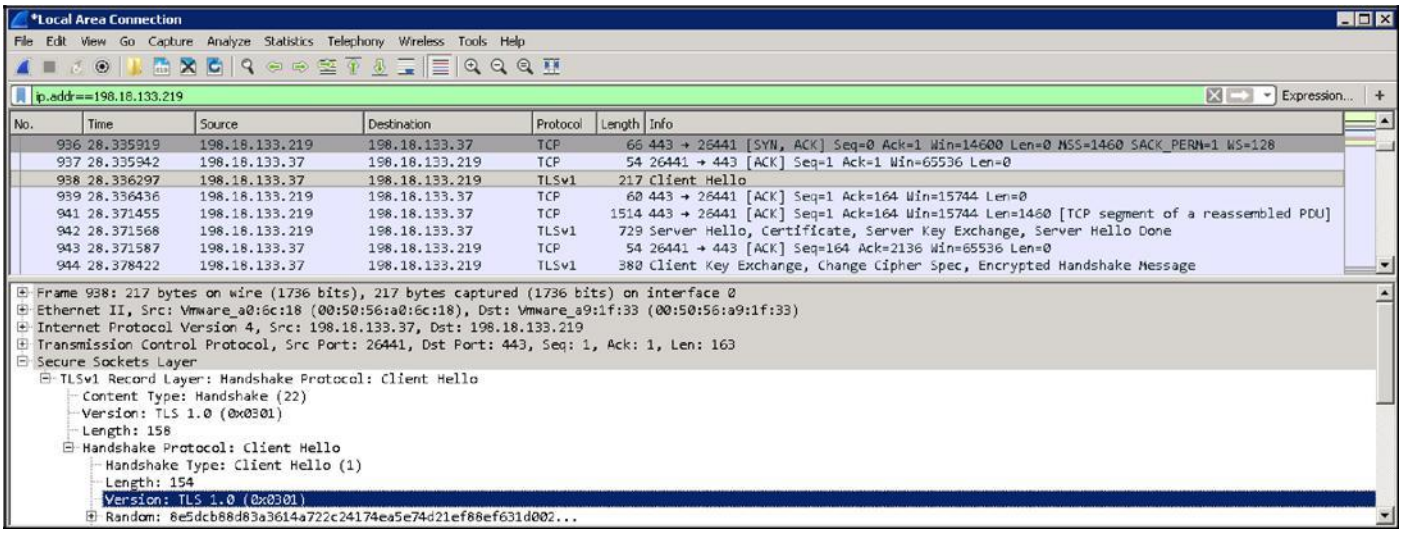
Wireshark に戻り、[パケットのキャプチャを開始（Start Capturing Packets）] ボタン を押してキャプチャを開始します。[保存せずに続行（Continue without Saving）] をクリックします。

新しいタブを開き、cucm1（https://cucm1.dcloud.cisco.com/ccmadmin）の Unified CM 管理インターフェイスに移動します。

Wireshark に戻り、停止ボタン を押してキャプチャを停止します。

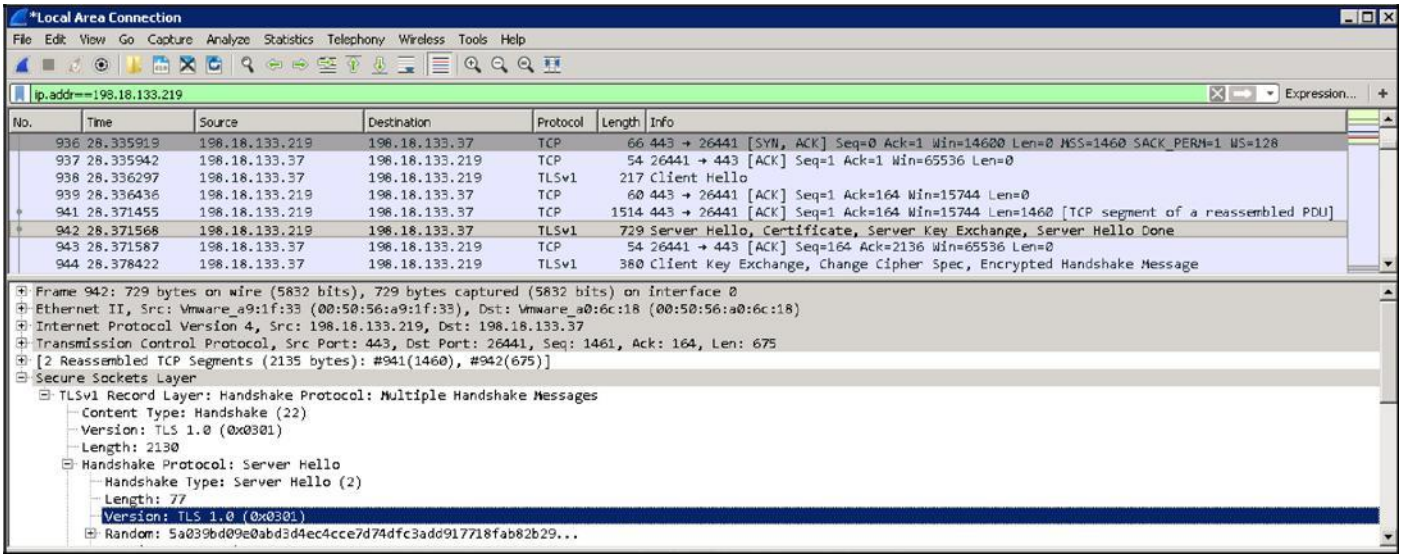
パケットの中から [Client Hello] パケットを探し、パケットの説明のフィールドを展開します。図 90 に示すように、[セキュアソケットレイヤ（Secure Socket Layer）] > [TLSv1.2 レコードレイヤ: ハンドシェイクプロトコル: Client Hello（TLSv1.2 Record Layer: Handshake Protocol: Client Hello）] > [ハンドシェイクプロトコル: Client Hello（Handshake Protocol: Client Hello）] の下に、TLS のバージョンが [バージョン: TLS 1.0 (0x301)（Version: TLS 1.0 (0x301)）] であると表示されます。これは、Unified CM との接続を開始する際に、ブラウザでは TLS 1.0 が使用されることを意味します。

図 90　TLS ハンドシェイクの Client Hello – TLS 1.0



下方向にスクロールし、[Server Hello, Certificate] パケットを見つけます。パケットの説明のフィールドを展開します。[セキュアソケットレイヤ（Secure Socket Layer）] > [TLSv1.2 レコードレイヤ: ハンドシェイクプロトコル: Client Hello（TLSv1.2 Record Layer: Handshake Protocol: Server Hello）] > [ハンドシェイクプロトコル: Client Hello（Handshake Protocol: Server Hello）] の下に、TLS のバージョンが [バージョン: TLS 1.0 (0x301)（Version: TLS 1.0 (0x301)）] であると表示されます（図 91 を参照）。これは、サーバである Unified CM が TLS 1.0 のオファーを承認し、TLS 接続で TLS 1.0 が使用されることを意味します。

図 91　TLS ハンドシェイクの Server Hello – TLS 1.0



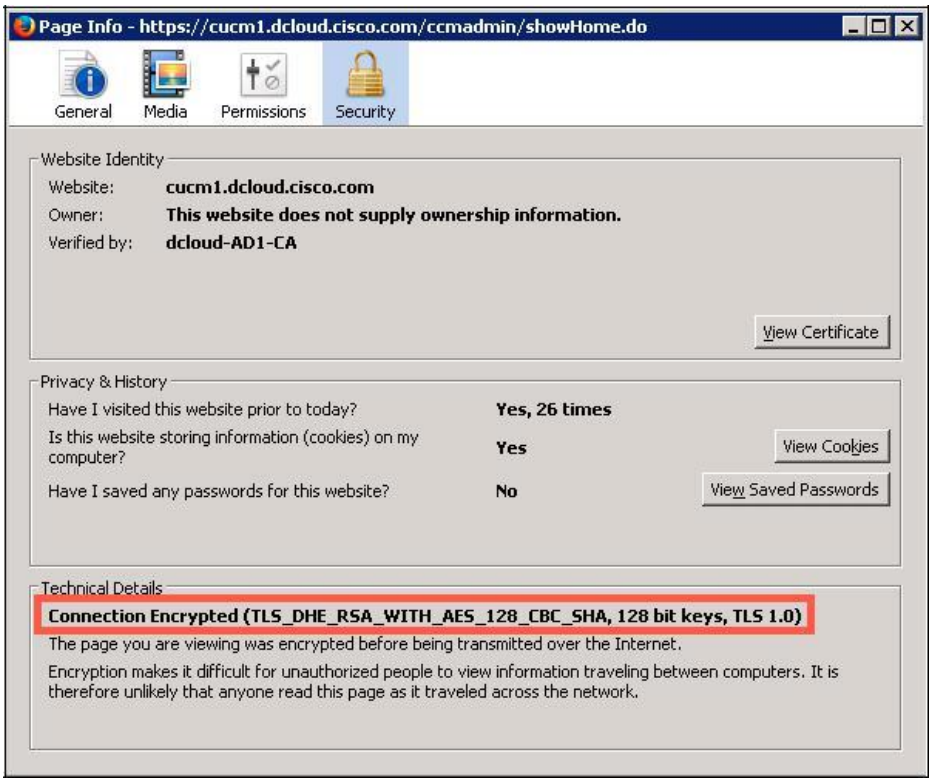
Firefox で Unified CM 管理インターフェイス（https://cucm1.dcloud.cisco.com/ccmadmin）に接続しているタブに戻ります。図 92 に示すように、Firefox バーのロック アイコンをクリックします。

図 92　Firefox でのセキュリティ情報の取得

[詳細情報（More Information…）] をクリックします（図 92 を参照）。

ウィンドウの下部には、ネゴシエートされた TLS のバージョンが表示されます。この例では、図 93 に示すように TLS 1.0 になっています。

図 93　Firefox での TLS 接続の詳細



スニファ トレースでは、クライアントから提供された暗号と、サーバが選択した暗号が表示されます。収集したトレースで Client Hello を見つけ、ブラウザが提供する暗号スイートを確認します（図 94 を参照）。この情報は [セキュアソケットレイヤ（Secure Socket Layer）] > [TLSv1 レコードレイヤ: ハンドシェイクプロトコル: Client Hello（TLSv1 Record Layer: Handshake Protocol: Client Hello）] > [暗号スイート(X スイート)（Cipher Suites (X suites)）] に表示されます。X は TLS クライアント（この場合はブラウザ）が提供する暗号スイートの数を示します。

図 94　TLS ハンドシェイクの Client Hello – 提供される暗号

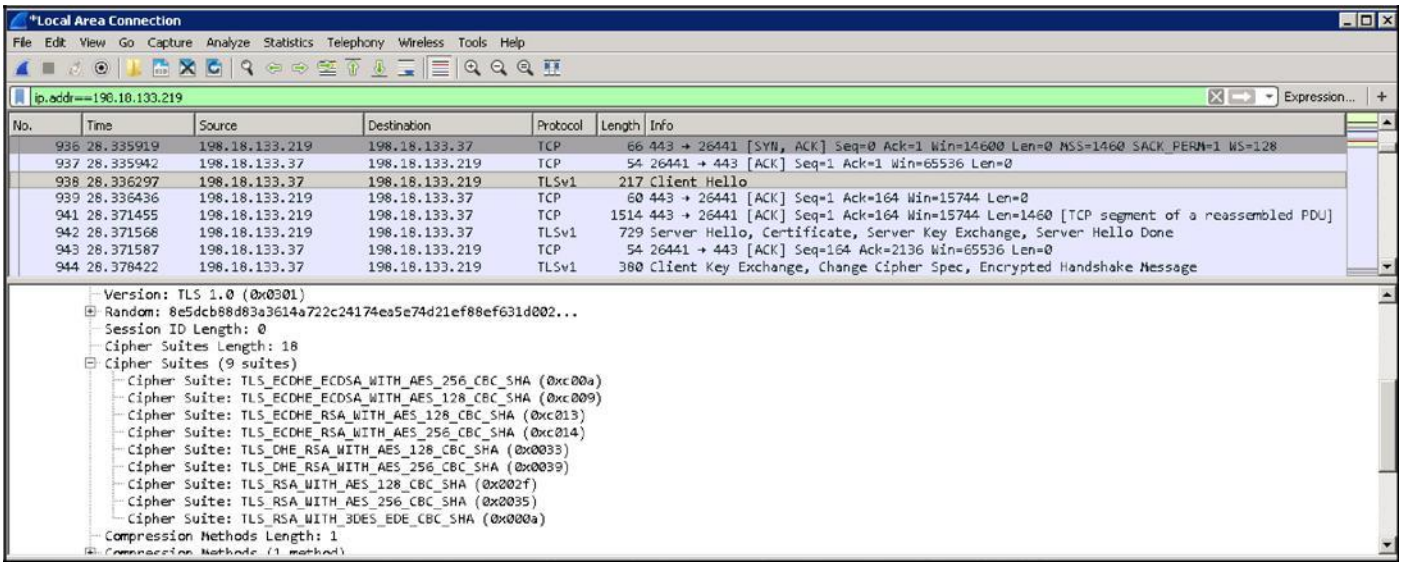
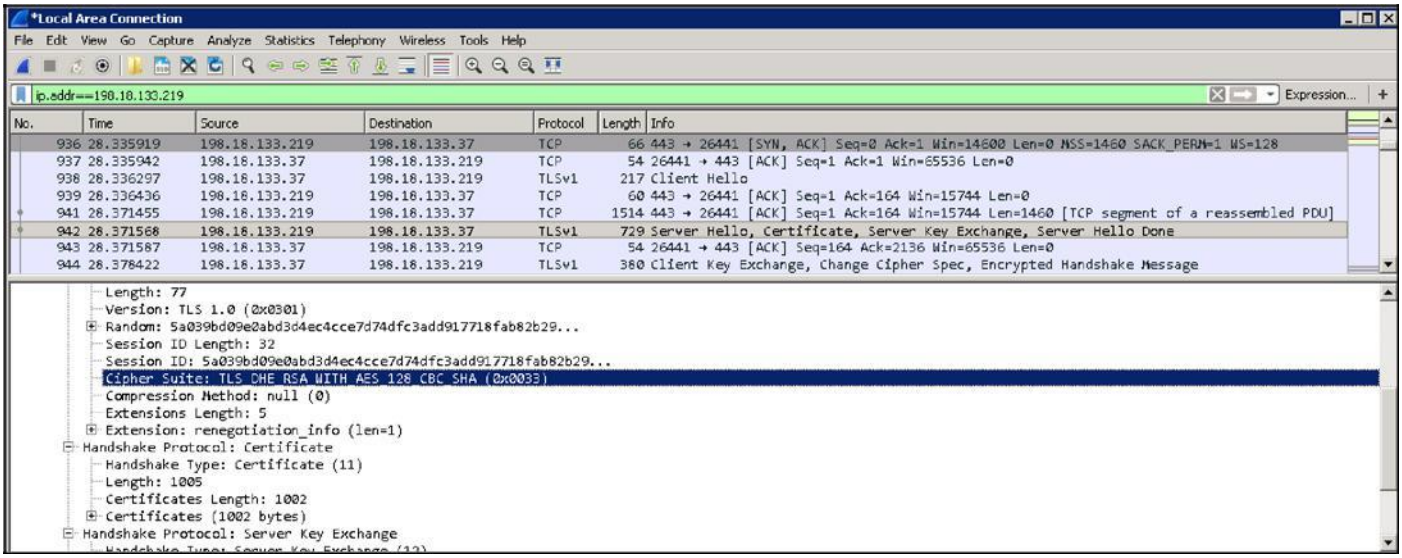


図 95 に示すように、Server Hello では Unified CM が選択した暗号を確認できます。

図 95　TLS ハンドシェイクの Server Hello – 暗号の選択



C. NMAP を使用して、Web および SIP インターフェイスで許可される TLS のバージョンと暗号を確認する

nmap ツールも非常に役立ちます。nmap Web サイト（https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html）からダウンロードできる **ssl-enum-ciphers** スクリプトを使用して、TLS サーバ インターフェイス で使用できる TLS のバージョンと暗号を判定できます。このラボでは、nmap の GUI バージョンである zenmap を使用します。zenmap はすでに WKST3 にインストールされています。

WKST3 で、Nmap - Zenmap GUI という nmap プログラムを開きます。 

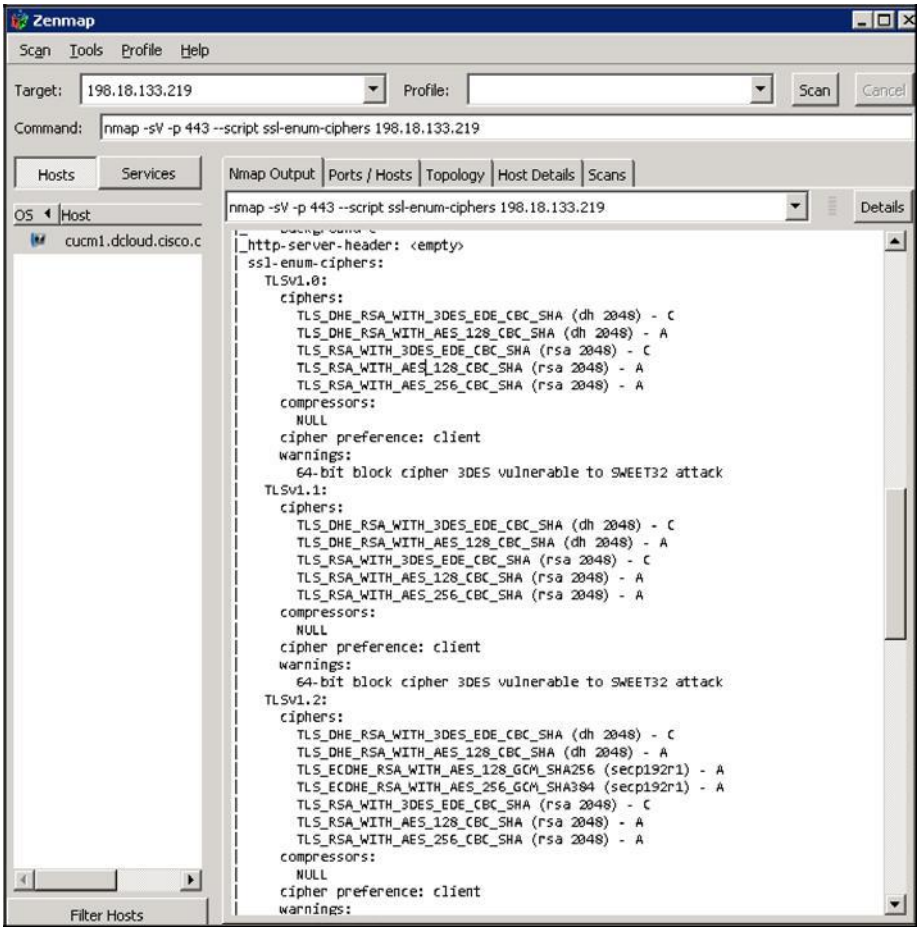
[コマンド（Command）] ウィンドウに次のコマンドを入力します（図 96 を参照）。

```
nmap -sV --script ssl-enum-ciphers -p 443 198.18.133.219
```

このコマンドの実行には、しばらく時間がかかる場合があります。スキャンが完了したら、必要に応じて上方向にスクロールします。

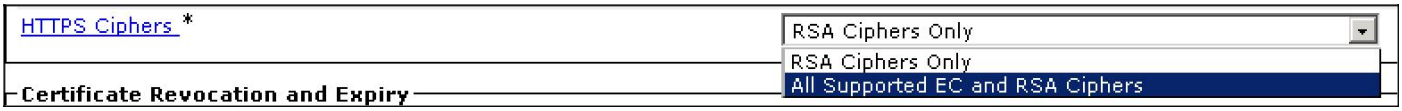
図 96 に示すように、Unified CM のポート 443 では、TLS 1.0、TLS 1.1、TLS 1.2 を使用できます。これらのバージョンの TLS で使用可能な暗号を確認してください。ここでわかるように、ECDSA ベースの暗号はありません。デフォルトでは、HTTPS インターフェイスで ECDSA は無効になっています。

図 96. NMAP を使用して HTTPS インターフェイスをスキャン



なお、ECDSA ベースの暗号を有効にするには、[エンタープライズパラメータ（Enterprise Parameter）] ページに移動し、[HTTPS 暗号（HTTPS Ciphers）] を、デフォルトの [RSA 暗号のみ（RSA Ciphers Only）] ではなく [サポートされているすべての EC および RSA 暗号（All Supported EC and RSA Ciphers）] に設定します（図 97 を参照）。ただしこれは、tomcat-ECDSA に CA が署名していないため、**このラボでは行いません**。

図 97. HTTPS インターフェイスの暗号設定



次に、TLS のバージョンと、Unified CM SIP インターフェイスのポート 5061 で許可されている暗号を確認します。次のコマンドを入力します（図 98 を参照）。

```
nmap -sV --script ssl-enum-ciphers -p 5061 198.18.133.219
```

図 98. NMAP を使用して SIP TLS インターフェイスをスキャン

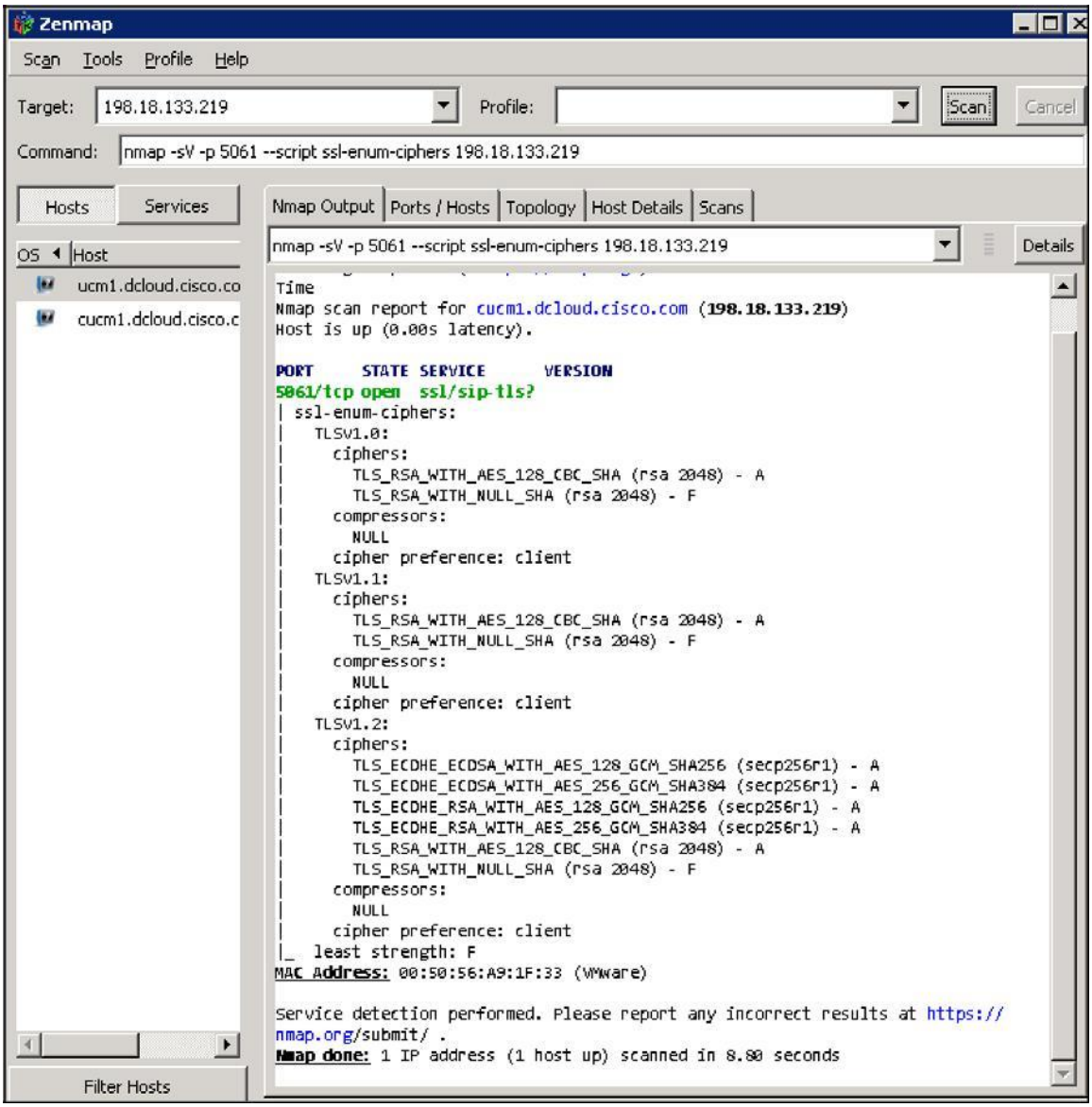


図 98 では、Unified CM のポート 5061（SIP TLS ポート）で TLS 1.0、TLS 1.1、TLS 1.2 を使用できることを示しています。また、それらのバージョンの TLS で使用可能な暗号も確認できます。ここでわかるように、NULL 暗号が許可されています。これは、証明書の検証によって接続が認証されながら実際に暗号化されない（NULL 暗号）、「認証済み」のセキュリティ モード専用です。この暗号は、この認証済みセキュリティ モードが設定された端末でのみ承認されるため、セキュリティ上の問題にはなりません。

続行する前に、**Nmap - Zenmap** GUI を閉じます。

D. TLS 1.0 および 1.1 の無効化

組織によっては、Payment Card Industry（PCI）の要件に適合するために、TLS 1.0/1.1 を完全に無効にする場合があります。その場合は、TLS サーバ インターフェイスで実際に TLS 1.0/1.1 を無効にすることになります。これはほとんどの Cisco Collaboration 製品で行うことができます。次のページで、Cisco Collaboration TLS 1.2 の互換性マトリックスとホワイト ペーパーを参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html [英語]、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/TLS/TLS-1-2-for-On-Premises-Cisco-Collaboration-Deployments.html [英語]

Unified CM では、これは 11.5(1) SU3 と 12.0(1) から可能になります。このセクションでは、TLS の最小バージョンを 1.2 に設定することで、実際上 TLS 1.0 と TLS 1.1 を無効にします。これは 11.5(1) SU3 システム（cucm1.dcloud.cisco.com）で行います。

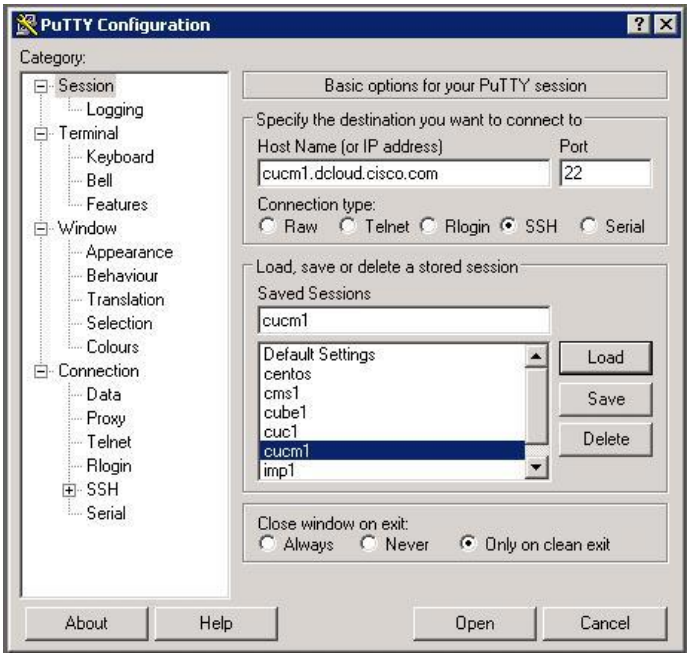
PuTTY アイコンをダブルクリックして 

起動します。

SSH 経由で cucm1.dcloud.cisco.com に接続します（図 99 を参照）。

注：次の設定は、11.5(1) SU3 システム **cucm1.dcloud.cisco.com** で行います。

図 99. PuTTY を使用して cucm1 に接続

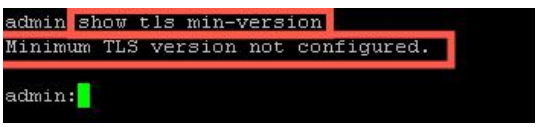


[開く（Open）] をクリックして、セキュリティ アラートが表示された場合は承認します。ユーザ名/パスワード：

administrator/dCloud123! を使用してログインします。

show tls min-version コマンドを入力して、現在の設定を確認します。図 100 にデフォルトの設定を示します。

図 100. Unified CM における現在の TLS の最小バージョンを確認する



デフォルトでは TLS の最小バージョンが設定されていないため、TLS 1.0、1.1、1.2 が許可されます。

set tls min-version 1.2 コマンドを入力して、TLS の最小バージョンを 1.2 に設定します。

注：「**Yes**」と入力して確定すると、画面に [Yes] と表示されなくなります。「Yes」と入力したら Enter を押します。

実際上、これで TLS 1.0 と TLS 1.1 が無効になります。このコマンドはすべての TLS サーバ インターフェイスに適用されます。また、LDAP インターフェイスや SIP クライアント インターフェイスなど、一部の TLS クライアント インターフェイスにも適用されます。

図 101 に示すように、このコマンドを入力すると、システムが自動的に再起動します。

ここで休憩を取ることもできます。☺

このコマンドは、接続しているノードだけに適用されます。Unified CM クラスタには複数のノードがあるため、このコマンドはクラスタ内のすべてのノードで発行する必要があります。

図 101. Unified CM における TLS の最小バージョンの設定

```
admin:set tls min-version 1.2

This command will result in setting minimum TLS version to 1.2 on all the secure interfaces.
 If you have custom applications that makes secure connection to the system, please ensure they support the TLS version
you have chosen to configure.
 Also, please refer to the Cisco Unified Reporting Administration Guide to ensure all the endpoints in your deployment s
upports this feature

********************************************************************************

Warning: This will set the minimum TLS to 1.2 and the server will reboot.

********************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.2

The system will reboot in a few minutes.

Stopping Service Manager...
/ Service Manager shutting down services... Please Wait
```

E. ブラウザ専用の TLS 1.0 に対応している場合、TLS 接続が拒否されることを確認する

先に、TLS の最小バージョンを 1.0 にして Firefox ブラウザを設定しました。TLS の最小バージョンを 1.2 にして Unified CM を設定していたため、Firefox ブラウザと Unified CM との TLS 接続が失敗します。このセクションの状況はこのようになります。

サーバが再起動したら、**SSH** 経由で（PuTTY を使用して）サーバに再度接続します。

図 102 に示すように、**show tls min-version** コマンドを入力して現在の設定を確認します。

図 102. Unified CM における現在の TLS の最小バージョンを確認する

```
admin:show tls min-version
Configured TLS minimum version: 1.2

admin:
```

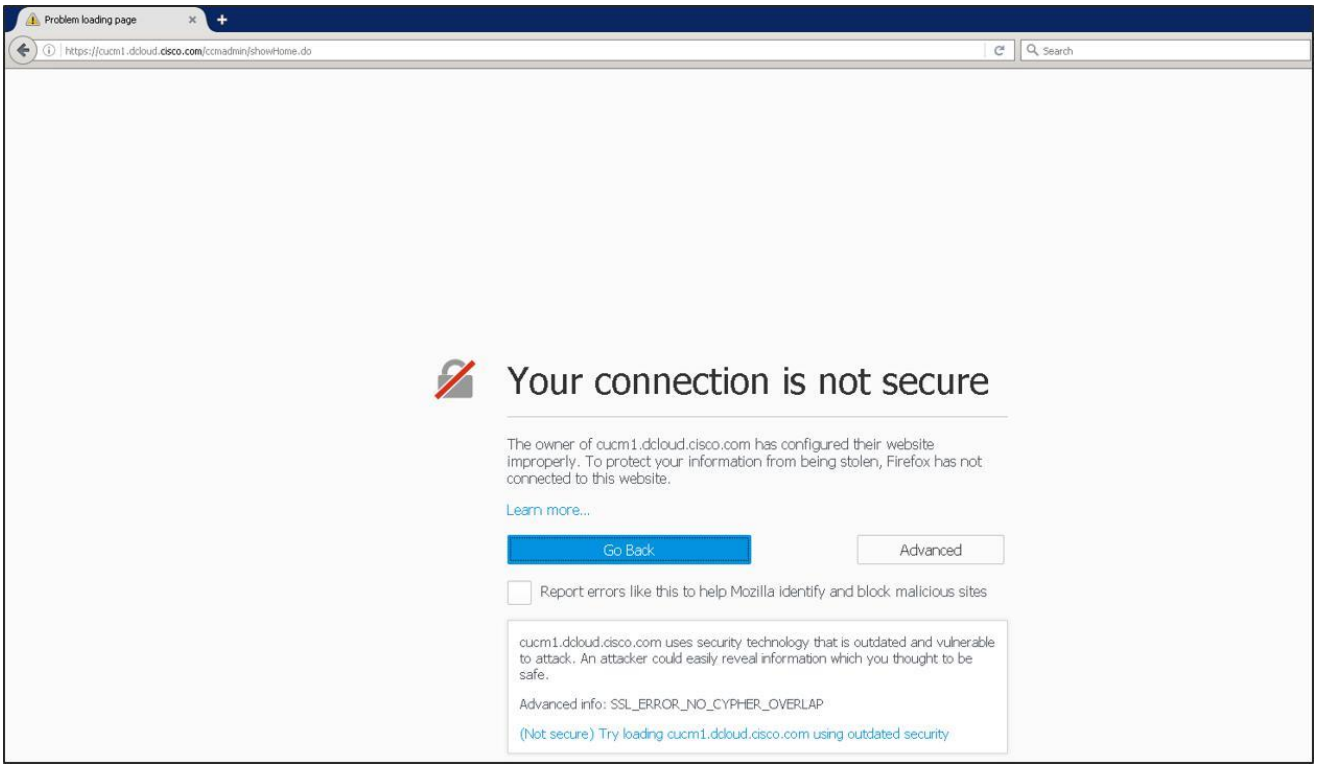
開いていない場合は Wireshark を開き、キャプチャを開始します。

まだ入力されていなければ、フィルタバーに「**ip.addr==198.18.133.219**」と入力します。

Firefox Web ブラウザで、**cucm1** に接続されているすべてのタブを閉じます。Unified CM 管理インターフェイス（https://cucm1.dcloud.cisco.com/ccmadmin）に接続する新しいタブを開きます。ログインを試みます。

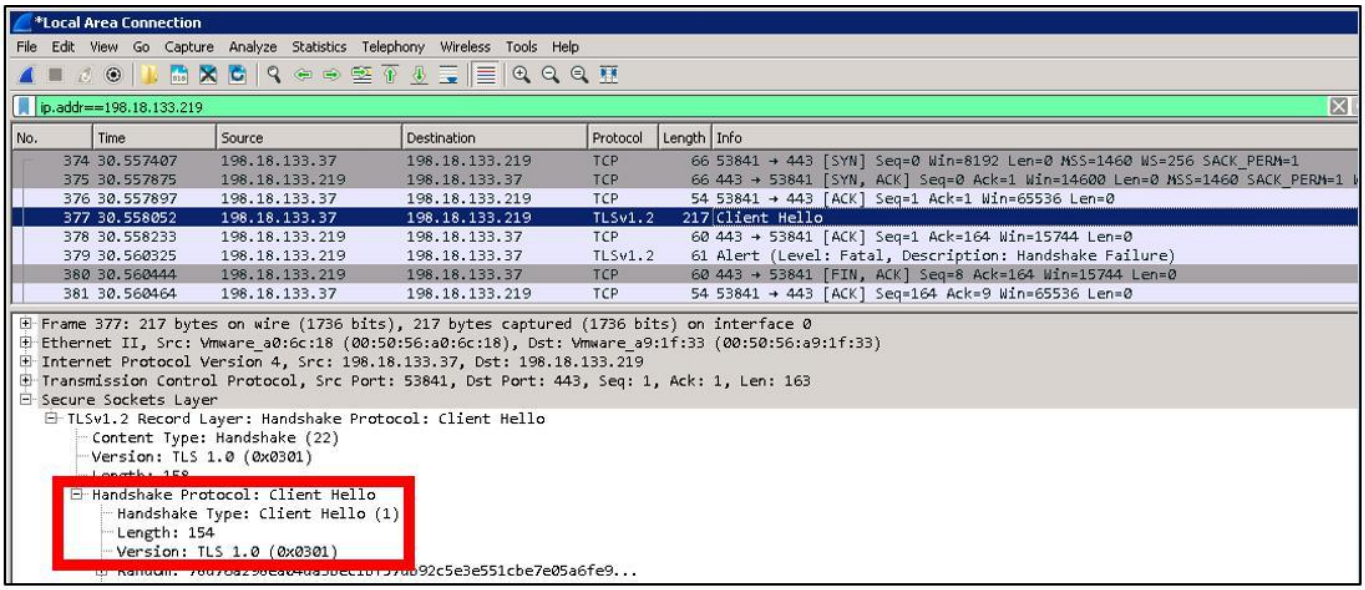
図 103 に示すように、ログインが失敗します。これは Firefox が、バージョン 1.0 の TLS を使用するように設定されていたためです。このバージョンは **cucm1** では許可されていません。次の図のように表示されます。エラー メッセージは Firefox のバージョンによって異なります。通常は他の Web ブラウザについても同様です。

図 103. TLS バージョンの不一致によって TLS の接続に失敗した場合の Firefox のエラー



Wireshark でスニファのキャプチャを停止します。ブラウザから送信された Client Hello を探します。図 104 に示すように、提示された TLS のバージョンは TLS 1.0 です。

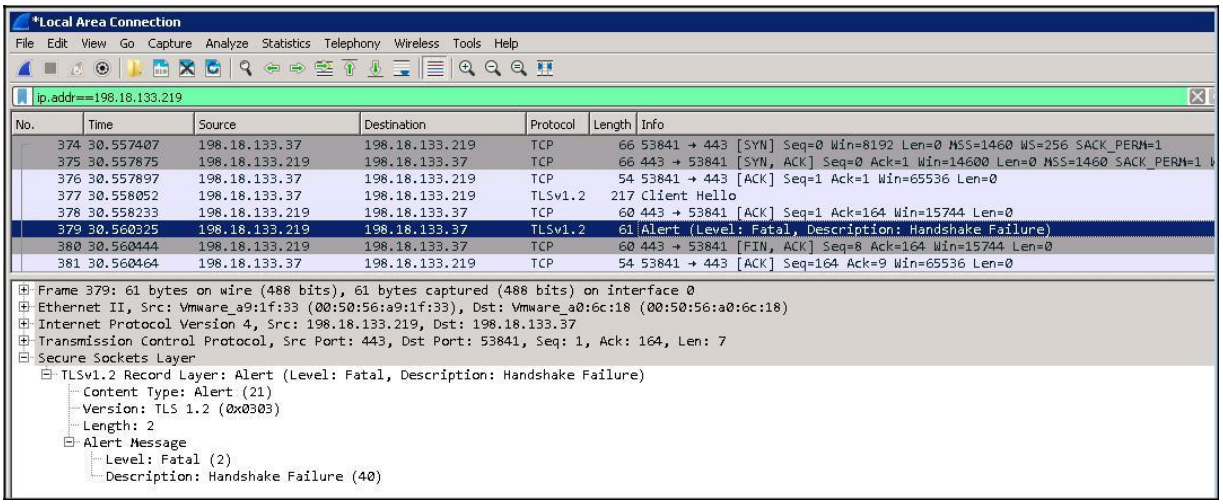
図 104. Firefox で TLS 1.0 がサポートされている場合の TLS ハンドシェイクでの Client Hello



注: ここでも最初の TLS バージョン（ヘッダーの TLS バージョン）ではなく、Client Hello の TLS バージョンを確認します（[Client Hello] > [Handshake Protocol: Client Hello]）。図 104 を参照してください。

cucm1 が送信する応答を見てください。Server Hello ではなく、TLS ハンドシェイクが失敗したことを示す Alert メッセージが送信されています（図 105 を参照）。

図 105. Unified CM が TLS 接続を拒否した場合の TLS ハンドシェイクのエラー



次に Firefox で、TLS 1.1 と TLS 1.2 を再度有効にします。

Firefox ブラウザで、新しいタブに「**about:config**」と入力し、[検索（Search）] ボックスに「**tls**」と入力し、[security.tls.version.max] を [3] に設定して、TLS 1.1 と 1.2 を再度有効にします。

Firefox ブラウザで、**cucm1** Unified CM 管理インターフェイス（https://cucm1.dcloud.cisco.com/ccmadmin）に再度接続します。これは成功するはずです。

図 106 に示すように TLS 1.0 と 1.1 を再度有効にするには、**set tls min-version 1.0** コマンドを入力して、TLS 1.0、1.1、1.2 が許可されるデフォルト設定に戻します。確定すると、Unified CM が自動的に再起動します。

注：これは方法を示すための説明です。TLS 1.0 と 1.1 を再度有効にするにはシステムの再起動が必要になるため、時間の関係から、**この操作は行わない**でください。再起動には 10 分程度かかる可能性があります。

図 106. TLS 1.0 と 1.1 を再度有効にする*

```
admin:set tls min-version 1.0

This command will result in setting minimum TLS version to 1.0 on all the secure interfaces.
 If you have custom applications that makes secure connection to the system, please ensure they
support the TLS version you have chosen to configure.
 Also, please refer to the Cisco Unified Reporting Administration Guide to ensure all the endpoi
nts in your deployment supports this feature

********************************************************************************

Warning: This will set the minimum TLS to 1.0 and the server will reboot.

********************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.0

The system will reboot in a few minutes.

Stopping Service Manager...
/ Service Manager shutting down services... Please Wait
```

** ここでは図を示しているだけです。システムの再起動が必要であり、時間がかかるため、このラボではこの手順を実行しません。*

F. 他のアプリケーションで TLS 1.0 と 1.1 を無効にする方法

TLS の最小バージョンを設定する機能は、このラボで示す他の製品でも使用できます。

IM & Presence や Unity Connection でも、機能は同じです。Unified CM と同じプラットフォームを使用しており、CLI も同一であるため、このラボでは設定を確認しません。

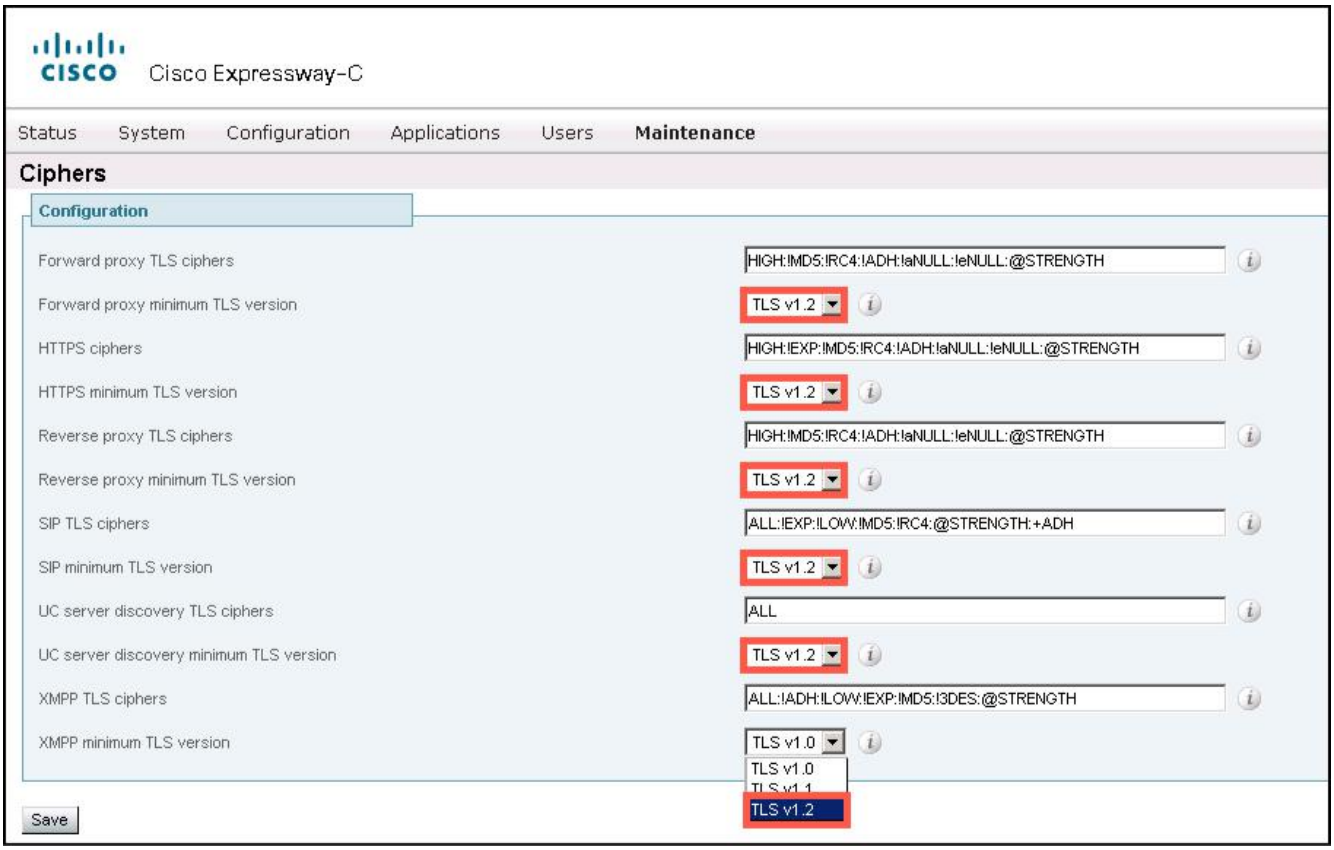
Cisco Expressway

Expressway にも TLS の最小バージョンを設定する機能がありますが、さらにきめ細かい設定が可能であり、各種のインターフェイスで TLS の最小バージョンを設定できます。WKST3（198.18.133.38）の Firefox ブラウザで、https://exp-c-1.dcloud.cisco.com の **Expressway-C サーバ**に移動し、ユーザ名/パスワード：**admin/dCloud123!** でログインします。信頼できない接続を示す警告が表示された場合は承認し、[この例外を永久に保存（Permanently store this exception）] をオフにします。

[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [暗号（Ciphers）] に移動します。図 107 に示すように、各種のインターフェイスで、TLS の最小バージョンを 1.2 に設定できることを確認します。

注：次の図 107 は、Expressway における TLS の最小バージョンの設定方法を示しています。図のように、Expressway には、TLS の最小バージョンを TLS v.1.2 に設定するオプションがあります。この設定を行っても、ラボの結果には影響しません。

図 107. Expressway-C サーバの暗号設定



Cisco Unified Border Element（CUBE）

SIP インターフェイスでは、Cisco IOS ベースの製品について、TLS のバージョンを正確に設定することも可能です。デフォルトでは、すべての TLS バージョンが許可されます。管理者は、許可される TLS のバージョンを指定して、このデフォルトの動作を上書きできます。

それによって TLS 1.2 だけを許可することができます。TLS 1.1 だけを許可することも可能です。ただし、TLS 1.0 を無効にして TLS 1.1 と TLS 1.2 を有効にすることはできません。

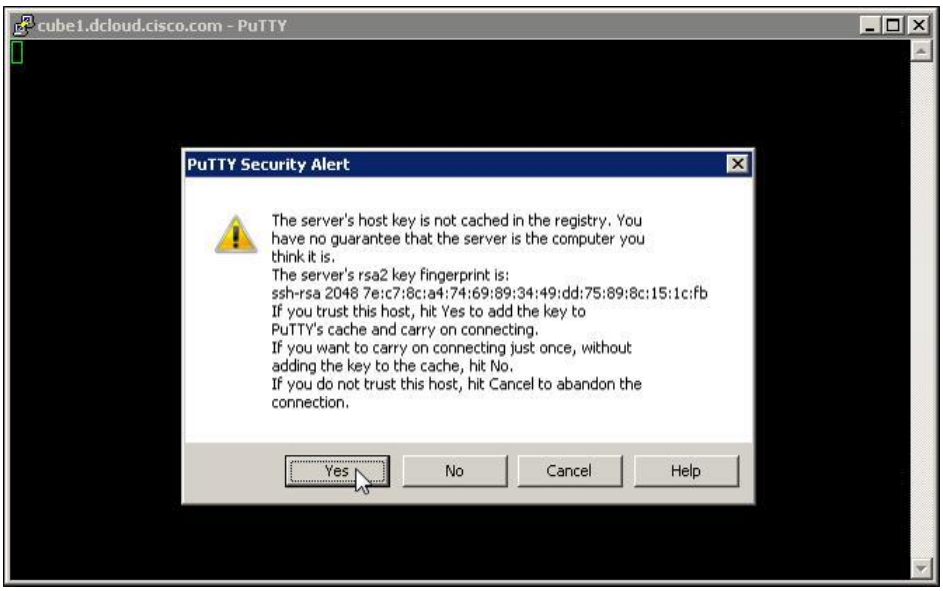
WKST3 で PuTTY を使用して、CUBE（cube1.dcloud.cisco.com）コマンド ライン インターフェイスに **SSH** 接続します。

PuTTY アイコンをダブルクリックして 

起動します。**cube1** プロファイルを選択するか、[ホスト名（Host Name）] フィールド（または [IP アドレス（IP Address）] フィールド）に「**cube1.dcloud.cisco.com**」と入力します。[開く（Open）] をクリックします。

図 108 に示すように、[はい（Yes）] をクリックして ssh-rsa2 キーをキャッシュします。

図 108. CUBE との SSH 接続におけるキー キャッシュの確認



ユーザ名/パスワード：**admin/dCloud123!** でログインします。

ログインしたら、**show run | section sip-ua** コマンドを実行して現在の設定を確認し、sip-ua の設定が空白であることを確認します（図 109 を参照）。

図 109. IOS での SIP インターフェイス設定の表示

```
cube1#sh run | section sip-ua
cube1#
```

次のように入力して設定モードに入ります。

```
config t
```

さらに図 110 に示すように次のコマンドを実行して、IOS 端末で TCP と TLS v1.2 を使用するように設定します。

```
sip-ua
transport tcp tls v1.2
```

図 110. IOS の SIP インターフェイスにおける TLS のバージョン設定

```
cube1(config)#sip-ua
cube1(config-sip-ua)#transport tcp tls v1.2
cube1(config-sip-ua)#end
```

CUBE の SIP インターフェイスで TLS 1.2 を設定しました。

次のコマンドを入力して、CUBE の設定を保存します。

```
write memory
```

Cisco Meeting Server

Cisco Meeting Server では、TLS の最小バージョンを CMS リリース 2.3 から設定することもできます。CMS で TLS の最小バージョンを設定するには、**tls <service> min-tls-version <minimum version string>** コマンドを実行します。サービスとしては、sip、webadmin、または ldap を指定します。sip サービスは SIP プロトコル用です。webadmin サービスは Web サービス用であり、たとえば Unified CM が CMS との接続に使用する HTTP 管理インターフェイスや HTTP インターフェイスが含まれます。ldap サービスは LDAP サーバとのアウトバウンド接続用です。

コマンドはたとえば **tls sip min-tls-version 1.2** にします。11.5.1 SU3 より前のリリースの Unified CM では、CMS に対する HTTPS インターフェイスで、TLS 1.2 はサポートされていません。そのため、Web インターフェイスでそれらの Unified CM リリースを実行している場合は、TLS 1.2 を使用できません。このラボはそれに該当しないため、以降のリリースの Unified CM を実行します。

ここで、CMS での TLS の最小バージョンを設定しましょう。

WKST3（198.18.133.38）で PuTTY を使用し、cms1.dcloud.cisco.com（198.18.134.175）に **SSH** 接続します。[PuTTY セキュリティアラート（PuTTY Security Alert）] ウィンドウが表示されたら、[はい（Yes）] をクリックしてホスト キーをキャッシュします（図 111 を参照）。

図 111. SSH キーのキャッシュに関する警告

ユーザ名/パスワード：**admin/dCloud123!** でログインします。ログインしたら、コマンド プロンプトで次のコマンドを入力します。

```
tls sip min-tls-version 1.2
tls ldap min-tls-version 1.2
tls webadmin min-tls-version 1.2
```

これを次の図 112 に示します。

図 112. CMS で TLS の最小バージョンを設定

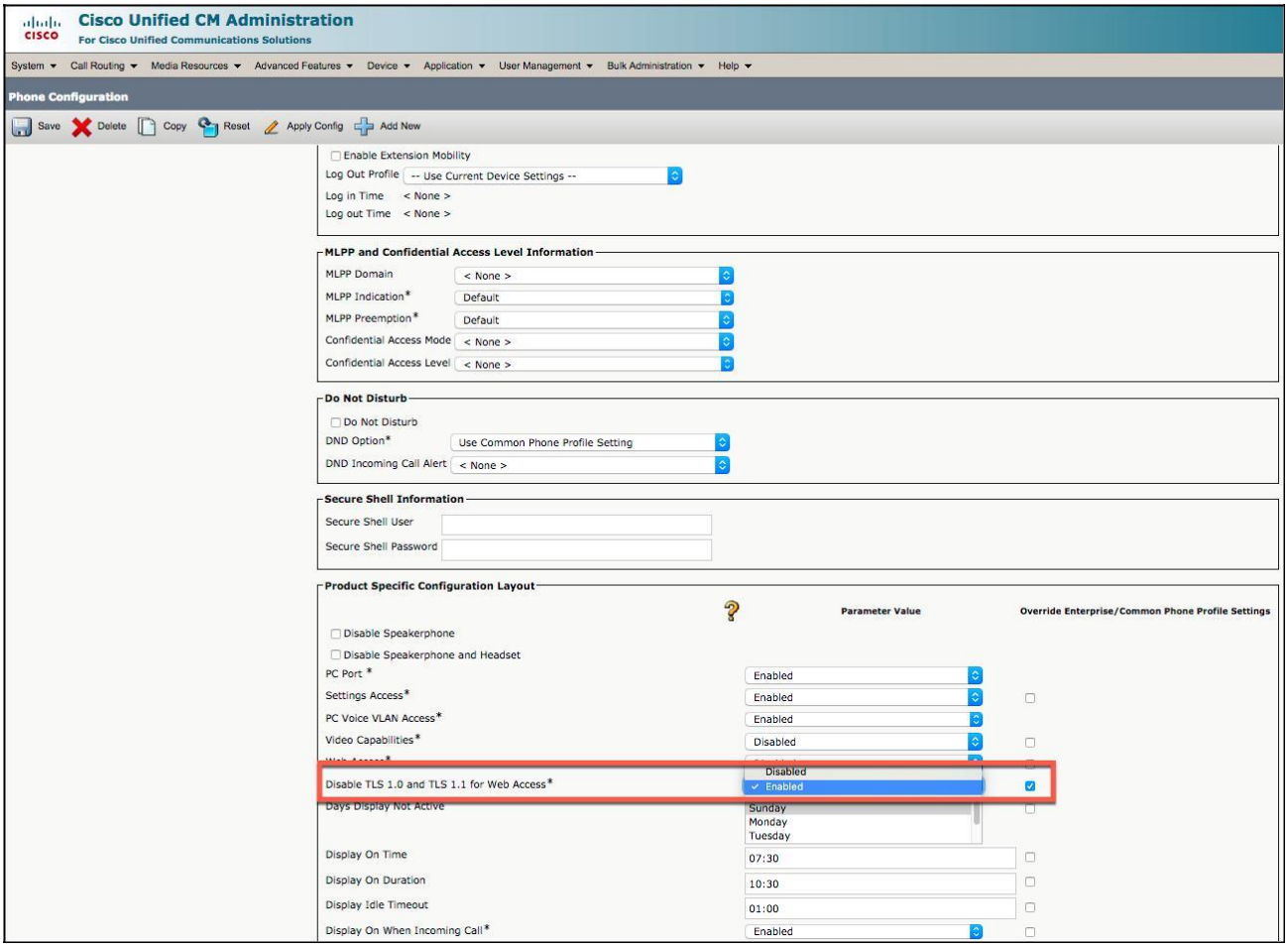
```
cms1> tls sip min-tls-version 1.2
cms1> tls ldap min-tls-version 1.2
cms1> tls webadmin min-tls-version 1.2
cms1>
```

これで、CMS で TLS の最小バージョンを設定しました。

Cisco IP Phone 7800 および 8800 シリーズ

IP Phone の 7800 と 8800 では、TLS 1.0/1.1 の無効化は Unified CM の電話設定ページの設定フィールドで行います。このラボの開発時には、適切な設定フィールドは用意されていませんでしたが、次の図 113 にプレビューを示します。

図 113. 7800/8800 シリーズ用に TLS の最小バージョンを設定



7800/8800 シリーズの IP 電話では、この方法で TLS 1.0 と TLS 1.1 を無効にします。

Wireshark、Firefox、開いているその他のアプリケーションまたはウィンドウを閉じます。これで、TLS 1.2 に関するモジュールは終了です。

***** モジュール #3 の終了 *****

モジュール 4. ITL リカバリ

モジュールの概要

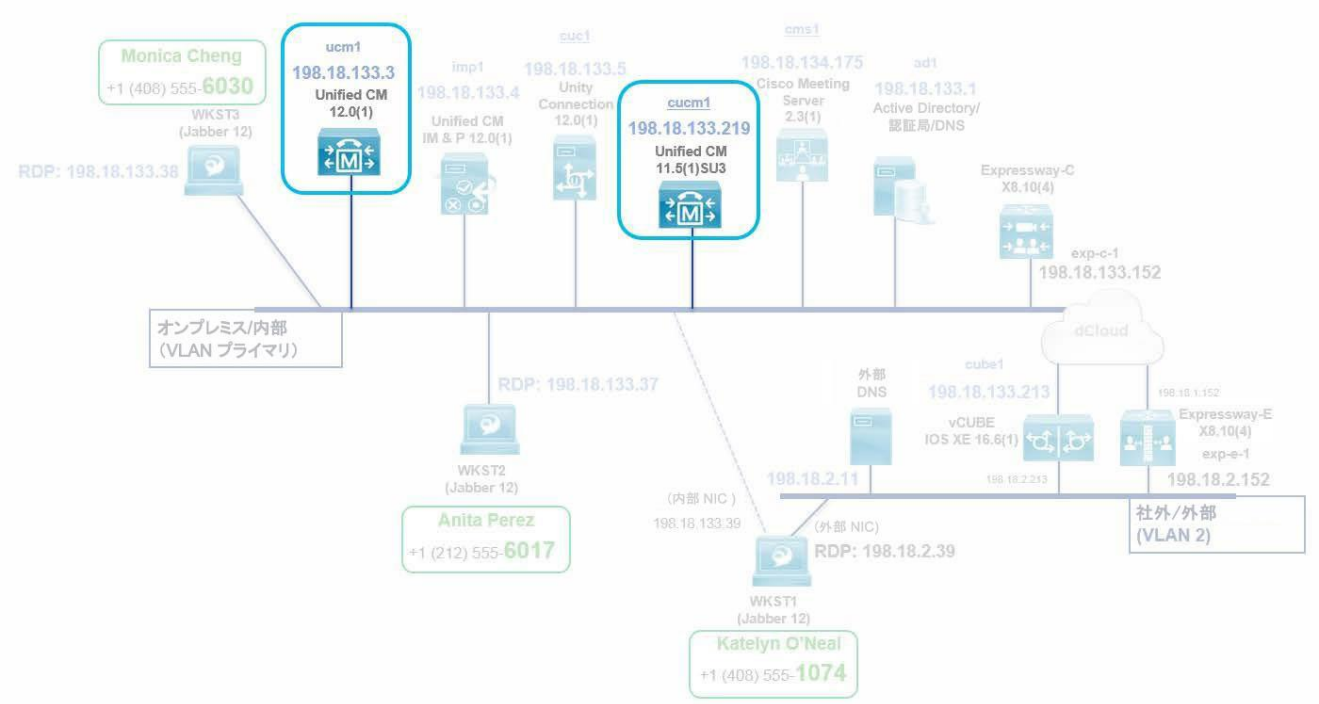
このモジュールでは、ITL ファイルやトークンレス CTL ファイルの署名者に関する、Unified CM 12.0(1) の変更点を示します。
このモジュールは次の 2 つのセクションに分かれています。

A. ITL ファイルとトークンレス CTL ファイルの新しい署名者の確認

B. Phone-SAST 信頼ストアに ITL リカバリ証明書をインポートして新しい ITL ファイルとトークンレス CTL ファイルを確認する

図 114 に、このモジュールでのトポロジおよび関連するコンポーネントを示します。

図 114. モジュール 4：ITL リカバリ トポロジ



手順

A. ITL ファイルとトークンレス CTL ファイルの新しい署名者の確認

Unified CM リリース 12.0(1) 以降、ITL ファイルとトークンレス CTL ファイルは、CallManager キーではなく ITLRecovery キーによって署名されるようになります。それにより、CallManager 証明書と TVS 証明書が再生成された場合などに、電話機と Unified CM 間の信頼状態が失われることが防止されます。ITLRecovery は 20 年間有効な長期的なトラスト アンカーであり、CallManager 証明書や TVS 証明書が再生成されても変更されません。

WKST3（198.18.133.38、ユーザ名/パスワード：**DCLOUD\mcheng/C1sco12345**）に **RDP** 接続します。

PuTTY アイコン 

をダブルクリックして起動します。[ホスト名（Host Name）] フィールド（または [IP アドレス（IP Address）] フィールド）に「**ucm1.dcloud.cisco.com**」と入力するか、リストに含まれている場合はそれを選択します。[開く（Open）] をクリックします。セキュリティ アラート ウィンドウが表示されたら、[はい（Yes）] をクリックして ssh-rsa2 キーをキャッシュします。

ユーザ名/パスワード：**administrator/dCloud123!** でログインし、**show ctl** コマンドを入力します。

ITLRecovery 証明書が含まれているレコード（SubjectName の先頭が CN=ITLRECOVERY）を探します。レコードの末尾が「**This eToken was used to sign the CTL File**」であることを確認します。

これは Unified CM リリース 12.0(1) で変更された動作です。従来は、トークンレス CTL が CallManager キーによって署名されていました。同じことが ITL ファイルにも当てはまります。**show itl** コマンドを実行します。ITLRecovery 証明書が含まれているレコード（SubjectName の先頭が CN=ITLRECOVERY）を探します。図 115 に示すように、レコードの末尾が「This etoken was used to sign the ITL File」であることを確認します。

図 115. ITL ファイルの署名者

```
        ITL Record #:2
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1758
2       DNSNAME         2
3       SUBJECTNAME     90      CN=ITLRECOVERY_ucm1.dcloud.cisco.com;OU=dCloud;O=Cisco Systems;L=Richardson;ST=Texas;C=US
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      90      CN=ITLRECOVERY_ucm1.dcloud.cisco.com;OU=dCloud;O=Cisco Systems;L=Richardson;ST=Texas;C=US
6       SERIALNUMBER    16      66:C1:0F:B2:4A:8E:E9:15:F1:50:E3:E4:33:98:44:E1
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     1003    78 78 27 44 59 DB CF DD 4D 98 79 00 B7 A4 7A 8C 68 0B E8 A8 (SHA1 Hash HEX)
This etoken was used to sign the ITL file.
```

Unified CM 12.0 より前は、CallManager 証明書と TVS 証明書を再生成すると、Unified CM に対する電話機の信頼が失われる場合がありました。この状況は、たとえば電話機がネットワークに接続されていないときに、管理者が CallManager と TVS 両方の証明書を再生成して、電話機をネットワークに再接続した場合などに生じます。その場合は、電話機から Unified CM に対する信頼が失われ、トークンレス CTL ファイルや ITL ファイルの署名を確認できないため承認せず、新しい CallManager 証明書を取得できません。それによって TFTP 設定ファイルが承認されないため、電話機が暗号化モードである場合は登録ができなくなります。

Unified リリース 12.0 以降では、トークンレス CTL ファイルと ITL ファイルが ITL リカバリ キーによって署名されます。CallManager 証明書と TVS 証明書を再生成すれば、電話機がすでに信頼している ITL リカバリ キーによってファイルが署名されるため、上述の状況は発生しません。新しいトークンレス CTL ファイルと ITL ファイルを承認することで、電話機がトークンレス CTL ファイルと ITL ファイル内の Unified CM から新しい証明書を取得することになり、信頼が維持されます。

ITLRecovery は、有効期限が 20 年の長期的なトラスト アンカーです。CallManager 証明書を更新しても変更されません。

B. Phone-SAST 信頼ストアに ITL リカバリ証明書をインポートして新しい ITL ファイルとトークンレス CTL ファイルを確認する

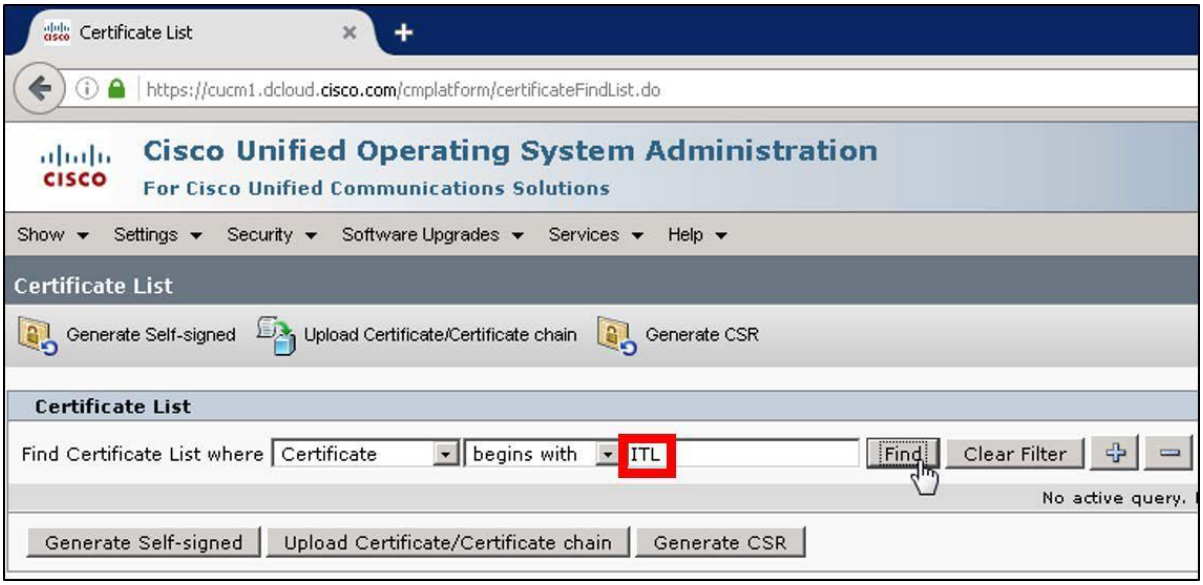
注：この手順では最初に、このモジュールのこれまでの手順とは異なる Unified CM にログインします。正しいサーバ **cucm1.dcloud.cisco.com** に移動したことを確認します。

この手順では、ITL リカバリ証明書を cucm1（Unified CM 11.5(1) SU3）から ucm1（Unified CM 12.0(1)）の phone-sast 信頼ストアにインポートします。ファイルをインポートしたら、ITL ファイルとトークンレス CTL ファイルを確認し、その利点について考えます。

Firefox Web ブラウザを開き、**cucm1**（https://cucm1.dcloud.cisco.com/cmplatform）の Unified CM Operating System 管理インターフェイスに移動し、必要に応じてユーザ名/パスワード：**administrator/dCloud123!** でログインします。

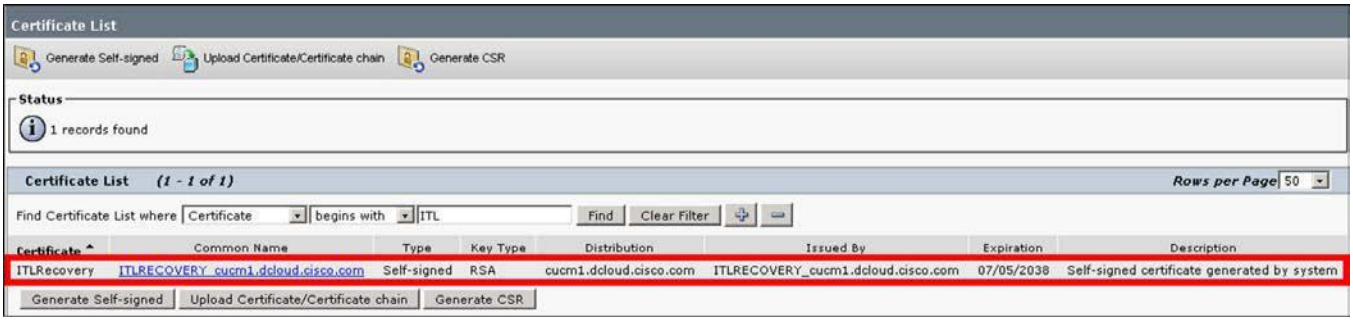
[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。[先頭が（begins with）] ドロップダウンの横に「**ITL**」と入力し、[検索（Find）] をクリックします（図 116 を参照）。

図 116. 証明書管理：ITLRecovery 証明書の検索



[共通名（Common Name）] が ITLRECOVERY_cucm1.dcloud.cisco.com である **ITLRecovery** 証明書を確認します（図 117 を参照）。

図 117. ITLRecovery

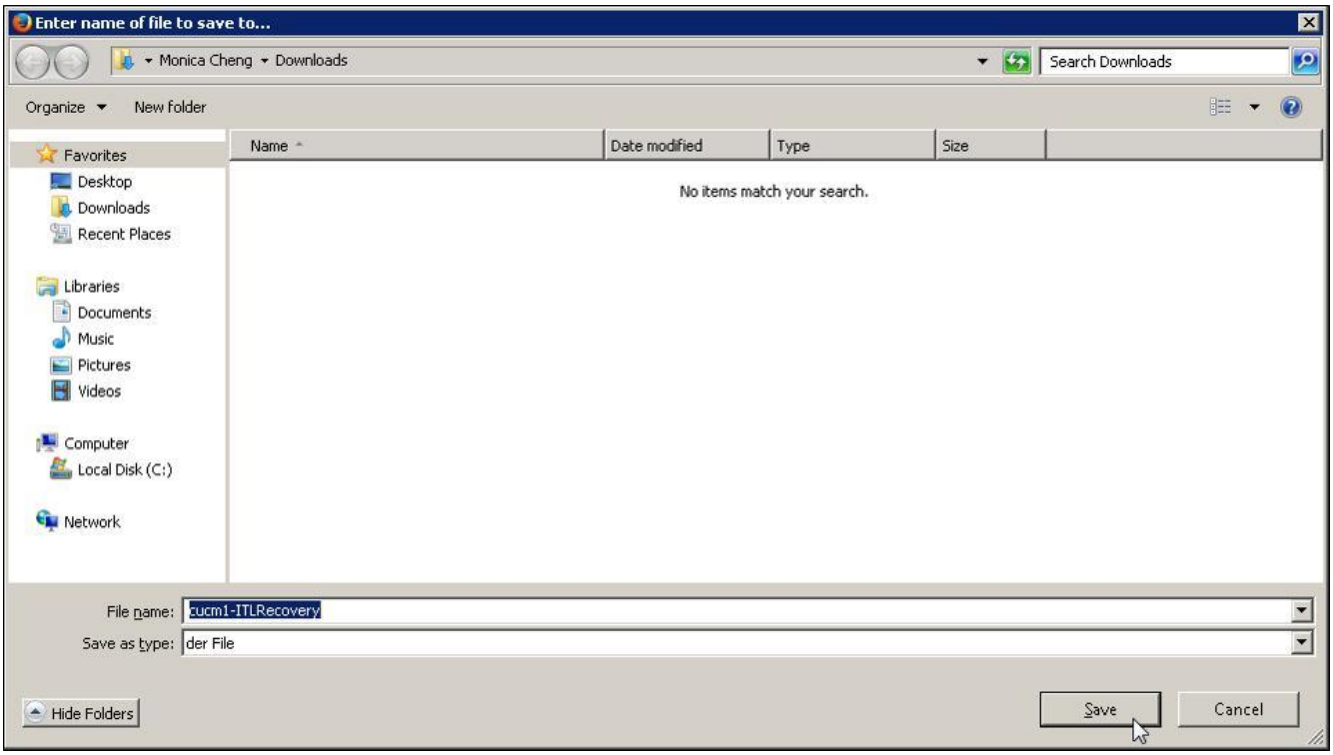


ITLRecovery 証明書をクリックして詳細を確認します（図 118 を参照）。次に [.DER ファイルをダウンロード（Download .DER File）] をクリックして証明書をダウンロードします。PEM と DER のどちらの形式でもダウンロードできます。このガイドでは DER 形式の例を示します。

図 118. ITLRecovery 証明書の詳細

図 119 に示すように、**Download** フォルダに .DER ファイルを保存し、**cucm1-ITLRecovery** という名前を付けます。

図 119. cucm1 ITLRecovery 証明書をダウンロードして保存する



次の手順では、この cucm1-ITLrecovery 証明書を ucm1 の phone-SAST-trust 信頼ストアにアップロードします。これは、1 つのソース クラスタから移行先クラスタに電話機を移行するときに行います。その場合は、移行先クラスタの ITLRecovery 証明書を、ソース クラスタの phone-SAST-trust にインポートする必要があります。

注:この最後の部分では、前の Unified CM, **ucm1** に戻ります。正しいサーバ **ucm1.dcloud.cisco.com** に移動したことを確認してください。

Firefox ブラウザで、ucm1 に接続しているタブに移動し(タブがない場合は新しいタブを開き)、**ucm1**(https://ucm1.dcloud.cisco.com/cmplatform)の Unified CM Operating System 管理インターフェイスに移動します。ユーザ名/パスワード:**administrator/dCloud123!** でログインします。

[セキュリティ(Security)] > [証明書の管理(Certificate Management)] に移動します。図 120 に示すように、[証明書/証明書チェーンのアップロード(Upload Certificate/Certificate chain)] をクリックします。

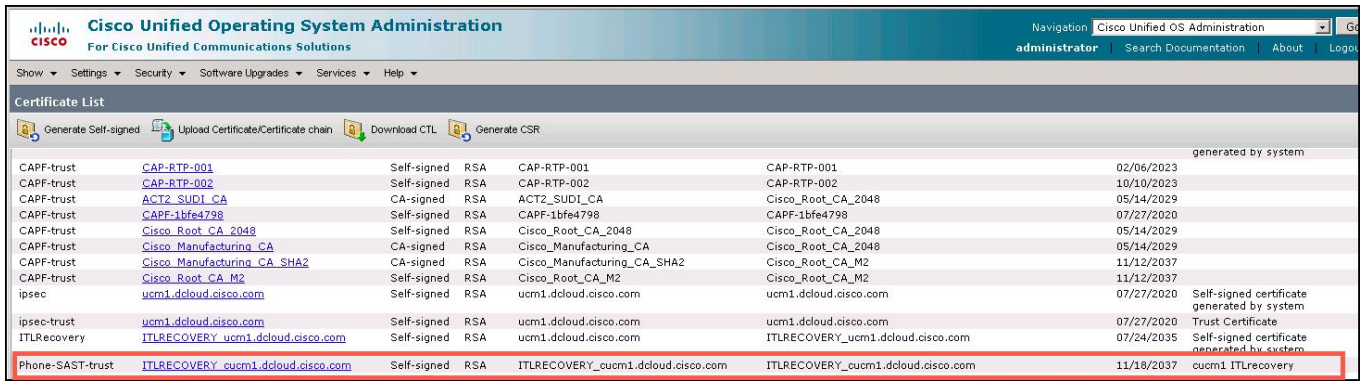
図 120. ITLRecovery 証明書のアップロードの開始

次に、ダウンロードした cucm1 ITLRecovery 証明書をアップロードします。[証明書の用途(Certificate Purpose)] から [Phone-SAST-trust] を選択します。次に [参照(Browse)] をクリックし、保存してある証明書 **cucm1-ITLRecovery.der**(C:\Users\mcheng\Downloads)を選択します。[開く(Open)] をクリックします。[説明(Description)] フィールドに「**cucm1 ITLrecovery**」と入力します(図 121 を参照)。

図 121. Phone-SAST-trust に ITLRecovery 証明書をアップロード

次に [アップロード（Upload）] をクリックします。証明書がアップロードされたら、ウィンドウを閉じます。cucm1 ITLRecovery 証明書が ucm1 の phone-SAST-trust にあることを確認します（図 122 を参照）。

図 122. Phone-SAST-trust の ITLRecovery 証明書



PuTTY を使用して **ucm1.dcloud.cisco.com** に SSH 接続します。

show ctl コマンドを実行します。古い CTL ファイルが表示されます。これには、cucm1 の ITLRecovery 証明書のレコードは含まれていません。

utils ctl update CTLFile コマンドを実行して CTL ファイルを更新します。

注:「**Y**」と入力して確定すると、画面に [Y] と表示されなくなります。「Yes」と入力したら Enter を押します。

表示されたように、クラスタ内の各ノードで、CallManager サービスと CTIManager サービスを再起動する必要があります。このラボでは CallManager サービスだけを再起動しますが、通常は CTIManager サービスも再起動する必要があります。

Unified CM サービスアビリティ ポータル（https://ucm1.dcloud.cisco.com/ccmservice/）にアクセスし、ユーザ名/パスワード: **administrator/dCloud123!** でログインします。

[ツール（Tools）] > [コントロールセンター － 機能サービス（Control Center－Feature Services）] に移動し、ドロップダウンから **ucm1.dcloud.cisco.com － CUCM Voice/Video** サーバを選択して [移動（Go）] をクリックします。次の画面で [Cisco CallManager] オプション ボタンをオンにして、[再起動（Restart）] を再度クリック（[OK] をクリックして再起動を確定）します。

次に **show ctl** コマンドを再度入力すると、新しい CTL ファイルが表示されます。cucm1 の ITLRecovery 証明書のレコードが CTL ファイルの一部になり、**System Administrator Security Token** 機能が有効になったことを確認します（図 123 を参照）。

