証明書とサーバ セキュリティの管理

この章は、次の項で構成されています。

- サーバ証明書の管理 （1 ページ）
- 証明書署名要求の生成 （2 ページ）
- 自己署名証明書の作成 （5 ページ）
- Windows を使用した自己署名証明書の作成 （7 ページ）
- サーバ証明書のアップロード （8 ページ）
- キー管理相互運用性プロトコル （9 ページ）

サーバ証明書の管理

証明書署名要求（CSR）を生成して新しい証明書を取得し、新しい証明書を Cisco IMC にアップロードして現在のサーバ証明書と交換することができます。サーバ証明書は、Verisign のようなパブリック認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。生成される証明書キーの長は 2048 ビットです。

（注） この章に記載されている以下のタスクを実行する前に、Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 Cisco IMC から CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書を Cisco IMC にアップロードします。

（注） アップロードされた証明書は、Cisco IMC によって生成された CSR から作成される必要があります。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

（注） [Common Name] および [Organization Unit] フィールドには特殊文字（たとえばアンパサンド（**&**））を使用しないでください。

始める前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Certificate Management] をクリックします。

ステップ 3 [Actions] 領域で、[Generate New Certificate Signing Request] リンクをクリックします。

[Generate New Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 4 [Generate New Certificate Signing Request] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[コモンネーム（Common Name）] フィールド	Cisco IMC の完全修飾名。 デフォルトでは、サーバの CN は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号で YYYYYY はシリアル番号です）。 最新バージョンにアップグレードするとき、CN はそのまま保持されます。

名前	説明
サブジェクト代替名（SAN）	これでサブジェクト代替名の追加の入力パラメータを入力できます。これには証明書の subject フィールドを使用して関連付けられるさまざまな値を使用できます。 SAN のさまざまなオプションには次のものがあります。 • Email • DNS name • IP アドレス • Uniform Resource Identifier（URI） （注） このフィールドは任意です。各タイプの SAN インスタンスの数をどのようにも設定できますが、インスタンスの合計の数は 10 を超えることはできません。
[Organization Name] フィールド	証明書を要求している組織。
[組織単位（Organization Unit）] フィールド	組織ユニット。
[地域（Locality）] フィールド	証明書を要求している会社の本社が存在する市または町。
[State Name] フィールド	証明書を要求している会社の本社が存在する州または行政区分。
[Country Code] ドロップダウンリスト	会社が存在する国。
[Email] フィールド	会社の電子メールの連絡先。
Signature Algorithm	証明書署名要求を生成するための署名アルゴリズムを選択できます。次のいずれかになります。 • SHA384 • SHA1 • SHA256 • SHA512 証明書署名要求を生成するために選択されているデフォルトの署名アルゴリズムは SHA384 です。

名前	説明
[Challenge Password (チャレンジ パスワード)] チェック ボックス	**チャレンジ パスワード**は、証明書署名要求 (CSR) ダイアログ ボックスに組み込まれています。このダイアログ ボックスでは、発行元認証局 (CA) が証明書を認証するために使用します。 **[Challenge Password (チャレンジ パスワード)]** オプションが選択されている場合は、有効なパスワード文字列を入力するためユーザーに**チャレンジ パスワード文字列**が入力されます。 （注） ユーザーには**チャレンジ パスワード**を選択しないオプションがあります。この場合、**チャレンジ パスワード文字列**は入力されません。ただし、ユーザーは CSR の正常な生成に進むことができます。
[String Mask (文字列マスク)] ドロップダウン リスト	これにより、証明書署名要求 (CSR) ダイアログ ボックスで許可される文字列タイプのマスクが設定されます。このオプションは、特定のフィールドの特定の文字列タイプを使用する場合にはマスクしません。文字列のタイプは次のとおりです。 • **デフォルト**: Printablestring、T61String、bmpstring を使用します。 • **pkix**: Printablestring、BMPstring を使用します。 • **utf8only**: UTF8Strings のみを使用します。 • **nombstr**: Printablestring、T61String (BMPStrings または UTF8Strings 以外) を使用します。
[**Self Signed Certificate**] チェックボックス	自己署名した証明書を生成します。 警告 証明書の生成が成功した後、Cisco IMC Web GUI が再起動します。管理コントローラとの通信が一時的に切断され、再ログインが必要な場合があります。 （注） イネーブルの場合、CSR が生成され、自動的に署名およびアップロードが行われます。

