SSLを使用したクライアント/サーバ接続の保護

• SSL を使用したクライアント/サーバ接続の保護 （1 ページ）

SSL を使用したクライアント/サーバ接続の保護

はじめに

この章では、Cisco Personal Communications Assistant（Cisco PCA）、および IMAP 電子メール クライアントが Cisco Unity Connection へ安全にアクセスするための、証明書署名要求の作成、SSL 証明書の発行（または外部の認証局による証明書の発行）、および Cisco Unity Connection サーバにおける証明書のインストールについて説明します。

Cisco PCA の Web サイトでは、ユーザが Unity Connection でのメッセージと個人設定の管理に使用できる、各種 Web ツールにアクセスできます。IMAP クライアントから Unity Connection のボイス メッセージへのアクセスは、ライセンスが必要な機能です。

関連資料

この章には、マルチサーバの証明書またはシングルサーバの証明書を使用して、ユーザが証明書署名要求（CSR）を作成、生成、ダウンロードおよびアップロードする必要がある場合の複数のインスタンスが含まれています。詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14*』の「セキュリティ」の章 を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html からご利用いただけます。

SSL 証明書をインストールして Cisco PCA、Unity Connection SRSV および IMAP 電子メール クライアントから Unity Connection へのアクセスを保護するかどうかの決定

Unity Connection をインストールする場合、ローカル自己署名証明書が自動的に作成されてインストールされ、Cicso PCA と Unity Connection との間の通信、IMAP 電子メール クライアントと Unity Connection との間の通信、および Unity Connection SRSV と中央 Unity Connection サーバとの間の通信が保護されます。これは、Cisco PCA と Unity Connection との間のすべてのネットワーク トラフィック（ユーザ名、パスワード、その他のテキスト データ、およびボイス メッセージを含む）が自動的に暗号化され、IMAP クライアントで暗号化を有効にした場合は IMAP 電子メール クライアントと Unity Connection との間のネットワーク トラフィックが自動的に暗号化され、Unity Connection SRSV と中央 Unity Connection サーバとの間のネットワーク トラフィックが自動的に暗号化されることを意味しています。ただし、中間者攻撃のリスクを軽減する必要がある場合は、この章で説明する手順を実行してください。

SSL 証明書のインストールを決定した場合は、認証局の信頼証明書をユーザのワークステーションの信頼されたルート ストアに追加することも検討してください。この追加を行わないと、Cisco PCA にアクセスするユーザ、および一部の IMAP 電子メール クライアントで Unity Connection のボイス メッセージにアクセスするユーザに対して、Web ブラウザでセキュリティ アラートが表示されます。

セキュリティ アラートの管理については、『*User Workstation Setup Guide for Cisco Unity Connection Release 14*』の「Setting Up Access to the Cisco Personal Communications Assistant」の章にある「Managing Security Alerts When Using Self-Signed Certificates with SSL Connections」の項を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user_setup/guide/b_14cucuwsx.html からご利用いただけます。

自己署名証明書の詳細については、『*Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV), Release 14*』の「Security in Cisco Unity Connection Survivable Remote Site Voicemail」の章を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/srsv/guide/b_14cucsrsvx.html からご利用いただけます。

Connection Administration、Cisco PCA、Unity Connection SRSV、および IMAP 電子メール クライアントから Unity Connection へのアクセスの保護

Cisco Unity Connection Administration、Cisco Personal Communications Assistant、Unity Connection SRSV、および IMAP 電子メール クライアントから Unity Connection へのアクセスを保護するには、次のタスクを実行して SSL サーバ証明書を作成およびインストールします。

1. Microsoft 証明書サービスを使用して証明書を発行する場合は、Microsoft 証明書サービスをインストールします。

2. 別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションをインストールします。インストールの方法については、製造元が提供しているドキュメントを参照してください。その後で、タスク 3 に進みます。

   外部の認証局を使用して認定証を発行する場合は、タスク 3 に進みます。

   (注) Microsoft 証明書サービス、または証明書署名要求を作成できる別のアプリケーションをすでにインストールしてある場合は、タスク 3 に進みます。

3. Unity Connection クラスタが設定されている場合は、`set web-security` CLI コマンドを実行するか、あるいはクラスタの両方の Unity Connection サーバ用のマルチサーバ SAN 証明書（SIP 統合の場合のみ）を生成し、両方のサーバに同じ別名を割り当てます。ユーザの別名は、証明書署名要求と証明書に自動的に含められます。`set web-security` CLI コマンドについては、該当する『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html から入手可能です。