図 123. CTL ファイルの cucm1 の ITLRecovery 証明書

```
        CTL Record #:5
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1772
2       DNSNAME         5       ucm1
3       SUBJECTNAME     91      CN=ITLRECOVERY_cucm1.dcloud.cisco.com;OU=dCloud;O=Cisco Systems;L=Richardson;ST=Texas;C=US
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      91      CN=ITLRECOVERY_cucm1.dcloud.cisco.com;OU=dCloud;O=Cisco Systems;L=Richardson;ST=Texas;C=US
6       SERIALNUMBER    16      54:DE:D0:70:41:64:74:FD:9A:86:6A:02:86:BE:AA:63
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     1005    6C 2D 29 08 63 E4 0C A2 EE 91 DF 5B 9B 34 74 73 AC 64 43 26 (SHA1 Hash HEX)
10      IPADDRESS       4       198.18.133.3
This etoken was not used to sign the CTL file.
```

Unified CM サービスアビリティ ポータル（https://ucm1.dcloud.cisco.com/ccmservice/）に戻り、必要に応じて [ツール（Tools）] > [コントロールセンター – 機能サービス（Control Center – Feature Services）] に移動し、[サーバ（Server）] ドロップダウン メニューから [ucm1.dcloud.cisco.com--CUCM Voice/Video] を選択して、[移動（Go）] をクリックします。[Cisco TFTP] の横のオプション ボタンをオンにして、[再起動（Restart）] ボタンをクリックします。

show itl コマンドを実行すると、cucm1 の ITLRecovery 証明書のレコードも表示されます。

これは Unified CM 12.0(1) 以降で変更された動作です。phone-SAST-trust の ITLRecovery 証明書が ITL ファイルとトークンレス CTL ファイルに追加されます（**System Administrator Security Token** 機能を使用）。これには、別の Unified CM クラスタに移行する場合に、TVS との依存関係が解消されるという利点があります。

以前の Unified CM リリースでは、1 つのソース Unified CM クラスタから新しい移行先 Unified CM クラスタにエンドポイントを移行する場合は、移行先 Unified CM TFTP サーバの CallManager 証明書を、ソース Unified CM クラスタの phone-SAST-trust にインポートする必要がありました。エンドポイントが新しい移行先クラスタに接続され、移行先クラスタのトークンレス CTL ファイルと ITL ファイルをダウンロードしている場合は、証明書の既存のリストを使用してそれらのファイルを検証できませんでした。それらのファイルを検証するには、ソース クラスタの TVS サーバに接続する必要がありました。そのため、ソース クラスタはオンラインに維持され、電話機はソース クラスタの現行の TVS 証明書を必要としました。Unified 12.0(1) 以降ではこれは不要になりました。

注：暗号化に LSC を使用していたハードウェア フォンを移行する場合は、クラスタ移行時に、従来のクラスタ（11.5(1)）から新しいクラスタ（12.0(1)）の CAPF-trust および CallManager-trust ストアに CAPF 証明書をインポートする必要があります。それらの操作は手動で行うか、[証明書の一括管理（Bulk Certificate Management）] ページを使用して実行できます。

***** モジュール #4 の終了 *****

モジュール 5. Jabber エンドポイントの暗号化

モジュールの概要

このモジュールでは、オンプレミスおよび MRA Jabber クライアントについて、シグナリングとメディア暗号化を設定して有効にします。最初に電話セキュリティ プロファイルを確認して設定します。次にオンプレミスの Jabber クライアントを CAPF 登録し、それらの端末を暗号化に対応させます。CAPF 登録が完了し、Jabber クライアントに証明書を登録すると、2 つのオンプレミスの Jabber クライアントが、暗号化された通話を確認します。このモジュールは、次の 3 つのセクションに分割されています。

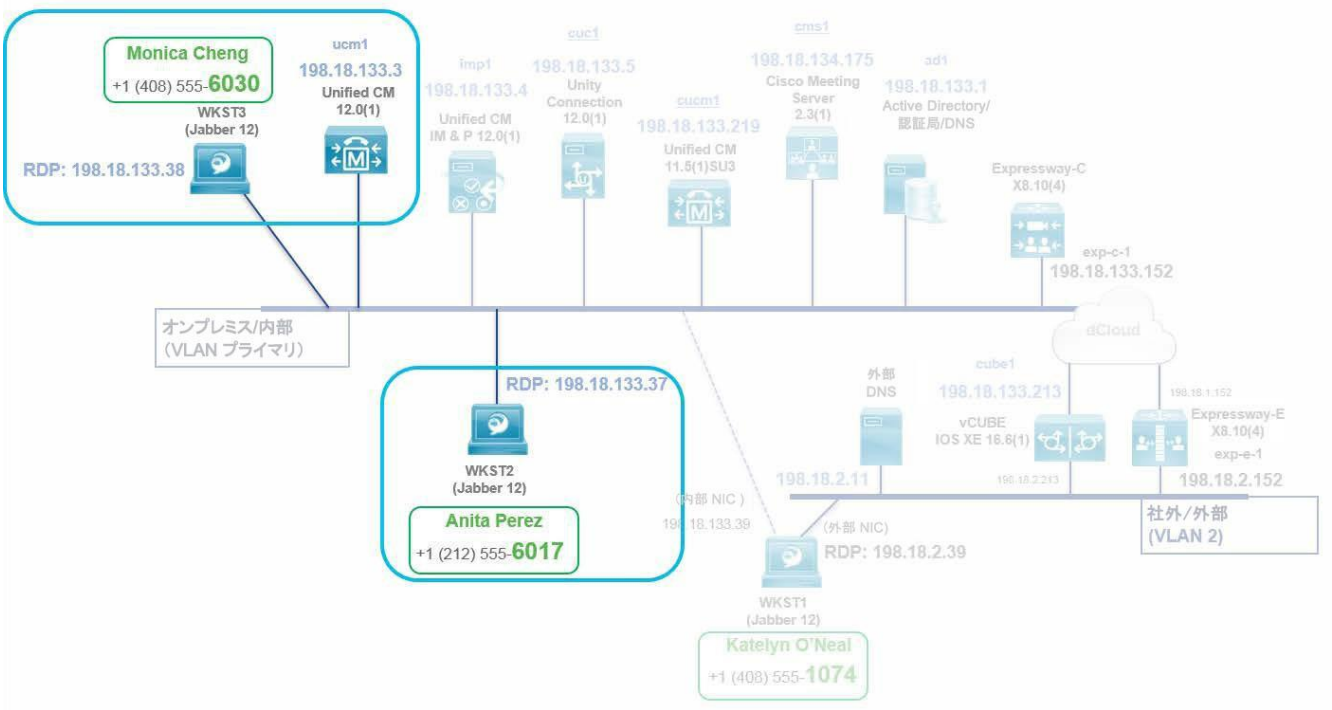
A. 暗号化のための電話セキュリティ プロファイル

B. Jabber オンプレミス端末での Unified CM CAPF 登録

C. Jabber オンプレミス端末でセキュアな暗号化された通話を確認する

次の図 124 は、このモジュールのトポロジおよび関連するコンポーネントを示しています。

図 124. モジュール 5：Jabber エンドポイント暗号化ラボ トポロジ



手順

A. 暗号化のための電話セキュリティ プロファイル

このセクションでは、Cisco Collaboration 12.0 エンタープライズ オンプレミス導入で推奨されるアーキテクチャの推奨事項に基づいて、電話セキュリティ プロファイルを確認します。ここでは、認証文字列 CAPF の登録と暗号化された通話が有効な、1 つの電話セキュリティを作成します。

「オンプレミス導入環境での Cisco Collaboration 12.0 エンタープライズ向け」（https://www.cisco.com/c/ja_jp/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd/security.html）のセキュリティの章に示すように、セキュアな端末セキュリティ プロファイルが 4 つ推奨されています。このシステムでもそれらを設定します。次の表 4 に、推奨されるプロファイルのリストを示します。

表 4. Enterprise Collaboration PA で推奨されるセキュアな電話セキュリティ プロファイル

電話セキュリティ プロファイル名 1	端末セキュリティ モード	TFTP 暗号化設定	CAPF 登録のための認証モード
UDT-Encrypted-LSC-TFTPenc.dcloud.cisco.com[2] [3]	暗号化	有効	既存の証明書（LSC に優先）
UDT-Encrypted-LSC.dcloud.cisco.com[3]	暗号化	無効	既存の証明書（LSC に優先）
UDT-Encrypted-NullString.dcloud.cisco.com[3]	暗号化	無効	Null 文字列
UDT-Encrypted-AuthString.dcloud.cisco.com	暗号化	無効	認証文字列

1 すべてのプロファイルは「Universal Device Template - Model-independent Security Profile」に基づきます。
2 これらのセキュリティ プロファイルのドメイン部分（dcloud.cisco.com）は、システムのドメインに一致します。
3 これらのプロファイルはすでに事前設定されています。

表 4 に示すように、4 つの端末セキュリティ プロファイルにより、管理者は最小のプロファイル数で導入内のすべてのエンドポイント タイプを保護できます。Expressway Mobile and Remote Access の導入では、Expressway-C サーバ証明書に影響する端末セキュリティ プロファイル数が重要になります。オンプレミスのエンドポイントと MRA に接続されたエンドポイント間でエンドツーエンドの暗号化を行うには、MRA に接続された端末に割り当てられた各端末セキュリティ プロファイルが、Expressway-C サーバ証明書のサブジェクト代替名（SAN）である必要があります。MRA エンドポイントに割り当てられる端末セキュリティ プロファイルの数が多いほど、Expressway-C サーバ証明書に含まれる SAN を増やす必要があります。推奨される端末セキュリティ プロファイルの詳細については、PA Cisco Collaboration CVD セキュリティの章を参照してください。

1. WKST2（198.18.133.37）の Firefox Web ブラウザから、Unified CM 管理インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin/）にアクセスします。

   [システム（System）] > [セキュリティ（Security）] > [電話セキュリティプロファイル（Phone Security Profile）] に移動し、「Name begins with」で検索し、「UDT-Encrypted」と入力して、[検索（Find）] をクリックします（図 125 を参照）。

   図 125. 電話セキュリティ プロファイル：UDT

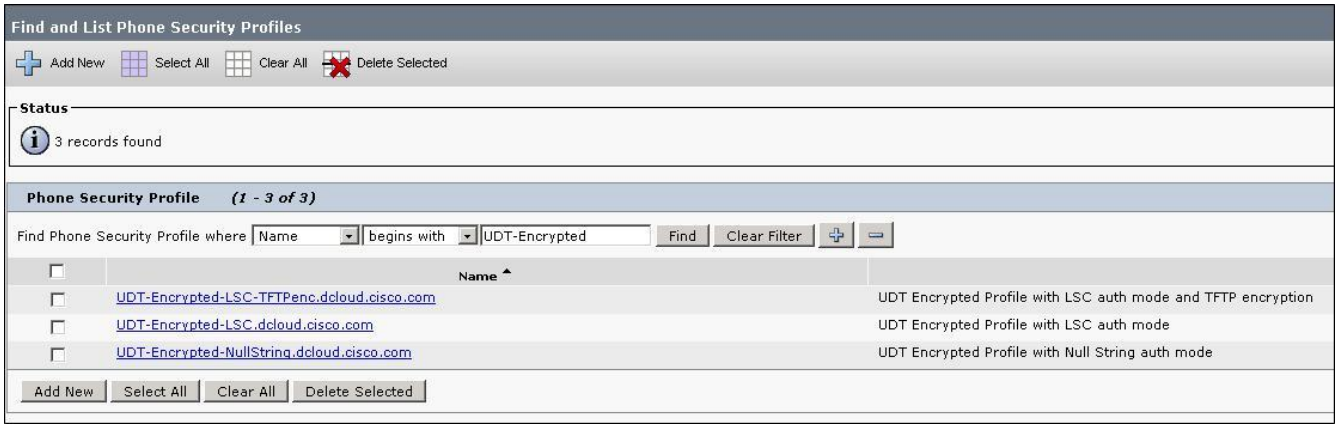
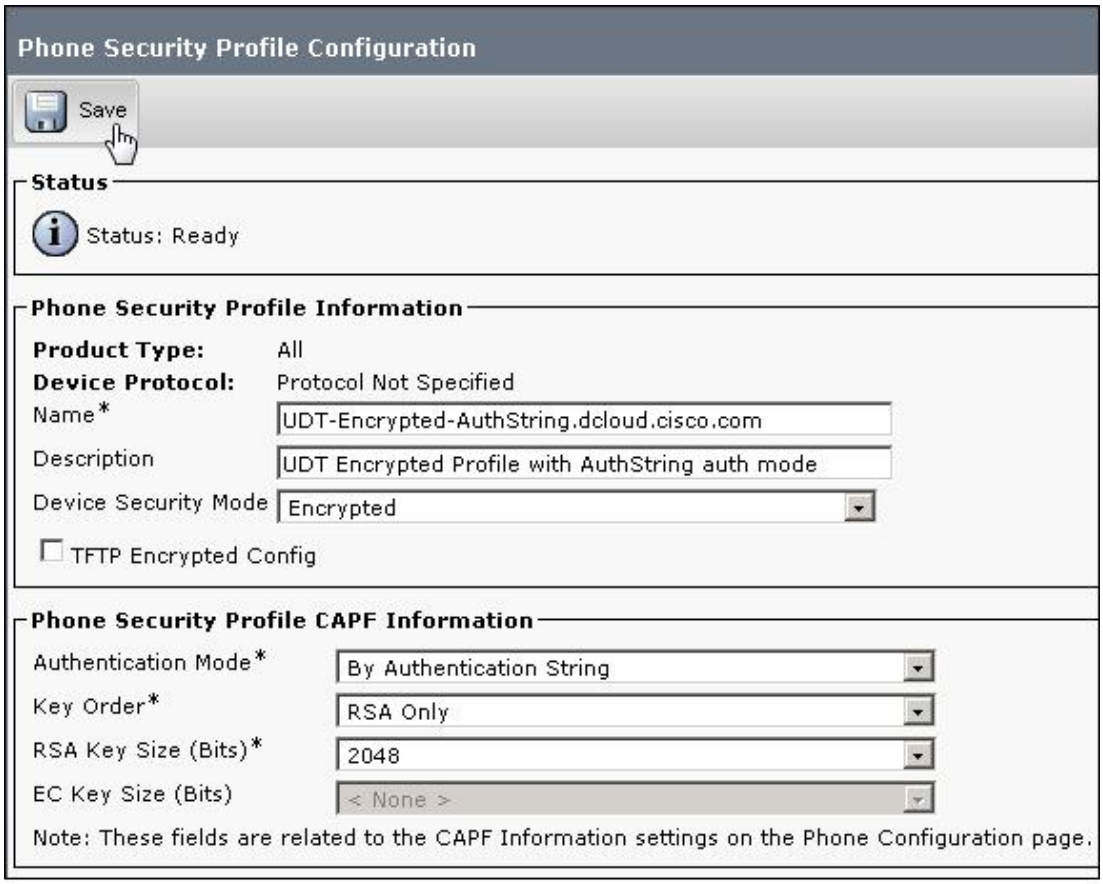


   表 4 に示す、PA で推奨される電話セキュリティ プロファイルのうち、**UDT-Encrypted-NullString.dcloud.cisco.com**、**UDT-Encrypted-LSC.dcloud.cisco.com**、**UDT-Encrypted-LSC-TFTPenc.dcloud.cisco.com** の 3 つがすでに設定されています。

UDT-Encrypted-NullString.dcloud.cisco.com プロファイルの横の  (コピー アイコン)をクリックして、コピーを作成します。プロファイルの名前を **UDT-Encrypted-AuthString.dcloud.cisco.com** に変更します。[説明(Description)] フィールドを [UDT Encrypted Profile with Auth String auth mode] に変更します。[端末セキュリティモード(Device Security Mode)] は [Encrypted] を選択したままにします。[認証モード(Authentication Mode)] ドロップダウンから [By Authentication String] を選択します。その他の設定はデフォルト値のままにします(図 126 を参照)。

図 126. UDT-Encrypted-AuthString.dcloud.cisco.com の電話セキュリティ プロファイル

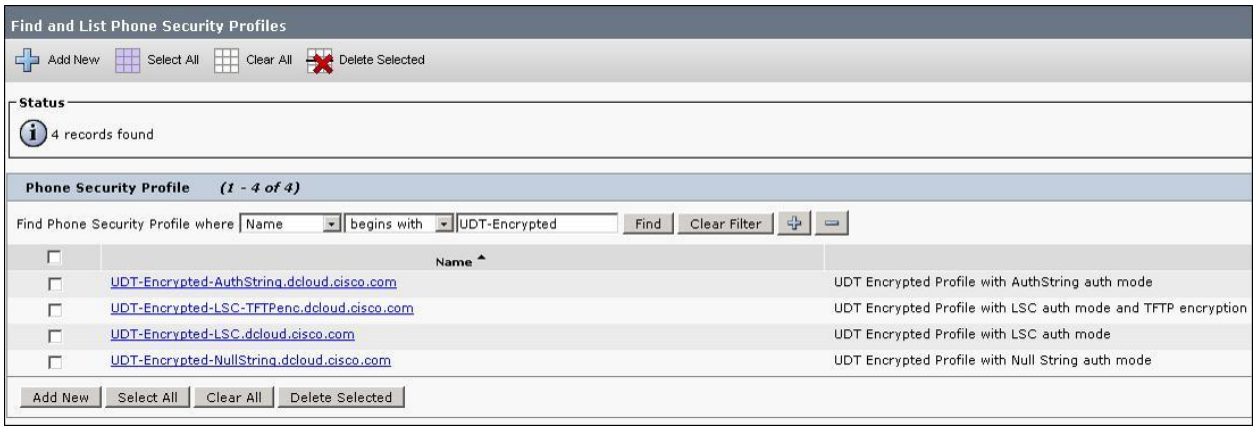


をクリックします。

2. システムの電話セキュリティ プロファイル リストが、推奨されるプロファイルのセットに一致することを確認する

[電話セキュリティプロファイル（Phone Security Profile）] リストに戻り、表 4 に示す推奨されるすべての電話セキュリティ プロファイルが、図 127 に示すように設定されていることを確認します。

図 127. 電話セキュリティ プロファイル：推奨アーキテクチャで推奨されるすべての UDT



B. オンプレミスの Jabber 端末での Unified CM CAPF 登録

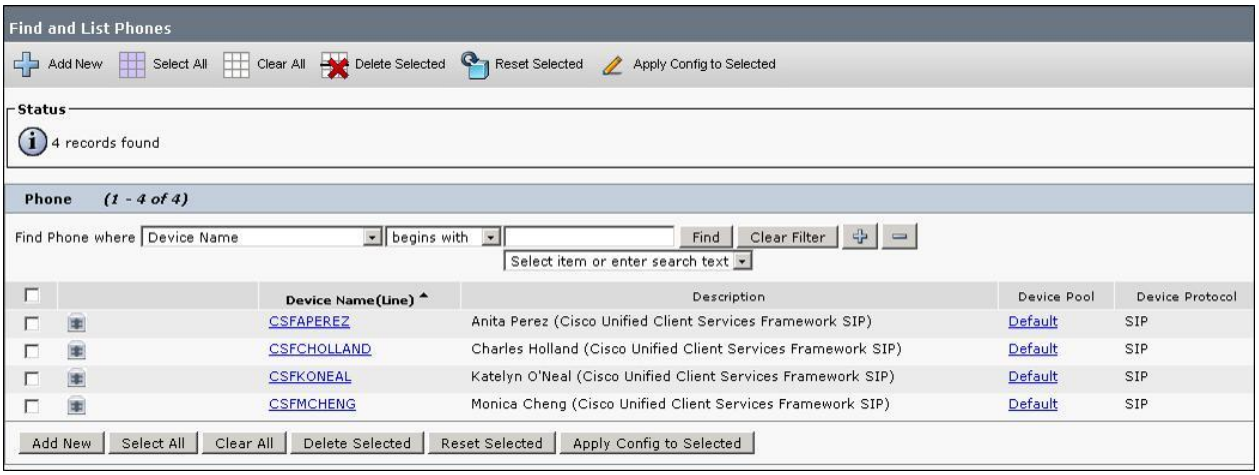
このセクションでは CAPF 登録を行い、前の手順で作成した電話セキュリティ プロファイル（**UDT-Encrypted-AuthString**.dcloud.cisco.com）をオンプレミスの Jabber for Windows クライアントに適用して、暗号化された通話を可能にします。

3. 暗号化された電話セキュリティ プロファイルを適用し、オンプレミスの Jabber クライアントの CAPF 登録を行う
   次に、作成した暗号化された電話セキュリティ プロファイルを、オンプレミスの Jabber for Windows クライアントに適用します。

   - CSFAPEREZ（WKST2）
   - CSFMCHENG（WKST3）

   [端末（Device）] > [電話（Phone）] に移動し、[検索（Find）] をクリックすると、システム上のエンドポイント端末のリストが表示されます（図 128 を参照）。

図 128. Unified CM 電話のリスト

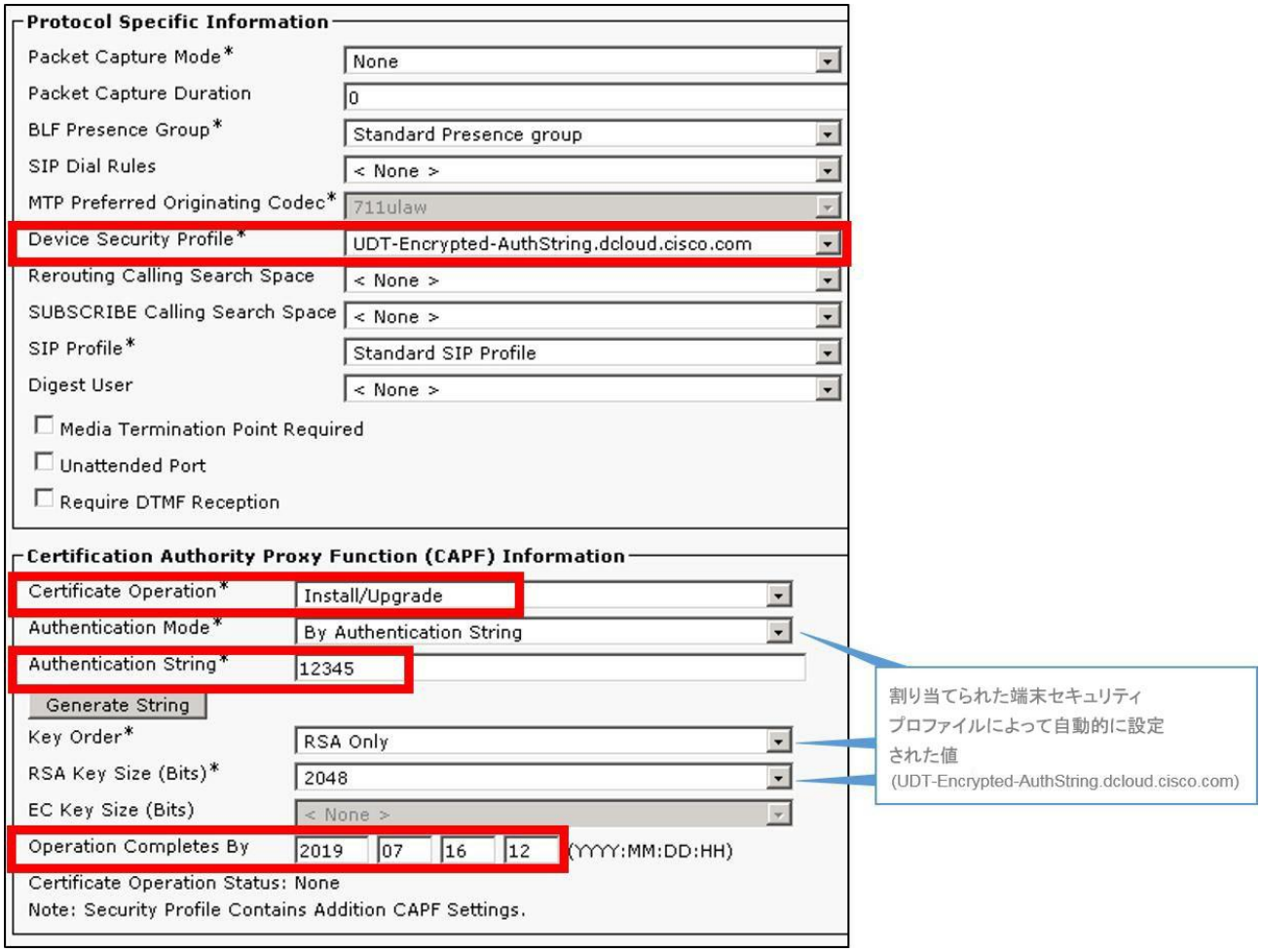


[CSFAPEREZ] をクリックして、端末設定ページをロードします。図 129 に示すように設定します。

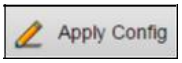
- [端末セキュリティプロファイルのプロトコル固有情報（Protocol Specific Information for the Device Security Profile）] フィールドで、作成した暗号化されたセキュリティ プロファイル **UDT-Encrypted-AuthString.dcloud.cisco.com** を選択します。

- [認証局プロキシ機能（CAPF）情報（Certificate Authority Proxy Function (CAPF) Information）] の [証明書の操作（Certificate Operation）] フィールドで、[インストール/アップグレード（Install/Upgrade）] を選択します。
- [認証文字列（Authentication String）] フィールドに「**12345**」と入力します。
- [操作の完了期限（Operation Completes By）] フィールドに、YYYY:MM:DD:HH の形式で未来の日付/時刻を設定します。このラボでは、これを現在の日付 + 1 日（翌日の日付）に設定します。

図 129. UDT-Encrypted-AuthStrning.dcloud.cisco.com 端末セキュリティ プロファイルを適用し、CAPF を有効にする*



[操作の完了期限（Operation Completes By）] フィールドが上記と一致しなくても、将来の日付/時刻が設定され、CAPF 登録が完了するだけの時間があれば問題はありません。

をクリックします。続くダイアログで [OK] をクリックし、 

をクリックします。次のダイアログで [OK] をクリックし、設定変更を適用します。Jabber クライアントが次回 Unified CM への登録を試みると、シンプルな認可文字列のチャレンジによって CAPF 登録が強制されます。Jabber クライアントが CAPF 登録を完了すると、クライアントが暗号化電話モードで動作します。

同一の [端末セキュリティプロファイル（Device Security Profile）] を設定し、他のオンプレミス Jabber クライアント **CSFMCHENG** について **CAPF** 登録を有効にします。

設定を保存して CSFMCHENG 端末に適用したら、次の手順に進みます。

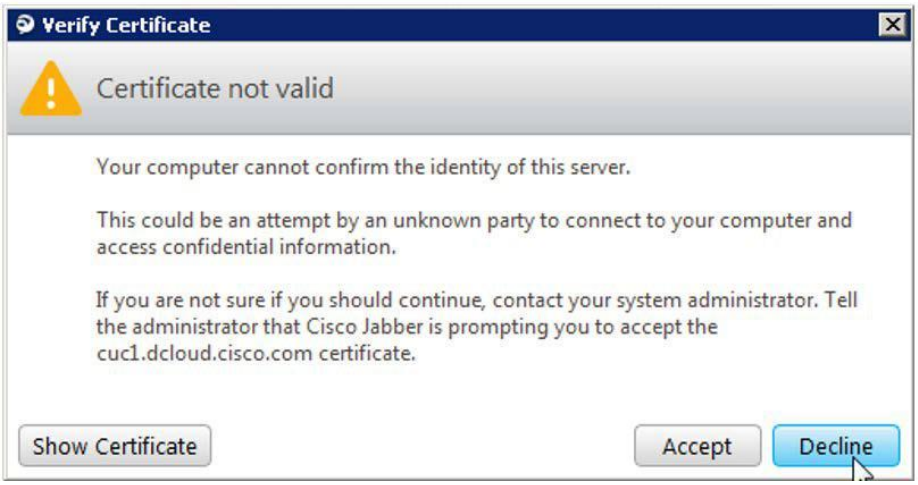
4. オンプレミスの Jabber クライアントを登録して CAPF 登録を完了する

   最初に WKST2 で Jabber クライアントを使用します。まだ接続していない場合は、WKST2（DCLOUD**aperez/C1sco12345**）に **RDP** 接続します。

デスクトップの Jabber アイコンをダブルクリックし、ユーザ名/パスワード：**aperez/C1sco12345** でログインします。

クライアントを登録する前に、図 130 に示すように、Unity Connection ボイスメール サービス証明書が無効であるという警告が表示されます。

図 130. Jabber Unity Connection ボイスメール サービス証明書の警告



この警告メッセージが表示されるのは、ラボの Unity Connection ボイスメール サービス ノードから受信した証明書がデフォルトの自己署名証明書で、ラボのワークステーションのローカル信頼ストアに存在しないためです。ここでは [拒否（Decline）] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。[承認（Accept）] をクリックすると、証明書がローカル ワークステーションの信頼ストアに保存され、クライアントがボイスメール システムに接続します。ただし、有効なボイスメール システムに確実に接続し、有効なサーバ証明書を受け取るには、この証明書を手動で検証してから続行する必要があります。検証しないと、システムが侵害される可能性があります。

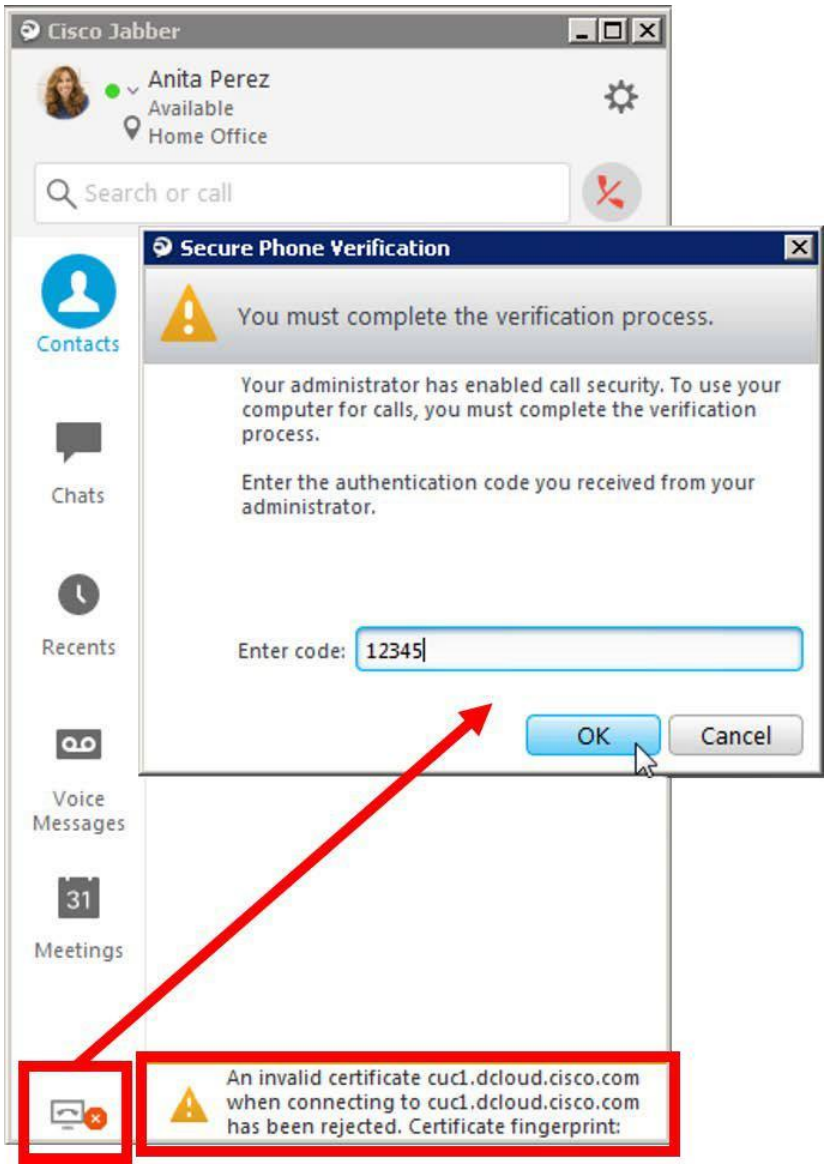
[拒否（Decline）] をクリックすると、Jabber クライアントにエラー メッセージが表示され、ビジュアル ボイスメール サービスは接続されません。このメッセージは、証明書が無効であるため、Unity Connection サーバ（cuc1.dcloud.cisco.com）との接続が拒否されたことを示します（図 131 を参照）。

注：このラボのモジュール 8（次世代暗号化によるセキュアなボイスメール）では、エンタープライズ CA によって Unity Connection tomcat 証明書に署名します。それにより、無効な証明書警告メッセージを受信しなくなり、ボイスメール サービスが自動証明書検証に接続するようになります。

次に、CAPF 登録認可文字列のプロンプトであるポップアップ ウィンドウが表示されます。前に指定した認証ストリング「**12345**」を入力します。[OK] をクリックします。

図 131 に示すように、Jabber IP 電話サービスは、ユーザが認証ストリングを入力し、CAPF 登録操作が完了するまで接続されません。図 131 は、Unity Connection サーバ証明書のエラー メッセージも示しています。

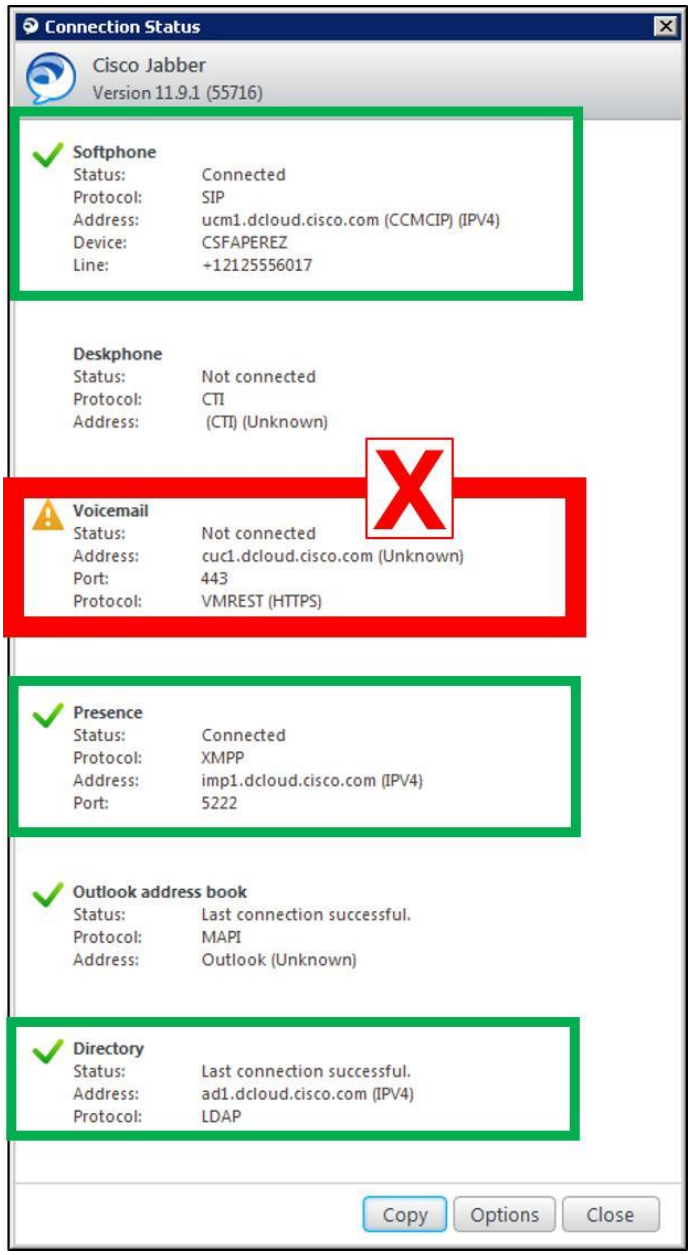
図 131. 認証ストリングによる CAPF 登録 – Cisco Jabber for Windows



認証文字列を入力すると、クライアントが自動的に、電話サービスにセキュアに再接続されます。

図 132 に示すように、登録した Jabber クライアントは、Voice/Video over IP 通話、IM & Presence、ディレクトリ サービスを行うために Unified CM、IM & P、Active Directory（LDAP）サーバに自動的にログインして接続します。これらの接続を確認するには、[設定（Settings）]（  ） > [ヘルプ（Help）] > [接続ステータスの表示（Show connection status）] の順にクリックします。

図 132. Jabber の接続ステータス情報



プレゼンス サービスと通話制御サービスに接続したときには、サーバまたはサーバ証明書の有効期限に関する警告は表示されていません。これは、Unified CM IM & P および Unified CM システムの証明書が、すでにエンタープライズ CA によって署名されていたためです。さらに、エンタープライズ CA ルート証明書が、ローカル ワークステーションの証明書信頼リストに追加されています。プレゼンス サービスと通話制御サービス接続の際にこれらの証明書がクライアントに提供されると、クライアントはローカルの信頼ストアと対照して、提供されたサーバ証明書を自動的に検証できました。

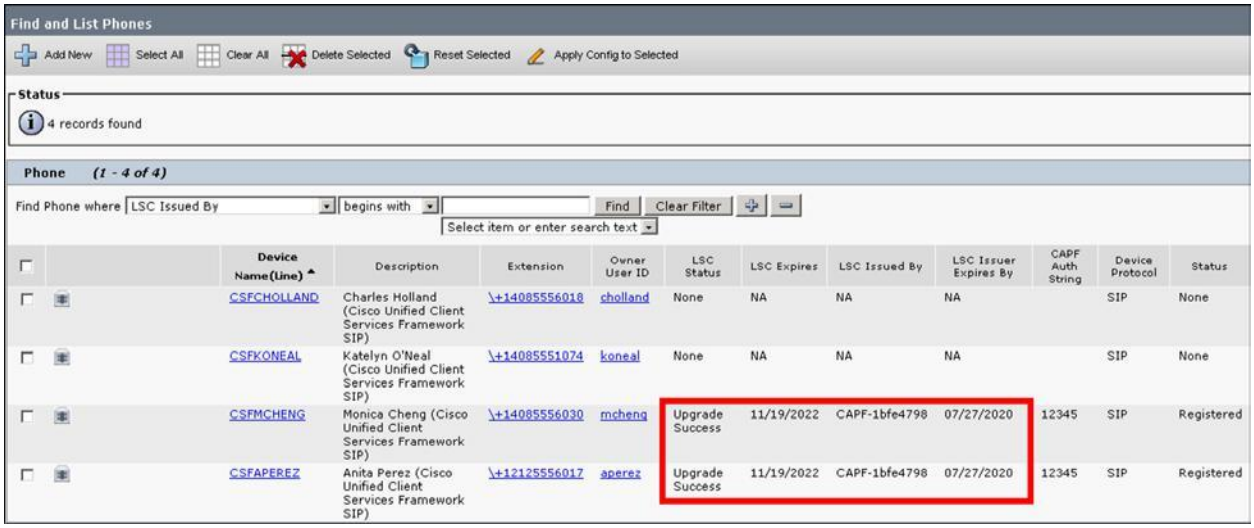
サーバの警告は**拒否**し、上記の手順を繰り返して、WKST3（CSFMCHENG）で Jabber for Windows クライアントの登録と CAPF 登録を行います。続行する前に、WKST3 の Jabber クライアントが Unified CM に再登録されていることを確認してください。

5. オンプレミスの Jabber クライアントで CAPF 登録と LSC のインストールを確認する

続行する前に、CAPF 登録が完了し、オンプレミスの両方の Jabber クライアントに LSC がインストールされていることを確認します。Jabber クライアントが再登録されれば、CAPF 登録が正常に完了したと判断できますが、Unified CM でステータスを確認すれば確実です。

[電話(Phone)] ページに戻ります([端末(Device)] > [電話(Phone)] に移動)。[電話の検索場所(Find Phone where)] ドロップダウンから [LSC の発行元(LSC Issued By)] を選択し、[検索(Find)] をクリックすると、システム上のエンドポイント端末のリストが表示されます。図 133 に示すように、CSFMCHENG と CSFAPEREZ が登録され、CAPF サービスによって LSC が発行されています。LSC により、Jabber クライアントでは SIP シグナリングと RTP メディア トラフィックを暗号化できます。

図 133. Jabber オンプレミス クライアントの CAPF 登録と LSC のインストール



何度か通話を行い、暗号化を示す「ロック」アイコンが各エンドポイントに表示されていることを確認し、暗号化されたセキュアな通話が正しく設定されたことを確認します。

C. Jabber オンプレミス端末でセキュアな暗号化された通話を確認する

続行する前に、RDP 経由で WKST2(DCLOUD**aperez/C1sco12345**)と WKST3(DCLOUD**mcheng/C1sco12345**)の両方に接続していて、両方のワークステーションの Jabber クライアントが起動し、Unified CM に登録されていることを確認します。

6. デスク フォン間で通話を行い、暗号化を示す「ロック」アイコンが表示されていることを確認します。

   WKST2 で Anita Perez の Jabber クライアントから、検索または通話ウィンドウに「6030」と入力し、緑色の電話ボタンをクリックして Monica Cheng に発信します(図 134 を参照)。

図 134. 発信:Anita Perez(WKST2)が 6030 にダイヤルして Monica Cheng(WKST3)に発信

WKST3 において Monica Cheng の Jabber クライアントで応答します。通話が接続されたら、両方の Jabber クライアントに暗号化を示す「ロック」アイコンが表示されていることを確認します（図 135 を参照）。

図 135. 暗号化されたセキュアな通話の確認：オンプレミスの Jabber 間通話

通話を終了します。

このラボの他のモジュールに進む前に、WKST2（198.18.133.137）と WKST3（198.18.133.138）で Jabber for Windows クライアントを終了します。

***** モジュール #5 の終了 *****

モジュール 6. OAuth2 での更新ログイン フロー

モジュールの概要

このモジュールでは、Unified CM、Unified CM IM & P、Unity Connection、Expressway などのコラボレーション アプリケーションについて、Jabber クライアント用に OAuth2 ログイン フローを設定して有効にします。OAuth2 ログイン フローを有効にすると、Jabber クライアント ログインが設定を検証します。このモジュールは、次の 3 つのセクションに分割されています。

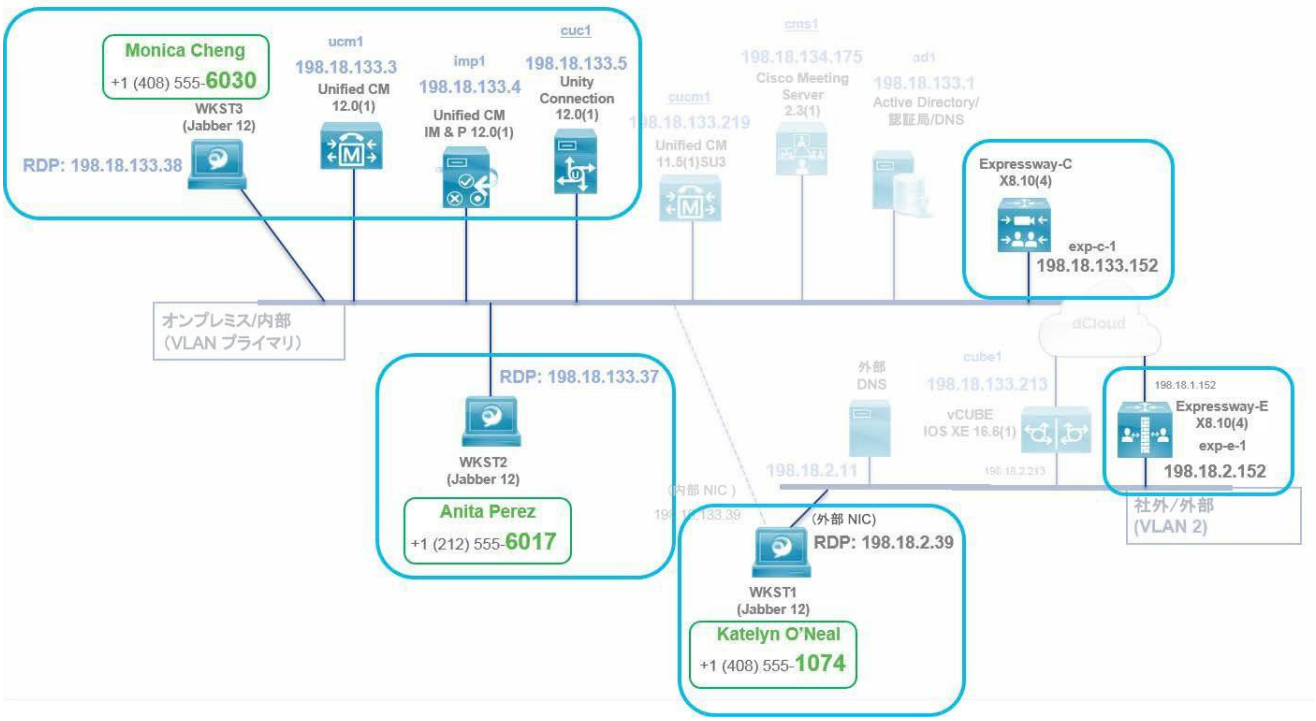
A. Unified CM および Unified CM IM&P で更新ログイン フローによる OAuth を有効にする

B. Unity Connection で更新ログイン フローによる OAuth を有効にする

C. オンプレミスの Jabber クライアントで更新ログイン操作によって OAuth を検証する

次の図 136 は、このモジュールのトポロジおよび関連するコンポーネントを示しています。

図 136. モジュール 6：OAuth2 での更新ログイン フロートポロジ



OAuth2 ログインと更新ログイン フロー

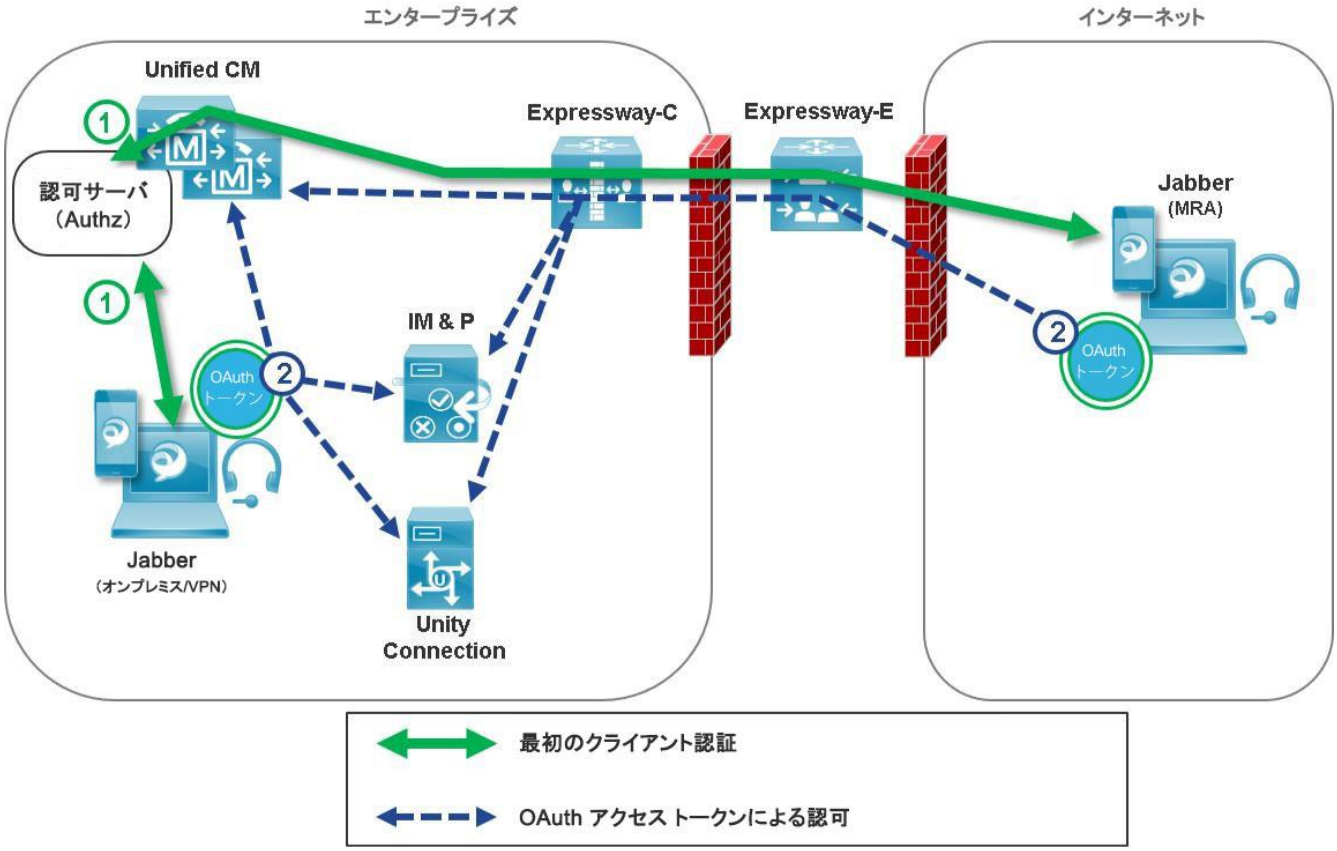
更新トークンを使用する OAuth2 ログイン フローは、Jabber 11.9 以降のすべてのクライアントに対応する新機能です。Jabber のログイン プロセスが簡素化され、頻繁に再認証する必要がなくなります。この新しいログイン フローでは、OAuth 2.0 認可プロトコルと、ユーザのクレデンシャルによる認証によって発行される認可トークンまたはアクセス トークンの概念が活用されています。クライアントはアクセス トークンを使用することで、ユーザがログイン クレデンシャルを再入力しなくても、他のサーバやサービスの認証を受けることができます。それにより、ID プロバイダー（IdP）を使用しなくても、シングル サインオン（SSO）と同様の機能が得られます。

アクセス トークンに加えて、クライアントには認証後に更新トークンが発行されます。これは、元のアクセス トークンの有効期限が切れたときに、認可を更新するために使用します。それによりクライアントは、更新トークンの有効期限が切れるまで自動的に再認証されます。

更新トークンの有効期限が切れたら、クライアントは完全なログインによって再度認証を受ける必要があります。デフォルトでは OAuth アクセス トークンの有効期限は 60 分であり、OAuth 更新トークンの有効期限は 60 日です。ただしこれらのデフォルト値は、組織のポリシーに応じてエンタープライズ パラメータによって設定可能です。

図 137 に、Jabber 用更新トークン アーキテクチャによる OAuth2 ログインを示します。緑色の矢印で示すように（手順 1）、最初のクライアント ログインでは、クライアントはいずれかのクラスタ Unified CM ノードで動作する認可サーバによって認証され、OAuth アクセス トークン（および更新トークン）を受け取ります。クライアントは OAuth トークンを取得すると、導入内の他のサーバによる認証にトークンを使用します（手順 2）。

図 137. OAuth2 アーキテクチャの概要



Unified CM サーバに加えて、Unified CM IM & P、および Unity Connection サーバも、クライアント認証のために OAuth アクセス トークンを検証します。同様に、Expressway Mobile and Remote Access（MRA）経由で接続する Jabber クライアントは、Expressway-C サーバと Expressway-E サーバを通じて OAuth2 ログイン フローを活用します。

手順

A. Unified CM および Unified CM IM & P で更新ログイン フローによる OAuth を有効にする

続行する前に、WKST2（CSFAPEREZ）、WKST3（CSFMCHENG）、および WKST1（CSFKONEAL）のすべての Jabber クライアントがシャットダウンされたことを確認してください。

最初に、Unified CM および Unified CM IM & P で、更新トークンを使用した OAuth を有効にします。

1. Unified CM で更新ログイン フローによる OAuth を有効にする

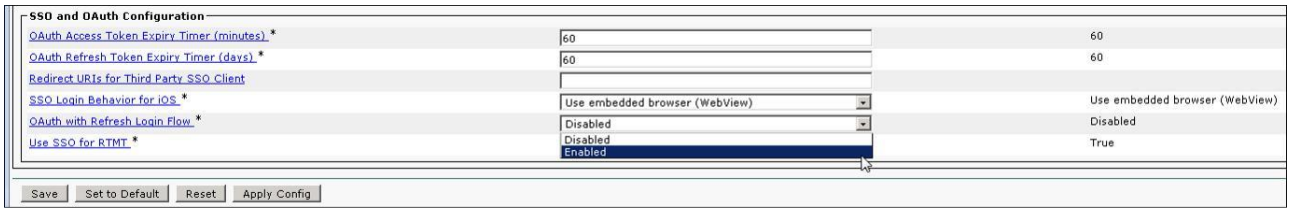
   ユーザ名/パスワード：DCLOUD**aperez/C1sco12345** で WKST2（198.18.133.37）に RDP 接続します。

   WKST2 で Firefox Web ブラウザを使用して接続したら、Unified CM 管理インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin）に移動し、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

   [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] に移動します。画面下部にある SSO および OAuth 設定サブセクションまでスクロールします。

   図 138 に示すように、[更新ログインフローによる OAuth（OAuth with Refresh Login Flow）] ドロップダウン メニューから [有効（Enable）] を選択します。

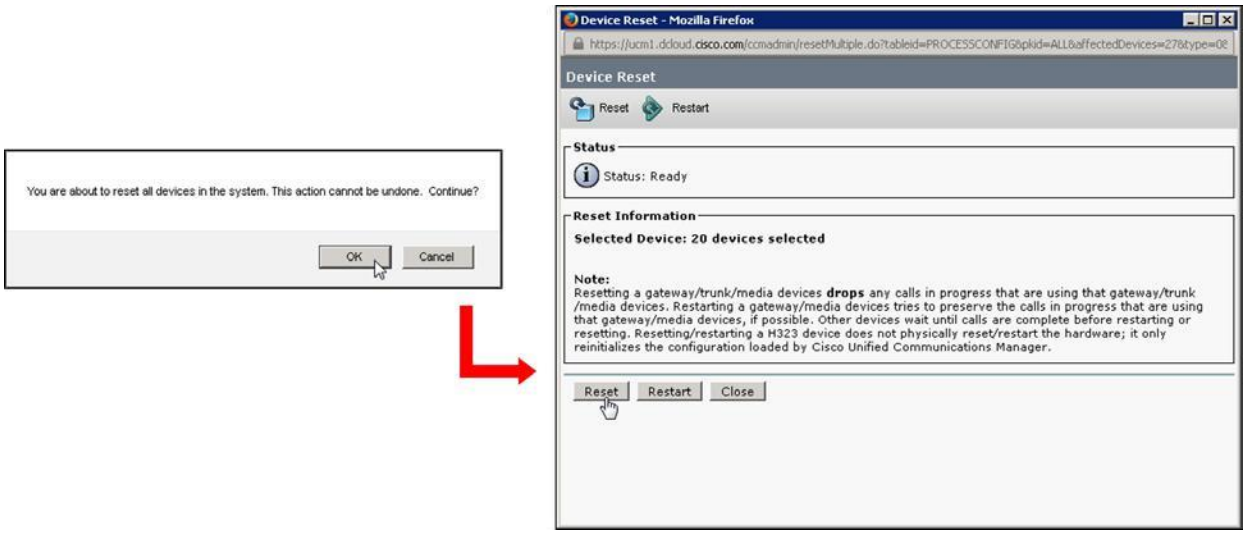
   図 138. Unified CM：更新ログインフローによる OAuth の有効化



   [保存（Save）] をクリックします。

   次に [設定の適用（Apply Config）] をクリックし、[OK] をクリックして確定します。最後に、図 139 に示すように、[リセット（Reset）] をクリックし、[OK] をクリックして確定し、もう一度 [リセット（Reset）] をクリックします。

   図 139. Unified CM：更新ログイン フロー エンタープライズ パラメータを使用した OAuth を有効にしてリセット



   「リセット要求の送信に成功しました（Reset request was sent successfully）」というメッセージが表示されたら、[閉じる（Close）] をクリックします。

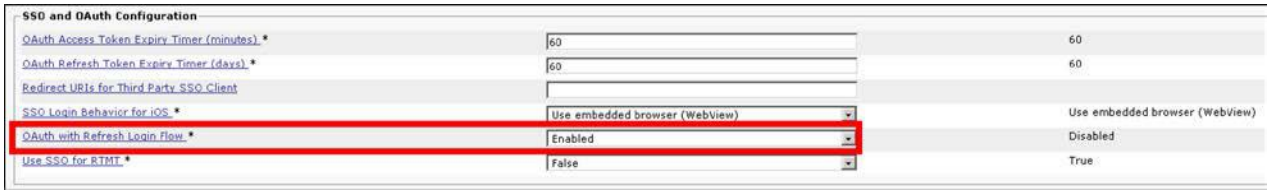
2. Unified CM IM & P で更新ログイン フローによって OAuth を確認する

   Unified CM で更新ログイン フローによる OAuth を有効にすると、クラスタ内の Unified CM IM & P ノードでも自動的に有効になります。そのことを確認しましょう。WKST2 の Firefox Web ブラウザで、Unified CM IM およびプレゼンス管理インターフェイス（https://imp1.dcloud.cisco.com/cupadmin）にアクセスし、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

   [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] に移動します。画面下部にある SSO および OAuth 設定サブセクションまでスクロールします。

図 140 に示すように、更新ログイン フローによる OAuth が [有効(Enabled)] に設定されています。

図 140. Unified CM IM & P:更新トークンを有効にした OAuth



パラメータがデフォルト値([無効(Disabled)])に設定されている場合は、ドロップダウンから [有効(Enabled)] を選択し、[保存(Save)] をクリックしてから続行します。

B. Unity Connection で更新ログイン フローによる OAuth を有効にする

3. システム認可サーバの追加

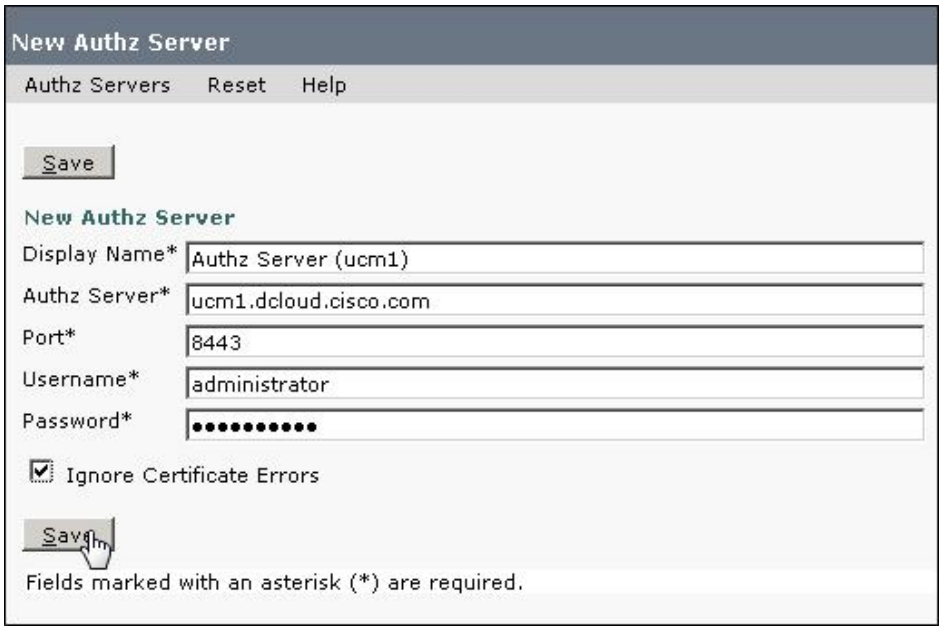
WKST2 の Firefox Web ブラウザで、Unity Connection 管理インターフェイス(https://cuc1.dcloud.cisco.com/cuadmin/)にアクセスし、ユーザ名/パスワード:**administrator/dCloud123!** でログインします。プロンプトが表示されたら、証明書をローカル信頼ストアに一時的に保存して、セキュリティ例外を作成します([詳細設定(Advanced)] > [例外の追加(Add Exception)] > [セキュリティの例外を確認(Confirm Security Exception)] の順に選択し、[この例外を永久に保存(Permanently store this exception)] をオフにする)。

[システム設定(System Settings)] > [Authz サーバ(Authz Servers)] に移動します。

[新規追加(Add New)] をクリックして、Unified CM パブリッシャをシステムの Authz サーバとして追加します。

図 141 に示すように、Authz サーバの表示名として「**Authz Sever (ucm1)**」および「**ucm1.dcloud.cisco.com**」と入力します。[ユーザ名(Username)] および [パスワード(Password)] フィールドに、Unified CM 管理ログイン クレデンシャル(**administrator/dCloud123!**)を入力します。[証明書エラーを無視する(Ignore Certificate Errors)] の横のチェックボックスをオンにします。

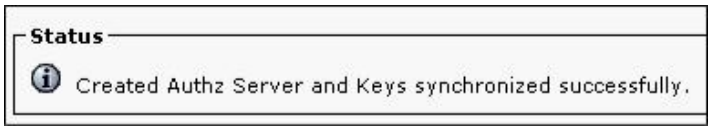
図 141. Unity Connection:Unified CM パブリッシャをシステム認可サーバとして追加



注: Unity Connection セキュア ボイスメール モジュール（モジュール 8）がまだ完了しておらず、Unity Connection サーバの tomcat 証明書が自己署名されるため、Unified CM に信頼されません。モジュール 8 でエンタープライズ CA を使用して Unity Connection tomcat 証明書に署名した後は、[証明書エラーを無視する（Ignore Certificate Errors）] チェックボックスをオンにする必要はありません。

[保存（Save）] をクリックします。図 142 に示すように、認可サーバとキーが同期されたことを確認するメッセージが表示されます。

図 142. Unity Connection：認可サーバが追加された

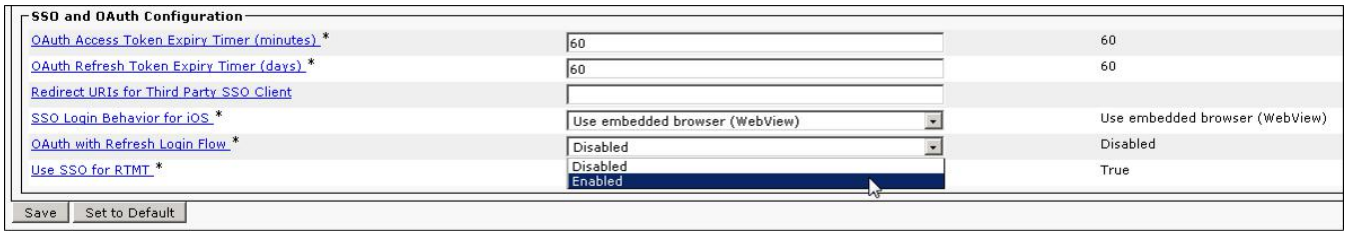


4. 更新ログイン フローによる OAuth の有効化

[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] に移動します。画面下部にある SSO および OAuth 設定サブセクションまでスクロールします。

図 143 に示すように、[更新ログインフローによる OAuth（OAuth with Refresh Login Flow）] ドロップダウン メニューから [有効（Enable）] を選択します。

図 143. Unity Connection：更新ログインフローによる OAuth の有効化



[保存（Save）] をクリックします。

C. オンプレミスの Jabber クライアントで更新ログイン フロー操作によって OAuth を検証する

次に、新しい OAuth ログイン フローが Jabber クライアントで機能しているかどうかを検証します。

5. オンプレミスの Jabber クライアントを起動してログインし、WKST2 で OAuth ログイン フローを検証し、Jabber クライアントを起動します。クライアントは自動的にサインインします。

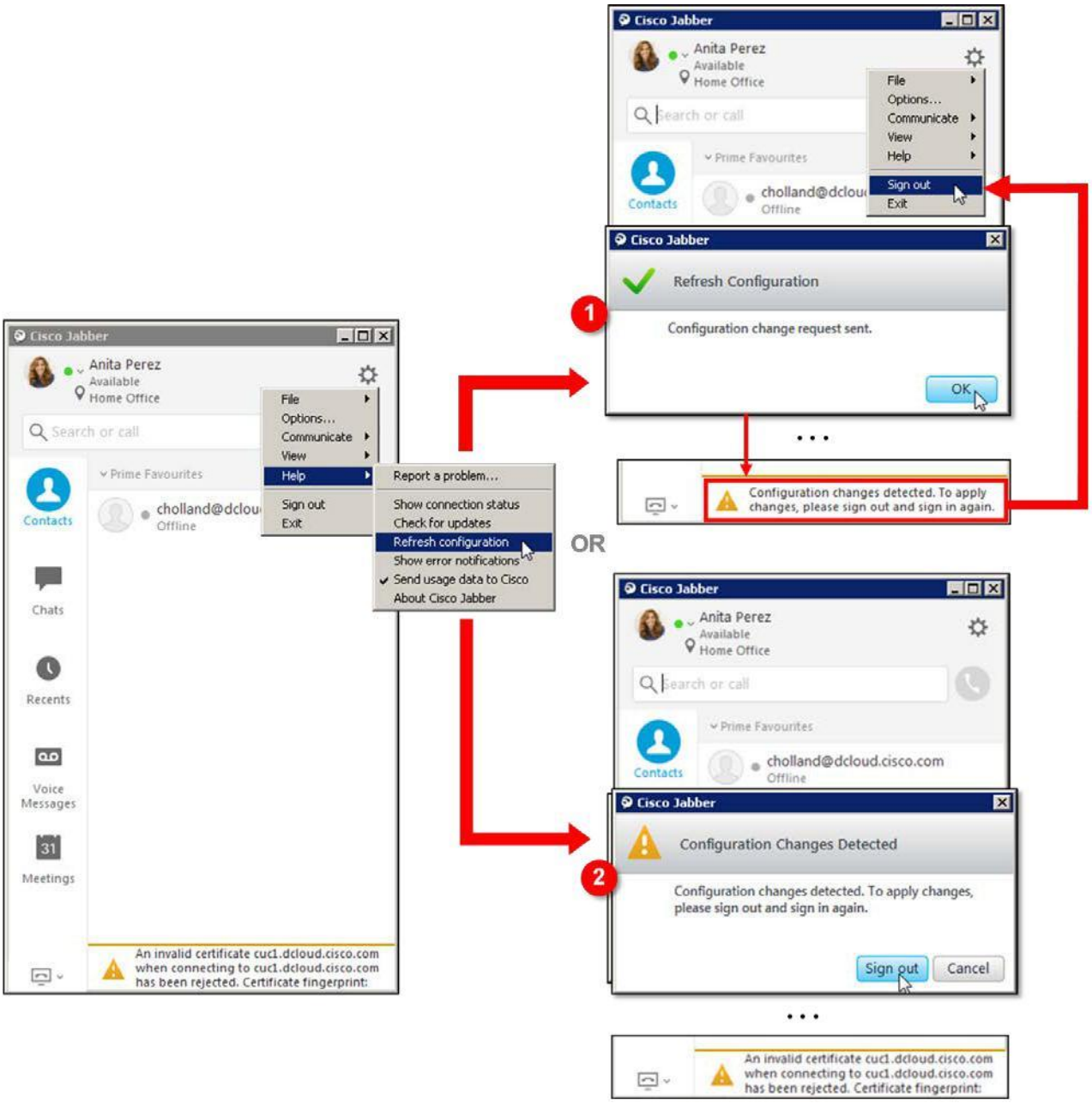
注: この場合も、「cuc1.dcloud.cisco.com への接続時に証明書 cuc1.dcloud.cisco.com が無効であるため拒否されました（An invalid certificate cuc1.dcloud.cisco.com when connecting to cuc1.dcloud.cisco.com has been rejected…）」が表示されます。この警告メッセージが表示されるのは、ラボの Unity Connection ボイスメール サービス ノードから受信した証明書がデフォルトの自己署名証明書で、ラボのワークステーションのローカル信頼ストアに存在しないためです。[拒否（Decline）] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。Jabber クライアントにエラー メッセージが表示され、ビジュアル ボイスメール サービスは接続されません。このメッセージは、証明書が無効であるために Unity Connection サーバ（cuc1.dcloud.cisco.com）との接続が拒否されたことを示します。このメッセージは、後でこのラボ（モジュール 8：次世代暗号化によるセキュアなボイスメール）でエンタープライズ CA を使用して Unity Connection サーバ証明書に署名すると表示されなくなり、OAuth ログイン フローによって、クライアントがボイスメール システムに自動的に接続されます。

この通常のログイン フローを使用するのは、すでにキャッシュされた認証セッションがあるためです。このキャッシュされた認証セッション キーをクリアして、OAuth による新しいログイン フローを強制するには、[設定（Settings）] メニューを選択し（図 144 を参照）、

[ヘルプ（Help）] > [設定の更新（Refresh configuration）] に移動します。図 168 に示すように、設定の更新とサインアウトが開始されますが、ネットワークとクライアントの応答時間に応じて、次のいずれかのようになります。

- [設定の更新（Refresh Configuration）] ウィンドウが表示されます。[OK] をクリックすると、[設定の変更が検出されました。変更を適用するには、サインアウトして再度サインインしてください（Configuration changes detected. To apply changes, please sign out and sign in again）] というメッセージが、クライアント ウィンドウの下部に表示されます。設定メニューに戻り、[サインアウト（Sign out）] をクリックしてクライアントからサインアウトします（#1、図 144 を参照）。
- [設定変更の検出（Configuration Changes Detected）] ウィンドウが（[設定の更新（Refresh Configuration）] ウィンドウの上または右に）表示されます。クライアント ウィンドウの下部に、Unity Connection の [無効な証明書 cuc1.dcloud.cisco.com（An invalid certificate cuc1.dcloud.cisco.com…）] メッセージが表示されます。[サインアウト（Sign out）] をクリックしてクライアントからサインアウトします（#2、図 144 を参照）。

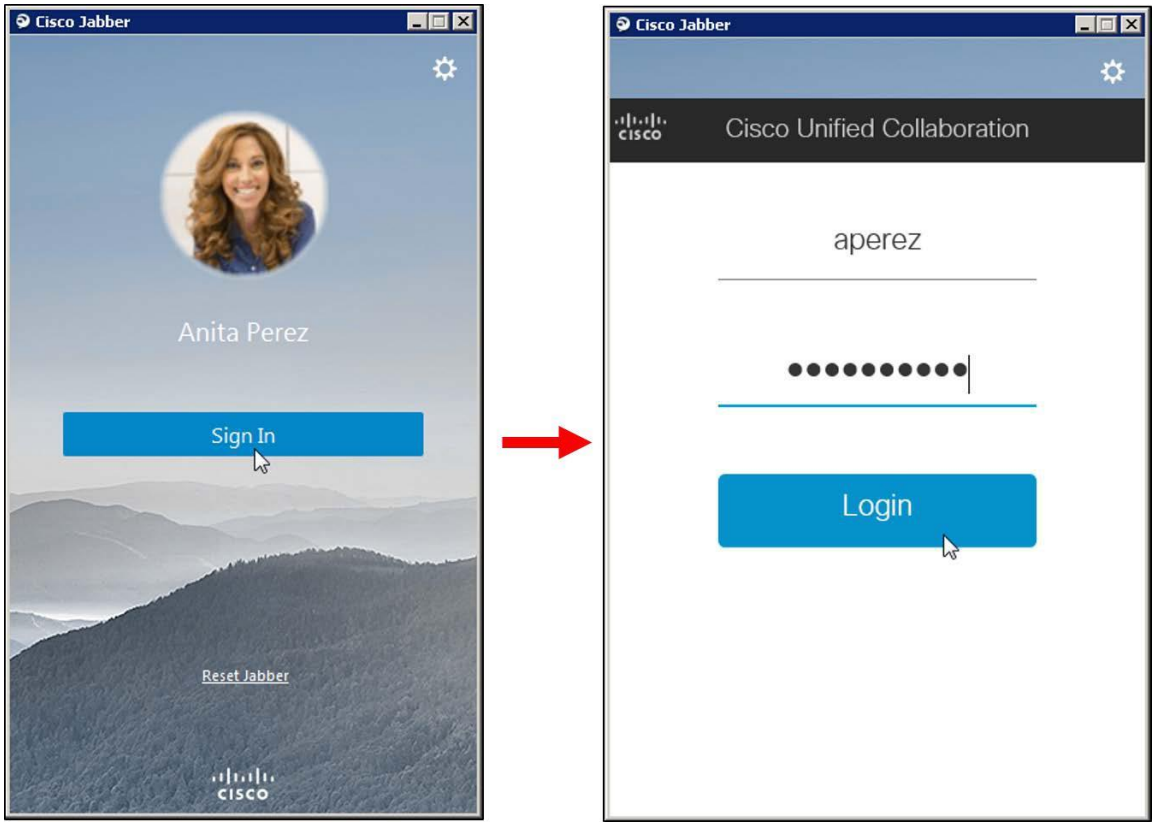
図 144. オンプレミスの Jabber クライアントの設定更新



注: キャッシュされた既存の Jabber 認証セッションは短期間で無効になるため、通常は設定の更新は不要です。このラボでは設定を手動で更新してプロセスの効率化を図るため、既存のログイン認証セッションの期限切れを待つ必要はありません。

[サインイン(Sign In)] ボタンを再度クリックすると、新しい OAuth ログイン画面が表示されます(図 145 を参照)。ユーザ名/パスワード: **aperez/C1sco12345** を入力します。

図 145. オンプレミスの Jabber クライアント(CSFAPEREZ)OAuth ログイン



Unity Connection 証明書警告ウィンドウで、再度 [拒否(Decline)] をクリックします。クライアント ウィンドウの下部に、「cuc1.dcloud.cisco.com への接続時に証明書 cuc1.dcloud.cisco.com が無効であるため拒否されました(An invalid certificate cuc1.dcloud.cisco.com when connecting to cuc1.dcloud.cisco.com has been rejected…)」という警告メッセージまたは [エラー通知の表示(Show error notifications)] メッセージが表示されます。クリックしてメッセージを承認すると、[エラー通知(Error Notifications)] ウィンドウが表示され、無効な cuc1.dcloud.cisco.com 証明書に関連する 1 つ以上の警告通知が示されます。

新しい OAuth ログイン フローによって、クライアントが適切なサービス(通話、IM and Presence)に接続されたことを確認します。

次に、WKST3 の Monica Cheng の Jabber クライアントで、上記の手順を繰り返します。WKST3(198.18.133.38、ユーザ名/パスワード: **DCLOUD\mcheng/C1sco12345**)に RDP 接続します。接続して Jabber クライアントを起動すると、自動的にログインします。次に設定を更新して([設定(Settings)] > [ヘルプ(Help)] > [設定の更新(Refresh configuration)])古いセッションをクリアし、新しいログイン フローを開始します。新しい OAuth ログイン画面で、ユーザ名/パスワード: **mcheng/C1sco12345** を入力します。新しい OAuth ログイン フローによって、クライアントが適切なサービス(通話、IM and Presence)に接続されたことを確認します。

注:この場合も、「cuc1.dcloud.cisco.com への接続時に証明書 cuc1.dcloud.cisco.com が無効であるため拒否されました(An invalid certificate cuc1.dcloud.cisco.com when connecting to cuc1.dcloud.cisco.com has been rejected…)」(または [エラー通知の表示(Show error notifications)])が表示されます。[拒否(Decline)] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。このメッセージは、後でこのラボ(モジュール 8:次世代暗号化によるセキュアなボイスメール)でエンタープライズ CA を使用して Unity Connection サーバ証明書に署名すると表示されなくなり、OAuth ログイン フローによって、クライアントがボイスメール システムに自動的に接続されます。

続行する前に、WKST2 と WKST3 の両方で Jabber を終了します。

***** モジュール #6 の終了 *****

モジュール 7. Cisco Unified Border Element（CUBE）とのセキュアな統合

モジュールの概要

このモジュールでは、Unified CM と Cisco Unified Border Element（CUBE）間のセキュアな統合を可能にし、PSTN とのセキュアな通話を実現します。最初に CUBE 証明書のセットアップ、CA 署名、管理について取り上げます。次に、CUBE での暗号化を有効にし、CUBE に対する Unified CM SIP トランクで暗号化を設定します。最後にテスト通話を行い、CUBE との暗号化された統合を確認します。このモジュールは、次の 4 つのセクションに分割されています。