（注） 自己署名証明書が有効な場合は、ステップ 5 および 6 を無視します。

ステップ 5 [Generate CSR] をクリックします。

[Opening csr.txt] ダイアログボックスが表示されます。

ステップ 6 CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。

a) [Open With] をクリックして csr.txt を表示します。

b) [Save File] をクリックしてから [OK] をクリックし、ローカル マシンに csr.txt を保存します。

次のタスク

- 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。
- 証明書のタイプが [Server] であることを確認します。

自己署名証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注） これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

始める前に

- 組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 2048`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。

	コマンドまたはアクション	目的
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** 例： `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。
ステップ 5	**openssl x509 -noout -text -purpose -in <cert file>** 例： `openssl x509 -noout -text -purpose -in <cert file>`	生成された証明書のタイプが [Server] であることを確認します。 （注） フィールド [Server SSL] および [Netscape SSL] サーバの値が [Yes] でない場合は、タイプが [Server] の証明書を生成するように openssl.conf が設定されていることを確認します。
ステップ 6	（任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、ステップ 1 ～ 5 を繰り返して証明書を再生成します。	正しい使用期限が設定された証明書が作成されます。

例

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 2048 Generating RSA private key, 2048
bit long modulus .............++++++ .....++++++ e is 65537 (0x10001) #
/usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt You are about
 to be asked to enter information that will be incorporated into your certificate
 request. What you are about to enter is what is called a Distinguished Name
or a DN. There are quite a few fields but you can leave some blank For some
fields there will be a default value, If you enter '.', the field will be left
 blank. ----- Country Name (2 letter code) [GB]:US State or Province Name (full
 name) [Berkshire]:California Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A Common Name (eg, your name or
 your server's hostname) []:example.com Email Address []:admin@example.com #
echo "nsCertType = server" > openssl.conf # /usr/bin/openssl x509 -req -days
365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
 openssl.conf Signature ok subject=/C=US/ST=California/L=San Jose/O=Example
Inc./OU=Unit A/CN=example.com/emailAddress=john@example.com Getting CA Private
 Key #
```

次のタスク

新しい証明書を Cisco IMC にアップロードします。

Windows を使用した自己署名証明書の作成

始める前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 [IIS マネージャ（IIS Manager）] を開いて管理するレベルに移動します。

ステップ 2 [**Features**] 領域で、[**Server Certificate**] をダブルクリックします。

ステップ 3 [**Action**] ペインで、[**Create Self-Signed Certificate**] をクリックします。

ステップ 4 [Create Self-Signed Certificate] ウィンドウで、[**Specify a friendly name for the certificate**] フィールドに証明書の名前を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 （任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、ステップ 1 ～ 5 を繰り返して証明書を再生成します。
正しい使用期限が設定された証明書が作成されます。

サーバ証明書のアップロード

サーバにアップロードする証明書を参照して選択するか、または署名付き証明書のすべての内容をコピーして [Paste certificate content] テキスト フィールドに貼り付け、それをアップロードできます。

始める前に

- 証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 生成された証明書のタイプが [Server] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

（注） [Cisco IMC Certificate Management] メニューを使用して最初に CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Certificate Management] をクリックします。

ステップ 3 [Actions] 領域で、[Upload Server Certificate] をクリックします。

[Upload Certificate] ダイアログボックスが表示されます。

ステップ 4 [Upload Certificate] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[File] フィールド	アップロードする証明書ファイル。
[Browse] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。
[Paste Certificate content] オプション ボタン	署名付き証明書のすべての内容をコピーして、[Paste certificate content] テキスト フィールドに貼り付けることができるダイアログボックスが開きます。 （注） アップロードする前に証明書が署名済みであることを確認します。
[Upload Certificate] ボタン	証明書をアップロードできます。

ステップ 5 [Upload Certificate] をクリックします。

キー管理相互運用性プロトコル