4. Unity Connection クラスタを設定している場合は、タスク 3 で割り当てた別名が含まれている DNS A レコードを設定します。最初にパブリッシャ サーバを一覧表示します。これにより、すべての IMAP 電子メール アプリケーション、Cisco Personal Communications Assistant、および Unity Connection SRSV が、同一の Unity Connection サーバ名を使用して Unity Connection ボイス メッセージにアクセスできます。

5. 証明書署名要求を作成する。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。

   Unity Connection クラスタをシングルサーバ証明書署名要求により設定する場合は、Unity Connection クラスタ内の両方のサーバでこのタスクを実行します。

6. Microsoft 証明書サービスを使用してルート証明書のエクスポートおよびサーバ証明書の発行を行う場合は、次を参照します。

   証明書の発行に別のアプリケーションを使用する場合は、証明書の発行についてアプリケーションの資料を参照してください。

   証明書の発行に外部の CA を使用する場合は、外部の CA に証明書署名要求を送信します。外部 CA から証明書が返されたら、タスク 7 に進みます。

   Unity Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。

   Unity Connection クラスタをシングルサーバ証明書署名要求により設定する場合は、Unity Connection クラスタ内の両方のサーバでこのタスクを実行します。

7. ルート証明書とサーバ証明書を Unity Connection サーバにアップロードします。

   Unity Connection クラスタをシングルサーバ証明書署名要求により設定する場合は、Unity Connection クラスタ内の両方のサーバでこのタスクを実行します。

8. Unity Connection IMAP サーバ サービスを再起動して、Unity Connection および IMAP 電子メール クライアントが新しい SSL 証明書を使用するようにします。「Connection IMAP サーバ サービスの再起動」を行います。

   Unity Connection クラスタが設定されている場合は、Unity Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

9. ユーザが Connection Administration、Cisco PCA、または IMAP 電子メール クライアントを使用して Unity Connection にアクセスするたびにセキュリティアラートが表示されないようにするには、ユーザが Unity Connection へのアクセスを行うすべてのコンピュータ上で、次のタスクを実行します。

   タスク 7 で Unity Connection サーバにアップロードしたサーバ証明書を証明書ストアにインポートします。手順は、使用するブラウザまたは IMAP 電子メール クライアントによって異なります。詳細については、ブラウザまたは IMAP 電子メール クライアントのドキュメントを参照してください。

   タスク 7 で Unity Connection サーバにアップロードしたサーバ証明書を Java ストアにインポートします。手順は、クライアント コンピュータ上で実行されているオペレーティング システムによって異なります。詳細については、オペレーティング システムのドキュメントおよび Java ランタイム環境のドキュメントを参照してください。

IMAP サーバ サービスの再起動

ステップ 1 Cisco Unity Connection Serviceability にサインインします。

ステップ 2 [ツール（Tools）] メニューで **[サービス管理（Service Management）]** を選択します。

ステップ 3 [オプション サービス（Optional Services）] セクションで、Connection IMAP サーバ サービスに対し **[停止（Stop）]** を選択します。

ステップ 4 Connection IMAP サーバ サービスが正常に停止したことを示すメッセージが [ステータス（Status）] エリアに表示されたら、このサービスの **[開始（Start）]** を選択します。

Cisco Unified MeetingPlace へのアクセスの保護

MeetingPlace へのアクセスを保護するには、次のタスクを実行します。

1. MeetingPlace に対し SSL を設定します。詳細については、『*Administration Documentation for Cisco Unified MeetingPlace Release 8.0*』の「Configuring SSL for the Cisco Unified MeetingPlace Application Server」の章を参照してください。このガイドは、https://www.cisco.com/c/en/us/support/conferencing/unified-meetingplace/products-maintenance-guides-list.html から入手可能です。

2. Unity Connection と MeetingPlace を統合します。Unity Connection を MeetingPlace の予定表と連動するように設定するときには、セキュリティ トランスポート用に SSL を指定します。

3. Unity Connection サーバで、タスク 1 で MeetingPlace サーバにインストールしたサーバ証明書の入手元認証局のルート証明書をアップロードします。次の点に注意してください。

4. このルート証明書は、MeetingPlace サーバにインストールした証明書と同じものではありません。認証局のルート証明書には、MeetingPlace サーバにアップロードした証明書の信頼性を確認するのに使用できる、公開キーが含まれています。

   - このルート証明書は、MeetingPlace サーバにインストールした証明書と同じものではありません。認証局のルート証明書には、MeetingPlace サーバにアップロードした証明書の信頼性を確認するのに使用できる、公開キーが含まれています。
   - Unity Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。
   - ルート証明書のファイル名には、スペースを含めることはできません。