A. CUBE 証明書の管理

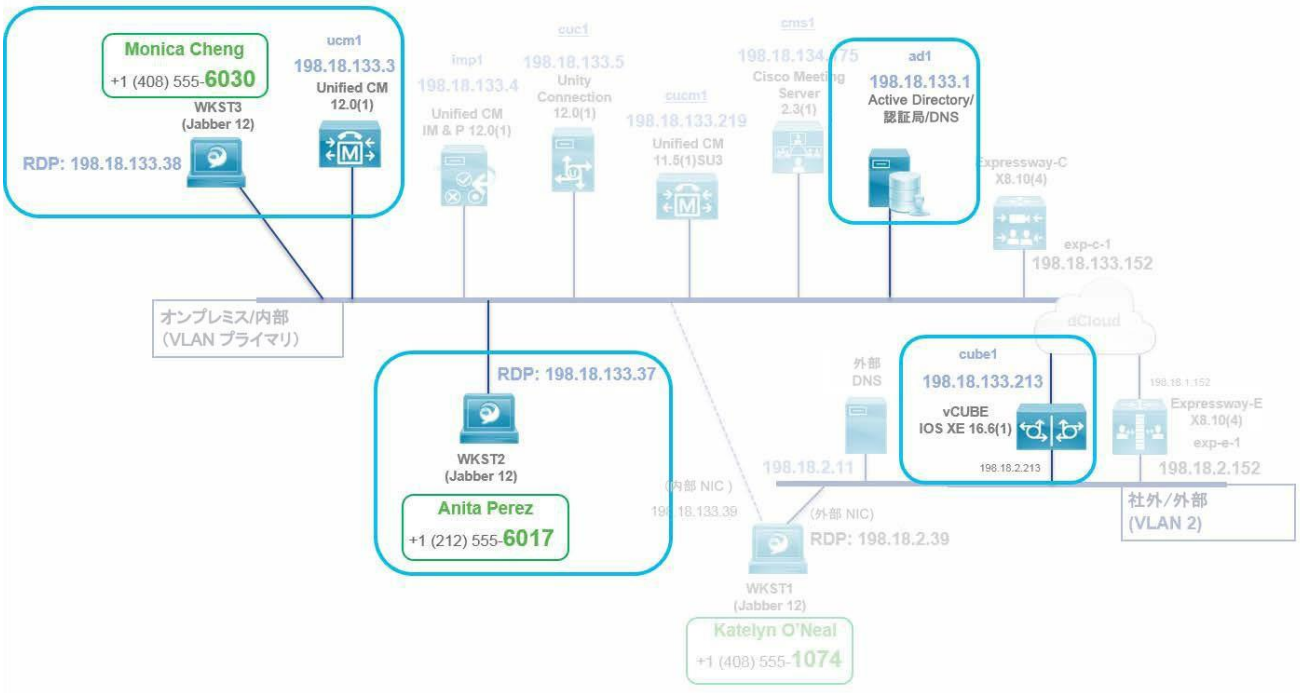
B. CUBE での暗号化の有効化

C. CUBE での Unified CM セキュア SIP トランクの設定

D. エンドポイントと CUBE 間の暗号化された通話の確認

次の図 146 は、このモジュールのトポロジおよび関連するコンポーネントを示しています。

図 146.　モジュール 7：CUBE ラボ トポロジとのセキュアな統合



手順

A. CUBE 証明書の管理

このセクションでは、CUBE でセキュリティトラストポイントを有効にして証明書を管理します。これは、暗号化と Unified CM とのセキュアな統合を行う前に実行する必要があります。

1.　RSA キー ペアを作成する

WKST2（198.18.133.37）に **RDP** 接続して、ユーザ名/パスワード：**DCLOUD\aperez/C1sco12345** でログインします。

WKST2 で PuTTY を使用して、CUBE（cube1.dcloud.cisco.com）コマンド ライン インターフェイスに **SSH** 接続します。

PuTTY アイコン 

をダブルクリックして起動します。cube1 プロファイルを選択するか、[ホスト名（Host Name）]（または [IP アドレス（IP Address）] フィールドに「**cube1.dcloud.cisco.com**」と入力します。[開く（Open）] をクリックします。

図 147 に示すように、プロンプトが表示されたら [はい（Yes）] をクリックして、ssh-rsa2 キーをキャッシュします。

図 147. CUBE との SSH 接続におけるキー キャッシュの確認

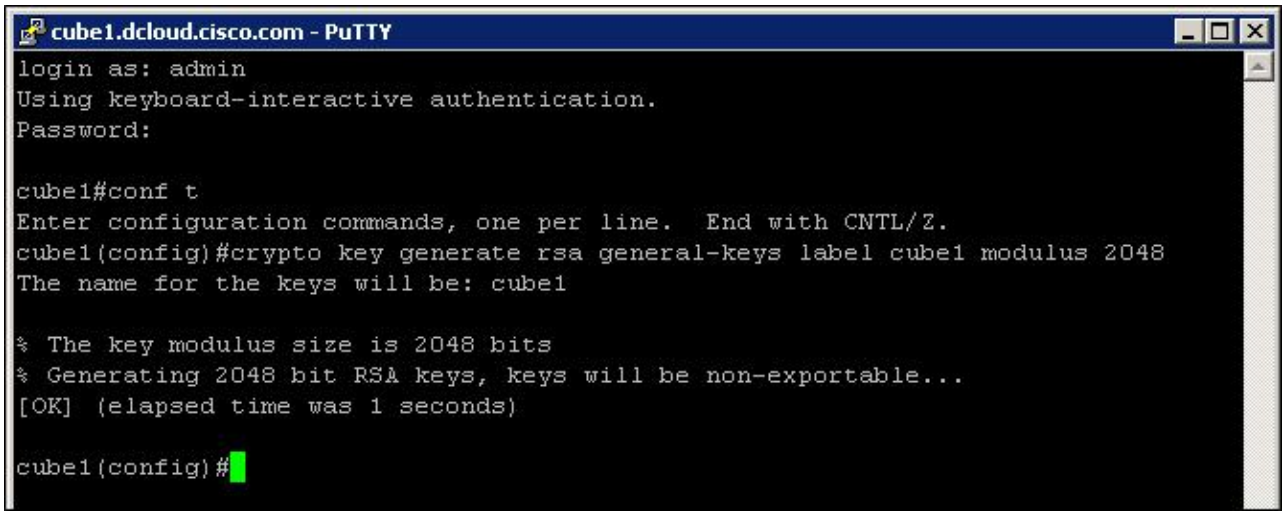
ユーザ名/パスワード：**admin/dCloud123!** でログインします。ログインしたら、次のように入力して設定モードに入ります。

```
config t
```

次のコマンドを入力して、セキュアなキー ペアを生成します（図 148 を参照）。

```
crypto key generate rsa general-keys label cube1 modulus 2048
```

図 148. CUBE：セキュアなキー ペアの生成



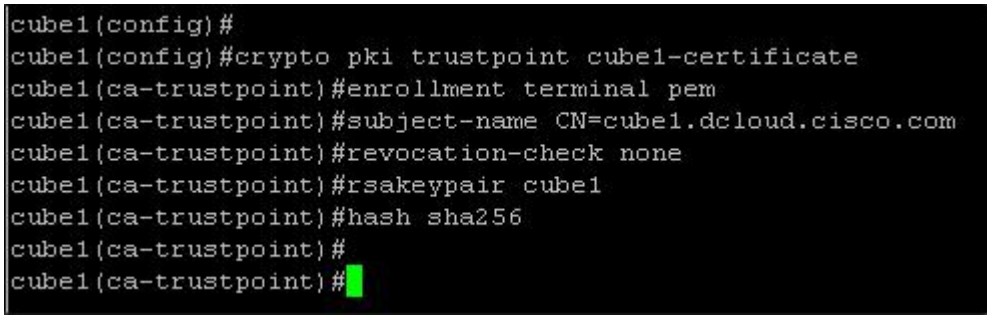
2. Cisco Unified Border Element（CUBE）用に PKI トラストポイントを作成する

次に、前の手順で作成したキー ペアを使用して、トラストポイントを作成します。これが、証明書署名要求を生成するためのトラストポイント アンカーになります。

設定モード プロンプトに次のコマンドを入力します（図 149 を参照）。

```
crypto pki trustpoint cube1-certificate
enrollment terminal pem subject-name
CN=cube1.dcloud.cisco.com revocation-
check none
rsakeypair cube1
hash sha256
```

図 149. CUBE：CUBE 用のトラストポイント アンカーの作成



3. CA によってトラストポイントを認証し、CA 証明書を承認する

エンタープライズ CA ルート証明書を使用してトラストポイントを認証し、CUBE 証明書に署名する必要があります。最初に、エンタープライズ CA ルート証明書を Base 64 形式でダウンロードして、内容を CLI にコピーします。

WKST2（198.18.133.37、DCLOUD**aperez/C1sco12345**）の Firefox ブラウザで、https://ad1.dcloud.cisco.com/certsrv にアクセスします。ユーザ名/パスワード：**administrator/C1sco12345** でログインします。

[CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] リンクをクリックします。次の画面で、エンコード方式として [Base 64] を選択して、[CA 証明書のダウンロード（Download CA Certificate）] をクリックします（図 150 を参照）。

図 150. Base 64 でエンコードされたエンタープライズ CA ルート証明書をダウンロード

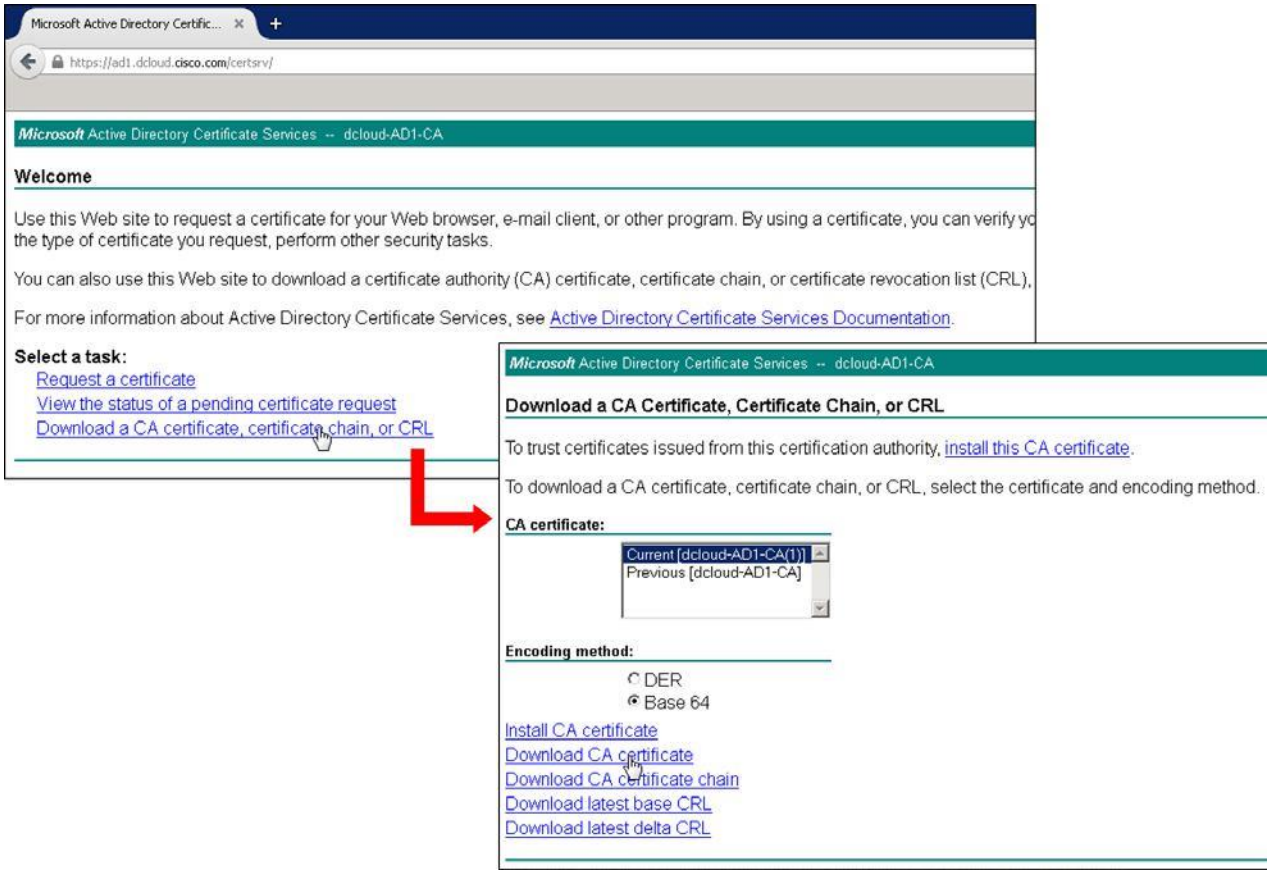
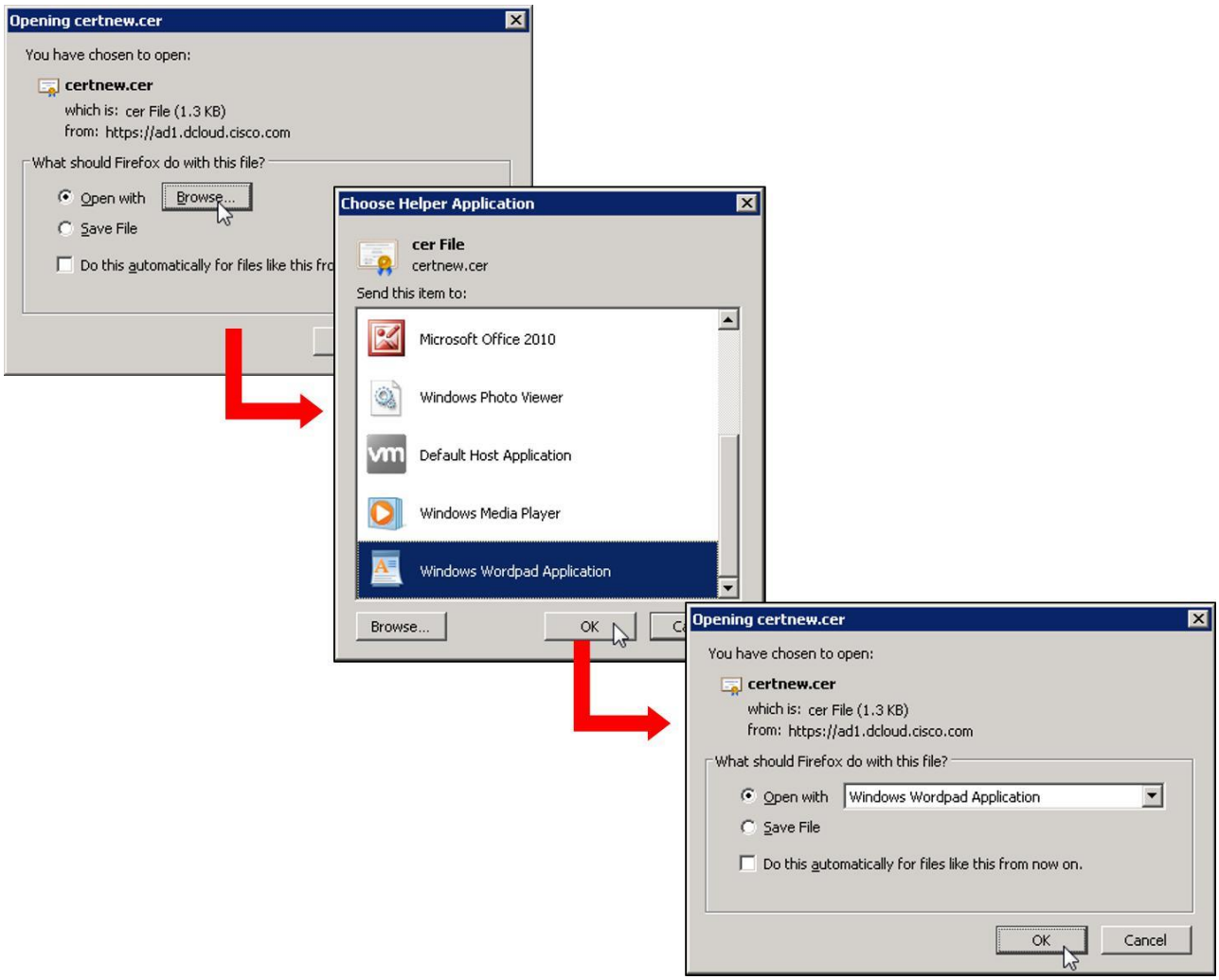


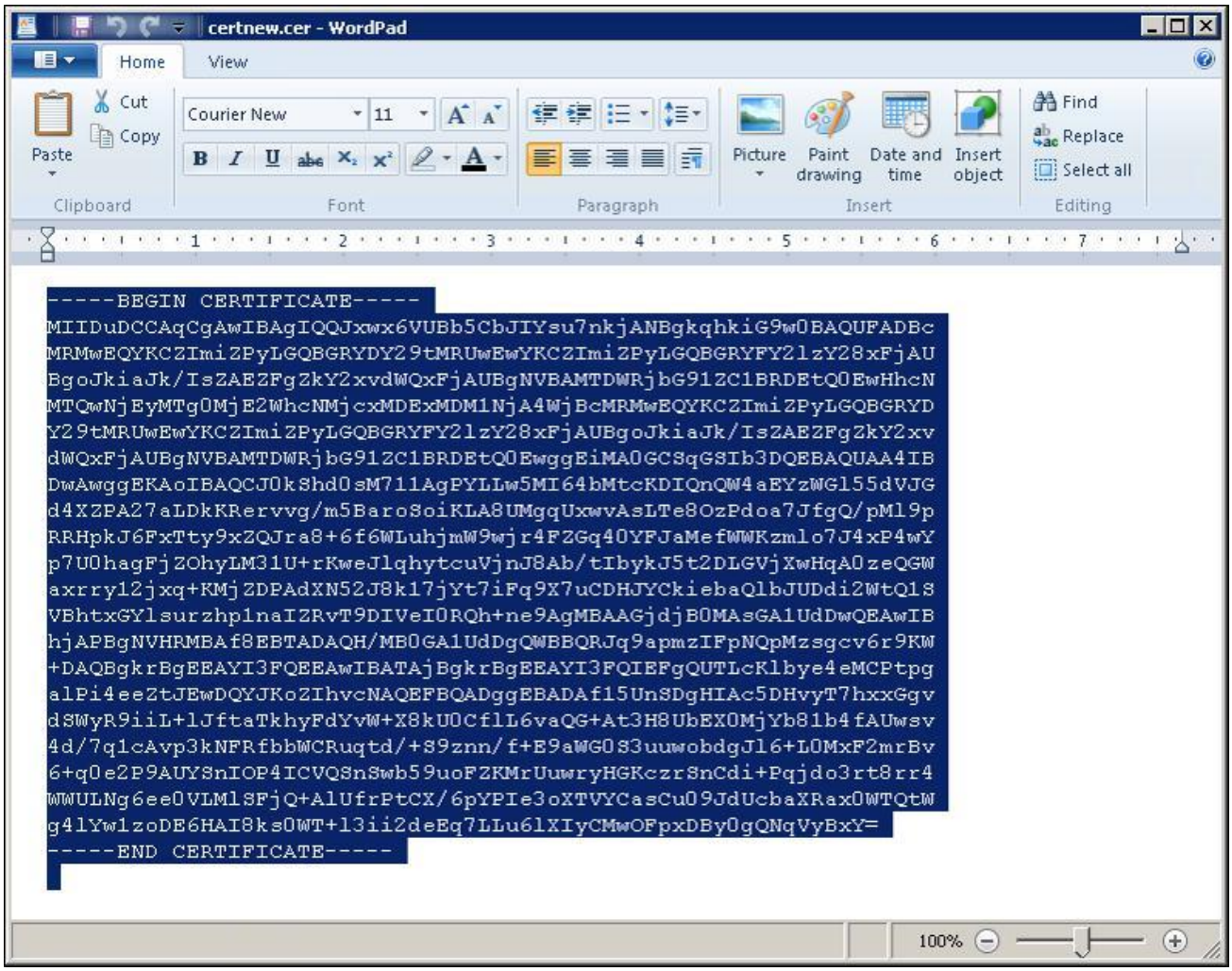
図 151 に示すように、ダウンロードしたファイルをワードパッド（またはメモ帳）で開きます。

図 151. Base 64 でエンコードされたエンタープライズ CA ルート証明書を開く



ワードパッドが開き、Base 64 でエンコードされた証明書が表示されます。このファイル内のテキストをコピーして貼り付け、トラストポイントを認証します（図 152 を参照）。

図 152. Base 64 でエンコードされたエンタープライズ CA ルート証明書*



上の図の証明書文字列は、実際のポッドと異なる場合があります。

CUBE に対する SSH PuTTY セッションに戻る新しい SSH 接続を開き、セッションが終了していた場合は再度ログインします（cube1.dcloud.cisco.com、**admin/dCloud123!**）。

設定モード（`conf t`）に入り、図 153 に示すように、次のコマンドを入力して認証プロセスを開始します。

```
crypto pki authenticate cube1-certificate
```

ワードパッドに戻り、Base 64 でエンコードされた CA ルート証明書の内容（末尾の空白行を含む）を、クリップボードにコピー（Ctrl+C）します（図 176 を参照）。

PuTTY セッションに戻り、認証プロンプトが表示されたら、コピーした CA ルート証明書を貼り付けます（右クリック）。リターン/Enter を押して証明書の終了を示し、プロンプトに「**yes**」と入力し、さらに Enter を押して証明書をインポートします（図 177 を参照）。

図 153. CUBE：エンタープライズ CA ルート証明書のアップロード*

```
cube1(config)#crypto pki authenticate cube1-certificate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDuDCCAqCgAwIBAgIQQJxwx6VUBb5CbJIYsu7nkjANBgkqhkiG9w0BAQUFADBc
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFjAU
BgoJkiaJk/IsZAEZFgZkY2xvdWQxFjAUBgNVBAMTDWRjbG91ZC1BRDEtQ0EwHhcN
MTQwNjEyMTgOMjE2WhcNMjcxMDExMDM1NjA4WjBcMRMwEQYKCZImiZPyLGQBGRYD
Y29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFjAUBgoJkiaJk/IsZAEZFgZkY2xv
dWQxFjAUBgNVBAMTDWRjbG91ZC1BRDEtQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCJOkShdOsM711AgPYLLw5MI64bMtcKDIQnQW4aEYzWG155dVJG
d4XZPA27aLDkKRervvg/m5BaroSoiKLA8UMgqUxwvAsLTe8OzPdoa7JfgQ/pMl9p
RRHpkJ6FxTty9xZQJra8+6f6WLuhjmW9wjr4FZGq4OYFJaMefWWKzmlo7J4xP4wY
p7UOhagFjZOhyLM31U+rKweJlqhytcuVjnJ8Ab/tIbykJ5t2DLGVjXwHqAOzeQGW
axrry12jxq+KMjZDPAdXN52J8k17jYt7iFq9X7uCDHJYCkiebaQlbJUDdi2WtQ1S
VBhtxGYlsurzhp1naIZRvT9DIVeIORQh+ne9AgMBAAGjdjBOMAsGA1UdDwQEAwIB
hjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQRJq9apmzIFpNQpMzsgcv6r9KW
+DAQBgkrBgEEAYI3FQEEAwIBATAjBgkrBgEEAYI3FQIEFgQUTLcK1bye4eMCPtpg
alPi4eeZtJEwDQYJKoZIhvcNAQEFBQADggEBADAf15UnSDgHIAc5DHvyT7hxxGgv
dSWyR9iiL+lJftaTkhyFdYvW+X8kUOCflL6vaQG+At3H8UbEXOMjYb81b4fAUwsv
4d/7q1cAvp3kNFRfbbWCRuqtd/+S9znn/f+E9aWGOS3uuwobdgJ16+LOMxF2mrBv
6+qOe2P9AUYSnIOP4ICVQSnSwb59uoFZKMrUuwryHGKczrSnCdi+Pqjdo3rt8rr4
WWULNg6eeOVLMlSFjQ+AlUfrPtCX/6pYPIe3oXTVYCasCuO9JdUcbaXRax0WTQtW
g4lYw1zoDE6HAI8ksOWT+l3ii2deEq7LLu61XIyCMwOFpxDByOgQNqVyBxY=
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: F1B457D8 B311EFA5 E1F245D1 106381C3
      Fingerprint SHA1: F0719345 5E345E55 0B3D0A6A 6D28CB5C 99B410DB

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

cube1(config)#
```

*上の図の証明書文字列は、実際のポッドと異なる場合があります。

4. CA サーバでトラストポイントを登録する

エンタープライズ CA ルート証明書をインポートしたので、CUBE 証明書の証明書署名要求（CSR）を登録または生成します。設定プロンプトで、次のコマンドを入力します。

```
crypto pki enroll cube1-certificate
```

ルータのシリアル番号と IP アドレスを入力するプロンプトが表示されたら、「**no**」と入力します。ターミナルに証明書要求を表示するプロンプトが表示されたら、「**yes**」と入力します。図 154 に、登録の手順と登録結果の CSR を示します。

図 154. CUBE：CUBE 証明書署名要求（CSR）*

```
cube1(config)#crypto pki enroll cube1-certificate
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=cube1.dcloud.cisco.com
% The subject name in the certificate will include: cube1.dcloud.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQAwSDEfMB0GA1UEAxMWY3ViZTEuZGNsb3VkLmNpc2NvLmNvbTEl
MCMGCSqGSIb3DQEJAhYWY3ViZTEuZGNsb3VkLmNpc2NvLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALGGq6uU6G6KzK99gVVR+OFO7f3ZKkZk2ozd
WVBp+HObZ/xkm2e/uWBCvvF/mpzYaVEdhM1tQHUdt/TKOwxzU2IlR5WqhWg7PuyI
qSWN8GFVO9yvLuRkH3TOh3WrvCqPOVpAmfnJJCkyjDrRoCAORugHWxQIIQa8RKZ+
ATQs+hi7JobWCYfOWewCdGOUGYSZl8KJIP8XFjwznzWwRv3+V7qu8eLT9DsaeCuq
gNiR7PJgnF1bytXdKpRw2sKj7xqPXLgDuAIt31Q7AQBOHSRRTD1XVvGCw4XnU/vx
bxfUwh2jMbvBtjlzbzR5Hk2coDL8BI4Wajb1z5NV7pcKh7beeeMCAwEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVROPAQH/BAQDAgWgMA0GCSqGSIb3DQEBCwUAA4IB
AQBxEic5NqutuZrHdXnGNPw2hnx5TpdYRZMO1S82/rOiyemdLXbWih/a+fXjuOUS
/pjOrHkh8hoemAGau88yUnM3H7VfWS3NwcMacfyEUqktwxGT/XuNmgt5KyEmk6mg
RkQHktjaZTmjCJByGxz3PJNsDmU9g6cSiSnmQQwLIQGyFrm64typARwHvoHGbLgp
6zJIJKIk9BkYBZgNXEkCpIomPIHjjMHxwqnvpheN+mx3FVKEOhLRpybFwE6uDz1H
PpME3ili4hy2EtUUApRzLsgEswSP7WQrwq3MgA+wHptfavw6HjB6PqhuiQe/sRHG
vJux4FRYtLN3H2ER8U8HONo4
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

上の図の証明書署名要求文字列は、実際のポッドと異なる場合があります。

再表示登録要求プロンプトに「**no**」を入力して、CSR の内容をクリップボードにコピーします。これは、エンタープライズ CA によって証明書に署名するために使用します（図 155 を参照）。

図 155. CUBE：CUBE CSR のコピー*

```
cube1(config)#crypto pki enroll cube1-certificate
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=cube1.dcloud.cisco.com
% The subject name in the certificate will include: cube1.dcloud.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQAwSDEfMB0GA1UEAxMWY3ViZTEuZGNsb3VkLmNpc2NvLmNvbTEl
MCMGCSqGSIb3DQEJAhYWY3ViZTEuZGNsb3VkLmNpc2NvLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALGGq6uU6G6KzK99gVVR+OFO7f3ZKkZk2ozd
WVBp+HObZ/xkm2e/uWBCvvF/mpzYaVEdhMltQHUdt/TKOwxzU2IlR5WqhWg7PuyI
qSWN8GFVO9yvLuRkH3TOh3WrvCqPOVpAmfnJJCkyjDrRoCAORugHWxQIIQa8RKZ+
ATQs+hi7JobWCYfOWewCdGOUGYSZl8KJIP8XFjwznzWwRv3+V7qu8eLT9DsaeCuq
gNiR7PJgnF1bytXdKpRw2sKj7xqPXLgDuAIt31Q7AQBOHSRRTDlXVvGCw4XnU/vx
bxfUwh2jMbvBtjlzbzR5Hk2coDL8BI4Wajb1z5NV7pcKh7beeeMCAwEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVROPAQH/BAQDAgWgMA0GCSqGSIb3DQEBCwUAA4IB
AQBxEic5NqutuZrHdXnGNPw2hnx5TpdYRZMO1S82/rOiyemdLXbWih/a+fXju0US
/pjOrHkh8hoemAGau88yUnM3H7VfWS3NwcMacfyEUqktwxGT/XuNmgt5KyEmk6mg
RkQHktjaZTmjCJByGxz3PJNsDmU9g6cSiSnmQQwLIQGyFrm64typARwHvoHGbLgp
6zJIJKIk9BkYBZgNXEkCpIomPIHjjMHxwqnvpheN+mx3FVKEOhLRpybFwE6uDz1H
PpME3ili4hy2EtUUApRzLsgEswSP7WQrwq3MgA+wHptfavw6HjB6PqhuiQe/sRHG
vJux4FRYtLN3H2ER8U8HONo4
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
cube1(config)#
```

**上の図の証明書署名要求文字列は、実際のポッドと異なる場合があります。*

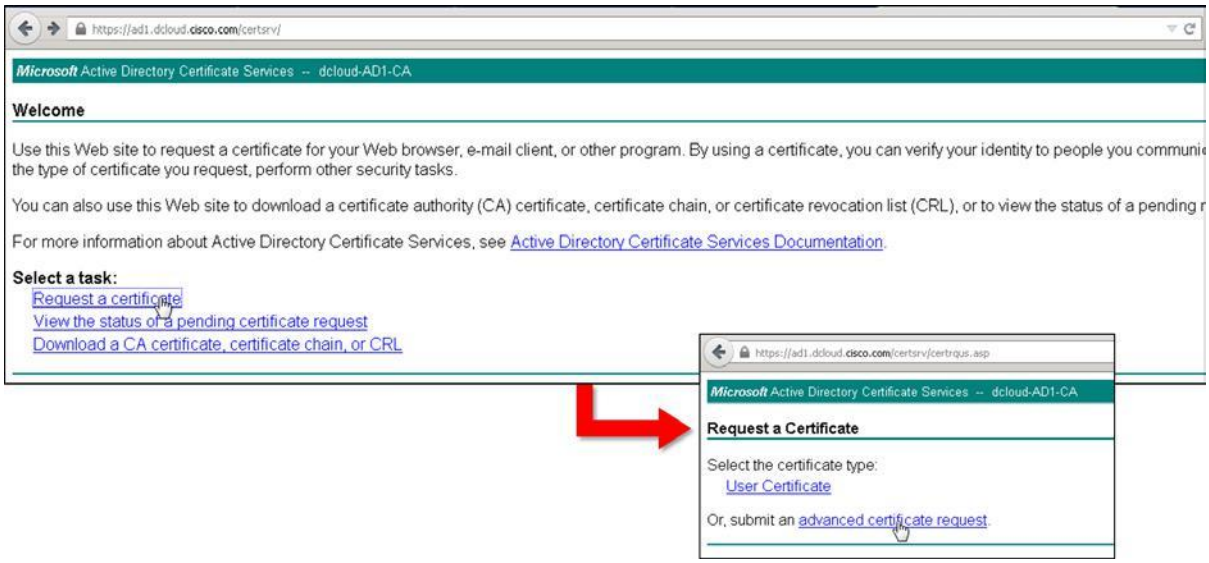
5. エンタープライズ CA で CUBE CSR に署名する

   次に、エンタープライズ CA（ad1.dcloud.cisco.com）を使用して、CUBE 用に CA 署名付き証明書を生成します。

   WKST2（198.18.133.37）で Firefox Web ブラウザを使用して、https://ad1.dcloud.cisco.com/certsrv に戻ります。認証を求められたら、ユーザ名/パスワード：**administrator/C1sco12345** を使用してログインします。

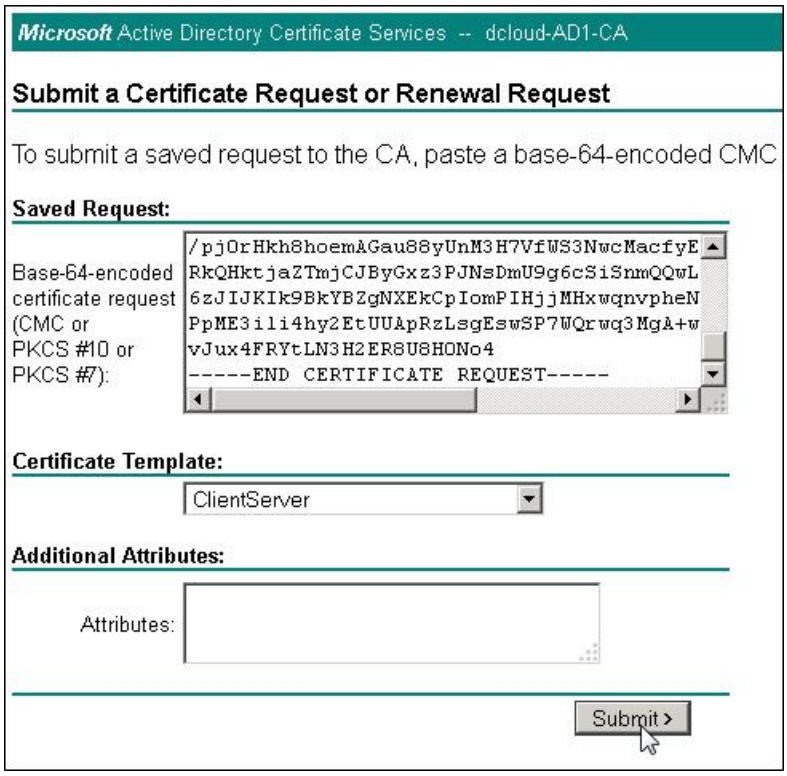
   [証明書を要求する（Request a certificate）] をクリックします。次に [または詳細証明書要求を送信する（Or, submit an advanced certificate request）] をクリックします（図 156 を参照）。

図 156. エンタープライズ CA で署名付き証明書を要求



（前の手順で CSR からコピーした）クリップボードの内容を、[Base-64 でエンコードされた証明書要求（Base-64-encoded certificate request）] フィールドに貼り付けます（Ctrl+V）。図 157 に示すように、**ClientServer** 証明書テンプレートを選択して [送信>（Submit >）] をクリックします。

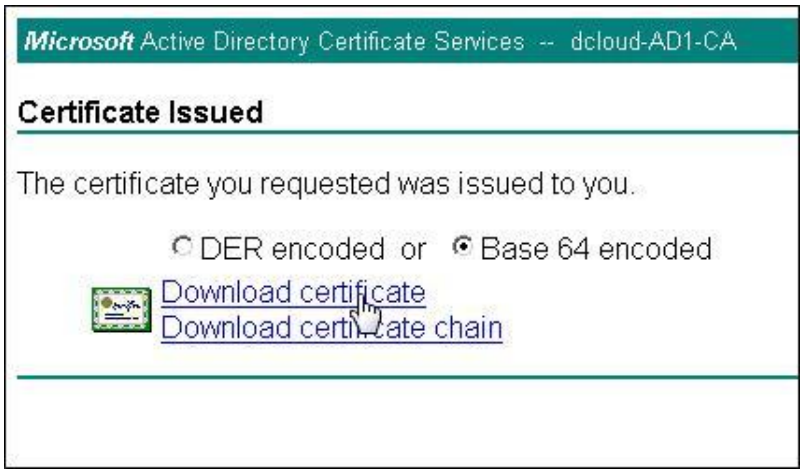
図 157. CUBE 証明書要求を送信*



上の図の証明書署名要求文字列は、実際のポッドと異なる場合があります。

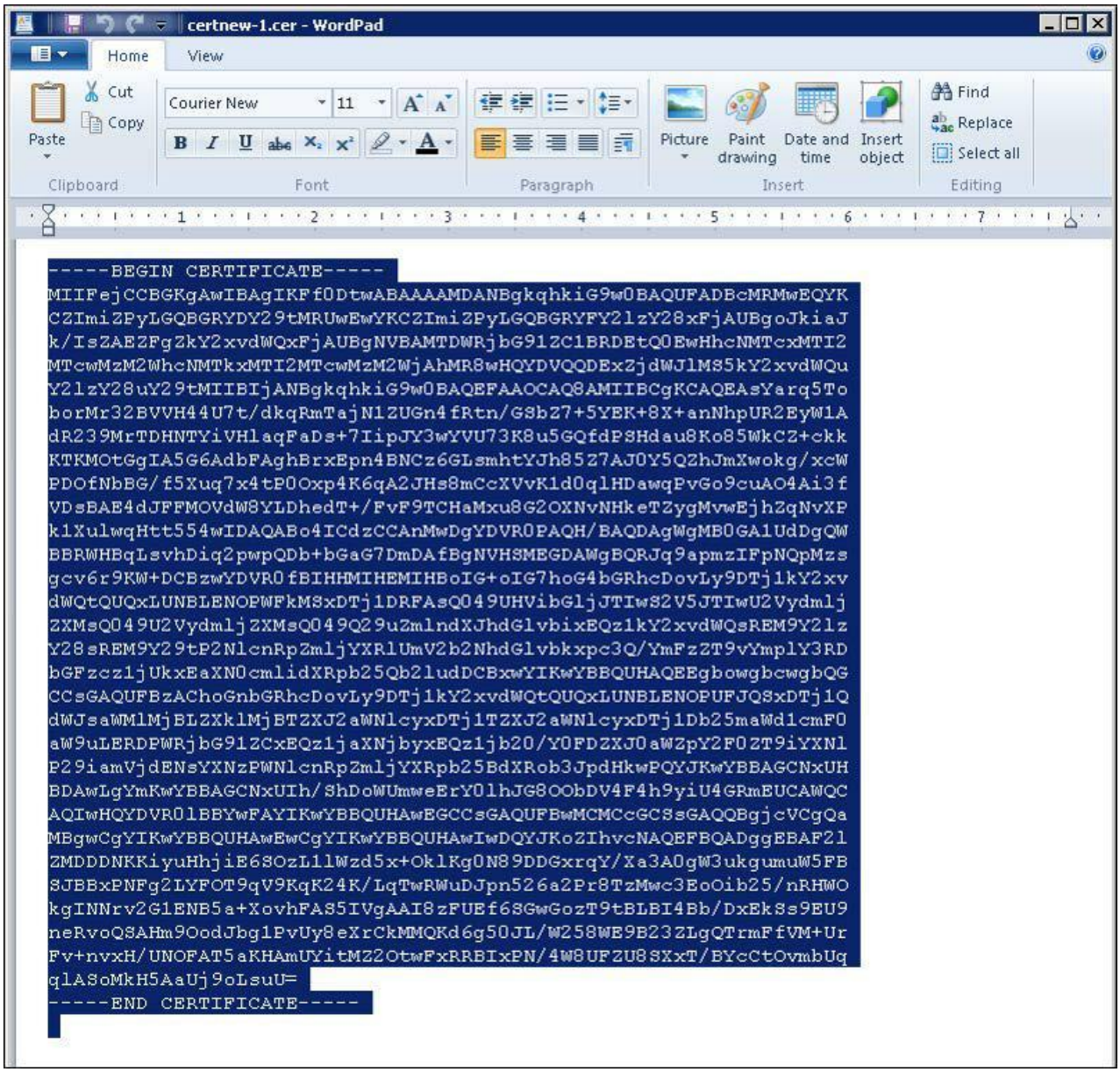
次の画面で [Base 64 でエンコード（Base 64 encoded）] を選択し、[証明書をダウンロード（Download certificate）] をクリックします（図 158 を参照）。

図 158. CA 署名付き CUBE 証明書のダウンロード



前回と同様に、ダウンロードしたファイルを Windows ワードパッド アプリケーションで開きます（[参照（Browse…）] をクリックして、アプリケーション リストからワードパッドを選択し、[OK] をクリックして選択し、[OK] をクリックして証明書を開きます）。末尾の空白行を含めてファイルの内容を選択し、クリップボードにコピー（Ctrl+C）します（図 159 参照）。

図 159. CUBE CA 署名付き証明書*



***上の図の証明書文字列は、実際のポッドと異なる場合があります。**

6. 生成された証明書を CUBE にインポートする

エンタープライズ CA 署名付き証明書を入手したところで、次に証明書を CUBE にインポートする必要があります。インポートするには、CUBE に対する SSH PuTTY セッションに戻ります。必要に応じて、新しい SSH 接続を開いて再度ログインします（cube1.dcloud.cisco.com、**admin/dCloud123!**）。

図 160 に示すように、設定モード（`conf t`）に入り、次のコマンドを入力して、CA 署名付き証明書をインポートします。

```
crypto pki import cube1-certificate certificate
```

プロンプトが表示されたら、CA 署名付き CUBE 証明書をターミナルに（右クリックで）貼り付け、Enter を押して証明書をインポートします。証明書がインポートされたことを確認してから次に進んでください（図 184 を参照）。

図 160. CA 署名付き CUBE 証明書のインポート*

```
cube1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cube1(config)#crypto pki import cube1-certificate certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFejCCBGKgAwIBAgIKFfODtwABAAAAMDANBgkqhkiG9w0BAQUFADBcMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFjAUBgoJkiaJ
k/IsZAEZFgZkY2xvdWQxFjAUBgNVBAMTDWRjbG91ZC1BRDEtQOEwHhcNMTcxMTI2
MTcwMzM2WhcNMTkxMTI2MTcwMzM2WjAhMR8wHQYDVQQDExZjdWJlMS5kY2xvdWQu
Y2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsYarq5To
borMr32BVVH44U7t/dkqRmTajN1ZUGn4fRtn/GSbZ7+5YEK+8X+anNhpUR2EyW1A
dR239MrTDHNTYiVHlaqFaDs+7IipJY3wYVU73K8u5GQfdPSHdau8Ko85WkCZ+ckk
KTKMOtGgIA5G6AdbFAghBrxEpn4BNCz6GLsmhtYJh85Z7AJOY5QZhJmXwokg/xcW
PDOfNbBG/f5Xuq7x4tPOOxp4K6qA2JHs8mCcXVvK1dOqlHDawqPvGo9cuAO4Ai3f
VDsBAE4dJFFMOVdW8YLDhedT+/FvF9TCHaMxu8G2OXNvNHkeTZygMvwEjhZqNvXP
k1XulwqHtt554wIDAQABo4ICdzCCAnMwDgYDVR0PAQH/BAQDAgWgMB0GA1UdDgQW
BBRWHBqLsvhDiq2pwpQDb+bGaG7DmDAfBgNVHSMEGDAWgBQRJq9apmzIFpNQpMzs
gcv6r9KW+DCBzwYDVR0fBIHHMIHEMIHBoIG+oIG7hoG4bGRhcDovLy9DTj1kY2xv
dWQtQUQxLUNBLENOPWFkMSxDTj1DRFAsQO49UHVibGljTIwS2V5JTIwU2Vydmlj
ZXMsQO49U2VydmljZXMsQO49Q29uZmlndXJhdGlvbixEQz1kY2xvdWQsREM9Y2lz
Y28sREM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RD
bGFzcz1jUkxEaXNOcmlidXRpb25Qb2ludDCBxwYIKwYBBQUHAQEEgbowgbcwgbQG
CCsGAQUFBzAChoGnbGRhcDovLy9DTj1kY2xvdWQtQUQxLUNBLENOPUFJQSxDTj1Q
dWJsaWM1MjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1cmFO
aW9uLERDPWRjbG91ZCxEQz1jaXNjbyxEQz1jb20/YOFDZXJOaWZpY2FOZT9iYXN1
P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25BdXRob3JpdHkwPQYJKwYBBAGCNxUH
BDAwLgYmKwYBBAGCNxUIh/ShDoWUmweErYO1hJG8OObDV4F4h9yiU4GRmEUCAWQC
AQIwHQYDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCcGCSsGAQQBgjcVCgQa
MBgwCgYIKwYBBQUHAwEwCgYIKwYBBQUHAwIwDQYJKoZIhvcNAQEFBQADggEBAF2l
ZMDDDNKKiyuHhjiE6SOzL11Wzd5x+OklKgON89DDGxrqY/Xa3AOgW3ukgumuW5FB
SJBBxPNFg2LYFOT9qV9KqK24K/LqTwRWuDJpn526a2Pr8TzMwc3EoOib25/nRHWO
kgINNrv2G1ENB5a+XovhFAS5IVgAAI8zFUEf6SGwGozT9tBLBI4Bb/DxEkSs9EU9
neRvoQSAHm9OodJbg1PvUy8eXrCkMMQKd6g5OJL/W258WE9B23ZLgQTrmFfVM+Ur
Fv+nvxH/UNOFAT5aKHAmUYitMZ2OtwFxRRBIxPN/4W8UFZU8SXxT/BYcCtOvmbUq
qlASoMkH5AaUj9oLsuU=
-----END CERTIFICATE-----

% Router Certificate successfully imported

cube1(config)#
```

***上の図の証明書文字列は、実際のポッドと異なる場合があります。**

B. CUBE での暗号化の有効化

証明書管理を実施したところで、CUBE で暗号化を有効にする必要があります。

7. セキュアなシグナリングを有効にする

まず、以前作成した cube1-certificate トラストポイントと Unified CM を関連付けることで、セキュアなシグナリングを有効にします。CUBE に対する SSH PuTTY セッションに戻る必要に応じて、新しい SSH 接続を開いて再度ログインします（cube1.dcloud.cisco.com、**admin/dCloud123!**）。

図 161 に示すように、設定モード（conf t）に入り、次のコマンドを入力して、トラストポイントと Unified CM シグナリング パスをバインドします。

```
sip-ua
 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint cube1-certificate
```

図 161. CUBE トラストポイント/証明書を Unified CM シグナリング パスにバインド*

```
cube1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cube1(config)#sip-ua
cube1(config-sip-ua)#$8.18.133.3 255.255.255.255 trustpoint cube1-certificate
cube1(config-sip-ua)#
```

****上記の暗号シグナリング コマンドはターミナルによって省略されており、完全に表示されていません。***

8. ダイヤルピアに対する TLS トランスポートを有効にする

セキュアなトラストポイントと Unified CM シグナリング パスを関連付けたので、次に適切なダイヤルピアに対して TLS 暗号化を有効にします。ここでは、300 と 400 の 2 つのダイヤルピアで TLS 暗号化を有効にします。

ダイヤルピア 300 と 400 でセキュアなシグナリングを有効にするには、図 162 に示すように、設定プロンプト（conf t）で次のコマンドを入力します。

```
dial-peer voice 300
 session transport tcp tls
!
dial-peer voice 400
 session transport tcp tls
```

図 162. ダイヤルピアに対する TLS 暗号化の有効化

```
cube1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cube1(config)#dial-peer voice 300
cube1(config-dial-peer)# session transport tcp tls
cube1(config-dial-peer)#!
cube1(config-dial-peer)#dial-peer voice 400
cube1(config-dial-peer)# session transport tcp tls
cube1(config-dial-peer)#
cube1(config-dial-peer)#
```

9. SRTP パススルーを設定する

シグナリング暗号化を設定したら、次に RTP 暗号化（SRTP）を設定する必要があります。このステップでは、SRTP パススルー モードを有効にします。SRTP パススルーによって、CUBE では、暗号化された RTP パケットが、B2BUA が復号することなくそのまま転送されるため、送信元端末と宛先端末間で強力な暗号を使用できるようになります。

図 163 に示すように、SRTP パススルー モードを設定するには、設定プロンプトで次のコマンドを入力します。

```
voice service voip
  srtp pass-thru
```

図 163. SRTP パススルーの有効化

```
cube1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cube1(config)#voice service voip
cube1(conf-voi-serv)# srtp pass-thru
cube1(conf-voi-serv)#
cube1(conf-voi-serv)#
```

最後に、図 164 に示すように、コマンド プロンプトで次のコマンドを入力して、CUBE 設定を保存してから続行します。

```
write memory
```

図 164. CUBE 設定の保存

```
cube1#write memory
Building configuration...
[OK]
cube1#
```

PuTTY の SSH セッションを終了してから続行します。

C. CUBE での Unified CM セキュア SIP トランクの設定

CUBE 証明書にエンタープライズ CA が署名し、CA が署名した証明書を CUBE が信頼できるようになると、Unified CM システムで必要な設定を完了して、CUBE との暗号化されたセキュアな統合が可能になります。このセクションでは、最初に CUBE 用にセキュア SIP トランクのセキュリティ プロファイルを設定し、そのプロファイルを CUBE の既存の SIP トランクに割り当てます。

10. Unified CM と CUBE トランク セキュリティ プロファイル間のトランク用に、セキュアな暗号化 SIP トランク プロファイルを設定する

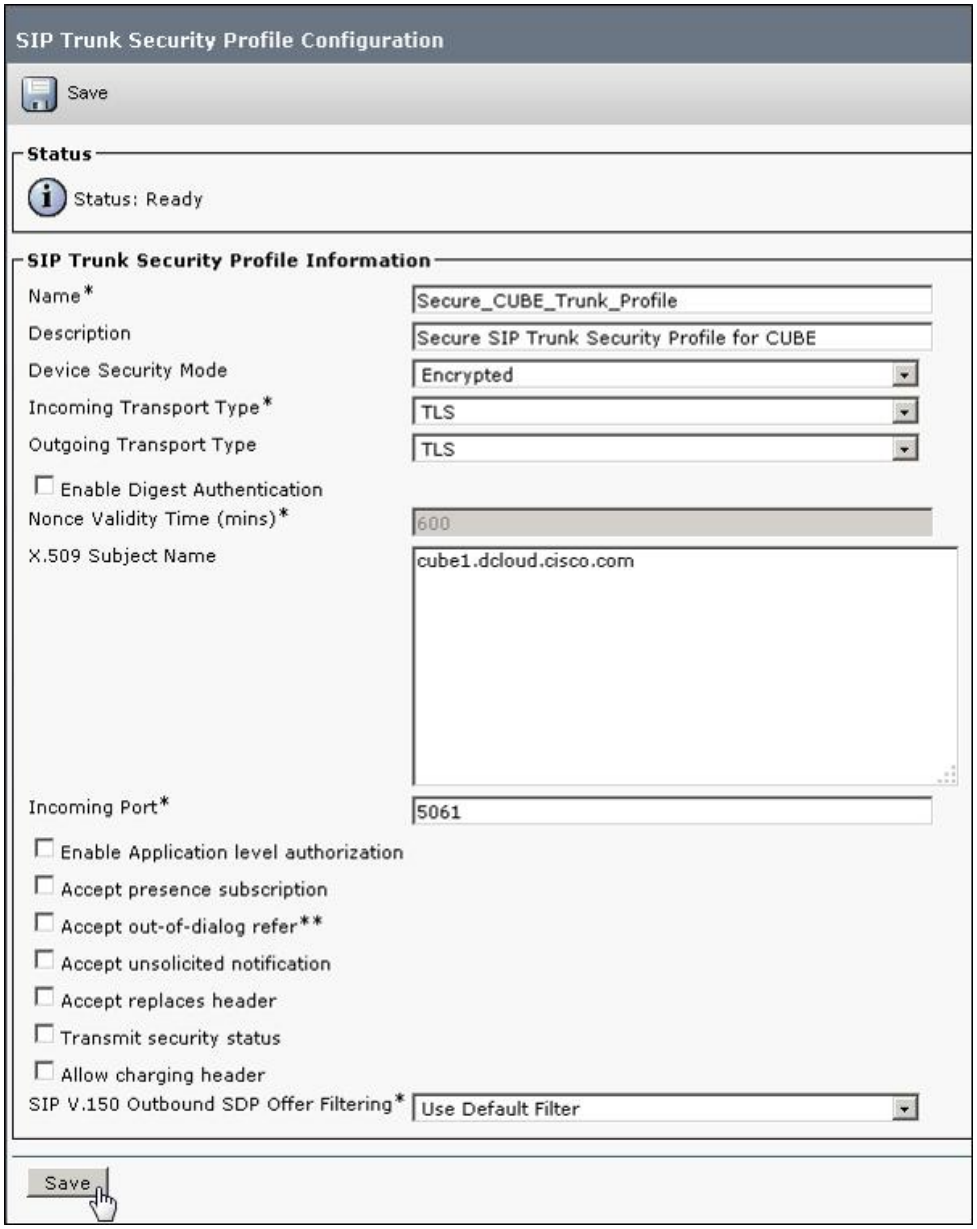
    WKST2（198.18.133.37）で Firefox Web ブラウザを使用して、Unified CM Administrative インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin）に移動し、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

    [システム（System）] > [セキュリティ（Security）] > [SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]

    を選択します。[新規追加（Add New）] をクリックし、新規プロファイルを作成します。

    図 165 に示すように、[名前（Name）] フィールドに「**Secure_CUBE_Trunk_Profile**」と入力し、[説明（Description）] フィールドに「**Secure SIP Trunk Security Profile for CUBE**」と入力して、[端末セキュリティモード（Device Security Mode）] ドロップダウンから [暗号化（Encrypted）] を選択します。[着信トランスポートタイプ（Incoming Transport Type）]、[発信トランスポートタイプ（Outgoing Transport Type）]、[着信ポート（Incoming Port）] の各フィールドが、それぞれ [TLS]、[TLS]、[5061] に自動的に更新されます。[X.509 サブジェクト名（X.509 Subject Name）] に、CUBE 証明書で使用している共通名（CN）「**cube1.dcloud.cisco.com**」を入力します。[保存（Save）] をクリックすると新規プロファイルが作成されます。

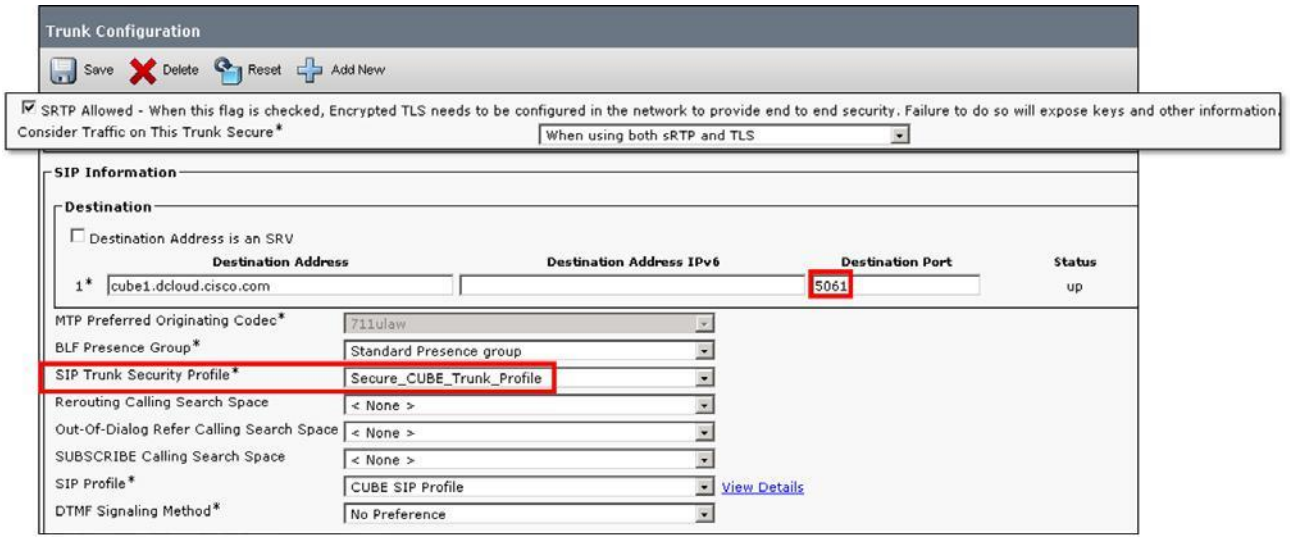
図 165. CUBE SIP トランク用の Unified CM 暗号化 SIP トランク セキュリティ プロファイル



11. 暗号化 SIP トランク プロファイルを CUBE 宛の SIP トランクに適用する

次に、新しく暗号化されたこの SIP トランク セキュリティ プロファイルを適用して、CUBE 宛の既存の SIP トランクを保護します。Unified CM（ucm1.dcloud.cisco.com）で [端末（Device）] > [トランク（Trunk）] に移動し、[検索（Find）] をクリックします。CUBE 用の SIP トランク **cube1_SIP_Trunk** を見つけます。トランク名をクリックすると、設定ページが表示されます。図 166 に示すように、[SRTP 許可（SRTP Allowed）] チェックボックスをオンにしてトランク設定を更新します。次に、[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）] ドロップダウンから、作成した SIP トランク セキュリティ プロファイル（**Secure_CUBE_Trunk_Profile**）を選択して、SIP トランク宛先ポートを **5061** に変更します。

図 166. Unified CM：CUBE 宛の SIP トランクの保護



をクリックします。続くダイアログで [OK] をクリックし、 

をクリックします。続くダイアログで [リセット（Reset）] をクリックして、トランクをリセットします。「リセット要求の送信に成功しました（Reset request was sent successfully）」というメッセージが表示されたら、[閉じる（Close）] をクリックします。

この SIP トランクがサービスに戻ったこと（約 1 分）を確認してから続行してください。

D. エンドポイントと CUBE 間の暗号化された通話の確認

次に、CUBE を通じてオンプレミスの Jabber クライアント間でテスト通話を行い、CUBE へのセキュアな統合を確認します。

12. CUBE を通じて発信し、暗号化によるセキュアな統合を確認する

    WKST2（198.18.133.37、**DCLOUD\aperez/C1sco12345**）で Jabber を起動します。WKST3（198.18.133.38、**DCLOUD\mcheng/C1sco12345**）に RDP 接続し、Jabber を起動します。

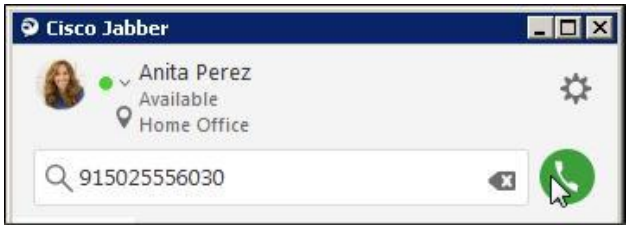
    Refresh Login Flow モジュール（モジュール 6）を使用して OAuth を完了している場合は、ボイスメール クレデンシャルが無効であることを示す [クレデンシャルの更新（Update Credentials）] ウィンドウが表示される場合があります。これは、OAuth が Jabber ログイン フローで使用されているためです。図 167 に示すように、この問題は無視して、そのまま [キャンセル（Cancel）] をクリックします。この問題には、証明書の問題を解決した時点で対応します（図 167 の下の注を参照）。

図 167. Jabber：ボイスメール クレデンシャル無効の警告

注: 両方の Jabber クライアントで、「cuc1.dcloud.cisco.com への接続時に証明書 cuc1.dcloud.cisco.com が無効であるため拒否されました(An invalid certificate cuc1.dcloud.cisco.com when connecting to cuc1.dcloud.cisco.com has been rejected…)」という警告が表示されます。この警告メッセージが表示されるのは、ラボの Unity Connection ボイスメール サービス ノードから受信した証明書がデフォルトの自己署名証明書で、ラボのワークステーションのローカル信頼ストアに存在しないためです。[拒否(Decline)] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。両方の Jabber クライアントについてエラー メッセージが表示され、ビジュアル ボイスメール サービスは接続されません。これらのメッセージは、証明書が無効であるために Unity Connection サーバ(cuc1.dcloud.cisco.com)との接続が拒否されたことを示します。このメッセージは、後でこのラボ(モジュール 8:次世代暗号化によるセキュアなボイスメール)で Enterprise CA を使用して Unity Connection サーバ証明書に署名すると表示されなくなり、クライアントがボイスメール システムに自動的に接続されます。

両方のクライアントが登録されたら、Anita Perez の Jabber クライアント(WKST2)で 915025556030 にダイヤルし、[発信(Call)] をクリックして、CUBE を通じて Monica Cheng の Jabber クライアント(WKST3)に発信します(図 168 を参照)。

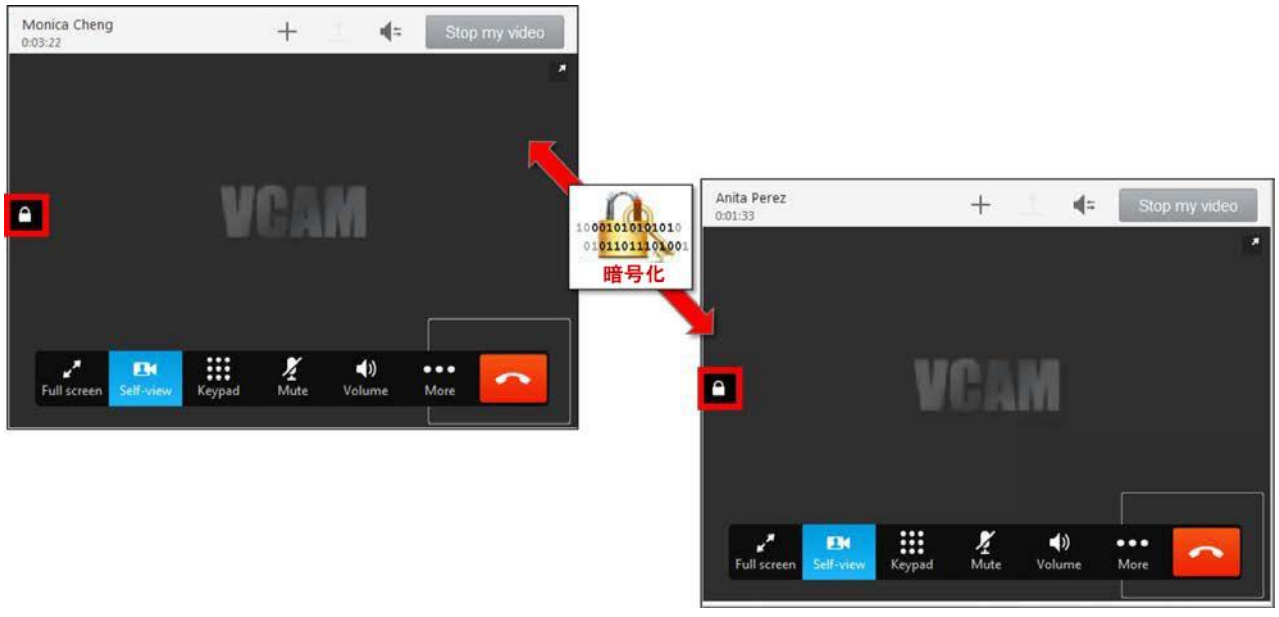
図 168. CUBE を通じた発信



この通話は、91 プレフィックスによって CUBE にルーティングされます。CUBE は数字を 915025556030 から 4085556030 に変換してから Unified CM にルーティングします。その場合、プレフィックス +1 が追加されて、+14085556030 の Monica Cheng に発信されます。

Monica Cheng の Jabber クライアントで着信通話に応答します。図 169 に示すように、通話が接続されると、ロック アイコンが表示されます。これは、メディアが暗号化されただけでなく、Unified CM と CUBE 間のシグナリング パスも暗号化されたことを示します。

図 169. CUBE を通じたセキュアな暗号化通話



cube1 のコマンド ラインで次のコマンドを実行して、通話が暗号化されていることを確認することもできます。