キー管理相互運用性プロトコル（KMIP）は、主要な管理サーバでキーまたは機密データを処理するためのメッセージ形式を定義する通信プロトコルです。KMIP はオープン スタンダードで、複数のベンダーによってサポートされています。キー管理には、複数の相互運用可能な実装が伴うため、KMIP クライアントは KMIP サーバと効率的に連動します。

（注） KMIP 機能は、C220 M4、C240 M4 および S3260 M4 サーバでのみサポートされています。

自己暗号化ドライブ（SED）には、リアルタイムで着信データを暗号化し、発信データを復号するハードウェアが含まれています。ドライブまたはメディア暗号化キーは、この機能を制御します。しかし、セキュリティを維持するために、ドライブはロックされている必要があります。セキュリティ キー ID とセキュリティ キー（キー暗号キー）を使用すると、この目的を達成できます。キー ID では、ドライブに一意の ID が提供されます。

異なるキーには異なる使用要件があります。現在、ローカル キーの管理および追跡の責任は主にユーザにあるため、人的ミスが生じる可能性があります。ユーザはさまざまなキーとそれらの機能を覚えている必要があり、それが困難な場合があります。KMIP は、この懸念領域に対処し、人的関与なしでキーを効率的に管理します。

クライアント証明書のダウンロード

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Download Client Certificate] をクリックします。

ステップ 5 [Download Client Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Download From Remote Location] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：クライアント証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[Download Through Browser Client] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[Paste Content] オプション ボタン	このオプションを選択することで、署名付き証明書の内容全体をコピーして [Paste Certificate Content] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。

クライアント証明書のエクスポート

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Export Client Certificate] をクリックします。

ステップ 5 [Export Client Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバフィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモートサーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
	• [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local File]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

クライアント証明書の削除

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Delete Client Certificate] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてクライアント証明書を削除するか、または [Cancel] をクリックして操作をキャンセルします。

クライアント秘密キーのダウンロード

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Download Client Private Key] をクリックします。

ステップ 5 [Download Client Private Key] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Download From Remote Location] オプション ボタン	このオプションを選択することで、秘密キーをリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：クライアント秘密キーを保管するサーバの IP アドレスまたはホスト名。[Download Certificate From] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[Download Through Browser Client] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている秘密キーに移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[Paste Content] オプション ボタン	このオプションを選択することで、署名付き秘密キーの内容全体をコピーして [Paste Private Key Content] テキスト フィールドに貼り付けることができます。

次のタスク

クライアント秘密キーのエクスポート

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Export Client Private Key] をクリックします。

ステップ 5 [Export Client Private Key] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
	• [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local File]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

クライアント秘密キーの削除

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] ペインの [Actions] 領域で、[Delete Client Private Key] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてクライアント秘密キーを削除するか、または [Cancel] をクリックして操作をキャンセルします。

ルート CA 証明書のダウンロード

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Download Root CA Certificate] をクリックします。

ステップ 5 [Download Root CA Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Download From Remote Location] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：ルート CA 証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[Download Through Browser Client] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[Paste Content] オプション ボタン	このオプションを選択することで、署名付き証明書の内容全体をコピーして [Paste Certificate Content] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。

ルート CA 証明書のエクスポート

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Export Root CA Certificate] をクリックします。

ステップ 5 [Export Root CA Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバフィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモートサーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
	• [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local File]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ルート CA 証明書の削除

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Delete Root CA Certificate] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてルート CA 証明書を削除するか、または [Cancel] をクリックして操作をキャンセルします。

KMIP ログイン詳細の削除

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] ペインの [Actions] 領域で、[Delete KMIP Login] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックして KMIP ログインの詳細を削除するか、または [Cancel] をクリックして操作をキャンセルします。

KMIP サーバのデフォルト設定への復元

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [KMIP Servers] 領域で、チェックボックスをオンにすることで行を選択し、[Delete] をクリックします。

ステップ 5 プロンプトで [OK] をクリックします。

これで、KMIP サーバがデフォルト設定に復元されます。

KMIP サーバ接続のテスト

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Secure Key Management] タブの [KMIP Servers] 領域で、チェックボックスをオンにすることで行を選択し、[Test Connection] をクリックします。

ステップ 5 接続に成功すると、成功メッセージが表示されます。

セキュアなキー管理設定の表示

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 [Server] タブの [Secure Key Management] をクリックします。

ステップ 4 [Work] ペインで、次の情報を確認します。

名前	説明
[Enable Secure Key Management] チェックボックス	オンにすると、セキュアなキー管理機能を有効にできます。

ステップ 5 [Actions] 領域で、次の情報を確認します。

名前	説明
[Download Root CA Certificate] リンク	ルート CA 証明書を Cisco IMC にダウンロードできます。
[Export Root CA Certificate] リンク	ダウンロードしたルート CA 証明書をローカル ファイルまたはリモート サーバにエクスポートできます。
[Delete Root CA Certificate] リンク	ルート CA 証明書を削除できます。
[Download Client Certificate] リンク	クライアント証明書を Cisco IMC にダウンロードできます。
[Export Client Certificate] リンク	ダウンロードしたクライアント証明書をローカルファイルまたはリモートサーバにエクスポートできます。
[Delete Client Certificate] リンク	クライアント証明書を削除できます。
[Download Client Private Key] リンク	クライアント秘密キーを Cisco IMC にダウンロードできます。
[Export Client Private Key] リンク	ダウンロードしたルート CA 証明書をローカル ファイルまたはリモート サーバにエクスポートできます。
[Delete Client Private Key] リンク	ルート CA 証明書を削除できます。
[Delete KMIP Login] リンク	KMIP ログインの詳細を削除できます。

ステップ 6 [KMIP Servers] 領域で、次のフィールドを確認します。

名前	説明
[ID] フィールド	KMIP サーバ設定の ID。
[IP Address] フィールド	KMIP サーバの IP アドレス。
[Port] フィールド	KMIP サーバへの通信ポート。
[Timeout] フィールド	Cisco IMC が KMIP サーバからの応答を待機する時間。

名前	説明
[Delete] ボタン	KMIP サーバ設定を削除します。
[Test Connection] ボタン	KMIP 接続が成功したかどうかをテストします。

ステップ 7 [KMIP Root CA Certificate] 領域で、次のフィールドを確認します。

名前	説明
[Server Root CA Certificate] フィールド	ルート CA 証明書の可用性を示します。
[Download Status] フィールド	このフィールドには、ルート CA 証明書のダウンロード ステータスが表示されます。
[Download Progress] フィールド	このフィールドには、ルート CA 証明書のダウンロードの進行状況が表示されます。
[Export Status] フィールド	このフィールドには、ルート CA 証明書のエクスポート ステータスが表示されます。
[Export Progress] フィールド	このフィールドには、ルート CA 証明書のエクスポートの進行状況が表示されます。

ステップ 8 [KMIP Client Certificate] 領域で、次のフィールドを確認します。

名前	説明
[クライアント証明書（Client Certificate）] フィールド	クライアント証明書の可用性を示します。
[Download Status] フィールド	このフィールドには、クライアント証明書のダウンロード ステータスが表示されます。
[Download Progress] フィールド	このフィールドには、クライアント証明書のダウンロードの進行状況が表示されます。
[Export Status] フィールド	このフィールドには、クライアント証明書のエクスポート ステータスが表示されます。
[Export Progress] フィールド	このフィールドには、クライアント証明書のエクスポートの進行状況が表示されます。

ステップ 9 [KMIP Login Details] 領域で、次のフィールドを確認します。

名前	説明
[Use KMIP Login] チェックボックス	KMIP ログインの詳細を使用するかどうかを選択できます。

名前	説明
[Login name to KMIP Server] フィールド	KMIP サーバのユーザ名。
[Password to KMIP Server] フィールド	KMIP サーバのパスワード。
[Change Password] チェックボックス	KMIP パスワードを変更できます。
[New Password] フィールド	KMIP サーバに割り当てる新しいパスワードを入力できます。 （注） このオプションは、[Change Password] チェックボックスを有効にしている場合にのみ表示されます。
[パスワードの確認（Confirm Password）] フィールド	このフィールドにもう一度新しいパスワードを入力します。 （注） このオプションは、[Change Password] チェックボックスを有効にしている場合にのみ表示されます。

ステップ 10 [KMIP Client Private Key] 領域で、次のフィールドを確認します。

名前	説明
[Client Private Key] フィールド	クライアント秘密キーの可用性を示します。
[Download Status] フィールド	このフィールドには、クライアント秘密キーのダウンロード ステータスが表示されます。
[Download Progress] フィールド	このフィールドには、クライアント秘密キーのダウンロードの進行状況が表示されます。
[Export Status] フィールド	このフィールドには、クライアント秘密キーのエクスポート ステータスが表示されます。
[Export Progress] フィールド	このフィールドには、クライアント秘密キーのエクスポートの進行状況が表示されます。