



認証局およびデジタル証明書の設定

この章は、次の項で構成されています。

- [認証局およびデジタル証明書について, on page 1](#)
- [認証局およびデジタル証明書の設定, on page 6](#)
- [設定例, on page 18](#)
- [上限, on page 57](#)
- [デフォルト設定, on page 57](#)

認証局およびデジタル証明書について

公開キーインフラストラクチャ（PKI）サポートは、ネットワーク上での安全な通信を確保するために、Cisco MDS 9000 ファミリ スイッチに、デジタル証明書を取得および使用する手段を提供します。PKIサポートにより、IPsec/IKE および SSH の管理機能およびスケラビリティが提供されます。

認証局およびデジタル証明書の目的

認証局（CA）は証明書要求を管理して、ホスト、ネットワーク デバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスまたはユーザーに、秘密キーと公開キーの両方を含むキーペアが設定されます。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザです。一方、公開キーは誰もが知っているものです。両方のキーは、相互に補完的に動作します。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書自体は、受信者が身元を証明し、デジタル証明書を作成するうえで確実に信頼できるサードパーティである、CA により署名されます。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識する必要があります。このプロセスは通常、アウトオブバンド、またはインストール時に実行される操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。IPSec の基本コンポーネントであるインターネット キー交換 (IKE) は、デジタル シグニチャをスケールで使用して、セキュリティ アソシエーションを設定する前にピア デバイスを認証できます。

信頼モデル、トラストポイント、アイデンティティ 証明機関

PKI サポートで使用されるトラスト モデルは、設定可能な複数の信頼できる証明機関 (CA) による階層構造です。各加入エンティティには、セキュリティ プロトコル エクスチェンジによって取得したピアの証明書を確認できるように、信頼できる CA のリストが設定されます。ただし、その証明書がローカルの信頼できる CA の 1 つから発行されていることが条件になります。これを実行するために、CA が自己署名したルート証明書 (または下位 CA の証明書チェーン) がローカルに保管されます。これをローカルに安全に取得して保存するプロセスは、[CA 認証 (CA authentication)] と呼ばれます。これは、CA を信頼する上で必須の手順です。

ローカルに設定された信頼できる CA の情報を [トラストポイント (trust point)]、CA そのものを [トラストポイント CA (trust point CA)] と呼びます。この情報は、CA 証明書 (または下位 CA の証明書チェーン) と、証明書失効チェック情報によって構成されます。

[アイデンティティ (identity)] はデバイスの名前です。[アイデンティティ証明書 (identity certificate)] (公開鍵またはデジタル証明書とも呼ばれる) は、トラストポイントによって署名されたデバイスの公開鍵証明書です。[アイデンティティ CA (identity CA)] は、アイデンティティ証明書を発行できるトラストポイントです。

一連のアプリケーション (たとえば、IPsec/IKE) の ID 証明書を取得するためにトラストポイントを使用して MDS スイッチを [登録 (enrollment)] するプロセスは、登録と呼ばれます。このトラストポイントをアイデンティティ CA と呼びます。

RSA キー ペアおよびアイデンティティ証明書

1 つ以上の RSA キー ペアを生成し、各 RSA キー ペアに、アイデンティティ証明書を取得するために MDS スイッチを登録するトラストポイント CA を関連付けることができます。MDS スイッチは、各 CA について 1 つのアイデンティティ、つまり 1 つのキー ペアと 1 つのアイデンティティ証明書だけを必要とします。

Cisco MDS NX-OS では、RSA キー ペアの生成時に、キーのサイズ (または絶対値) を設定できます。他のデバイスでキー ペアを生成し、MDS スイッチにインポートすることもできます。RSA キー ペアごとにラベルを構成できます。RSA キー ペアの最大値とデフォルトの詳細につ

いては、[Table 1: CA およびデジタル証明書の最大限度](#) および [Table 2: CA およびデジタル証明書のパラメータのデフォルト値](#) を参照してください。

次に、トラストポイント、RSA キー ペア、およびアイデンティティ証明書の関連についての要約を示します。

- トラストポイントは、MDS スイッチが任意のアプリケーション (IKE または SSH など) に関して、ピアの証明書を確認するために信頼する特定の CA になります。
- MDS スイッチには多数のトラストポイントを設定でき、スイッチ上のすべてのアプリケーションは、いずれかのトラストポイント CA から発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- MDS スイッチは、アイデンティティ証明書を取得するためのトラストポイントに相当する CA に登録されます。スイッチを複数のトラストポイントに登録して、各トラストポイントから個別のアイデンティティ証明書を取得できます。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張情報として証明書に保管されます。
- トラストポイントへの登録時に、認証される RSA キー ペアを指定する必要があります。このキー ペアは、登録要求を作成する前に生成して、トラストポイントに関連付ける必要があります。トラストポイント、キー ペア、およびアイデンティティ証明書間のアソシエーションは、証明書、キー ペア、またはトラストポイントを削除して明示的に廃棄されるまで有効です。
- アイデンティティ証明書のサブジェクト名は、MDS スイッチの FQDN です。
- スイッチに 1 つ以上の RSA キー ペアを生成して、各キー ペアを 1 つ以上のトラストポイントに関連付けることができます。ただし、トラストポイントに関連付けることができるキー ペアは 1 つだけです。つまり、各 CA から取得できるアイデンティティ証明書は 1 つだけです。
- 複数のアイデンティティ証明書を (それぞれ異なる CA から) 取得した場合、アプリケーションがピアとのセキュリティプロトコルエクステンションに使用する証明書は、アプリケーションによって異なります。
- 1 つのアプリケーションにトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- 1 つのトラストポイントから複数のアイデンティティ証明書を取得したり、1 つのトラストポイントに複数のキー ペアを関連付ける必要はありません。CA 証明書は、付与されたアイデンティティ (の名前) を一度だけ使用し、同じサブジェクト名で複数の証明書は発行しません。1 つの CA から複数のアイデンティティ証明書を取得する必要がある場合には、同じ CA に対して別のトラストポイントを定義し、別のキー ペアを関連付けて、認証を受けます。ただし、その CA が同じサブジェクト名で複数の証明書を発行できることが条件になります。

複数の信頼された証明機関

複数の信頼された（証明機関）CA のサポートにより、スイッチはさまざまな CA ドメインに登録されているデバイスの識別子を検証できます。複数の信頼できる CA を設定する場合、ピアに証明書を発行した特定の CA に対して、スイッチに登録する必要はありません。代わりに、ピアも信頼する複数の信頼できる CA をスイッチに設定します。スイッチは、ピアの証明書がローカルスイッチのアイデンティティ証明書を定義した CA 以外の CA から発行されていても、設定された信頼できる CA を使用して、ピアの証明書を確認できます。これは、IPsec トンネルを確立するときに IKE で使用できます。

複数のアイデンティティ証明機関

複数のアイデンティティ認証局（CA）をサポートすることにより、スイッチを複数のトラストポイントに登録できます。その結果、異なる CA から1つずつ、複数のアイデンティティ証明書を取得できます。これにより、各ピアで許容される適切な CA から発行された証明書を使用して、多数のピアとの IPsec および他のアプリケーションにスイッチを加入させることができます。

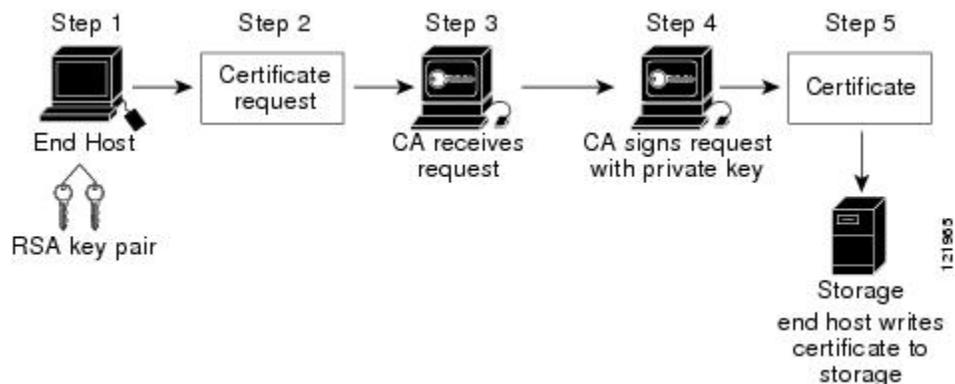
複数の RSA キーペアのサポート機能により、スイッチ上で、登録した各 CA ごとに異なるキーペアを保持できます。したがって、キーの長さなど、他の CA から指定された要件と対立することなく、各 CA のポリシー要件と一致させることができます。トラストポイントへの登録時に、関連付けたキーペアを使用して証明書署名要求を作成できます。

PKI 登録

Public Key Infrastructure (PKI) 登録は、IPsec/IKE または SSH などのアプリケーションに使用する、スイッチのアイデンティティ証明書を取得するプロセスです。このプロセスは、証明書を要求する MDS スイッチと証明機関の間で実行されます。

下の図のおよび次の手順によって、証明書の登録プロセスを説明します。

Figure 1: 証明書の登録プロセス



このプロセスには次の手順が含まれます。

1. RSA 秘密キーと公開キーのキーペアを生成します。

2. 証明書サイン要求 (CSR) を標準形式で生成し、CA に転送します。
3. CA の CSR を承認して、CA の秘密キーで署名された識別子証明書を生成し、それを MDS スイッチ管理者に転送します。要求を承認する場合、CA 上で CA 管理者による手動操作が必要になることがあります。
4. CA からの識別子証明書を MDS スイッチにインストールします。
5. 証明書を MDS スイッチの不揮発性ストレージ領域に保存します。

RSA キーペアと証明書署名要求は、スイッチまたは適切なユーティリティを使用して別のデバイスで生成できます。キーペアが別のデバイスで生成された場合、それらは識別子証明書と同様に MDS スイッチにインストールする必要があります。MDS スイッチは、証明書署名要求に使用できるすべてのフィールドをサポートしているわけではありません。他のデバイスの証明書署名要求生成ツールでは、MDS スイッチからの登録よりも多くのフィールドを指定できる場合があります。

カットアンドペーストによる手動登録

Cisco MDS NX-OS は、手動でのカットアンドペースト方式による証明書の検索および登録をサポートしています。カットアンドペーストによる登録では、スイッチと CA 間で、証明書要求と生成された証明書をカットアンドペーストする必要があります。手順は、次のとおりです。

1. 登録証明書署名要求を作成します。この要求は、base64 符号化テキスト形式で表示されます。
2. 符号化された証明書要求テキストを、Eメールまたは Web 形式にカットアンドペーストして、CA に送信します。
3. Eメールメッセージまたは Web ブラウザでのダウンロードにより、CA から発行された証明書 (base64 符号化テキスト形式) を受信します。
4. 証明書インポート機能の **certificate import** コマンドを使用して、発行された証明書をスイッチにカットアンドペーストします。

ピア証明書の検証

MDS スイッチの PKI サポートを使用して、ピアの証明書を確認できます。スイッチは、IPsec/IKE および SSH など、アプリケーションのセキュリティ エクスチェンジの実行時に、ピアから提示された証明書を確認します。アプリケーションは、提示されたピア証明書の有効性を確認します。ピア証明書の確認プロセスでは、次の手順が実行されます。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること (期限切れでない) ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

失効チェックの場合、スイッチは証明書失効リスト（CRL）方式を使用することができます。トラストポイントではCRL方法を使用して、ピア証明書が取り消されていないことを確認します。

CRLのダウンロード、キャッシュ、およびチェックのサポート

証明書失効リスト（CRL）は、失効された証明書の情報を提供するためにCAによって保持され、レポジトリで公開されます。ダウンロード用のURLが公開され、すべての発行済み証明書にも指定されています。ピア証明書を検証するクライアントは、発行したCAから最新のCRLを入手して、これを使用して証明書が取り消されていないかどうかを確認する必要があります。クライアントは、自身の信頼できるCAのすべてまたは一部のCRLをローカルにキャッシュして、そのCRLが期限切れになるまで必要に応じて使用することができます。

Cisco MDS NX-OS では、トラストポイント用のCRLを事前にダウンロードして、スイッチ証明書ストアにキャッシュされるように手動で設定できます。ピア証明書の確認では、CRLがローカルでキャッシュされ、失効チェックにCRLが使用されるように設定されている場合にかぎり、発行元CAのCRLが参照されます。それ以外の場合、他の失効チェック方式が設定されていない場合は、失効チェックは実行されず、証明書は失効していないと見なされます。このモードのCRLチェックは、CRLオプションと呼ばれています。

証明書および関連キーペアのインポートとエクスポート

CA認証と登録のプロセスの一環として、下位CA証明書（または証明書チェーン）とアイデンティティ証明書を標準のPEM（base64）フォーマットでインポートされています。キーペアが外部で生成された場合は、別の手順でインポートする必要があります。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護されるPKCS12標準フォーマットでファイルにエクスポートできます。この情報を、以降で同じスイッチ（システムクラッシュ後など）または交換したスイッチにインポートできます。PKCS12ファイル内の情報は、RSAキーペア、アイデンティティ証明書、およびCA証明書（またはチェーン）で構成されています。

認証局およびデジタル証明書の設定

ここでは、Cisco MDS スイッチ装置でCAおよびデジタル証明書を相互運用するために必要な作業について説明します。

ホスト名およびIPドメイン名の設定

スイッチのホスト名およびIPドメイン名が未設定の場合には、これらを設定する必要があります。アイデンティティ証明書の情報カテゴリとして、スイッチのFQDNが使用されるからです。また、キーペアの生成時にキーラベルを指定しない場合、デフォルトのキーラベルとしてスイッチのFQDNが使用されます。たとえば、SwitchA.example.comという名前の証明書は、

SwitchA というスイッチのホスト名と、example.com というスイッチの IP ドメイン名で構成されています。



Caution 証明書の生成後に IP ホスト名または IP ドメイン名を変更すると、証明書が無効になることがあります。

スイッチの IP ホスト名および IP ドメイン名を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **switchname SwitchA**

スイッチの IP ホスト名を「SwitchA」として構成します。

ステップ 3 SwitchA(config)# **ip domain-name example.com**

スイッチの IP ドメイン名を「example.com」として構成します。

RSA キーペアの生成

RSA キーペアは、IKE/IPsec および SSH などのアプリケーションによるセキュリティプロトコル エクステンジの実行中に、署名およびセキュリティ ペイロードの暗号化/復号化に使用されます。RSA キーペアは、スイッチの証明書を取得する前に必要になります。

RSA サーバー キーペアを生成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto key generate rsa**

デフォルトのラベルとしてスイッチの FQDN を使用し、デフォルトのモジュラスとして 512 を使用する RSA キーペアを生成します。デフォルトでは、キーペアはエクスポートできません。

Note キーの絶対値を指定するときは、ローカルサイト（MDS スイッチ）および CA（登録先）のセキュリティポリシー（または要件）を考慮する必要があります。

サポートされる最大の RSA キー ペアの詳細については、[上限, on page 57](#) を参照してください。

ステップ 3 switch(config)# **crypto key generate rsa label SwitchA modulus 768**

ラベル SwitchA、モジュラス 768 の RSA キー ペアを生成します。有効なモジュラスの値は 512、768、1024、2048、および 4096 です。デフォルトでは、キー ペアはエクスポートできません。

。

ステップ 4 switch(config)# **crypto key generate rsa exportable**

デフォルトのラベルとしてスイッチの FQDN を使用し、デフォルトのモジュラスとして 512 を使用する RSA キー ペアを生成します。キーはエクスポート可能です。

Caution キー ペアのエクスポート設定は、キー ペアの生成後は変更できません。

Note RKCS#12 形式でエクスポートできるのは、エクスポート可能なキー ペアだけです。

トラストポイント認証局関連付けを作成

Cisco MDS デバイスとトラストポイント CA を関連付ける必要があります。

トラストポイント CA アソシエーションを作成する手順は、次のとおりです。

Procedure

ステップ 1 switch(config)# **crypto ca trustpoint admin-ca**

switch(config-trustpoint)#

「admin-ca」というスイッチが信頼するトラストポイント CA を宣言し、このトラストポイントのトラストポイント構成サブモードを開始します。

Note スイッチに設定できるトラストポイントの最大数は 16 です。

ステップ 2 switch(config)# **no crypto ca trustpoint admin-ca**

(オプション) トラストポイント CA を削除します。

ステップ 3 switch(config-trustpoint)# **enroll terminal**

カットアンドペーストによる手動での証明書登録を指定します（デフォルト）。

Note 手動でのカット&ペーストの証明書の登録は登録でサポートされている唯一の方法です。

ステップ 4 switch(config-trustpoint)# **rsa**keypair SwitchA

登録の目的でこのトラストポイントに関連付ける RSA キーペアのラベルを指定します。RSA キーペアの生成, on page 7の項で作成した名前です。各 CA に 1 つの RSA キーペアだけを指定できます。