```
show sip-ua calls

show sip-ua connections tcp tls details

show sip-ua srtp
```

続行する前に、通話を終了し、すべての Jabber Windows クライアントを終了して、開いている SSH セッションまたはブラウザ セッションを閉じます。

***** モジュール #7 の終了 *****

モジュール 8. 次世代暗号化によるセキュアなボイスメール

モジュールの概要

このモジュールでは、Unified CM と Unity Connection ボイスメール システム間でセキュアな統合を確立します。最初に予備ボイスメール通話を行い、暗号化されていない通話でのボイスメールの動作を確認します。次に Unity Connection 証明書と、Unity Connection tomcat 証明書の CA 署名を調査します。その後で、Unified CM SIP トランクで Unity Connection の暗号化を有効にし、Unity Connection で必要な設定変更を行い、Unified CM と Unity Connection 間、およびエンドポイントと Unity Connection 間で、エンドツーエンドの暗号化を可能にします。最後に、ボイスメールのテスト通話を行い、Unity Connection との暗号化された統合を確認します。このモジュールは、次の 6 つのセクションに分割されています。

A. ボイスメールの動作を確認するボイスメールのテスト通話

B. Unity Connection ライセンスを確認して暗号化を有効化

C. Unity Connection 証明書管理

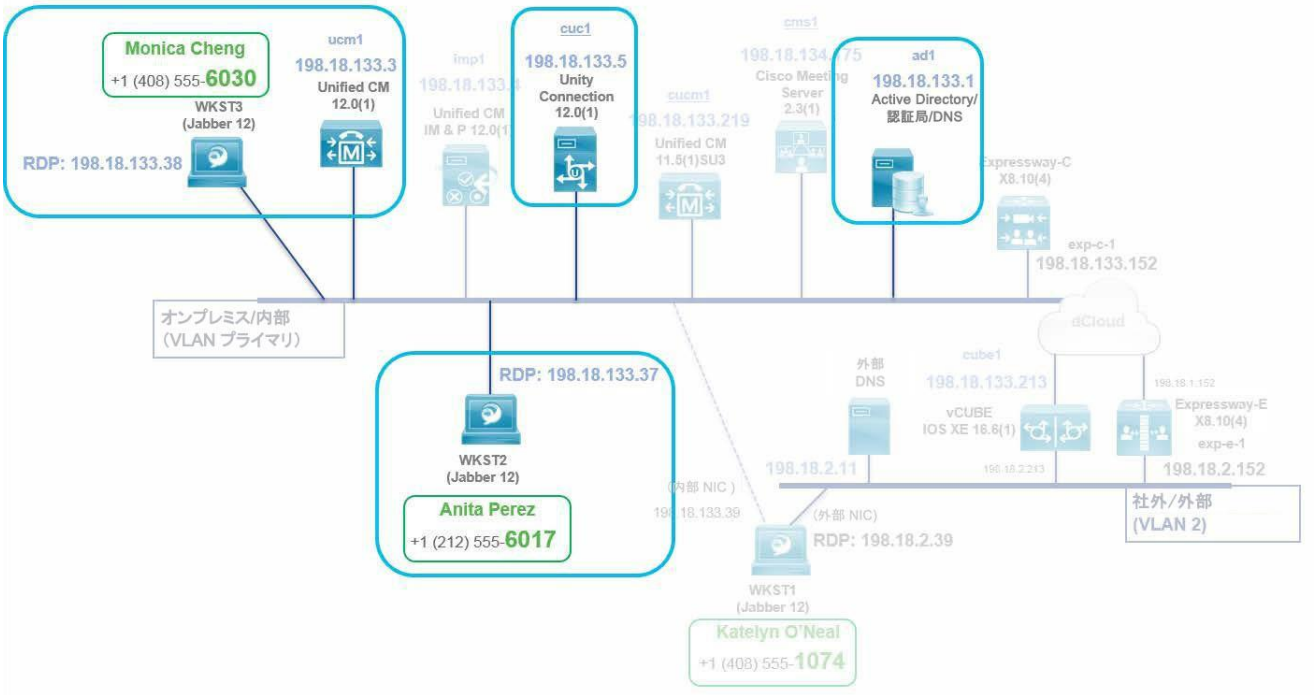
D. Unity Connection のための Unified CM セキュア SIP トランク設定

E. Unity Connection テレフォニー統合の暗号化

F. エンドポイントとボイスメール システム間の暗号化された通話の確認

次の図 170 は、このモジュールのトポロジおよび関連するコンポーネントを示しています。

図 170. モジュール 8：次世代暗号化トポロジによるセキュアなボイスメール



手順

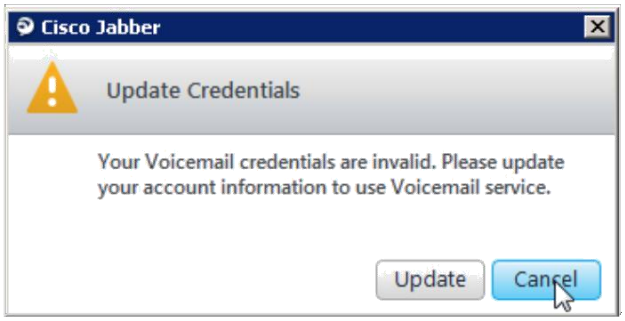
A. ボイスメールの動作を確認するボイスメールのテスト通話

1. 発信して、Unity Connection ボイスメール システムに通話が転送されるようにする

   WKST2（198.18.133.37、**DCLOUD\aperez/C1sco12345**）に RDP 接続し、Jabber を起動します。クライアントは自動的にログインします。WKST3（198.18.133.38、**DCLOUD\mcheng/C1sco12345**）に RDP 接続し、Jabber を起動します。クライアントは自動的にログインします。

   「OAuth2 での更新ログイン フロー」モジュール（モジュール 6）を完了している場合は、ボイスメール クレデンシャルが無効であることを示す [クレデンシャルの更新（Update Credentials）] ウィンドウが表示される場合があります。これは、OAuth が Jabber ログイン フローで使用されているためです。図 171 に示すように、この問題は無視して、そのまま [キャンセル（Cancel）] をクリックします。この問題には、証明書の問題を解決した時点で対応します（see the note below 図 171 の下の注を参照）。

   図 171. Jabber：ボイスメール クレデンシャル無効の警告

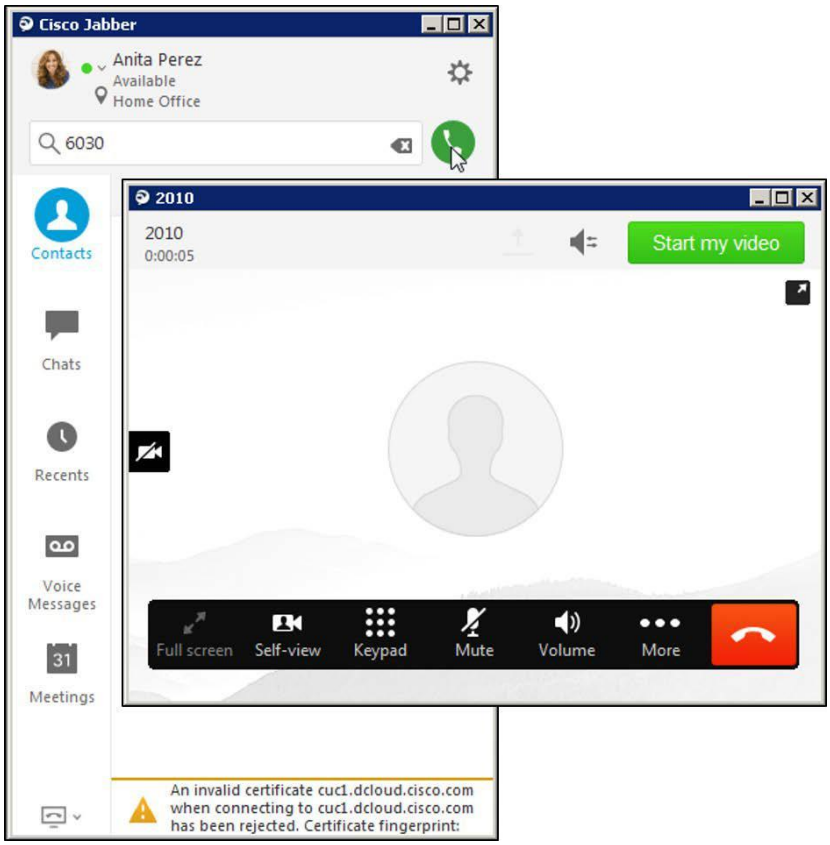
   

   注：両方の Jabber クライアントで、「cuc1.dcloud.cisco.com への接続時に証明書 cuc1.dcloud.cisco.com が無効であるため拒否されました（An invalid certificate cuc1.dcloud.cisco.com when connecting to cuc1.dcloud.cisco.com has been rejected…）」という警告が表示されます。この警告メッセージが表示されるのは、ラボの Unity Connection ボイスメール サービス ノードから受信した証明書がデフォルトの自己署名証明書で、ラボのワークステーションのローカル信頼ストアに存在しないためです。[拒否（Decline）] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。両方の Jabber クライアントについてエラー メッセージが表示され、ビジュアル ボイスメール サービスは接続されません。これらのメッセージは、証明書が無効であるために Unity Connection サーバ（cuc1.dcloud.cisco.com）との接続が拒否されたことを示します。このメッセージは、後でこのラボで Enterprise CA を使用して Unity Connection サーバ証明書に署名すると表示されなくなり、クライアントがボイスメール システムに自動的に接続されます。

   両方のクライアントが登録されたら、Anita Perez の Jabber クライアント（WKST2）で **6030** にダイヤルし、[発信（Call）] をクリックして、Monica Cheng の Jabber クライアント（WKST3）に発信します（図 168 を参照）。Monica Cheng の Jabber クライアントでは着信通話に応答しないでください。代わりに、通話がボイスメールに転送されるようにします。着信通話ダイアログで [拒否（Decline）] をクリックして、通話をボイスメールにただちにプッシュします。ここでは、無応答通話後に発信者がメッセージを残すところをモデリングしています。

   ボイスメール システムに通話が接続されると、Unity Connection ボイスメール システムに（Anita のクライアントから）リダイレクトされた通話が、暗号化されていないことがわかります。これは、通話ウィンドウにロック アイコンが表示されていないことで確認できます。Monica のボイスメール ボックスにメッセージを残す必要はないため、通話がボイスメール パイロット（2010）に接続され、暗号化されていないことを確認したら（図 172 を参照）、Anita の Jabber クライアントでそのまま通話を終了します。

図 172. Unity Connection：通話が無応答であるか拒否/無視された場合にボイスメールに転送

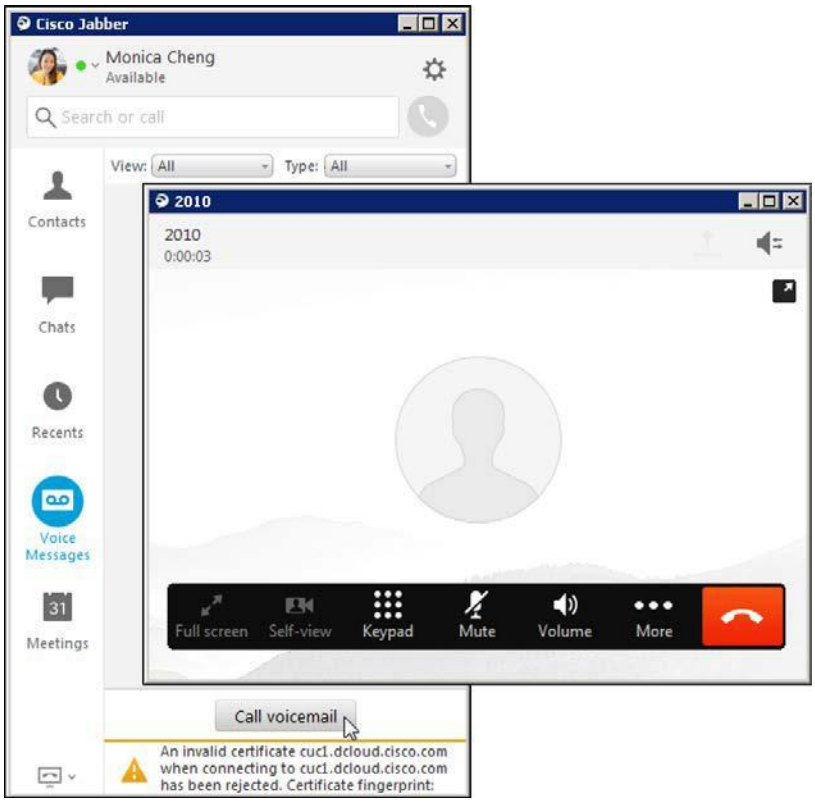


2. [ボイスメールに発信（Call Voicemail）] ボタンで Unity Connection ボイスメール システムに直接発信する

   Monica Cheng の Jabber クライアント（WKST3）から、[ボイスメール（Voicemail）] タブで [ボイスメールに発信（Call Voicemail）] ボタンをクリックして（または手動でボイスメール システムのパイロット番号：2010 にダイヤルして）、ボイスメール システムに発信します。ここでは、メッセージ待機通知の表示後に発信者がメッセージを取得するところをモデリングしています。

   通話がボイスメール パイロット（2010）に接続され、図 173 に示すように、通話が暗号化されていない（ロック アイコンがない）ことを確認します。

図 173. Unity Connection：ボイスメール システムからメッセージを取得



Monica Cheng の Jabber クライアントで、Unity Connection との通話を終了またはハングアップします。

続行する前に、WKST2 および WKST3 で Cisco Jabber クライアントをクローズ/終了します。

B. Unity Connection ライセンスを確認して暗号化を有効化

次に、システムがライセンスを取得していることを確認し、CLI を通じて暗号化を有効にします。

3. システムが適切にライセンスを取得していて、エクスポート コンプライアンスが有効であることを確認する

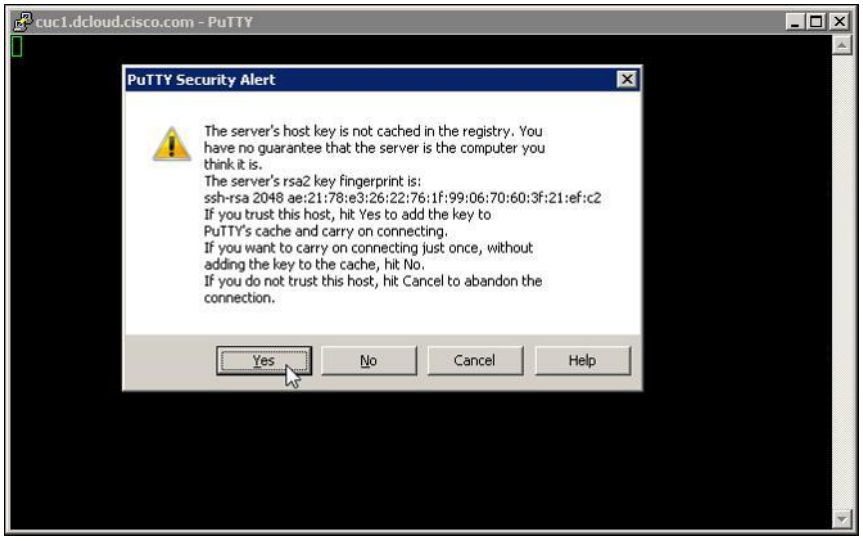
   WKST2（198.18.133.37）で PuTTY を使用して、Unity Connection（cuc1.dcloud.cisco.com）コマンド ライン インターフェイスに **SSH** 接続します。

   PuTTY アイコン 

をダブルクリックして起動します。**cuc1** プロファイル エントリを選択するか、[ホスト名（Host Name）] フィールド（または [IP アドレス（IP Address）] フィールド）に「**cuc1.dcloud.cisco.com**」と入力します。[開く（Open）] をクリックします。

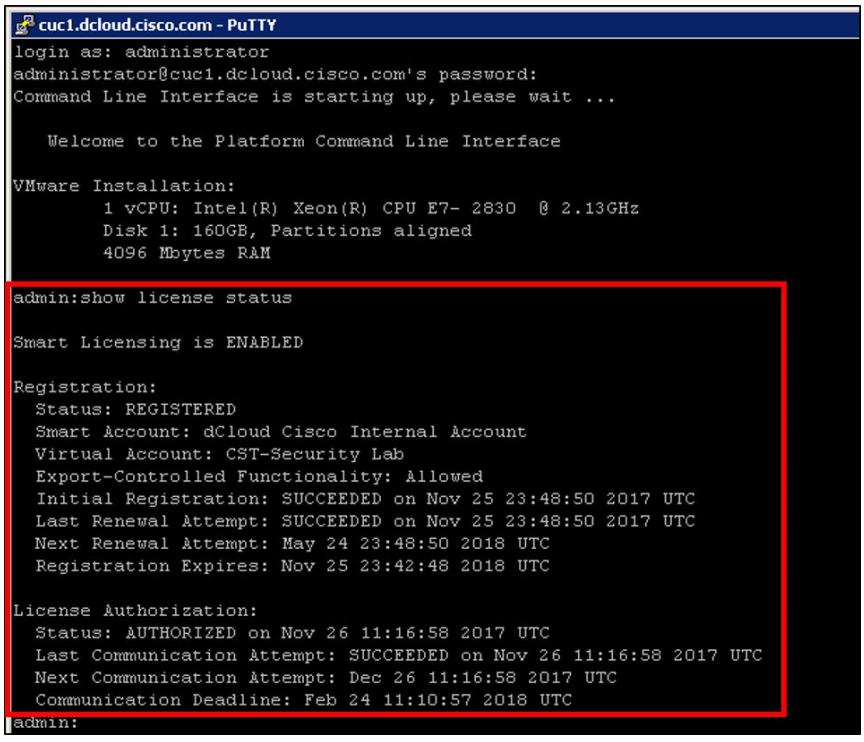
   図 174 に示すように [PuTTY セキュリティアラート（PuTTY Security Alert）] ウィンドウが表示されたら、[はい（Yes）] をクリックして ssh-rsa2 キーをキャッシュします。

図 174. Unity Connection との SSH 接続のためのキーのキャッシュ確認



ユーザ名/パスワード：**administrator/dCloud123!** でログインしたら、コマンド ラインに **show license status** コマンドを入力します（図 175 を参照）。スマート ライセンスがシステムで [有効（Enabled）] で [登録済み（Registered）] であり、ライセンスが [認可済み（Authorized）] であることがわかります。さらに輸出管理機能が [許可（Allowed）] され、システムで暗号化が可能であることを確認できます。

図 175. Unity Connection ライセンスと輸出管理機能のステータス



4. Unity Connection システムで暗号化が有効であることを確認する

暗号化されたボイス メッセージングと、Unity Connection と Unified CM 間のセキュアな統合を有効にするには、システムで暗号化が有効である必要があります。システムで暗号化が有効であることを確認しましょう。スマート ライセンス モジュール（モジュール 2）で有効にしているため、暗号化は有効であるはずです。

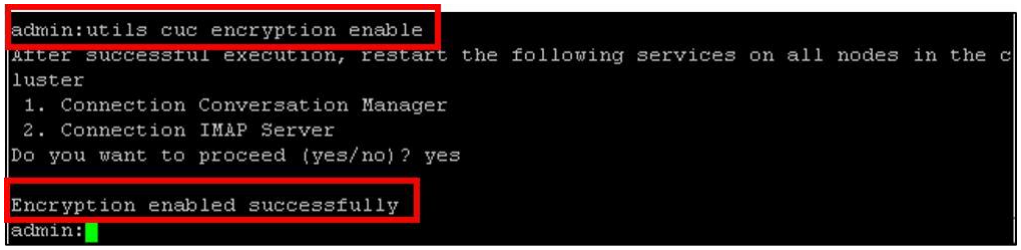
SSH セッション ウィンドウで、コマンド ラインに **utils cuc encryption status** コマンドを入力して、システムの暗号化を確認します（図 176 を参照）。

図 176. Unity Connection：システムで暗号化が有効であることを確認

システムがライセンスされ、暗号化が有効であることを確認したので、「exit」と入力して SSH セッションを終了し、Unity Connection に戻ります。

スマート ライセンス モジュール（モジュール 2、図 80、59 ページ）で Unity Connection での暗号化を有効にしたときに、Connection Conversation Manager と Connection IMAP Server サービスの再起動が必要であると表示されました（図 177 を参照）。

図 177. Unity Connection で暗号化を有効化（モジュール 2）



この時点までは、Unity Connection 用にセキュアな統合を設定していなかったため、サービスの再起動は不要でした。これからは Unified CM と Unity Connection の統合で次世代の暗号化を有効にするため、これらのサービスを再起動する必要があります。

WKST2 の Firefox ブラウザで、[Unity Connection サービスアビリティ（Unity Connection Serviceability）] インターフェイス（https://cuc1.dcloud.cisco.com/cuservice）にアクセスします。必要に応じて、証明書警告をバイパスします（[リスクを理解しました（I Understand the Risks）] をクリックし、[例外の追加（Add Exception…）] ボタンをクリックし、[この例外を永久に保存（Permanently store this exception）] をオフにして、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）。ユーザ名/パスワード：**administrator/dCloud123!** を使用してログインします。

[Unity Connection サービスアビリティ（Unity Connection Serviceability）] インターフェイスにログインしたら、[ツール（Tools）] > [サービス管理（Service Management）] を選択します。Connection Conversation Manager サービス（[重要なサービス（Critical Services）] の下）で、[停止（Stop）] ボタンをクリックします。続くダイアログで [OK] をクリックして確定します。[サービス停止が成功しました（Stop service succeeded）] というメッセージが表示されたら、[開始（Start）] ボタンを押してサービスを再起動します。

次に下方向にスクロールして Connection IMAP Server サービス（[オプションサービス（Options Services）] の下）を見つけ、[停止（Stop）] ボタンをクリックします。[サービス停止が成功しました（Stop service succeeded）] というメッセージが表示されたら、下方向にスクロールして Connection IMAP Server の横の [開始（Start）] ボタンをクリックして、サービスを再起動します。

C. Unity Connection 証明書の調査と管理

デフォルトでは、Unity Connection tomcat 証明書は自己署名されます。シスコの他のアプリケーション サーバ（Unified CM や Unified CM IM & P）と同様に、デフォルトの自己署名証明書を使用するのではなく、認証局（CA）が署名した証明書をシステムにインストールすることをお勧めします。パブリック CA または民間のエンタープライズ CA によって、Unity Connection tomcat 証明書に署名する必要があります。

前述のように、CA 署名付き証明書を使用すれば、1 つの CA 証明書をエンドユーザのワークステーションにインストールして管理できるため、複数のサービスが使用する複数の証明書をインストールするよりも、管理が大幅に容易になります。その他の場合は、Cisco Jabber ワークステーションで、Unified CM、IM & Presence、Unity Connection（ビジュアル ボイスメール用 HTTPS 接続）用に、tomcat 証明書を別個にインストールする必要があります。Unity Connection tomcat 証明書は、サーバの Web インターフェイスで使用するだけでなく、エンドユーザが Cisco Personal Communications Assistant に接続している場合や、Unified CM と Unity Connection 間の SIP トランク経由による SIP 通信（暗号化を有効にした場合）にも使用します。

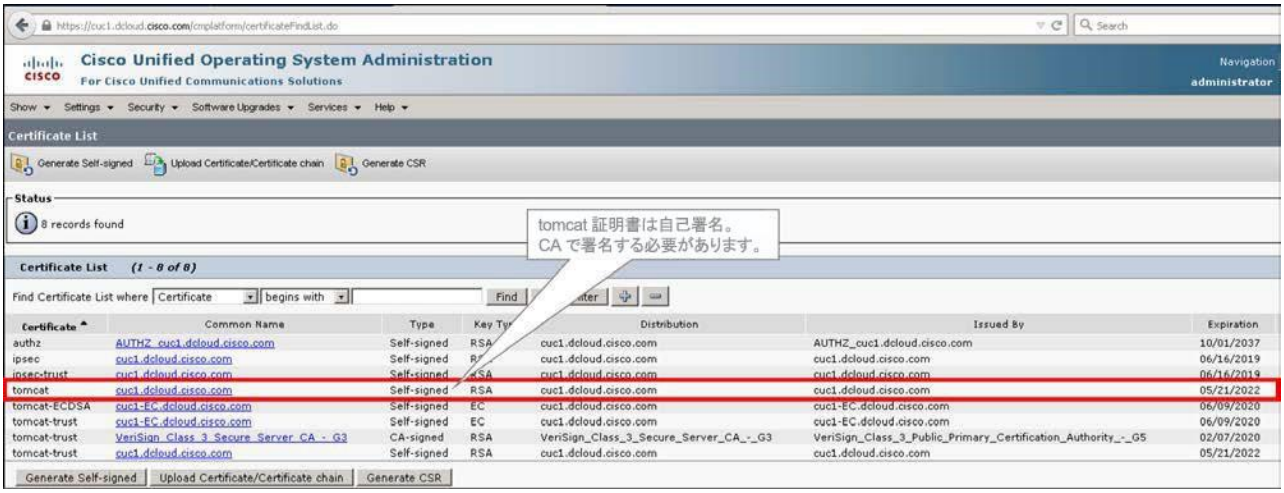
5. Unity Connection システム証明書を確認し、証明書署名要求（CSR）を生成する

   まだ接続していない場合は、WKST2（198.18.133.37、ユーザ名/パスワード：**DCLOUD\aperez/C1sco12345**）に RDP 接続します。Firefox Web ブラウザを使用して、Unity Connection で Cisco Unified Operation System 管理インターフェイス（https://cuc1.dcloud.cisco.com/cmplatform）に移動します。プロンプトが表示されたら、証明書警告をバイパスします（[リスクを理解しました（I Understand the Risks）] をクリックし、[例外の追加（Add Exception…）] ボタンをクリックし、[この例外を永久に保存（Permanently store this exception）] をオフにして、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）。ユーザ名/パスワード：**administrator/dCloud123!** を使用してログインします。

   Unity Connection Operating System 管理インターフェイスにログインしたら、[セキュリティ（Security） > [証明書の管理（Certificate Management）] を選択します。[検索（Find）] をクリックします。

   図 178 に、Unity Connection OS 証明書管理インターフェイスと、システム証明書のリストを示します。

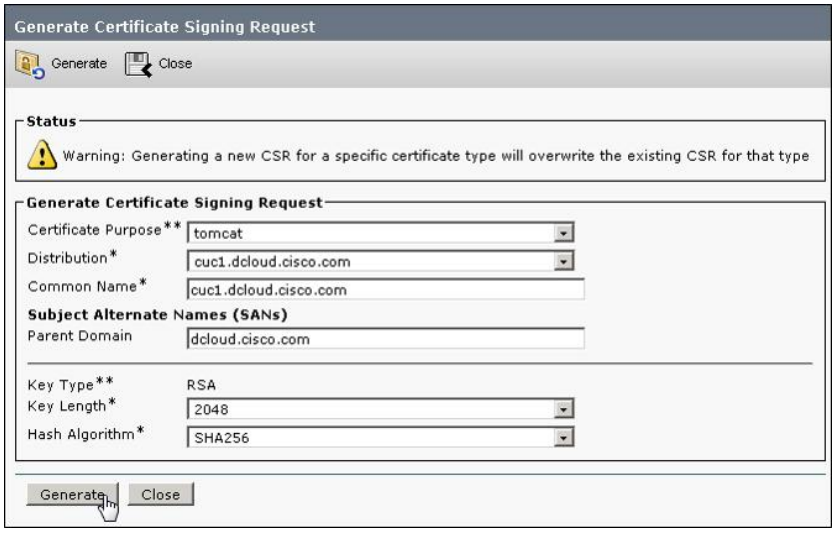
図 178. Unity Connection 証明書のリスト



[CSR の生成（Generate CSR）] ボタンを再度クリックして CA 署名プロセスを開始し、必要に応じて [証明書の用途（Certificate Purpose）] ドロップダウンから [tomcat]（デフォルト値）を選択します。その他の値はすべてデフォルトのままにし、キー長とハッシュアルゴリズムが、図 179 に示すようにそれぞれ 2048 と SHA256 に設定されていることを確認します。[生成（Generate）] をクリックします。

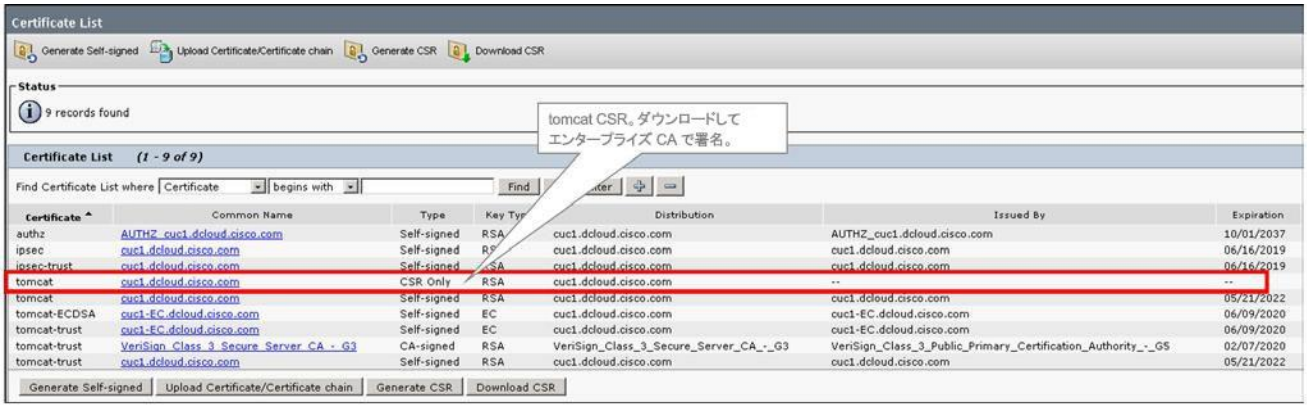
注：Unity Connection クラスタ内にはノードが 1 つしかないため、マルチサーバ SAN は [配布（Distribution）] フィールドでは使用できません。複数ノードの Unity Connection クラスタでは、マルチサーバ SAN CSR を生成して、サーバ証明書の管理を自動化してシンプルにすることもできます。

図 179. Unity Connection tomcat CSR の生成



CSR が作成されたら、[閉じる（Close）] をクリックします。証明書リストがリロードされたら、生成した tomcat CSR を確認します（図 180 を参照）。

図 180. Unity Connection tomcat CSR



注：証明書リストをリロードするには、必要に応じて [検索（Find）] をクリックします。

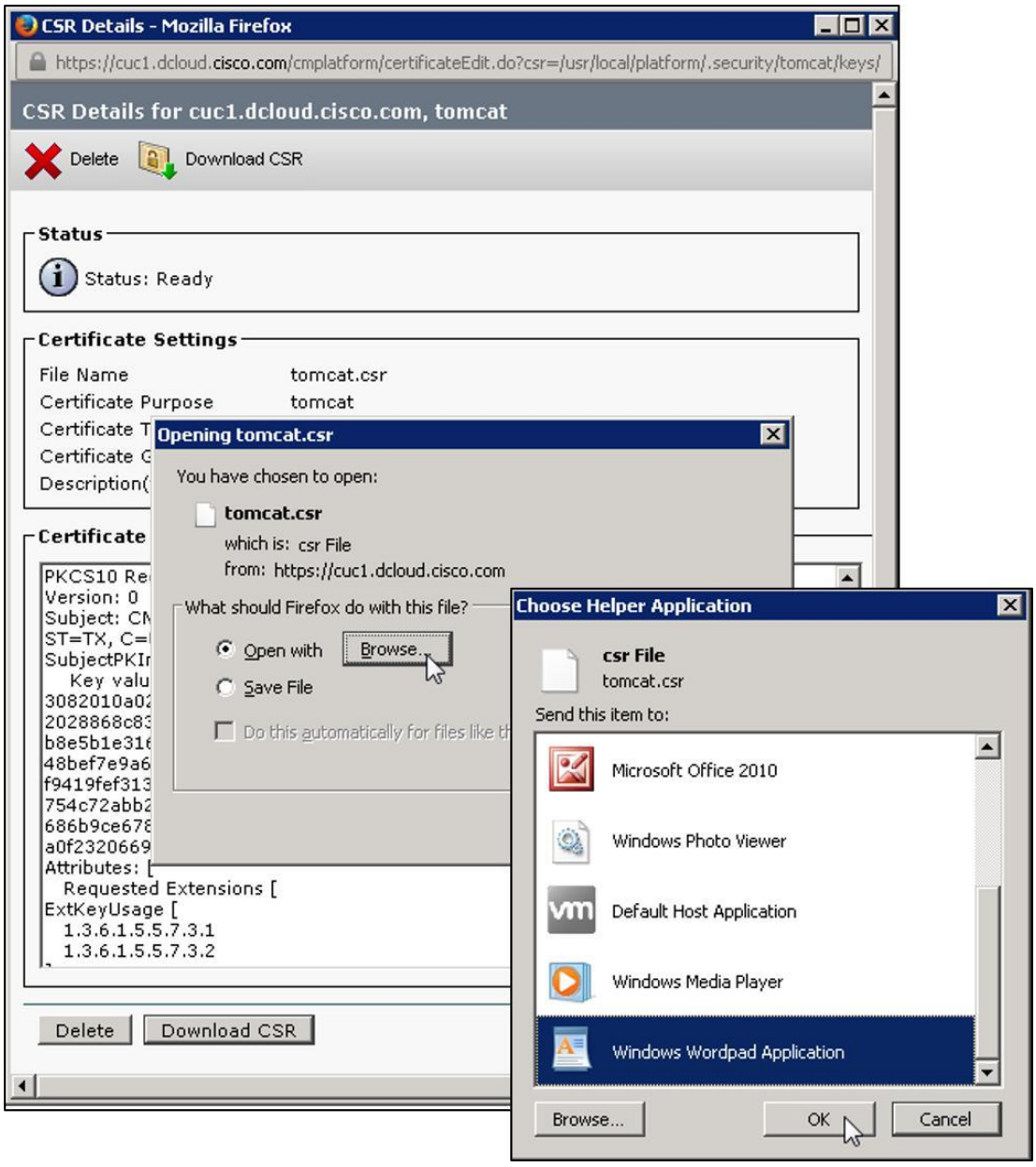
CSR をクリックして CSR をダウンロードし、[CSR のダウンロード（Download CSR）] をクリックします（図 181 を参照）。

図 181. Unity Connection tomcat CSR をダウンロード*

上の図の証明書ファイルの日付は、実際のシステムと異なる場合があります。

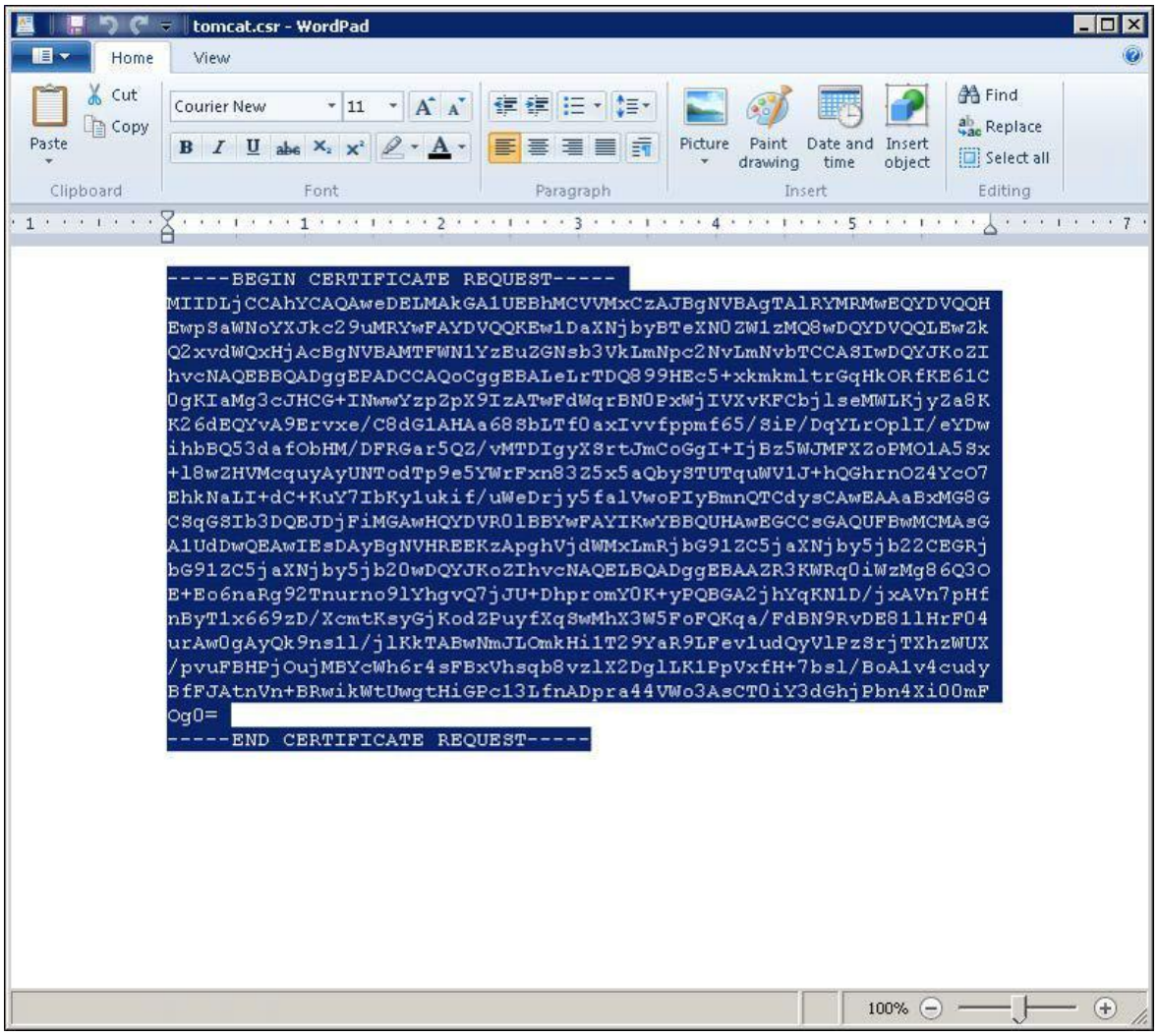
[プログラムから開く(Open with)]/[ファイルの保存(Save File)] ダイアログで、[プログラムから開く(Open with)] を選択します。[参照(Browse)] をクリックします。ワードパッド アプリケーション(またはメモ帳)を選択します。図 182 を参照してください。

図 182. tomcat CSR を開いてコピーする



[OK] をクリックしてワードパッドを選択します。[OK] を再度クリックしてファイルを開きます。ファイルが開いたら、ファイルの内容を選択してクリップボードにコピー（Ctrl+C）します。図 183 を参照してください。

図 183. CSR テキストのコピー*



上の図の証明書署名要求文字列は、実際の CSR と異なる場合があります。

[CSR の詳細（CSR Details）] ウィンドウを閉じます。

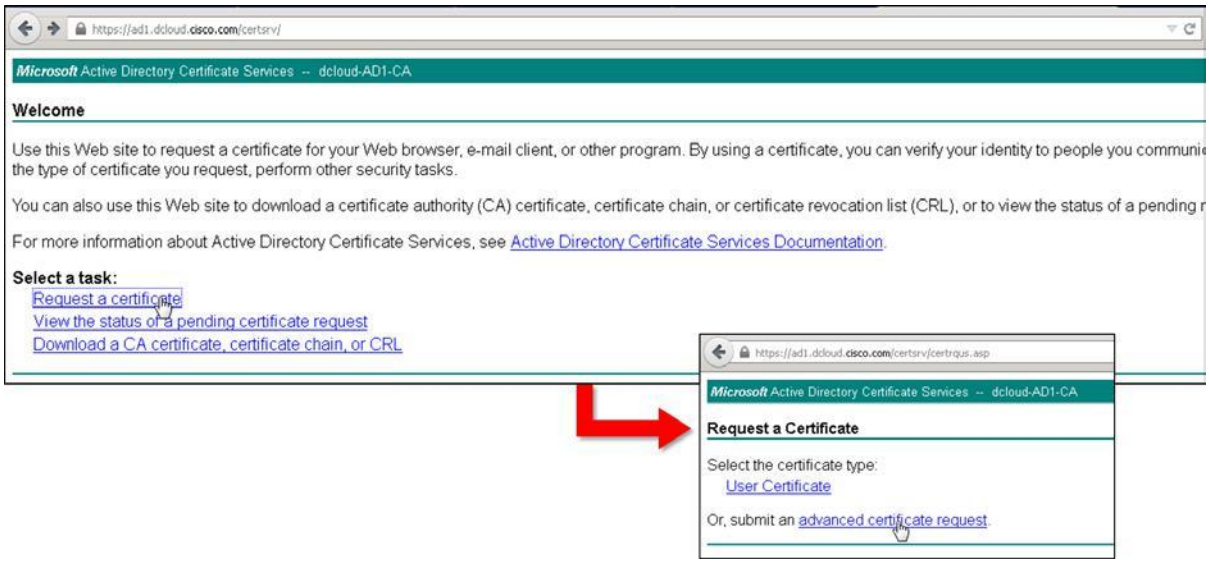
6. Unity Connection 用に、認証局（CA）が署名した tomcat 証明書を要求して取得する

   次に、エンタープライズ CA（ad1.dcloud.cisco.com）を使用して、Unity Connection tomcat サービス用に CA 署名付き証明書を生成します。

   WKST2（198.18.133.37）で Firefox Web ブラウザを使用して、https://ad1.dcloud.cisco.com/certsrv に移動します。認証を求められたら、ユーザ名/パスワード：**administrator/C1sco12345** を使用してログインします。

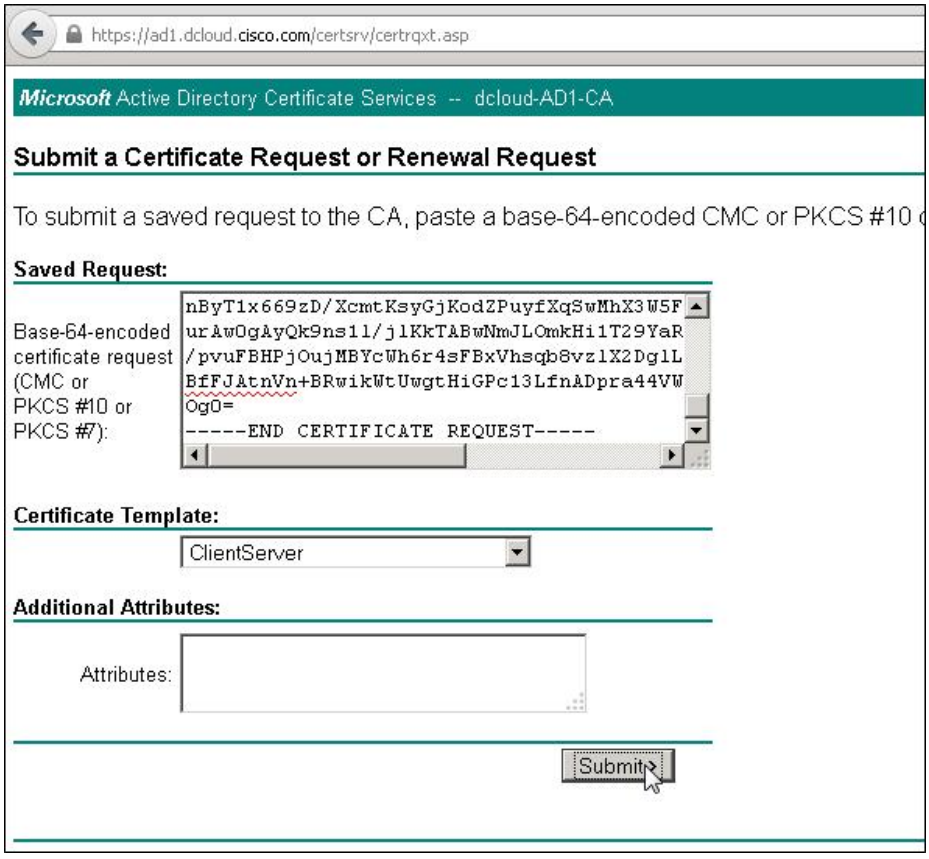
   [証明書を要求する（Request a certificate）] をクリックします。次に [または詳細証明書要求を送信する（Or, submit an advanced certificate request）] をクリックします（図 184 を参照）。

図 184. エンタープライズ CA で署名付き証明書を要求



（前の手順で CSR からコピーした）クリップボードの内容を、[Base-64 でエンコードされた証明書要求（Base-64-encoded certificate request）] フィールドに貼り付けます（Ctrl+V）。図 185 に示すように、**ClientServer** 証明書テンプレートを選択して [送信 >（Submit >）] をクリックします。

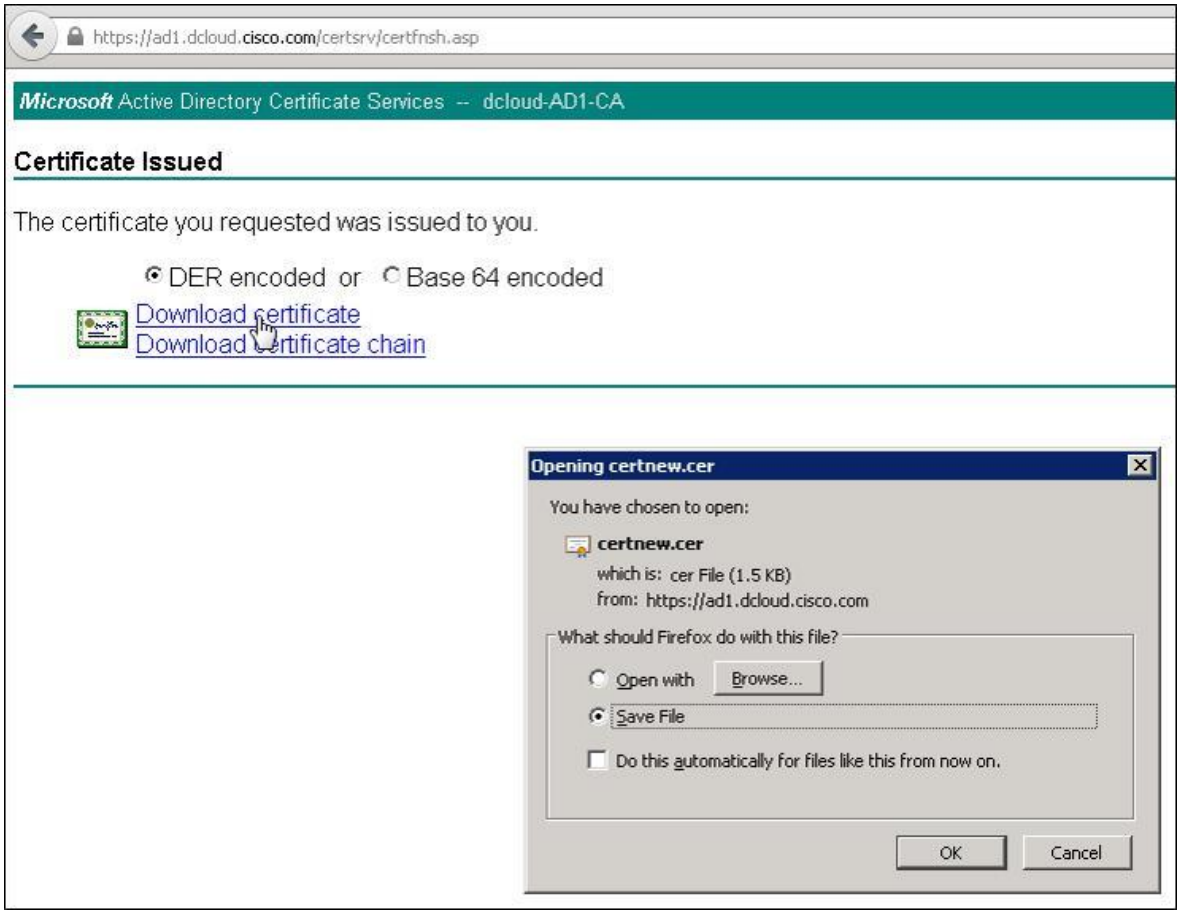
図 185. Unity Connection tomcat 証明書要求を送信*



**** 上の図の証明書署名要求文字列は、実際の CSR と異なる場合があります。***

次の画面で [DER でエンコード（DER encoded）]（デフォルト）または [Base 64 でエンコード（Base 64 encoded）] を選択し、[証明書をダウンロード（Download certificate）] をクリックします（図 186 を参照）。[ファイルの保存（Save File）] を選択して [OK] をクリックし、ファイルをローカル ワークステーションに保存します。ファイルに「**tomcat.cer**」という名前を付けます。

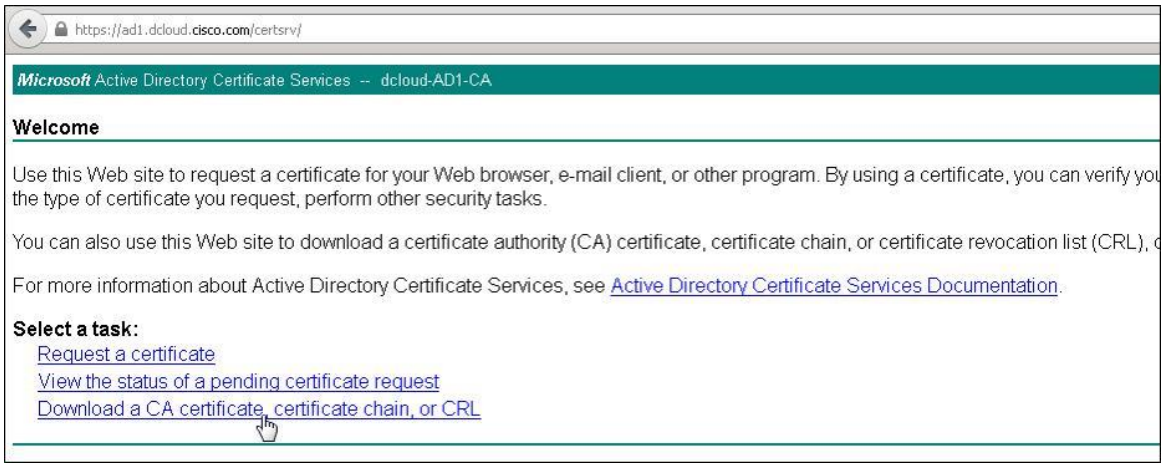
図 186. 署名付き Unity Connection tomcat 証明書を保存



7. エンタープライズ CA ルート証明書をダウンロードする

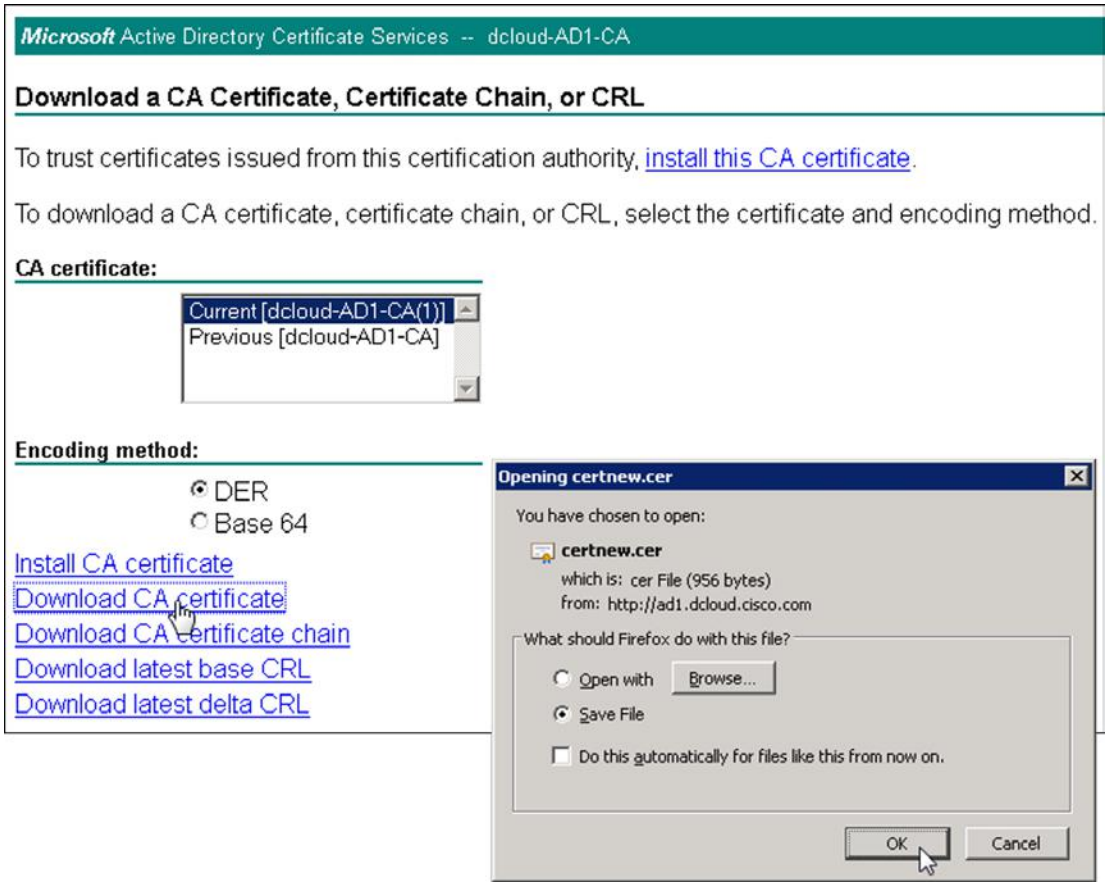
   エンタープライズ CA から離れる前に、CA ルート証明書をダウンロードします。https://ad1.dcloud.cisco.com/certsrv/ に戻り（右上隅の [ホーム（Home）] リンクをクリック）、[CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します（図 187 を参照）。

図 187. エンタープライズ CA ルート証明書のダウンロード（1/2）



次の画面では、[現在の[dcloud-AD1-CA]（Current [dcloud-AD1-CA]）] がデフォルトで選択されています。[CA 証明書のダウンロード（Download CA certificate）] をクリックします（図 188 を参照）。[ファイルの保存（Save File）] を選択して [OK] をクリックし、**dCloud_root.cer** としてローカル ワークステーションに保存します。

図 188. エンタープライズ CA ルート証明書のダウンロード（2/2）



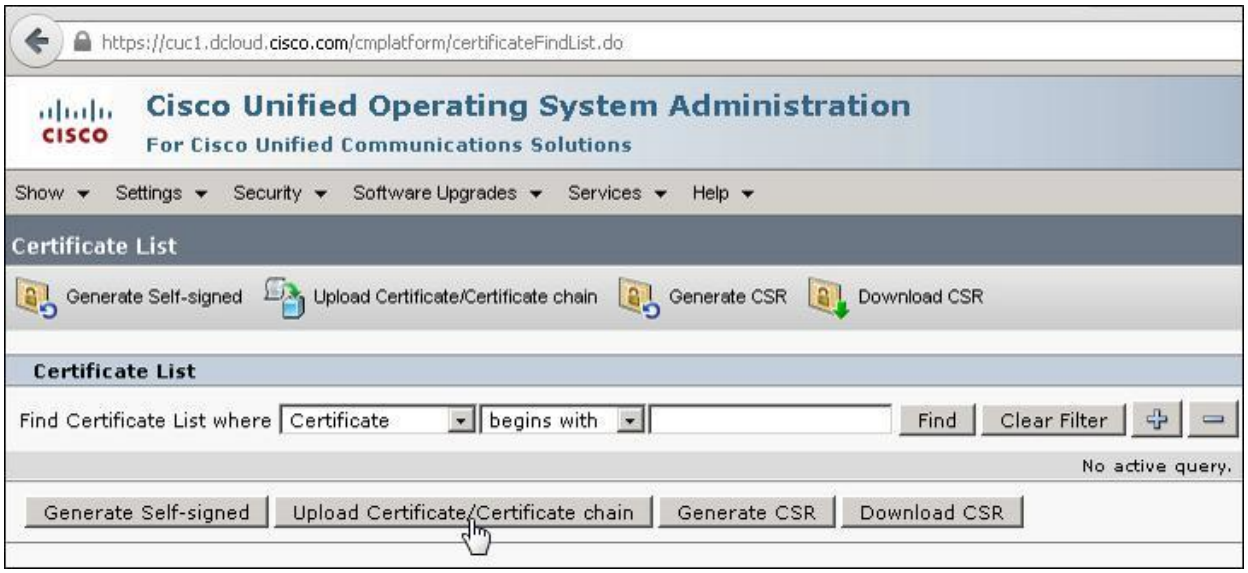
8. CA ルート証明書と CA 署名付き tomcat 証明書を Unity Connection Certificate Store にアップロード

   tomcat 証明書が発行され署名されたので、次にエンタープライズ CA ルート証明書と署名付き tomcat 証明書を Unity Connection にアップロードします。

Unity Connection Operating System 管理インターフェイス（https://cuc1.dcloud.cisco.com/cmplatform/）に戻り、必要に応じてユーザ名/パスワード：**administrator/dCloud123!** を使用してログインします。

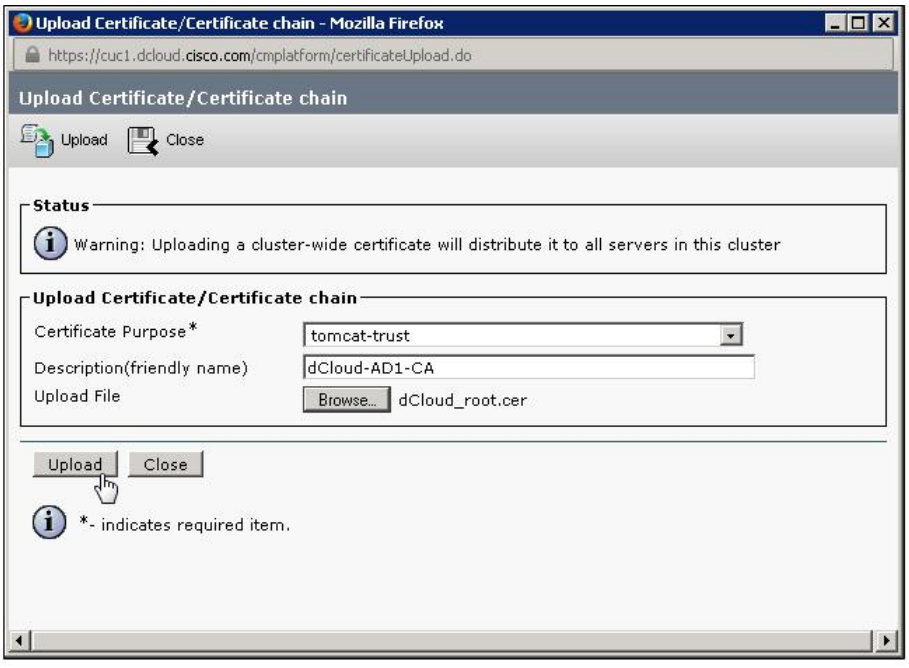
[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択し、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします（図 189 を参照）。

図 189. CA 署名付き tomcat 証明書と CA Root 証明書を Unity Connection にアップロード



最初にエンタープライズ CA ルート証明書を tomcat-trust ストアにアップロードします。[証明書の用途（Certificate Purpose）] ドロップダウンから [tomcat-trust] を選択し、[説明（Description）] フィールドに「**dCloud-AD1-CA**」と入力します。[参照（Browse）] をクリックして、保存してある証明書 **dCloud_root.cer**（C:\Users\aperez\Downloads）を選択します。[開く（Open）] をクリックします。最後に [アップロード（Upload）] をクリックします（図 190 を参照）。

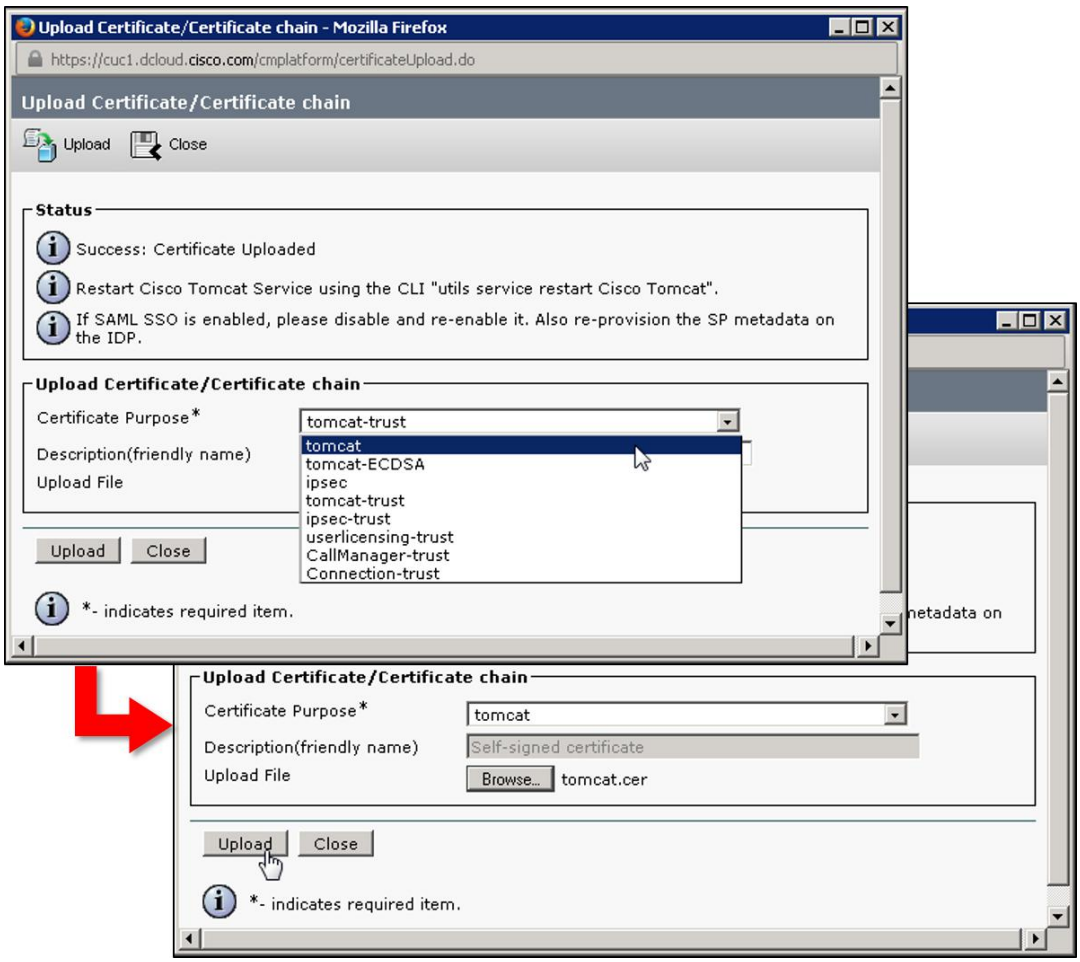
図 190. CA ルート証明書を Unity Connection tomcat-trust にアップロード



注：tomcat サービスの再起動は、このセクションの最後に行います。

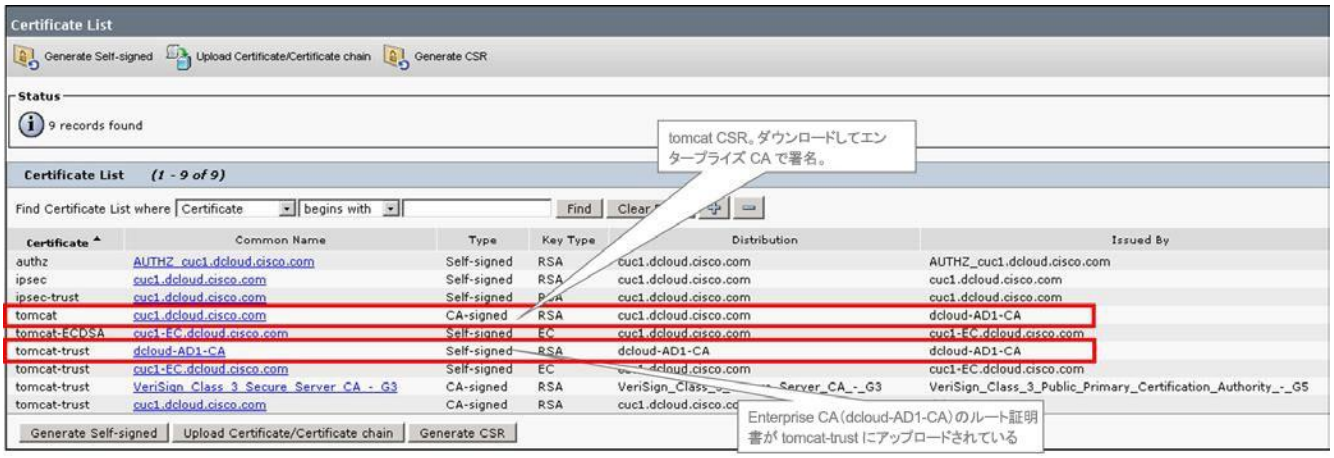
次に、CA 署名付き tomcat 証明書をアップロードします。[証明書の用途（Certificate Purpose）] ドロップダウンから [tomcat] を選択します。[参照（Browse）] をクリックして、保存してある証明書 **tomcat.cer**（C:\Users\aperez\Downloads）を選択します。[開く（Open）] をクリックします。[アップロード（Upload）] をクリックします（図 191 を参照）。

図 191. CA 署名付き tomcat 証明書のアップロード



[閉じる（Close）] をクリックします。[証明書リスト（Certificate List）] ページ（[セキュリティ（Security）] > [証明書の管理（Certificate Management）]）で [検索（Find）] をクリックすると、新しくアップロードされた CA ルート証明書と CA 署名付き tomcat 証明書が表示されます（図 192 を参照）。先ほど署名した CA 署名付き tomcat 証明書が、tomcat-trust ストアでエンタープライズ CA ルート証明書とともにリストされていることを確認します。また、新しい CA 署名付き tomcat 証明書が、tomcat-trust ストアに自動的にインポートされていることを確認します。

図 192. Unity Connection にアップロードされた CA 署名付き tomcat 証明書と CA ルート証明書



9. Unity Connection で Cisco Tomcat Service を再起動します。

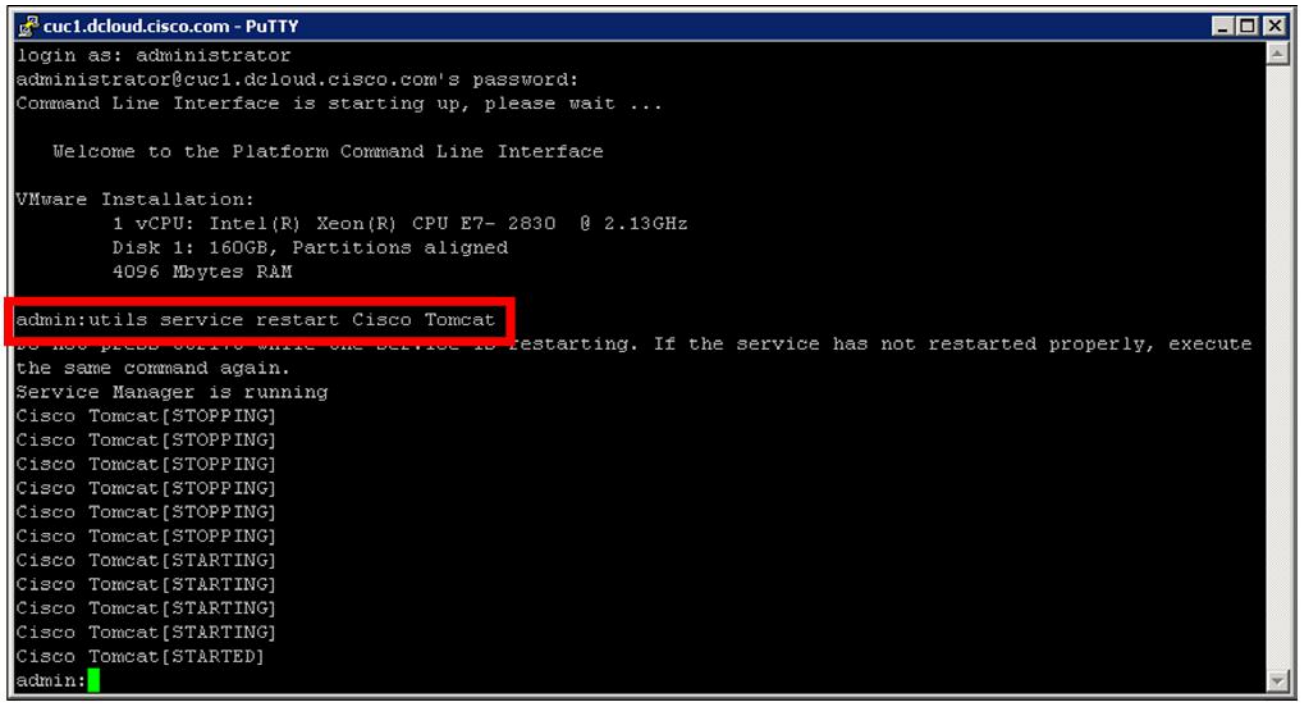
   新しい CA 署名付き証明書をアップロードし、tomcat-trust を更新したので、次のセクションに進む前に Cisco Tomcat サービスを再起動する必要があります。Cisco Tomcat を再起動しないと、古い自己署名 tomcat 証明書が引き続き使用されます。

   WKST2（198.18.133.37）で PuTTY を使用して、Unity Connection（cuc1.dcloud.cisco.com）コマンド ライン インターフェイスに **SSH** 接続します。

   PuTTY アイコン 

をダブルクリックして起動します。**cuc1** プロファイル エントリを選択するか、[ホスト名（Host Name）] フィールド（または [IP アドレス（IP Address）] フィールド）に「**cuc1.dcloud.cisco.com**」と入力します。[開く（Open）] をクリックします。ユーザ名/パスワード：**administrator/dCloud123!** でログインし、コマンド ラインに **utils service restart Cisco Tomcat** コマンドを入力します（図 193 を参照）。Cisco Tomcat サービスが再起動します。図 193 に示すようにサービスが再起動したら、「**exit**」と入力して、Unity Connection に対する SSH セッションを終了します。

図 193. Unity Connection で Cisco Tomcat Service を再起動



注: Cisco Tomcat サービスが再起動して、さまざまな Web 管理インターフェイスが利用できるようになるまでには数分かかる場合があります。

元の Unity Connection 証明書警告で一時的な例外を作成していた場合は、次回新しくブラウザを開いてずれかの Unity Connection Web 管理インターフェイスに移動したときには、証明書警告が表示されません。これは元の自己署名 tomcat 証明書が、エンタープライズ CA の署名付き証明書に置き換えられたためです。エンタープライズ CA ルート証明書は、すでに Windows ワークステーションの Firefox ブラウザの証明書信頼ストアにインポートされているため、ブラウザでは証明書が自動的に検証されます。これをテストするには、WKST2（198.18.133.37）で Firefox ブラウザ ウィンドウを閉じて Firefox を再起動し、https://cuc1.dcloud.cisco.com/cuadmin/ にアクセスします。証明書警告が表示されなくなります。

WKST2 または WKST3（オンプレミス エンドポイント）で次回 Jabber クライアントを起動すると、ワークステーションの信頼ストアでエンタープライズ ルート CA 証明書によって自動的に検証されるため、Unity Connection サーバ証明書を承認するプロンプトが表示されなくなります。

D. Unity Connection のための Unified CM セキュア SIP トランク設定

Unity Connection 証明書にエンタープライズ CA が署名し、CA が署名した証明書を Unity Connection サーバが信頼できるようになると、Unified CM システムで必要な設定を完了して、Unity Connection との暗号化されたセキュアな統合が可能になります。このセクションでは、最初にセキュア SIP トランク セキュリティ プロファイルを使用して Unified CM を設定します。次に、Unity Connection に対する既存の SIP トランクにそのプロファイルを割り当てます。

13. Unified CM と Unity Connection 間のトランクにセキュア SIP トランク プロファイルを設定する

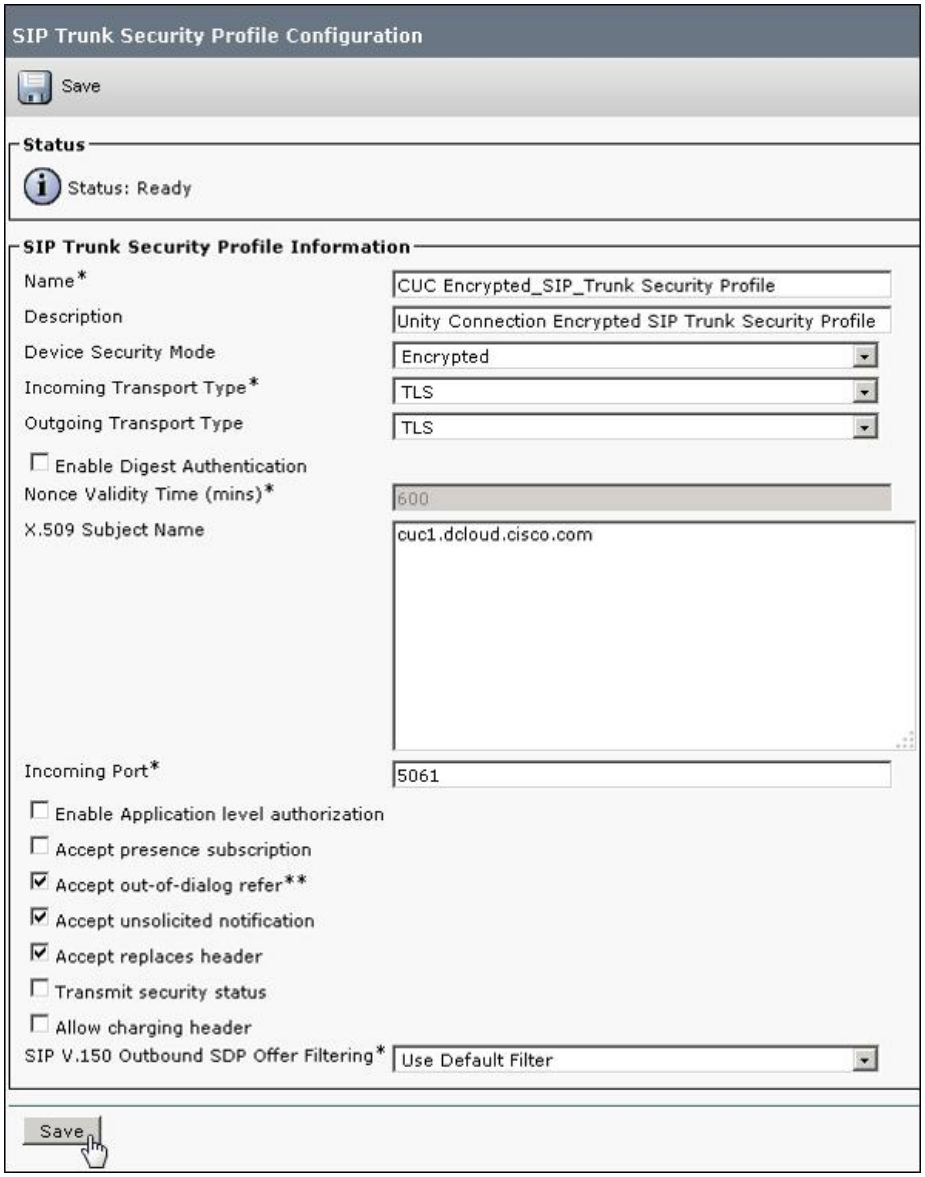
    このタスクでは、最初にセキュア SIP トランク セキュリティ プロファイルを使用して Unified CM を設定し、Unity Connection に対する既存の SIP トランクについてそのプロファイルを選択します。次に、Unity Connection と Unified CM 間で暗号化を使用するように Unity Connection を設定します。

WKST2（198.18.133.37）で Firefox Web ブラウザを使用して、Unified CM 管理インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin）に移動し、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

[システム（System）] > [セキュリティ（Security）] > [SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）] を選択します。[検索（Find）] をクリックして、CUC SIP トランク セキュリティ プロファイル **CUC SIP Trunk Security Profile** を見つけ、  （コピー アイコン）をクリックして、このプロファイルを新しいプロファイルにコピーします。

図 194 に示すように、[名前（Name）] フィールドに「**CUC Encrypted_SIP_Trunk Security Profile**」と入力し、[説明（Description）] フィールドに「**Unity Connection Encrypted SIP Trunk Security Profile**」と入力して、[端末セキュリティモード（Device Security Mode）] ドロップダウンから [暗号化（Encrypted）] を選択します。[着信トランスポートタイプ（Incoming Transport Type）]、[発信トランスポートタイプ（Outgoing Transport Type）]、[着信ポート（Incoming Port）] の各フィールドが、それぞれ [TLS]、[TLS]、[5061] に自動的に更新されます。[X.509 サブジェクト名（X.509 Subject Name）] に、Unity Connection tomcat 証明書で使用している共通名（CN）「**cuc1.dcloud.cisco.com**」を入力します。[保存（Save）] をクリックすると新規プロファイルが作成されます。

図 194. Unity Connection SIP トランク用の Unified CM 暗号化 SIP トランク セキュリティ プロファイル

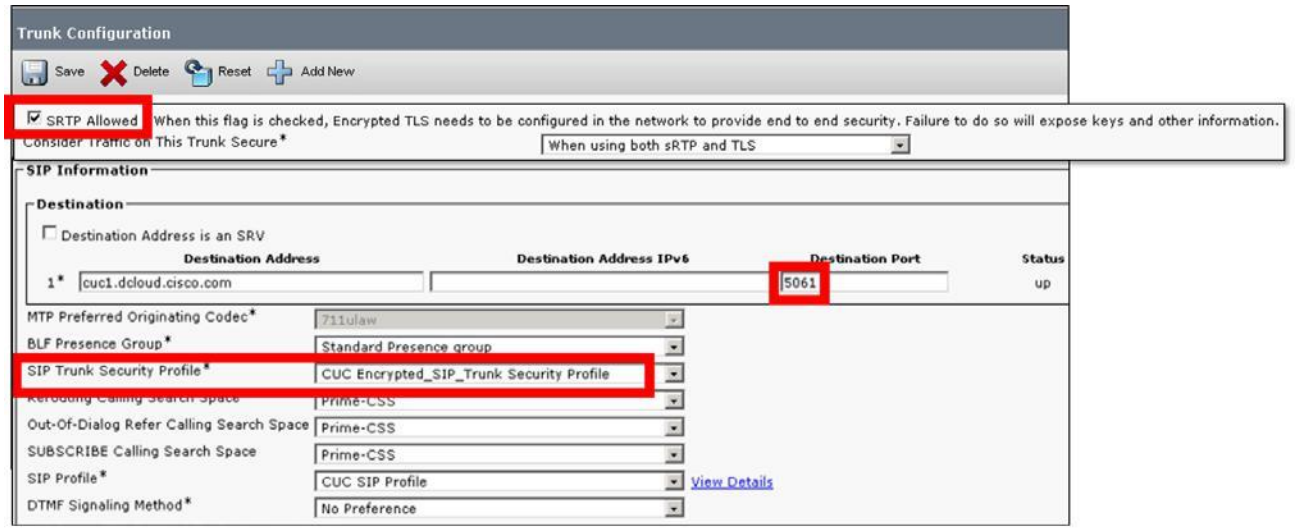


注:認証には証明書の署名検証が使用され、それによってフルサービスの SIP トランクが許可されます。認可には SIP トランク セキュリティ プロファイルの [X.509 サブジェクト名(X.509 Subject Name)] フィールドが使用されます。[X.509 サブジェクト名(X.509 Subject Name)] フィールドが正しくなくても SIP トランクが表示される場合がありますが、Unity Connection に対する SIP 要求は失敗します。

14. ncrypted SIP トランク プロファイルを Unity Connection 宛の SIP トランクに適用する

次に、新しく暗号化されたこの SIP トランク セキュリティ プロファイルを適用して、Unity Connection 宛の既存の SIP トランクを保護します。Unified CM(ucm1.dcloud.cisco.com)で [端末(Device)] > [トランク(Trunk)] に移動し、[検索(Find)] をクリックします。Unity Connection 用の SIP トランク **cuc1_SIP_Trunk** を見つけます。トランク名をクリックすると、設定ページが表示されます。図 195 に示すように、[SRTP 許可(SRTP Allowed)] チェックボックスをオンにしてトランク設定を更新します。次に、[SIP トランクセキュリティプロファイル(SIP Trunk Security Profile)] ドロップダウンから、作成した SIP トランク セキュリティ プロファイル(**CUC Encrypted_SIP_Trunk Security Profile**)を選択して、SIP トランク宛先ポートを **5061** に変更します。

図 195. Unified CM:Unity Connection 宛の SIP トランクの保護



をクリックします。続くダイアログで [OK] をクリックし、 

をクリックします。続くダイアログで [リセット(Reset)] をクリックして、トランクをリセットします。「リセット要求の送信に成功しました(Reset request was sent successfully)」というメッセージが表示されたら、[閉じる(Close)] をクリックします。

この時点では、Unity Connection サーバのセキュリティ設定を完了するまで、SIP トランクは稼働しません。

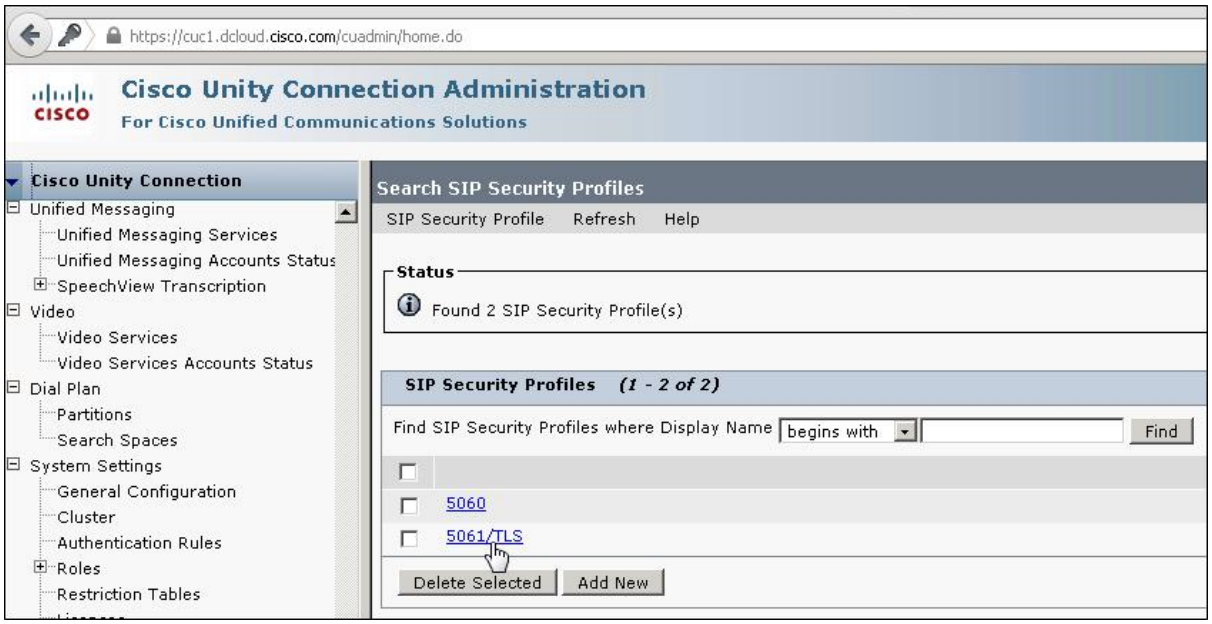
E. Unity Connection テレフォニー統合の暗号化

Unified CM の設定が完了したら、Unity Connection システム設定に移ります。

15. デフォルトのシステム TLS SIP セキュリティ プロファイルを確認する

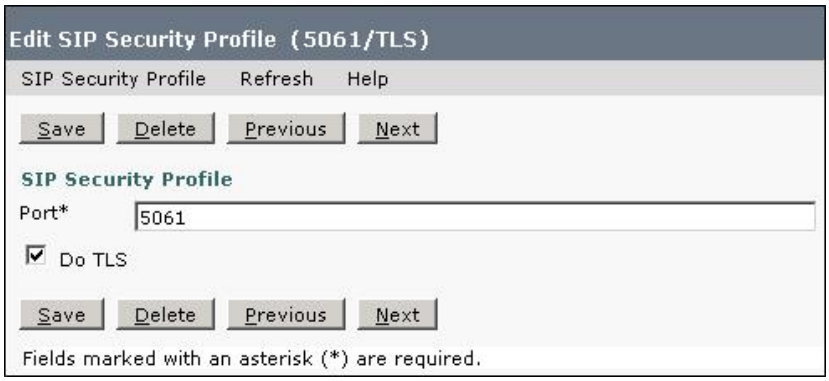
Unity Connection 管理インターフェイス(https://cuc1.dcloud.cisco.com/cuadmin/)にアクセスし、ユーザ名/パスワード: **administrator/dCloud123!** を使用してログインします。[Cisco Unity 管理(Cisco Unity Administration)] > [テレフォニー統合(Telephony Integrations)] > [セキュリティ(Security)] > [SIP セキュリティプロファイル(SIP Security Profile)] に移動します。図 196 に示すように、**5061/TLS** プロファイルが存在することを確認します。

図 196. Unity Connection：5061/TLS SIP セキュリティ プロファイル



プロファイル名をクリックし、続くページで、[ポート（Port）] フィールドに **5061** と表示されていて、図 197 に示すように [TLS を実行（Do TLS）] チェックボックスがオンになっていることを確認します。

図 197. Unity Connection：5061/TLS SIP セキュリティ プロファイルの確認



16. Unity Connection のテレフォニー統合に暗号化を設定する

テレフォニー統合に暗号化を設定するには、最初に Unity Connection システムで Unified CM クラスタ TFTP サーバを設定します。それにより、暗号化を有効にすると、Unity Connection で Unified CM CallManager 証明書が自動的にダウンロードされます。

[テレフォニー統合（Telephony Integrations）] > [ポートグループ（Port Group）] に移動します。図 198 に示すように、[UCM1_PhoneSystem-1] をクリックしてポート グループを編集します。次に [編集（Edit）] メニューを開き、[サーバ（Servers）] を選択します。

図 198. Unity Connection：ポート グループのセキュリティ設定 - サーバ

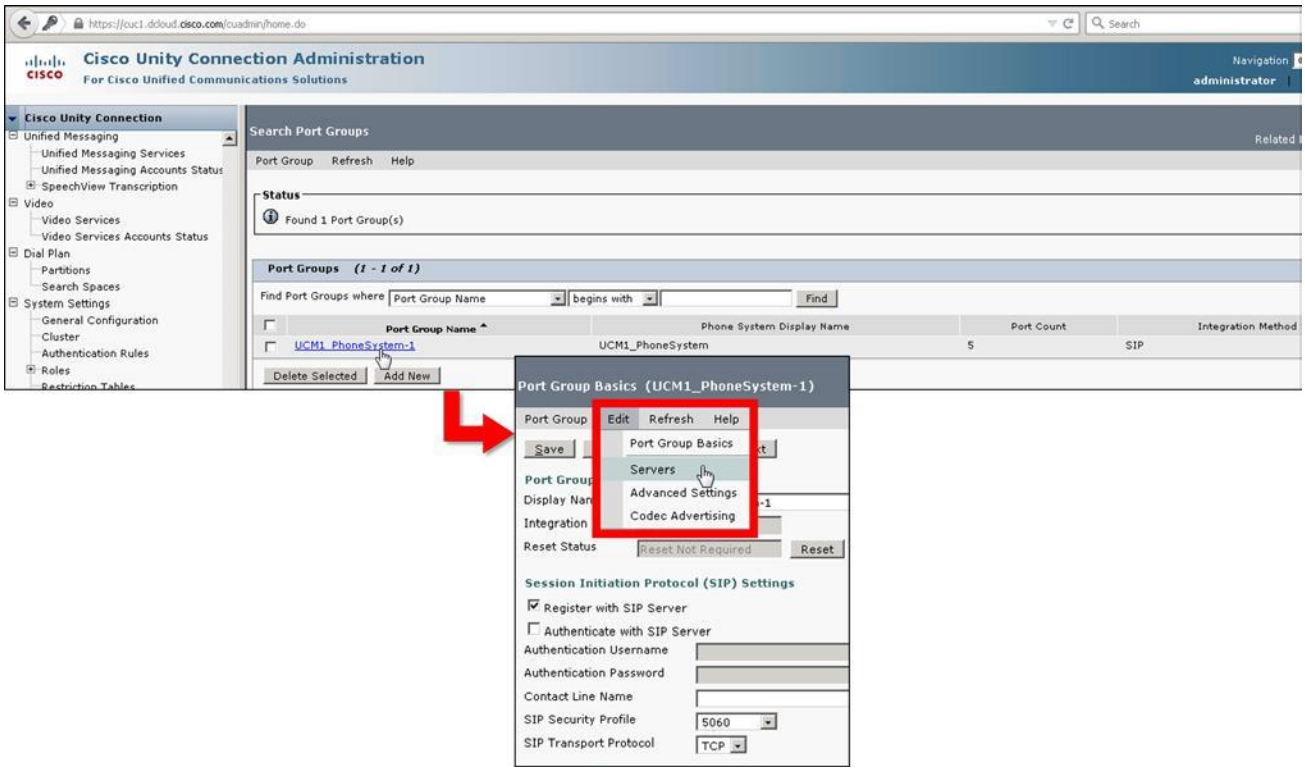
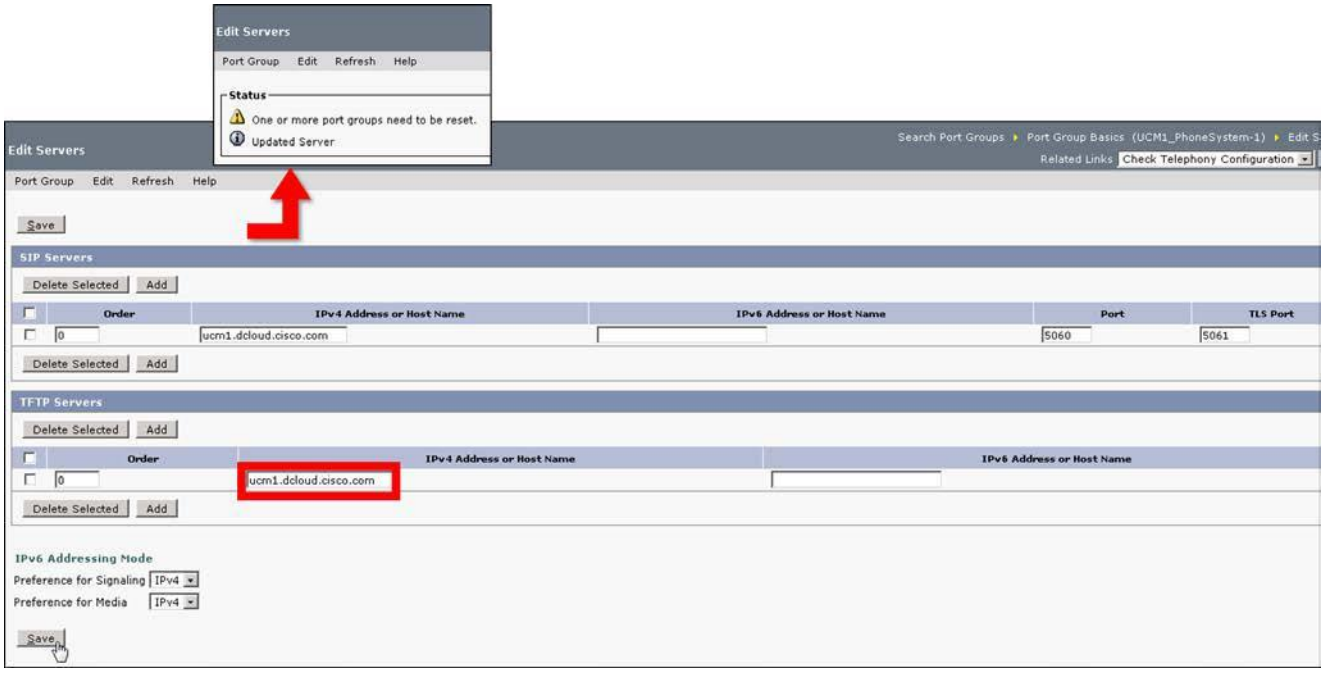


図 199 に示すように、[サーバの編集（Edit Servers）] ページの [TFTP サーバ（TFTP Servers）] セクションで、Unified CM TFTP サーバの FQDN として「**ucm1.dcloud.cisco.com**」と入力し、画面下部の [保存（Save）] をクリックします。

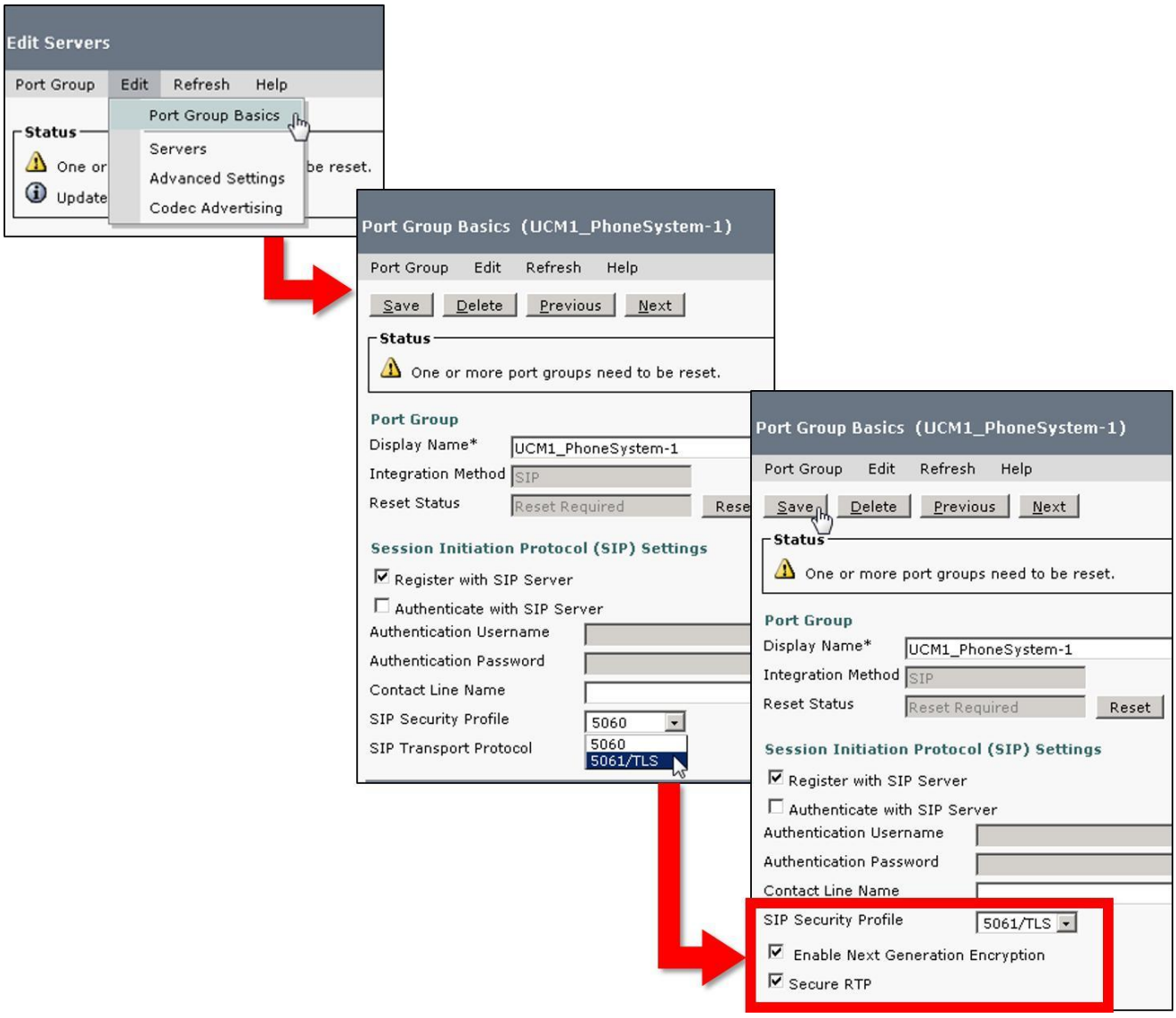
図 199. Unity Connection：ポート グループに Unified CM TFTP サーバを追加



注:このラボでは、ラボのポッドのレプリケーションとキャパシティを設定しやすいように、SIP サーバと TFTP サーバが同じになっています。ただし、ベスト プラクティスで推奨される設計では、TFTP サーバ ノードをスタンドアロンにして、Unified CM 呼処理サブスクライバ ノードから分離します。

ポート グループをリセットする前に、ポート グループのセキュリティを有効にします。図 200 に示すように、[編集(Edit)] メニューから [ポートグループの基本設定(Port Group Basics)] を選択し、メイン ポート グループの設定ページに戻ります。

図 200. Unity Connection:電話システム ポート グループの保護

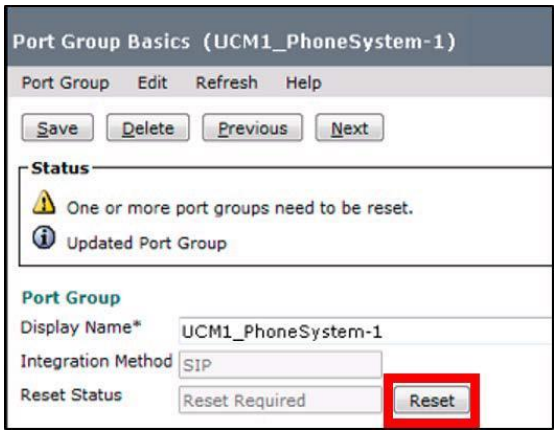


[SIP セキュリティプロファイル(SIP Security Profile)] ドロップダウンから [5061/TLS] を選択し、ポート グループのセキュリティを有効にします。チェックボックスとして、[次世代暗号化の有効化(Enable Next Generation Encryption)] と [セキュア(Secure RTP)] が表示されます。これら両方のチェックボックスをオンにして、暗号化とセキュアな通話を有効にします

(図 200 を参照)。[保存(Save)] をクリックして、設定を保存します。

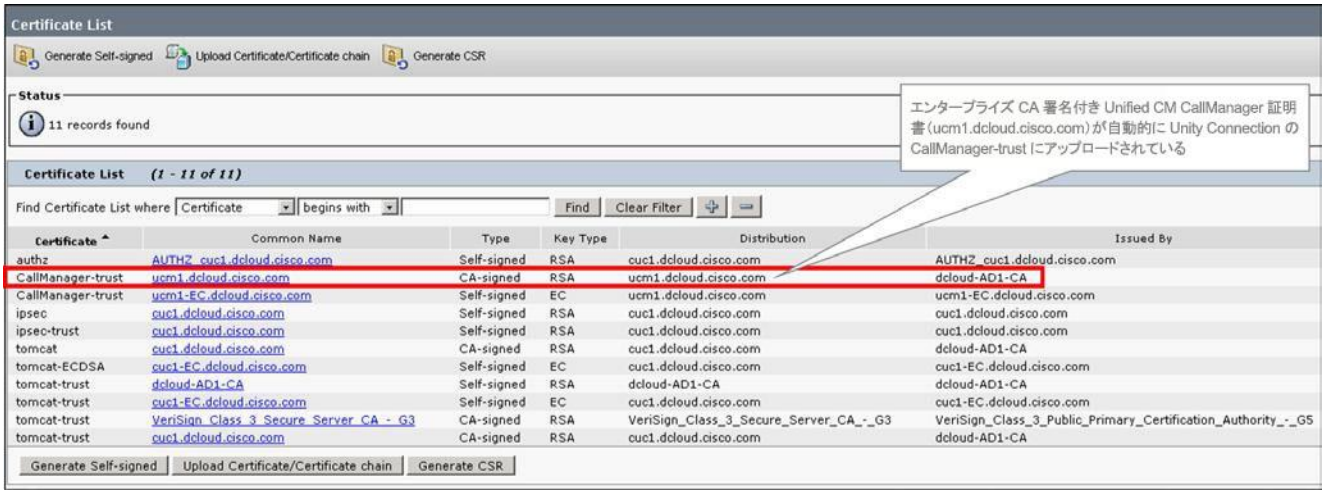
最後に [リセット(Reset)] ボタンをクリックして、図 201 に示すようにポート グループをリセットします。

図 201. Unity Connection：電話システム ポート グループのリセット



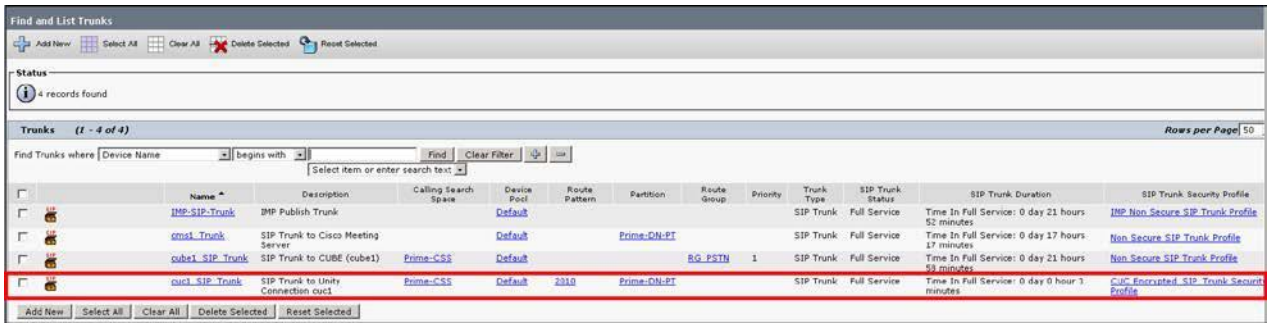
Unity Connection と Unified CM 電話システム（ucm1.dcloud.cisco.com）間で暗号化を有効にしたため、ポート グループがリセットされると、Unity Connection が Unified CM TFTP サーバから Unified CM CallManager 証明書を自動的に取得し、ローカルの CallManager-trust ストアにアップロードします。これを確認するには、Unity Connection Operating System 管理ポータル（https://cuc1.dcloud.cisco.com/cmplatform/）（ユーザ名/パスワード = **administrator/dCloud123!**）に戻り、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] に移動します。[検索（Find）] をクリックすると、図 202 のように、証明書の完全なリストと注記が表示され、Unified CM CallManager 証明書（ucm1.dcloud.cisco.com）が CallManager-trust に自動的にアップロードされたことが示されます。

図 202. Unity Connection：ローカルの CallManager-trust ストアに自動的にアップロードされた Unified CM CallManager 証明書



数分後に、Unified CM 管理ポータル（https://ucm1.dcloud.cisco.com/ccmadmin）に戻り、必要に応じてユーザ名/パスワード：**administrator/dCloud123!** でログインして、トランクがフルサービスであることを確認します。[端末（Device）] > [トランク（Trunk）] に移動します。[検索（Find）] をクリックして SIP Trunk リストをロード/リロードし、図 203 に示すように、Unity Connection SIP トランクが [フルサービス（Full Service）] に戻ったことを確認します。

図 203. Unified CM：Unity Connection 宛のフルサービス セキュア SIP トランク*



完了したモジュールによっては、トランク リストが上の図と異なる場合があります。

F. エンドポイントとボイスメール システム間の暗号化された通話の確認

最後に、Jabber クライアントと Unity Connection ボイスメール システム間で、セキュアな暗号化された通話が有効になっていることを確認する必要があります。

17. 発信して、Unity Connection ボイスメール システムに通話が転送されるようにする

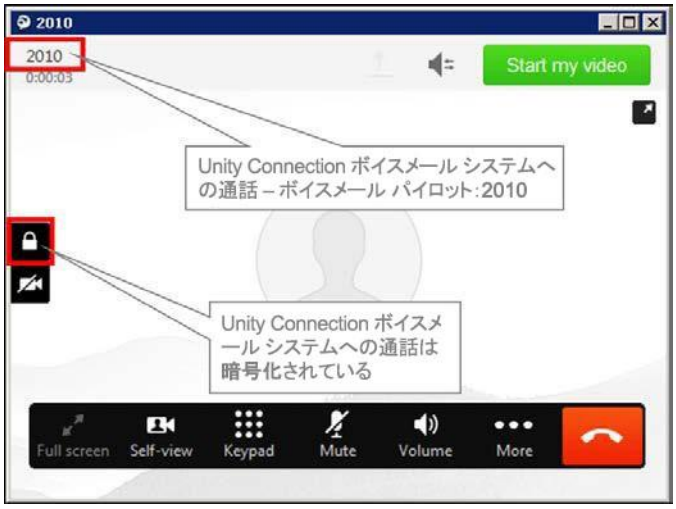
    WKST2（198.18.133.37, DCLOUD**aperez/C1sco12345**）と WKST3（198.18.133.38, DCLOUD**mcheng/C1sco12345**）で Jabber を起動します。クライアントが自動的にログインします（プロンプトが表示された場合は、ユーザ名/パスワード：**aperez | mcheng/C1sco12345**）を入力します。

    注：Jabber が登録されたときに Unity Connection サーバ証明書を**承認**または**拒否**するプロンプトはなくなりました。エンタープライズ CA が Unity Connection サーバ証明書に署名したため、Jabber クライアントはローカル ワークステーションの証明書信頼ストアにあるエンタープライズ CA ルート証明書を使用して、証明書を自動的に検証できます。

    Jabber クライアントが登録されたら、再度 Anita Perez の Jabber クライアント（WKST2）で **6030** にダイヤルし、[発信（Call）] をクリックして、Monica Cheng の Jabber クライアント（WKST3）に発信します（図 168 を参照）。Monica Cheng の Jabber クライアントでは着信通話に応答しないでください。代わりに、通話がボイスメールに転送されるようにします。着信通話ダイアログで [拒否（Decline）] をクリックして、通話をボイスメールにただちにプッシュします。この場合も、無応答通話後に発信者がメッセージを残すところをモデリングしています。