Unity Connection と Cisco Unity ゲートウェイ サーバ間の通信の保護

ネットワークが Unity Connection で設定されている場合に、Connection Administration、Cisco Personal Communications Assistant、および IMAP 電子メール クライアントから Unity Connection へのアクセスを保護するには、次のタスクを実行して、SSL サーバ証明書を作成し、インストールします。

1. Microsoft 証明書サービスを使用して証明書を発行する場合は、Microsoft 証明書サービスをインストールします。それ以降のバージョンの Windows Server を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、Microsoft 社のドキュメントを参照してください。

   別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションをインストールします。インストールの方法については、製造元が提供しているドキュメントを参照してください。その後で、タスク 2 に進みます。

   外部の認証局を使用して証明書を発行する場合は、タスク 2 に進みます。

   

   （注） Microsoft 証明書サービス、または証明書署名要求を作成できる別のアプリケーションをすでにインストールしてある場合は、タスク 2 に進みます。

2. Unity Connection クラスタが Unity Connection ゲートウェイ サーバ用に構成されている場合は、`set web-security` CLI コマンドをクラスタ内の両方の Unity Connection サーバで実行し、両方のサーバに同じユーザの別名を割り当てます。ユーザの別名は、証明書署名要求と証明書に、自動的に含められます。`set web-security` CLI コマンドについては、該当す

る『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html から入手可能です。

3. Unity Connection ゲートウェイ サーバに対応して Unity Connection クラスタを設定している場合は、タスク 2 で割り当てた別名が含まれている DNS A レコードを設定します。最初にパブリッシャ サーバを一覧表示します。これにより、Cisco Unity が同じ Unity Connection サーバ名を使用して Unity Connection のボイス メッセージにアクセスできます。

注 Unity Connection ゲートウェイ サーバで、証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。Unity Connection クラスタが設定されている場合は、Unity Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

注 Cisco Unity ゲートウェイ サーバで、証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。Cisco Unity フェールオーバーが設定されている場合は、このタスクをプライマリ サーバとセカンダリ サーバに対して実行します。

4. ルート証明書のエクスポートとサーバ証明書の発行に Microsoft 証明書サービスを使用している場合は、「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」で説明する手順を実行します。

   証明書の発行に別のアプリケーションを使用する場合は、証明書の発行についてアプリケーションの資料を参照してください。

   外部の CA を使用して証明書を発行する場合は、証明書署名要求をその外部 CA に送信します。外部 CA から証明書が返されたら、タスク 7 に進みます。

   Unity Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。

   このタスクを、Unity Connection サーバ（Unity Connection クラスタが設定されている場合は両方のサーバ）と Cisco Unity サーバ（フェールオーバーが設定されている場合は両方のサーバ）に対して実行します。

5. ルート証明書とサーバ証明書を Unity Connection サーバにアップロードします。

(注) Unity Connection クラスタが設定されている場合は、Unity Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

6. Unity Connection IMAP サーバ サービスを再起動して、Unity Connection および IMAP 電子メール クライアントが新しい SSL 証明書を使用するようにします。「IMAP サーバ サービスの再起動」を行います。

   Unity Connection クラスタが設定されている場合は、Unity Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

7. ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードします。

(注) フェールオーバーが設定されている場合は、このタスクをプライマリ サーバとセカンダリ サーバに対して実行します。

Cisco Unity ゲートウェイ サーバでの証明書署名要求の作成とダウンロード

ステップ 1 Windows の [スタート（Start）] メニューで、**[プログラム（Programs）]** > **[管理ツール（Administrative Tools）]**> **[インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services (IIS) Manager）]** を選択します。

ステップ 2 Cisco Unity サーバ名を展開します。

ステップ 3 **[Web サイト（Web Sites）]** を展開します。

ステップ 4 **[既定の Web サイト（Default Web Site）]** を右クリックし、**[プロパティ（Properties）]** を選択します。

ステップ 5 [既定の Web サイト プロパティ（Default Web Site Properties）] ダイアログボックスで、**[ディレクトリのセキュリティ（Directory Security）]** タブを選択します。

ステップ 6 [セキュア通信（Secure Communications）] の **[サーバ証明書（Server Certificate）]** を選択します。