ステップ 5 switch(config-trustpoint)# **no** rsakeypair SwitchA

(オプション) トラストポイントから RSA キーペアの関連付けを解除します。

ステップ 6 switch(config-trustpoint)# **end**

switch#

トラストポイント コンフィギュレーション サブモードを終了します。

ステップ 7 switch# **copy running-config startup-config**

実行中の設定を起動構成にコピーして、構成がリブート後も保持されるようにします。

トラストポイントの認証局

信頼できる認証局 (CA) の設定プロセスは、MDS スイッチに対して CA が認証された場合にかぎり、完了します。スイッチは、CA を認証する必要があります。CA を認証するには、CA の公開キーが含まれている CA の自己署名付きの証明書を PEM 形式で取得します。この CA の証明書は自己署名 (CA が自身の証明書を署名したもの) であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。



Note 認証される CA が自己署名した CA ではない場合 (つまり、別の CA の下位 CA で、その別の CA もまた、最終的に自己署名した別の CA の下位 CA であるような場合) には、CA 認証の手順で、認証チェーンに含まれるすべての CA の CA 証明書の完全なリストを入力する必要があります。これは、認証される CA の [CA 認証チェーン (CA certificate chain)] と呼ばれます。CA 証明書チェーン内の証明書の最大数は 10 です。

電子メールまたは Web サイトからの証明書のカットアンドペーストにより CA の証明書を認証するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

Procedure

ステップ 1 switch(config)# **crypto ca trustpoint admin-ca**

```
switch(config-trustpoint)#
```

スイッチが信頼するトラストポイントCAを宣言し、トラストポイントコンフィギュレーションサブモードを開始します。

ステップ 2 switch(config-trustpoint)# **revocation-check crl**

このトラストポイントと同じCAによって発行されたピア証明書の検証の際に適用される失効チェック方式としてCRLを指定します（デフォルト）。

ステップ 3 switch(config-trustpoint)# **revocation-check none**

失効証明書をチェックしません。

ステップ 4 (Optional) switch(config-trustpoint)# **no revocation-check**

デフォルトの方式に戻ります。

証明書署名要求の生成

スイッチの各RSAキーペアについて、トラストポイントCAからアイデンティティ証明書を取得するには、要求を生成する必要があります。さらに、表示された要求を、CA宛てのEメールメッセージまたはWebサイトフォームにカットアンドペーストします。

CAから署名入り証明書要求を生成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **crypto ca enroll admin-ca**

```
Create the certificate request..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: abc123
The subject name in the certificate will be: SwitchA.example.com
Include the switch serial number in the subject name? [yes/no]: no
Include an IP address in the subject name [yes/no]: yes
ip address: 192.168.31.162
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnYXNjby5jb20wgZ8wDQYJ
KoZlHvcNAQEeBBQAdgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNiGJ2kt8r141KY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxBLdKTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAAGGtZAVBqkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsQGSib3DQeJ
DjEpMCCwJQYDVR0RAQH/BBswGYIRVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlHvcNAQEeBBQAdgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6U188nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

認証した CA に対する証明書要求を作成します。

Note チャレンジパスワードは、設定には保存されません。このパスワードは、証明書を失効する必要がある場合に要求されるので、パスワードを覚えておく必要があります。

アイデンティティ証明書のインストール

CA からのアイデンティティ証明書は、base64 符号化テキスト形式で、E メールまたは Web ブラウザで受信します。CLI インポート機能を使用して符号化テキストをカットアンドペーストすることにより、CA のアイデンティティ証明書をインストールする必要があります。

電子メールまたは Web ブラウザで CA から受信したアイデンティティ証明書をインストールするには、次の手順を実行します。

Procedure

ステップ 1 switch# configure terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# crypto ca import admin-ca certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCj00oQAAAAAAdANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSib3DQeJARYRYWlhbmrRzUBjaXNjby5jb20xZzA5BGNVBAZTAklOMRlWEAYD
VQIEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2l2
Y28xZzARBgNVBAsTCm5ldHN0b3JhZ2UxZjAQBGNVBAmtCUFwYXJuYSDQTAeFw0w
NTEeMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLzE2
Y2l2Y28uY29tMIGfMA0GCSqGSib3DQeBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQlWkjkjSICdpLfk5eJSmNCQujGpzcukSZPFxjF2UoiyeCYE8y1ncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYA8rDfz8jMcnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABO4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVnYXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWm1Vyo9jngMIHMBGNVHSMegcQwgcGAFCCo8kaDG6wjTEVNjSkYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZlHvcNAQkBFhFhbWFWuzGt1QGnPC2NvLmNvbTELMakGA1UE
BhMCSU4xEjAQBGNVBAgTCUthcm5hdGFryTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDAjXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
cm5hIENBghAFYnkjRlQZlE9JEiWMrR16MGsGA1UdHwRkMGIIwLqAsocqGKgh0dHA6
Ly9cZ2UtdMgVQ2VydEVucm9sb3Bc9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZlJ0RW5yb2xsXEFwYXJuYSDUyMENBmNybDDBiGyIKwYBBQUH
AQEefjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0N1cnRfbnJvbGwvc3N1
```

```
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xccc3N1LTA4
XEN1cnRfbnJvbGxccc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

admin-ca という名前の CA に対するアイデンティティ証明書をカットアンドペーストするよう、プロンプトが表示されます。証明書がルート CA によって発行されていない場合、これには複数の「BEGIN CERTIFICATE」行があり、ルート CA 証明書で終わります。CA から提供された証明書チェーン全体を貼り付け、テキストが「END CERTIFICATE」行で終了していることを確認します。

Note スイッチに設定できるアイデンティティ証明書の最大数は 16 です。

トラストポイントの設定がリブート後も維持されていることの確認

トラストポイント設定は、標準の Cisco NX-OS コンフィギュレーションであるため、スタートアップ コンフィギュレーションに明示的にコピーした場合にかぎり、システム リブート後も存続します。トラストポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラストポイントに関連する証明書、キーペア、および CRL が自動的に保持されます。逆に、トラストポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キーペア、および関連 CRL は保持されません。リブート後に、対応するトラストポイント設定が必要になるからです。設定した証明書、キーペア、および CRL を確実に保持するために、必ず、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてください。また、証明書またはキーペアを削除した場合も、削除を反映させるために、実行コンフィギュレーションを保存してください。

特定のトラストポイントがスタートアップ コンフィギュレーションに保存されていれば、トラストポイントに関連する証明書および CRL は、インポートした時点で（スタートアップ コンフィギュレーションに明示的にコピーしなくても）自動的に存続します。

また、パスワードで保護したアイデンティティ証明書のバックアップを作成して、外部サーバーに保存しておくことを推奨します（[PKCS12 フォーマットのアイデンティティ情報をエクスポート](#), on page 14を参照）。



Note スタートアップまたは実行中の構成を外部サーバーにコピーすると、証明書およびキーペアも保存されます。

1. switch# copy running-config startup-config

現在の構成をスタートアップ構成に保存します。

認証局および証明書の構成のモニタリングとメンテナンス

このセクションの作業は、オプションです。

違うデバイスにキーペアと証明書署名要求を生成

RSA キーペアと CSR は、別のデバイスで生成される場合があります。たとえば、`openssl` を使用してホストでこれらを生成するには、次の手順に従います。

1. `host$ openssl req -newkey rsa:2048 -keyout SwitchA.example.com-rsa-pem.privatekey -out SwitchA.example.com-pkcs10.csr`

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to SwitchA.example.com-rsa-pem.privatekey'
Enter PEM pass phrase:abc123
Verifying - Enter PEM pass phrase:abc123
-----
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) []:BE
State or Province Name (full name) []:Brussels
Locality Name (eg, city) []:Brussels
Organization Name (eg, company) []:Example
Organizational Unit Name (eg, section) []:SAN
Common Name (eg, fully qualified host name) []:SwitchA.example.com
Email Address []:cert-admin@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
```

スイッチの FQDN を使用して、2048 ビットのキー モジュールと CSR を持つ RSA キーペアを生成します。

2. `host$ cat SwitchA.example.com-pkcs10.csr`

```
-----BEGIN CERTIFICATE REQUEST-----
...
-----END CERTIFICATE REQUEST-----
```

CA に送信するために生成された base-64 フォーマットの証明書署名要求を表示します。

PKCS12 フォーマットのアイデンティティ情報をエクスポート

アイデンティティ証明書を、トラストポイントの RSA キーペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS12 ファイルにバックアップ目的でエクスポートすることができます。後で、スイッチをシステムクラッシュから回復する場合、またはスーパーバイザ モジュールを交換する場合に、証明書および RSA キーペアをインポートできます。



Note エクスポートおよびインポートの URL の指定では、`bootflash:filename` 形式のローカル構文だけがサポートされます。

証明書およびキーペアを PKCS12 フォーマットファイルにエクスポートする手順は、次のとおりです：

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto ca export admin-ca pkcs12 bootflash:adminid.p12 abc123**

トラストポイント admin-ca のアイデンティティ証明書および関連付けられたキーペアと CA 証明書をファイル bootflash:adminid.p12 に、パスワード「abc123」によって保護された PKCS12 フォーマットでエクスポートします。

ステップ 3 switch(config)# **exit**

switch#

EXEC モードに戻ります。

ステップ 4 switch# **copy bootflash:adminid.p12 tftp:adminid.p12**

PKCS12 フォーマットのファイルを TFTP サーバにコピーします。

PKCS12 形式でのアイデンティティ情報のインポート

証明書および/またはキーペアを PKCS12 フォーマットファイルからインポートする手順は、次のとおりです：

Procedure

ステップ 1 switch# **copy tftp:adminid.p12 bootflash:adminid.p12**

PKCS12 フォーマットのファイルを TFTP サーバからコピーします。

ステップ 2 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 3 switch(config)# **crypto ca import admin-ca pkcs12 bootflash:adminid.p12 abc123**

トラストポイント `admin-ca` のアイデンティティ証明書および関連付けられたキーペアと CA 証明書をファイル `bootflash:adminid.p12` から、パスワード「`abc123`」によって保護された PKCS12 フォーマットでインポートします。

CRL の設定

ファイルからトラストポイントに CRL をインポートする手順は、次のとおりです。

Procedure

-
- ステップ 1** `switch# copy tftp:adminca.crl bootflash:adminca.crl`
CRL をダウンロードします。
- ステップ 2** `switch# configure terminal`
`switch(config)#`
コンフィギュレーションモードに入ります。
- ステップ 3** `switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl`
ファイルで指定されている CRL を設定するか、現在の CRL と置き換えます。
-

認証局構成から認定を削除

トラストポイントに設定されているアイデンティティ証明書や認証局 (CA) 証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除したあと、トラストポイントから RSA キーペアの関連付けを解除できます。期限切れまたは失効した証明書、キーペアが信用できない (または信用できない可能性がある) 証明書、または信頼できなくなった CA を除去するには、証明書を削除する必要があります。

トラストポイントから CA 証明書 (または下位 CA のチェーン全体) を削除する手順は、次のとおりです。

Procedure

-
- ステップ 1** `switch# configure terminal`
`switch(config)#`
コンフィギュレーションモードに入ります。
- ステップ 2** `switch(config)# crypto ca trustpoint myCA`
トラストポイント コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config-trustpoint)# **delete ca-certificate**

CA 証明書または証明書チェーンを削除します。

ステップ 4 switch(config-trustpoint)# **delete certificate**

アイデンティティ証明書を削除します。

ステップ 5 switch(config-trustpoint)# **delete certificate force**

アイデンティティ証明書を削除します。

Note 削除するアイデンティティ証明書が、デバイスの最後または唯一のアイデンティティ証明書である場合には、**force** オプションを使用して削除する必要があります。これは、管理者が最後または唯一のアイデンティティ証明書を誤って削除し、アプリケーション（IKE および SSH など）で使用する証明書が存在しない状態になるのを防止するためです。

ステップ 6 switch(config-trustpoint)# **end**

switch#

EXEC モードに戻ります。

ステップ 7 switch# **copy running-config startup-config**

実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。

スイッチからの RSA キーペアの削除

特定の状況では、スイッチの RSA キーペアの削除が必要になることがあります。たとえば、何らかの原因で RSA キーペアの信用性が失われ、もはや使用しない場合には、そのキーペアを削除すべきです。

スイッチから RSA キーペアを削除する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto key zeroize rsa MyKey**

ラベルが MyKey である RSA キーペアを削除します。

ステップ 3 switch(config)# **end**

switch#

EXEC モードに戻ります。

ステップ 4 switch# copy running-config startup-config

実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。

Example

Note スイッチから RSA キーペアを削除した後、CA でそのスイッチの証明書を失効するように、CA 管理者に依頼してください。その証明書を要求した場合には、作成したチャレンジパスワードを提供する必要があります。「[証明書署名要求の生成, on page 11](#)」を参照してください。

キーペアと証明機関情報の表示

キーペアと証明機関 (CA) 情報を表示するには、次のコマンドを使用します：

| コマンド | 目的 |
|--------------------------------------|-------------------------------|
| switch# show crypto key mypubkey rsa | スイッチの RSA 公開キーに関する情報が表示されます。 |
| switch# show crypto ca certificates | CA とアイデンティティ証明書についての情報を表示します。 |
| switch# show crypto ca crl | CA の CRL についての情報を表示します。 |
| switch# show crypto ca trustpoints | CA トラストポイントについての情報を表示します。 |

設定例

ここでは、Microsoft Windows Certificate サーバを使用して、Cisco MDS 9000 ファミリスイッチ上に証明書および CRL を設定するための作業例を示します。

MDS スイッチでの証明書の設定

MDS スイッチで証明書を設定する手順は、次のとおりです。

Procedure

ステップ 1 スイッチの FQDN を設定します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# switchname SwitchA
SwitchA(config)#
```

ステップ 2 スイッチの DNS ドメイン名を設定します。

```
SwitchA(config)# ip domain-name example.com
SwitchA(config)#
```

ステップ 3 トラストポイントを作成します。

```
SwitchA(config)# crypto ca trustpoint myCA
SwitchA(config-trustpoint)# exit
SwitchA(config)# show crypto ca trustpoints

trustpoint: myCA; key:
revokation methods: crl
SwitchA(config)#
```

ステップ 4 スイッチの RSA キーペアを作成します。

```
SwitchA(config)# crypto key generate rsa label myKey exportable modulus 1024
SwitchA(config)# show crypto key mypubkey rsa

key label: myKey
key size: 1024
exportable: yes
SwitchA(config)#
```

ステップ 5 RSA キーペアとトラストポイントを関連付けます。

```
SwitchA(config)# crypto ca trustpoint myCA
SwitchA(config-trustpoint)# rsaakeypair myKey
SwitchA(config-trustpoint)# exit
SwitchA(config)# show crypto ca trustpoints

trustpoint: myCA; key: myKey
revokation methods: crl
SwitchA(config)#
```

ステップ 6 Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします ([認証局の CA 証明書をダウンロード](#), on page 22 を参照) 。

ステップ 7 トラストポイントに登録する CA を認証します。

```
SwitchA(config)# crypto ca authenticate myCA

input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk10
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21lZy28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJuYSBD
QTAEFw0wNTA1MDMyMjQzMzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWVufuZGt1QGnpc2NvLmNvbTELMARGA1UEBhMCSU4xEjAQBGNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMjQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECXMkbnV0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwDQYJKoZIhvcN
```

```
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMperXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxyYKvysCAwEAAoBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJlYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xccc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JSMGAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
```

```
Do you accept this certificate? [yes/no]:y
SwitchA(config)#
SwitchA(config)# show crypto ca certificates
```

```
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
notAfter=May 3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

ステップ 8 トラストポイントに登録するために使用する証明書要求を作成します。

```
SwitchA(config)# crypto ca enroll myCA

Create the certificate request..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:abc123
The subject name in the certificate will be: SwitchA.example.com
Include the switch serial number in the subject name? [yes/no]:no
Include an IP address in the subject name [yes/no]:yes
ip address:10.10.1.1
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnVnYXNjby5jb20wgZ8wDQYJ
KoZlHvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl41KY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsqGSIb3DQEJ
DjEpMccwJQYDVR0RAQH/BBswGyIRVmVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlHvcNAQEBBQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U188nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

SwitchA(config)#
```