    ボイスメール システムに通話が接続されると、Unity Connection ボイスメール システムに（Anita のクライアントから）リダイレクトされた通話が暗号化されていることがわかります。これは、通話ウィンドウにロック アイコンが表示されていることで確認できます。Monica のボイスメール ボックスにメッセージを残す必要はないため、通話がボイスメール パイロット（2010）に接続され、暗号化されていないことを確認したら（図 204 を参照）、Anita の Jabber クライアントでそのまま通話を終了します。

図 204. Unity Connection に対する暗号化されたセキュアなリダイレクト通話



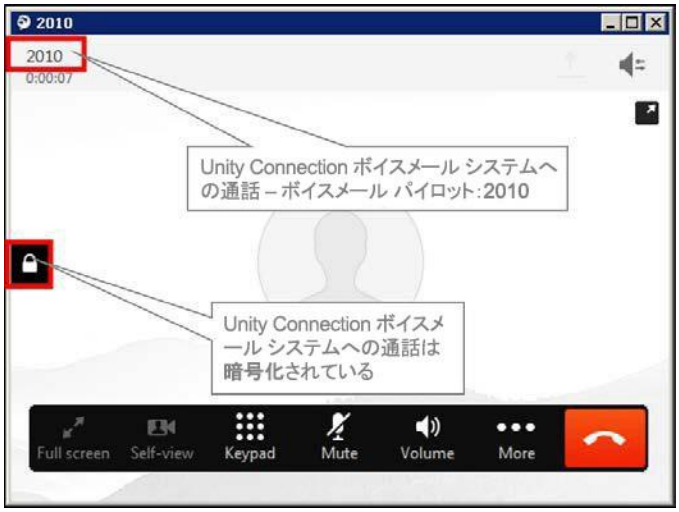
Jabber で、Unity Connection に対する通話を終了します。

18. [ボイスメールに発信（Call Voicemail）] ボタンで Unity Connection ボイスメール システムに直接発信する

Monica Cheng の Jabber クライアント（WKST3）で、[ボイスメッセージ（Voice Messages）] タブの [ボイスメールに発信（Call Voicemail）] ボタンをクリックして、ボイスメール システムに発信します。ここでは、メッセージ待機通知の受信後に発信者がメッセージを取得するところをモデリングしています。または、ボイスメール システムのパイロット番号：2010 を手動でダイヤルすることもできます。

通話がボイスメール システムのパイロット（2010）に接続すると、Cisco Jabber に、ボイスメール システムに対する通話が暗号化されていることを示すアイコンが表示されます（図 205 を参照）。

図 205. Unity Connection に対する暗号化されたセキュアなボイスメール取得通話



Jabber で、Unity Connection に対する通話を終了します。

続行する前に、WKST2 および WKST3 で Jabber クライアントを終了します。

***** モジュール #8 の終了 *****

モジュール 9. Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー

モジュールの概要

このモジュールでは、Expressway Mobile and Remote Access（MRA）のエンドツーエンドの暗号化と、Cisco Jabber のための新しい MRA アクセス ポリシーの詳細を示します。最初に Expressway-C で Unified CM サーバを検出します。次に、暗号化された電話セキュリティ プロファイルを使用してリモート Jabber クライアントを設定し、エンドツーエンドで暗号化された通話を可能にします。エンドツーエンドで暗号化された通話を確認したら、新しい Jabber MRA アクセス ポリシー機能について確認します。これは、どのユーザとどのタイプの Jabber クライアントが MRA 経由で接続できるかを、管理者が制御するポリシーです。このモジュールは、次の 4 つのセクションに分割されています。

A. Expressway-C Unified CM サーバの検出

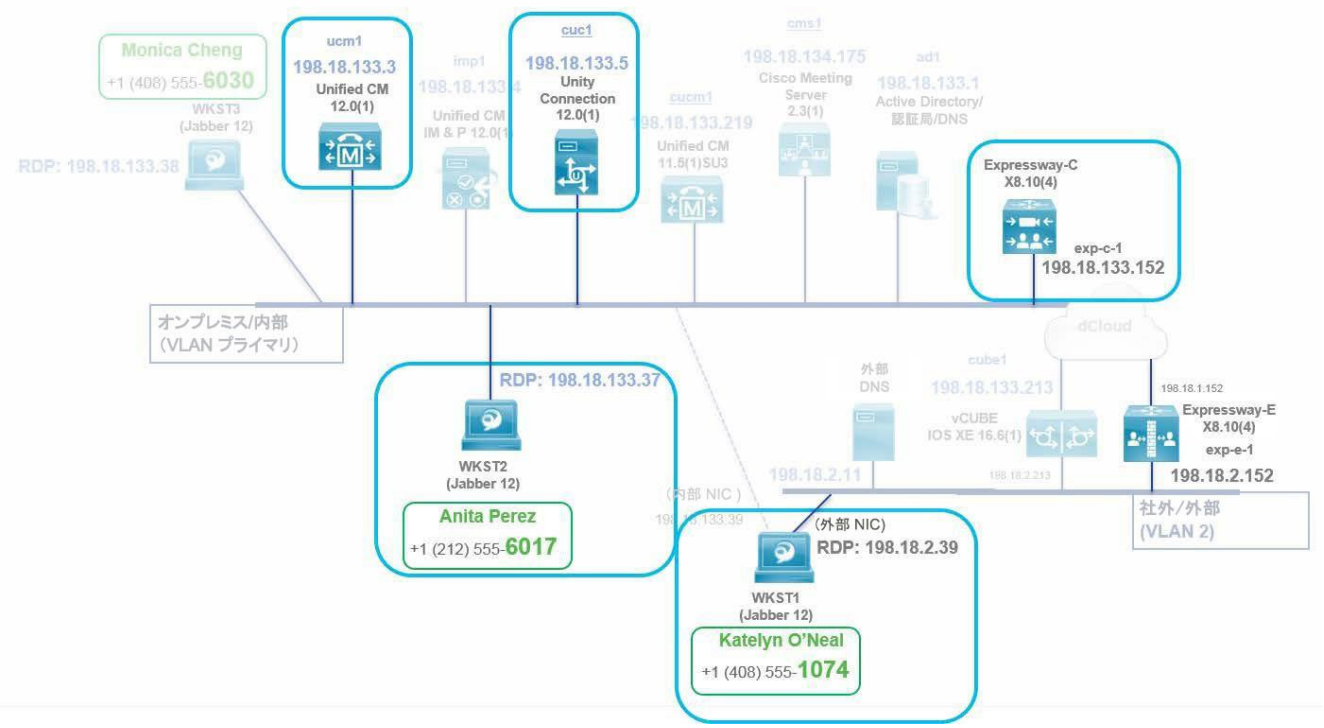
B. MRA Jabber クライアント用のエンドツーエンドの暗号化の設定

C. Jabber エンドポイント用の MRA アクセス ポリシー

D. MRA を経由した Unity Connection ボイスメール システム宛通話のエンドツーエンドの暗号化

次の図 206 は、このモジュールのトポロジおよび関連するコンポーネントを示しています。

図 206. モジュール 9：Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー



手順

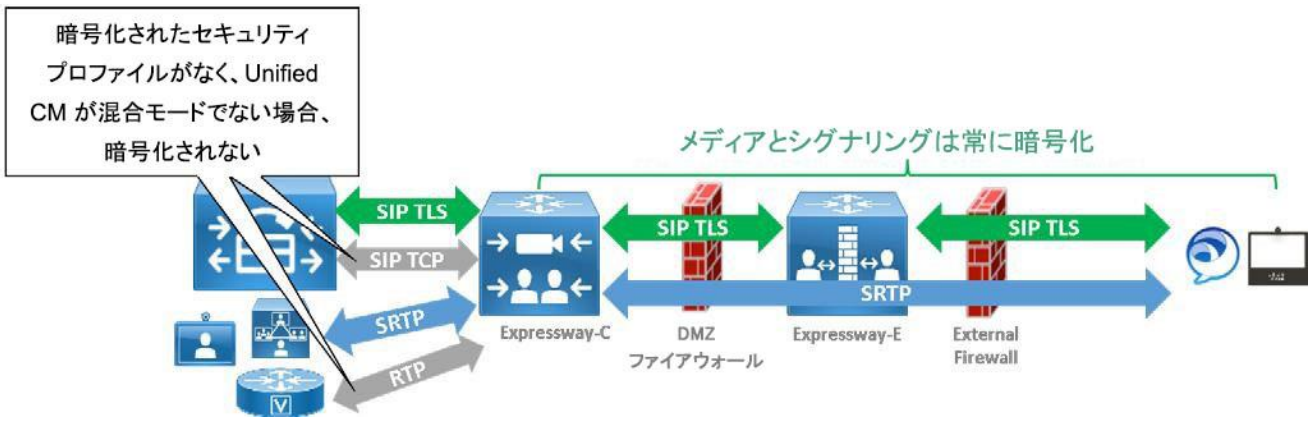
このモジュールでは、Expressway MRA 経由で接続された、オフプレミスの Jabber エンドポイントについて、エンドツーエンドの暗号化を設定して確認します。図 207 に示すように、MRA エンドポイント（Jabber エンドポイントまたはハードウェア エンドポイント）と Expressway-C 間のメディアとシグナリングは、常に暗号化されます。ただし、MRA エンドポイントが社内ネットワーク内部のエンドポイントに発信すると、社内ネットワーク内部のコール レッグ（Expressway-C と Unified CM 間のシグナリング、Expressway-C と内部エンドポイント間のメディア）は、次のルールに示す設定に応じて、暗号化される場合とされない場合があります。

a. MRA エンドポイントが非暗号化電話セキュリティ プロファイルを使用して設定されている場合、内部コール レッグは暗号化されません。

b. Unified CM が混合モードであり、MRA エンドポイントが暗号化された電話セキュリティ プロファイルを使用してされている場合、Expressway-C と Unified CM 間の SIP シグナリング（TLS）は暗号化されます。

c. Unified CM が混合モードで、暗号化された電話セキュリティ プロファイルを使用して MRA エンドポイントが設定されていて、内部のエンドポイントも暗号化されたプロファイルを使用して設定されている場合は、Expressway-C と内部エンドポイント間のメディアは暗号化（SRTP）されます。その場合、メディアとシグナリングは**エンドツーエンドで暗号化**（正確にはすべてのコール レッグが暗号化）されます。

図 207. MRA エンドポイントでのメディアとシグナリングの暗号化



MRA を使用して SIP TLS 認証で使用される証明書は、オンプレミス通話の場合とは多少異なります。エンドポイントが MRA 経由でエンタープライズと接続すると、エンドポイントでは Expressway-E サーバ証明書が確認されますが、サーバではエンドポイント証明書がチェックされません。この TLS 接続では相互認証は使用されません。MRA クライアントの MIC または LSC 証明書は、その有無にかかわらず確認されません。次に MRA クライアントのユーザが、Cisco Unified CM ユーザ データベースまたは統合された LDAP サーバ（Jabber がシングル サインオンによって導入されている場合は IdP）に対するユーザ名とパスワードを使用して認証されます。Expressway-C と Unified CM 間のコール レッグについては、MRA エンドポイントが暗号化モードで設定されている場合、Expressway-C によって Unified CM との SIP TLS 接続が確立され、MRA エンドポイントに変わって Expressway-C の証明書が送信されます。Unified CM はこの証明書を受け取ると、その MRA エンドポイントに設定された電話セキュリティ プロファイルの名前が、Expressway-C 証明書の SAN 拡張の一部であることを確認します。

A. Expressway-C Unified CM サーバの検出

このラボでは、Expressway Mobile and Remote Access がほぼ完全に事前設定されています（事前設定の内容については「付録 A: Expressway Mobile and Remote Access の設定」を参照）。

WKST1（198.18.2.39）は、MRA を使用して Windows クライアント用 Jabber をオンプレミスのコラボレーション サービスに接続する必要がある、オフプレミスのユーザを表します（例：音声/ビデオ、メッセージングとプレゼンス、ビジュアル ボイスメール）。

リモート/オフプレミスの Windows クライアント用 Jabber を MRA 経由で接続するには、導入内の Unified CM サーバに対するセキュア TLS 接続を検出してセットアップするように、Expressway-C を設定する必要があります。

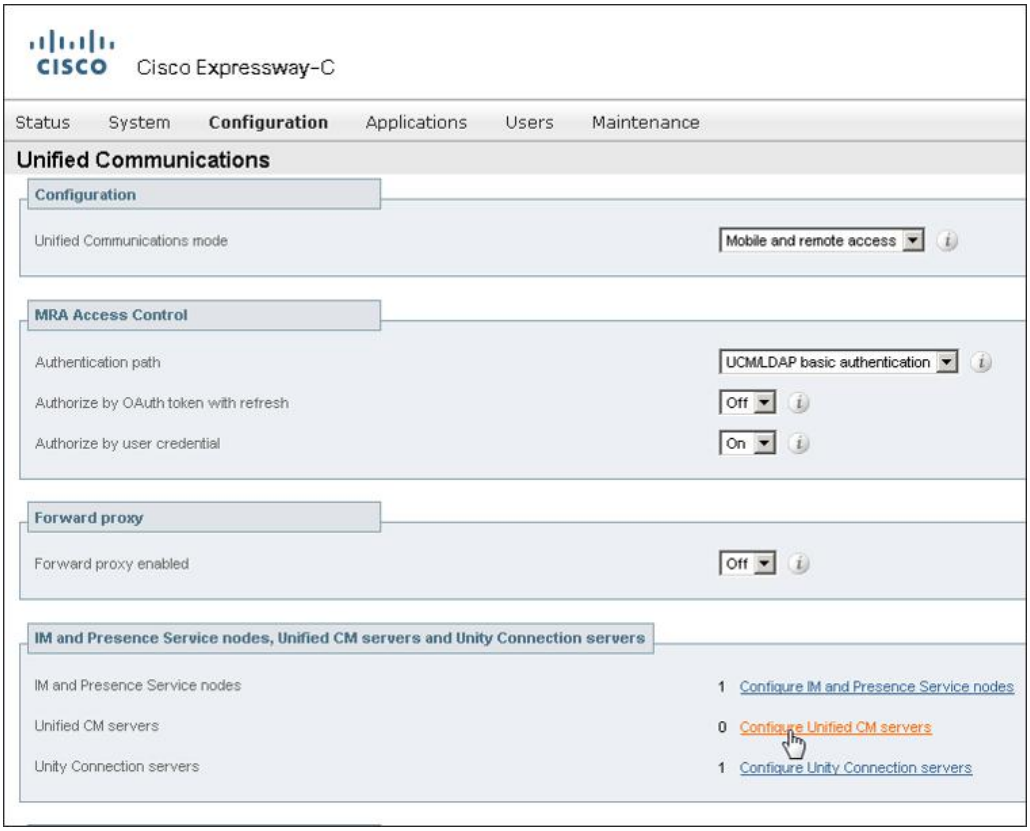
注：MRA が正しく機能するには、MRA 設定を正しく完了し、リモート Jabber クライアントが接続されるように、次のステップを**必ず実行**します。

1. Expressway-C が Unified CM サーバを検出するように設定する

WKST2（198.18.133.37）で Firefox を使用して、Expressway-C 管理インターフェイス（https://exp-c-1.dcloud.cisco.com/）にアクセスし、ユーザ名/パスワード：**admin/dCloud123!** を使用してログインします。

Unified Communications 設定ページ（[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）]）に移動し、[Unified CM サーバの設定（Configure Unified CM servers）] をクリックします（図 208 を参照）。

図 208. Expressway-C の Unified Communications の設定：Unified CM サーバ



[追加（Add）] をクリックします。次の画面で、図 209 に示すように設定します。

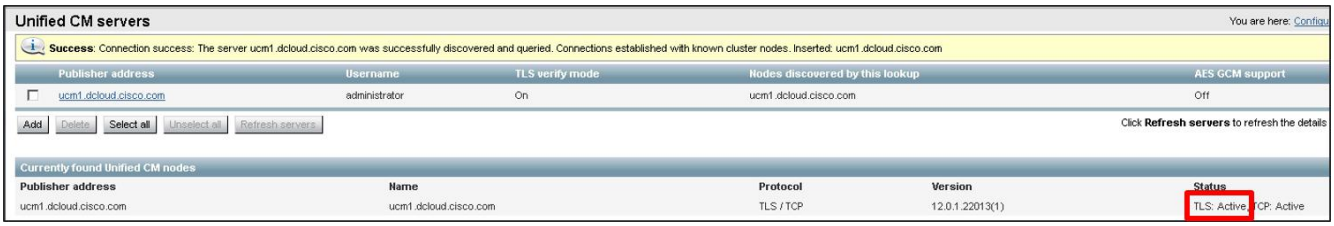
- [Unified CM パブリッシャアドレス（Unified CM publisher address）]：**ucm1.dcloud.cisco.com**
- [ユーザ名（Username）]：**administrator**
- [パスワード（Password）]：**dCloud123!**
- [TLS 検証モード（TLS verify mode）]：**オン**（デフォルト）
- [AES GCM のサポート（AES GCM Support）]：**オフ**（デフォルト）

[アドレスの追加（Add Address）] をクリックします。

図 209. Expressway-C での Unified CM サーバの検出

Unified CM は混合モードであるため、Unified CM サーバが検出されれば、図 210 に示すように Unified CM と Expressway-C 間にアクティブな TLS 接続が確立されています。これは、MRA とオンプレミスのエンドポイント間でエンドツーエンドの暗号化が可能になったことを意味します。

図 210. Expressway-C で検出された Unified CM サーバ



B. MRA Jabber クライアント用のエンドツーエンドの暗号化の設定

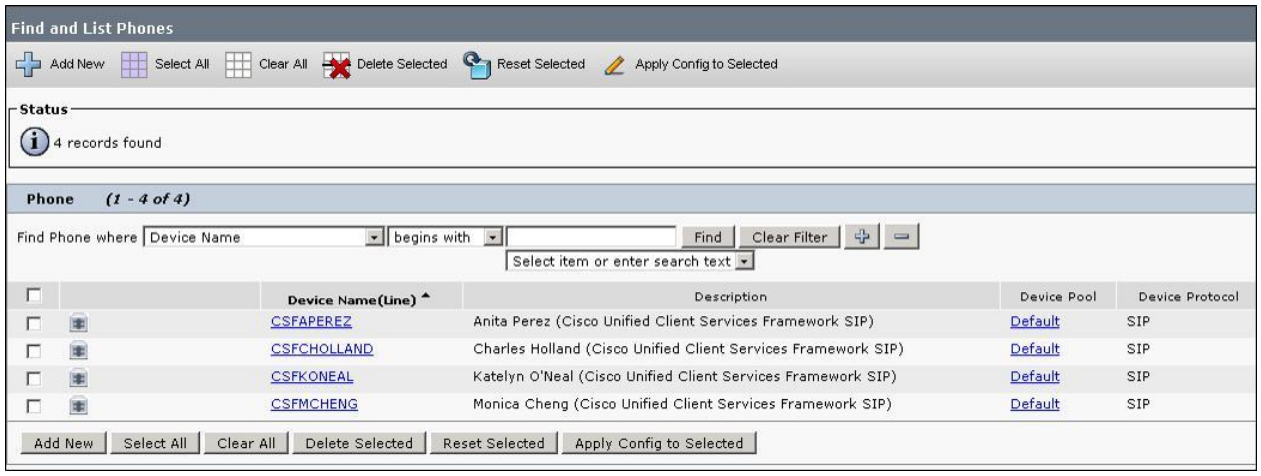
次に、MRA Jabber クライアント（CSFKONEAL）で暗号化を有効にする必要があります。

2. MRA/オフプレミス Jabber クライアントに暗号化された電話セキュリティ プロファイルを適用する

   Unified CM 管理インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin/）にアクセスし、ユーザ名/パスワード：**administrator / dCloud123!** を使用してログインします。

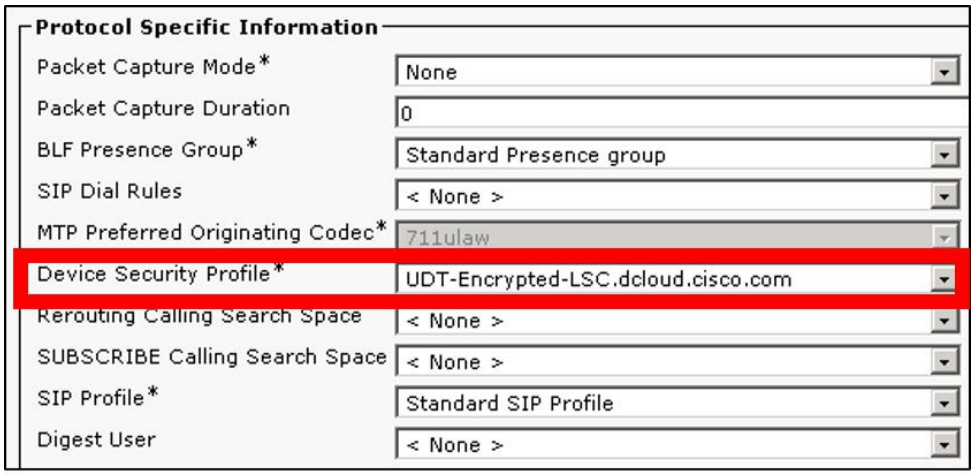
   [端末（Device）] > [電話（Phone）] に移動し、[検索（Find）] をクリックすると、システム上のエンドポイント端末のリストが表示されます（図 211 を参照）。

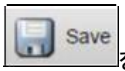
図 211. Unified CM 電話のリスト

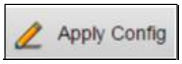


ユーザ Katelyn O'Neal の CSF 端末 **CSFKONEAL** をクリックして、端末設定ページをロードします。[端末セキュリティプロファイル（Device Security Profile）] フィールドの [プロトコル固有情報（Protocol Specific Information）] で、暗号化されたセキュリティ プロファイル **UDT-Encrypted-LSC.dcloud.cisco.com** を選択します（図 212 を参照）。

図 212. UDT-Encrypted-LSC.dcloud.cisco.com 端末セキュリティ プロファイルを適用





をクリックします。続くダイアログで [OK] をクリックし、 

をクリックします。次のダイアログで [OK] をクリックし、設定変更を適用します。

注: リモート MRA Jabber クライアント端末には LSC がないため（この端末については CAPF 登録を実行していないため）、この端末には **UDT-Encrypted-LSC.dcloud.cisco.com** セキュリティ プロファイルを適用します。**UDT-Encrypted-dAuthString.dcloud.cisco.com** または **UDT-Encrypted-NullString.dcloud.cisco.com** セキュリティ プロファイルを適用して、エンドツーエンドの暗号化を有効にすることもできます。MRA 経由で接続する場合には端末では証明書が不要であるため、3 つのうちどのプロファイルでも適用できます。

3. MRA/オフプレミス Jabber クライアント（WKST1 の CSFKONEAL）の MRA 接続を確認します。

   次に、WKST1 で、オフプレミスの Jabber クライアントの MRA 接続を確認します。ユーザ名 **DCLOUD\koneal** とパスワード **C1sco12345** を使用して、WKST1（198.18.2.39）に RDP 接続します。

   デスクトップの Jabber アイコンをダブルクリックして Jabber を起動し、クレデンシャル：**koneal/C1sco12345** を使用してログインします。

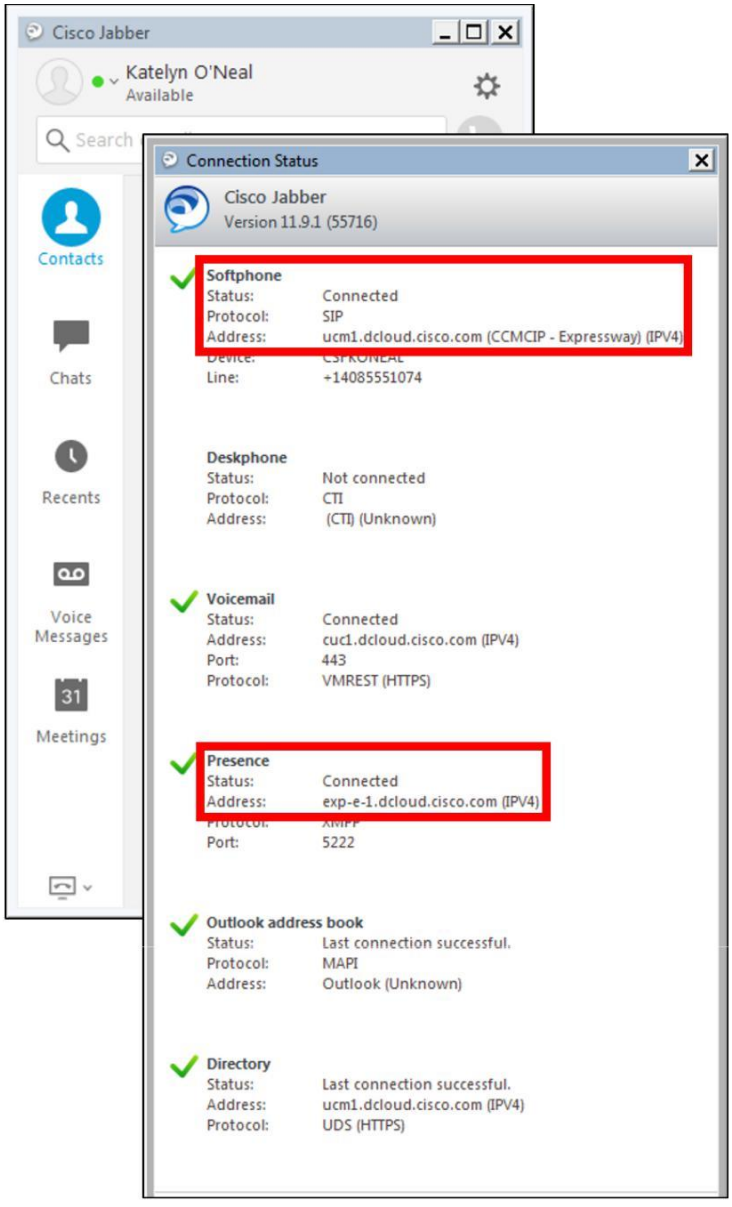
注:しばらくお待ちください。Jabber クライアントを最初に起動する場合は、1 分程度かかることがあります。

パブリック(外部)DNS の適切な DNS レコードを調べることで、Jabber クライアントが Expressway MRA サービスを検出し、Expressway-E を通じてエンタープライズ オンプレミス コラボレーション サービスに接続できることを確認できます。関連するパブリック DNS レコードは次のとおりです。

- SRV レコード:**_collab-edge._tls.dcloud.cisco.com → exp-e-1.dcloud.cisco.com**
- レコード:**exp-e-1.dcloud.cisco.com → 198.18.2.152**(「外部」インターフェイス)

Jabber がログインして完全に接続できるようにします。接続ステータスを調べることで、Jabber クライアントが Expressway MRA ソリューションを使用していることを確認できます。  ([設定(Settings)]) > [ヘルプ(Help)] > [接続ステータスの表示(Show connection status)] に移動します。図 213 に予想されるステータスを示します。

図 213. MRA Connected Jabber:接続ステータス



Softphone および Presence サービスは、どちらも Expressway を通じて接続していると示されています。Unity Connection との接続がアクティブで、証明書警告を受信していないことも確認できます。MRA の場合は、Unity Connection tomcat 証明書が自己署名であっても問題なく、また MRA に接続された Jabber クライアントでは Unity Connection 証明書を見ることはないため、検証対象のローカルの信頼ストアにも入りません。Jabber で必要なのは、ファースト ホップの TLS 接続（HTTPS REST）に、信頼される CA の署名付き Expressway-E 証明書が使用されていることを確認することだけです。そのため、証明書警告はありません。

4. Jabber MRA と Jabber オンプレミス端末間のエンドツーエンドで暗号化された通話を確認する

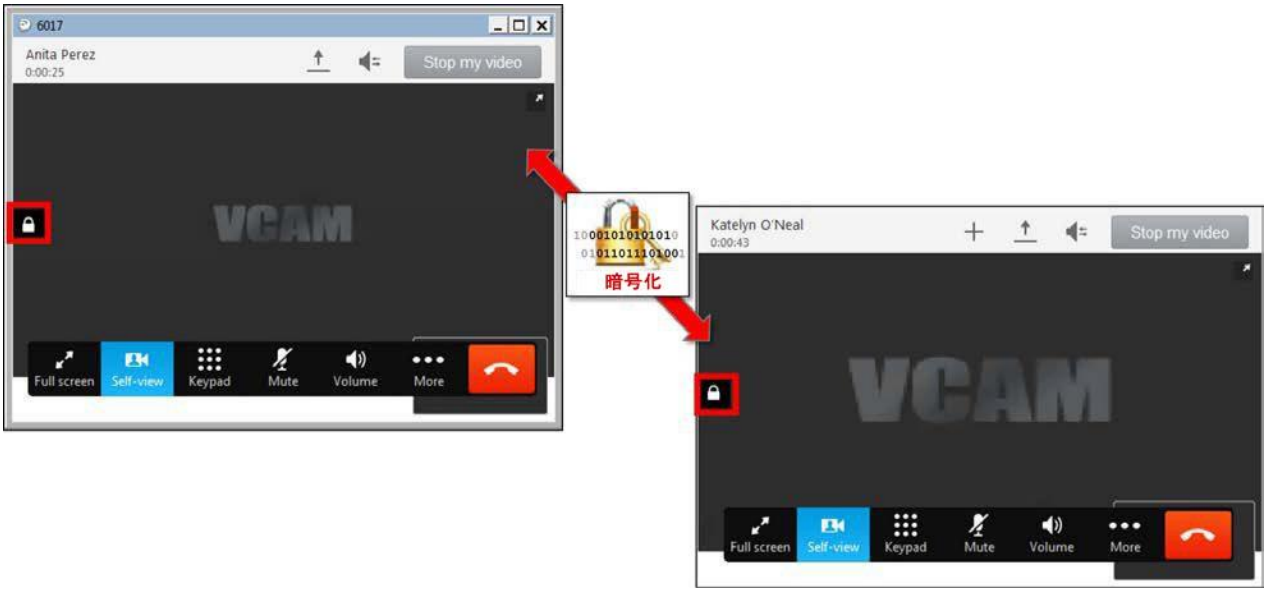
続行する前に、RDP 経由で WKST2（DCLOUD\aperez/C1sco12345）と WKST1（DCLOUD\koneal/C1sco12345）の両方に接続していて、両方のワークステーションの Jabber クライアントが起動し、Unified CM に登録されていることを確認します。

WKST1 で Katelyn O'Neal の Jabber クライアントから、[検索（Search）] または [通話（Call）] ウィンドウに「**6017**」と入力して、緑色の電話ボタンをクリックして Anita Perez に発信します（図 214 を参照）。

図 214. 発信：Katelyn O'Neal（WKST1、MRA）が 6017 とダイヤルして Anita Perez（WKST2）に発信

WKST2 で Anita Perez の Jabber クライアントで応答します。通話が接続されたら、両方の Jabber クライアントに暗号化を示す「ロック」アイコンが表示されていることを確認します（図 215 を参照）。

図 215. 暗号化されたセキュアな通話の確認：MRA Jabber からオンプレミスの Jabber への通話



通話を終了します。

続行する前に、すべてのワークステーション（WKST1 と WKST2）で実行されている Windows クライアント用 Jabber を終了します。

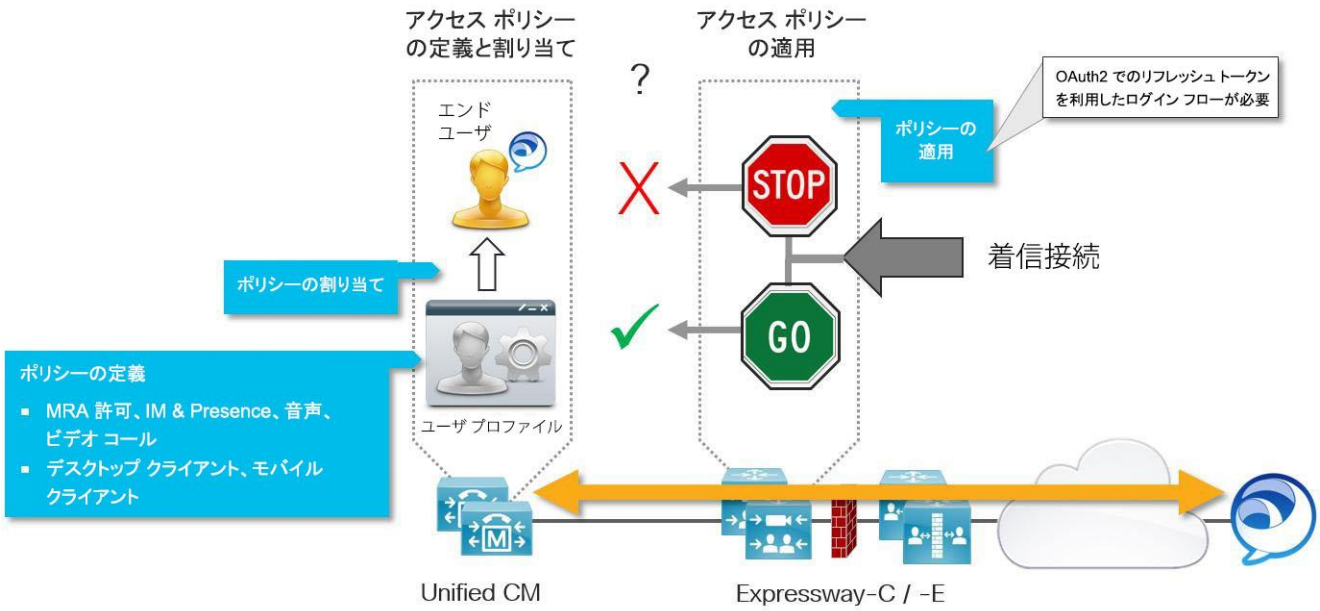
C. Jabber エンドポイント用の MRA アクセス ポリシー

このセクションでは、Expressway MRA 経由で接続されている Jabber エンドポイント用の新しい MRA アクセス ポリシーの詳細を示します。

注: モジュールのこのセクションを完了するには、モジュール 7（OAuth2）を完了している必要があります。MRA アクセス ポリシーは、OAuth ログイン フローに応じて異なります。

図 216 に、MRA アクセス ポリシーのアーキテクチャを示します。Unified CM 内にアクセス ポリシーの定義と割り当てが実装されていることを確認してください。アクセス ポリシーは、ユーザ プロファイルの構成内で定義し、エンド ユーザに割り当てる必要があります。一方で、Expressway はエッジでのアクセス ポリシーの適用を実際に処理します。

図 216. MRA アクセス ポリシーのアーキテクチャ



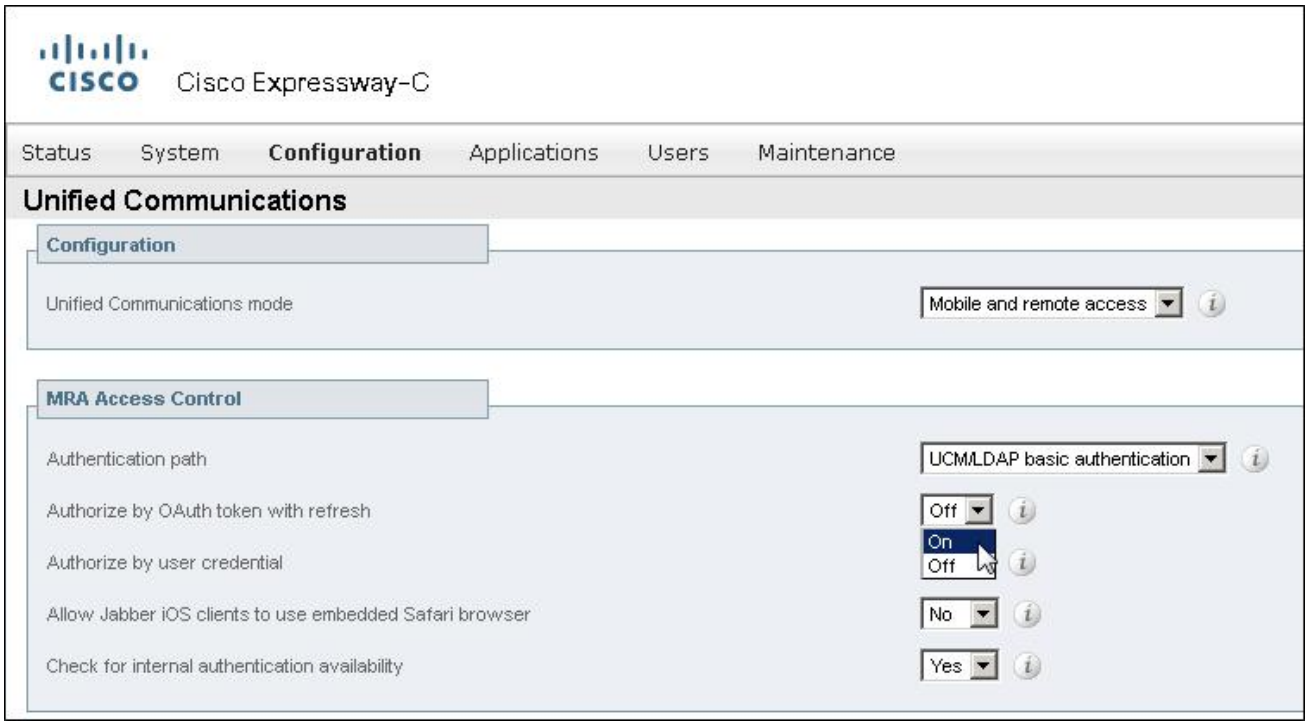
MRA アクセス ポリシーの設定を続行する前に、Expressway での更新トークンのログイン フローで OAuth を有効にする必要があります。OAuth は、MRA アクセス ポリシーを適切に導入するための前提条件になります。MRA ポリシー適用は、OAuth トークンのスコープ要素を使用して実装されます。このスコープにより、Jabber ユーザに許可されるサービスが定義されます。

5. Expressway-C での更新トークンのログイン フローによって OAuth を有効化

   WKST2（198.18.133.37）の Firefox ブラウザで https://exp-c-1.dcloud.cisco.com/ にアクセスし、ユーザ名/パスワード: **admin/dCloud123!** でログインします。

   [設定（Configuration）] > [Unified Communications] > [設定（Configuration）] に移動し、[更新時に OAuth トークンで許可（Authorize by OAuth token with refresh）] ドロップダウン メニューを [オン（On）] に設定します（図 217 を参照）。

図 217. Expressway-C：更新トークンで OAuth を有効化

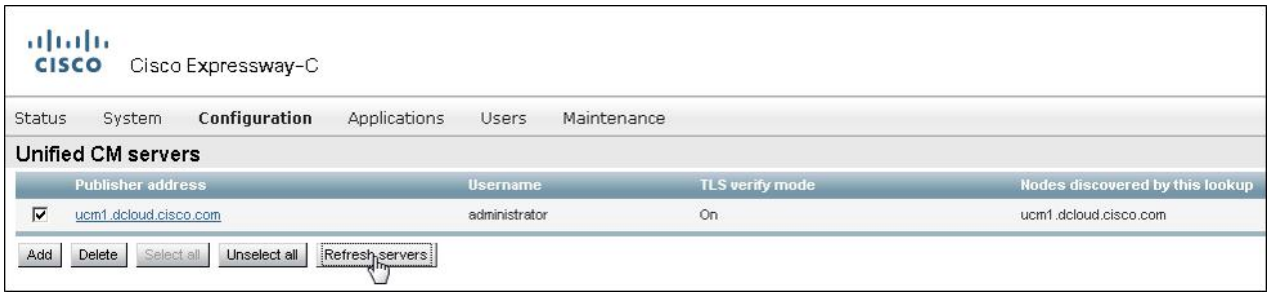


[保存（Save）] をクリックします。

注：デフォルトでは、Expressway-C で [更新時に OAuth トークンで許可（Authorize by OAuth token with refresh）] は [オン（On）] に設定されています。このラボでは、ユーザが前の「更新ログイン フローによる OAuth」モジュール（モジュール 6）を完了していない場合を考慮して、このパラメータが [オフ（Off）] に設定されていました。

次に、Unified CM パブリッシャ サーバ ノード設定を更新して、クラスタから新しい OAuth 設定を取得します。[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [Unified CM サーバ（Unified CM servers）] に移動します。図 218 に示すように、Unified CM サーバを更新します。**ucm1.dcloud.cisco.com** の横のチェックボックスをオンにして、[サーバの更新（Refresh servers）] をクリックします。

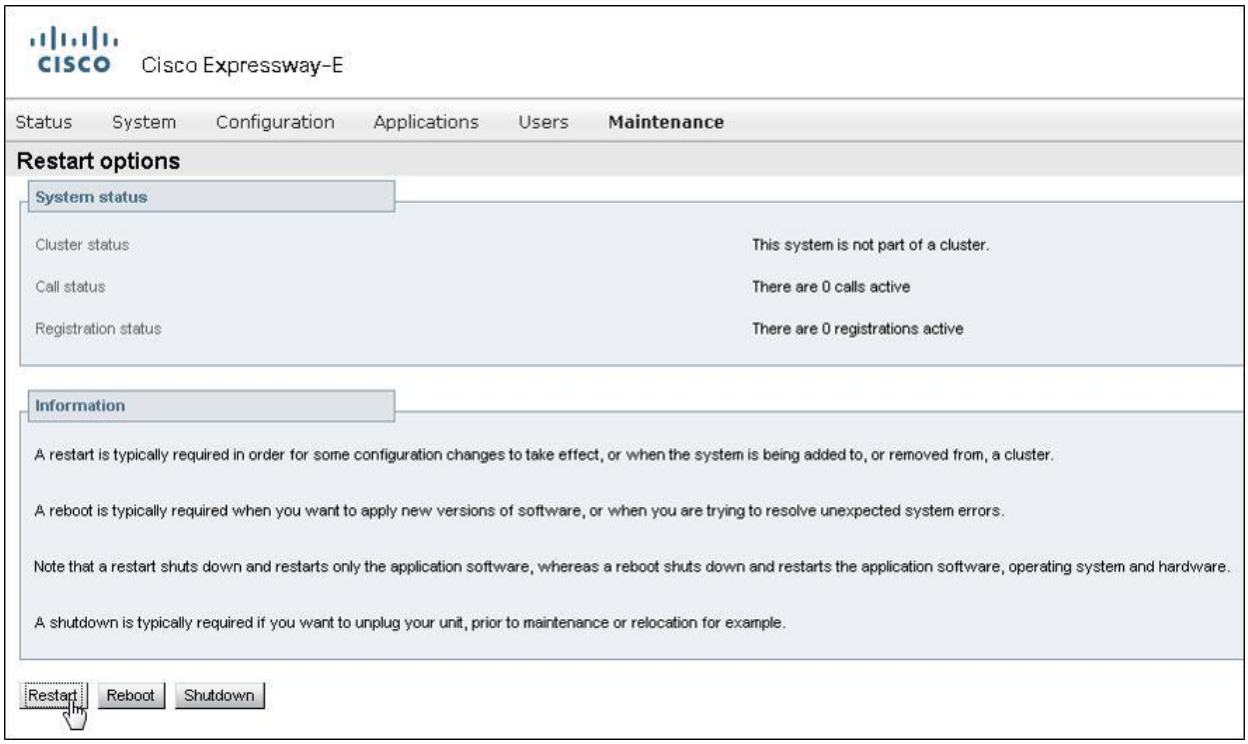
図 218. Expressway-C：Unified CM サーバの更新



最後に、Expressway-E サーバが新しい OAuth ログイン フローの処理を開始したことを確認するために、Expressway-E サーバを再起動します。

WKST2（198.18.133.37）の Firefox ブラウザで https://exp-e-1.dcloud.cisco.com にアクセスし、ユーザ名/パスワード：**admin/dCloud123!** でログインします。[メンテナンス（Maintenance）] > [再起動オプション（Restart options）] に移動します。図 219 に示すように、[再起動（Restart）] ボタンをクリックして Expressway-E サーバを再起動します。

図 219. Expressway-E：サーバの再起動



確認ウィンドウで [OK] をクリックして、再起動を続行します。この再起動は、通常 3 分以内で完了します。システムが再起動している間に、次のステップに進みます。

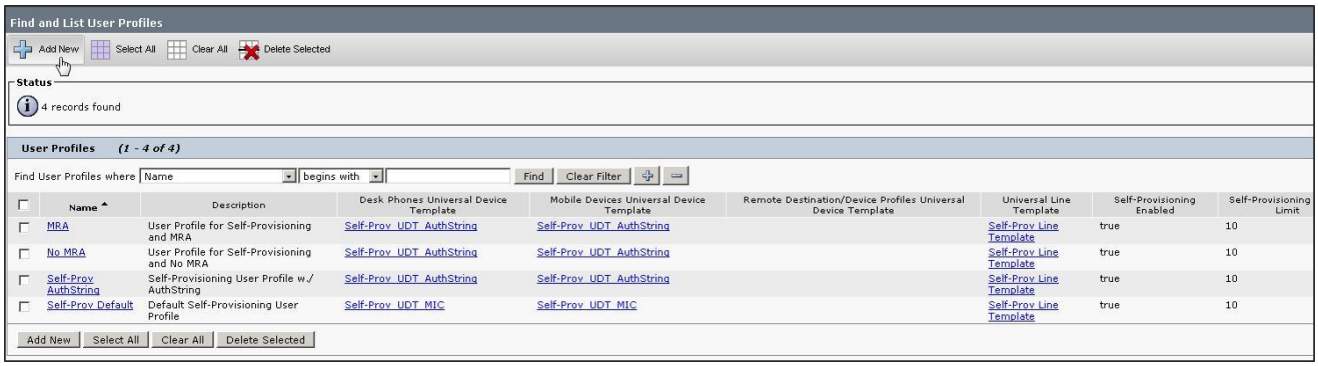
6. Unified CM の MRA アクセス ポリシーでユーザ プロファイルを設定し、ユーザ Katelyn O'Neal に適用する

MRA アクセス ポリシーは、Unified CM のユーザ プロファイル内で設定します。ユーザ プロファイルはユーザ単位で適用することも、同じユーザ プロファイルをユーザのグループに（手動または一括管理（BAT）によって）適用することもできます。

WKST2（198.18.133.37）の Firefox ブラウザで https://ucm1.dcloud.cisco.com/ccmadmin/ にアクセスし、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

ログインしたら、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）] に移動します。[検索（Find）] をクリックすると、ユーザ プロファイルのリストが表示されます。図 220 に示すように、システムにはすでに複数のプロファイルが設定されています。ここで重要なのは、[MRA] と [非 MRA（No MRA）] の 2 つのユーザ プロファイルです。これら 2 つのプロファイルによって、すべての端末 MRA が有効になるか（[MRA]）、すべての端末で MRA が無効になります（[非 MRA（No MRA）]）。

図 220. 初期の Unified CM ユーザ プロファイル リスト



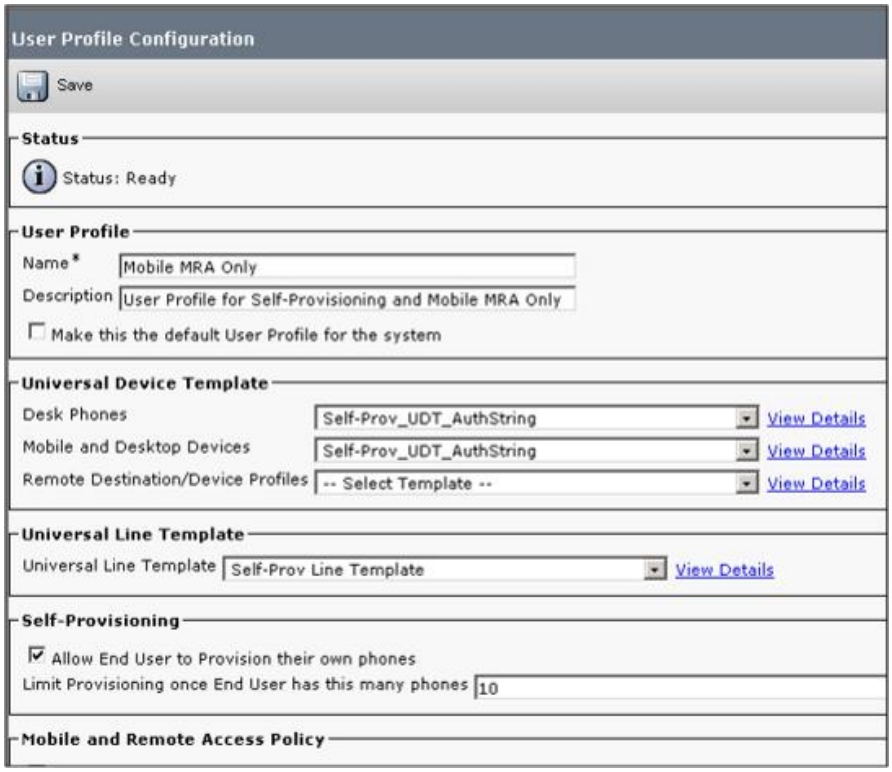
次に、Jabber モバイル クライアントについてのみ MRA を許可する、別のプロファイルを設定してみましょう。

[新規追加（Add New）] をクリックします。

図 221 に従って次のように設定します。

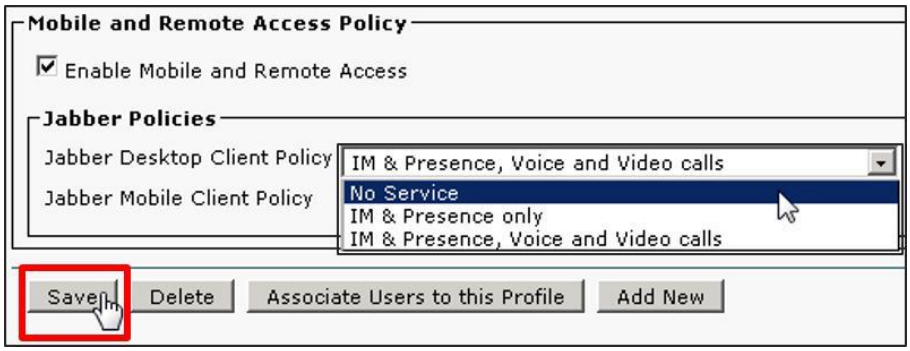
- [名前（Name）]：[モバイル MRA のみ（Mobile MRA Only）]
- [説明（Description）]：[セルフプロビジョニングとモバイル MRA 専用ユーザプロファイル（User Profile for Self-Provisioning and Mobile MRA Only）]
- [ユニバーサルデバイステンプレート（Universal Device Templates）]：
  - [デスクフォン（Desk Phones）]：[Self-Prov_UDT_AuthString]
  - [モバイルデバイスとデスクトップデバイス（Mobile and Desktop Devices）]：[Self-Prov_UDT_AuthString]
- [ユニバーサル回線テンプレート（Universal Line Template）]：[Self-Prov Line Template]
- [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）] をオンにする

図 221. モバイル MRA 専用ユーザ プロファイル



[モバイルおよびリモート アクセス ポリシー(Mobile and Remote Access Policy)] セクションでは、ユーザ プロファイルで MRA がデフォルトで有効であり、デスクトップ クライアントとモバイル クライアントの両方のポリシーで MRA のフルアクセスが有効になっていることを確認できます（[IM & Presence、音声およびビデオ通話（IM & Presence, Voice and Video calls）]）。このモバイル MRA 専用プロファイルで、[Jabber デスクトップクライアントポリシー（Jabber Desktop Client Policy）] ドロップダウン リストから [サービスなし（No Service）] を選択し、[保存（Save）] をクリックしてプロファイルを保存します（図 222 を参照）。

図 222. ユーザ プロファイル：モバイルおよびリモート アクセス ポリシー



新しいプロファイルを保存したら、[ユーザをこのプロファイルに関連付け（Associate Users to this Profile）] をクリックして、プロファイルを Katelyn O'Neal に割り当てます（図 223 を参照）。

図 223. モバイル MRA 専用ユーザ プロファイルを Katelyn O'Neal に関連付ける

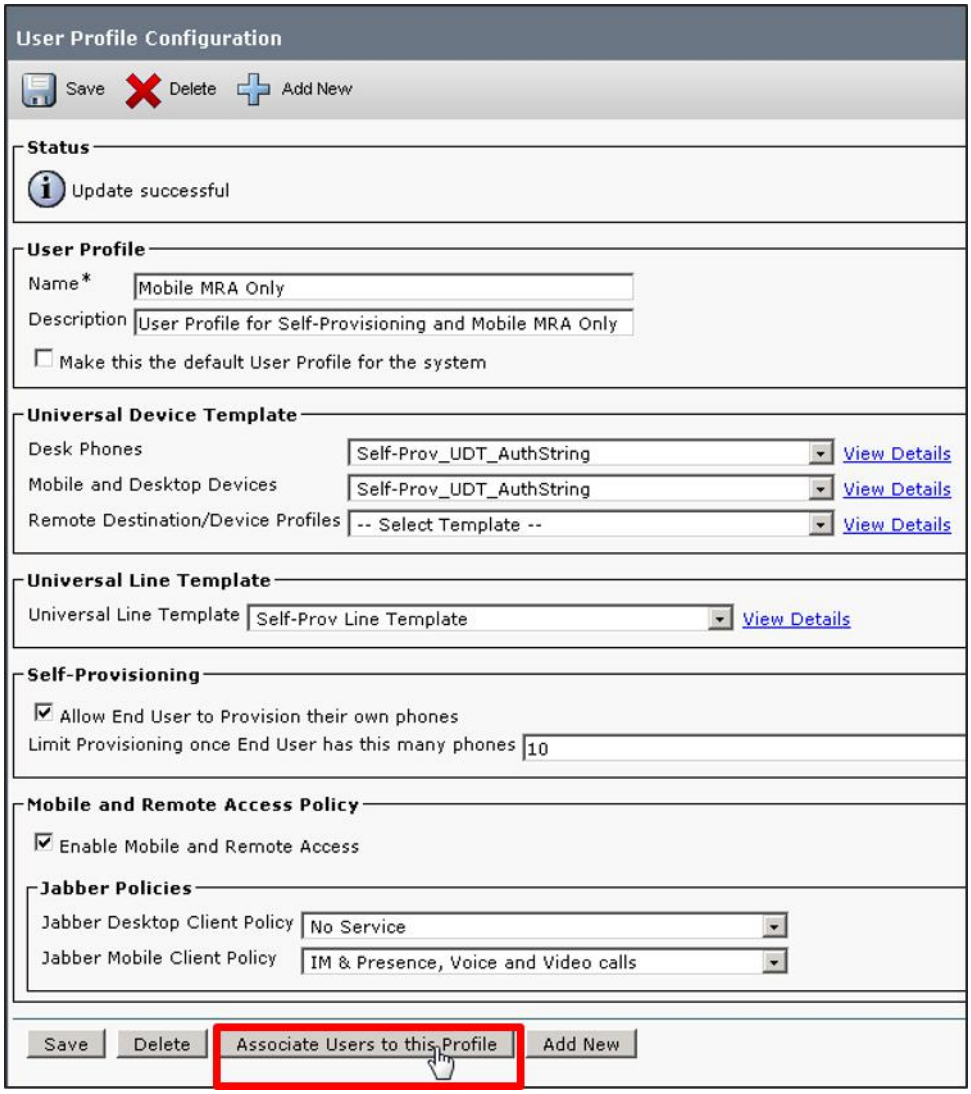


図 224 に示すように、次の画面で [ユーザの検索条件（Find User Where）] ドロップダウンから [ユーザ ID（User ID）] を選択します。[次で始まる（begins with）] フィールドに「**koneal**」と入力します。[検索（Find）] をクリックします。Katelyn O'Neal の横のチェックボックスをオンにして、[選択/変更の保存（Save Selected / Changes）] をクリックします。

図 224. Katelyn O'Neal を検索して選択

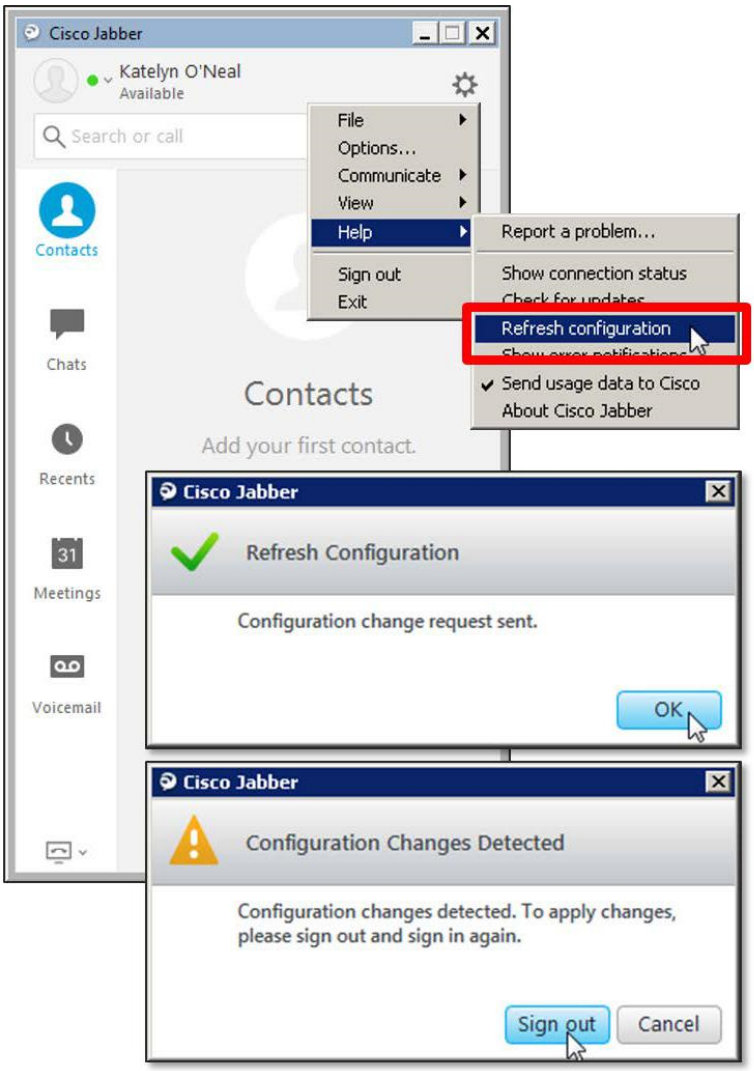
7. ユーザ Katelyn O'Neal の Windows クライアント用 Jabber が MRA 経由で接続することを制限する MRA アクセス ポリシーの確認

   モバイル MRA 専用ユーザ プロファイルをユーザに関連付けたので、次に MRA アクセス ポリシーが機能していて、Katelyn O'Neal が Windows クライアント用 Jabber から MRA 経由でログインすることを制限していることを確認します。

   ユーザ名/パスワード：DCLOUD**koneal/C1sco12345** で WKST1（198.18.2.39）に **RDP** 接続します。接続したら Jabber クライアントを起動します。前の Jabber セッションがキャッシュされているため、ユーザ名とパスワードのプロンプトが表示されることなく、自動的にログインします。証明書警告が表示された場合（例：idbroker.webex.com）は、[拒否（Decline）] をクリックします。

   クライアントがログインしたら設定を更新して、キャッシュされたセッションをクリアし、新たに OAuth 経由の認証を強制する必要があります。図 225 に示すように、**設定アイコン**をクリックして、[ヘルプ（Help）] > [設定の更新（Refresh Configuration）] を選択します。設定変更要求が送信されたことを示すダイアログが表示されます。[OK] をクリックして承認します（図 225 を参照）。続いて、サインアウトを確認して新しい設定を適用する、第 2 のダイアログが表示されます。[サインアウト（Sign out）] をクリックして確定します（図 225 を参照）。

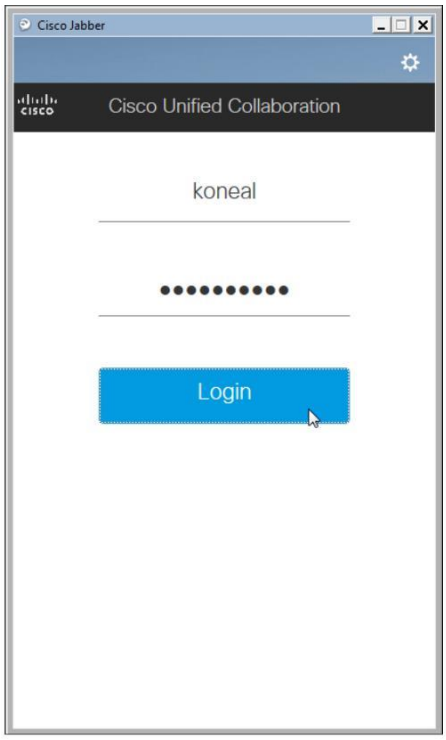
図 225. MRA Jabber クライアント用 OAuth：初期の接続失敗および設定更新の要求



注：図 225 に示すダイアログが両方表示されないか、1 つのダイアログが別のダイアログに重なって表示される場合があります。場合によっては、ダイアログが 1 つしか表示されないこともあります。これは最終的に、WKST1 で Jabber クライアントがログアウトしてから経過した時間によって異なります。

ログアウトが完了したら、[サインイン（Sign In）] ボタンをクリックして新しいログインをトリガーします。OAuth 認証画面で、ユーザ名/パスワード：**koneal/C1sco12345** を入力します（図 226 を参照）。

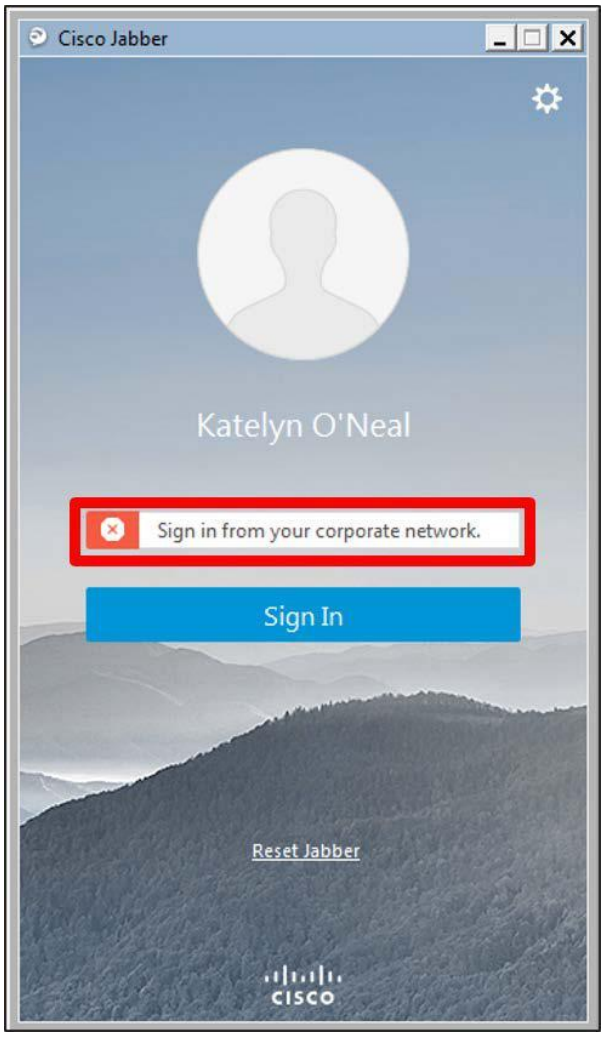
図 226. MRA Jabber クライアント（CSFKONEAL）の OAuth ログイン



注：場合によっては [サインイン（Sign In）] ボタンが表示され、クリックすることで OAuth プロンプトが最初に表示されることがあります。

Jabber クライアントのログインが失敗し、クライアントが接続されません。代わりに、「社内ネットワークからサインイン（Sign in from your corporate network）」というメッセージが表示されます（図 227 を参照）。これは、適用した MRA アクセス ポリシー（モバイル MRA 専用）によって、WKST1 でリモートの Windows クライアント用 Jabber が MRA 経由でアクセスすることが妨げられていることを示します。

図 227. MRA アクセス ポリシー：Windows デスクトップ クライアント用 Jabber の接続エラー



次に、MRA アクセス ポリシーを更新して、リモートの Windows クライアント用 Jabber が MRA 経由で接続することを許可します。図 227 に示すように、サインイン画面で Jabber クライアントを終了します。MRA ポリシーを更新した時点でサインインに戻ります。

8. Katelyn O'Neal のユーザ プロファイルを更新して、Windows クライアント用 Jabber が MRA 経由でアクセスすることを許可する

   Unified CM 管理インターフェイス（https://ucm1.dcloud.cisco.com/ccmadmin/）に戻ります。必要に応じて、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

   ログインしたら、[ユーザ管理（User Management）] > [エンドユーザ（End User）] に移動します。[検索（Find）] をクリックして、システム内のすべてのエンド ユーザのリストをロードします。

   次に、リスト内で Katelyn O'Neal のエントリを見つけ、ユーザ ID の **koneal** をクリックします。[エンドユーザ設定（End User Configuration）] ページで、[ユーザプロファイル（User Profile）] ドロップダウン リストから [MRA] を選択します（図 228 を参照）。

図 228. Katelyn O'Neal のユーザ プロファイル設定

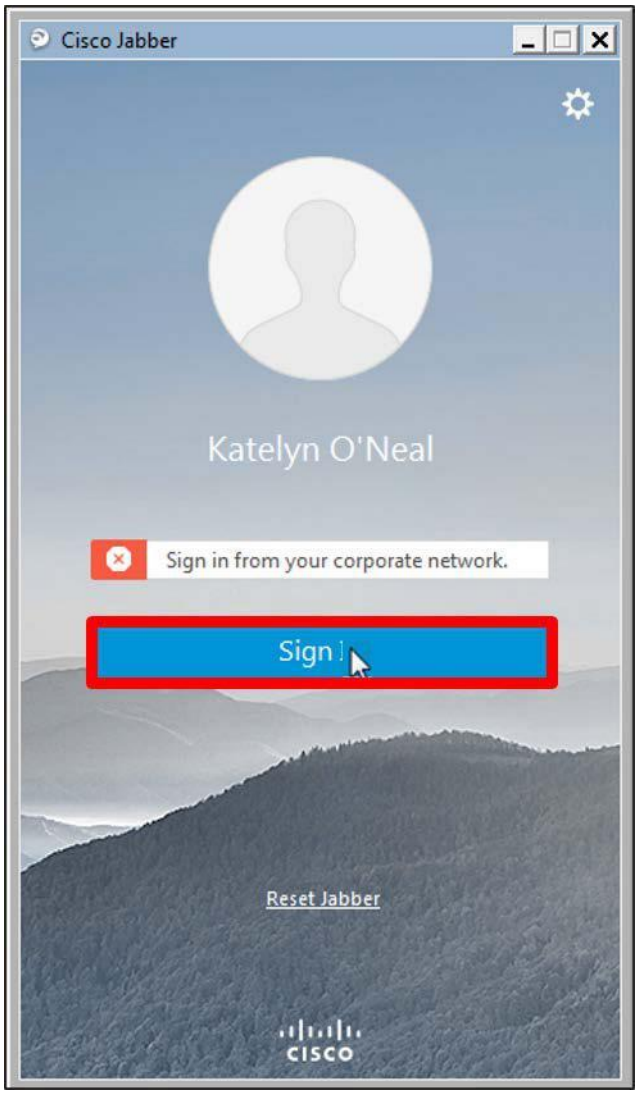
MRA ユーザ プロファイルによってモバイルおよびリモート アクセスが可能になり、Jabber デスクトップ クライアント ポリシーと Jabber モバイル クライアント ポリシーの両方で、フルセットのサービス（IM & Presence、音声およびビデオ通話）が許可されます。

[MRA] を選択し、[保存（Save）] をクリックしてユーザ アカウントを更新します。

Katelyn O'Neal の MRA ユーザ プロファイルを設定し、Jabber デスクトップ クライアント接続が許可されたので、WKST1 でリモートの Windows クライアント用 Jabber が MRA 経由で接続可能になったことを確認します。

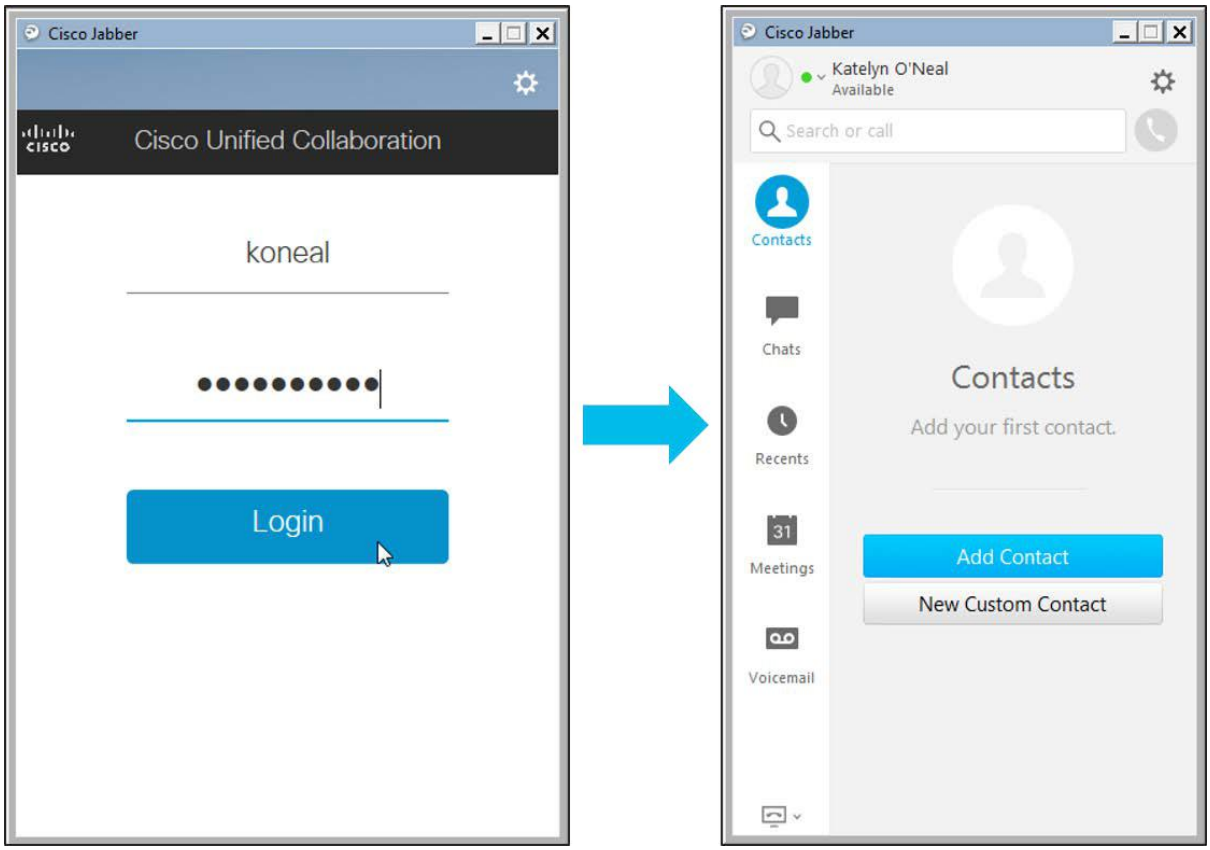
WKST1（198.18.2.39 に RDP 接続）に戻り、[サインイン（Sign In）] をクリックします（図 229 を参照）。

図 229. リモートの Windows 用 Jabber で再度サインイン



OAuth プロンプトで、再度ユーザ名/パスワード：**koneal/C1sco12345** を入力してログインします（図 230 を参照）。Jabber クライアントが MRA 経由で接続して登録されたことを確認します（図 230 を参照）。

図 230. Jabber MRA OAuth のログインと MRA アクセス ポリシー



D. MRA を経由した Unity Connection ボイスメール システム宛通話のエンドツーエンドの暗号化

このセクションでは、Expressway MRA 経由で接続した Jabber エンドポイントが、エンドツーエンドで暗号化された通話を Unity Connection ボイスメール システムに送信できることを検証します。

注: モジュールのこのセクションを完了するには、モジュール 8（次世代暗号化によるセキュアなボイスメール）を完了している必要があります。リモート Jabber クライアントと Unity Connection ボイスメール システム間のセキュアなエンドツーエンドの暗号化を検証するには、MRA 接続が必要です。

9. MRA に接続された Jabber と Unity Connection 間のエンドツーエンドの暗号化を確認する

   WKST1（198.18.2.39、DCLOUD**koneal**/**C1sco12345**）の Jabber クライアントに戻ります。必要に応じてクライアントに再度ログインします（ユーザ名/パスワード：**koneal**/**C1sco12345**）。

   Jabber クライアントが登録されたら、ボイスメール システムに発信します。[ボイスメッセージ（Voice Messages）] タブで、[ボイスメールに発信（Call Voicemail）] をクリックします。ここでは、メッセージ待機通知の受信後に発信者がメッセージを取得するところをモデリングしています。

   通話がボイスメール システムのパイロット（2010）に接続すると、Cisco Jabber に、ボイスメール システムに対する通話が暗号化されていることを示すアイコンが表示されます（図 231 を参照）。

図 231. MRA 接続された Jabber クライアントからの、Unity Connection に対する暗号化されたセキュアなボイスメール取得通話

続行する前に、通話を終了し、WKST1 で Windows クライアント用 Jabber を終了して、開いているブラウザ セッションを閉じます。

***** モジュール #9 の終了 *****

モジュール 10.Cisco Meeting Server によるセキュアな会議

モジュールの概要

このモジュールでは、Cisco Meeting Server の証明書を管理し、Unified CM との暗号化された統合を設定し、事前設定された固定スペースと Unified CM に登録されたアドホック会議用会議ブリッジによって、暗号化された会議を検証します。このモジュールは、次の 6 つのセクションに分割されています。

A. Cisco Meeting Server の証明書の管理

B. Cisco Meeting Server の設定

C. Cisco Meeting Server 用の Unified CM セキュア SIP トランクの設定

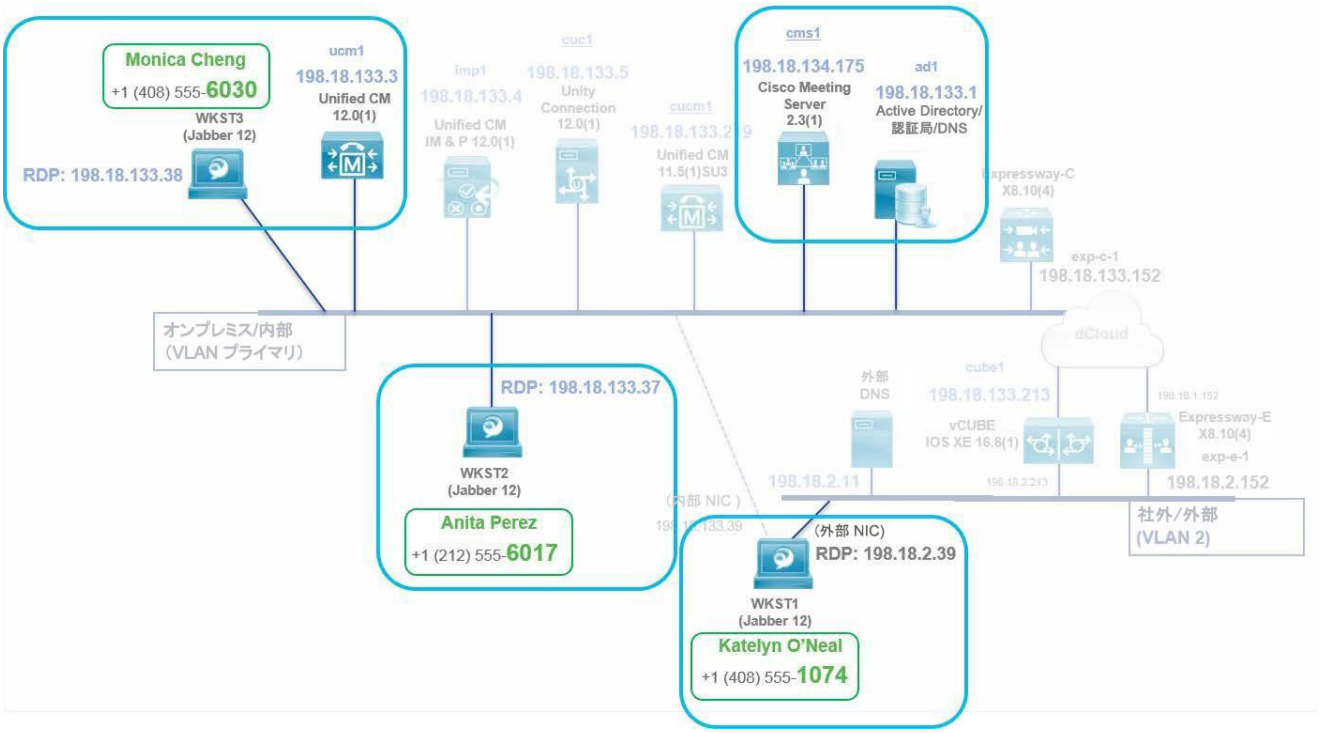
D. Cisco Meeting Server による暗号化されたセキュアな会議を確認する

E. Cisco Meeting Server による暗号化されたセキュアなアドホック会議を設定する

F. Cisco Meeting Server による暗号化されたセキュアなアドホック会議を確認する

次の図 232 は、このモジュールのトポロジおよび関連するコンポーネントを示しています。

図 232. モジュール 10：Cisco Meeting Server Topology によるセキュアな会議



手順

A. Cisco Meeting Server の証明書の管理

このセクションでは、Cisco Meeting Server の証明書を管理します。

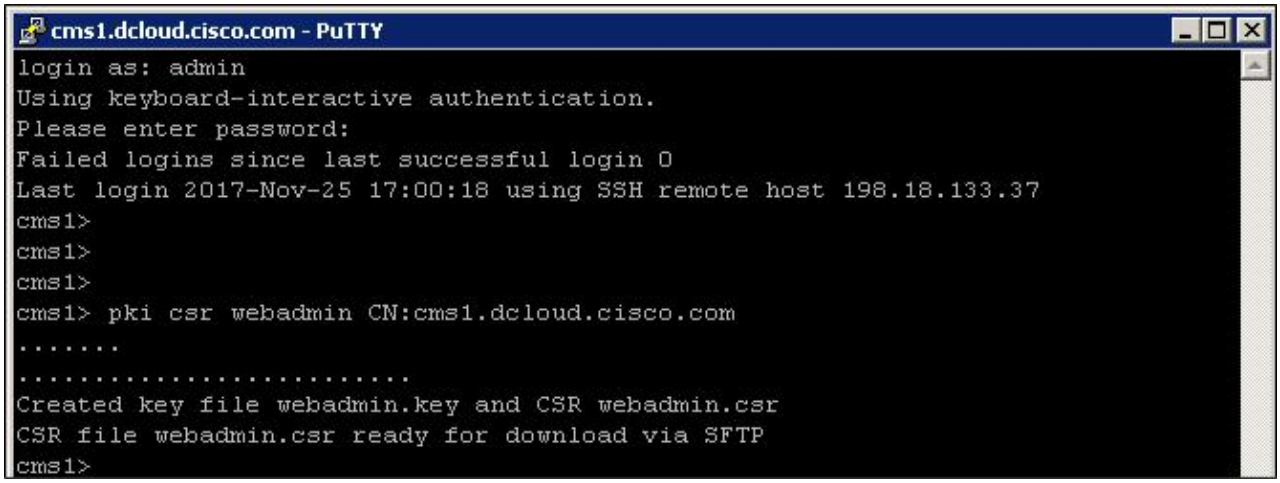
1. Cisco Meeting Server の CSR を生成し、エンタープライズ CA で署名する

   WKST2（198.18.133.37 に RDP 接続 – **DCLOUD\aperez/C1sco12345**）で PuTTY クライアントを使用し、cms1.dcloud.cisco.com（198.18.134.175）に SSH で接続します。プロンプトが表示されたら、[はい（Yes）] をクリックしてホストキーをキャッシュします（図 233 を参照）。

   図 233. SSH キーのキャッシュに関する警告

   ユーザ名/パスワード：**admin/dCloud123!** でログインします。ログインしたら、図 234 に示すように、コマンド プロンプトで **pki csr webadmin CN:cms1.dcloud.cisco.com** と入力して、サーバ CSR を生成します。

   図 234. Cisco Meeting Server：証明書署名要求（CSR）の生成



   次に、WKST2（198.18.133.37 に RDP 接続 - **DCLOUD\aperez/C1sco12345**）のタスクバーの WinSCP クライアントをクリックします（図 235 を参照）。

   図 235. Cisco Meeting Server のファイルにアクセスするために WinSCP を起動

ユーザ名/パスワード：**admin/dCloud123!** を使用して、cms1.dcloud.cisco.com に対する SFTP セッションを開きます（図 236 を参照）。

図 236. WinSCP：Cisco Meeting Server への SFTP セッションを開始

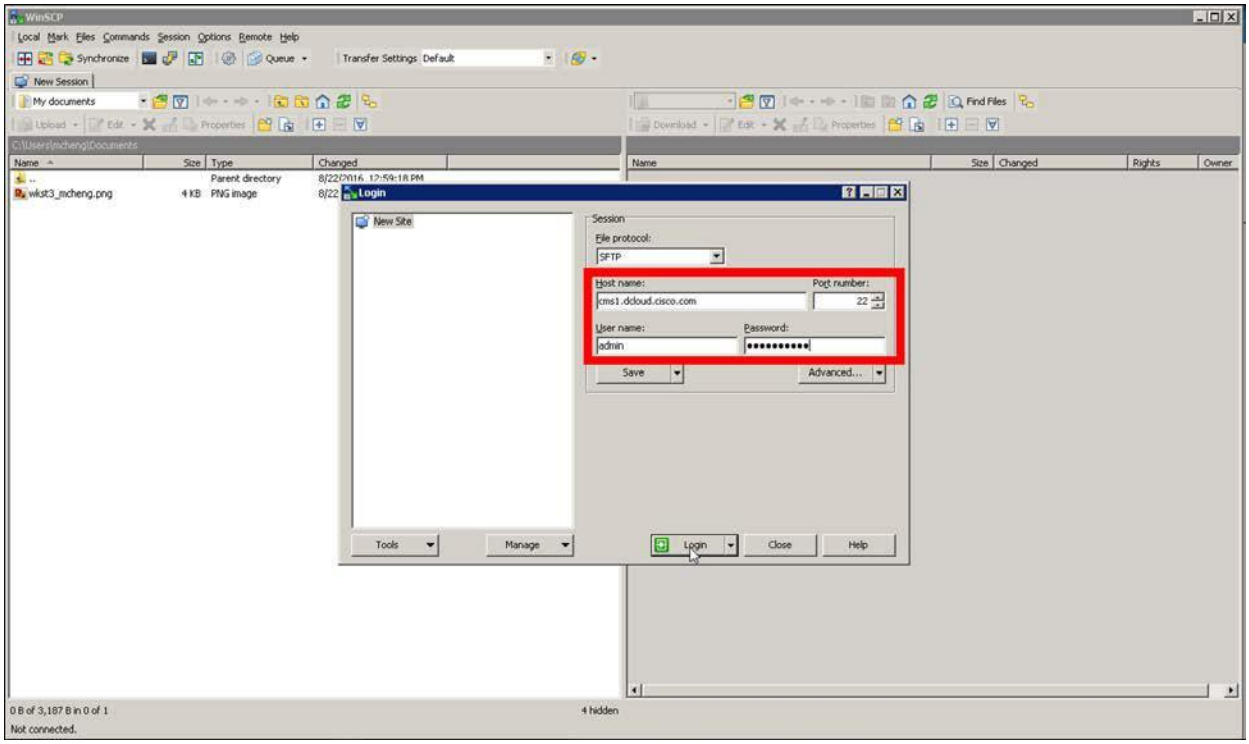


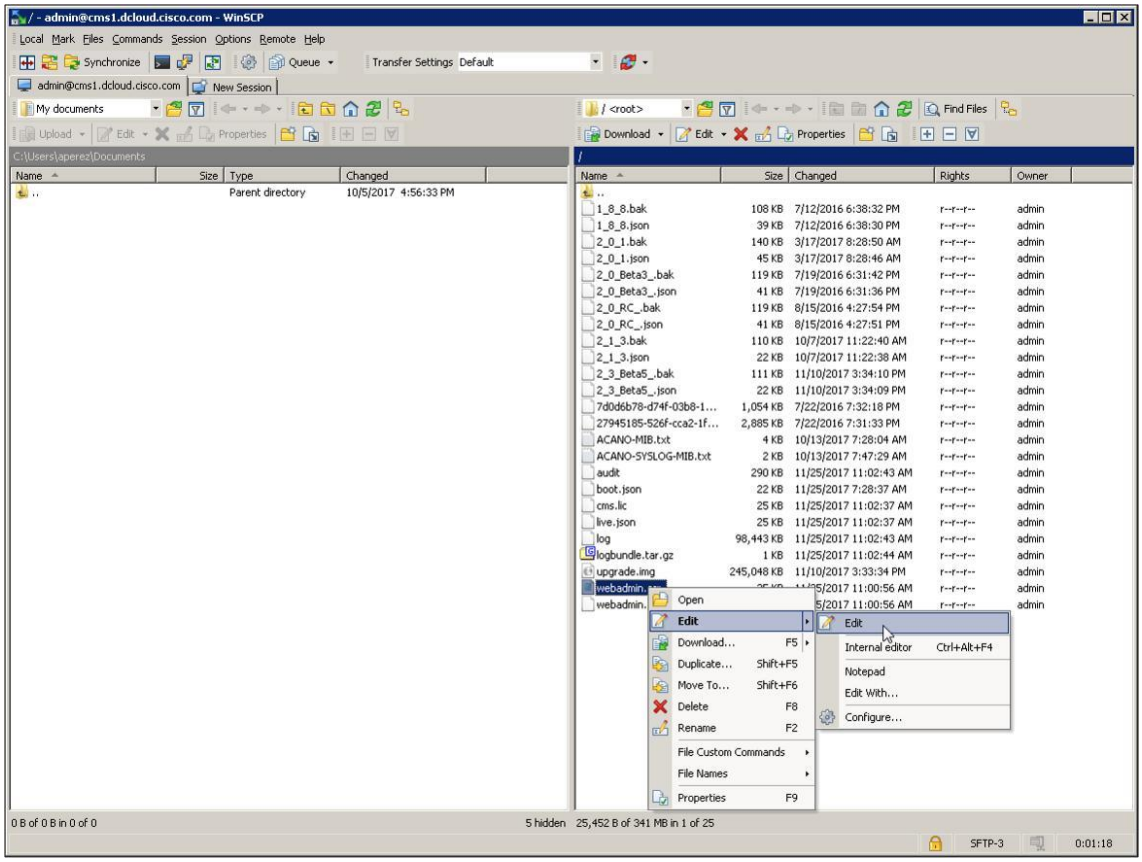
図 237 に示すように [はい（Yes）] をクリックして、Cisco Meeting Server ホストキーをキャッシュし、ログインします。

図 237. WinSCP：Cisco Meeting Server ホスト キーをキャッシュ

接続すると、右側のファイル リスト ウィンドウに新しく生成された CSR ファイル（**webadmin.csr**）が表示されています。

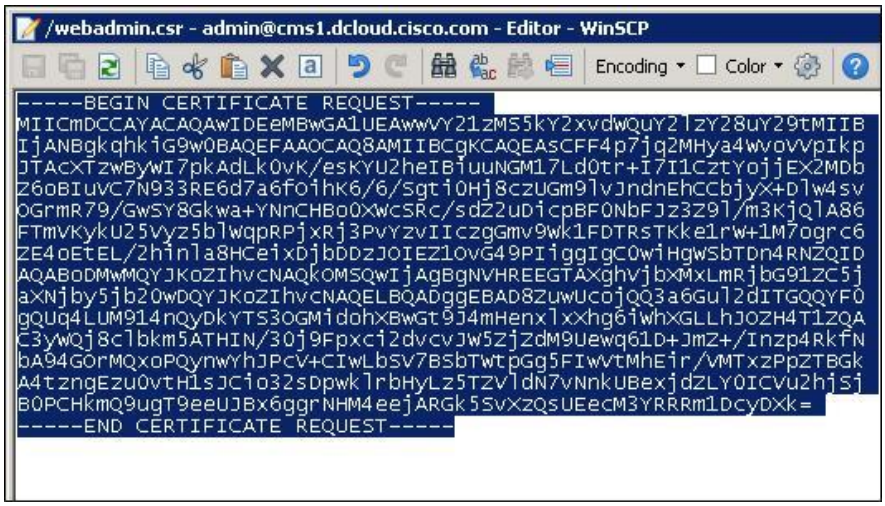
webadmin.csr ファイルを右クリックし、[編集（Edit）] > [編集（Edit）] の順に選択し、CSR ファイルを開きます（図 238 を参照）。

図 238. webadmin.csr 証明書署名要求（CSR）を開く



ワードパッドで CSR を開いて CSR のテキストをコピーし、それを使用して、ラボのエンタープライズ CA で署名付き証明書を要求します（図 239 を参照）。

図 239. Cisco Meeting Server の webadmin CSR の内容をコピー



ラボのエンタープライズ CA（https://ad1.dcloud.cisco.com/certsrv）に移動し、ユーザ名/パスワード：**administrator/C1sco12345** でログインします。ログインしたら、図 240 に示すように、[証明書を要求する（Request a certificate）] リンクをクリックします。次の画面で [または詳細証明書要求を送信する（Or, submit an advanced certificate request）] リンクをクリックします。

図 240. エンタープライズ CA で署名付き証明書を要求

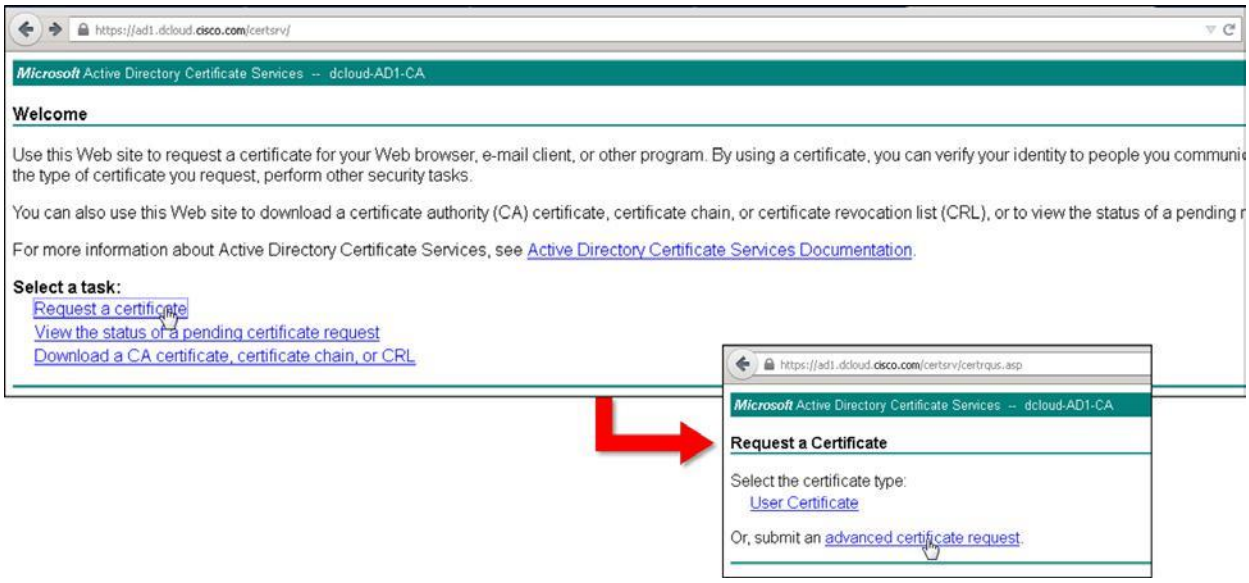
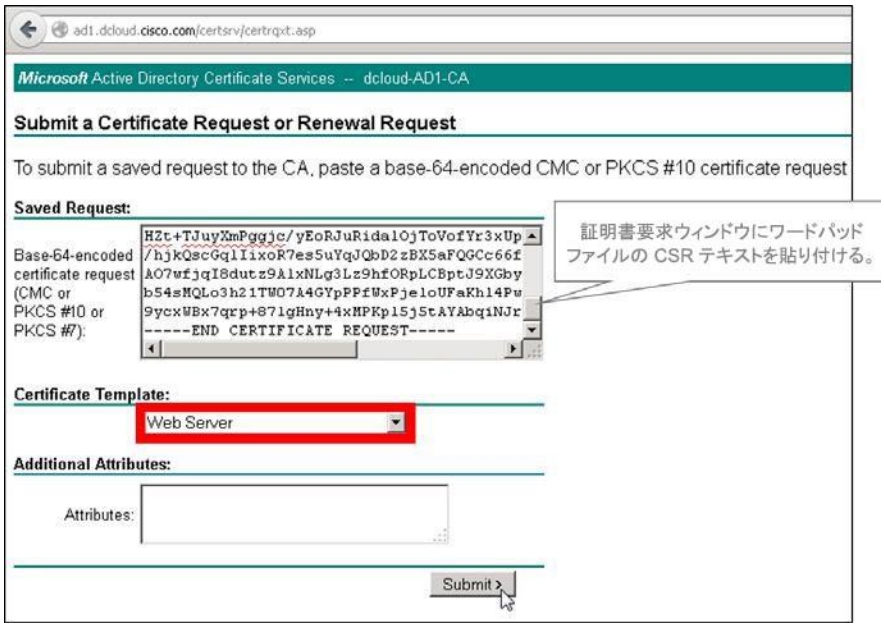


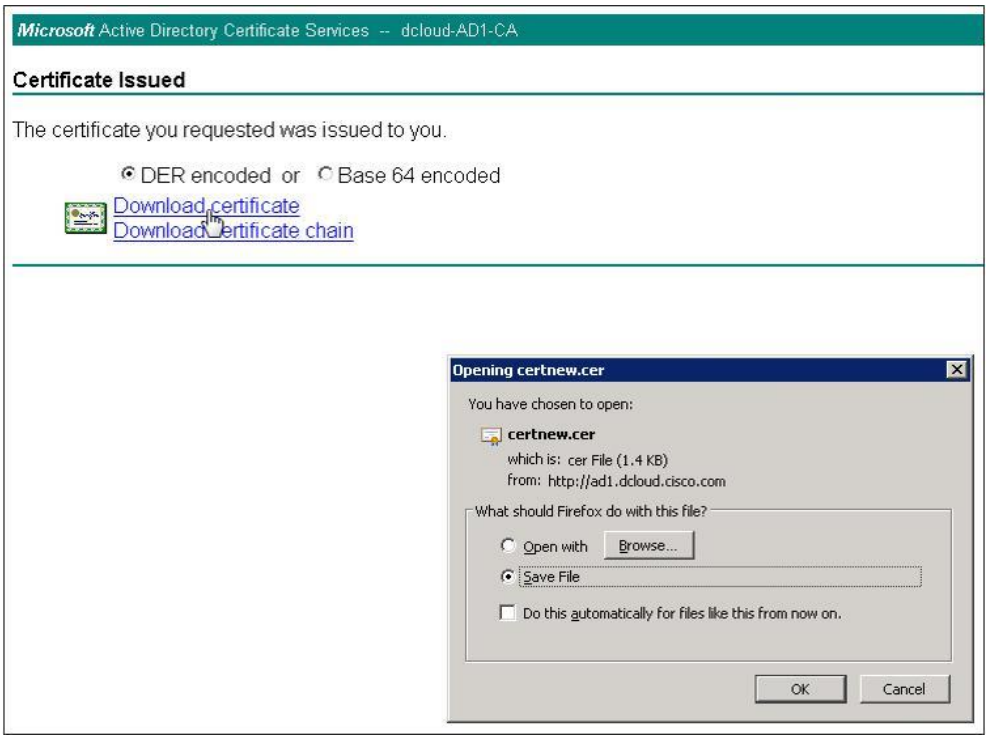
図 241 に示すように、webadmin.csr の CSR テキストを、[保存済み要求（Saved Request）] ウィンドウに貼り付けます。[証明書テンプレート（Certificate Template）] ドロップダウン リストから [Web サーバ（Web Server）] を選択し、[送信>（Submit >）] をクリックします。

図 241. エンタープライズ CA 証明書の署名：webadmin.cer



次の画面では、図 242 に示すように、エンコーディング設定は [DER でエンコード（DER encoded）] のままにし、[証明書をダウンロード（Download certificate）] をクリックします。[ファイルの保存（Save File）] を選択して [OK] をクリックし、ファイルをローカル ワークステーションに保存します。ファイルに「**webadmin.cer**」という名前を付けます。

図 242. 署名付き Webadmin 証明書の保存

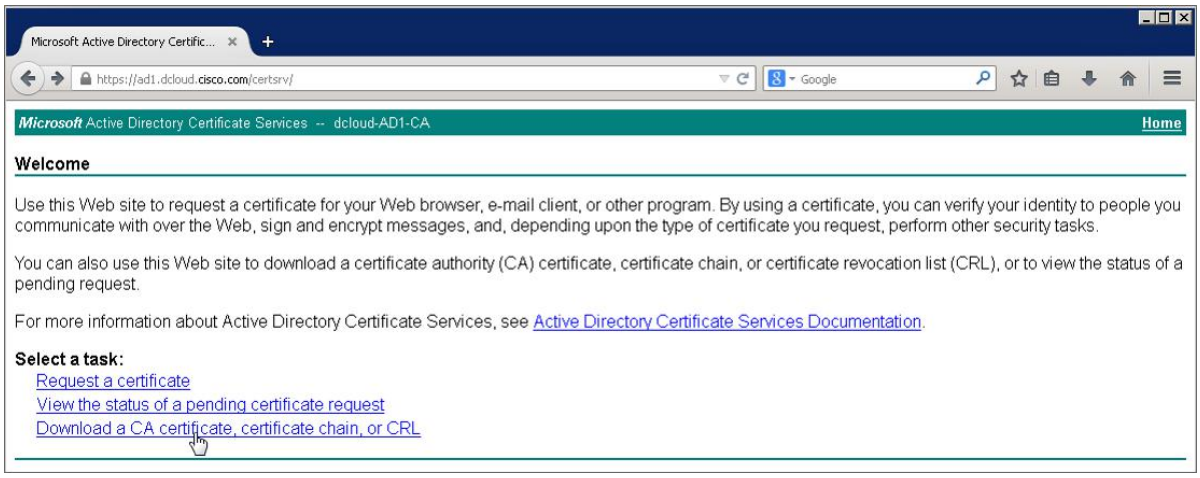


2. エンタープライズ CA ルート証明書をダウンロードする

前のモジュールですでにエンタープライズ CA 証明書をダウンロードしているかもしれませんが、その証明書は Base 64 形式になっている可能性があります。Cisco Meeting Server では DER 形式にする必要があります。

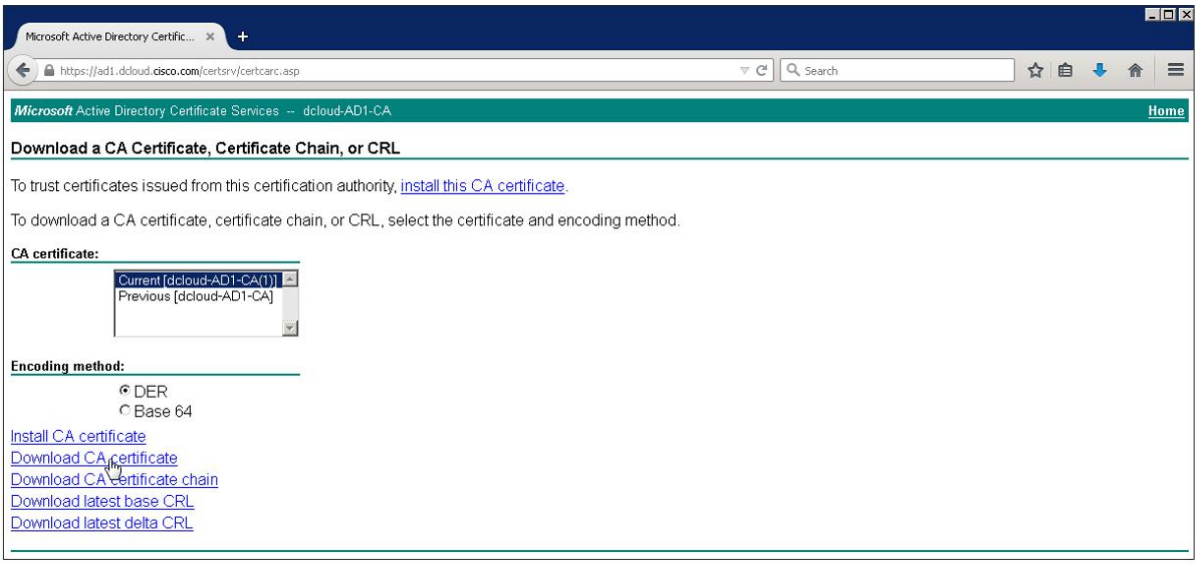
エンタープライズ CA から離れる前に、https://ad1.dcloud.cisco.com/certsrv/ に戻り（右上隅の [ホーム（Home）] リンクをクリック）、図 243 に示すように [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

図 243. エンタープライズ CA 証明書のダウンロード（1/2）



次の画面では [現在の[dcloud AD1 CA]（Current [dcloud-AD1-CA]）] がデフォルトで選択されており、[エンコード方式（Encoding method）] には、[DER] がデフォルトで設定されています。[CA 証明書のダウンロード（Download CA certificate）] をクリックします（図 244 を参照）。

図 244. エンタープライズ CA 証明書のダウンロード（2/2）



注：CA 証明書をダウンロードする前に、現在の CA 証明書（[現在の[dcloud-AD1-CA(1)]（Current [dcloud-AD1-CA(1)]）]）が選択されていることを確認してください。これは、前の CA 証明書に代わる新しい CA 証明書です。

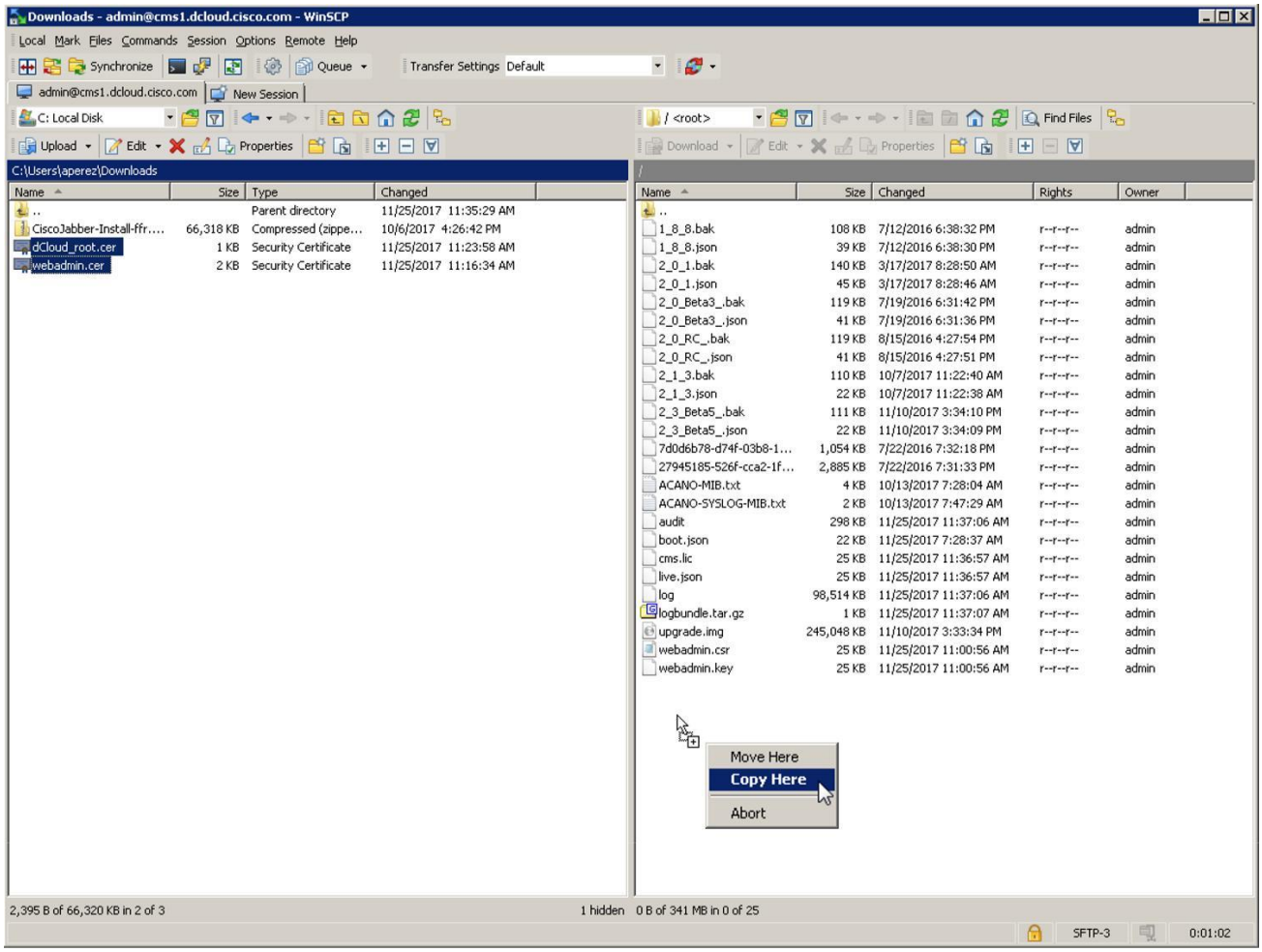
[ファイルの保存（Save File）] を選択し、[OK] をクリックします。ファイルに **dCloud_root.cer** という名前をつけ、[保存（Save）] をクリックしてローカル ワークステーションに保存します。

3. Web Admin および Call Bridge 用の CA 署名付き証明書とエンタープライズ CA ルート証明書をアップロードする

   WKST2 の WinSCP クライアントに戻ります（198.18.133.37 に RDP 接続 - **DCLOUD\aperez/C1sco12345**）。必要に応じて、ユーザ名/パスワード：**admin/dCloud123!** で cms1.dcloud.cisco.com にログインします。ウィンドウの左側で C:\Users\aperez\Downloads（ローカル ディスク）に移動します。

   直近にダウンロードした CA 署名付き証明書（**webadmin.cer**）と CA ルート証明書（**dCloud_root.cer**）をウィンドウの右側にドラッグアンド ドロップして Cisco Meeting Server のファイル システムにコピーします。図 245 に示すように、[ここにコピー（Copy Here）] を選択して、ファイルをコピーします。

図 245. Cisco Meeting Server ファイル システムに CA 署名付き証明書と CA ルート証明書をコピー



次のダイアログで [OK] をクリックして、ファイルを Cisco Meeting Server にコピーします。両方の証明書が右側のペインに表示されることを確認してから次に進みます。

4. CA 署名付き証明書を Web 管理インターフェイスに適用し、検証する

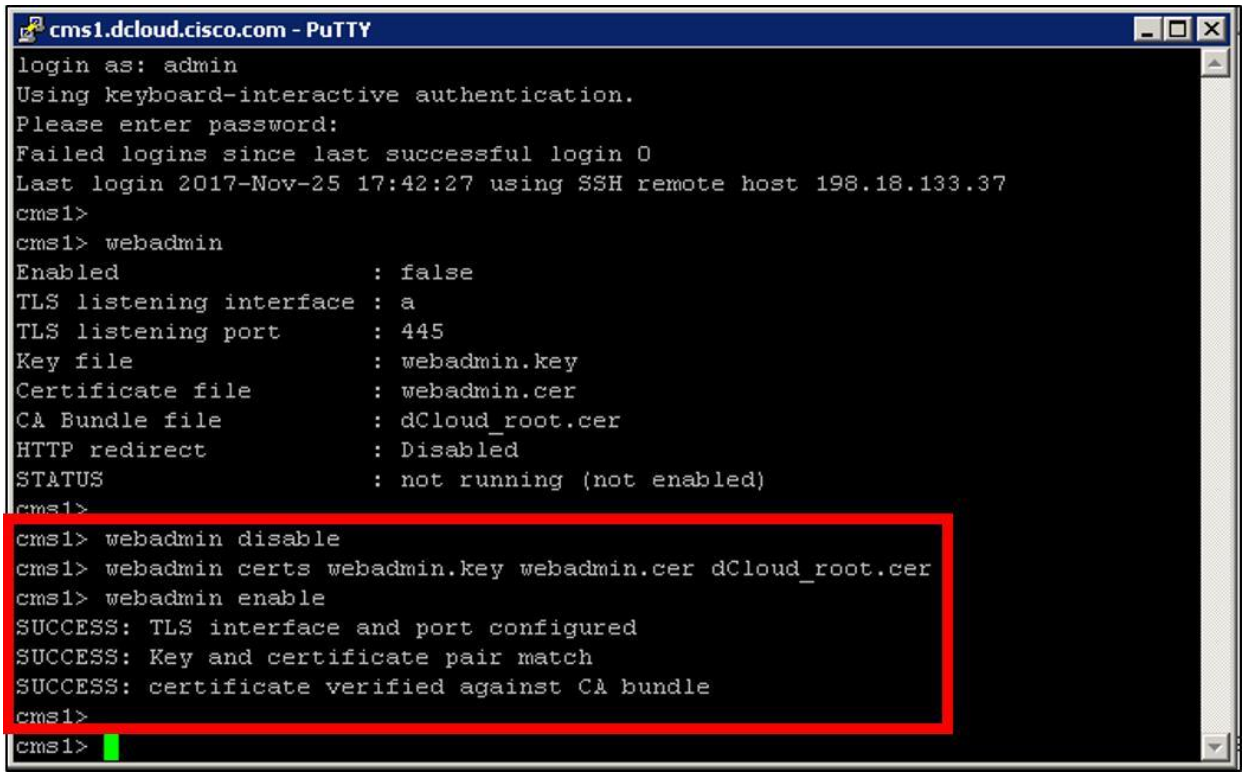
ここで、新しいエンタープライズ CA 署名付き証明書を使用して Cisco Meeting Server の Web 管理インターフェイスを有効化してみましょう。WKST3 で PuTTY クライアントを使用して Cisco Meeting Server（cms1.dcloud.cisco.com）に SSH 接続し、ユーザ名/パスワード：**admin/dCloud123!** でログインします。認証されたら、以下のコマンドを利用して、新しい CA 署名付き証明書と CA ルート証明書を Web 管理サービスに関連付けます。