ステップ 7 Web サーバ証明書ウィザード（Web Server Certificate Wizard）で、次の手順を実行します。

a) [**Next**] を選択します。

b) **[新しい証明書の作成（Create a New Certificate）]** を選択し、**[次へ（Next）]** を選択します。

c) **[要求を今用意し、後で送信する（Prepare the Request Now, But Send It Later）]** を選択し、**[次へ（Next）]** を選択します。

d) 証明書の名前と長さ（ビット）を入力します。

   512 ビットの長さを選択することを強く推奨します。ビット長を大きくすると、パフォーマンスが低下する可能性があります。

e) [**Next**] を選択します。

f) 組織の情報を入力し、**[次へ（Next）]** を選択します。

g) サイトの共通名として、Cisco Unity サーバのシステム名または完全修飾ドメイン名を入力します。

注意 この名前は、Unity Connection サイト ゲートウェイ サーバが Cisco Unity サーバにアクセスするために URL を構築するのに使用する名前と正確に一致する必要があります。この名前は、Connection Administration の [ネットワーク（Networking）] > [リンク（Links）] > [サイト間リンク（Intersite Links）] ページの [ホスト名（Hostname）] フィールドの値です。

h) [**Next**] を選択します。
i) 地理情報を入力し、**[次へ（Next）]** を選択します。
j) 証明書要求のファイル名と場所を指定します。このファイル名と場所の情報は次の手順で必要となるので、書き留めてください。
k) ファイルは、ディスク、または認証局（CA）のサーバがアクセスできるディレクトリに保存します。
l) [**Next**] を選択します。
m) 要求ファイルの情報を確認し、**[次へ（Next）]** を選択します。
n) **[終了（Finish）]** を選択して、Web サーバ証明書ウィザード（Web Server Certificate Wizard）を終了します。

ステップ 8 **[OK]** をクリックして、[既定の Web サイト プロパティ（Default Web Site Properties）] ダイアログボックスを閉じます。

ステップ 9 [インターネット インフォメーション サービス マネージャ（Internet Information Services Manager）] ウィンドウを閉じます。

Connection IMAP サーバ サービスの再起動

ステップ 1 Cisco Unity Connection Serviceability にサインインします。

ステップ 2 [ツール（Tools）] メニューで **[サービス管理（Service Management）]** を選択します。

ステップ 3 [オプションサービス（Optional Services）] セクションで、Connection IMAP サーバ サービスに対し **[停止（Stop）]** を選択します。

ステップ 4 Connection IMAP サーバ サービスが正常に停止したことを示すメッセージが [ステータス（Status）] エリアに表示されたら、このサービスの **[開始（Start）]** を選択します。

Cisco Unity サーバへのルート証明書とサーバ証明書のアップロード

ステップ 1 Cisco Unity サーバで、コンピュータ アカウントの証明書 MMC をインストールします。

ステップ 2 証明書をアップロードします。詳細については、Microsoft 社のドキュメントを参照してください。

Microsoft 証明書サービスのインストール（Windows Server 2008）

サードパーティの認証局を使用して SSL 証明書を発行する場合や、Microsoft 証明書サービスがすでにインストールされている場合は、この項の手順を省略してください。

ステップ 1 [サーバマネージャ（Server Manager）] を開き、[役割の追加（Add Roles）] をクリックし、[次へ（Next）] をクリックして、[Active Directory 証明書サービス（Active Directory Certificate Services）] をクリックします。[次へ（Next）] を 2 回クリックします。

ステップ 2 [役割サービスの選択（Select Role Services）] ページで、[認定機関（Certification Authority）] をクリックします。[次へ（Next）] をクリックします。

ステップ 3 [セットアップの種類の指定（Specify Setup Type）] ページで、[スタンドアロン（Standalone）] または [エンタープライズ（Enterprise）] をクリックします。[次へ（Next）] をクリックします。

（注） エンタープライズ CA をインストールするには、ドメインコントローラへのネットワーク接続がなければなりなりません。

ステップ 4 [CA の種類の指定（Specify CA Type）] ページで、[ルート CA（Root CA）] をクリックします。[次へ（Next）] をクリックします。

ステップ 5 [秘密キーの設定（Set Up Private Key）] ページで、[新しい秘密キーを作成する（Create a new private key）] をクリックします。[次へ（Next）] をクリックします。

ステップ 6 [暗号化の構成（Configure Cryptography）] ページで、暗号化サービスプロバイダー、キーの長さおよびハッシュ アルゴリズムを選択します。[次へ（Next）] をクリックします。

ステップ 7 [CA 名を構成（Configure CA Name）] ページで、CA を識別する一意の名前を作成します。[次へ（Next）] をクリックします。

ステップ 8 [有効期間の設定（Set Validity Period）] ページで、ルート CA 証明書を有効にする年数または月数を指定します。[次へ（Next）] をクリックします。

ステップ 9 証明書データベースおよび証明書データベース ログのカスタムの場所を指定しない場合は、[証明書データベースを構成（Configure Certificate Database）] ページで、デフォルトの場所をそのまま使用します。[次へ（Next）] をクリックします。

ステップ 10 [インストール オプションの確認（Confirm Installation Options）] ページで、選択した設定すべてを確認します。これらのオプションのすべてを受け入れる場合は、[インストール（Install）] をクリックして、セットアップ プロセスが終了するまで待ちます。

ステップ 11 [Active Directory 認証局（Active Directory Certificate Authority）] を右クリックします。[役割サービスの追加（Add Role Services）] を選択し、[認証局 Web 登録（Certificate Authority Web Enrollment）]、[オンライン レスポンダー（Online Responder）]、[ネットワークデバイス登録サービス（Network Device Enrollment Service）] のチェックボックスを選択し、これらのサービスをインストールします。

ステップ 12 [サーバマネージャ] ->[ロールの追加（Add Role）] ->[次へ（Next）] と移動し、[Web サーバ（IIS）（Web Server (IIS)）] ボックスを選択して、これをインストールします。

ステップ 13 [Web サーバ（IIS）（Web Server (IIS)）] を右クリックします。[役割サービスの追加（Add Role Services）] を選択し、役割サービスすべてを確認し、インストールします。

ルート証明書のエクスポートとサーバ証明書の発行（Microsoft証明書サービスの場合のみ）

ステップ 1 Microsoft 証明書サービスをインストールしたサーバで、ドメイン管理者グループのメンバであるアカウントを使用して Windows にサインインします。

ステップ 2 Windows の [スタート（Start）] メニューで、**[プログラム（Programs）]** > **[管理ツール（Administrative Tools）]** > **[認定機関（Certification Authority）]** を選択します。

ステップ 3 左側のペインで、**[認証局（ローカル）（Certification Authority (Local)）]** > **< 認証局の名前** を展開します。<認証局の名前> は、「Microsoft 証明書サービスのインストール（Windows Server 2008）」で Microsoft 証明書サービスをインストールしたときに認証局に付けた名前になります。

ステップ 4 ルート証明書をエクスポートします。

a) 認証局の名前を右クリックし、**[プロパティ（Properties）]** を選択します。
b) [全般（General）] タブで、**[証明書の表示（View Certificate）]** を選択します。
c) **[詳細（Details）]** タブを選択します。
d) **[ファイルのコピー（Copy to File）]** を選択します。
e) [証明書のエクスポート ウィザードの開始（Welcome to the Certificate Export Wizard）] ページで、**[次へ（Next）]** を選択します。
f) [エクスポート ファイルの形式（Export File Format）] ページで **[次へ（Next）]** をクリックして、デフォルト値 **[DER Encoded Binary X.509 (.CER)]** を受け入れます。
g) [エクスポートするファイル（File to Export）] ページで、.cer ファイルのパスとファイル名を入力します。Unity Connection サーバからアクセス可能なネットワーク上の場所を選択します。

   パスとファイル名を書き留めます。この情報は後の手順で必要になります。

h) ウィザードでエクスポートが完了するまで、画面に表示される指示に従って操作します。
i) **[OK]** を選択して [証明書（Certificate）] ダイアログボックスを閉じ、もう一度 **[OK]** を選択して [プロパティ（Properties）] ダイアログボックスを閉じます。

ステップ 5 サーバ証明書を発行します。

a) 認証局の名前を右クリックし、[すべてのタスク（All Tasks）] > **[新しい要求の送信（Submit New Request）]** を選択します。
b) 作成した証明書署名要求ファイルの場所を参照し、このファイルをダブルクリックします。
c) [認証局（Certification Authority）] の左側のペインで **[保留中の要求（Pending Requests）]** を選択します。
d) b. で送信した保留中の要求を右クリックし、**[すべてのタスク（All Tasks）]** > **[発行（Issue）]** を選択します。
e) [認証局（Certification Authority）] の左側のペインで **[発行済み証明書（Issued Certificates）]** を選択します。
f) 新しい証明書を右クリックし、**[すべてのタスク（All Tasks）]** > **[バイナリ データのエクスポート（Export Binary Data）]** を選択します。

g) [バイナリ データのエクスポート（Export Binary Data）] ダイアログボックスの [バイナリ データが含まれている列（Columns that Contain Binary Data）] リストで、**[バイナリ証明書（Binary Certificate）]** を選択します。

h) **[バイナリ データをファイルに保存する（Save Binary Data to a File）]** を選択します。

i) [OK] を選択します。

j) [バイナリ データの保存（Save Binary Data）] ダイアログボックスで、パスとファイル名を入力します。Cisco Unity Connection サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

k) [OK] を選択します。

ステップ 6 [認証局（Certification Authority）] を閉じます。