ステップ 9 Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求しま
す (アイデンティティ証明書の要求, [on page 30](#)を参照)。


```
SwitchA# copy running-config startup-config
```

認証局の CA 証明書をダウンロード

Microsoft Certificate Service の Web インターフェイスから認証局 (CA) 証明書をダウンロードする手順は、次のとおりです。

Procedure

- ステップ 1 Microsoft Certificate Services Web インターフェイスの [Retrieve the CA certificate or certificate revocation task] オプション ボタンを選択し、[Next] ボタンをクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and so on, depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

ステップ 2 表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] オプション ボタンをクリックし、[Download CA certificate] リンクをクリックします。

Microsoft Certificate Services -- Aparna CA

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this

It is not necessary to manually install the CA certification path if you request and install a c
CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: [Current \[Aparna CA\]](#)

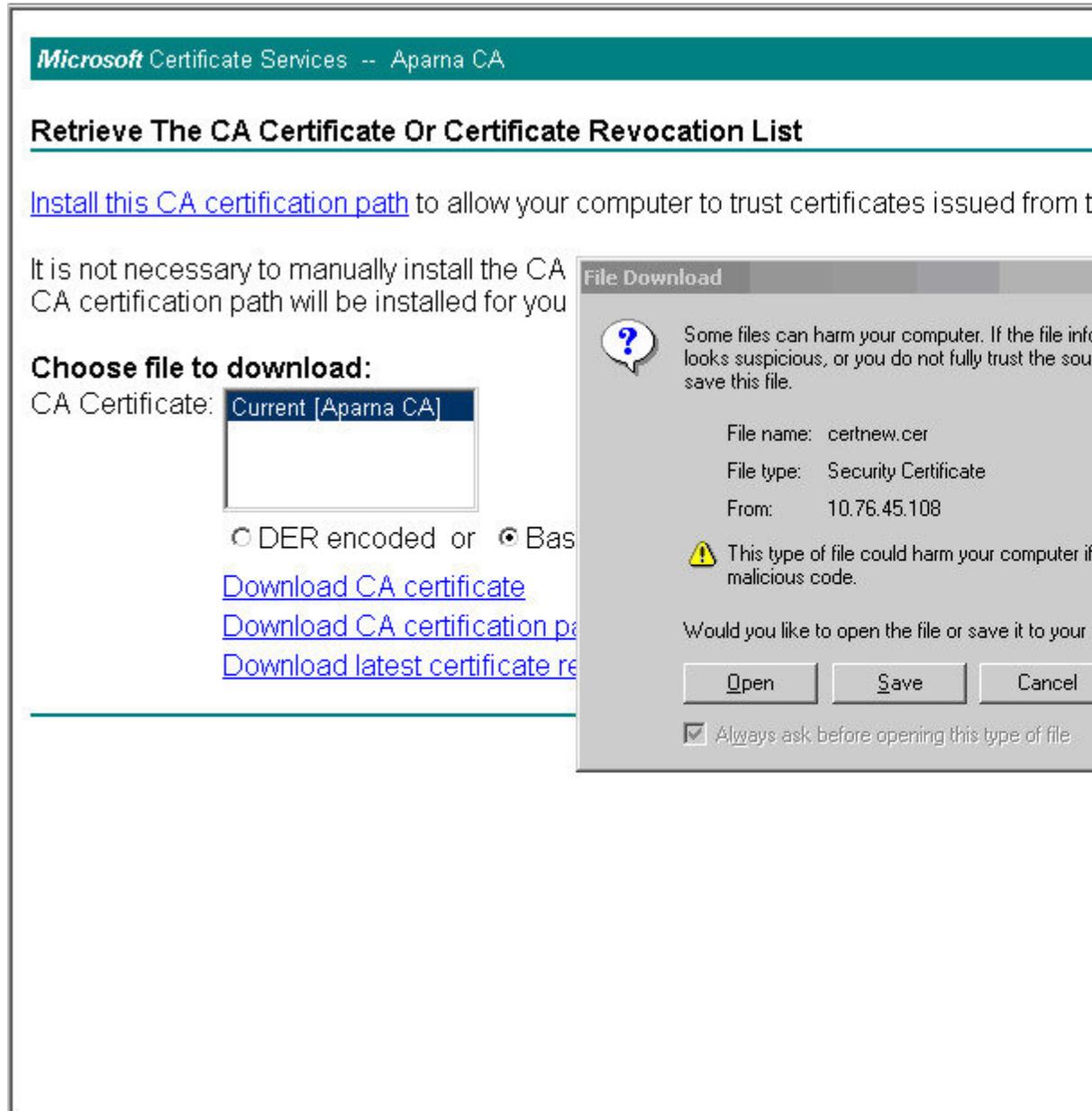
DER encoded or Base 64 encoded

[Download CA certificate](#)

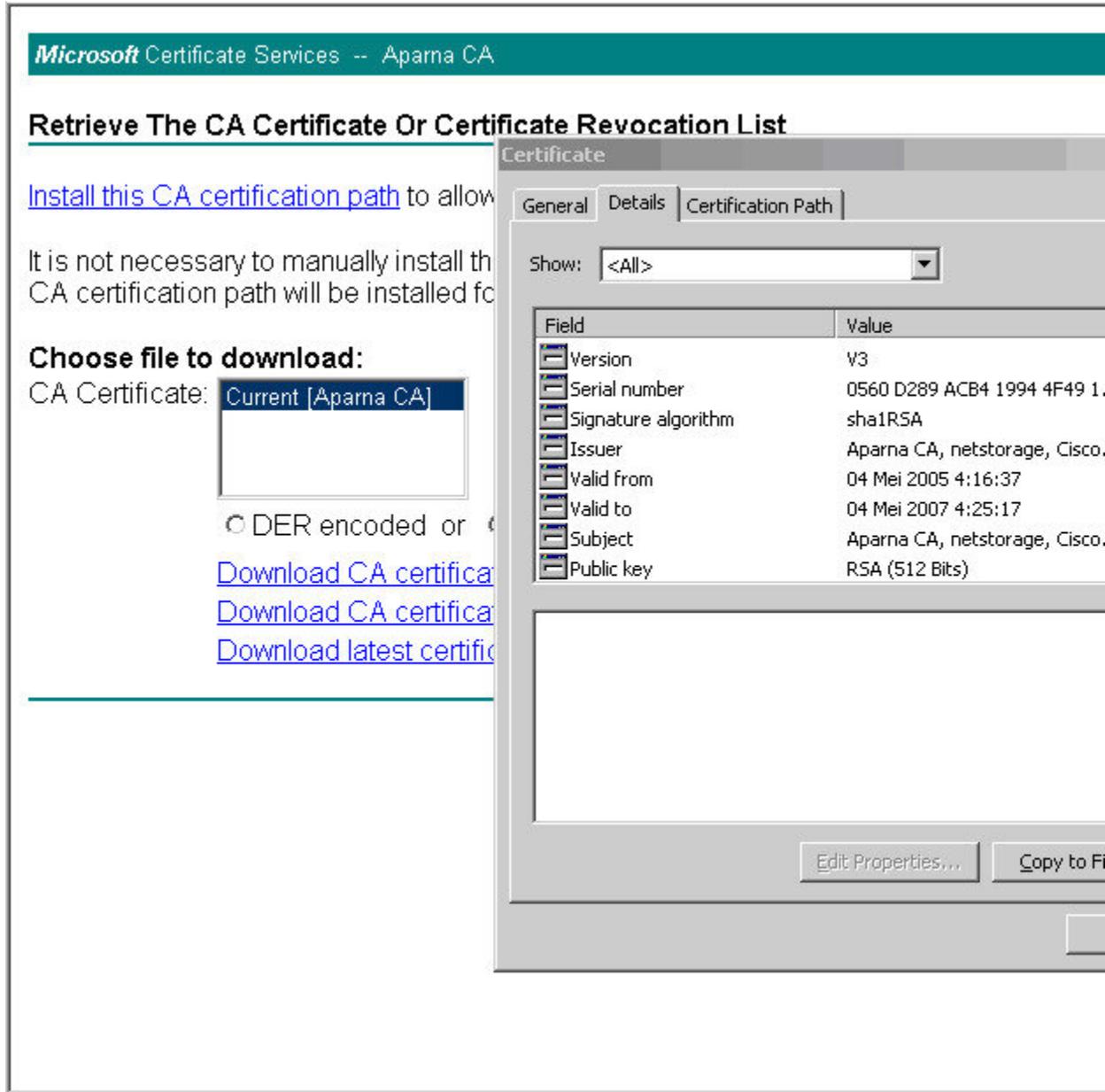
[Download CA certification path](#)

[Download latest certificate revocation list](#)

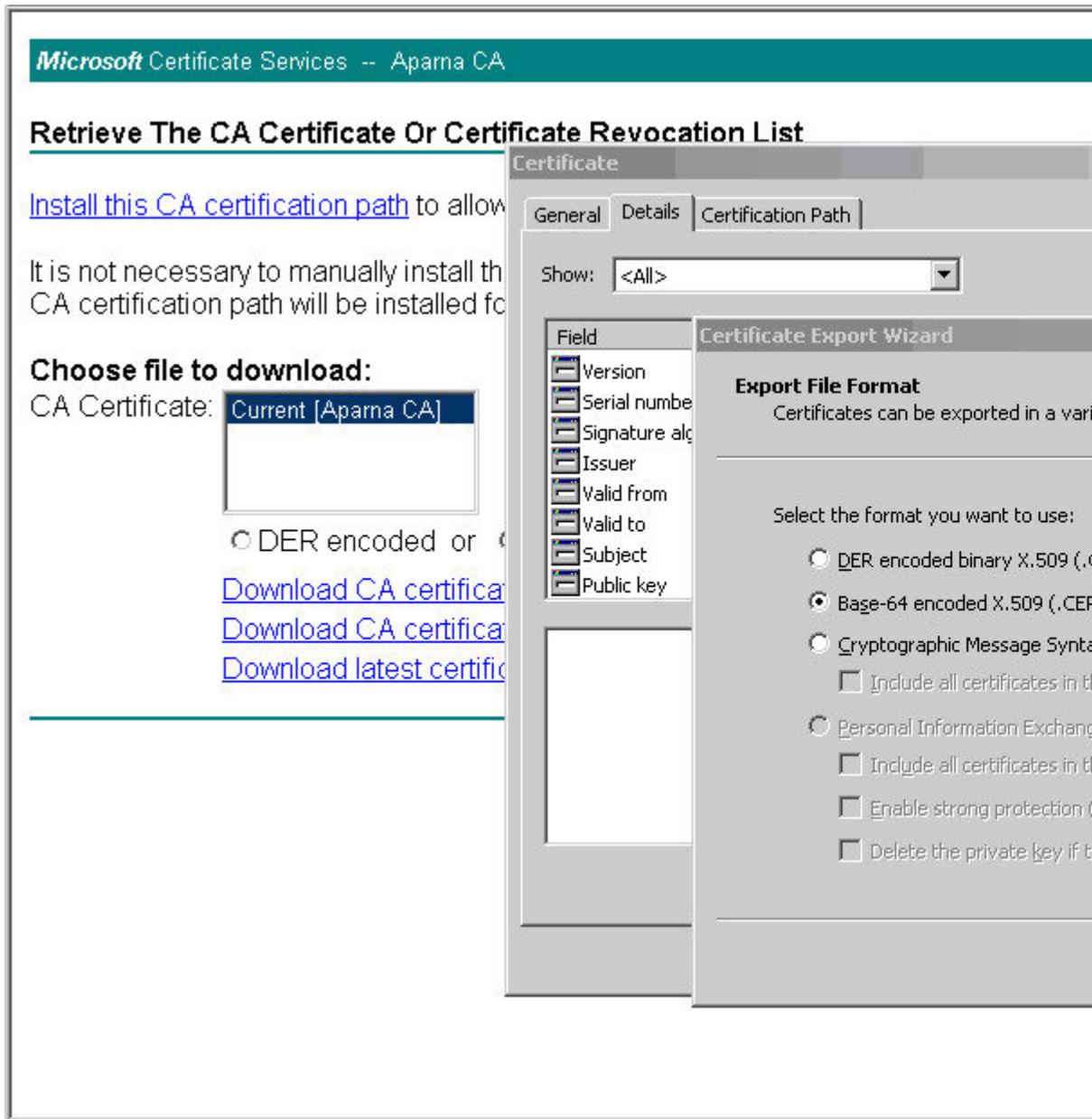
ステップ 3 [File Download] ダイアログボックスで、[Open] ボタンをクリックします。



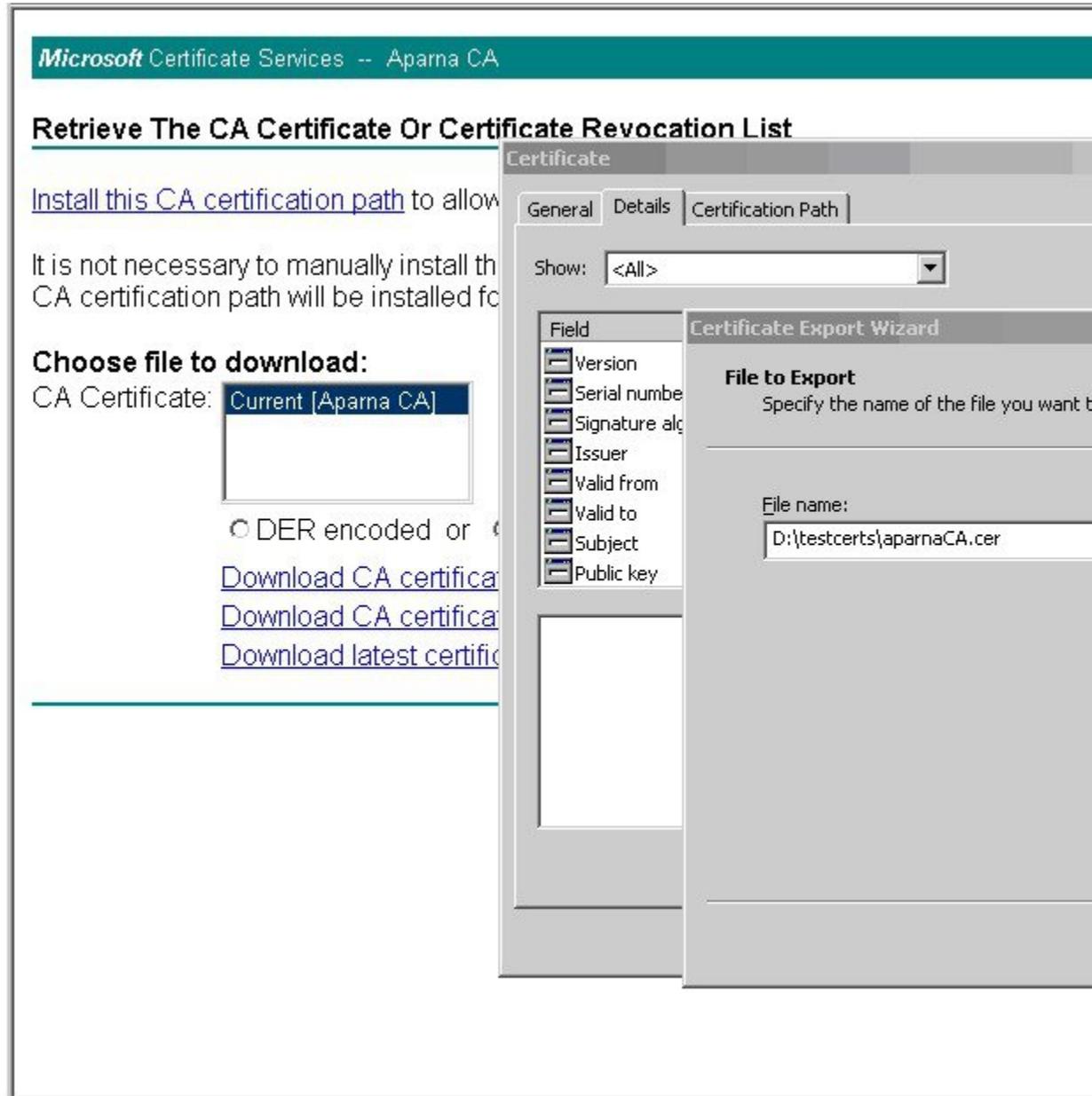
ステップ 4 [Certificate] ダイアログボックスで [Copy to File] ボタンをクリックし、[OK] をクリックします。