```
webadmin disable
webadmin certs webadmin.key webadmin.cer

dCloud_root.cer webadmin enable
```

図 246 に、ログインした CLI で webadmin サービスを確認し、上記のコマンドを入力してコンソールに結果が返ってきた状況を示しています。

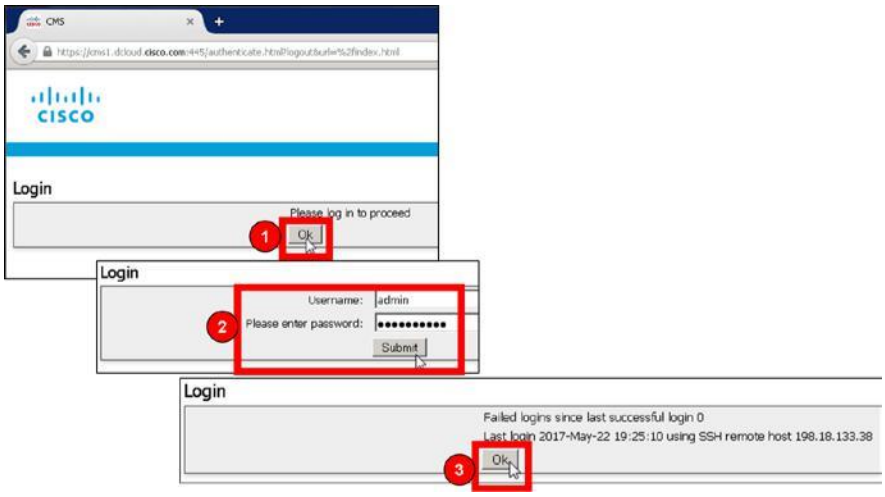
図 246. Cisco Meeting Server CLI：CA 署名付き証明書と CA ルート証明書を Web 管理サービスに関連付ける



Cisco Meeting Server の管理 Web インターフェイス（https://cms1.dcloud.cisco.com:445/）にアクセスすることで、証明書が正常に関連付けられていることを確認できます。

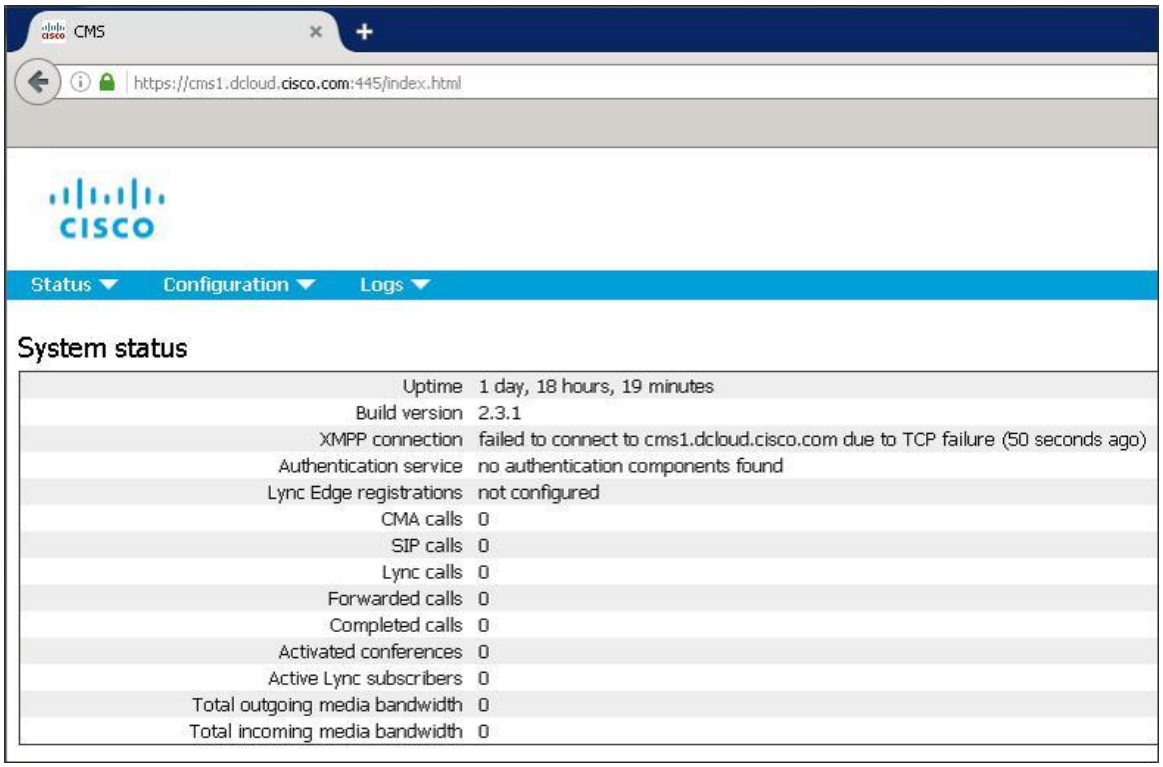
図 247 に示すように、[OK] をクリックし、ユーザ名/パスワード：**admin/dCloud123!** を入力してログイン後、[送信（Submit）] をクリックします。最後に、[OK] をクリックしてログインが成功したことを確認します。

図 247. Cisco Meeting Sever Web 管理ポータルへのログイン



ログインすると、[システムステータス（System status）] ページが表示され、Cisco Meeting Server に Web サーバ証明書が導入されたことを確認できます（図 248 を参照）。

図 248. ログイン後の Cisco Meeting Server の Web 管理インターフェイス



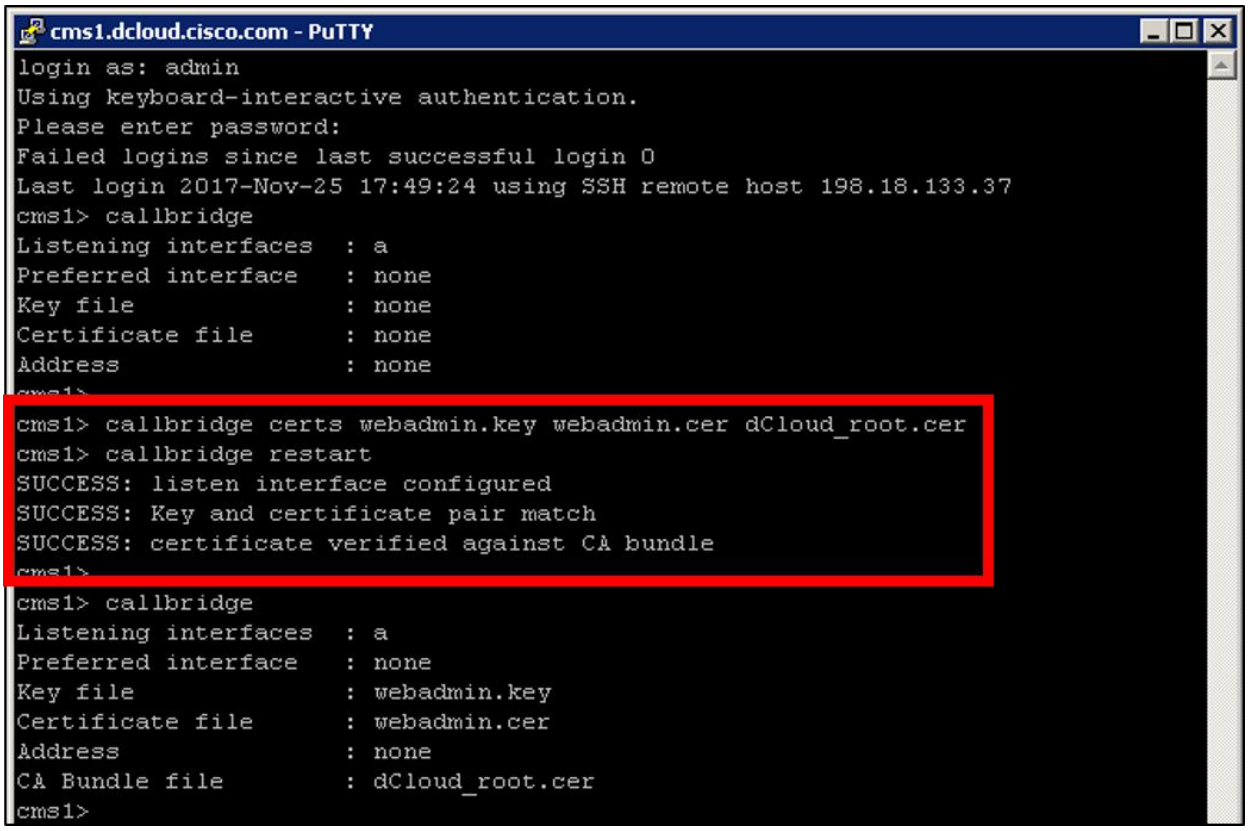
5. CA 署名付き証明書を Call Bridge サービス インターフェイスに適用する

次に、SSH で Cisco Meeting Server CLI インターフェイスに戻り、Call Bridge サービス インターフェイスに CA 署名付き証明書を関連付けます。同じ Web 管理用 CA 署名付き証明書を使用して、Call Bridge サービスを保護します。次のコマンドで Web 管理用 CA 署名付き証明書を Call Bridge サービスに関連付けます。

```
callbridge certs webadmin.key webadmin.cer
dCloud_root.cer callbridge restart
```

図 249 に、ログインした CLI で Call Bridge サービスを確認し、上記のコマンドを入力してコンソールに結果が返ってきた状況を示しています。

図 249. Cisco Meeting Server CLI：CA 署名付き証明書と CA ルート証明書を Call Bridge サービスに関連付ける



B. Cisco Meeting Server 設定

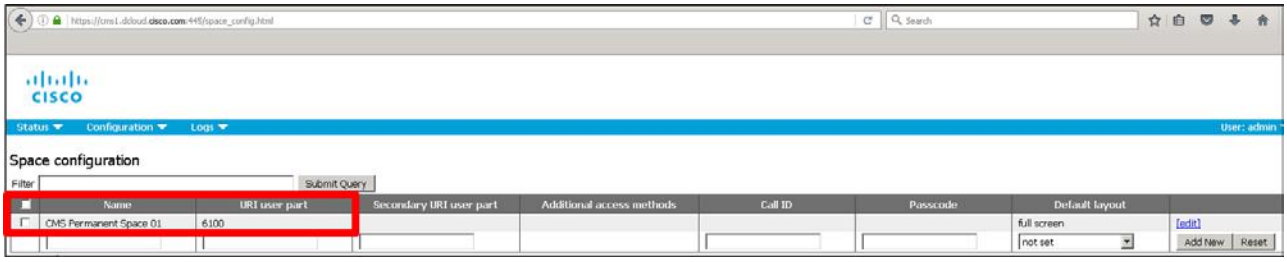
次に、永続的なミーティング スペースの設定を確認し、Cisco Meeting Server で通話の暗号化を有効にします。

6. 永続的なミーティング スペースの設定を確認する

   エンタープライズ CA 署名付き証明書を関連の Cisco Meeting Service インターフェイスに適用しましたので、Web インターフェイス（https://cms1.dcloud.cisco.com:445/）に戻り、必要に応じて再度ログインします（**admin/dCloud123!**）。永続的なミーティング スペースは、システムですでに設定されているため、[設定（Configuration）] > [スペース（Spaces）] に移動して設定を確認します。

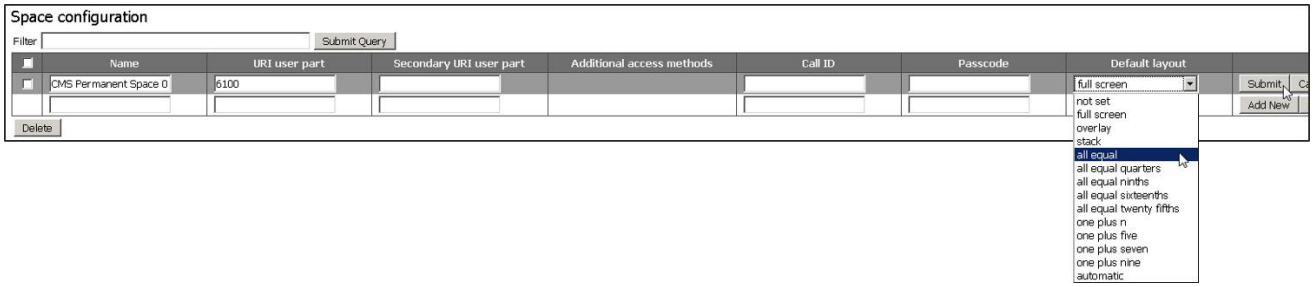
   図 250 に示すように、永続的なミーティング スペース（**CMS Permanent Space 01**、URI：**6100**（スペースの電話番号（DN）に対応））は、すでに設定されています。6100 は、このスペースに接続する際にエンドポイントからダイヤルする番号です。

図 250. Cisco Meeting Server：永続的なスペースの設定の確認（CMS Permanent Space 01）



先に進む前に、右側の [[編集]([edit])] をクリックしてスペースの設定を編集します。図 251 に示すように、さまざまなレイアウトオプションがあります。[デフォルトレイアウト(Default Layout)] ドロップダウン メニューから [すべて均等(all equal)] を選択し、[送信>(Submit >)] をクリックします。

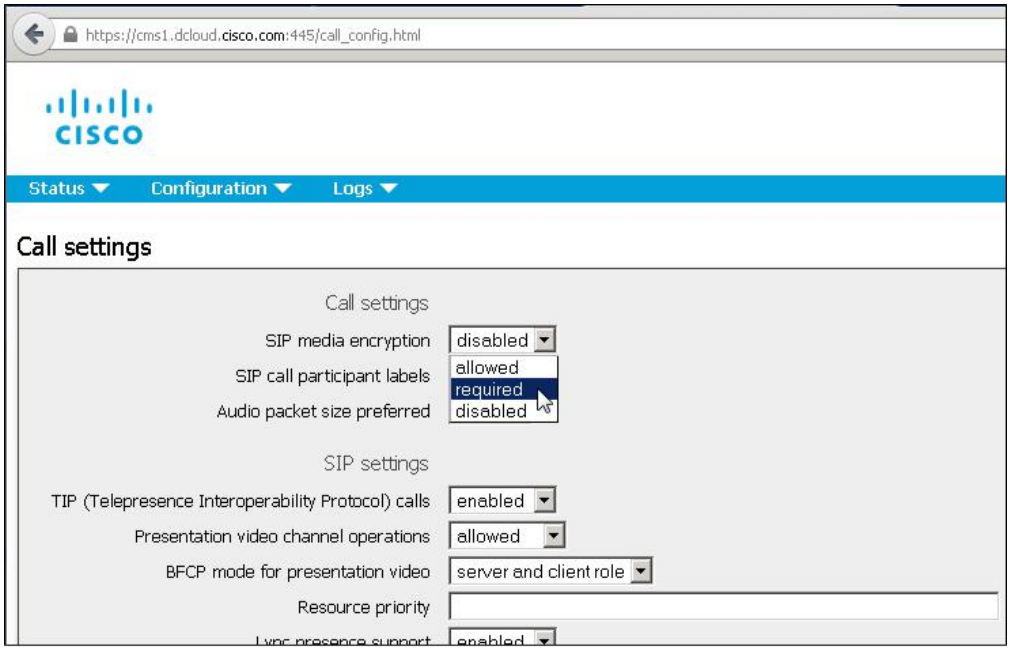
図 251. Cisco Meeting Server:永続的なスペースのデフォルト レイアウト設定(CMS Permanent Space 01)



7. システムで SIP 通話の暗号化を有効にする

先に進む前に、ラボの会議用に TLS/暗号化を有効にします。[設定(Configuration)] > [通話設定(Call settings)] に移動します。図 252 に示すように、[SIP メディア暗号化(SIP media encryption)] ドロップダウン フィールドから [必要(required)] を選択します。

図 252. Cisco Meeting Server:セキュアな会議のために通話を暗号化



画面の下部までスクロールし、Submit をクリックして、設定の変更を保存します。

これ以上 Cisco Meeting Server の設定変更はありませんので、Cisco Meeting Server の Web 管理インターフェイスへの接続は閉じて構いません。

C. Cisco Meeting Server に対する Unified CM のセキュアな SIP トランクの設定

Cisco Meeting Server の設定が完了したので、残っているのは、Unified CM と Cisco Meeting Server 間のセキュアな SIP トランク統合を設定することだけです。

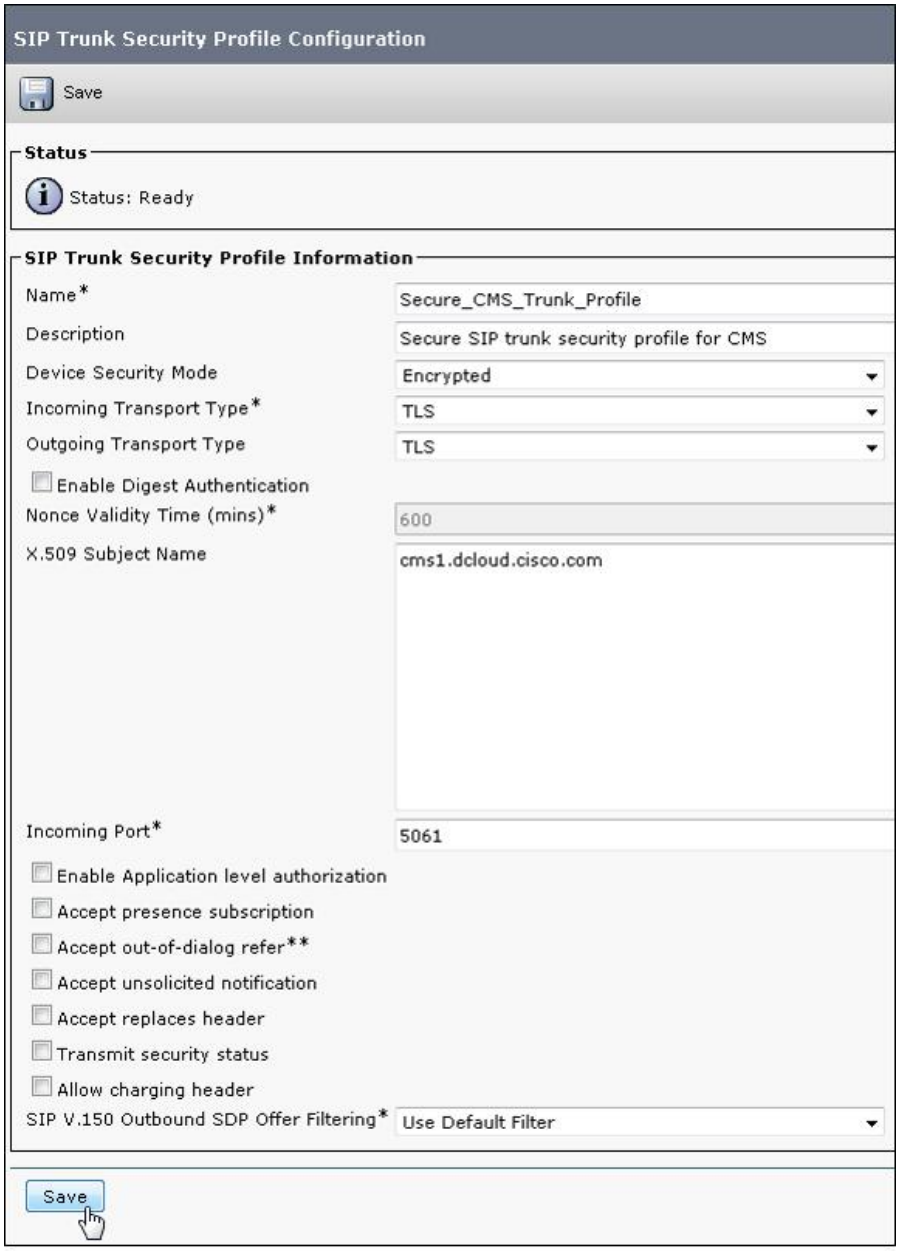
8. セキュアな（TLS 暗号化）SIP トランク プロファイルを設定し、Cisco Meeting Server への SIP トランクに適用する

   WKST2（198.18.133.37 に RDP 接続）のブラウザで、Unified CM 管理ポータル（https://ucm1.dcloud.cisco.com/ccmadmin/）にアクセスし、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。[システム（System）] > [セキュリティ（Security）] > [SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）] を選択します。

   [新規追加（Add New）] をクリックして、新しいセキュアな SIP トランクのセキュリティ プロファイルを設定します。図 253 に示すように、次の情報を入力します。

   - [名前（Name）]：**Secure_CMS_Trunk_Profile**
   - [説明（Description）]：**CMS 用のセキュアな SIP トランク セキュリティ プロファイル（Secure SIP trunk security profile for CMS）**
   - [端末セキュリティモード（Device Security Mode）]：[暗号化（Encrypted）]
   - [着信/発信転送タイプ（Incoming / Outgoing Transport Type）]：[TLS]/[TLS]
   - [X.509 のサブジェクト名（X.509 Subject Name）]：**cms1.dcloud.cisco.com**
   - [着信ポート（Incoming Port）]：**5061**

図 253. Cisco Meeting Server：セキュアな SIP トランク セキュリティ プロファイル

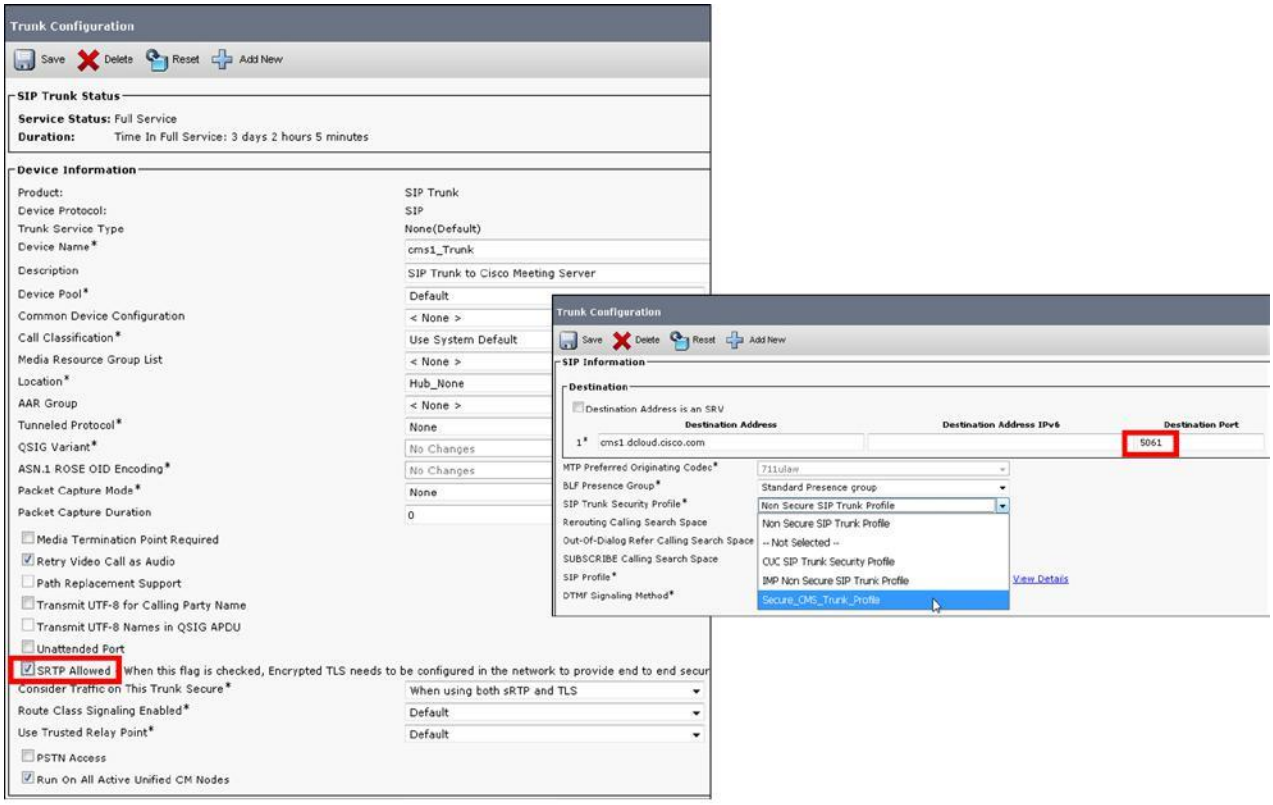


をクリックします。

次に、Cisco Meeting Server への既存の SIP トランクを設定し、Unified CM と Cisco Meeting Server 間でシグナリングを暗号化して安全に統合します。また、エンドポイントと Cisco Meeting Server の間のメディアも暗号化します。[端末（Device）] > [トランク（Trunk）] に移動します。[検索（Find）] をクリックします。システムの SIP トランク リストから **cms1_Trunk** というトランクを選択します。図 254 に示すように、設定ページでこのトランクに対して以下の変更を行います。

- [SRTP を許可（SRTP Allowed）]：**オン**
- [宛先ポート（Destination Port）]：**5061**
- [SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]：[Secure_CMS_Trunk_Profile]

図 254. Cisco Meeting Server：SIP トランク



をクリックします。次のダイアログで [リセット（Reset）] をクリック後 [OK] をクリックし、トランクをリセットして設定の変更を適用します。

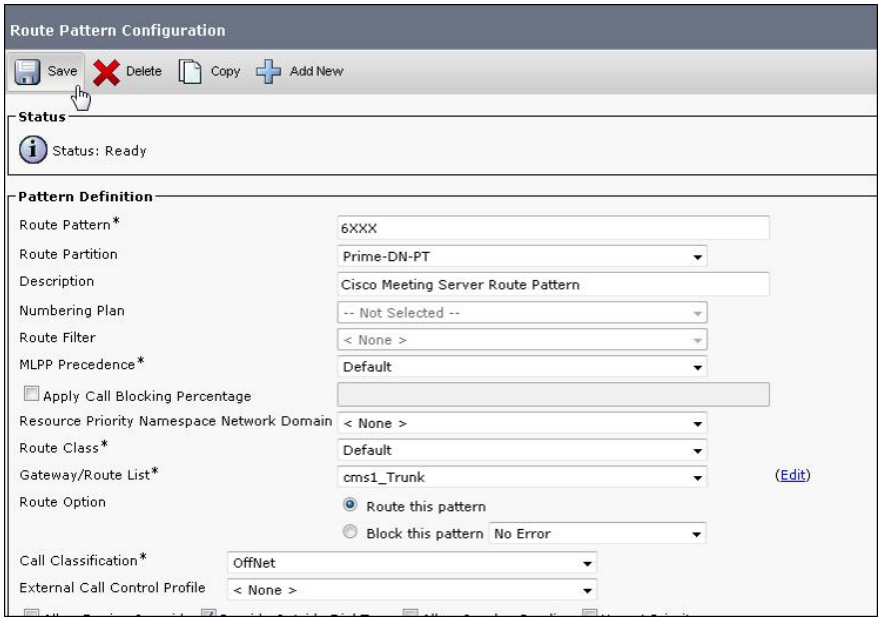
9. 永続的なスペースでのアドホックなビデオ会議に対する通話をルーティングする

ユーザが Cisco Meeting Server に設定されている永続的なスペースに到達できるようにするため、Unified CM のダイヤル プラン設定で、ユーザが永続的なスペースの URI にダイヤルできるように変更する必要があります。今回のケースでは、ユーザは、**CMS Permanent Space 01** の URI（**6100**）に到達できる必要があります。Unified CM 管理 Web ポータル（https://ucm1.dcloud.cisco.com/ccmadmin）にログインしたまま、[通話ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートパターン（Route Pattern）] の順に選択します。[新規追加（Add New）] をクリックして、次のように設定します。

- [ルートパターン（Route Pattern）]：**6XXX**
- [ルートパーティション（Route Partition）]：[Prime-DN-PT]
- [説明（Description）]：**Cisco Meeting Server Route Pattern（Cisco Meeting Server のルート パターン）**
- [ゲートウェイ/ルートリスト（Gateway/Route List）]：[cms1_Trunk]

残りの設定フィールドおよびパラメータは、すべて既存の値/デフォルト値のままにします（図 255 を参照）。

図 255. Unified CM：Cisco Meeting Server の永続的スペースのルート パターン



[保存（Save）] をクリックします。[OK] をクリックして、承認コードがアクティブになっていないことを示す警告を確認します。[OK] をクリックして、トランクがリセットされることを確認します。

最後に、[端末（Device）] > [トランク（Trunk）] に移動後、必要に応じて [検索（Find）] クリックしてシステムのトランクを表示します。次の手順に進む前に、**cms1_Trunk** が、完全にサービス状態に戻っていることを確認します。永続的なビデオ会議が可能になるまえに、サービス状態に戻す必要があります。

D. Cisco Meeting Server による暗号化されたセキュアな会議を確認する

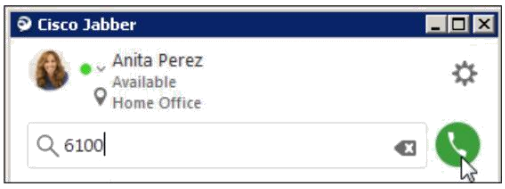
次に、セキュアな会議が機能していることを確認します。

10. セキュアな会議をセットアップして、セキュアな永続的スペースの操作を確認する

    ラボの Cisco Meeting Server の永続的スペース（URI/DN：6100）への通話が暗号化されていることを確認します。

    必要に応じて WKST2 に RDP 接続し（198.18.133.37、**DCLOUD\aperez/C1sco12345**）、Jabber を起動します。登録されたら、通話ウィンドウで **6100** と入力し、発信アイコンをクリックします（図 256 を参照）。

図 256. 発信：Anita Perez（WKST2）が 6100 の永続的ミーティング スペースに発信



注：モジュール 8（次世代暗号化によるセキュアなボイスメール）を完了していない場合、Unity Connection のボイス メール サービス証明書が無効であることを示す警告が表示されます。この警告メッセージが表示されるのは、ラボの Unity Connection ボイスメール サービス ノードから受信した証明書がデフォルトの自己署名証明書で、ラボのワークステーションのローカル信頼ストアに存在しないためです。[拒否（Decline）] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。Jabber クライアントにエラー メッセージが表示され、ビジュアル ボイスメール サービスは接続されません。このメッセージは、証明書が無効なため Unity Connection サーバ（cuc1.dcloud.cisco.com）への接続が拒否されたことを示しています。

接続したら、必要に応じて WKST3 に RDP で接続し（198.18.133.38、**DCLOUD\mcheng/C1sco12345**）、Jabber を起動します。登録されたら、発信ウィンドウで **6100** と入力し、発信アイコンをクリックします（図 257 を参照）。

図 257. 発信：Monica Cheng（WKST1）が 6100 の永続的ミーティング スペースに発信

注：モジュール 8（次世代暗号化によるセキュアなボイスメール）を完了していない場合、[拒否（Decline）] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否し、エラー メッセージは無視します。このメッセージは、証明書が無効なため Unity Connection サーバ（cuc1.dcloud.cisco.com）への接続が拒否されたことを示しています。

図 258 に示されている各 Jabber クライアントの鍵のアイコンは、Cisco Meeting Server の永続的スペースの会議通話が、接続されたエンドポイントと Cisco Meeting Server 間で暗号化されていることを示します。

図 258. Jabber クライアント：Cisco Meeting Server の永続的スペースに暗号化された通話で参加

通話を切って、両方の Jabber クライアントを終了します。最後に、WKST2 の PuTTY、WinSCP、Firefox ブラウザの各セッションをすべて閉じます。

E. Cisco Meeting Server による暗号化されたセキュアなアドホック会議を設定する

Cisco Meeting Server の永続的なスペースを利用したセキュアな会議の設定と確認が無事完了したので、今度は、Cisco Meeting Server を会議ブリッジとして使用したアドホックな会議を取り上げます。Cisco Meeting Server の会議ブリッジ リソースによって、[追加（+）（Add (+)）] ボタンと会議用のソフトキー/ボタンを使用して、すぐに音声/ビデオ会議を作成することができます。

注：このモジュールの残りの部分を完了するためには、モジュール 9（Expressway MRA におけるエンドツーエンドの暗号化とアクセス ポリシー）を完了している必要があります。モジュール 9 が必要なのは、セキュアなアドホック会議を検証するために、3 番目の参加者として WKST1（198.18.2.39）のリモート Jabber クライアントを使用するからです。このクライアントは Expressway Mobile and Remote Access（MRA）を利用して接続します。

MRA で接続された WKST1 の Jabber クライアントが参加していなくても、Unified CM で関連する設定を完了して会議ブリッジをセットアップすることはできますが、セキュアなアドホック会議の操作を検証することはできません。

11. Cisco Meeting Server を Unified CM で会議ブリッジとして設定する

WKST2（198.18.133.37 に RDP 接続）のブラウザで、Unified CM 管理ポータル（https://ucm1.dcloud.cisco.com/ccmadmin/）にアクセスし、必要に応じて、ユーザ名/パスワード：**administrator/dCloud123!** でログインします。

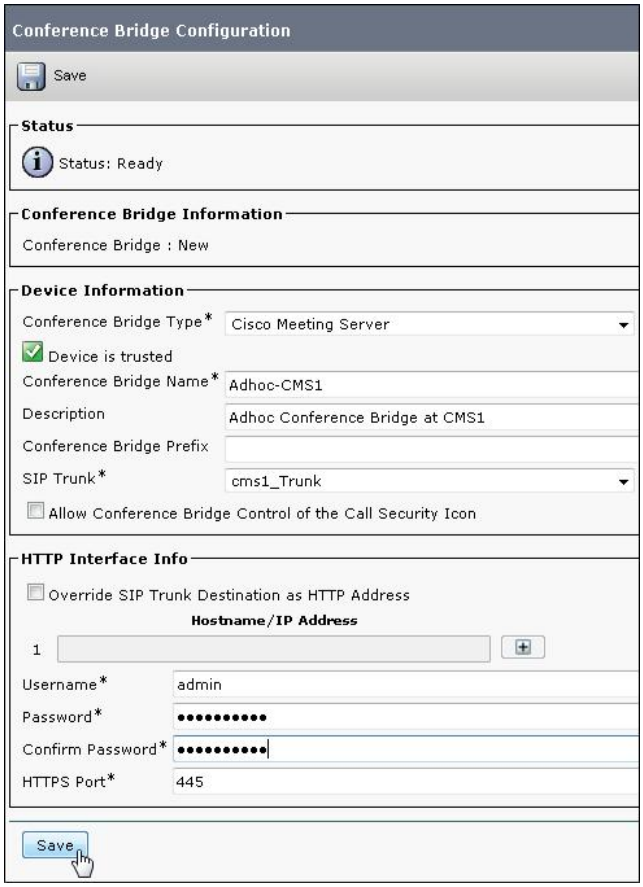
[メディアリソース（Media Resources）] > [会議ブリッジ（Conference Bridge）] を選択し、[新規追加（Add New）] をクリックします。図 283 に示すように、次の情報を入力します。

- [会議ブリッジのタイプ（Conference Bridge Type）]：[Cisco Meeting Server]
- [会議ブリッジ名（Conference Bridge Name）]：**Adhoc-CMS1**
- [説明（Description）]：**Adhoc Conference Bridge at CMS1（CMS1 のアドホック会議ブリッジ）**
- [SIP トランク（SIP Trunk）]：[cms1_Trunk]

[HTTP インターフェイス情報（HTTP Interface Info）] セクションで、CMS 管理者のユーザ名とパスワード（admin/dCloud123!）を入力します。[HTTPS ポート（HTTPS port）] 番号には **445**（Cisco Meeting Server webadmin サービスのポート）を指定します。図 259 を参照してください。

[保存（Save）] をクリック後、[リセット（Reset）] をクリックします。次のウィンドウで再度 [リセット（Reset）] をクリック後、[閉じる（Close）] をクリックします。

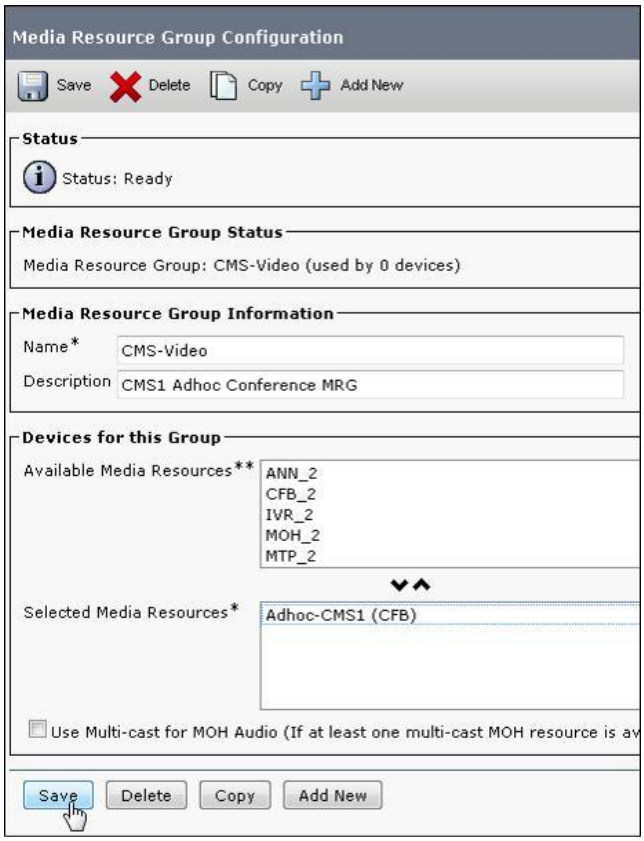
図 259. Unified CM：Cisco Meeting Server のアドホック会議用ブリッジの設定



次に、メディア リソース グループを設定し、メディア リソース リストに割り当てます。

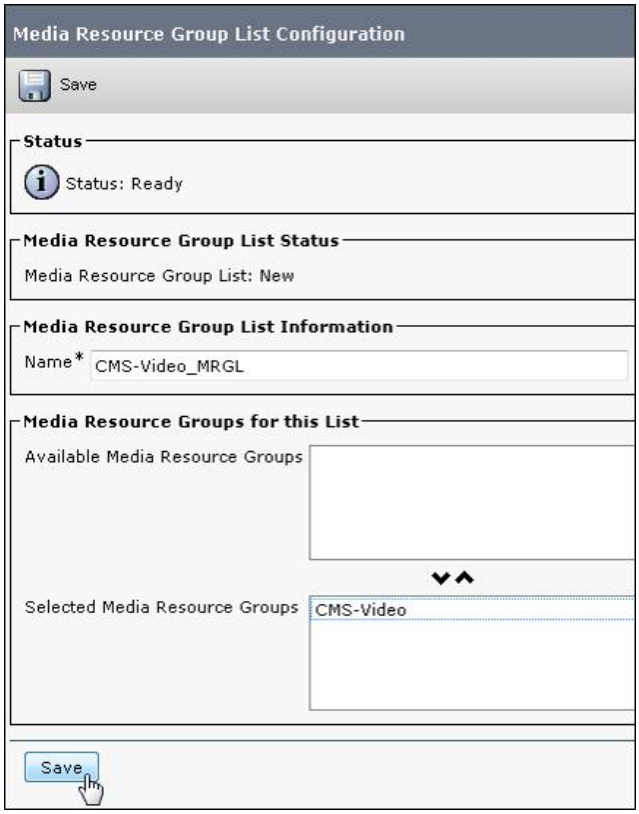
[メディアリソース（Media Resources）] > [メディアリソースグループ（Media Resource Group）] に移動します。[新規追加（Add New）] をクリックして、[名前（Name）] フィールドに **CMS-Video**、[説明（Description）] フィールドに **CMS1 Adhoc Conference MRG（CMS1 アドホック会議 MRG）**と入力します。最後に、図 260 に示すように、[利用可能なメディアリソース（Available Media Resources）] リストから、先に設定した会議ブリッジ（[Adhoc-CMS1 (CFB)]）を選択し、**下向きの矢印**アイコンをクリックして、[選択されたメディアリソース（Selected Media Resources）] リストに移動します。[保存（Save）] をクリックします。

図 260. Unified CM：CMS-Video メディア リソース グループと Cisco Meeting Server 会議ブリッジ



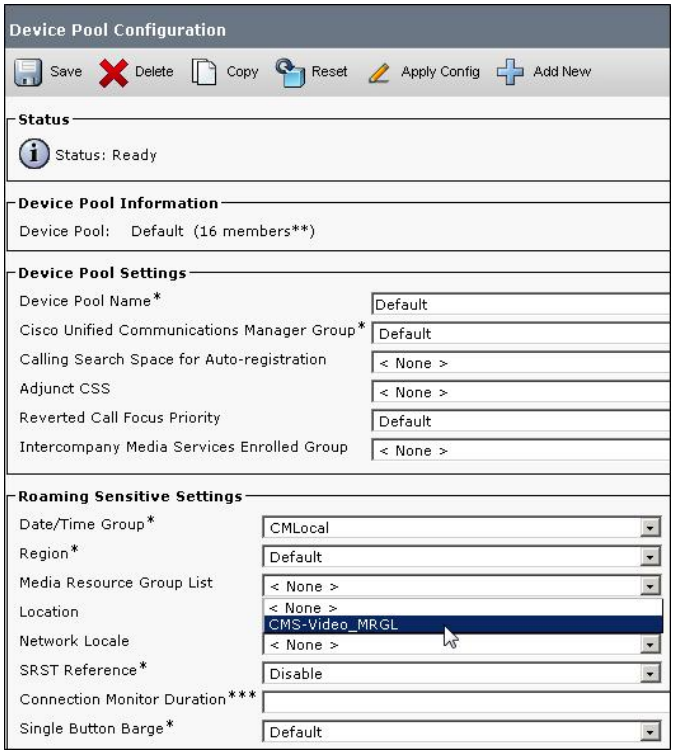
これで、会議ブリッジを作成し、新しく設定したメディア リソース グループに割り当てましたので、今度は、メディア リソース グループリストを設定し、新しいメディア リソース グループを割り当てる必要があります。[メディアリソース（Media Resources）] > [メディアリソースグループリスト（Media Resource Group List）] に移動します。[新規追加（Add New）] をクリックして、[名前（Name）] フィールドに **CMS-Video_MRGL** と入力します。図 261 に示すように、[使用可能なメディアリソースグループ（Available Media Resource Groups）] リストで、先に設定したメディア リソース グループ（**CMS-Video**）を選択し、**下向きの矢印**アイコンをクリックして、[選択されたメディアリソースグループ（Selected Media Resource Groups）] リストに移動します。[保存（Save）] をクリックします。

図 261. Unified CM：CMS-Video_MRGL メディア リソース グループ リスト



最後に、新しく設定したメディア リソース グループ リスト（**CMS-Video MRGL**）を、ラボのデフォルトの端末プールに割り当て、エンドポイントが Cisco Meeting Server のアドホック会議ブリッジを利用できるようにする必要があります。[システム（System）] > [端末プール（Device Pool）] を選択します。[検索（Find）] をクリック後、[デフォルト（Default）] を選択します。設定ページで、[メディアリソースグループ（Media Resource Group）] ドロップダウンから **CMS-Video_MRGL** を選択します（図 262 を参照）。[保存（Save）] をクリックして、設定を更新します。最後に [リセット（Reset）] をクリックして、新たに更新された端末プールの端末をリセットします。

図 262. Unified CM：CMS-Video メディア リソース グループ リストのために端末プールを更新



これで設定が完了しましたので、Unified CM によってルーティングされ、Cisco Meeting Server のメディア リソース（会議ブリッジ）を利用した、三者間のセキュアなアドホック ビデオ会議通話をセットアップします。

F. Cisco Meeting Server による暗号化されたセキュアなアドホック会議を検証する

最後に、Cisco Meeting Server によるセキュアなアドホック会議を検証します。

12. アドホック会議をセットアップし、セキュアな会議ブリッジ リソースとして Cisco Meeting Server が機能するのを確認する

    必要に応じて WKST2 に **RDP** で接続し（198.18.133.37、**DCLOUD\aperez/C1sco12345**）、Jabber を起動します。

    次に、必要に応じて WKST3 に RDP で接続し（198.18.133.38、**DCLOUD\mcheng/C1sco12345**）、Jabber を起動します。

    今度は、WKST1（198.18.2.39）に **RDP** で接続し、ユーザ名/パスワード：[DCLOUD]**\koneal/C1sco1245** でログインします。

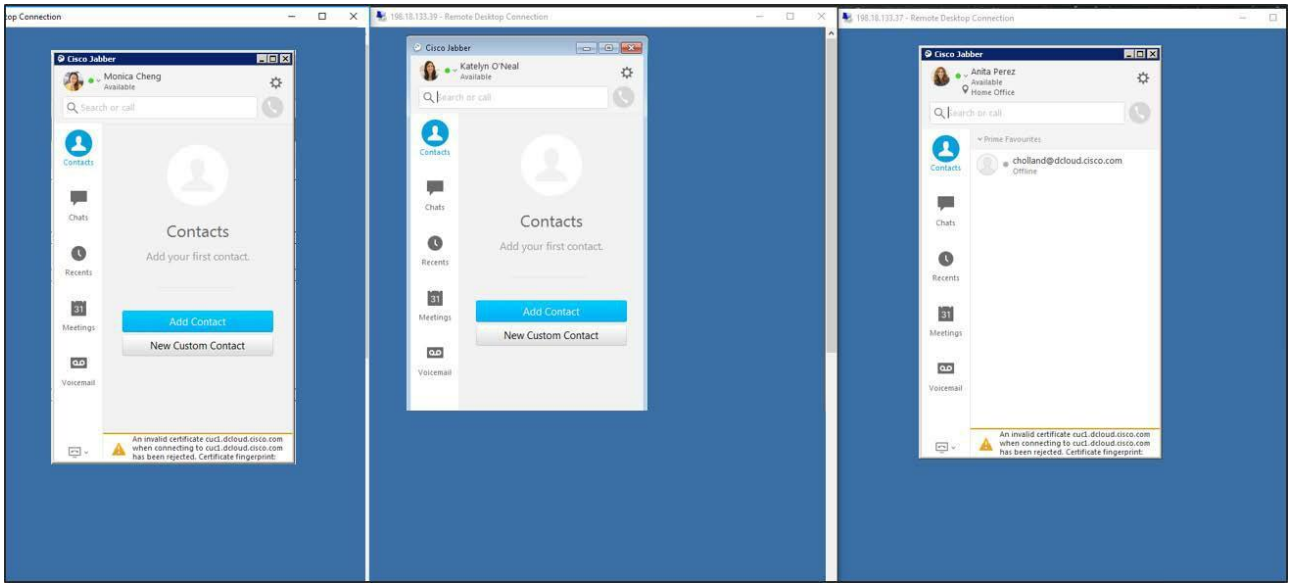
注：モジュール 8（次世代暗号化によるセキュアなボイスメール）を完了していない場合、Unity Connection のボイス メール サービス証明書が無効であることを示す警告が、WKST2 の Jabber クライアント（aperez）と WKST3 の Jabber クライアント（mcheng）の両方に表示されます。この警告メッセージが表示されるのは、ラボの Unity Connection ボイスメール サービス ノードから受信した証明書がデフォルトの自己署名証明書で、ラボのワークステーションのローカル信頼ストアに存在しないためです。[拒否（Decline）] をクリックして、ビジュアル ボイスメールについて、ボイスメール システムとの接続を拒否します。Jabber クライアントにエラー メッセージが表示され、ビジュアル ボイスメール サービスは接続されません。このメッセージは、証明書が無効なため Unity Connection サーバ（cuc1.dcloud.cisco.com）への接続が拒否されたことを示しています。

MRA で WKST3 の Jabber クライアント（koneal）と接続すると、証明書に関する警告メッセージやプロンプトは表示されません。先に示したように、MRA で Jabber クライアントに接続した場合、Unity Connection の tomcat 証明書が自己署名であることや、検証対象のローカルの信頼ストアに存在しないことは問題になりません。MRA 接続の Jabber クライアントは、Unity Connection の

証明書を確認しないからです。Jabber で必要なのは、ファースト ホップの TLS 接続（HTTPS REST）に、信頼される CA の署名付き Expressway-E 証明書が使用されていることを確認することだけです。

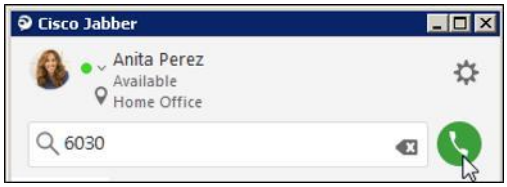
次に進む前に、図 263 に示すように、すべての Jabber クライアントが起動していて、Unified CM に登録されていることを確認します。

図 263. 3 つすべての Jabber クライアントが登録されている



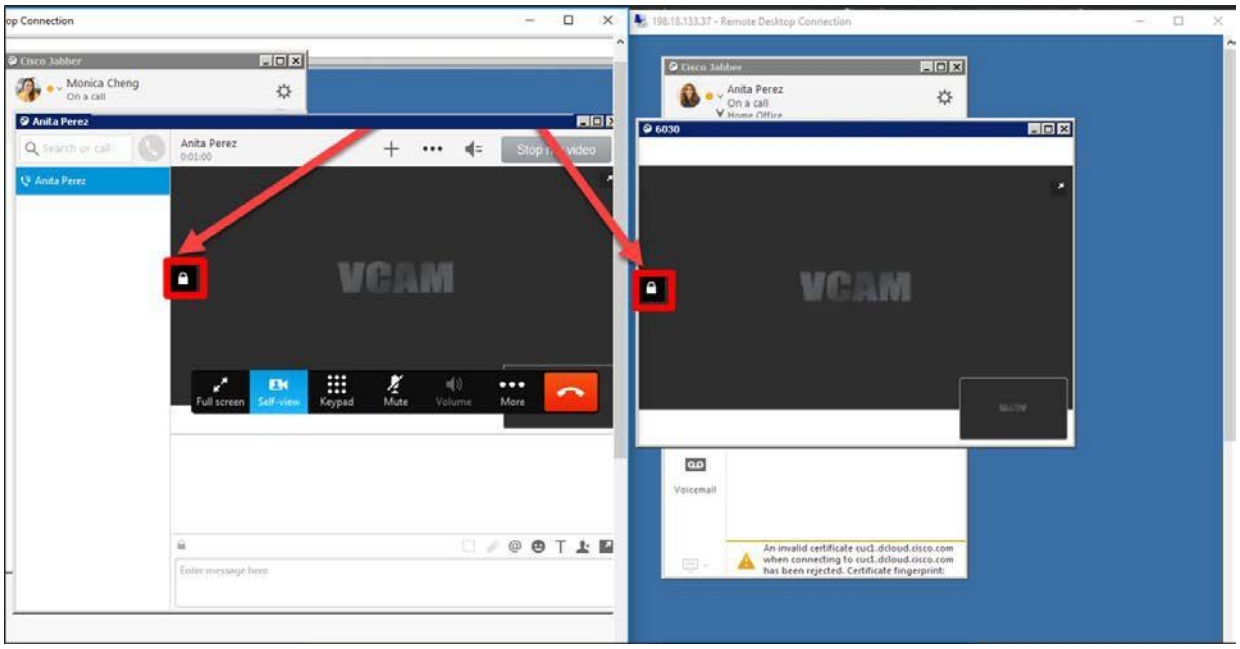
WKST2 の Anita Perez 用 Jabber クライアントで、検索/発信ウィンドウに 6030 と入力し、発信アイコンをクリックして、WKST3 の Monica Cheng 用 Jabber クライアントを呼び出します（図 264 を参照）。

図 264. Anita Perez（WKST2）から 6030 の Monica Cheng（WKST3）に発信



WKST3 の Jabber クライアント（6030/mcheng）で着信通話に応答します。図 265 に鍵のアイコンが表示されていることからわかるように、これら 2 台の Jabber クライアント間の 1 対 1 の通話は、この時点で暗号化されています。

図 265. Anita Perez と Monica Cheng の Jabber クライアント間の暗号化された 1 対 1 の通話

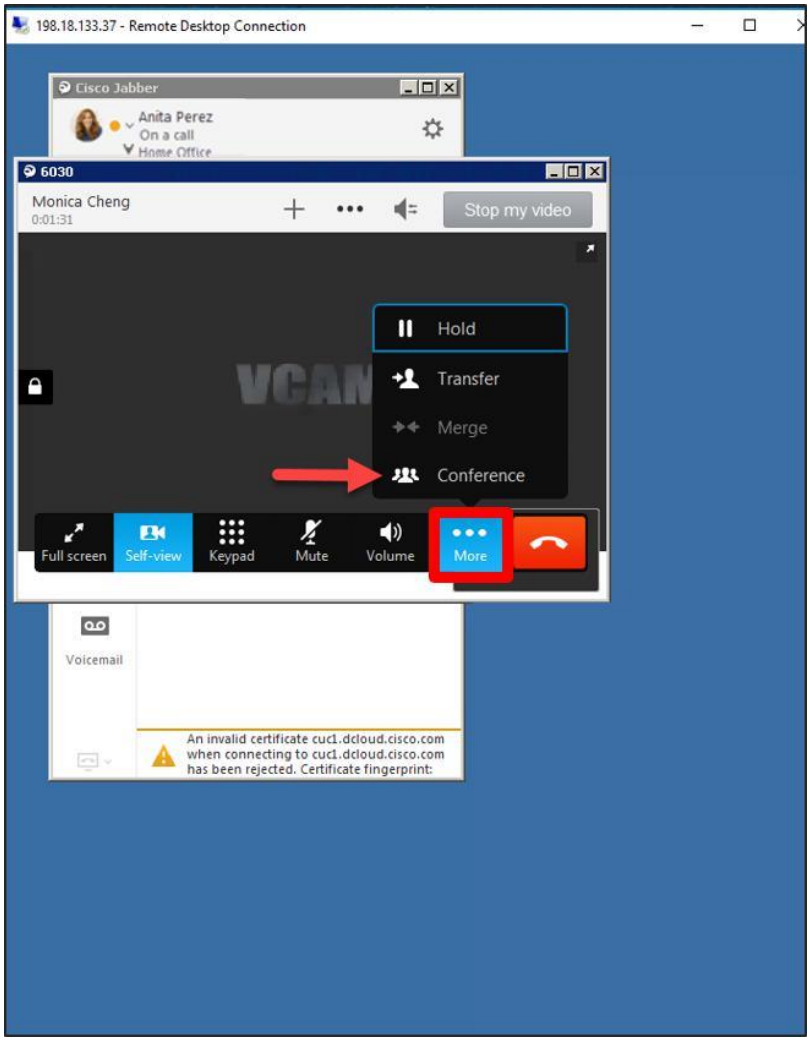


次に、3 番目の参加者を追加し、アドホック会議のブリッジとして Cisco Meeting Server を利用します。

図 266 に示すように、Anita Perez の Jabber クライアントの発信ウィンドウで、 

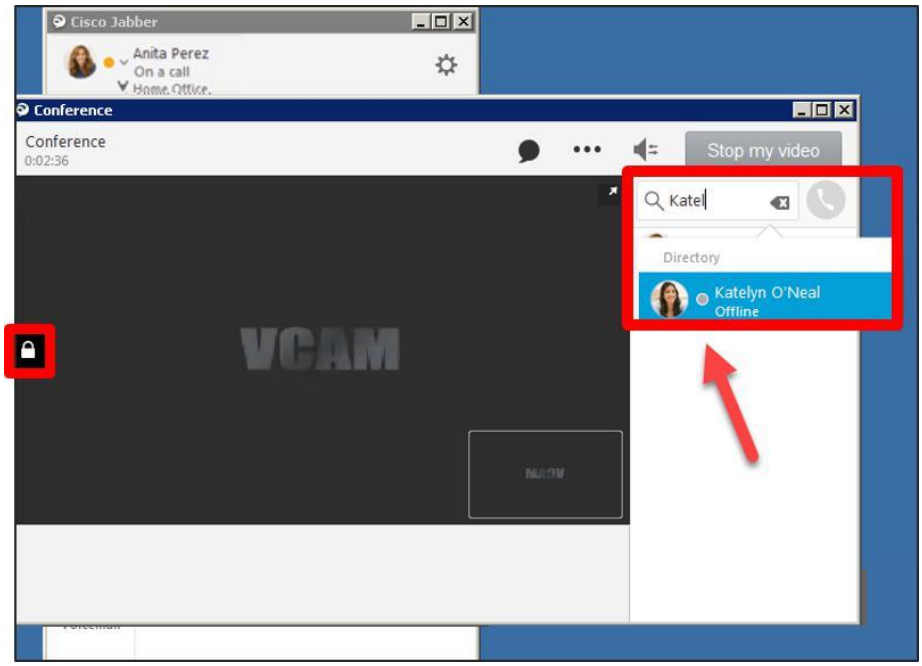
([その他(More)])ソフトキーをクリックし、[会議(Conference)] をクリックします。

図 266. Anita Perez の Jabber クライアントからアドホック会議を開始する



会議がセットアップされた時点で、Monica Cheng の Jabber クライアントは保留状態になります。図 267 に示すように、次の会議ウィンドウの [参加者の追加（Add participants）] フィールドに **Katelyn** と入力し、**Katelyn O'Neal** を選択して会議に追加します。

図 267. 会議の参加者リストに Katelyn O'Neal を追加



次に、図 268 に示すように、**発信**アイコンをクリックして Katelyn O'Neal を呼び出します。

図 268. Katelyn O'Neal を呼び出してアドホック会議に接続

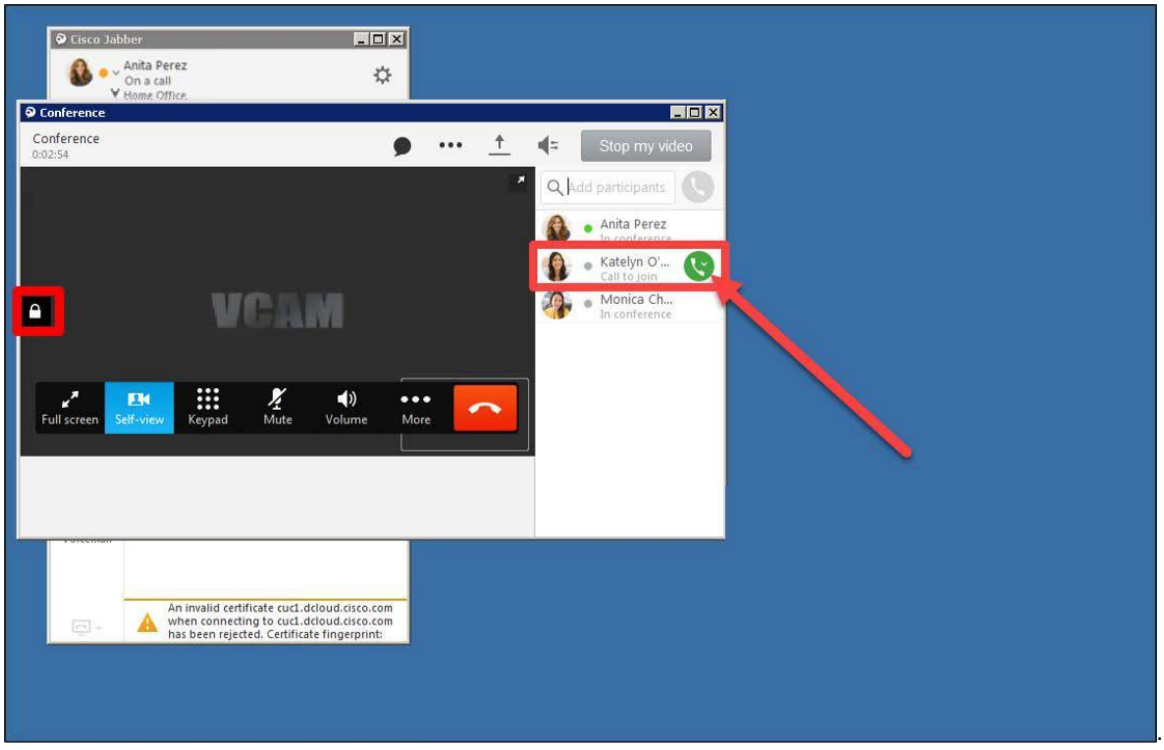
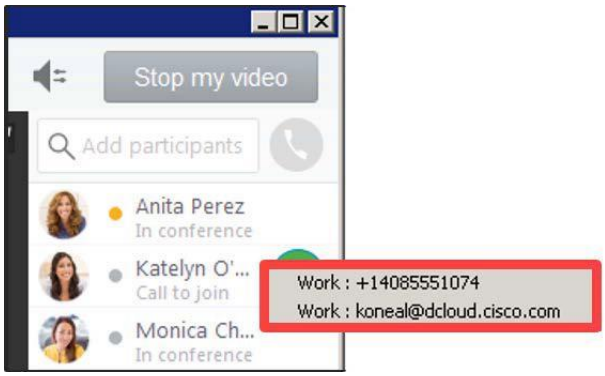


図 269 に示すように、E.164 番号または URI 番号を選択します。

図 269. Katelyn O'Neal を呼び出す番号または URI を選択



呼び出したら、WKST1 の Katelyn 用 Jabber クライアントで応答します。

最後に、図 270 に示すように、Katelyn の会議参加アイコンをクリックします。

図 270. Katelyn O'Neal がアドホック会議に参加

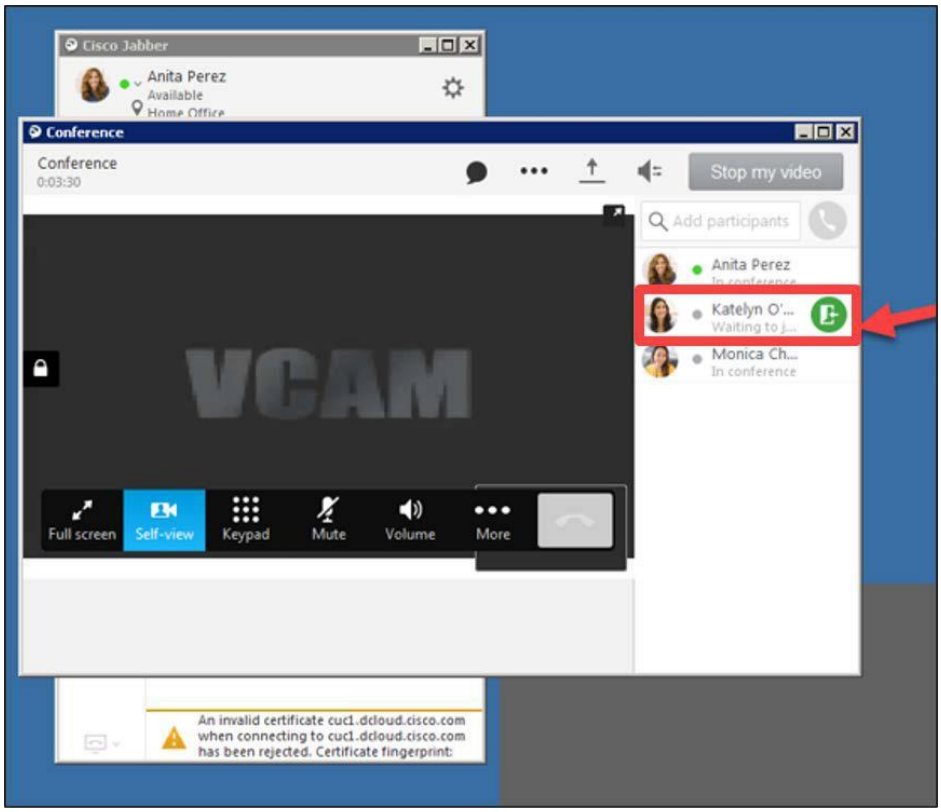
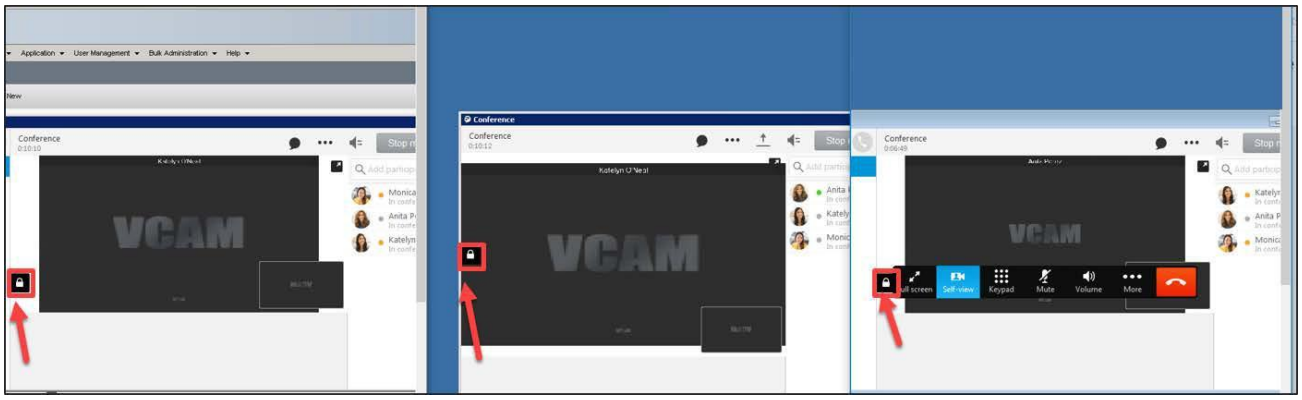


図 271 に示すように、3 台すべての Jabber クライアントがアドホック会議に接続し、会議が暗号化されていることを示す鍵のアイコンが各 Jabber クライアントに表示されていることを確認します。

図 271. 三者間での暗号化されたアドホック会議



各クライアントで通話を切り、すべてのクライアントとブラウザ ウィンドウを閉じて、3 つのワークステーションへの RDP セッションを終了します。

***** モジュール #10 の終了*****

付録 A.　Expressway Mobile and Remote Access の設定

このセクションでは、本ラボ用に Expressway Mobile and Remote Access を設定する手順を示します。この設定を実施する必要はありません。すべての設定はすでに行われています。

この付録は次の 3 つのセクションに分かれています。

手順

A. Expressway 証明書の調査およびタスク

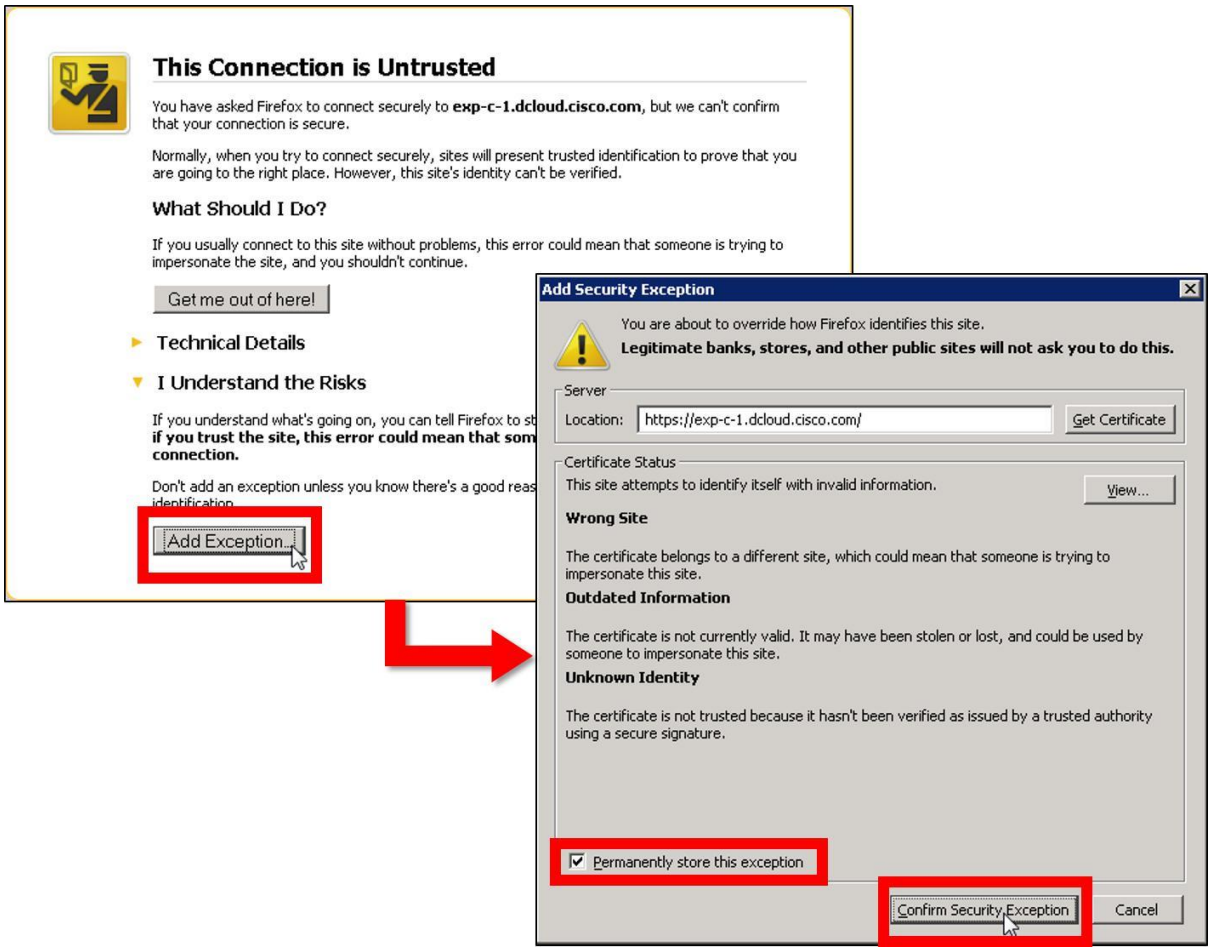
このセクションでは、Expressway 証明書のベスト プラクティスについて説明します。最初に Expressway-C の既存のデフォルトの証明書を確認します。次に Expressway-C サーバ証明書の CSR を生成し、証明書要求をエンタープライズ CA に送信します。その結果、証明書チェーンが信頼された CA にアップロードされます。この手順を Expressway-E サーバで繰り返します。最後に、署名付きサーバ証明書と CA ルート証明書が両方のサーバに存在することを確認します。

1. 既存のサーバおよび Expressway-C（exp-c-1.dcoud.cisco.com）の信頼できる CA 証明書を確認する

   証明書は、コラボレーション セキュリティで重要な役割を果たします。Expressway-C のさまざまな証明書を見てみましょう。

   WKST3（198.18.133.38 に RDP 接続、ユーザ名/パスワード：**DCLOUD\mcheng/C1sco12345**）で Firefox Web ブラウザを使用して、Expressway-C の管理インターフェイス（https://exp-c-1.dcloud.cisco.com/）に移動し、図 A.1 に示すように、証明書の警告をバイパスします（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception...）] をクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）。

図 A.1 Expressway-C：セキュリティの例外を確認し、Firefox ブラウザで証明書の警告をバイパス



次に、ユーザ名/パスワード：**admin/dCloud123!** でログインします。

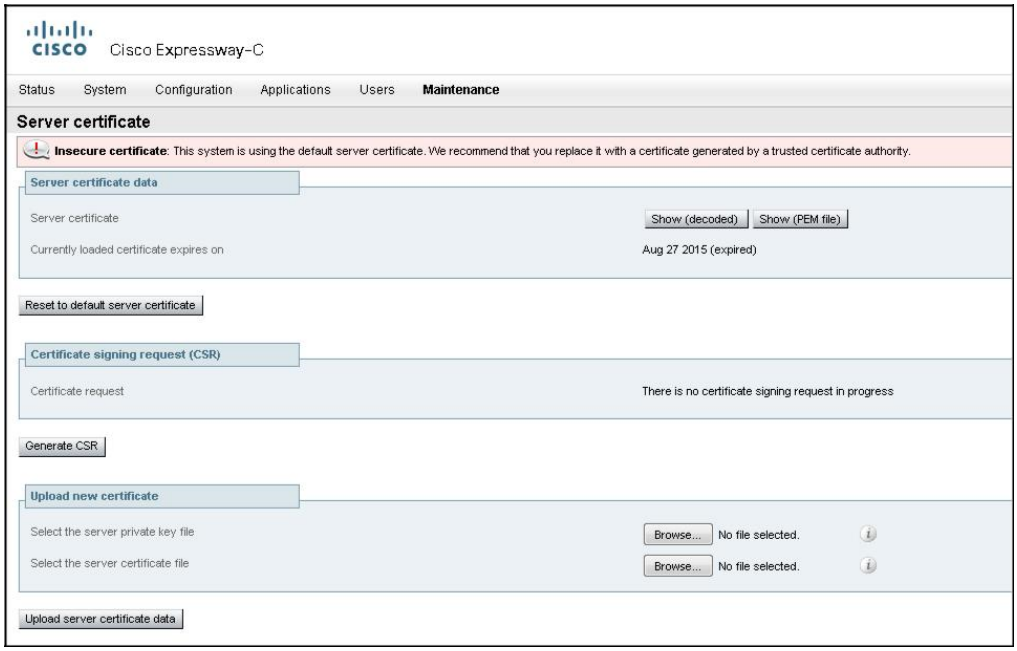
メニューで [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼できる CA 証明書（Trusted CA certificate）] を選択します。図 A.2 に示すように、デフォルトの一時 CA 証明書が表示されます。

図 A.2 Expressway-C のデフォルト CA 証明書*

*** *実際のシステムにおけるデフォルトの信頼された一時 CA 証明書の発行者情報は、上の図と異なる場合があります。***

次に、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server Certificate）] に移動して、デフォルトの Expressway-C 自己署名サーバ証明書を調べます。この証明書には警告メッセージが表示され、信頼された CA が生成した証明書と置き換えるよう推奨されます（図 A.3 を参照）。

図 A.3 Expressway-C のデフォルトの自己署名証明書



[表示（デコード）（Show (decoded)）] をクリックすると、一時サーバ証明書の詳細が表示されます。

Expressway-E でこの手順を繰り返します。最初に Expressway-E の管理インターフェイス（https://exp-e-1.dcloud.cisco.com/）に移動します。再度証明書の警告をバイパスし（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception...）] ボタンをクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）、ユーザ名/パスワード：**admin/dCloud123!** でログインします。

Expressway-C の場合と同様に、Expressway-E のデフォルトの一時証明書を確認します。

- [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼できる CA 証明書（Trusted CA certificate）] を選択して、デフォルトの証明書信頼ストアを確認します。
- [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server Certificate）] を選択して、デフォルトの一時サーバ証明書を確認します。

1. エンタープライズ CA で Expressway-C/E サーバの署名付き証明書を要求する

推奨に従って一時サーバ証明書を信頼された CA 署名付き証明書に置き換えるには、最初に証明書署名要求（CSR）を生成する必要があります。

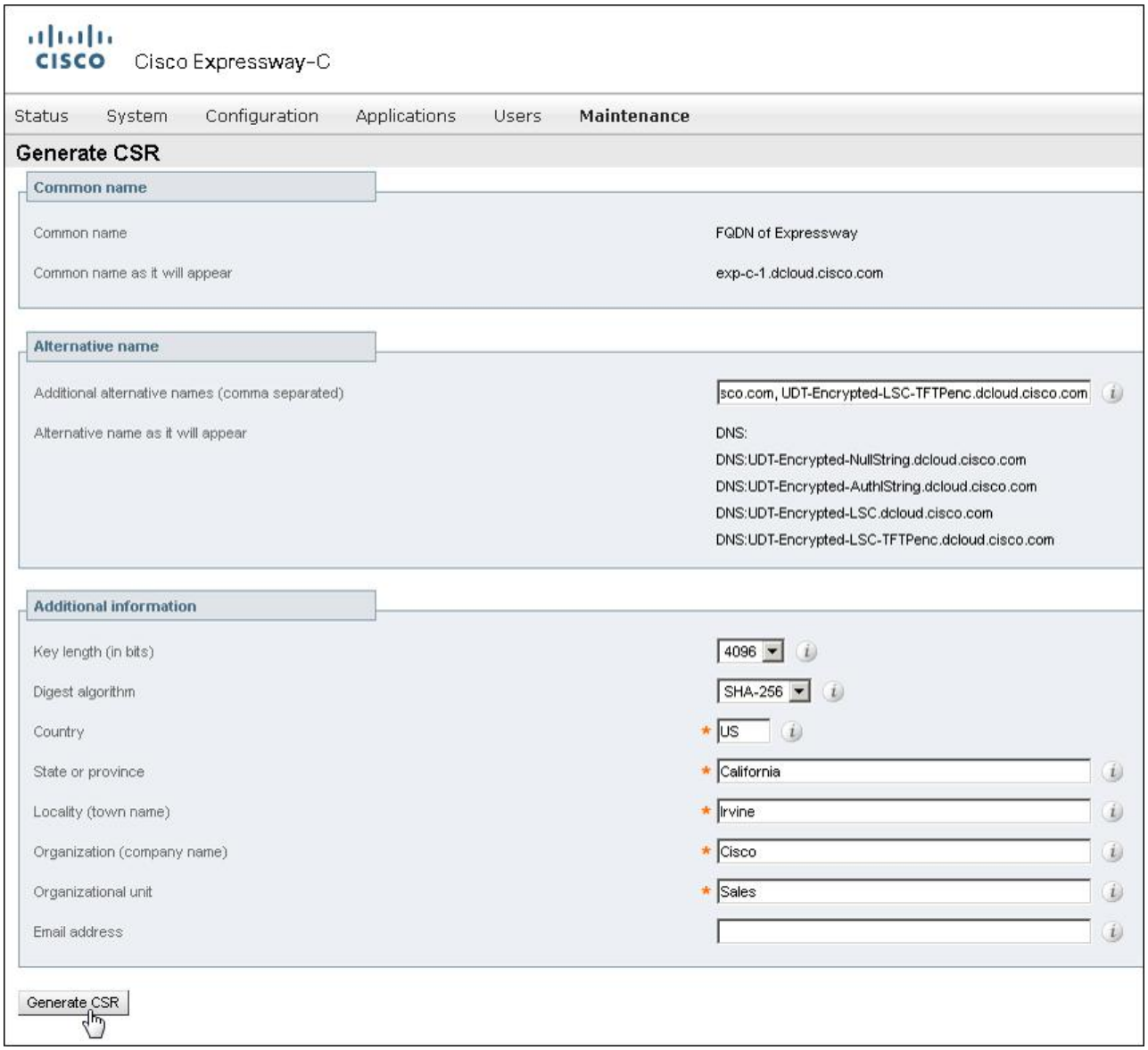
WKST3（198.18.133.38、ユーザ名/パスワード：**DCLOUD\mcheng/C1sco12345**）に RDP で接続します。

Expressway-C（https://exp-c-1.dcloud.cisco.com/）に移動します。必要に応じて、証明書の警告をバイパスし（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception...）] ボタンをクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）、ユーザ名/パスワード：**admin/dCloud123!** でログインします。

[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] を選択します。[サーバ証明書（Server certificate）] 画面で [CSR の生成（Generate CSR）] をクリックします。次の画面で、[追加代替名（Additional alternative names）] フィールドに、カンマで区切られたリスト（**UDT-Encrypted-NullString.dcloud.cisco.com, UDT-Encrypted-AuthString.dcloud.cisco.com, UDT-Encrypted-LSC.dcloud.cisco.com, UDT-Encrypted-LSC-TFTPenc.dcloud.cisco.com**）を入力します。これらの代替名は重要で、先に Unified CM で設定されている、暗号化された端末セキュリティ プロファイルの名前と一致している必要があります。

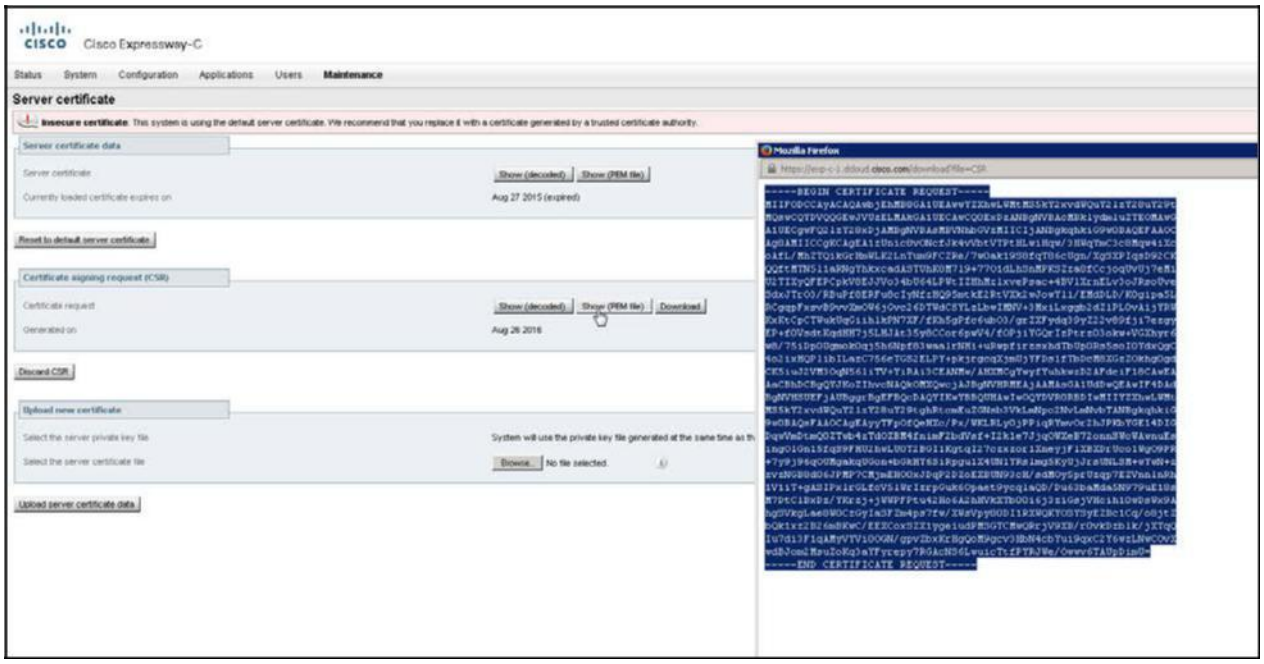
図 A.4 に示すように、[追加情報（Additional information）] セクションの必須フィールドに入力します。[キー長（Key length）] フィールドと [ダイジェストアルゴリズム（Digest algorithm）] フィールドはデフォルトのまま（それぞれ 4096 と SHA-256）にします。[CSR の生成（Generate CSR）] をクリックします。

図 A.4 Expressway-C の証明書署名要求（CSR）の生成



次の画面で、（上部の [サーバ証明書データ（Server certificate data）] セクションではなく）[証明書署名要求（CSR）（Certificate signing request (CSR)）] セクションの [表示（PEM ファイル）（Show (PEM file)）] ボタンをクリックすると、図 A.5 に示すように、作成した CSR が開きます。CSR の内容を選択して、クリップボードにコピー（Ctrl+C）します。これを使用して、エンタープライズ CA で署名付き証明書を要求します。

図 A.5 Expressway-CSR を表示*



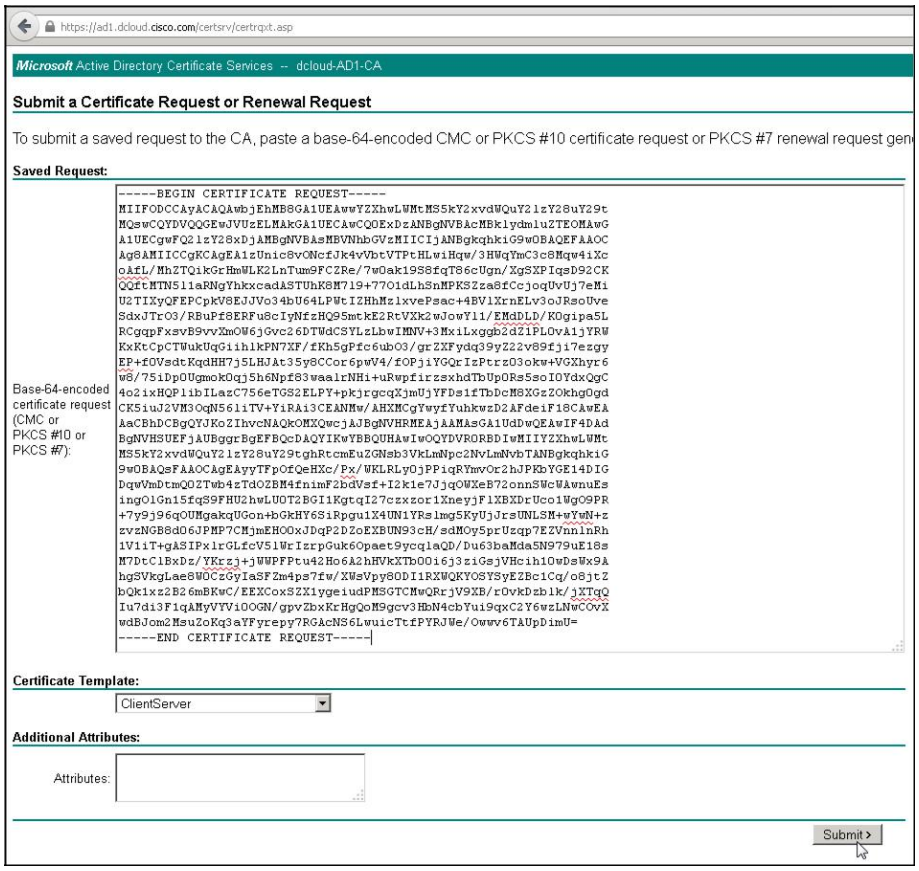
上の図の証明書署名要求文字列は、実際の CSR と異なる場合があります。

WKST3（198.18.133.38）で Firefox Web ブラウザを使用して https://ad1.dcloud.cisco.com/certsrv にアクセスし、認証を求められたら、ユーザ名/パスワード：**administrator/C1sco12345** でログインします。

[証明書を要求する（Request a certificate）] をクリックして、[または詳細証明書要求を送信する（Or, submit an advanced certificate request）] を選択します。

（前の手順で CSR からコピーした）クリップボードの内容を、[Base-64 でエンコードされた証明書要求（Base-64-encoded certificate request）] フィールドに貼り付けます。図 A.6 に示すように、[ClientServer] 証明書テンプレートを選択して [送信>（Submit >）] をクリックします。

図 A.6 エンタープライズ CA で Expressway-C の証明書を要求*

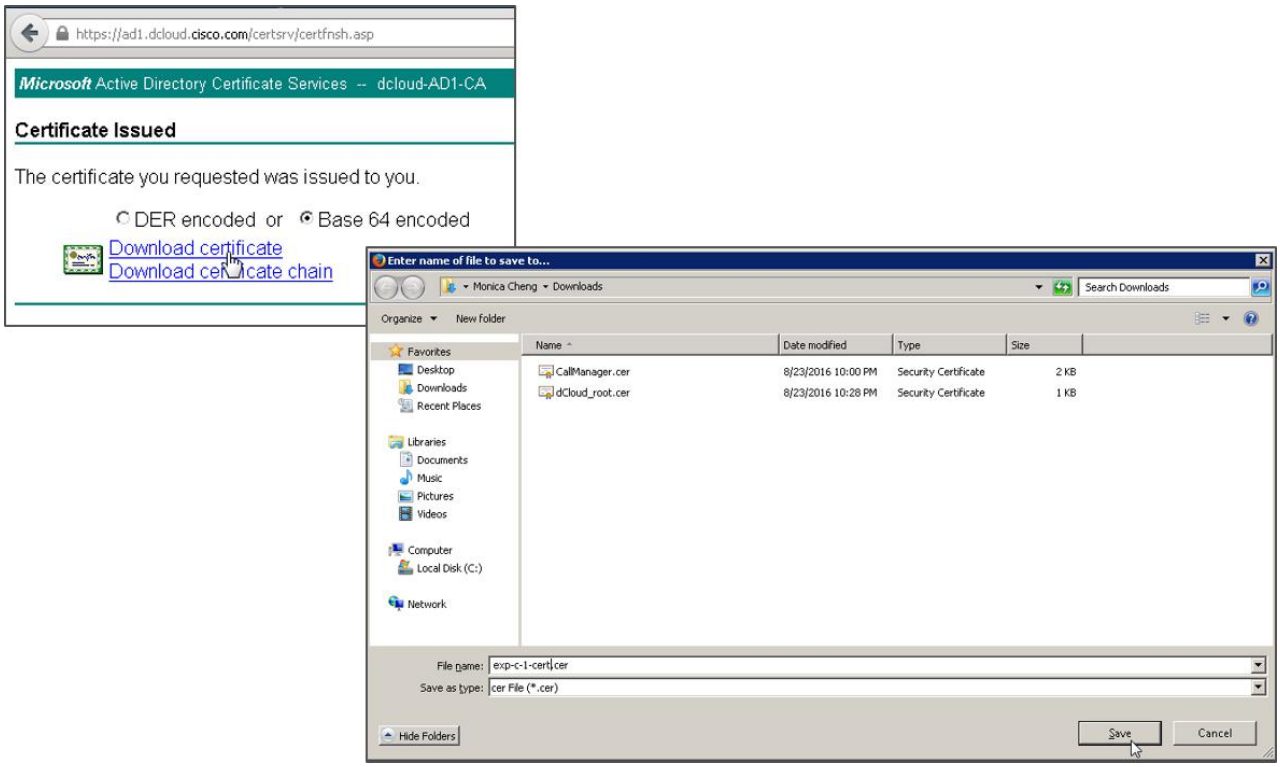


上の図の証明書署名要求文字列は、実際の CSR と異なる場合があります。

次の画面で、[Base 64 でエンコード（Base 64 encoded）] を選択して [証明書をダウンロード（Download Certificate）] をクリックします。次に [ファイルを保存（Save File）] を選択して [OK] をクリックし、ローカル ワークステーションに保存します。ファイルに「**exp-c-1-cert**」という名前を付けます（図 A.7 を参照）。

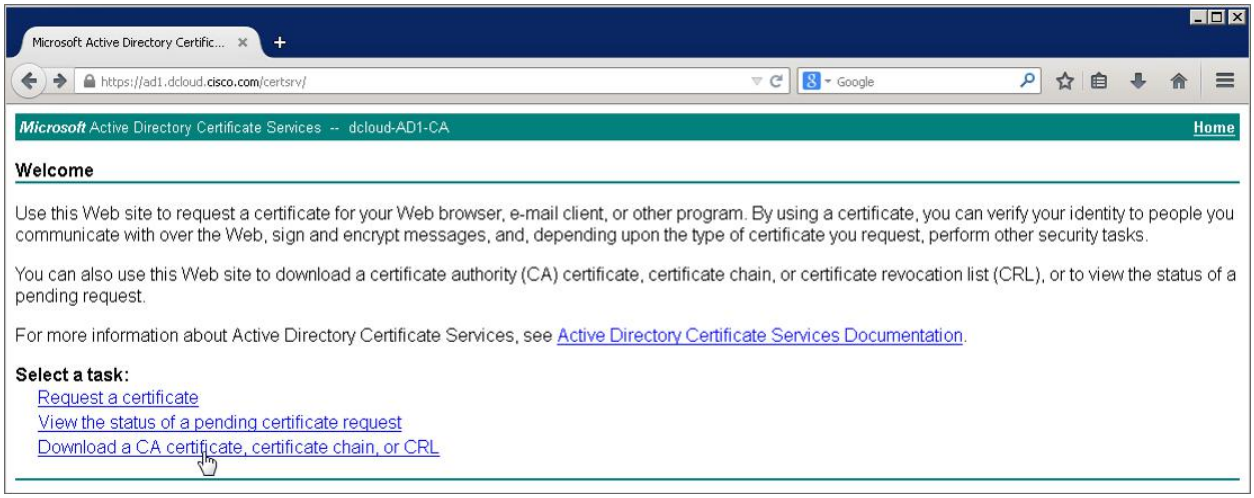
注：Unified CM では、DER と Base 64 のどちらでも証明書をエンコードできますが、Expressway では証明書を **Base 64 でエンコードする必要**があります。

図 A.7 署名付き Expressway-C 証明書の保存



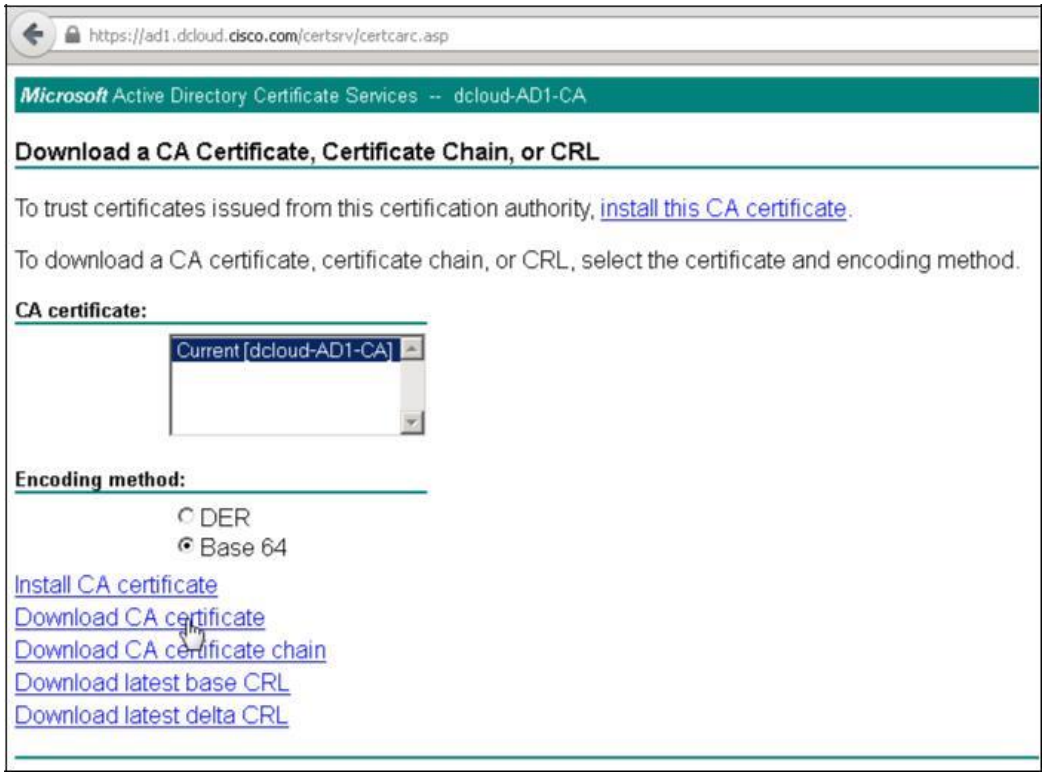
エンタープライズ CA から離れる前に、右上隅の [ホーム（Home）] リンク（https://ad1.dcloud.cisco.com/certsrv/）をクリックしてメインの CA ページに戻り、図 A.8 のように [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

図 A.8 エンタープライズ CA ルート証明書のダウンロード（1/2）



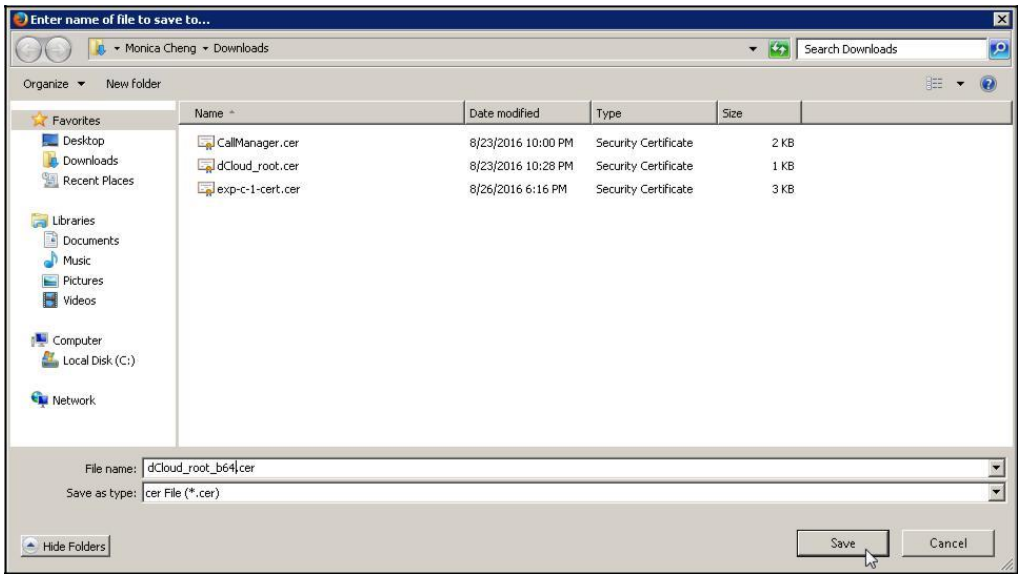
次の画面では、[現在の[dcloud-AD1-CA]（Current [dcloud-AD1-CA]）] がデフォルトで選択されています。[エンコード方式（Encoding Method）] で **[Base 64]** を選択します。[CA 証明書のダウンロード（Download CA certificate）] をクリックします（図 A.9 を参照）。

図 A.9 エンタープライズ CA ルート証明書のダウンロード（2/2）



最後に [ファイルの保存（Save File）] を選択して [OK] をクリックし、ファイルをローカル ワークステーションに保存します。図 A.10 に示すように、ファイルに「**dCloud_root_b64.cer**」という名前を付けて、[保存（Save）] をクリックします。

A.10 エンタープライズ CA ルート証明書を Base 64 で保存