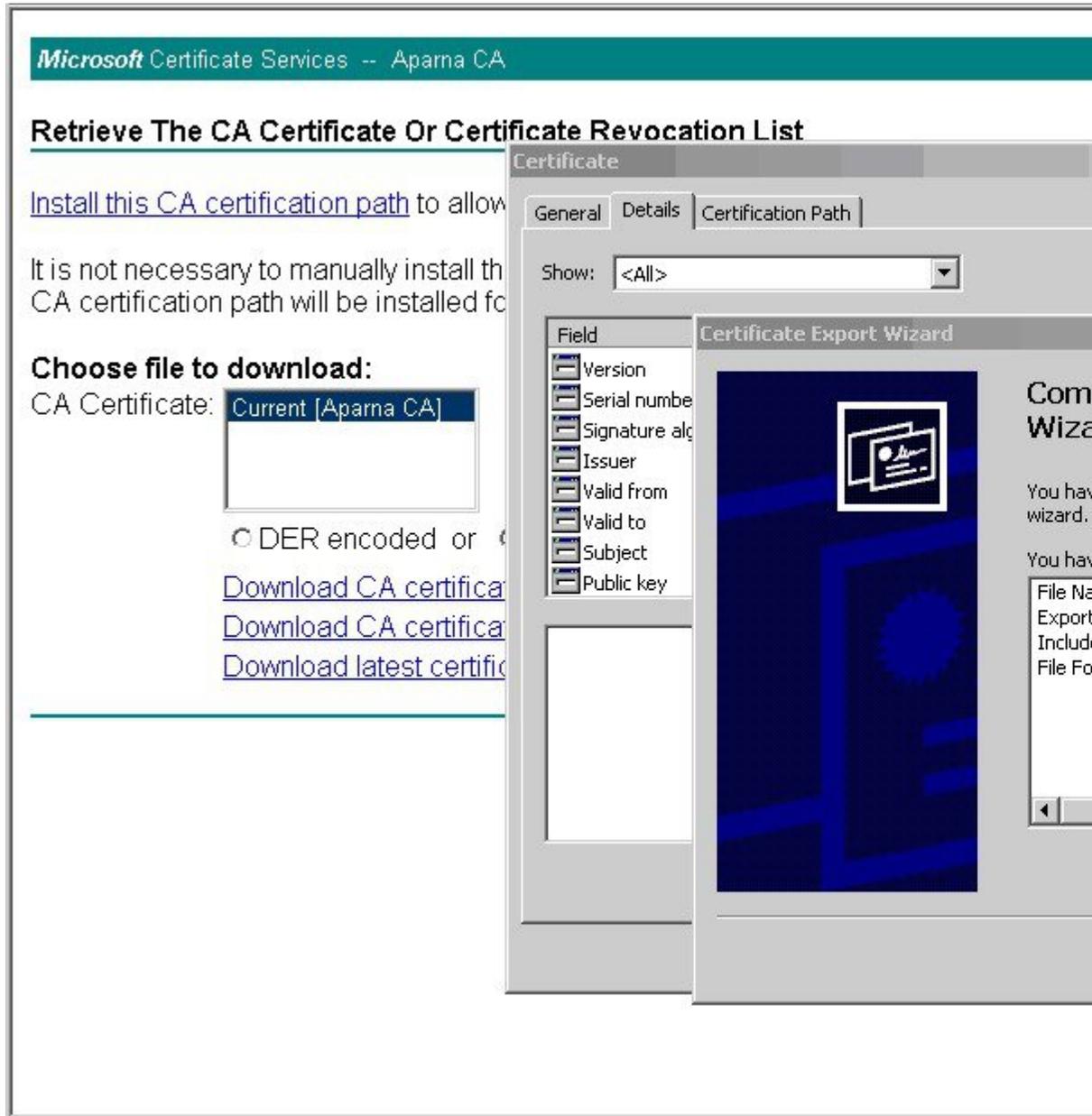
ステップ 5 [Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。



ステップ 6 [Certificate Export Wizard] ダイアログボックスの [File name:] テキストボックスに宛先ファイル名を入力し、[Next] をクリックします。

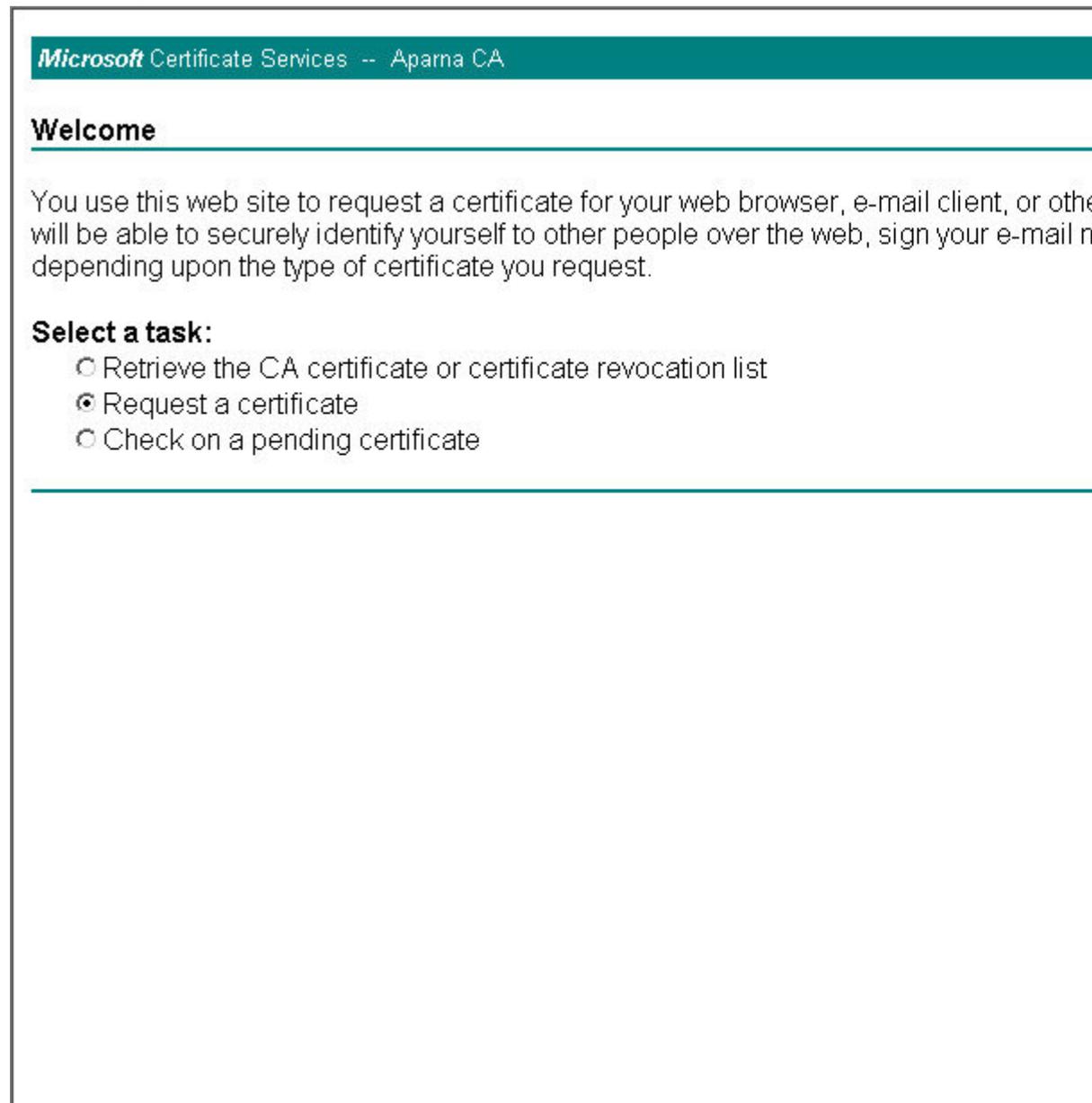


ステップ7 [Certificate Export Wizard] ダイアログボックスの [Finish] ボタンをクリックします。



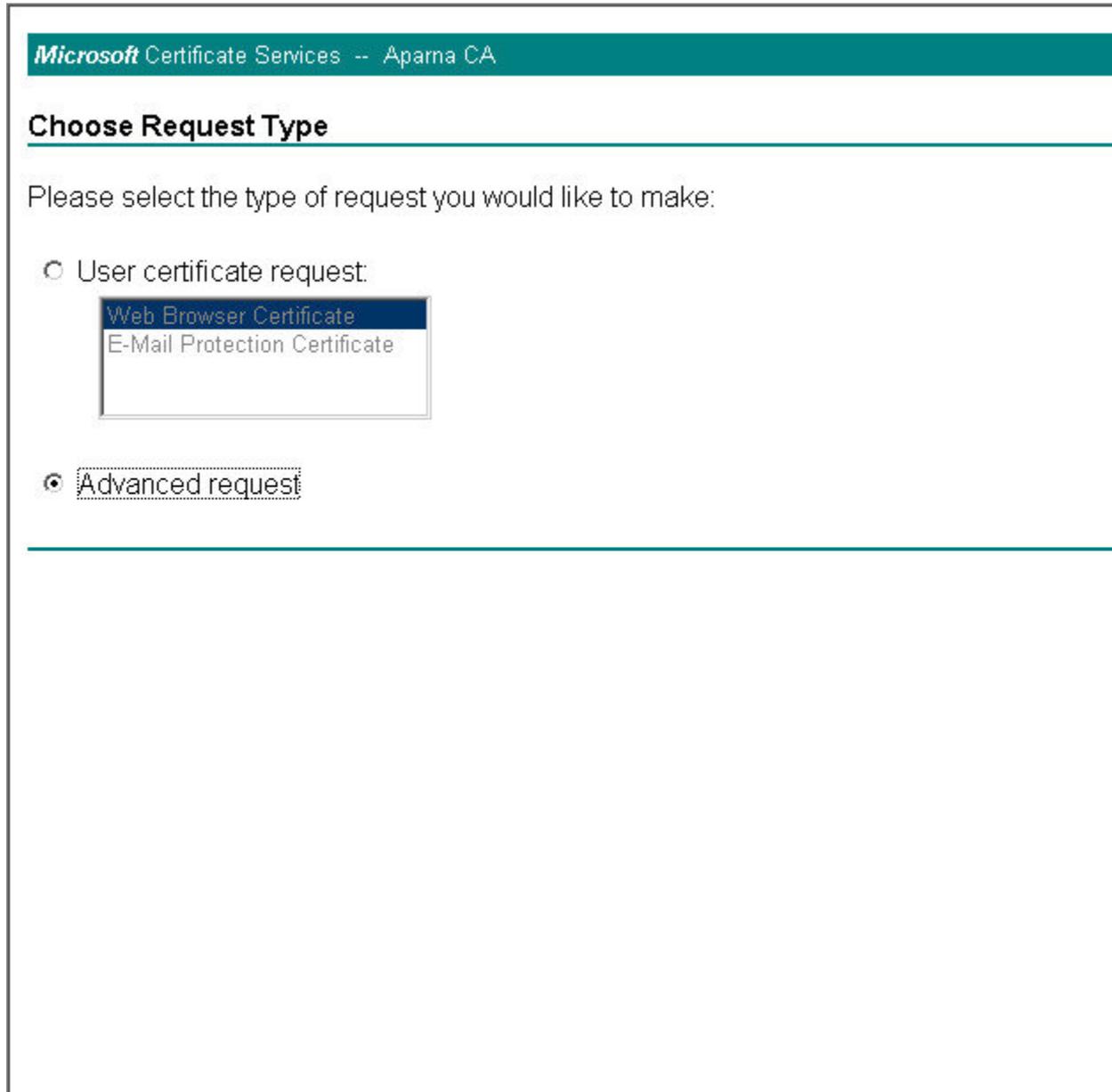
Procedure

- ステップ1 Microsoft Certificate Services Web インターフェイス上の [Request a certificate] ラジオ ボタンを選択し、[Next] を選択します。



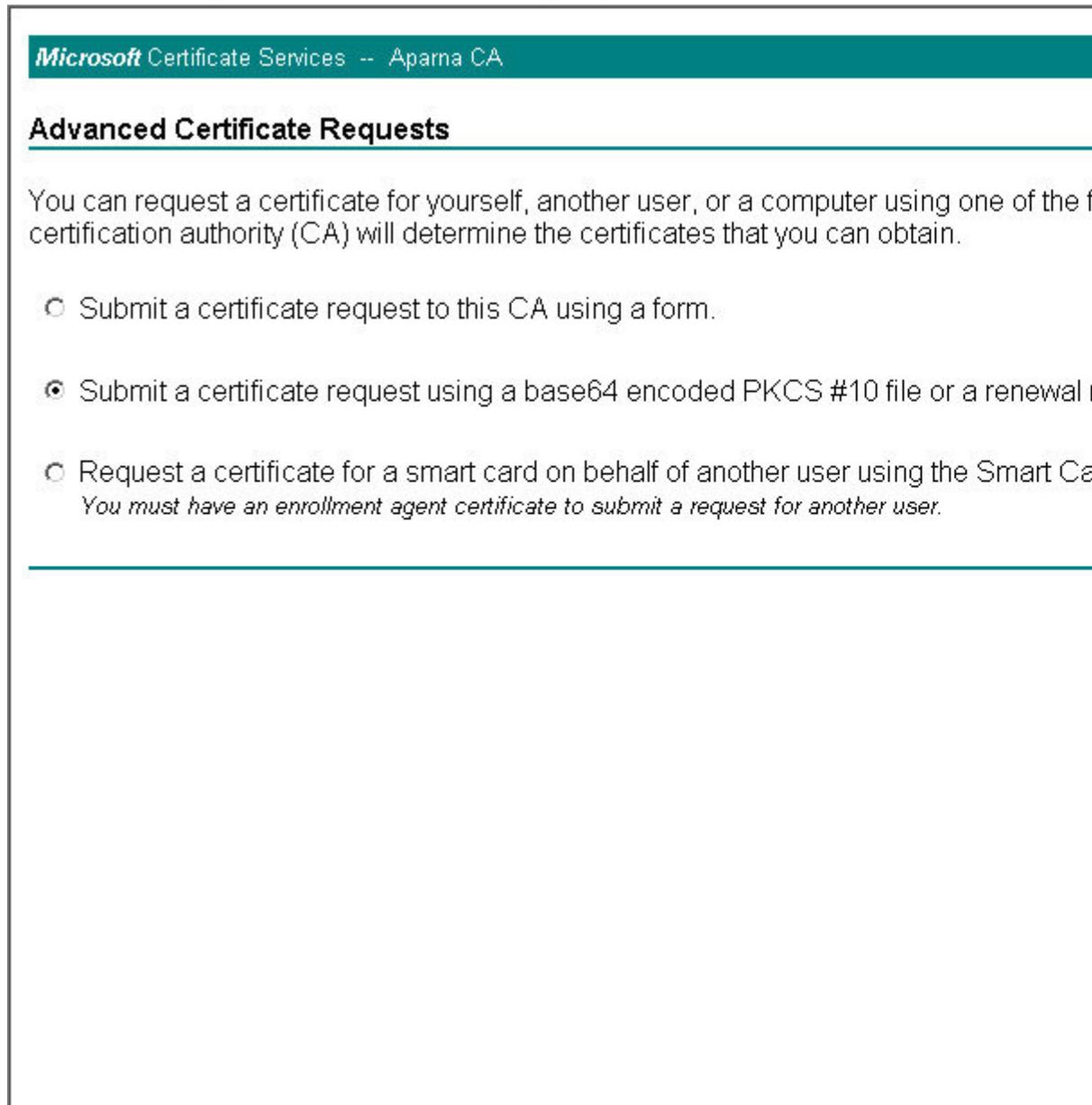
The screenshot displays the Microsoft Certificate Services Web interface for the Aparna CA. The page title is "Microsoft Certificate Services -- Aparna CA". Below the title, there is a "Welcome" section with a horizontal line. The text reads: "You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data depending upon the type of certificate you request." Below this text, there is a "Select a task:" section with three radio button options: "Retrieve the CA certificate or certificate revocation list", "Request a certificate" (which is selected), and "Check on a pending certificate". A horizontal line is visible below the "Select a task:" section.

ステップ2 [Advanced Request] ラジオ ボタンを選択し、[Next] をクリックします。



The screenshot shows a web browser window with the title "Microsoft Certificate Services -- Apama CA". The main heading is "Choose Request Type". Below the heading, the text reads "Please select the type of request you would like to make:". There are two radio button options: "User certificate request:" and "Advanced request". The "Advanced request" option is selected. A dropdown menu is open under "User certificate request:", showing "Web Browser Certificate" (highlighted) and "E-Mail Protection Certificate".

- ステップ 3 [Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] オプション ボタンを選択し、[Next] ボタンをクリックします。



The screenshot shows a web interface for 'Microsoft Certificate Services -- Aparna CA'. The main heading is 'Advanced Certificate Requests'. Below the heading, there is a paragraph: 'You can request a certificate for yourself, another user, or a computer using one of the following options. The certification authority (CA) will determine the certificates that you can obtain.' There are three radio button options: 1. 'Submit a certificate request to this CA using a form.' 2. 'Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.' (This option is selected with a filled radio button.) 3. 'Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Wizard. You must have an enrollment agent certificate to submit a request for another user.'

- ステップ 4 Saved Request テキスト ボックスに base64 PKCS 10 証明書要求をペーストし、[次 (Next)] をクリックします。

MDS スイッチのコンソールから、証明書要求がコピーされます (証明書署名要求の生成, on page 11 および MDS スイッチでの証明書の設定, on page 18 を参照)。

Microsoft Certificate Services -- Aparna CA

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by the client (or a request from a self-enrollment server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
VqyHOvEvAgMBAAGgTzAVBgkqhkiG9wOBCQcxCBMG
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j
KoZlhvcNAQEEBQADgYEAKT6OKER6Qo8nj0sDXZVH
PftRncWUE/pw6HayfQ12T3ecgNwe12d15133YBF2:
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPN
-----END CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

Additional Attributes:

Attributes:

ステップ5 CA アドミニストレータから証明書が発行されるまで、1～2日間待ちます。

Microsoft Certificate Services -- Aparna CA

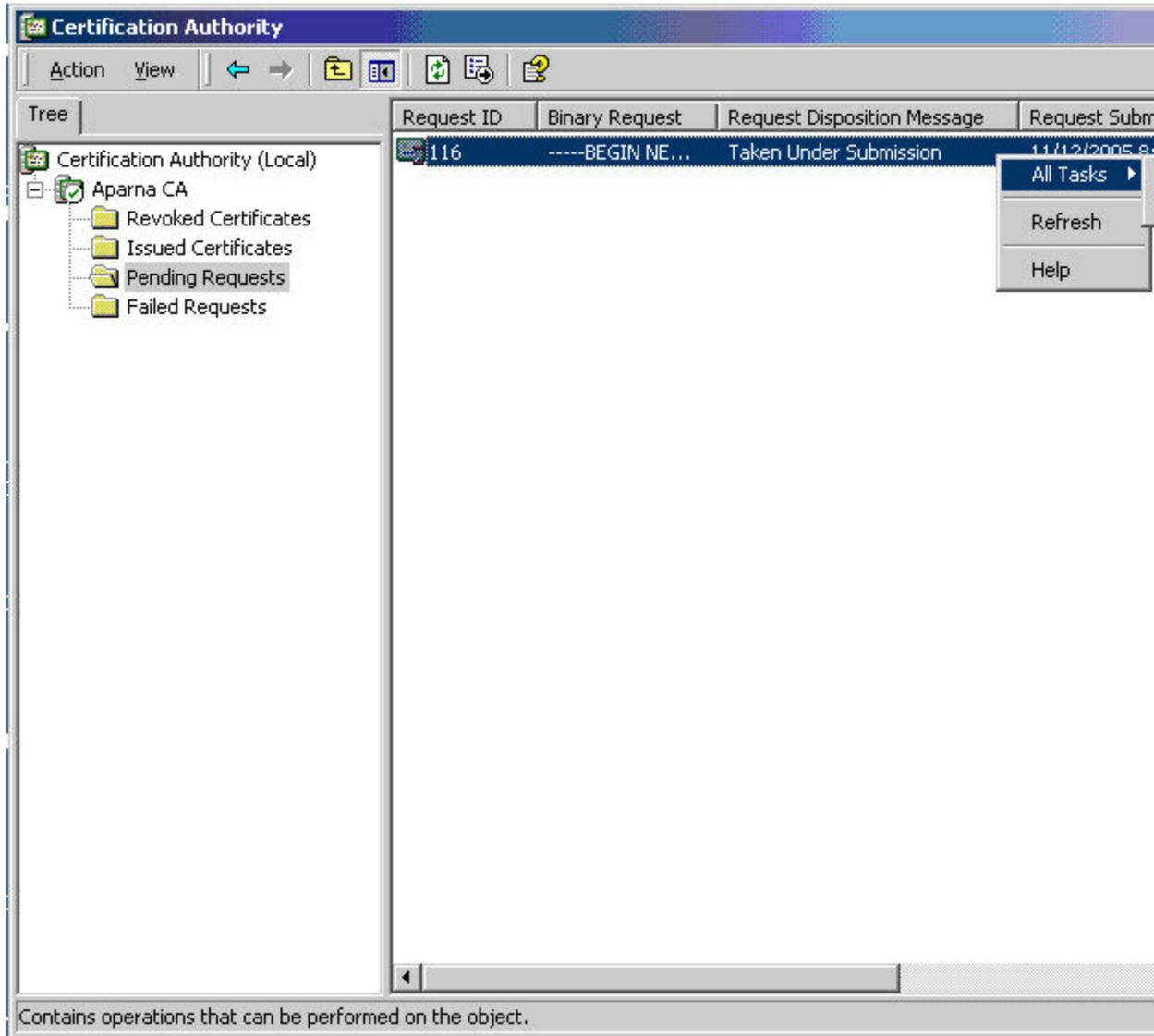
Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to approve your request.

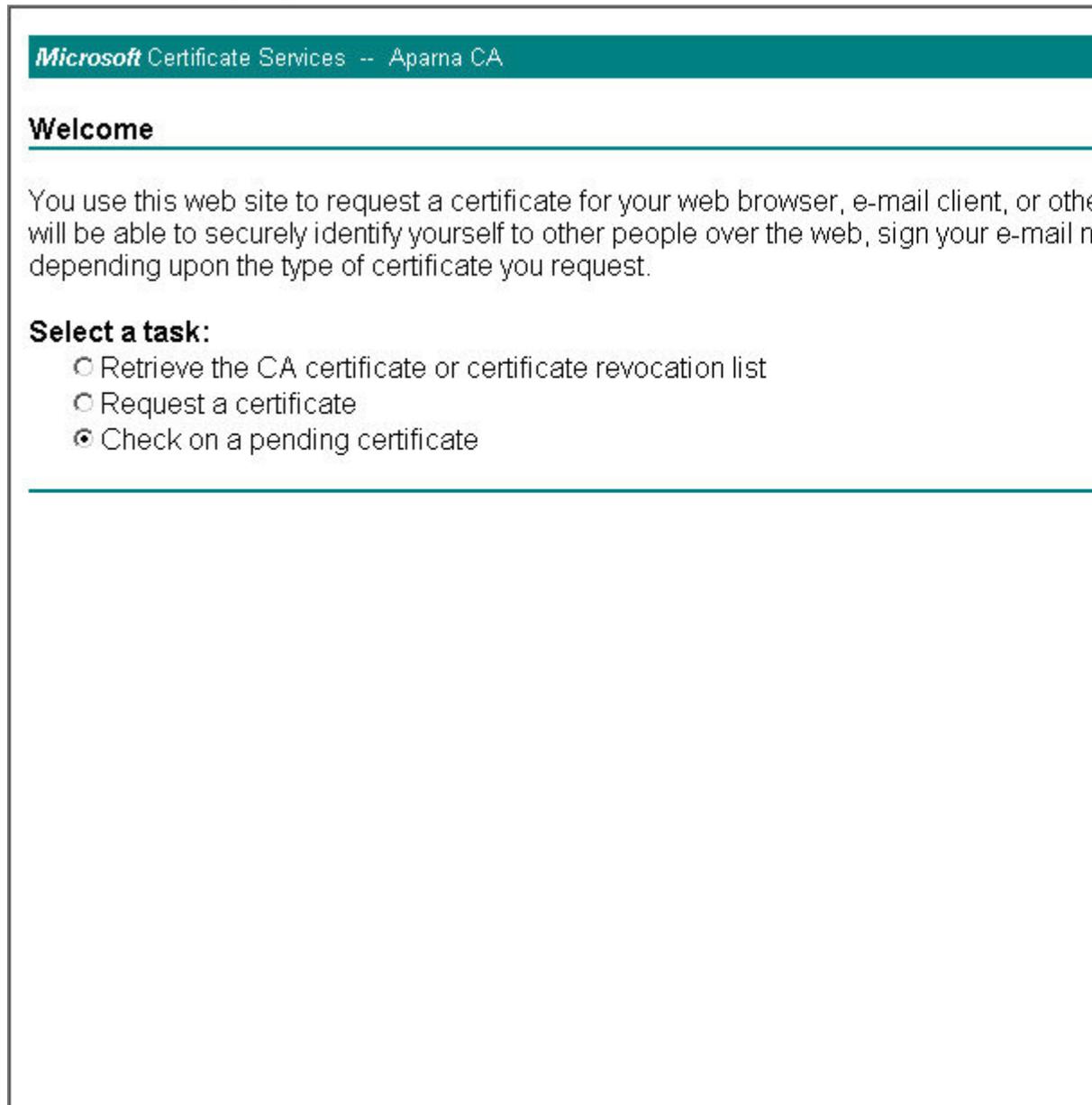
Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate.

ステップ 6 CA 管理者により証明書要求が承認されます。



- ステップ 7** Microsoft Certificate Services Web インターフェイス上の [Check on a pending certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。



The screenshot shows the Microsoft Certificate Services Web interface for the Aparna CA. The page title is "Microsoft Certificate Services -- Aparna CA". Below the title is a "Welcome" section with a horizontal line. The text reads: "You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data depending upon the type of certificate you request." Below this is a "Select a task:" section with three radio button options: "Retrieve the CA certificate or certificate revocation list", "Request a certificate", and "Check on a pending certificate". The "Check on a pending certificate" option is selected, indicated by a filled radio button. A horizontal line is visible below the list of tasks.

ステップ 8 確認する証明書要求を選択し、[Next] をクリックします。

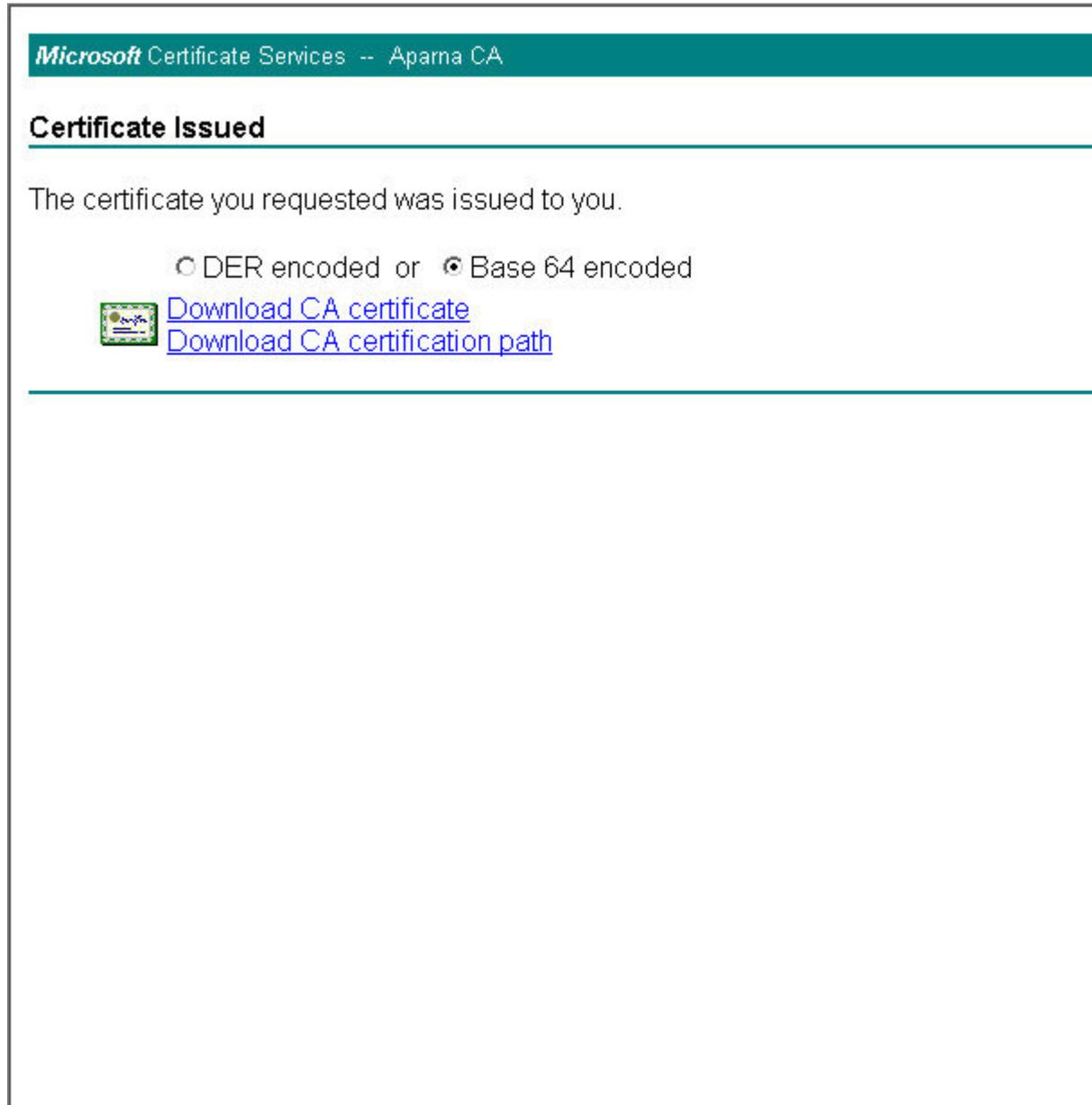
Microsoft Certificate Services -- Apama CA

Check On A Pending Certificate Request

Please select the certificate request you want to check:

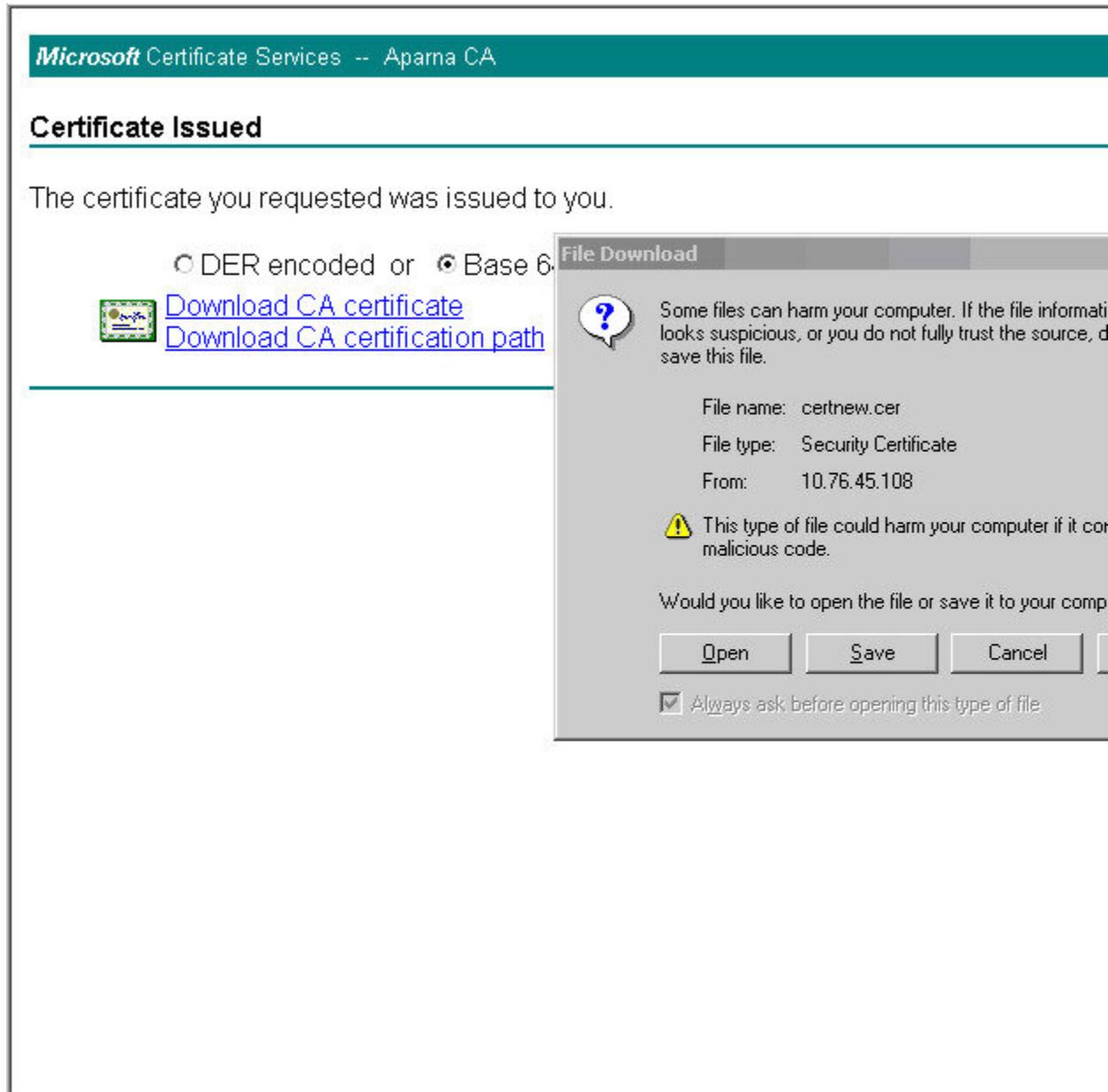
Saved-Request Certificate (12 Nopember 2005 20:30:22)

ステップ 9 [Base 64 encoded] を選択し、[Download CA certificate] リンクをクリックします。



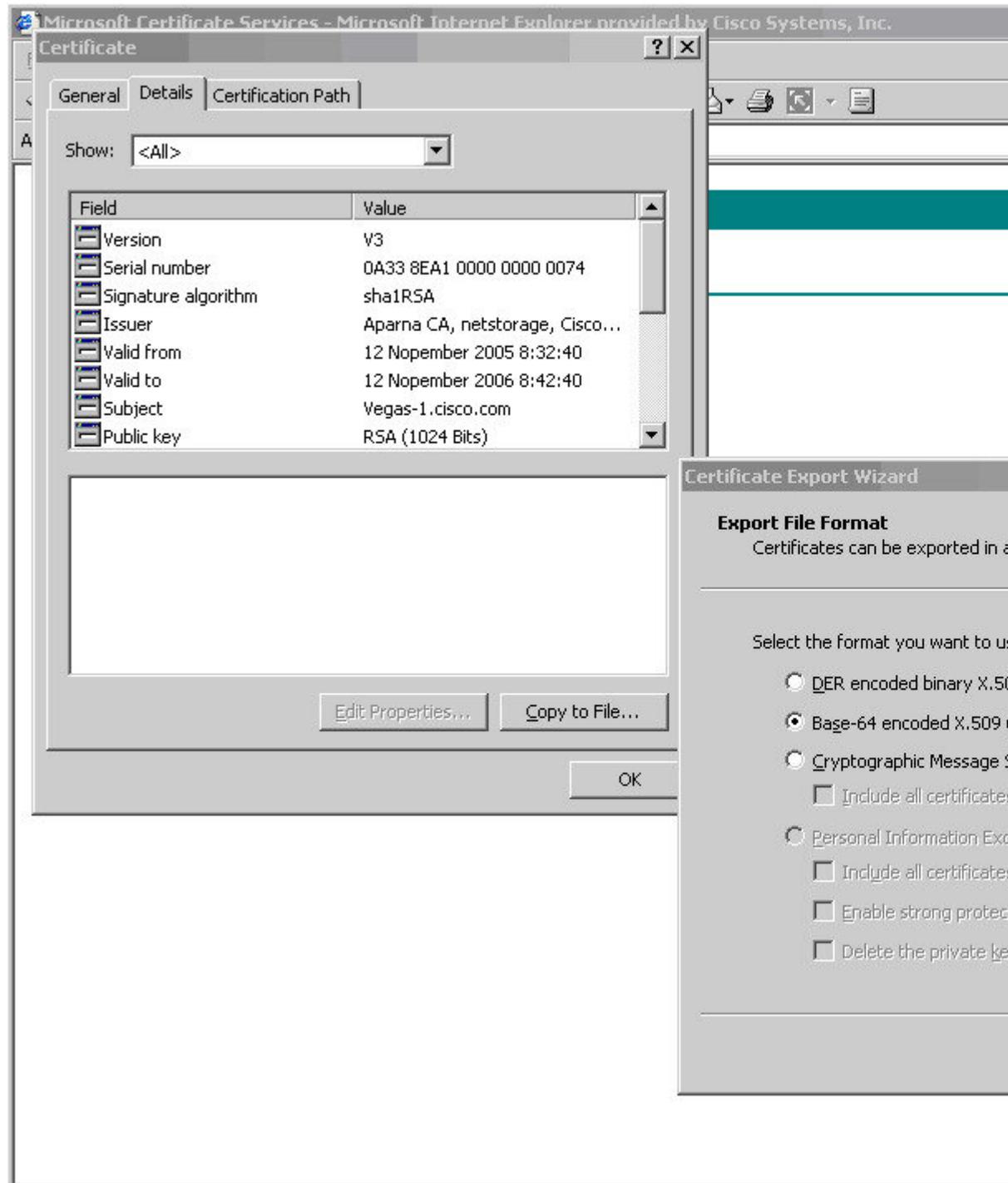
The screenshot displays the Microsoft Certificate Services interface for the 'Aparna CA'. The page title is 'Microsoft Certificate Services -- Aparna CA'. Below the title, the section 'Certificate Issued' is highlighted. The main message states: 'The certificate you requested was issued to you.' Below this message, there are two radio button options: 'DER encoded' (unselected) and 'Base 64 encoded' (selected). Underneath the radio buttons, there are two blue hyperlinks: 'Download CA certificate' and 'Download CA certification path'. A small icon of a certificate is visible to the left of the first link.

ステップ 10 [File Download] ダイアログボックスで、[Open] をクリックします。

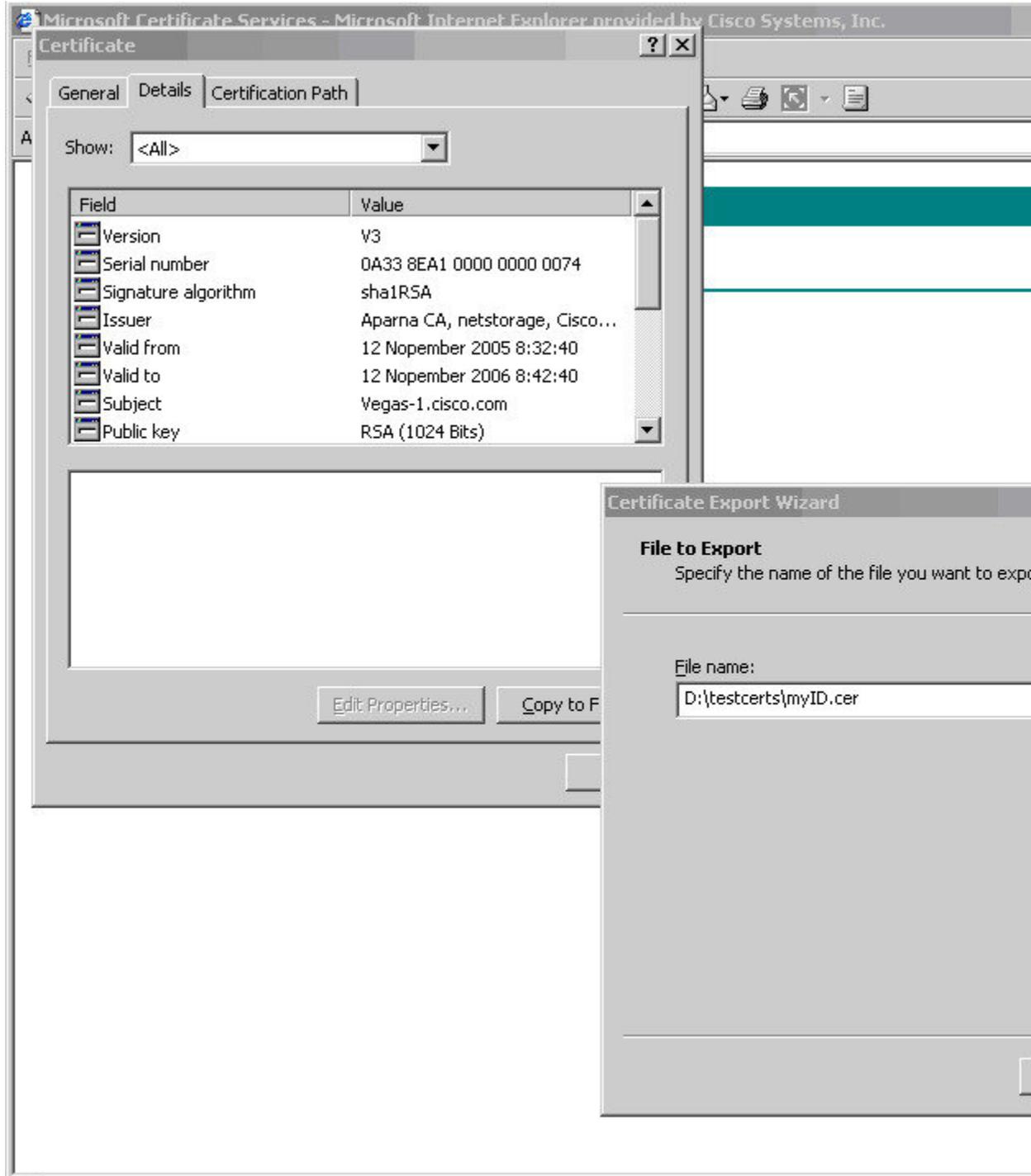


ステップ 11 [Certificate] ダイアログボックスで [Details] タブをクリックし、[Copy to File] ボタンをクリックします。[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (.CER)] オプション

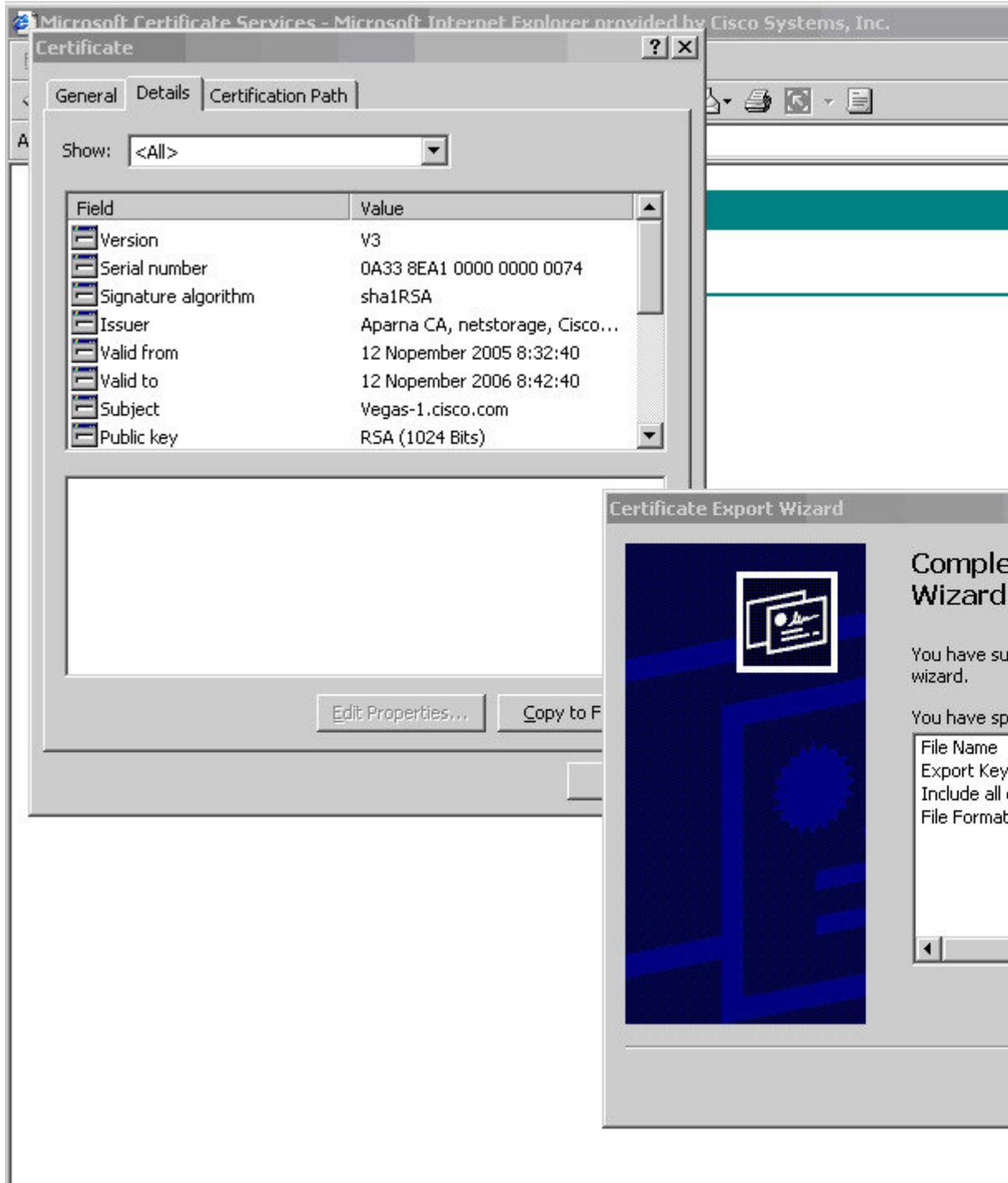
シヨン ボタンを選択し、[Next] ボタンをクリックします。



ステップ 12 [Certificate Export Wizard] ダイアログボックスの [File name:] テキストボックスに宛先ファイル名を入力し、[Next] をクリックします。



ステップ 13 [Finish] をクリックします。



ステップ 14 Microsoft Windows の **type** コマンドを使用して、base-64 符号化形式のアイデンティティ証明書を表示します。

```
C:\WINNT\system32\cmd.exe

D:\testcerts>type myID.cer
-----BEGIN CERTIFICATE-----
MIIEADCCA6ggAwIBAgIKCj00oQAAAAAADANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbWRRZUBjaXNjb20xCzA=JBgNUBAYTAkL0MRLiEAYD
UQQIEwLLYXJkYXRha2ExEjAQBgNUBAc1CUJhbmdhbG9yZTEOMAwwGA1UEChMFQ2
Y28xZ28uY28uY28uY28uY28uY28uY28uY28uY28uY28uY28uY28uY28uY28uY28u
NTExMTIwMzA0NDBaFw0wNjExMTIwMzE0NDBaMBwXGjA4YBgNUBAMTEUZI2Z2FzLT
EuY2IzY28uY29tMI GFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNUAcDjQu41C
dQ1WkjkjSICdpLfK5eJSmNCQujGpzcukS ZPFxjF2Uo iyeCYE8y1ncWyw5E08rJ47
gLx42/sI9IRIb/8udU/cj9jSSfKK56koa7xwYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdU06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAq8wJQYDUR0RAQH/BBsw
GYIRUmUnYXMcMS5jaXNjb20y2HBKwWH6IwHQYDUR0OBBYEFKCLi+2sspwEfgR
bhWm1Uyo9jngMIHMBgNUHSMEGcQwgcGAFCCo8kaDG6wJTEUNjskYUBoLPmxxoYGW
pIGTMIQMSAwHgYJKoZIHvcNAQBFhFhbWFuZGt1QGNpc2NoLmNoTELMAkGA1UE
BHMCSU4xEjAQBgNUBAgICUthcm5hdGFyYTESMBAGA1UEBxMjQmFuZ2Fsb3JlMQ4w
DAYDUQQKEwUDaXNjbzETMBEGA1UECzMKbmU0c3RvcnFnZTESMBAGA1UEAxMjQX
cm5hIENBghAFYnkjrLQZ1E9JEiWMrR16MGsGA1UdHwRkMG1wLqAsocGKkGh0dHA6
Ly9zc2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJkYXN5YmENBmNybDcBbigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChio9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJkYXN5YmENBmNybDcBbigYIKwYBBQUHAYESMBAGA1UEBxMjQmFuZ2Fsb3Jl
XENlcnRFbnJvbGwvc3NlLTA4X0FwYXJkYXN5YmENBmNybDANBgkqhkiG9w0BAQUF
AANBA DbGBGsbG9NLh9xe0TWNbm24U69ZSuDDc0cUZUUTgrpn1qUpPyejtsyf1w
E36cIZu4WsExREqxbTk8ycx7U5o=
-----END CERTIFICATE-----

D:\testcerts>
```

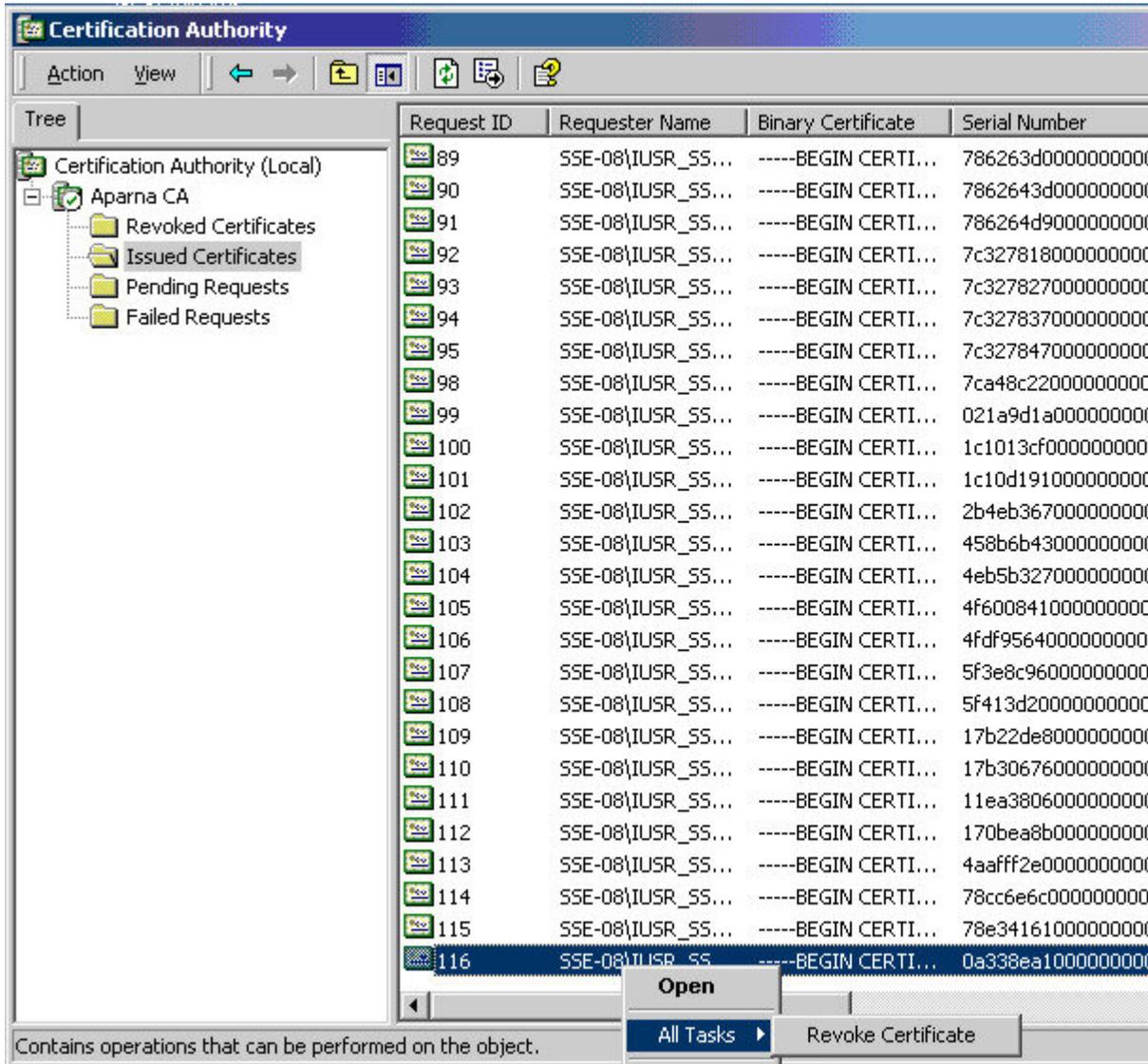
証明書の取り消し

Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

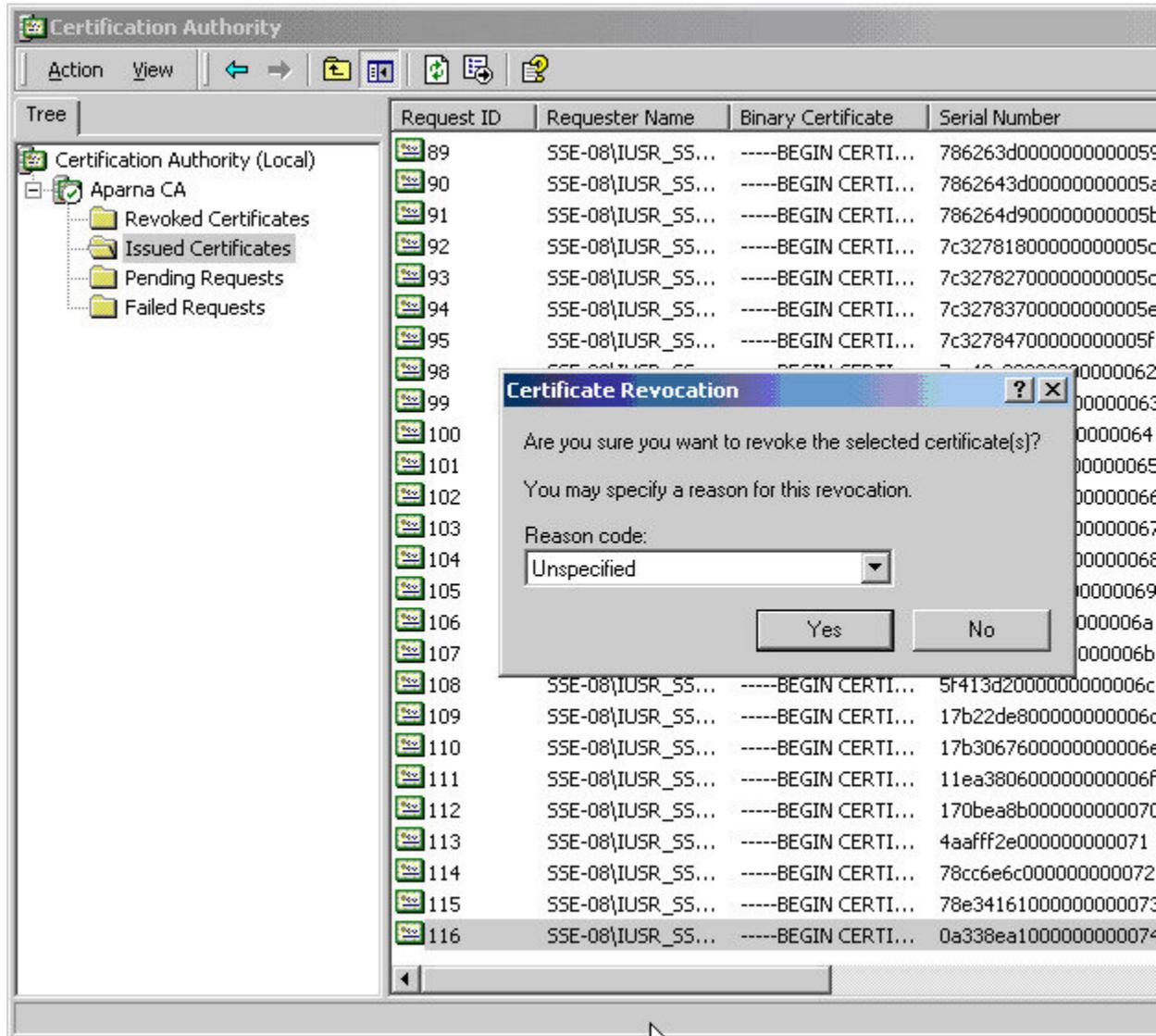
Procedure

ステップ 1 Certification Authority ツリーで、**Issued Certificates** フォルダをクリックします。リストから、失効させる証明書を右クリックします。

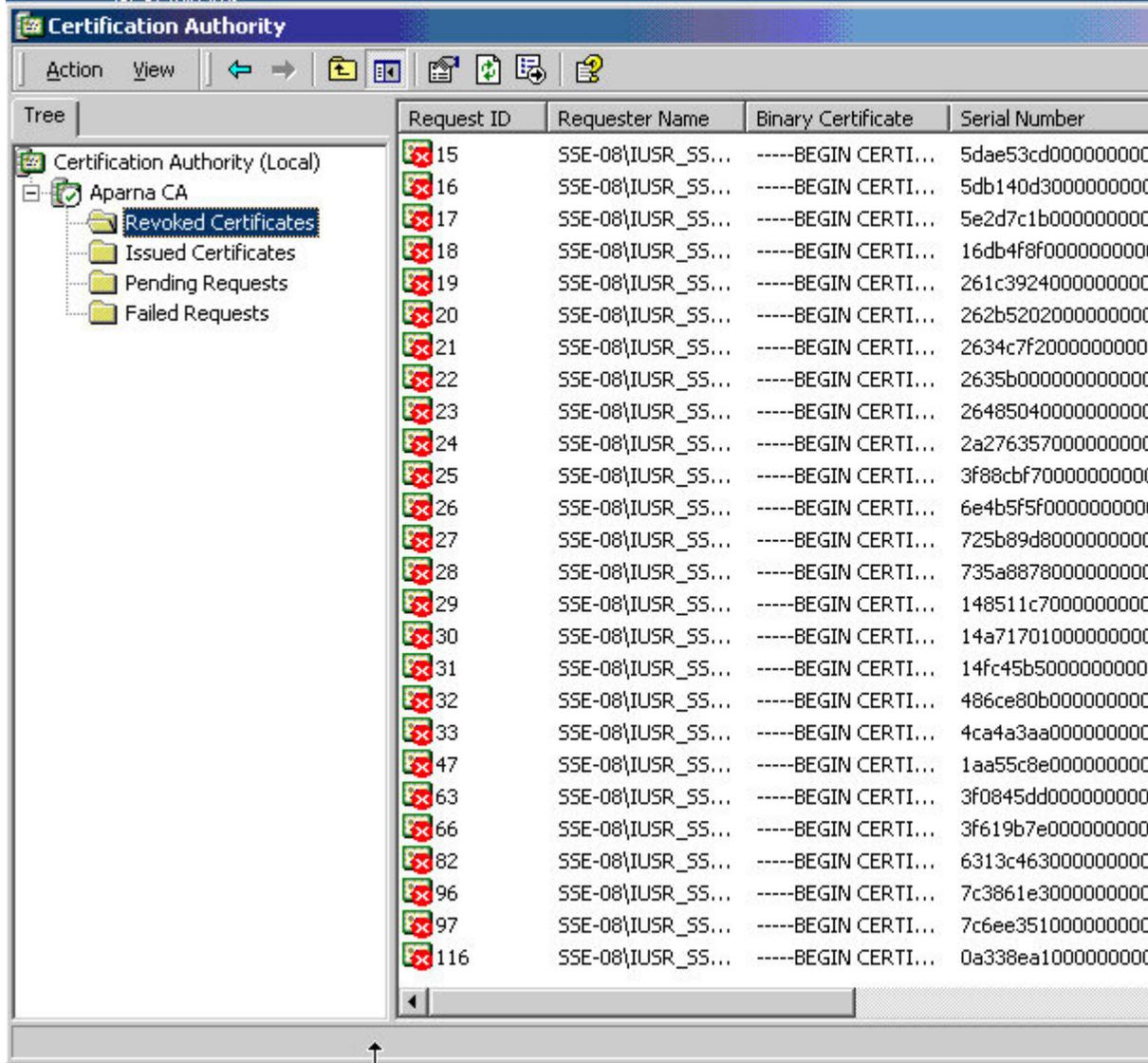
ステップ2 [All Tasks] > [Revoke Certificate] を選択します。



ステップ3 [Reason code] ドロップダウン リストから失効の理由を選択し、[Yes] をクリックします。



ステップ 4 [Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。

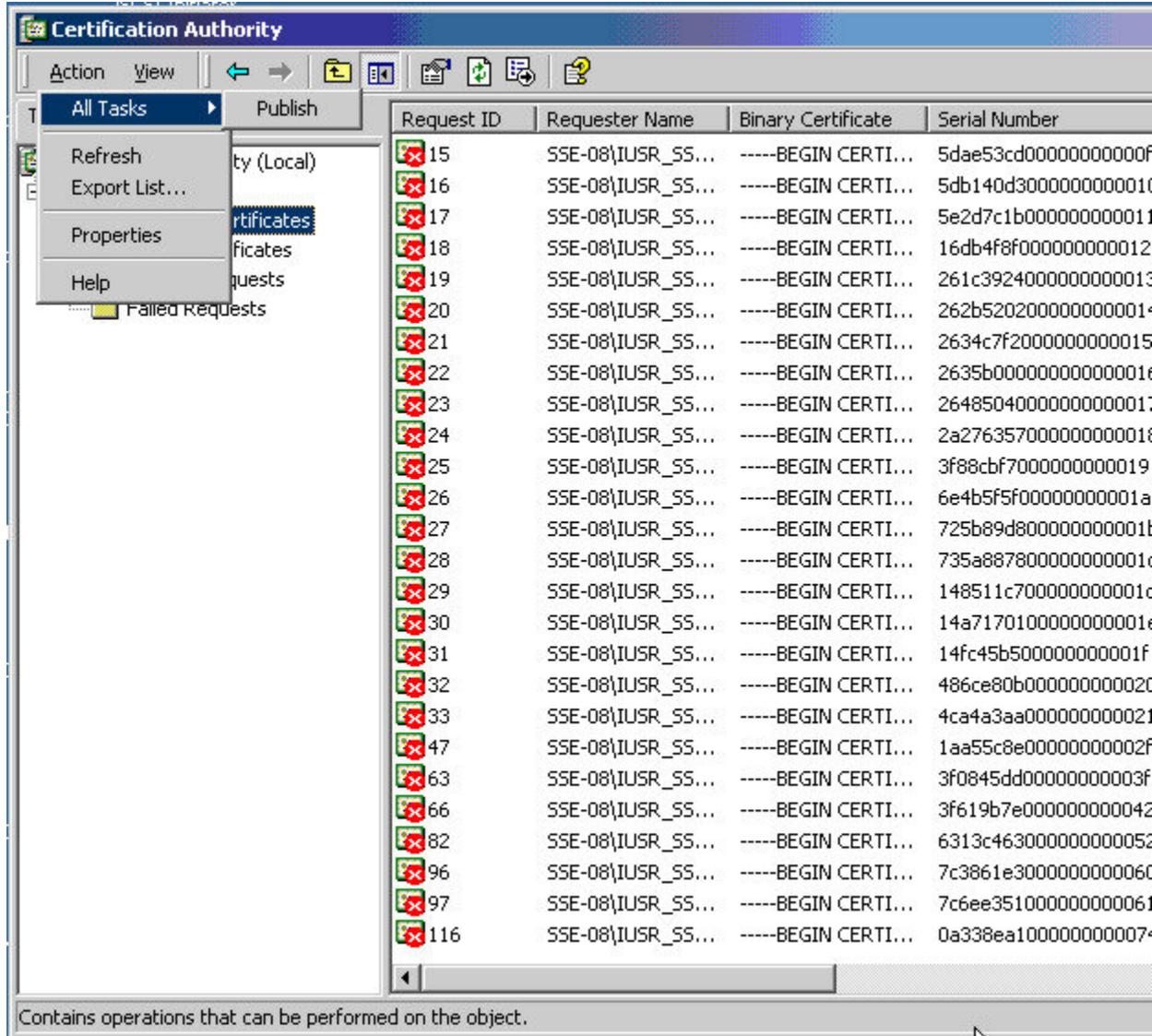


CRL の作成と公開

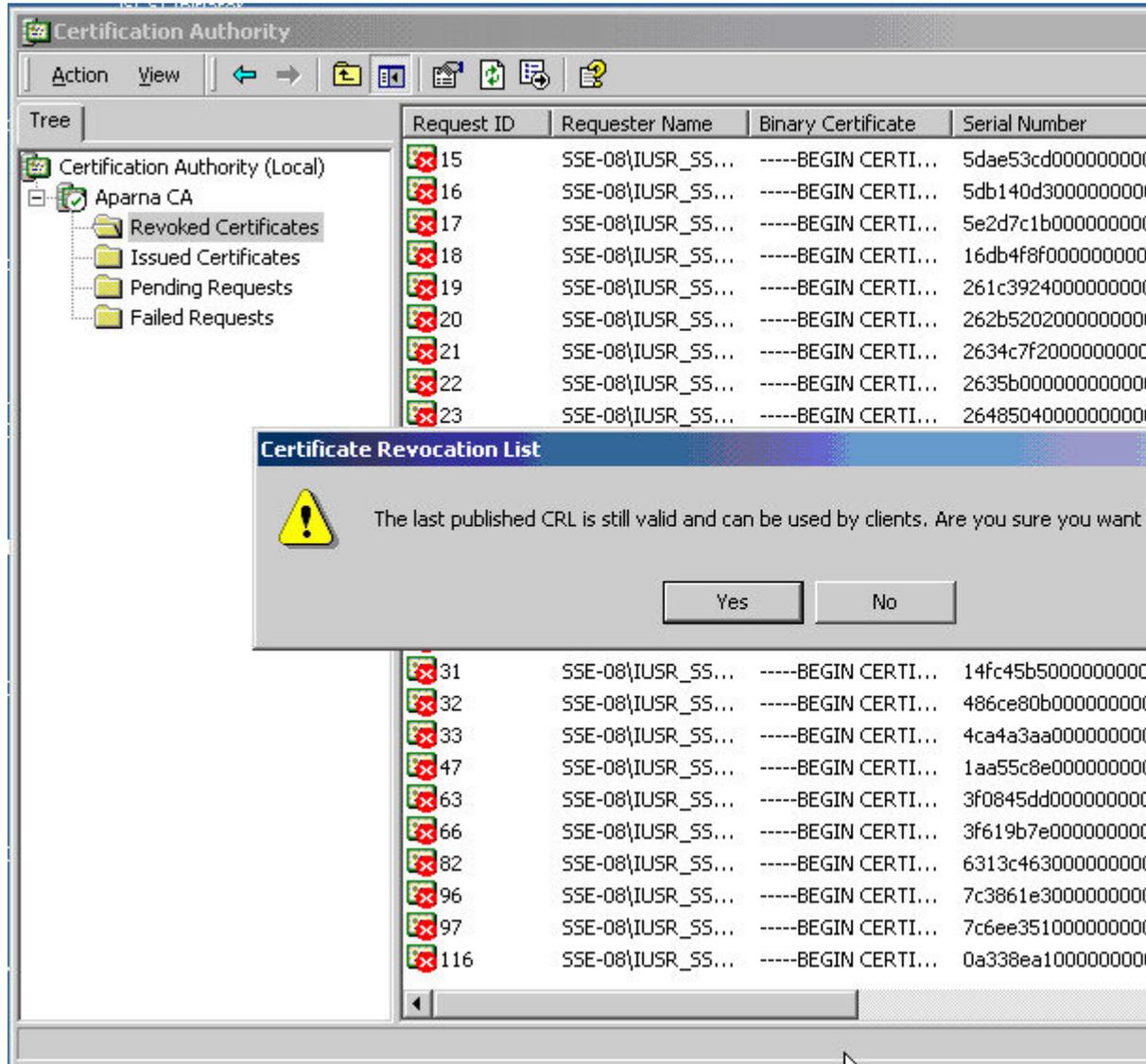
Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

Procedure

ステップ1 [Certification Authority] 画面で、[Action] > [All Tasks] > [Publish] を選択します。



ステップ2 [Certificate Revocation List] ダイアログボックスで [Yes] をクリックし、最新の CRL を公開します。



CRL のダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

Procedure

- ステップ1 Microsoft Certificate Services Web インターフェイス上の [Request the CA certificate or certificate revocation list] オプション ボタンを選択し、[Next] ボタンをクリックします。

Microsoft Certificate Services -- Apama CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and perform other tasks depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

ステップ2 [Download latest certificate revocation list] リンクをクリックします。

Microsoft Certificate Services -- Aparna CA

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from t

It is not necessary to manually install the CA certification path if you request and install a CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate:

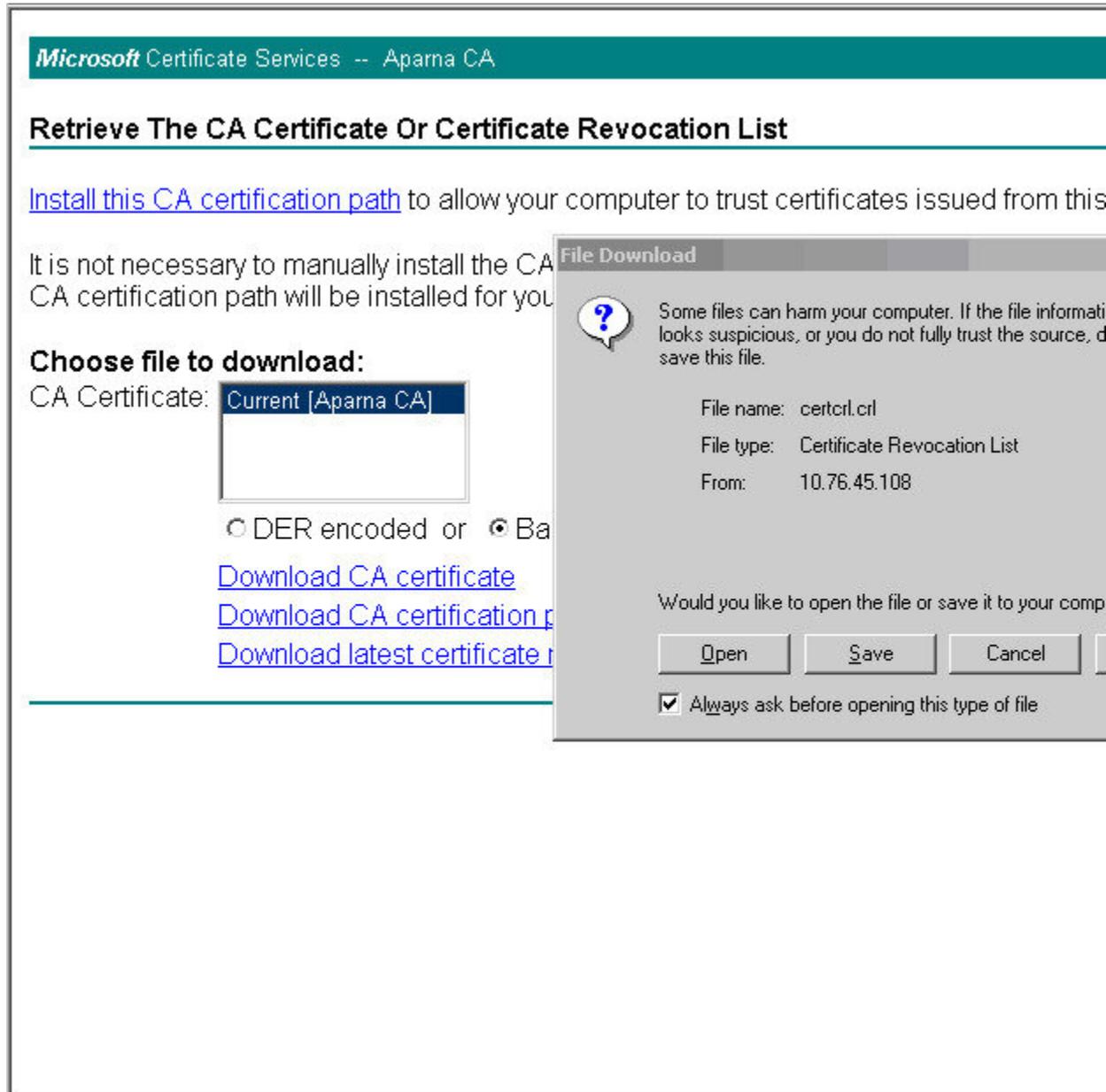
DER encoded or Base 64 encoded

[Download CA certificate](#)

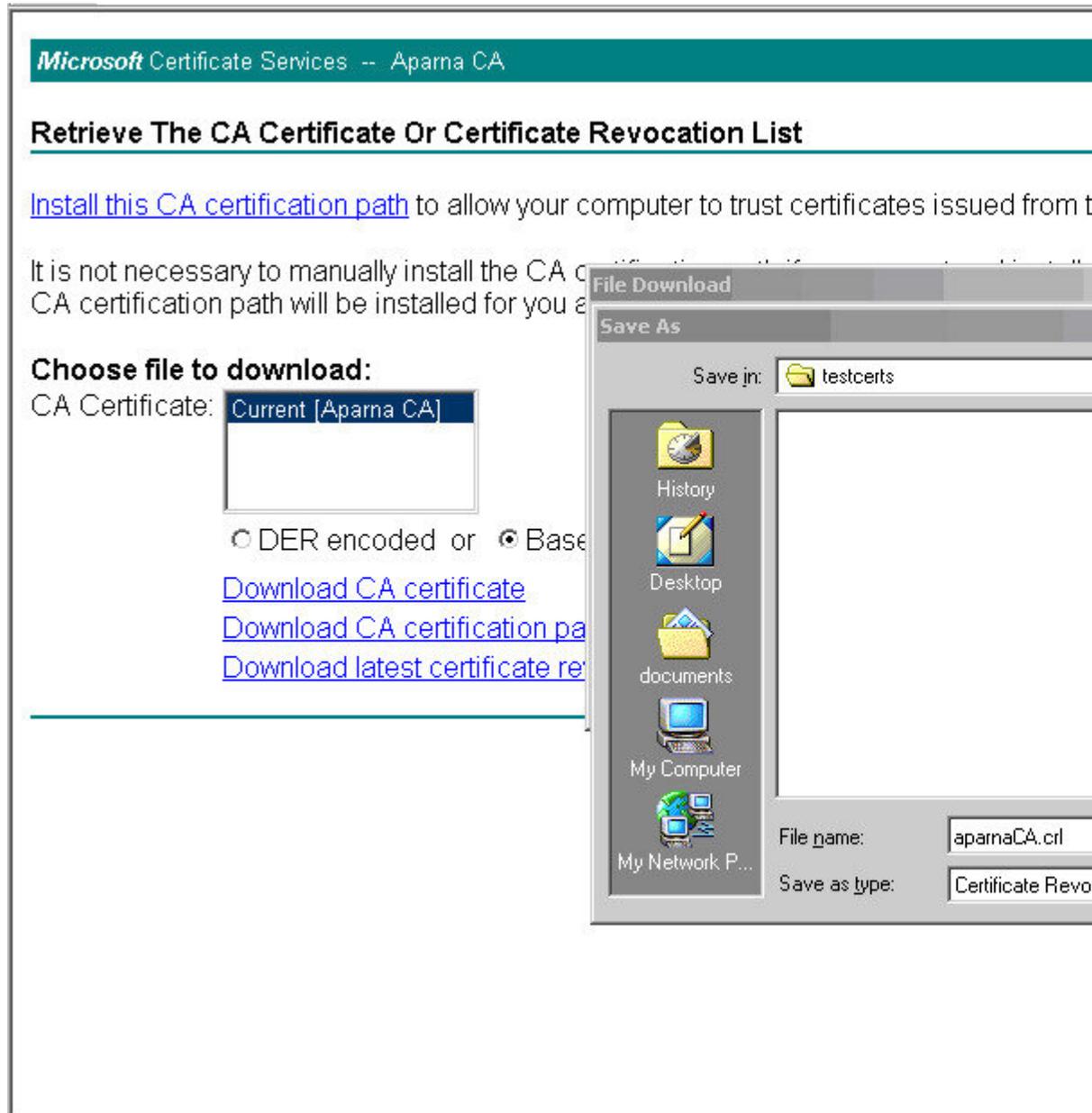
[Download CA certification path](#)

[Download latest certificate revocation list](#)

ステップ3 [File Download] ダイアログボックスで、[Save] をクリックします。



ステップ4 [Save As] ダイアログボックスに宛先ファイル名を入力し、[Save] をクリックします。




```
SwitchA(config)#
```

ステップ3 CRLの内容を表示します。

```
SwitchA(config)# show crypto ca crl myCA

Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
  Last Update: Nov 12 04:36:04 2005 GMT
  Next Update: Nov 19 16:56:04 2005 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
      1.3.6.1.4.1.311.21.1:
        ...
Revoked Certificates:
  Serial Number: 611B09A1000000000002
    Revocation Date: Aug 16 21:52:19 2005 GMT
  Serial Number: 4CDE464E000000000003
    Revocation Date: Aug 16 21:52:29 2005 GMT
  Serial Number: 4CFC2B42000000000004
    Revocation Date: Aug 16 21:52:41 2005 GMT
  Serial Number: 6C699EC2000000000005
    Revocation Date: Aug 16 21:52:52 2005 GMT
  Serial Number: 6CCF7DDC000000000006
    Revocation Date: Jun 8 00:12:04 2005 GMT
  Serial Number: 70CC4FFF000000000007
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 4D9B1116000000000008
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 52A80230000000000009
    Revocation Date: Jun 27 23:47:06 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        CA Compromise
  Serial Number: 5349AD4600000000000A
    Revocation Date: Jun 27 23:47:22 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        CA Compromise
  Serial Number: 53BD173C00000000000B
    Revocation Date: Jul 4 18:04:01 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Certificate Hold
  Serial Number: 591E7ACE00000000000C
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 5D3FD52E00000000000D
    Revocation Date: Jun 29 22:07:25 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Key Compromise
  Serial Number: 5DAB771300000000000E
    Revocation Date: Jul 14 00:33:56 2005 GMT
  Serial Number: 5DAE53CD00000000000F
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 5DB140D3000000000010
    Revocation Date: Aug 16 21:53:15 2005 GMT
```

```
Serial Number: 5E2D7C1B000000000011
  Revocation Date: Jul  6 21:12:10 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Cessation Of Operation
Serial Number: 16DB4F8F000000000012
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 261C3924000000000013
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 262B5202000000000014
  Revocation Date: Jul 14 00:33:10 2005 GMT
Serial Number: 2634C7F2000000000015
  Revocation Date: Jul 14 00:32:45 2005 GMT
Serial Number: 2635B000000000000016
  Revocation Date: Jul 14 00:31:51 2005 GMT
Serial Number: 26485040000000000017
  Revocation Date: Jul 14 00:32:25 2005 GMT
Serial Number: 2A276357000000000018
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 3F88CBF7000000000019
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 6E4B5F5F00000000001A
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 725B89D800000000001B
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 735A887800000000001C
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 148511C700000000001D
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14A7170100000000001E
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14FC45B500000000001F
  Revocation Date: Aug 17 18:30:42 2005 GMT
Serial Number: 486CE80B000000000020
  Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 4CA4A3AA000000000021
  Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 1AA55C8E00000000002F
  Revocation Date: Sep  5 17:07:06 2005 GMT
Serial Number: 3F0845DD00000000003F
  Revocation Date: Sep  8 20:24:32 2005 GMT
Serial Number: 3F619B7E000000000042
  Revocation Date: Sep  8 21:40:48 2005 GMT
Serial Number: 6313C463000000000052
  Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E3000000000060
  Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE351000000000061
  Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA1000000000074      <-- Revoked identity certificate
  Revocation Date: Nov 12 04:34:42 2005 GMT
Signature Algorithm: sha1WithRSAEncryption
0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
1a:9f:1a:49:b7:9c:58:24:d7:72
```

上限

次の表に、CA およびデジタル証明書のパラメータの最大限度を示します。

Table 1: CA およびデジタル証明書の最大限度

| 機能 | 最大制限 |
|--------------------------|----------|
| スイッチ上で宣言するトラストポイント | 16 |
| スイッチ上で生成する RSA キーペア | 16 |
| RSA キーペアサイズ | 4096 ビット |
| スイッチ上に設定するアイデンティティ証明書 | 16 |
| CA 証明書チェーンに含まれる証明書 | 10 |
| 特定の CA に対して認証されるトラストポイント | 10 |

デフォルト設定

次の表に、CA およびデジタル証明書のパラメータのデフォルト設定を示します。

Table 2: CA およびデジタル証明書のパラメータのデフォルト値

| パラメータ | デフォルト |
|--------------------|-------------|
| トラストポイント | なし |
| RSA キーペア | なし |
| RSA キーペアのラベル | Switch FQDN |
| RSA キーペアのモジュール | 1024 |
| RSA キーペアのエクスポートの可否 | Yes |
| トラストポイントの失効チェック方式 | CRL |

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。