次に、Expressway-E の証明書と信頼ストアで同じ手順を繰り返します。ただし Expressway-E の場合は、**シスコのベスト プラクティスとして、一般的に信頼されたサードパーティのパブリック CA によって Expressway-E サーバ証明書に署名することが推奨されます**。

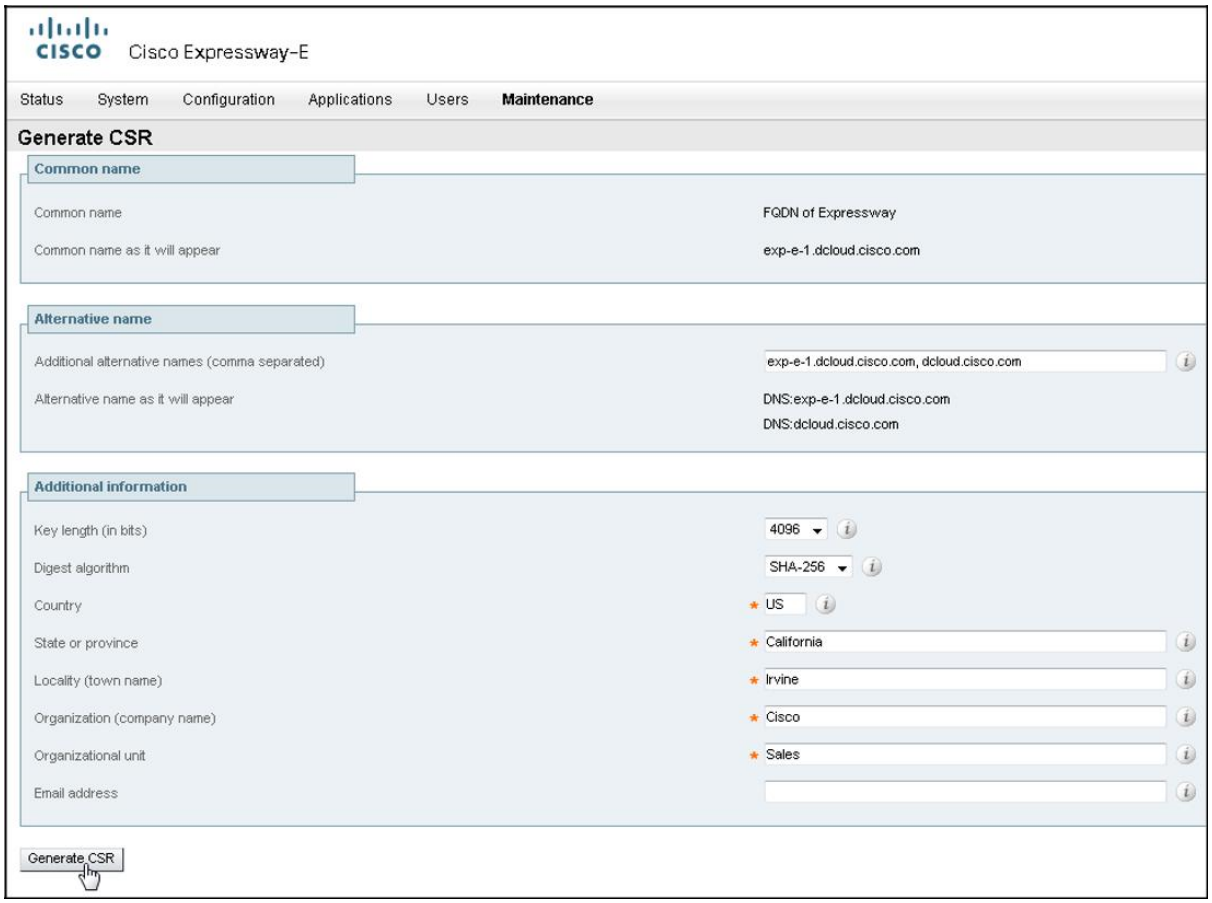
便宜上このラボでは、ベスト プラクティスに従ってパブリック CA によって Expressway-E サーバ証明書に署名するのではなく、Expressway-C サーバの場合と同様に、エンタープライズ CA によって証明書に署名します。

注: パブリック CA で Expressway-E サーバ証明書に署名するプロセスは、エンタープライズ CA で証明書に署名するプロセスと同じです。唯一の違いは、署名付きサーバ証明書とルート証明書（および必要な中間証明書）の両方を提供するパブリック CA に CSR を送信する必要があることです。エンタープライズ CA の場合と同様に、サーバ証明書をアップロードして、パブリック CA のルート証明書を追加します。

最初に Expressway-E の管理インターフェイス：https://exp-e-1.dcloud.cisco.com/（ユーザ名/パスワード：**admin/dCloud123!**）に移動します。必要に応じて、証明書の警告をバイパスします（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception...）] ボタンをクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）。

以前の Expressway-C の場合と同様、CSR を生成（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）]）し、[開く（.PEM file）（open (.PEM file)）] をクリックして、クリップボードにコピーします。図 A.11 に Expressway-E の CSR の画面を示します。今回のケースでは、追加の代替名として、**exp-e-1.dcloud.cisco.com** と **dcloud.cisco.com** の両方をカンマで区切って設定する必要があります（Expressway-C で代替名としてさまざまな端末暗号化セキュリティ プロファイルを設定したのと同様です。先の図 A.4 を参照してください）。

図 A.11 Expressway-E の証明書署名要求（CSR）の生成



エンタープライズ CA（https://ad1.dcloud.cisco.com/certsrv/）で証明書を要求し、**Base 64** 形式でダウンロードして、今回は「**exp-e-1-cert.cer**」という名前で保存します。

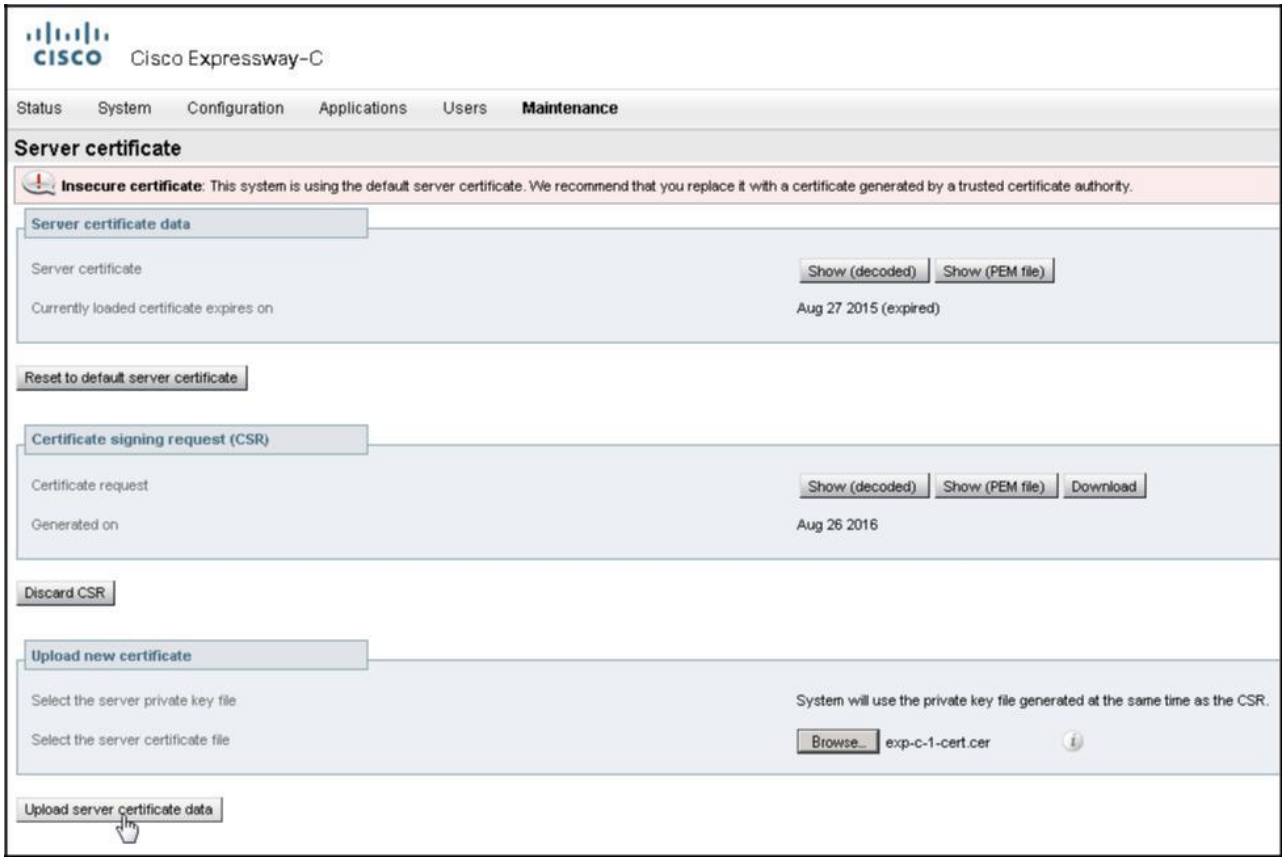
注: エンタープライズ CA ルート証明書を再度ダウンロードする必要はありません。Expressway-C と Expressway-E では、ダウンロード済みの証明書を使用できます。

2. CA 署名付きサーバ証明書とルート CA 証明書を Expressway-C/E にアップロードする

署名付き Expressway サーバ証明書をダウンロードして保存したら、それを Expressway-C サーバにアップロードする必要があります。また、エンタープライズ CA ルート証明書を、Expressway-C の信頼された CA に追加する必要もあります。

最初に、Expressway-C（（https://exp-c-1.dcloud.cisco.com/）に移動して [サーバ証明書（Server Certificate）] ページに戻ります（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）]）。[参照（Browse）] をクリックし、前にダウンロードした CA 署名付き Expressway-C 証明書（C:\Users\mcheng\Downloads の **exp-c-1-cert.cer**）を選択して、[開く（Open）] をクリックします。さらに図 A.12 に示すように、[サーバ証明書データのアップロード（Upload server certificate data）] をクリックします。

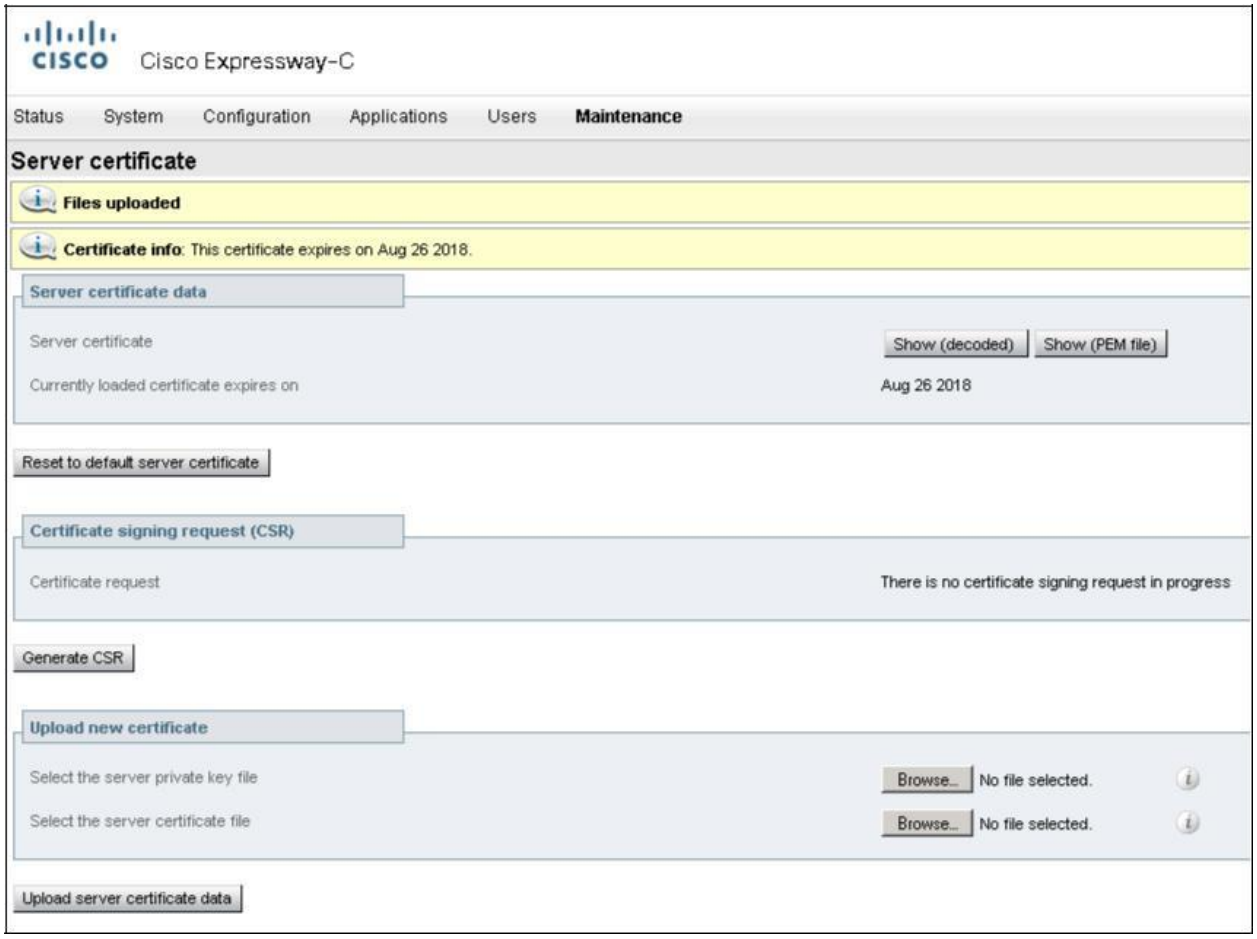
A.12 サーバ証明書データ（CA 署名付き証明書）を Expressway-C にアップロード



もう一度証明書の警告が表示されます。図 A.1 に示すように、証明書の警告をバイパスします（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception…）] をクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）。

図 A.13 に示すように、[ファイルがアップロードされました（Files uploaded）] というメッセージと証明書の有効期限ステータスを示すメッセージが表示されます。

図 A.13 正常にアップロードされた CA 署名付きサーバ証明書*

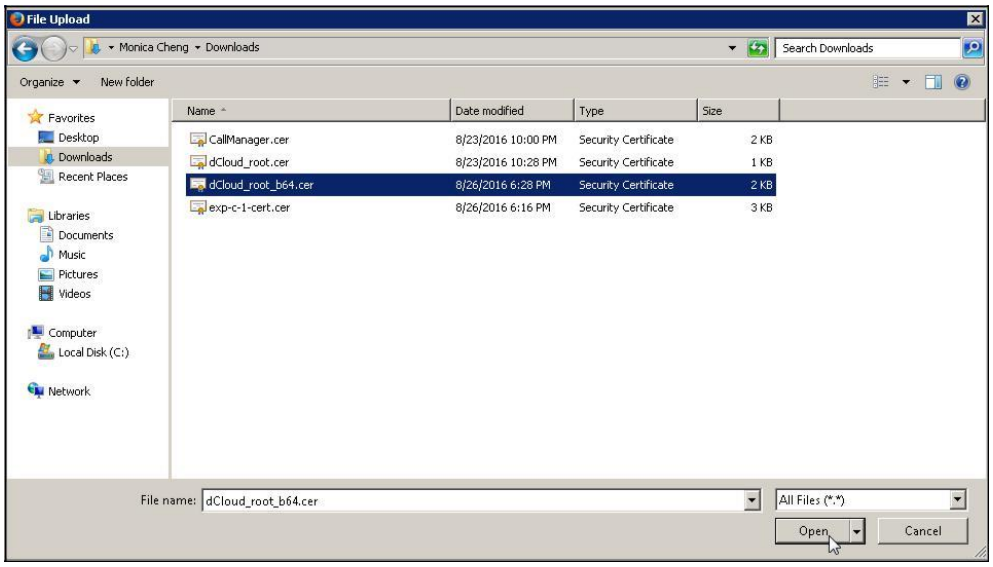


** ラボのサーバ証明書の有効期限は、上記の日付とは異なります。*

次に、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] に移動して、信頼された CA 信頼ストアに CA ルート証明書を追加します。ただし、新しいサーバ証明書をアップロードしているため、ここで移動しようとすると証明書の警告が表示されます。先に実施したように、新しい証明書を承認して証明書警告をバイパスし（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception...）] ボタンをクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）、再度接続します。

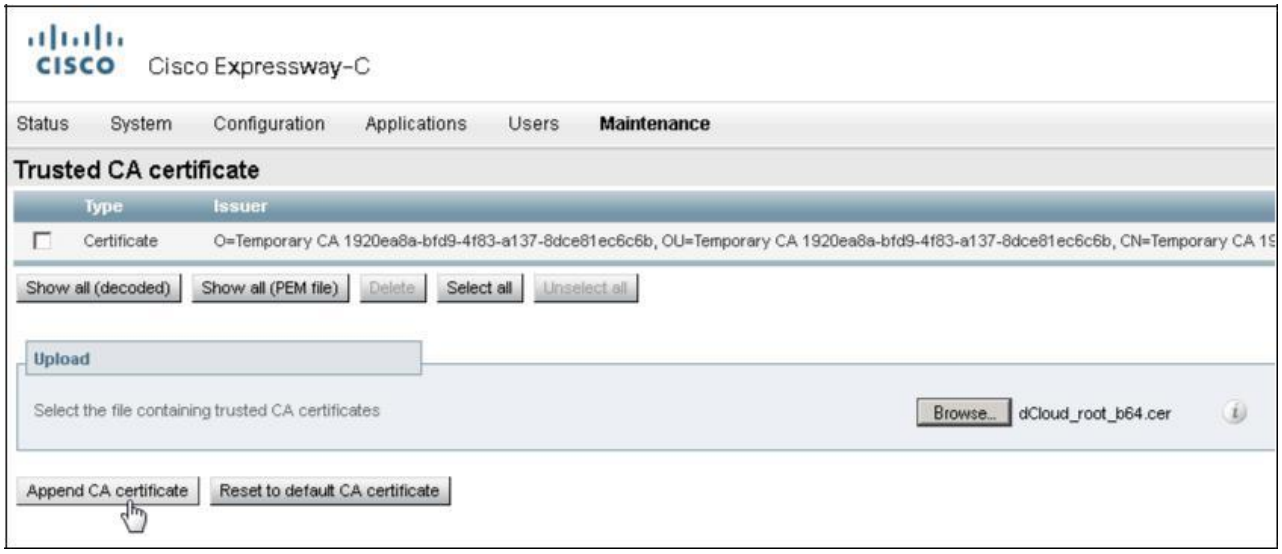
[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] に移動し、[参照（Browse）] をクリックして、Base 64 でエンコードされたエンタープライズ CA ルート証明書（C:\Users\mcheng\Downloads の **dCloud_root_b64.cer**）を選択し、[開く（Open）] をクリックします（図 A.14 を参照）。

図 A.14 Base 64 でエンコードされたエンタープライズ CA ルート証明書を選択



Base 64 でエンコードされたルート証明書を選択したら、[CA 証明書の追加（Append CA certificate）] をクリックします（図 A.15 を参照）。

図 A.15 エンタープライズ CA ルート証明書を Expressway-C の信頼された CA 信頼ストアに追加



**** 実際のシステムにおけるデフォルトの信頼された一時 CA 証明書の発行者情報は、上の図と異なる場合があります。***

図 A.16 に示すように、[ファイルがアップロードされました（Files uploaded）] というメッセージが表示されます。これは、エンタープライズ CA ルート証明書がアップロードされたことを示しています。信頼された CA 証明書リストにルート CA 証明書（dcloud-AD1-CA）が表示されます。

図 A.16 Expressway-C にアップロードされたエンタープライズ CA ルート証明書

Expressway-E サーバについても、この手順を繰り返します。再度 Expressway-E の管理インターフェイス：https://exp-e-1.dcloud.cisco.com/（ユーザ名/パスワード：**admin/dCloud123!**）に移動します。

Expressway-E で次のようにします。

- [サーバ証明書（Server Certificate）] ページに戻り（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）]）、前にダウンロードした CA 署名付き Expressway-E 証明書（C:\Users\mcheng\Downloads の **exp-e-1-cert.cer**）を選択し、[サーバ証明書データのアップロード（Upload server certificate data）] ボタンをクリックしてアップロードします。新しい証明書を承認して証明書警告をバイパスし（[リスクを理解しました（I Understand the Risks）] > [例外の追加...（Add Exception...）] をクリック後、[セキュリティの例外を確認（Confirm Security Exception）] をクリック）、再度接続します。
- [信頼された CA 証明書（Trusted CA certificate）] ページに戻り（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）]）、Base 64 でエンコードされたエンタープライズ CA のルート証明書（C:\Users\mcheng\Downloads の **dCloud_root_b64.cer**）を選択し、[CA 証明書の追加（Append CA certificate）] をクリックして追加/アップロードします。

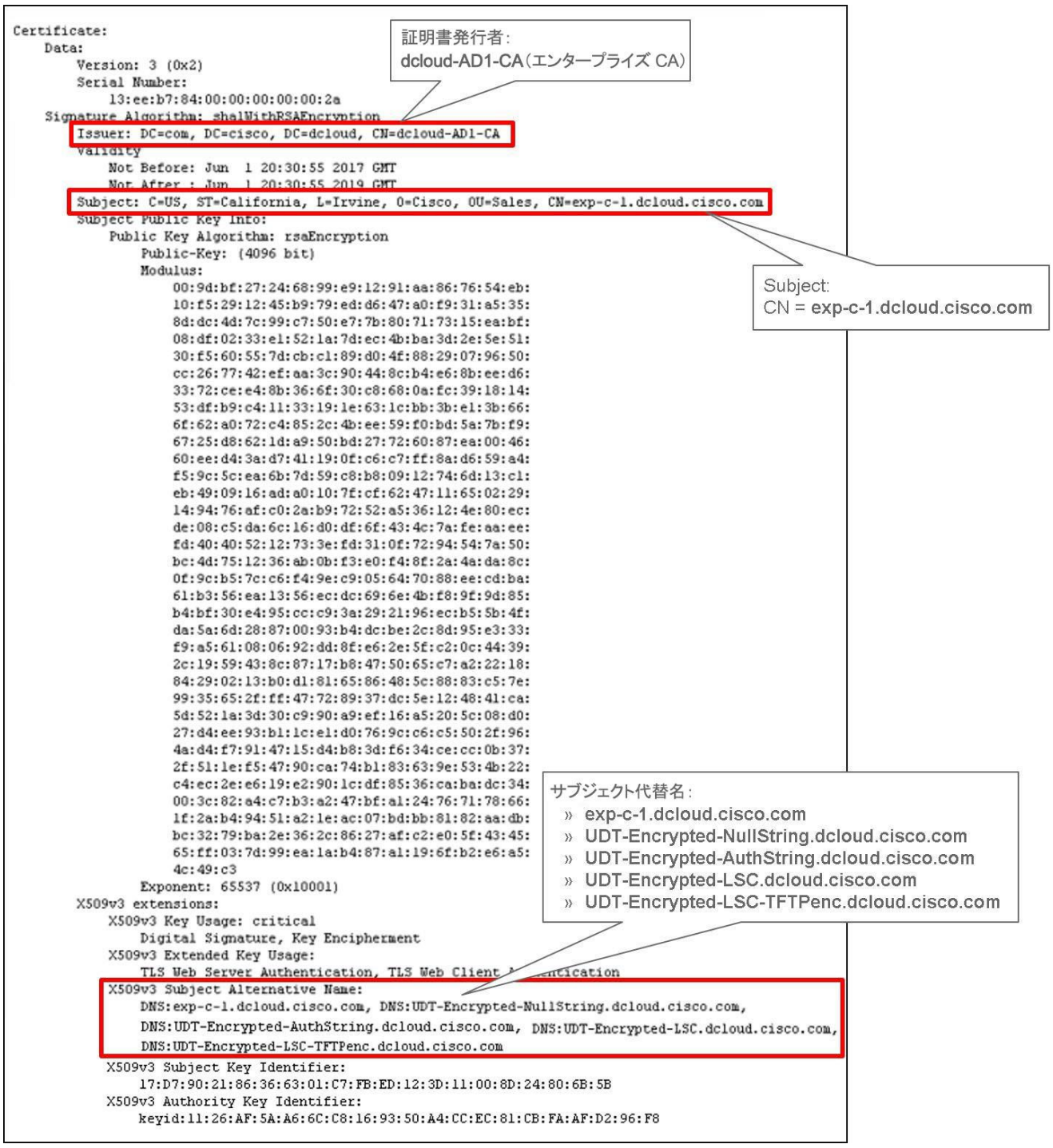
3. 署名付きサーバ証明書が Expressway サーバに存在することを確認し、内容を確認します。

   先に進む前に、署名付き Expressway サーバ証明書が存在することを確認し、証明書の内容を簡単に確認します。

   Expressway-C の管理インターフェイス：https://exp-c-1.dcloud.cisco.com/（ユーザ名/パスワード：**admin/dCloud123!**）に移動し、[サーバ証明書（Server Certificate）] ページ（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server Certificate）]）に戻ります。サーバ証明書データに、現在ロードされている証明書の有効期限が示されます。このサーバ証明書にはすでにラボで署名しているため、有効期限は今日の日付になっています。

   [表示（デコード）（Show (decoded)）] ボタンをクリックすると、図 A.17 に示すように証明書の詳細が表示されます。

図 A.17 信頼されたエンタープライズ CA 署名付き Expressway-C サーバ証明書*



**** 上記のシリアル番号、有効期限、およびキーは、ラボの証明書と一致しない場合があります。***

発行者情報（エンタープライズ CA：**dcloud-AD1-CA**）と、サブジェクト名（CN：**exp-c-1.dcloud.cisco.com**）、組織/組織単位、国、州などの証明書属性が表示されます。すべての証明書のサブジェクト代替名（SAN）（**exp-c-1.dcloud.cisco.com**、**UDT-Encrypted-NullString.dcloud.cisco.com**、**UDT-Encrypted-LSC.dcloud.cisco.com**、**UDT-Encrypted-LSC-TFTPenc.dcloud.cisco.com**、**UDT-Encrypted-AuthString.dcloud.cisco.com**）が表示されていることを確認します。

最後に、Expressway-E（（https://exp-e-1.dcloud.cisco.com/- ユーザ名/パスワード：**admin/dCloud123!**）に再度アクセスし、[サーバ証明書（Server Certificate）] ページ（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server Certificate）]）に戻ります。[サーバ証明書データ（Server certificate data）] で、[表示（デコード）（Show (decoded)）] をクリックして、エンタープライズ CA 署名付き Expressway-E サーバ証明書を確認します（図 A.18 を参照）。

図 A.18 信頼されたエンタープライズ CA 署名付き Expressway-E サーバ証明書*

* *上記のシリアル番号、有効期限、およびキーは、ラボの証明書と一致しない場合があります。*

ここでも、発行者情報（エンタープライズ CA：**dcloud-AD1-CA**）と、サブジェクト名（CN：**exp-e-1.dcloud.cisco.com**）、組織/組織単位、国、州などの証明書属性が表示されます。証明書 SAN：**exp-e-1.dcloud.cisco.com** および **dcloud.cisco.com** が表示されることを確認します。

ここまでで、Expressway 証明書が適切であり、ベスト プラクティスに従っている状態になったため、次に Mobile and Remote Access（MRA）を設定します。

B. Expressway-C の Mobile and Remote Access の設定

このセクションでは、Expressway-C で Expressway Mobile and Remote Access（MRA）を設定します。最初に Mobile and Remote Access を有効にし、コラボレーション アプリケーション ドメインを設定します。次に、コラボレーション アプリケーション サーバ（Unified CM、IM & P、Unity Connection）を検出し、Expressway-E へのトラバーサル ゾーンを設定します。最後に、自動的に設定されたトラバーサル ゾーン、検索ルール、HTTP 許可/ホワイト リストを確認します。

4. Expressway-C で Mobile and Remote Access を有効にする

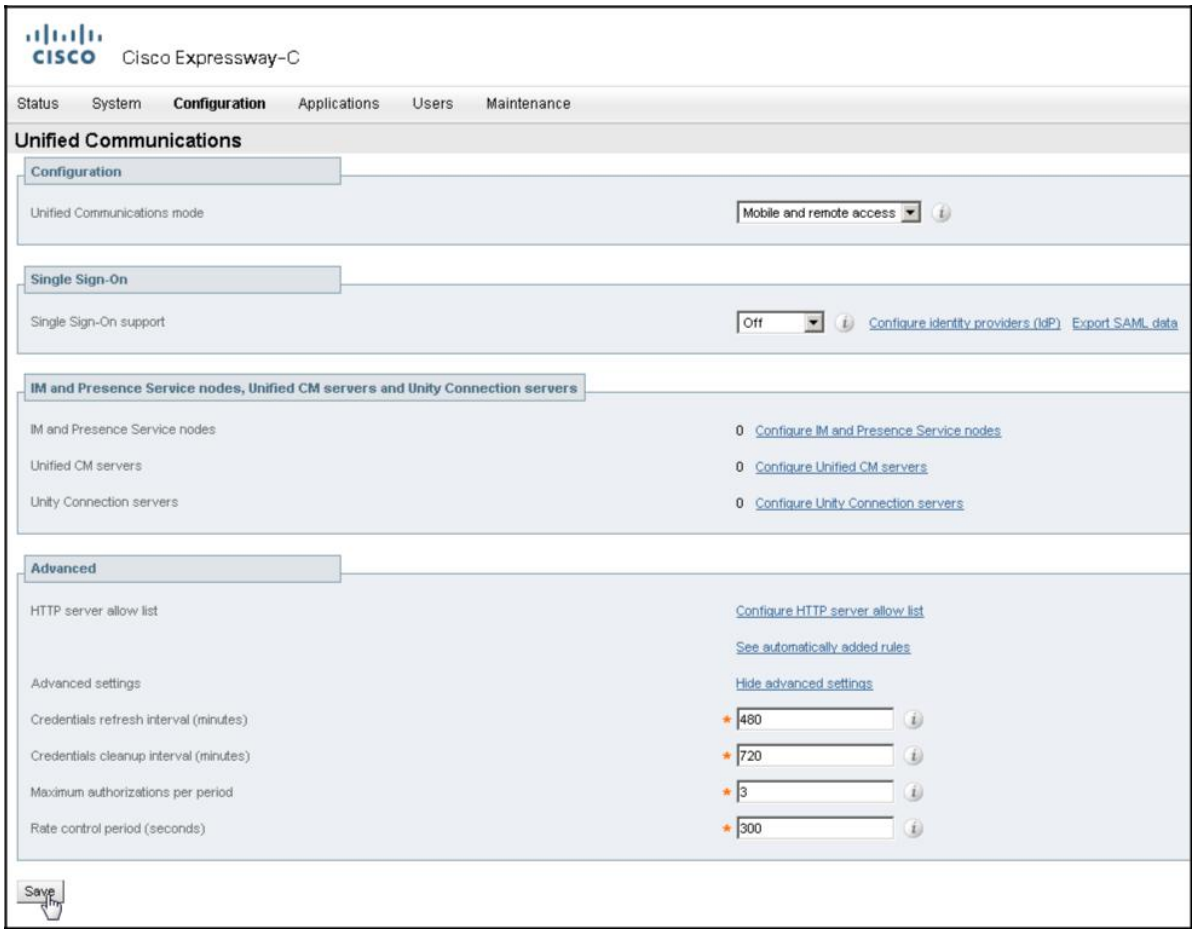
   Expressway-C の管理インターフェイス：https://exp-c-1.dcloud.cisco.com/（ユーザ名/パスワード：**admin/dCloud123!**）に戻ります。

   [設定（Configuration）] > [Unified Communications] > [設定（Configuration）] に移動します。[Unified Communications モード（Unified Communications mode）] ドロップダウン メニューから [Mobile and remote access] を選択します（図 A.19 を参照）。

   図 A.19 Expressway-C で Mobile and Remote Access を有効化

   [シングルサインオンのサポート（Single Sign-On support）] ドロップダウン リストから [オフ（Off）] を選択して無効にします。他のすべての設定をデフォルトのままにして [保存（Save）] をクリックします（図 A.20 を参照）。

図 A.20 Expressway-C で Mobile and Remote Access を設定

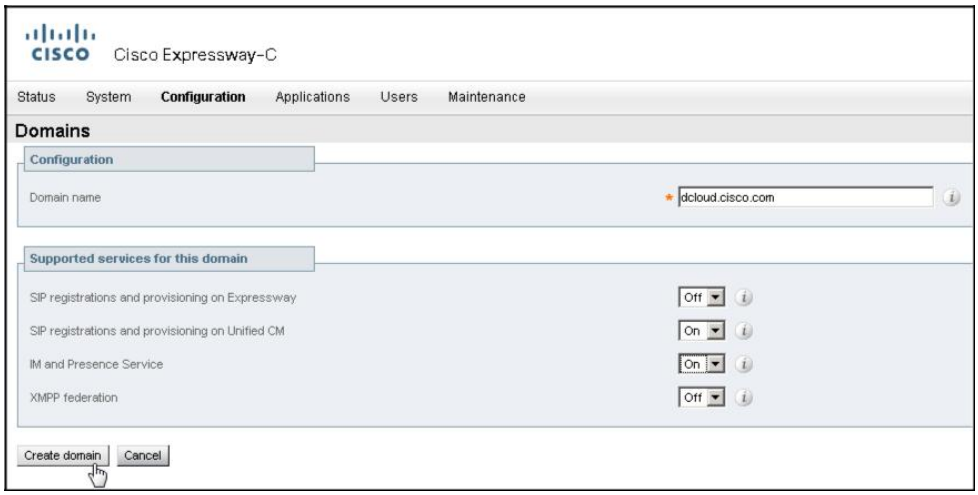


5. コラボレーション アプリケーション/サービス ドメインを設定する

次に、Expressway-C の管理インターフェイス（https://exp-c-1.dcloud.cisco.com/ - ユーザ名/パスワード：**admin/dCloud123!**）で、コラボレーション アプリケーションおよびサービスと関連付けるドメインを設定します。[設定（Configuration）] > [ドメイン（Domains）] に移動し、[新規（New）] をクリックしてドメインを追加します。

図 A.21 に示すように、新しい [ドメイン（Domains）] ページで、[ドメイン名（Domain name）] に **dcloud.cisco.com** と入力します。[サポートするサービス（Supported services）] で、[Expressway への SIP の登録およびプロビジョニング（SIP registration and provisioning on Expressway）] を [オフ（Off）] に、[Unified CM への SIP の登録およびプロビジョニング（SIP registration and provisioning on Unified CM）] と [IM and Presence サービス（IM and Presence Service）] を [オン（On）] に設定します（[XMPP フェデレーション（XMPP federation）] は [オフ（Off）] のままにします）。[ドメインの作成（Create domain）] をクリックします。

図 A.21 Expressway-C でコラボレーション アプリケーション用ドメインを設定



表示される画面で、ドメインが作成されたことを確認します（図 A.22 を参照）。

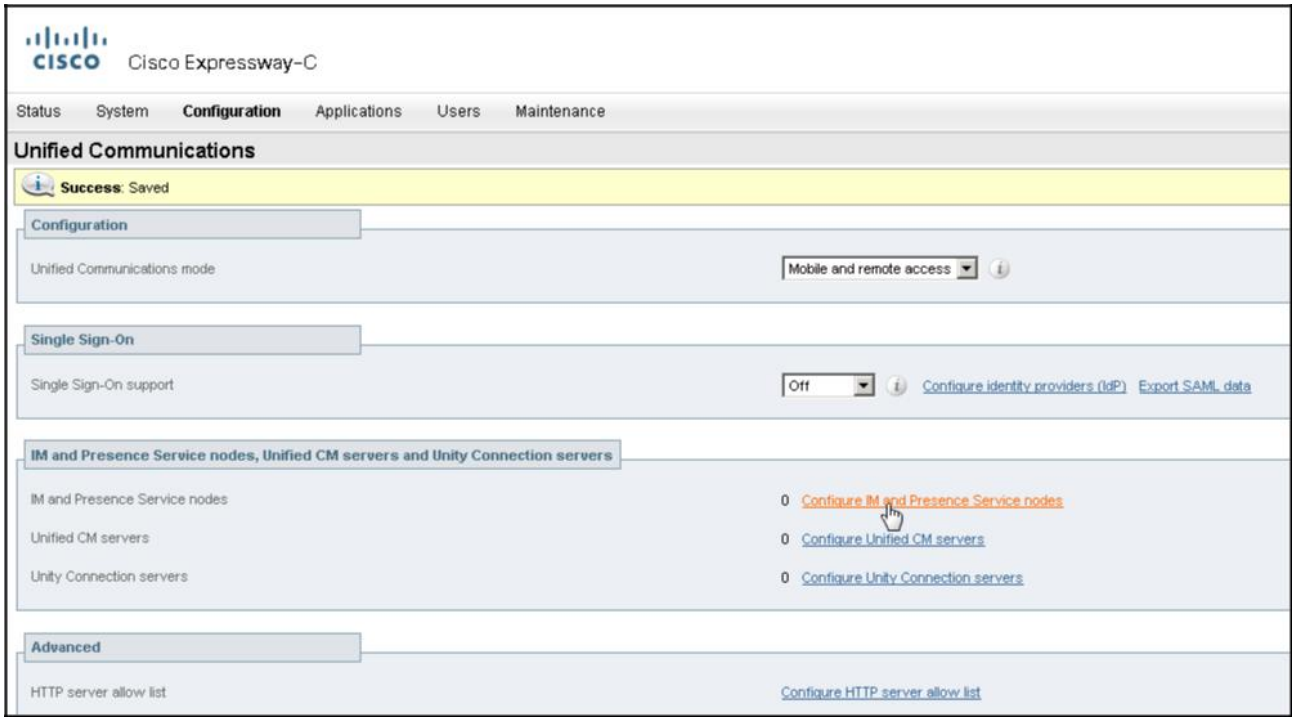
A.22 Expressway-C の dcloud.cisco.com コラボレーション アプリケーション ドメイン

6. コラボレーション アプリケーション サーバ ノードを検出する

コラボレーション サービスに関連付けるドメインを作成したところで、コラボレーション アプリケーション サーバ ノードを検出します。

Expressway-C 管理インターフェイス（https://exp-c-1.dcloud.cisco.com/）で、Unified Communications の設定ページ（[設定（Configuration）] > [Unified Communications] > [設定（Configuration）]）に戻り、[IM&Presence サービスノードの設定（Configure IM and Presence Service nodes）] をクリックします（図 A.23 を参照）。

図 A.23 Expressway-C の Unified Communications の設定：IM and Presence サービス ノード



[新規（New）] をクリックします。次の画面で、図 A.24 に示すように設定します。

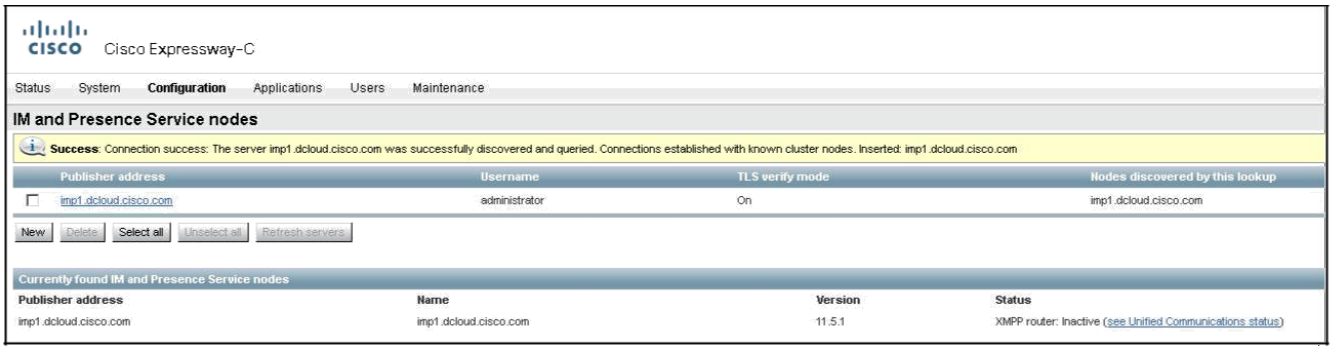
- [IM&Presence サービスデータベースパブリッシャノード（IM and Presence Service database publisher node）]：**imp1.dcloud.cisco.com**
- [ユーザ名（Username）]：**administrator**
- [パスワード（Password）]：**dCloud123!**
- [TLS 検証モード（TLS verify mode）]：[オン（On）]

[アドレスの追加（Add Address）] をクリックします。

図 A.24 Expressway-C での IM and Presence サービス ノード検出

図 A.25 に示すように、IM and Presence サービス ノードの検出に成功したことを確認します。

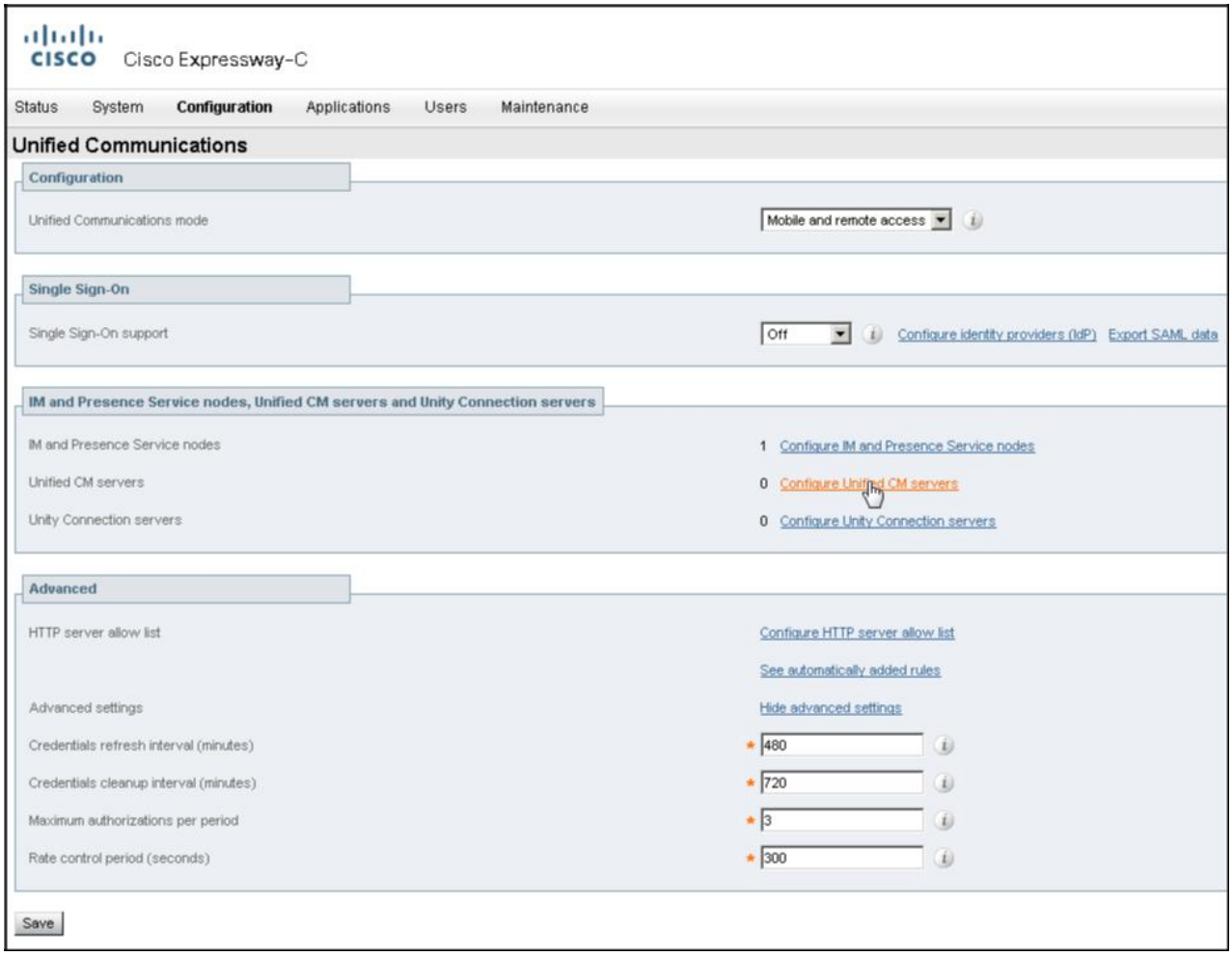
図 A.25 Expressway-C での IM and Presence サービス ノード検出



注: [XMPP ルータ: 非アクティブ (XMPP router: Inactive)] ステータス メッセージは、MRA の設定が完了し、Expressway-C と Expressway-E 間のトラバーサル ゾーンが設定されると表示されなくなります。

Unified Communications 設定ページ ([設定 (Configuration)] > [Unified Communications] > [設定 (Configuration)]) に戻り、[Unified CM サーバの設定 (Configure Unified CM servers)] をクリックします (図 A.26 を参照)。

図 A.26 Expressway-C の Unified Communications の設定: Unified CM サーバ

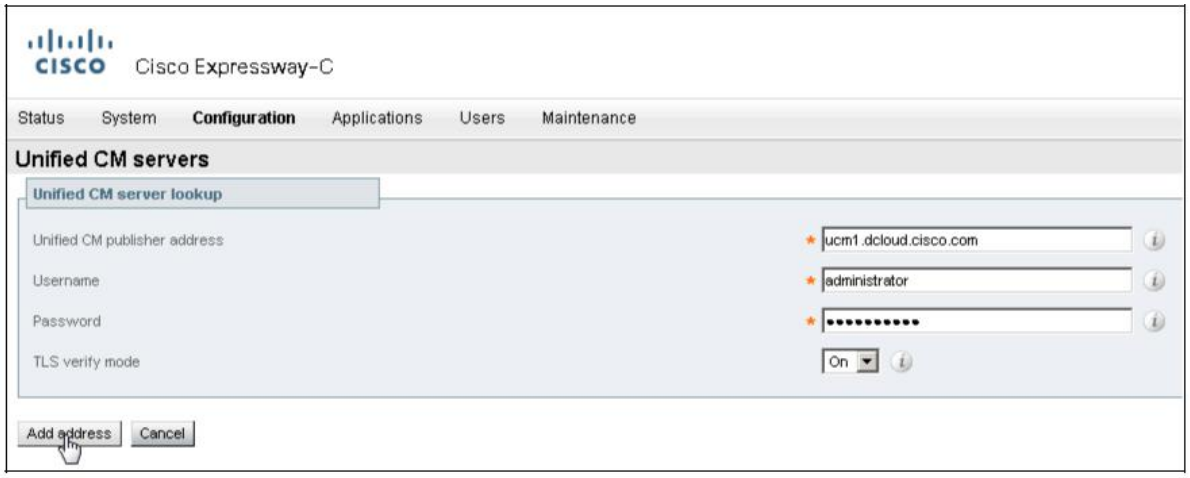


[新規（New）] をクリックします。次の画面で、図 A.27 に示すように設定します。

- [Unified CM パブリッシャアドレス（Unified CM publisher address）]：**ucm1.dcloud.cisco.com**
- [ユーザ名（Username）]：**administrator**
- [パスワード（Password）]：**dCloud123!**
- [TLS 検証モード（TLS verify mode）]：[オン（On）]

[アドレスの追加（Add Address）] をクリックします。

図 A.27 Expressway-C での Unified CM サーバの検出



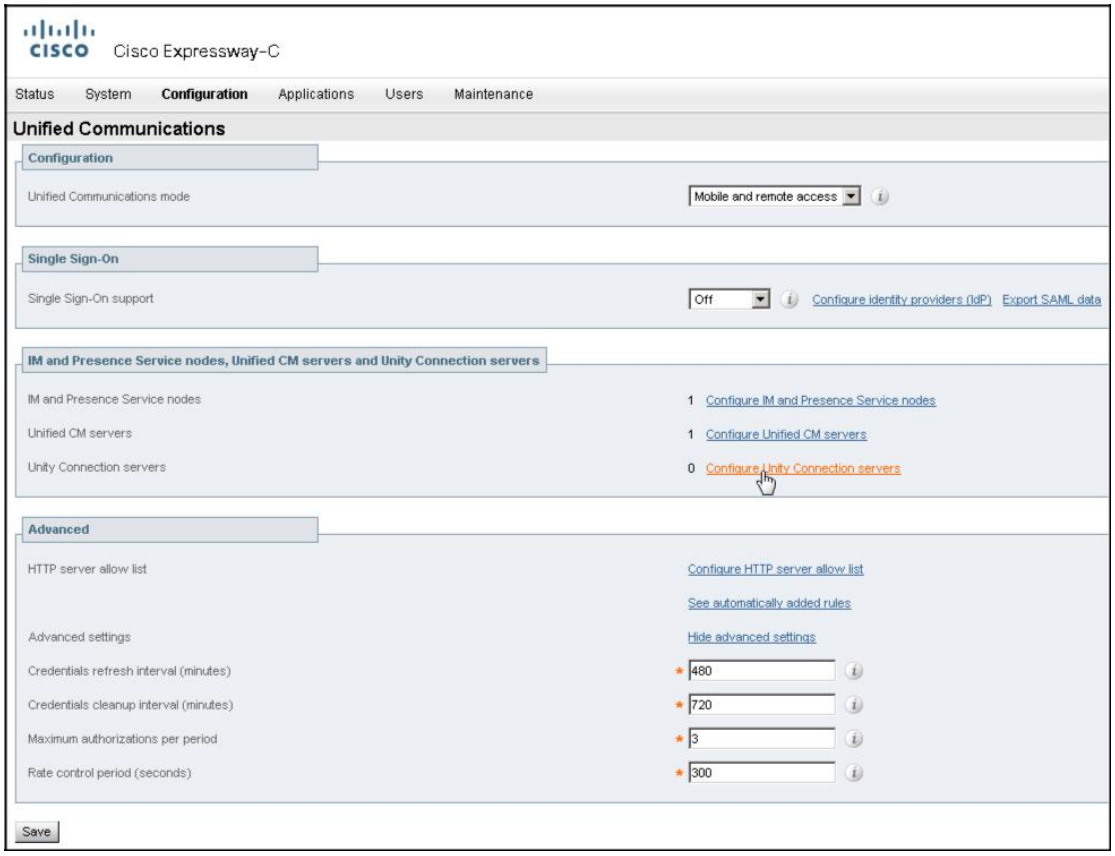
注：このラボでは、上記の設定手順（Unified CM サーバの検出）は実施されていません。この設定は、モジュール 10（Jabber MRA におけるエンドツーエンドの暗号化とアクセス ポリシー）で設定されます。

図 A.28 に示すように、Unified CM サーバの検出に成功したことを確認します。

図 A.28 Expressway-C での Unified CM サーバの検出

最後に、Unity Connection ボイスメール サーバを検出する必要があります。Unified Communications 設定ページ（[設定（Configuration）] > [Unified Communications] > [設定（Configuration）]）に戻り、[Unity Connection サーバの設定（Configure Unity Connection servers）] をクリックします（図 A.29 を参照）。

図 A.29 Expressway-C の Unified Communications の設定：Unity Connection サーバ



[新規（New）] をクリックします。次の画面で、図 A.30 に示すように設定します。

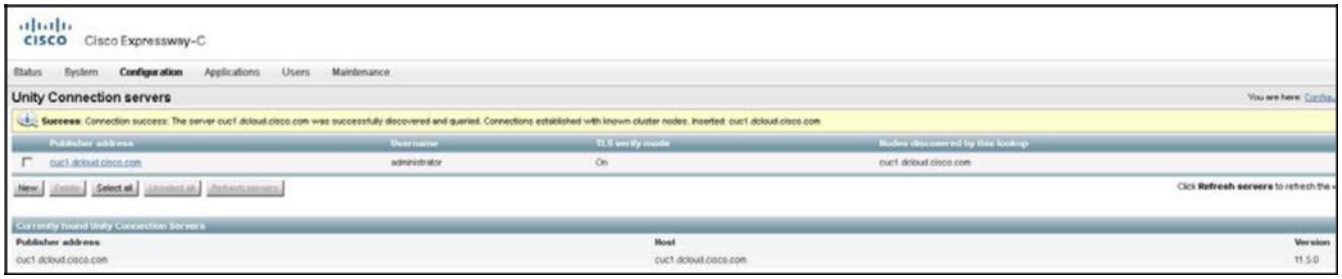
- [Unity Connection のアドレス（Unity Connection address）]：**cuc1.dcloud.cisco.com**
- [ユーザ名（Username）]：**administrator**
- [パスワード（Password）]：**dCloud123!**
- [TLS 検証モード（TLS verify mode）]：[オン（On）]

[アドレスの追加（Add Address）] をクリックします。

図 A.30 Expressway-C での Unity Connection サーバの設定

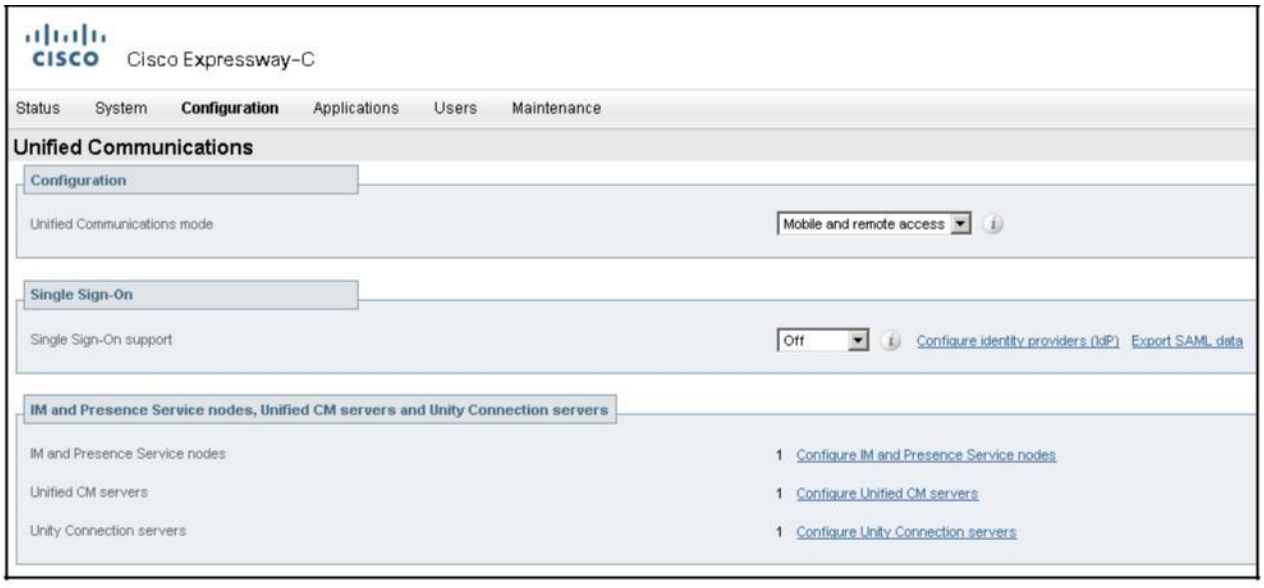
図 A.31 に示すように、Unity Connection サーバの検出に成功したことを確認します。

図 A.31 Expressway-C での Unity Connection サーバの検出



再度 Unified Communications 設定画面（[設定（Configuration）] > [Unified Communications] > [設定（Configuration）]）に戻ると、MRA 導入用の IM and Presence、Unified CM、および Unity Connection サービス ノードが検出されたことを確認できます（図 A.32 を参照）。

図 A.32 すべてのサービス ノードが検出された Unified Communications の設定画面

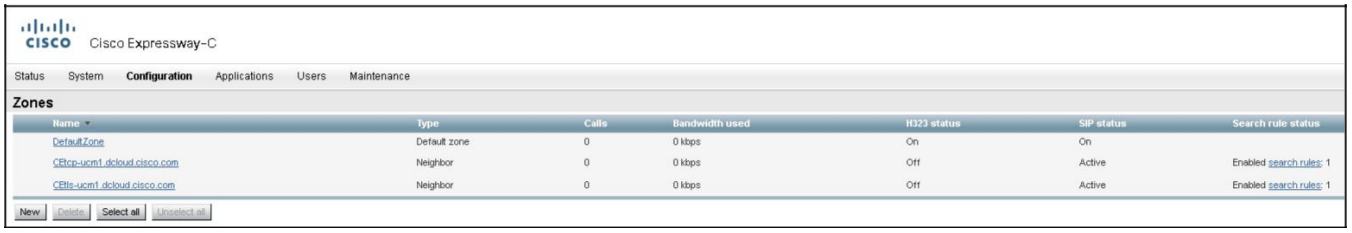


7. デフォルトのトラバーサル ゾーンを確認し、Expressway-E に Unified Communications トラバーサル ゾーンを設定する

Expressway-C での MRA の設定、コラボレーション アプリケーション ドメインの作成、コラボレーション アプリケーション サービス ノードの検出が完了したので、次に、Expressway-E とのセキュアな通信を確立するために、Unified Communications トラバーサル ゾーンを設定する必要があります。

Expressway-C の管理インターフェイス（https://exp-c-1.dcloud.cisco.com/）で、[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動します。図 A.33 に示すように、システムにはすでに複数のドメインが設定されています。1 つ目はデフォルト ゾーン（**DefaultZone**）で、自動的に作成されたものです。デフォルト ゾーンに加えて、2 つのネイバー ゾーン（**CEtcp-ucm1.dcloud.cisco.com**、**CEtls-ucm1.dcloud.cisco.com**）が、Unified CM サーバが検出されたときに自動的に作成されています。

図 A.33 Expressway-C のデフォルト ゾーン



次に、Expressway-E との通信用の新しいトラバーサル ゾーンを設定します。[新規（New）] をクリックして、新しいゾーンを追加します。

[名前（Name）] フィールドに「**mra-traversal**」と入力し、図 A.34 のように [タイプ（Type）] ドロップダウン リストから [Unified Communications トラバーサル（Unified Communications traversal）] を選択します。

図 A.34 Expressway-C に Unified Communications トラバーサル ゾーンを追加

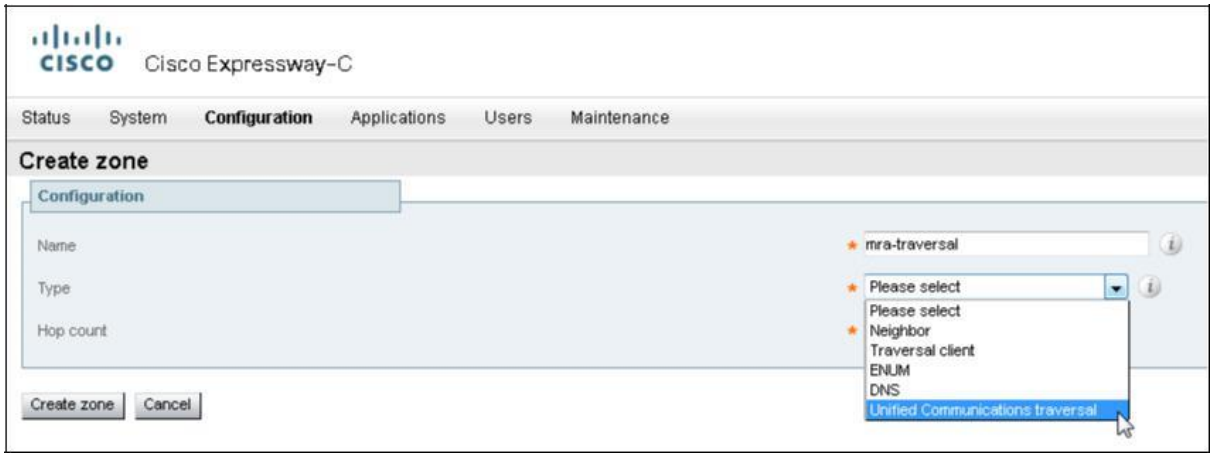
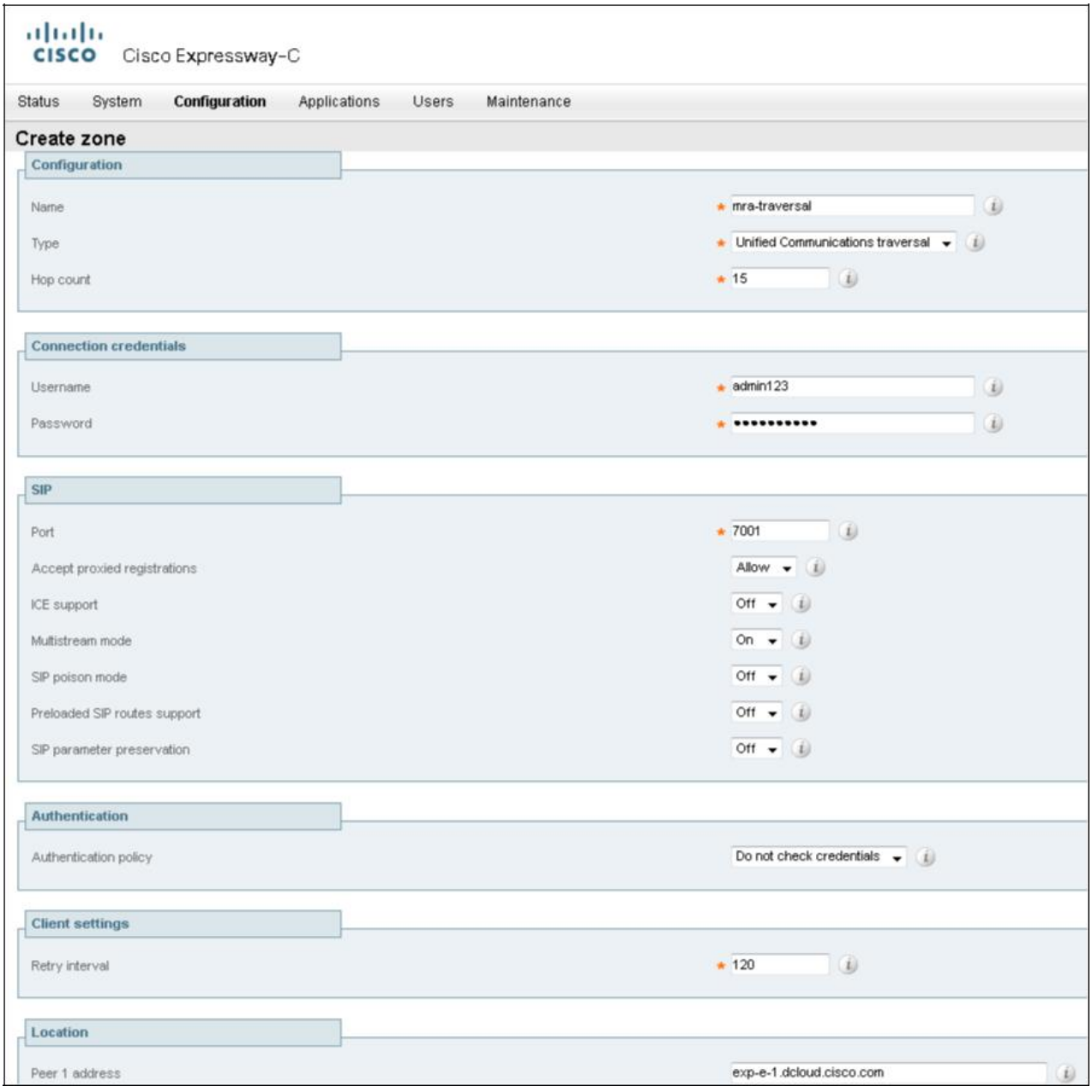


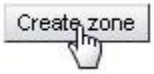
図 A.35 に示すように、残りのゾーン フィールドを次のように設定します（その他のフィールドはすべてデフォルトのまま）。

- [接続クレデンシャル（Connection credentials）] セクション
  - [ユーザ名（Username）]：**admin123**
  - [パスワード（Password）]：**dCloud123!**
- [SIP] セクション
  - [ポート（Port）]：**7001**

- [場所（Location）] セクション
  - [ピア 1 アドレス（Peer 1 address）]：**exp-e-1.dcloud.cisco.com**

図 A.35 Expressway-C で Unified Communications トラバーサル ゾーンを設定





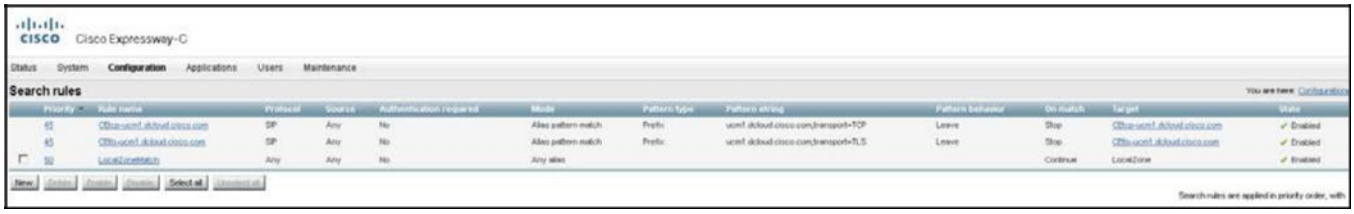
をクリックし、新しい Unified Communications トラバーサル ゾーンを作成して保存します。ゾーン ページに戻ると、作成した Unified Communications トラバーサル ゾーンの SIP ステータスが [失敗（Failed）] になっていますが、これは正常です。Expressway-E で Unified Communications トラバーサル ゾーンを設定すると、SIP ステータスが [アクティブ（Active）] に変わります。

8. 自動 MRA 設定（検索ルール、HTTP ホワイト リスト）を確認する

   Expressway-E MRA の設定に進む前に、Expressway-C のデフォルト/自動検索ルールと HTTP 許可リストを確認します。

Expressway-C の管理インターフェイス（https://exp-c-1.dcloud.cisco.com/）から、[設定（Configuration）] > [ダイヤルプラン（Dial plan）] > [検索ルール（Search rules）] に移動します。図 A.36 に示すように、システムには複数の検索ルールがすでに設定されています。1 つ目はデフォルトの検索ルール（**LocalZoneMatch**）で、システムによって自動的に作成されたものです。デフォルトの検索ルールに加えて、2 つの検索ルール（**CEtcp-ucm1.dcloud.cisco.com**、**CEtls-ucm1.dcloud.cisco.com**）が、Unified CM サーバが検出されたときに自動的に作成されています。

図 A.36 Expressway-C のデフォルトおよび自動 Unified CM 検索ルール

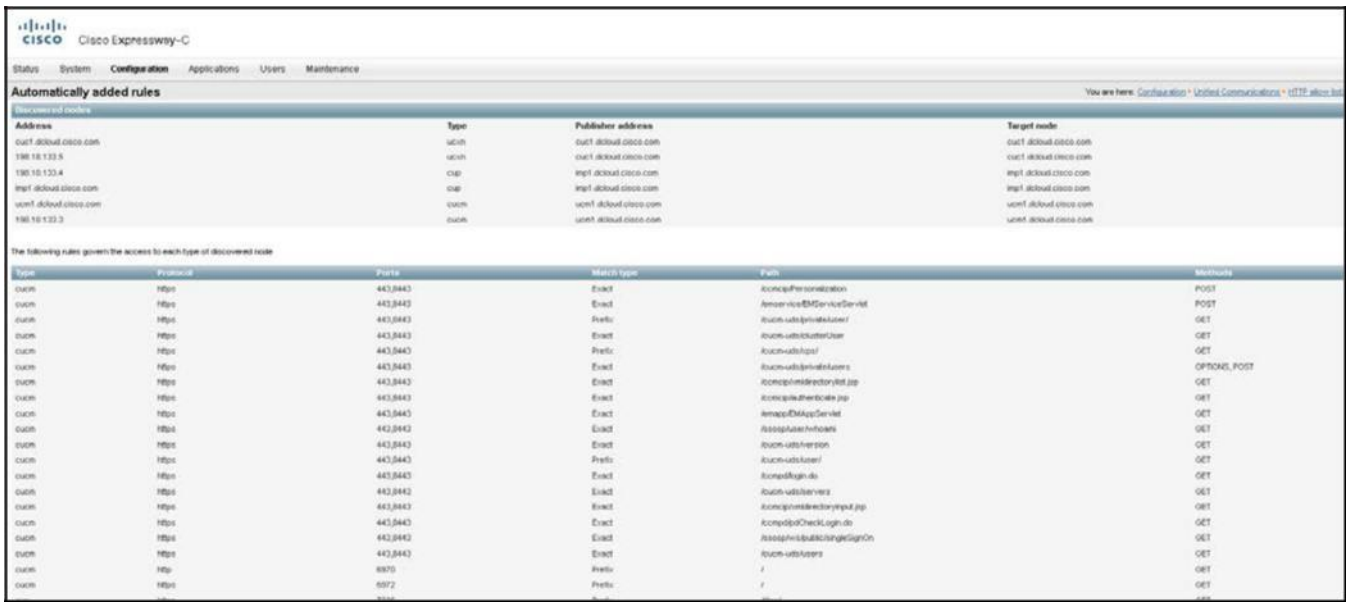


実稼働環境では、環境に応じて検索ルールを追加することがありますが、このラボでは自動生成されたルールのみを使用します。

注：MRA では、MRA トラバーサル ゾーンに関連する検索ルールを使用する必要はありません。MRA クライアントでは、SIP 登録、招待などのメッセージに SIP ルート ヘッダーが含まれます。これは、Expressway-E または Expressway-C を通じた、Cisco Unified CM への SIP パスを示します。Expressway-C では、MRA エンドポイントへの発信のリバース コール フローに、同じルート ヘッダーが付加されます。

[設定（Configuration）] > [Unified Communications] > [HTTP 許可リスト（HTTP Allow List）] > [自動的に追加されたルール（Automatically added rules）] に移動し、システムによって自動的に設定された HTTP 許可ルールを確認します。図 A.37 に示すように、システムで自動的に追加されたこれらのルールによって、検出されたコラボレーション アプリケーション ノードへのアクセスが制御されます。

図 A.37 Expressway-C のデフォルトの Unified Communications HTTP 許可ルール



これらのデフォルトの HTTP 許可ルールにより、MRA で接続されたエンドポイントへのコラボレーション フローが許可されます。

ルールのリストをスクロールして、見慣れたコラボレーション フローがあるかどうかを確認します。たとえば次のような例があります。

- 標準の HTTPS ポート（443、8443）で Unified CM ベースの各種の UDS（ユーザ データ サービス）HTTPS POST および GET コールを許可する、複数のルールがあることがわかります。

- エンドポイント設定のダウンロードに関連付けする許可ルールを 1 つ以上見つけられるかどうか確認してください。これらのフローでは、どのポート番号が使用されるでしょうか（ヒント：Unified CM サーバでは、TFTP サーバにエンドポイント設定が保存されます）。
- ボイスメール通信用の HTTP 許可ルールを見つけてください（リストの末尾までスクロール）。ボイス メッセージ通知用の HTTP 許可ルールでは、どのポート番号が使用されるでしょうか（ヒント：Unity Connection ではサーバ プッシュ通知用に Comet フレームワークを使用します）。

MRA を通じて利用できるコラボレーション サービスの導入とそのタイプに応じて、HTTP 許可ルールを手動で追加する必要があります。このラボでは、デフォルトの HTTP 許可ルールで十分です。

注：Expressway 検索ルール、HTTP ホワイト リスト、ゾーンの詳細については、『Cisco Expressway 基本設定 導入ガイド』、および『Cisco Expressway 経由の Mobile & Remote Access 導入ガイド』（https://www.cisco.com/c/ja_jp/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html）を参照してください。

C. Expressway-E の Mobile and Remote Access の設定

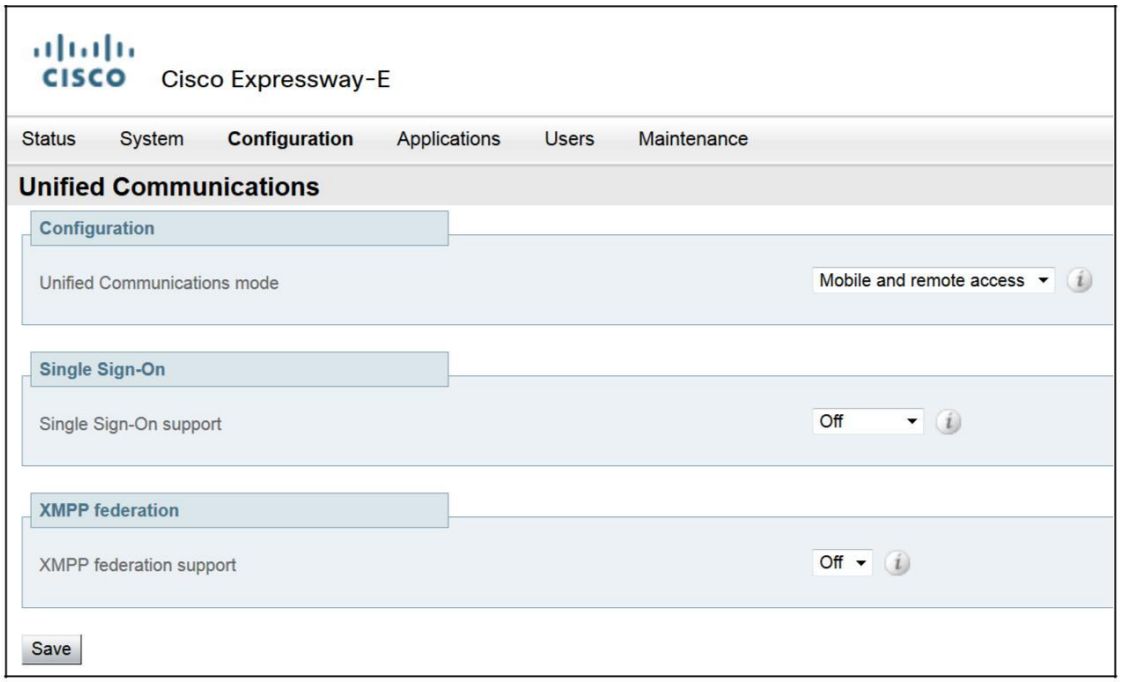
このセクションでは、Expressway の Mobile and Remote Access（MRA）の設定を Expressway-E サーバで行います。Mobile and Remote Access を有効にし、Expressway-C へのトラバーサル ゾーンを設定し、自動的に設定されるトラバーサル ゾーンと検索ルールを確認します。

9. Expressway-E で Mobile and Remote Access を有効にする

   Expressway-E の管理インターフェイス：https://exp-e-1.dcloud.cisco.com/（ユーザ名/パスワード：**admin/dCloud123!**）に移動します。

   [設定（Configuration）] > [Unified Communications] > [設定（Configuration）] に移動します。[Unified Communications モード（Unified Communications mode）] ドロップダウン メニューから [Mobile and remote access] を選択します（図 A.38 を参照）。

図 A.38 Mobile and Remote Access 用の Expressway-E の設定

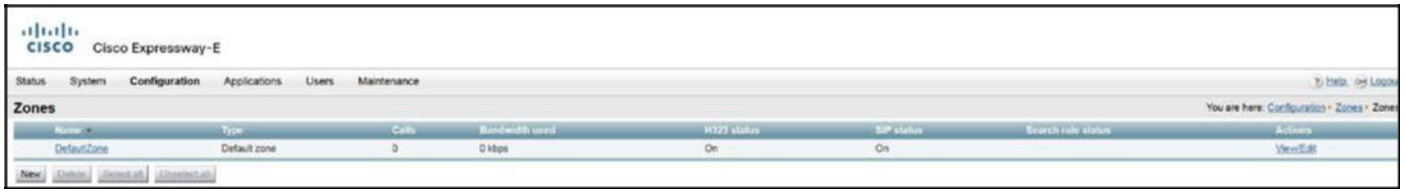


シングル サインオンおよび XMPP フェデレーション パラメータは [オフ(Off)] のままにし(ラボではこれらの機能を有効にしないため)、Save ボタンをクリックします。

10. デフォルトのトラバーサル ゾーンを確認し、Expressway-E へのトラバーサル ゾーンを設定する

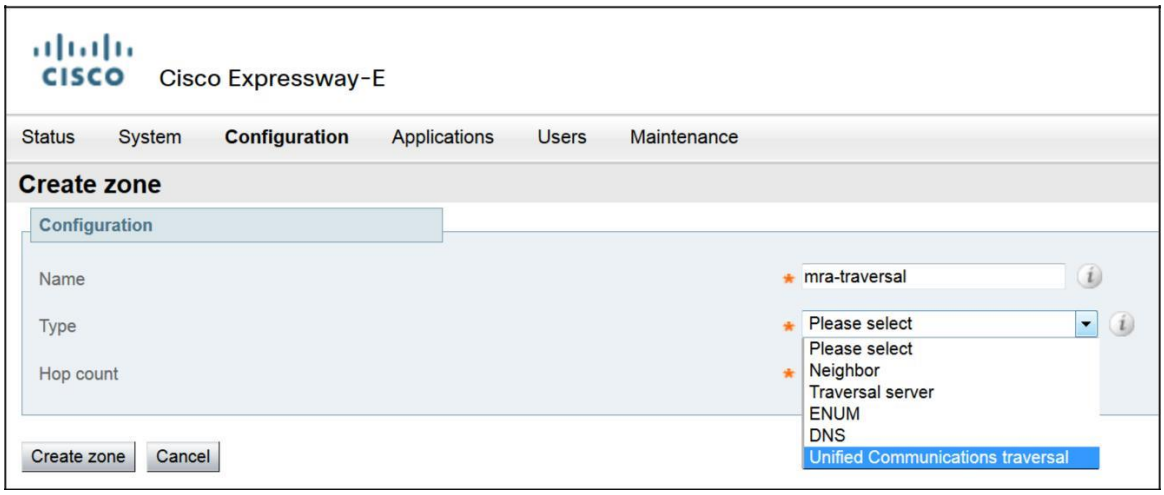
[設定(Configuration)] > [ゾーン(Zones)] > [ゾーン(Zones)] に移動します。デフォルトでは、Expressway-E には DefaultZone だけが作成されています(図 A.39 を参照)。

図 A.39 Expressway-E のデフォルト ゾーン



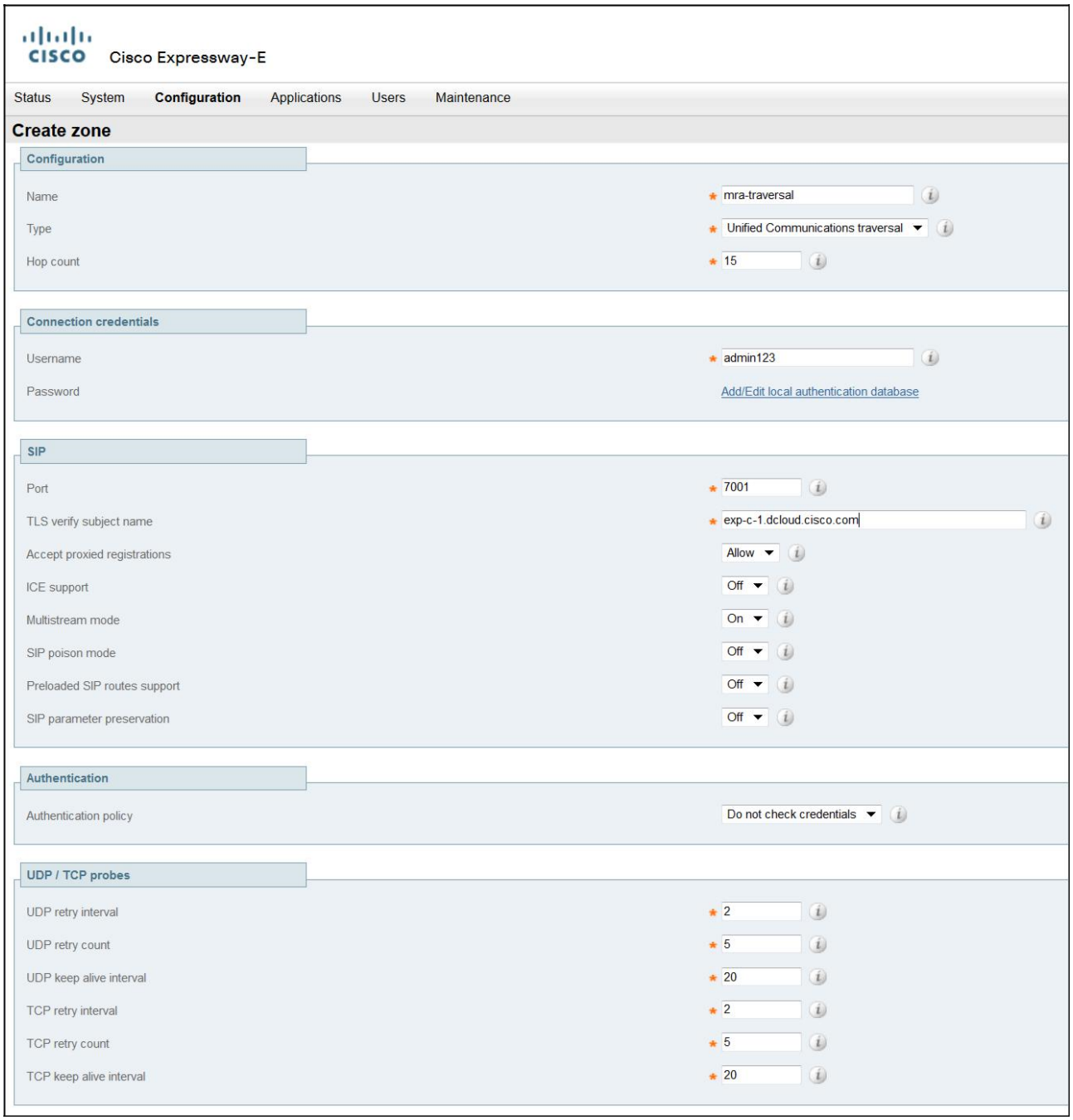
New ボタンをクリックして、Expressway-E の MRA トラバーサル ゾーンを作成します。「**mra-traversal**」という名前を付け、[タイプ(Type)] で [Unified Communications トラバーサル(Unified Communications traversal)] を選択します。[ホップ数(Hop Count)] はデフォルト値(15)のままにします図 A.40 を参照してください。

図 A.40 Expressway-E MRA トラバーサル ゾーンの作成



Unified Communications トラバーサルを選択すると、詳細なゾーン設定画面が表示されます(図 A.41 を参照)。

図 A.41 Expressway-E の詳細な MRA トラバーサル設定

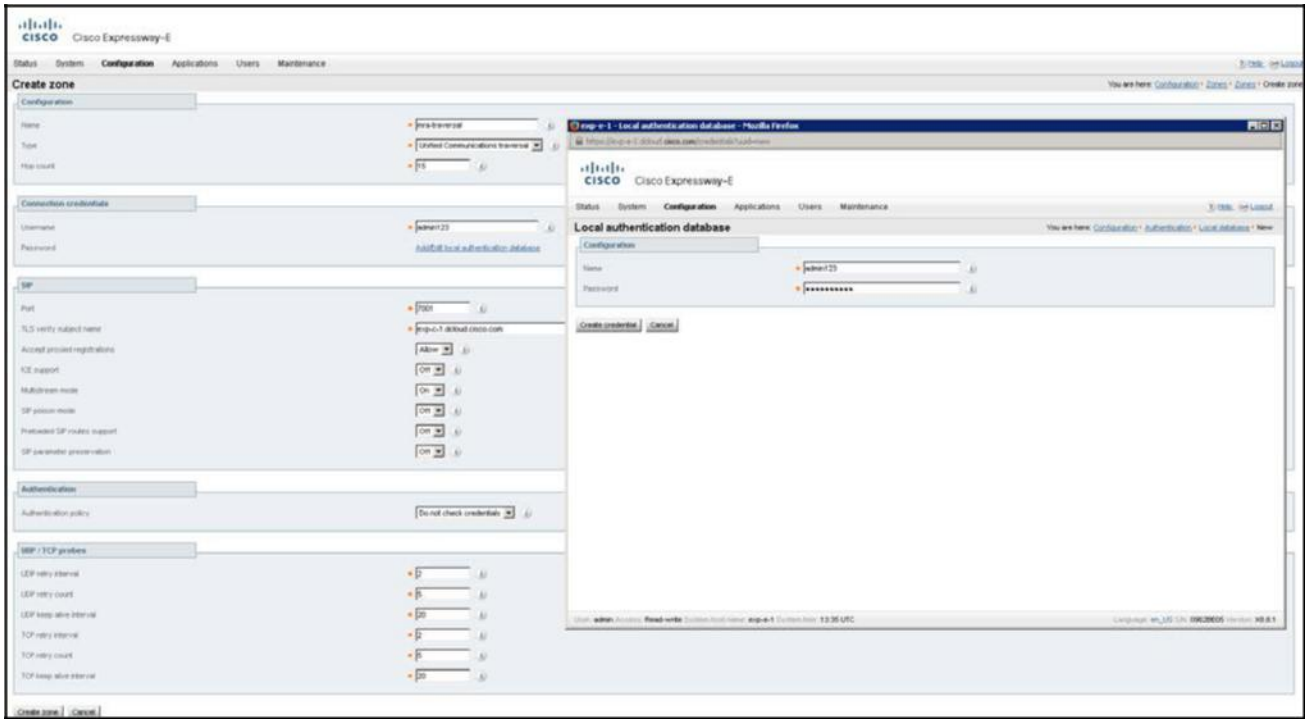


[接続クレデンシャル（Connection Credentials）] と [TLS 検証サブジェクト名（TLS verify subject name）] 以外の設定パラメータはデフォルトのままにします。TLS 検証のエントリには、Expressway-C 証明書の CN を設定します。ラボでは **exp-c-1.dcloud.cisco.com** になります。[接続クレデンシャル（Connection Credentials）] の [ユーザ名（Username）] と [パスワード（Password）] には、Expressway-C で設定されたクレデンシャル（**admin123**/**dCloud123!**）が反映されます。

[接続クレデンシャル（Connection Credentials）] の [ユーザ名（Username）] フィールドに「**admin123**」と入力し、Add/Edit local authentication database リンクをクリックすると、New エントリが作成され、[ユーザ名（Username）] と [パスワード（Password）] フィールドに、それぞれ「**admin123**」、「**dCloud123!**」と入力されます。Create credential ボタンをクリックします。図 A.42 を参照してください。

注: [ローカル認証データベースの追加/編集(Add/Edit local authentication database)] をクリックしても、ローカルの認証データベース ウィンドウが表示されない場合は、おそらく表示されているブラウザ ウィンドウの背後にあります。現在のウィンドウを最小化して、ローカル認証データベースの設定ページを表示させます。

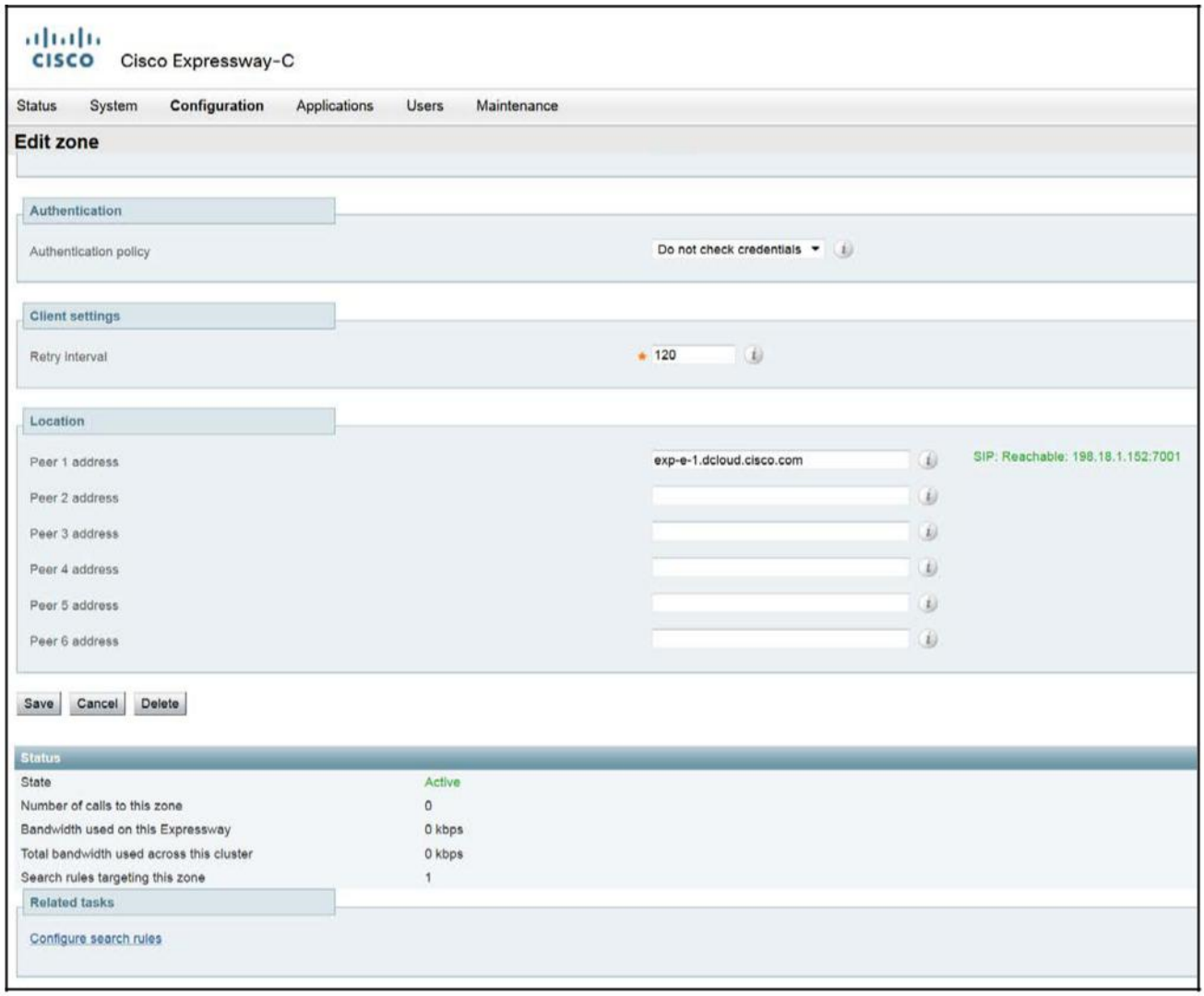
図 A.42 Expressway-E のローカル認証データベースの設定



ローカル認証データベースを更新したらウィンドウを閉じ、[ゾーンの作成(Create zone)] をクリックして、mra-traversal ゾーンの設定を完了します。

Expressway-C と Expressway-E が正しく設定されると、トラバーサル ゾーンがアクティブになります。これを確認するには、Expressway-C または Expressway-E で [設定(Configuration)] > [ゾーン(Zones)] > [ゾーン(Zones)] に移動して、**mra-traversal** ゾーン リンクをクリックします。正しく設定されていれば、ステータスが [アクティブ(Active)] になり、リモートのピア SIP にアクセスできるようになります(Expressway-C の例については図 A.43 を参照)。

図 A.43 Expressway-C のアクティブな MRA トラバーサル ゾーン



注: MRA 設定では、**mra-traversal** ゾーンに対する検索ルールは必要ありません。Expressway-E のデフォルトの検索ルールは **DefaultZone** だけです。これは自動的に作成されます。HTTP ホワイト リストは、Expressway-E では不要であるか、使用できません。

***** APPENDIX A の終了 *****

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp