CHAPTER 6

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。

CA およびデジタル証明書の概要

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ーラビリティが提供されます。

CA は、証明書の要求を管理して、ホスト、ネットワーク デバイス、またはユーザなどの加入エンティティに対して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だけです。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。

ここでは、認証局（CA）およびデジタル証明書の概要について説明します。内容は次のとおりです。

CA およびデジタル証明書の目的

CA は、証明書の要求を管理して、ホスト、ネットワーク デバイス、またはユーザなどの加入エンティティに対して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だけです。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 の公開キーを認識している必要があります。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 デバイスをスケーラブルに認証できます。

信頼モデル、トラストポイント、アイデンティティ CA

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 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。信頼できる CA のルート証明書（または下位 CA の場合には完全な証明書チェーン）を安全に取得し、ローカルで保管するプロセスは、*CA 認証*と呼ばれ、CA を信頼するための必須ステップです。

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*、CA そのものを *トラストポイント 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。

MDS スイッチも、（IPsec/IKE などの）アイデンティティ証明書を取得するために、トラスト ポイントに登録できます。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。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキー ラベルは、スイッチの完全修飾ドメイン名（FQDN）です。

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 エクスチェンジ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 1 つまたは複数の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。

複数の信頼できる CA のサポート

MDS スイッチには、複数のトラスト ポイントを設定して、それぞれ異なる CA に関連付けることにより、複数の信頼できる CA を設定できます。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、スイッチを登録する必要はありません。代わりに、ピアが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、ピアの証明書がスイッチのアイデンティティを定義した 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。

複数の信頼できる CA を設定することにより、IKE を使用して IPsec トンネルを確立する場合に、異なるドメイン（異なる CA）に登録した 2 台以上のスイッチ間で相互のアイデンティティを確認できます。

PKI の登録のサポート

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、証明書を要求するスイッチと CA 間で実行されます。

スイッチの PKI 登録プロセスでは、次の手順を実行します。

1. スイッチ上に RSA 秘密キーと公開キーのキー ペアを生成します。
2. 証明書要求を標準形式で生成し、CA に転送します。
3. CA が受信した登録要求を承認する場合、CA サーバ上で 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. 発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
5. 証明書を、スイッチ上の不揮発性ストレージ領域（ブートフラッシュ）に書き込みます。

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、文字通り、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。

複数の RSA キー ペアおよびアイデンティティ CA のサポート

複数のアイデンティティ 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。スイッチ上で複数の RSA キー ペアを生成し、各キー ペアを異なるトラスト ポイントに関連付けることができます。これにより、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要求を作成できます。

ピア証明書の確認

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、アプリケーション固有のセキュリティ 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。

失効チェックでは、2 つの方式がサポートされています。証明書失効リスト（CRL）および Online Certificate Status Protocol（OCSP）です。トラスト ポイントは、いずれかまたは両方の方式を使用して、ピア証明書が失効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、期限前に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、スイッチのブートフラッシュにキャッシュされるように手動で設定できます。IPsec または SSH による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ければ、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。

OCSP サポート

Online Certificate Status Protocol（OCSP）は、オンラインでの証明書失効チェックを容易にします。各トラスト ポイントに OCSP URL を指定できます。アプリケーションは、失効チェック方式を、指定された順序で選択します。CRL、OCSP、none、またはこれらの方式の組み合わせを指定できます。

証明書および関連キー ペアのインポート/エクスポートのサポート

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）形式でインポートできます。

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 PKCS#12 標準形式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。PKCS#12 ファイルには、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）の情報が含まれます。

CA 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。ここでは、次の内容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サブジェクトとして、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。

注意　証明書の生成後にホスト名または 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。

	コマンド	目的
ステップ 1	`switch# config terminal` `switch(config)#`	コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 2	`switch(config)# hostname SwitchA`	スイッチのホスト名（SwitchA）を設定します。
ステップ 3	`SwitchA(config)# ip domain-name example.com`	スイッチの IP ドメイン名（example.com）を設定します。

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 エクスチェンジの実行中に、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 キー ペアを生成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config 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。 （注）　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）を考慮してください。 （注）　スイッチに設定できるキー ペアの最大数は、16 です。
	`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、1536、および 2048 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。
	`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。 ⚠ 注意　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。 （注）　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 CA アソシエーションの作成

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。

	コマンド	目的
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。 (注)　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。
	`switch(config)# no crypto ca trustpoint admin-ca`	トラストポイント CA を削除します。
ステップ 2	`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)。 (注)　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 3	`switch(config-trustpoint)# rsakeypair 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」セクション (6-7 ページ)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。
	`switch(config-trustpoint)# no rsakeypair SwitchA`	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(デフォルト)。
ステップ 4	`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 5	`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。

CA の認証

信頼できる 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 が自身の証明書に署名したもの)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。

(注)　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*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。

	コマンド	目的
ステップ 1	switch# **config t** 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 authenticate admin-ca** input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : **-----BEGIN CERTIFICATE-----** **MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB** **kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO** **MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE** **ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD** **QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN** **AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth** **cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG** **A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN** **AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI** **OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E** **BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ** **GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs** **L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRfbnJv** **bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB** **BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/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**	CA の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。CA を宣言したときに使用した名前と同じ名前を使用します。 (注)　ある CA に対して認証できるトラストポイントの最大数は 10 です。

(注)　証明書の確認および PKCS#12 形式のエクスポートでは CA チェーンが必要になるので、下位 CA の認証の場合には、最終的に自己署名された CA までの CA 証明書の完全なチェーンが必要になります。

証明書取消確認方法の設定

クライアント（IKE ピアまたは SSH ユーザなど）とのセキュリティ エクスチェンジの実行中に、MDS スイッチはクライアントから送信されたピア証明書の確認を実行します。この確認プロセスには、証明書失効ステータスのチェックを含めることができます。

送信された証明書が失効しているかどうかを調べるには、複数の方式があります。スイッチが CA からダウンロードした CRL をチェックするように設定するか（「CRL の設定」セクション（6-14 ページ）を参照）、ネットワークでサポートされている場合には OSCP を使用するか、またはその両方を使用できます。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。ただし、CRL のダウンロード後に証明書が失効された場合、失効ステータスを認識できません。OSCP では、CA の最新の CRL をチェックできます。ただし、OSCP を使用するとネットワーク トラフィックが生成されるので、ネットワークの効率に影響することがあります。失効証明書をチェックする最も確実な方法は、ローカル CRL チェックと OSCP の両方を使用することです。

(注)　証明書の失効チェックを設定する前に、CA を認証する必要があります。

証明書失効確認方式を設定するには、次の手順を実行します。

	コマンド	目的
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)# ocsp url http://crlcheck.cisco.com`	OCSP の URL を失効証明書のチェックに使用するよう指定します。
	`switch(config-trustpoint)# no ocsp url http://crlcheck.cisco.com`	OCSP の URL を削除します。
ステップ 3	`switch(config-trustpoint)# revocation-check oscp`	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 OCSP を指定します。 (注)　OSCP の URL は、失効チェック方式として OSCP を指定する前に、設定しておく必要があります。
	`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)。
	`switch(config-trustpoint)# revocation-check crl oscp`	最初の失効チェック方式として CRL を指定し、次の方式として OCSP を指定します。CRL 方式を、このトラストポイントと同じ CA が発行したピア証明書の確認時に使用することに失敗した場合(たとえば、CRL が見つからないまたは期限切れのため)、OSCP が使用されます。 (注)　OSCP の URL は、失効チェック方式として OSCP を指定する前に、設定しておく必要があります。
	`switch(config-trustpoint)# revocation-check none`	失効証明書をチェックしません。
	`switch(config-trustpoint)# no revocation-check`	デフォルトの方式に戻ります。

証明書要求の生成

スイッチの各 RSA キーペアについて、関連付けたトラスト 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。

	コマンド	目的
ステップ 1	switch# **config 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:**nbv123** The subject name in the certificate will be: **Vegas-1.cisco.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:**172.22.31.162** The certificate request will be displayed... -----BEGIN CERTIFICATE REQUEST----- MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST-----	認証した CA に対する証明書要求を作成します。 (注)　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。

	コマンド	目的
ステップ 1	switch# **config 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-----** **MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G** **CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD** **VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz** **Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w** **NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu** **Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C** **dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47** **glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb** **x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw** **GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR** **bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW** **pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE** **BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w** **DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh** **cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6** **Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6** **Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH** **AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl** **LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4** **XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF** **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。 (注)　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。

コンフィギュレーションの保存

変更したコンフィギュレーションは、終了時に情報が失われないように、保存しておく必要があります。

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、外部サーバに保存しておくことを推奨します（「PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート」セクション（6-13 ページ）を参照）。

（注）　コンフィギュレーションを外部サーバにコピーすると、証明書およびキーペアも保存されます。

CA および証明書の設定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。この項では、次のトピックについて取り上げます。

- PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート（6-13 ページ）
- CRL の設定（6-14 ページ）
- CA 設定からの証明書の削除（6-14 ページ）
- スイッチからの RSA キーペアの削除（6-15 ページ）
- キーペアと CA 情報の表示（6-16 ページ）

PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート

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 PKCS#12 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。

（注）　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 PKCS#12 形式ファイルにエクスポートする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config 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 nbv123`	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 nbv123 によって保護された PKCS#12 形式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`	PKCS#12 形式のファイルを TFTP サーバにコピーします。

証明書およびキー ペアを PKCS#12 形式ファイルからインポートする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# copy tftp:adminid.p12 bootflash:adminid.p12`	PKCS#12 形式のファイルを TFTP サーバからコピーします。
ステップ 2	`switch# config 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 nbv123`	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 nbv123 によって保護された PKCS#12 形式でインポートします。

（注）　PKCS#12 ファイルを正常にインポートするには、トラスト ポイントが空白である（RSA キーペアが関連付けられていない、および CA 認証により CA が関連付けられていない）必要があります。

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。

	コマンド	目的
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# config 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。

CA 設定からの証明書の削除

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 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。

	コマンド	目的
ステップ 1	`switch# config t` `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。

	コマンド	目的
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。
	`switch(config-trustpoint)# delete certificate force`	アイデンティティ証明書を削除します。 (注)　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 5	`switch(config-trustpoint)# end` `switch#`	EXEC モードに戻ります。
ステップ 6	`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。

	コマンド	目的
ステップ 1	`switch# config 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。

(注)　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。「証明書要求の生成」セクション（6-10 ページ）を参照してください。

キーペアと CA 情報の表示

キーペアと CA 情報を表示するには、EXEC モードで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。

この項では、次のトピックについて取り上げます。

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。

ステップ 1　スイッチの FQDN を設定します。

```
switch# config t
Enter configuration commands, one per line.End with CNTL/Z.
switch(config)# switchname Vegas-1
Vegas-1(config)#
```

ステップ 2　スイッチの DNS ドメイン名を設定します。

```
Vegas-1(config)# ip domain-name cisco.com
Vegas-1(config)#
```

ステップ 3　トラストポイントを作成します。

```
Vegas-1(config)# crypto ca trustpoint myCA
Vegas-1(config-trustpoint)# exit
Vegas-1(config)# do show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
Vegas-1(config)#
```

ステップ 4　スイッチの RSA キーペアを作成します。

```
Vegas-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Vegas-1(config)# do show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes

Vegas-1(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。

```
Vegas-1(config)# crypto ca trustpoint myCA
Vegas-1(config-trustpoint)# rsakeypair myKey
Vegas-1(config-trustpoint)# exit
Vegas-1(config)# do show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods:  crl
Vegas-1(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（「CA 証明書のダウンロード」セクション（6-19 ページ）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。

```
Vegas-1(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-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/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
Vegas-1(config)#

Vegas-1(config)# do 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。

```
Vegas-1(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:nbv123
 The subject name in the certificate will be: Vegas-1.cisco.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-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

Vegas-1(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」セクション（6-24 ページ）を参照）。

ステップ 10　アイデンティティ証明書をインポートします。

```
Vegas-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyf1w
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Vegas-1(config)# exit
Vegas-1#
```

ステップ 11　証明書の設定を確認します。

```
Vegas-1# show crypto ca certificates
Trustpoint: myCA
certificate:
subject= /CN=Vegas-1.cisco.com
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0A338EA1000000000074
notBefore=Nov 12 03:02:40 2005 GMT
notAfter=Nov 12 03:12:40 2006 GMT
MD5 Fingerprint=3D:33:62:3D:B4:D0:87:A0:70:DE:A3:87:B3:4E:24:BF
purposes: sslserver sslclient ike

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
```

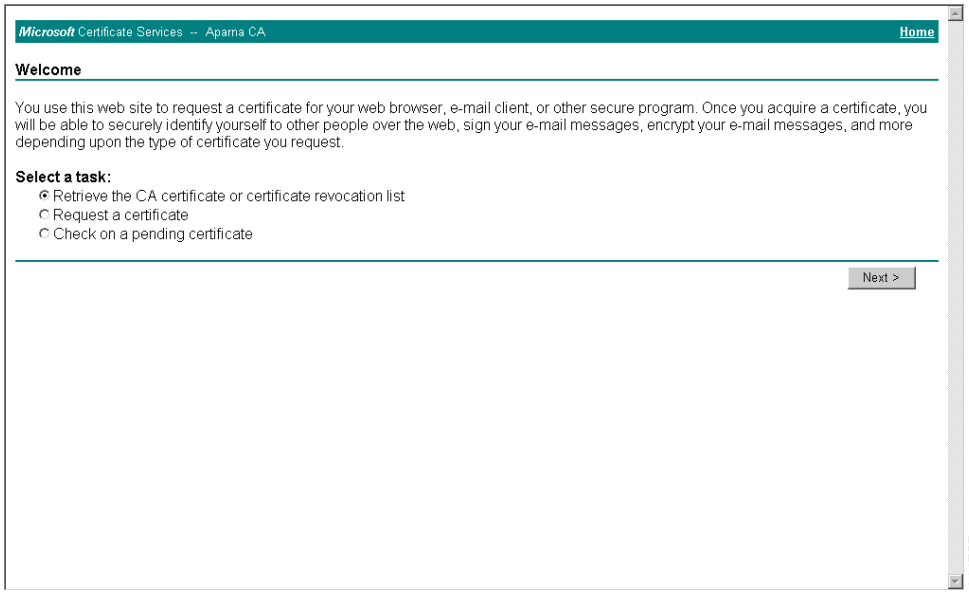
ステップ 12　証明書の設定をスタートアップ コンフィギュレーションに保存します。

```
Vegas-1# copy running-config startup-config
```

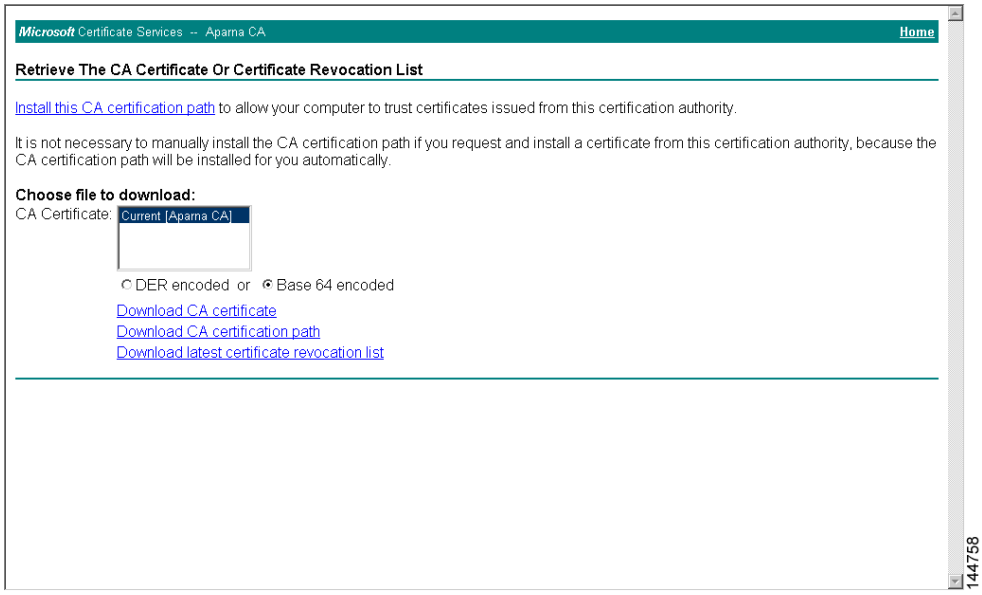
CA 証明書のダウンロード

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

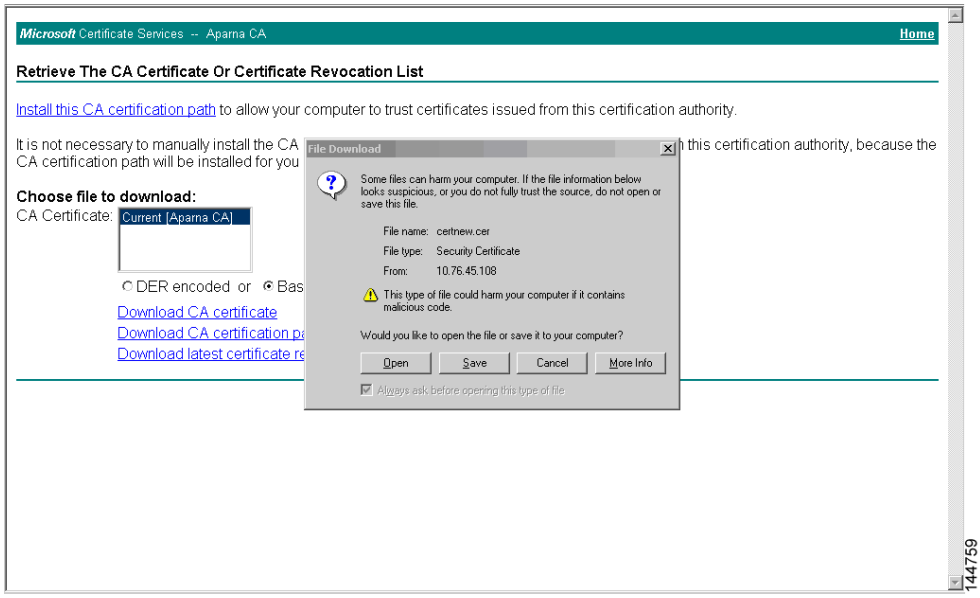
ステップ 1　Microsoft Certificate Services Web インターフェイスの [Retrieve the CA certificate or certificate revocation task] オプション ボタンを選択し、[Next] ボタンをクリックします。



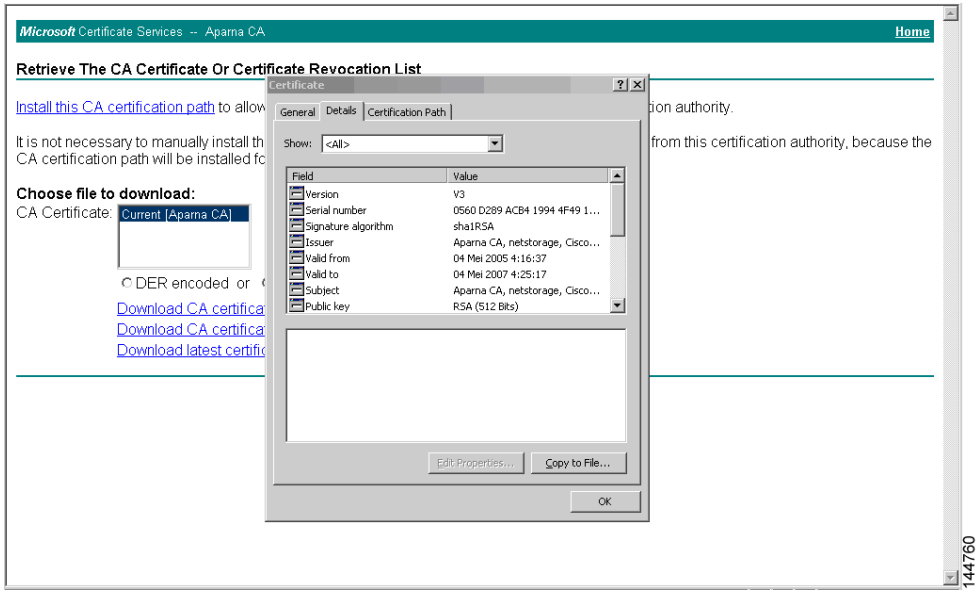
ステップ 2　表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] オプション ボタンをクリックし、[Download CA certificate] リンクをクリックします。



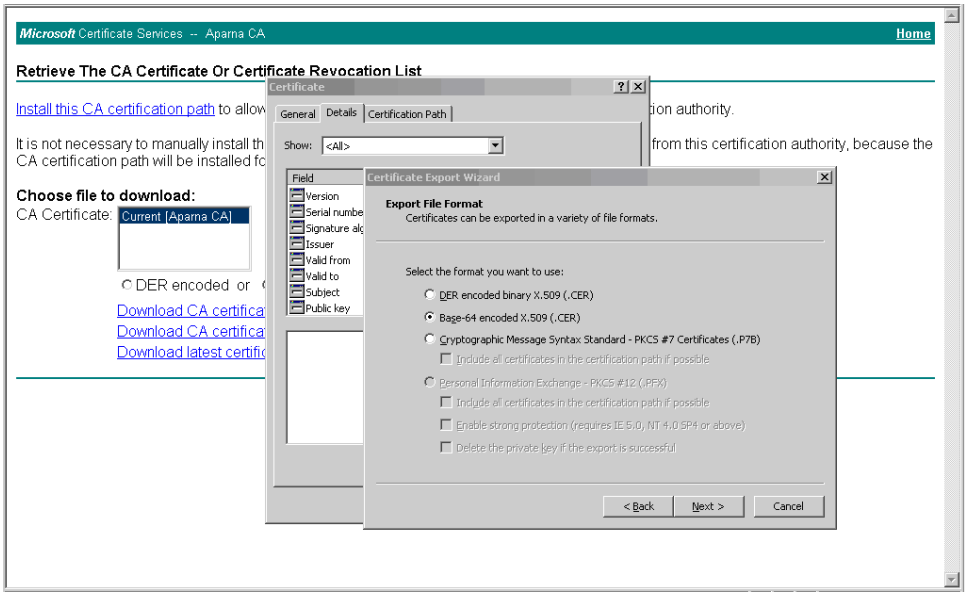
ステップ 3　[File Download] ダイアログボックスで、[Open] ボタンをクリックします。



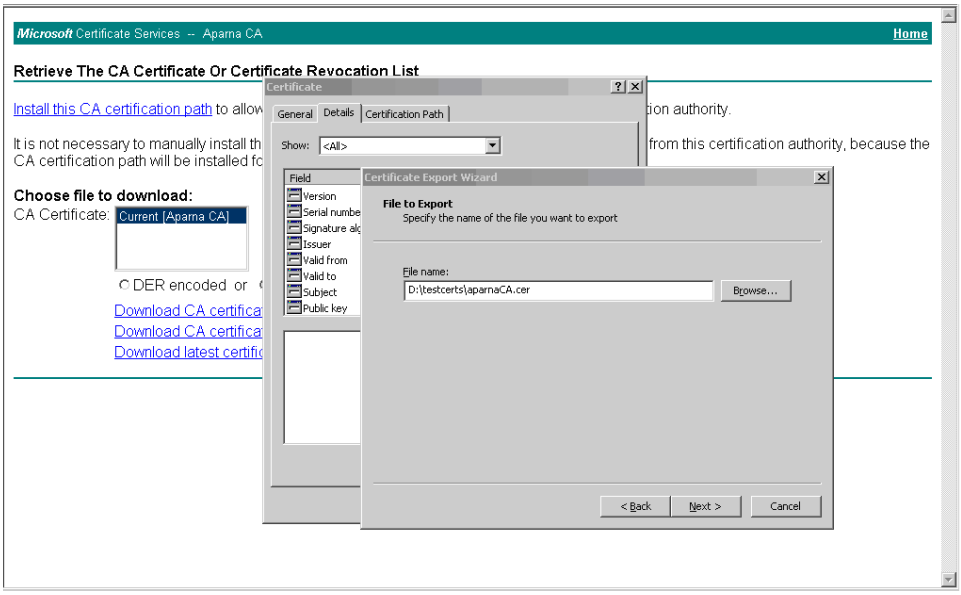
ステップ 4　[Certificate] ダイアログボックスで [Copy to File] ボタンをクリックし、[OK] をクリックします。



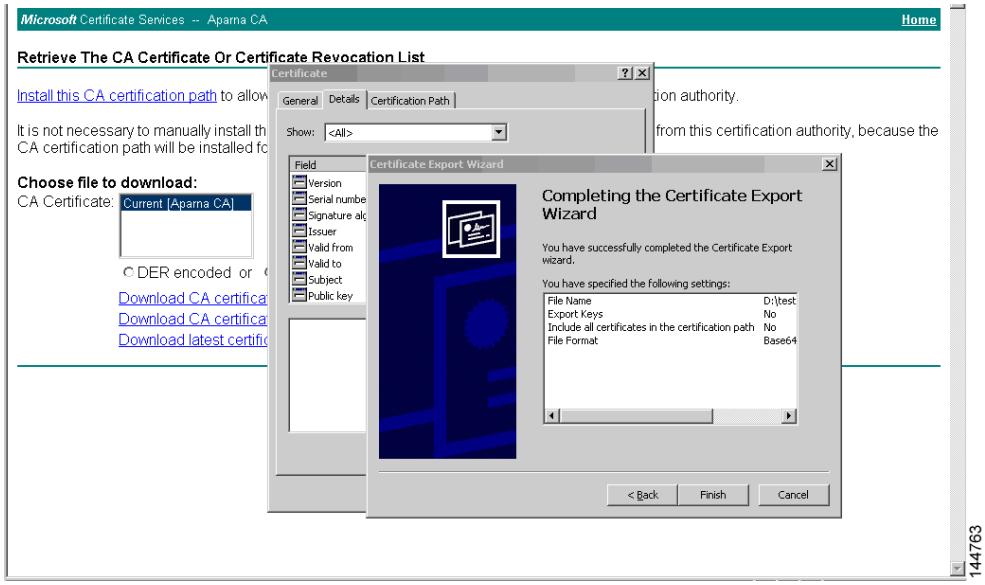
ステップ 5　[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。



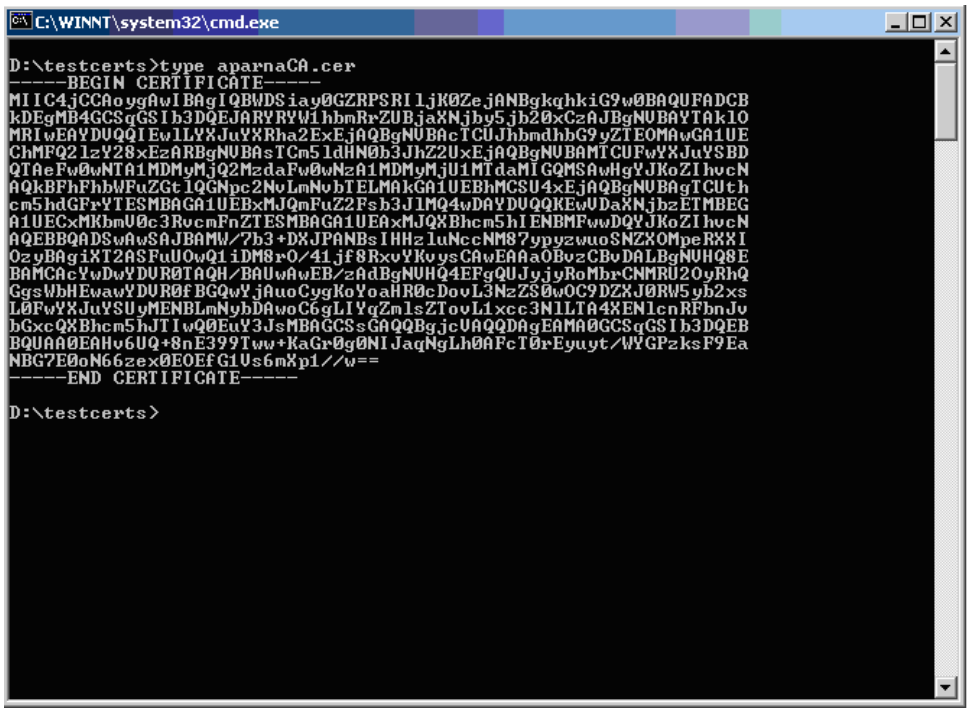
ステップ 6　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] をクリックします。



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。



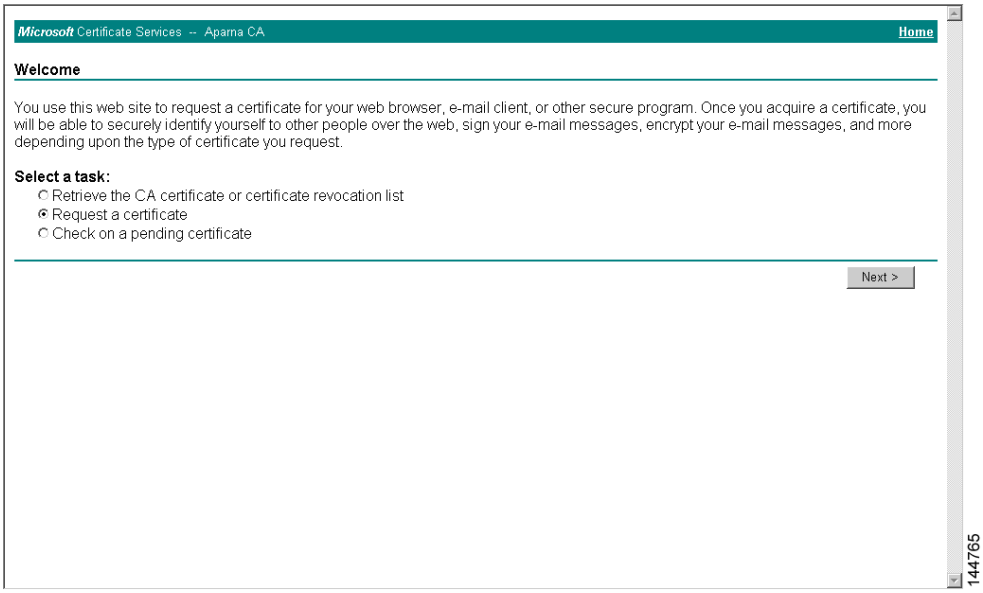
ステップ 8　Microsoft Windows の **type** コマンドを使用して、Base-64（PEM）形式で保存されている CA 証明書を表示します。



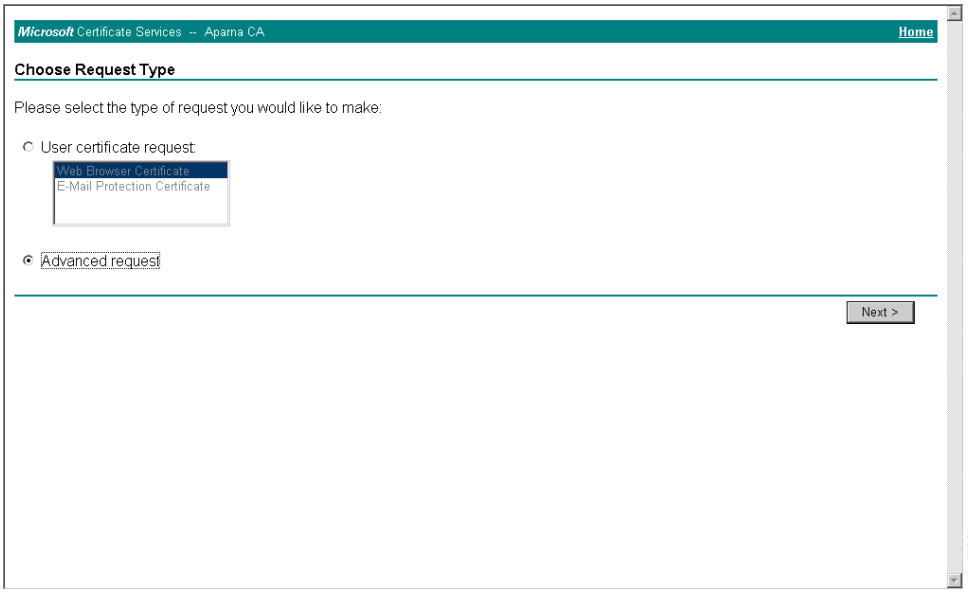
アイデンティティ証明書の要求

PKCS#10 CRS を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求する手順は、次のとおりです。

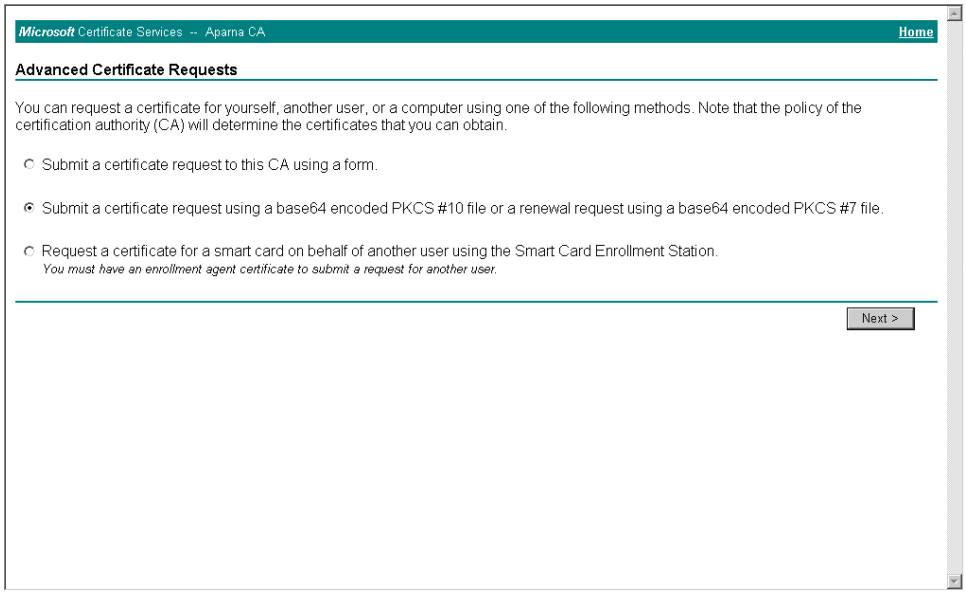
ステップ 1　Microsoft Certificate Services Web インターフェイス上の [Request a certificate] ラジオ ボタンを選択し、[Next] をクリックします。



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。

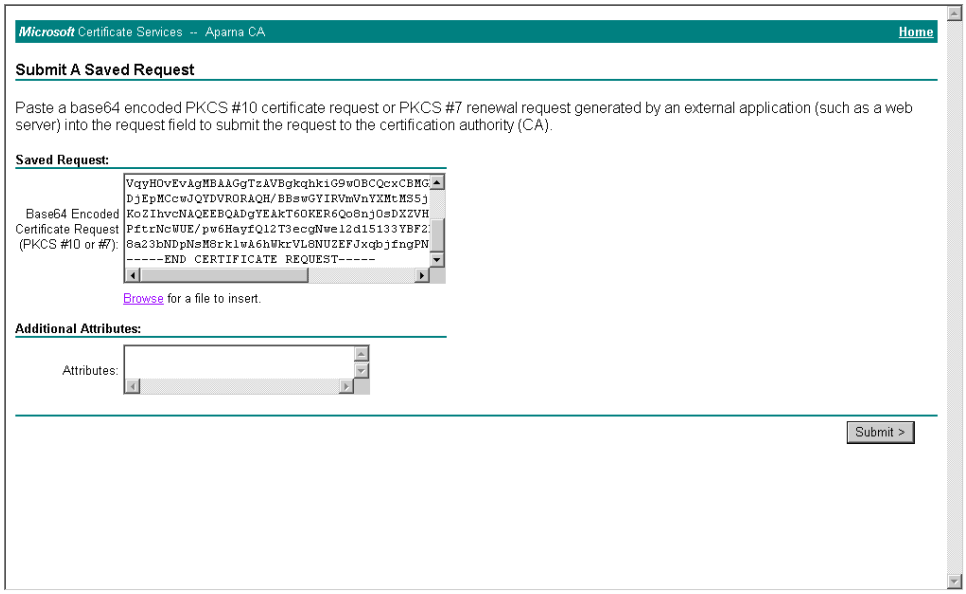


ステップ 3　[Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] オプション ボタンを選択し、[Next] ボタンをクリックします。

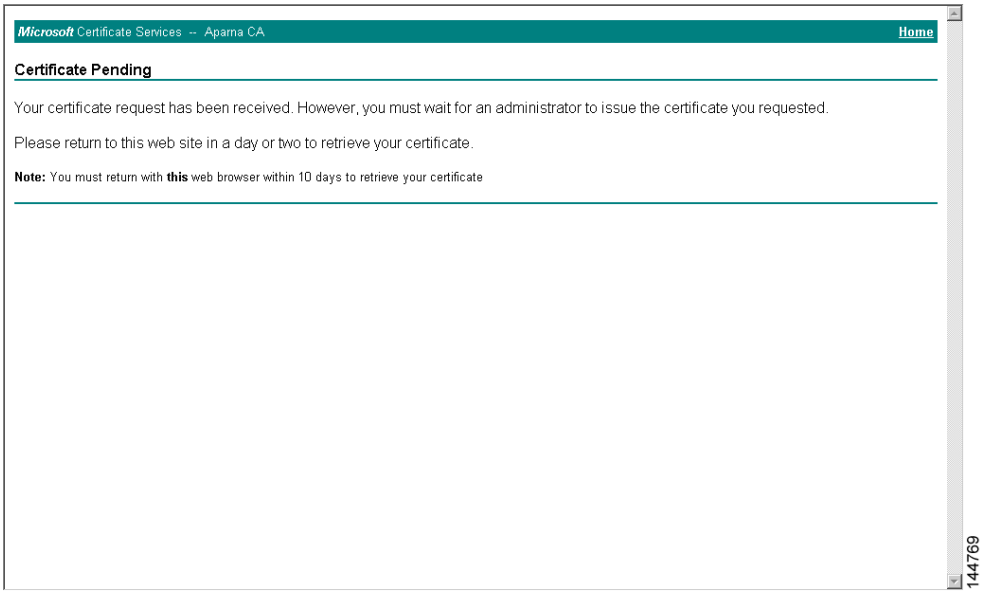


ステップ 4　[Saved Request] テキスト ボックスに base64 PKCS#10 証明書要求をペーストし、[Next] をクリックします。

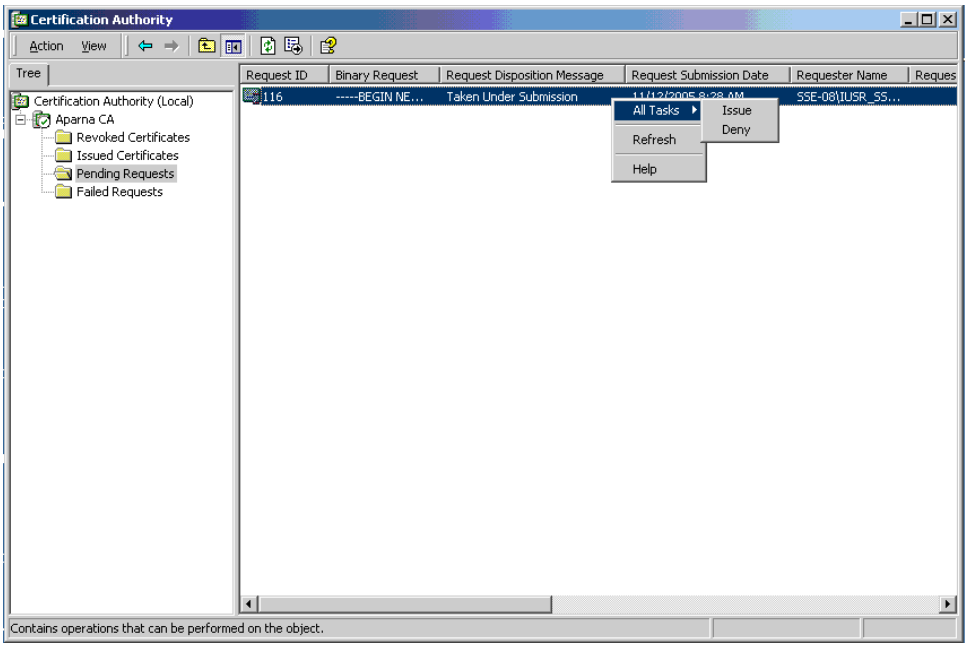
MDS スイッチのコンソールから、証明書要求がコピーされます（「証明書要求の生成」セクション（6-10 ページ）および「MDS スイッチでの証明書の設定」セクション（6-16 ページ）を参照）。



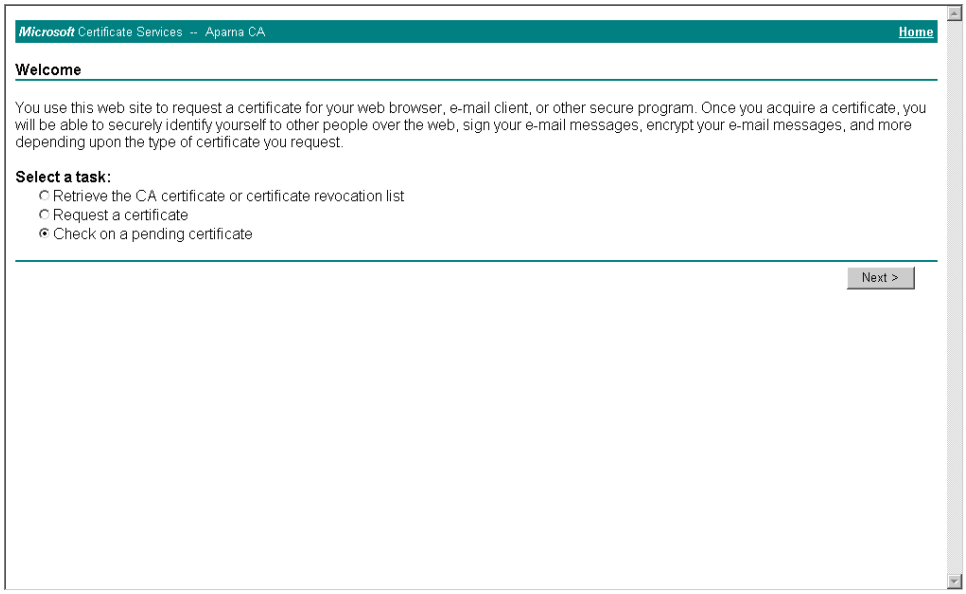
ステップ 5　CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。



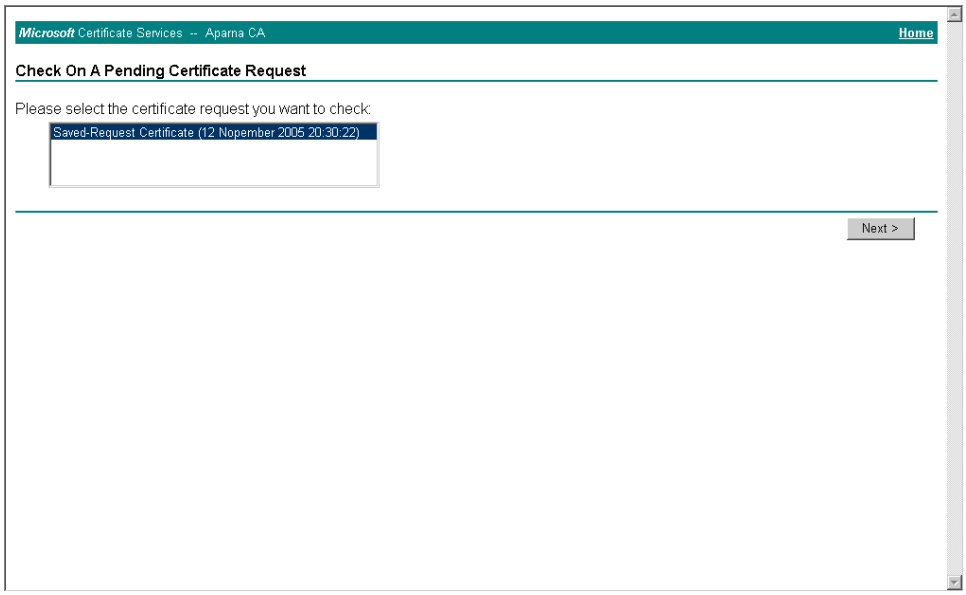
ステップ 6　CA 管理者により証明書要求が承認されます。



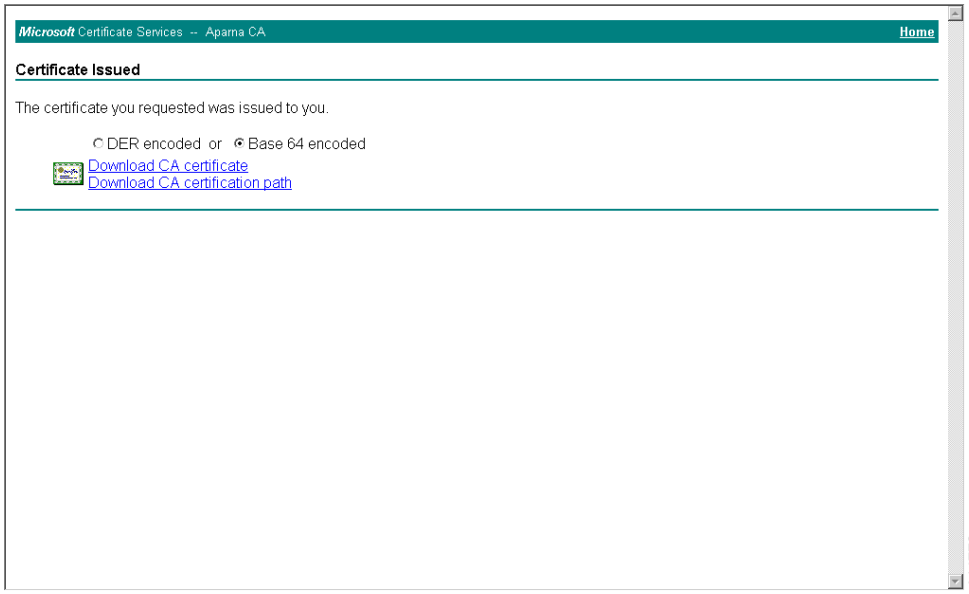
ステップ 7　Microsoft Certificate Services Web インターフェイス上の [Check on a pending certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。



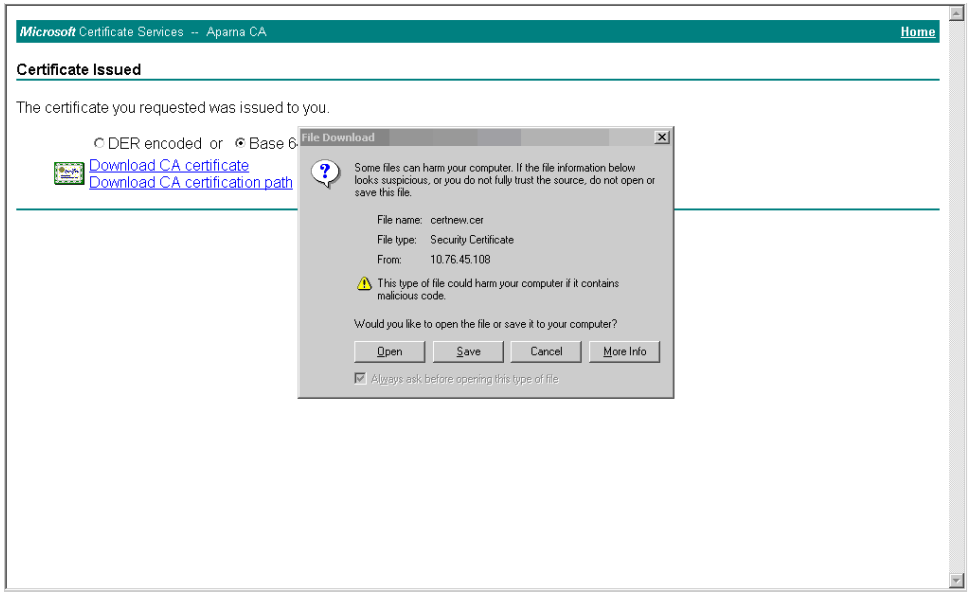
ステップ 8　確認する証明書要求を選択し、[Next] をクリックします。



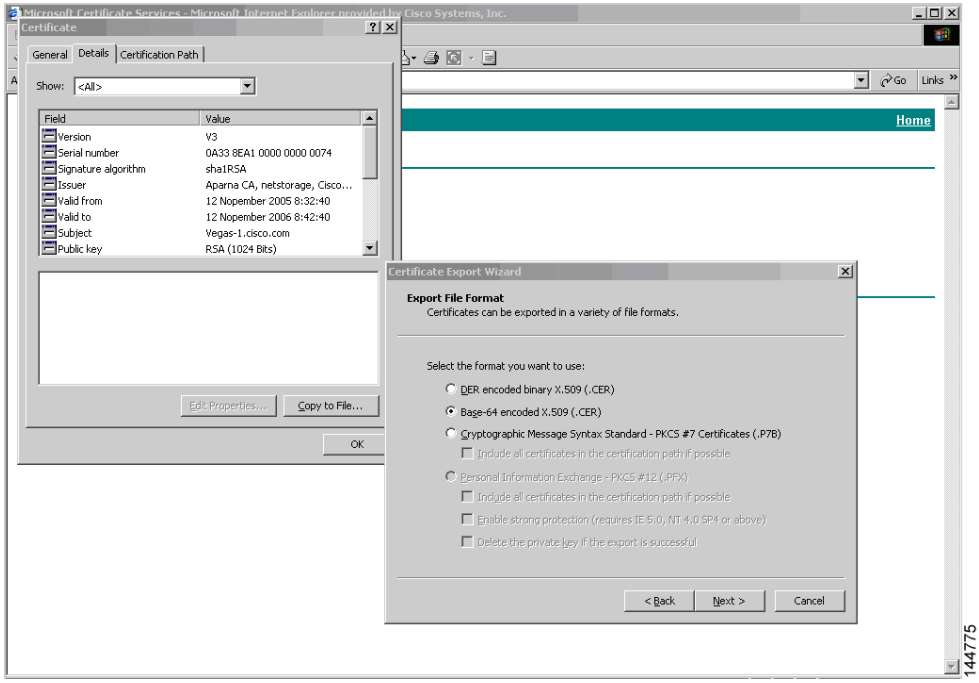
ステップ 9　[Base 64 encoded] を選択し、[Download CA certificate] リンクをクリックします。



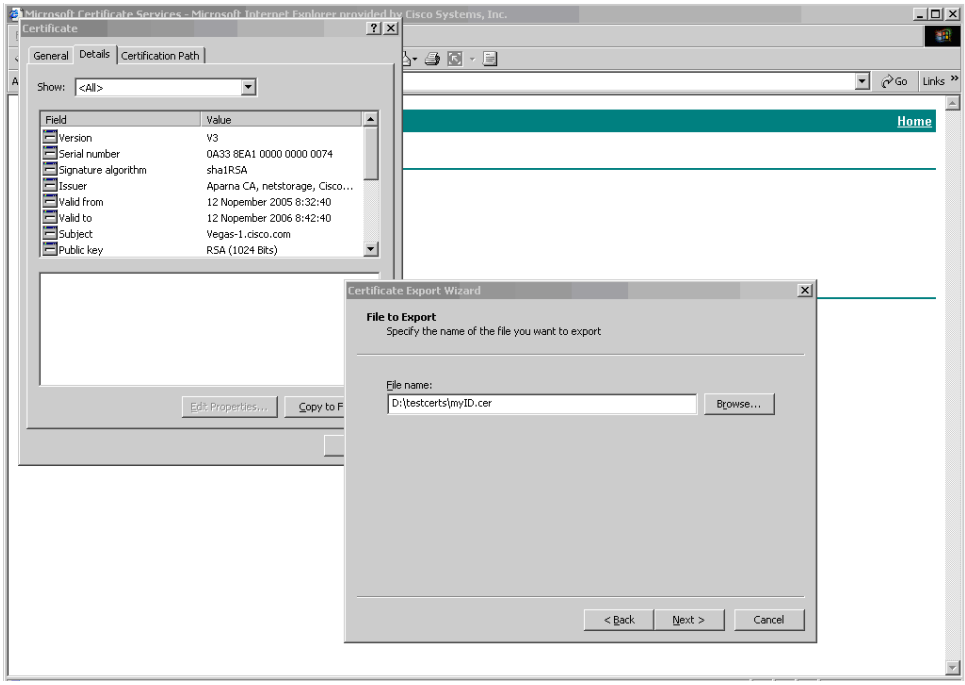
ステップ 10　[File Download] ダイアログボックスで、[Open] をクリックします。



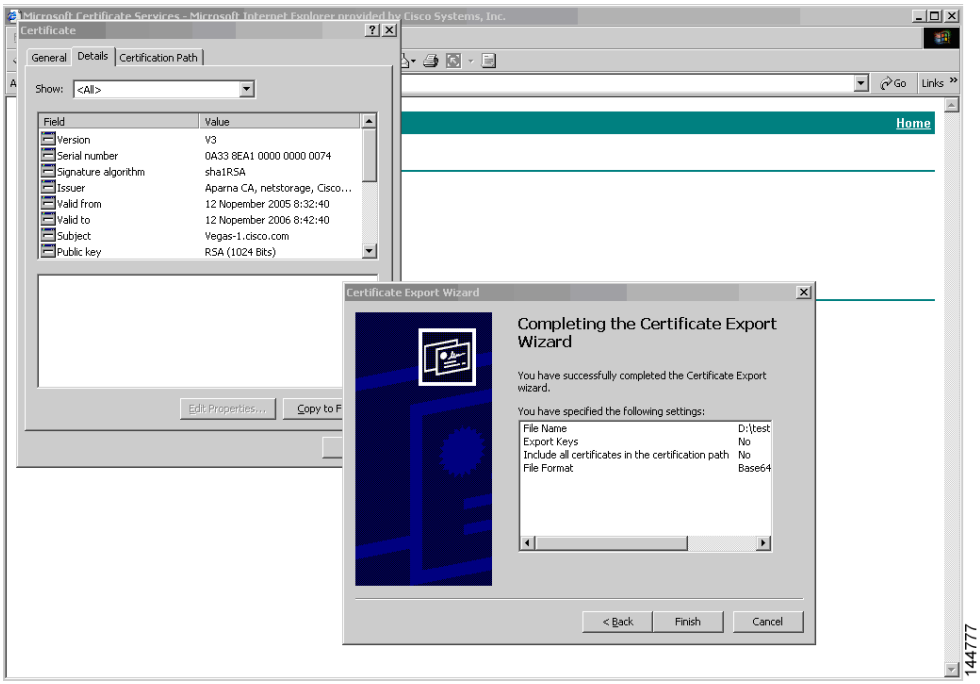
ステップ 11　[Certificate] ダイアログボックスで [Details] タブをクリックし、[Copy to File] ボタンをクリックします。[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (.CER)] オプション ボタンを選択し、[Next] ボタンをクリックします。



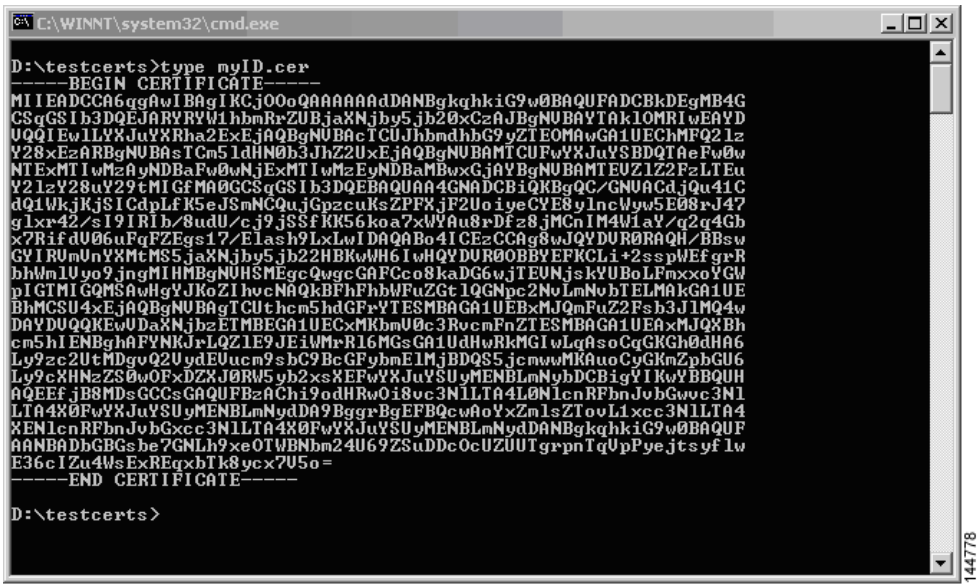
ステップ 12　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] をクリックします。



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。

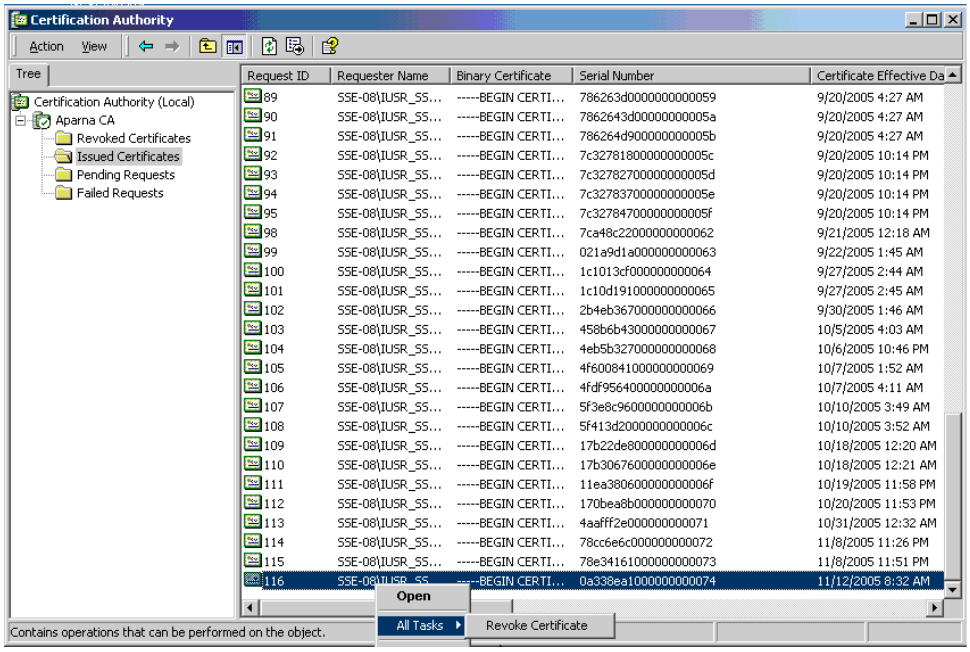


証明書の失効

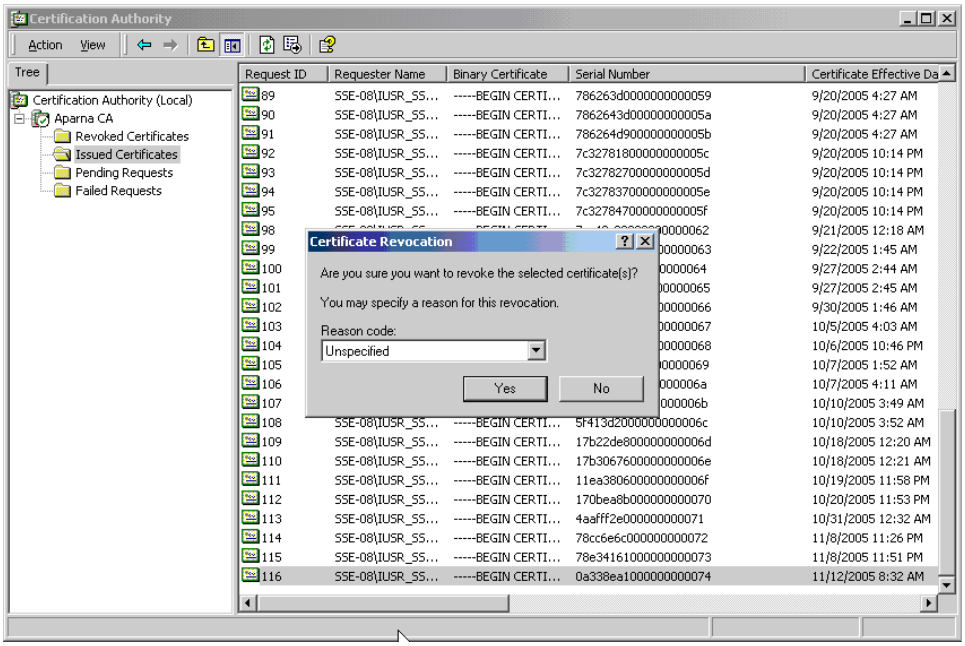
Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

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。

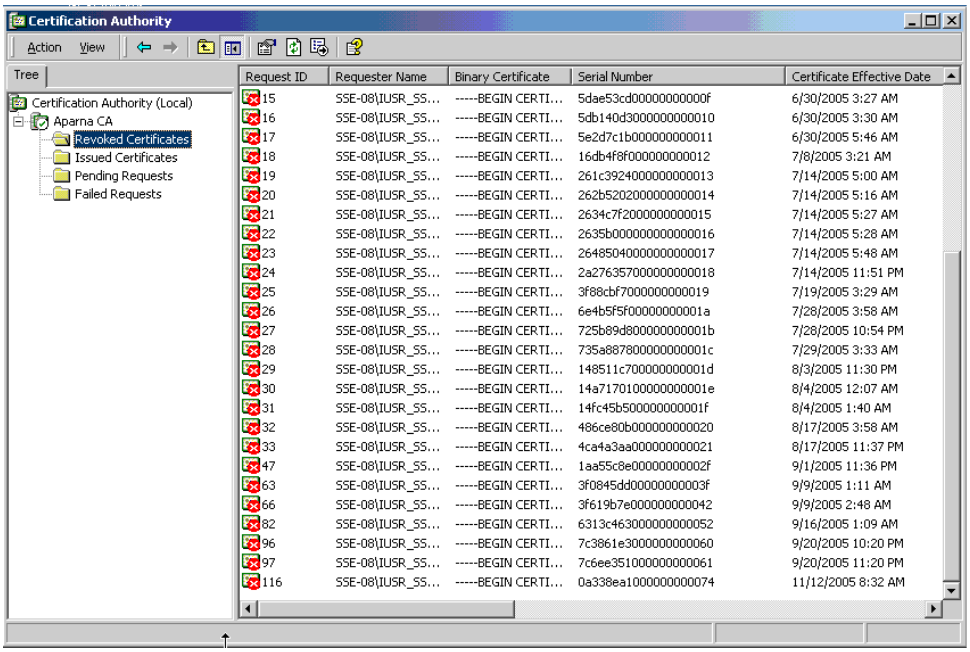
ステップ 2　[All Tasks] > [Revoke Certificate] を選択します。



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。



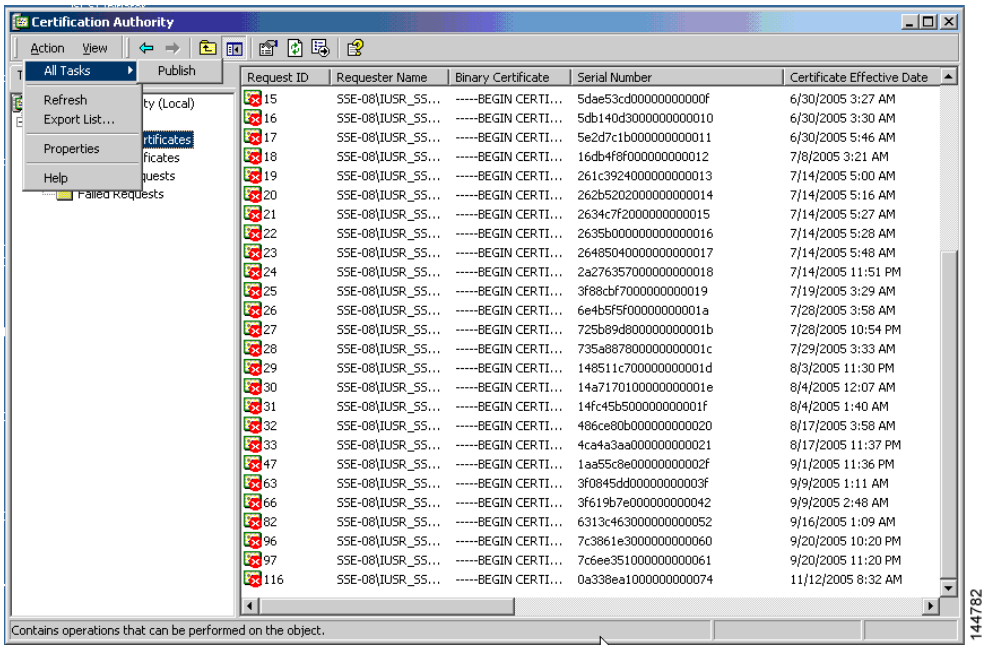
ステップ 4　[Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。



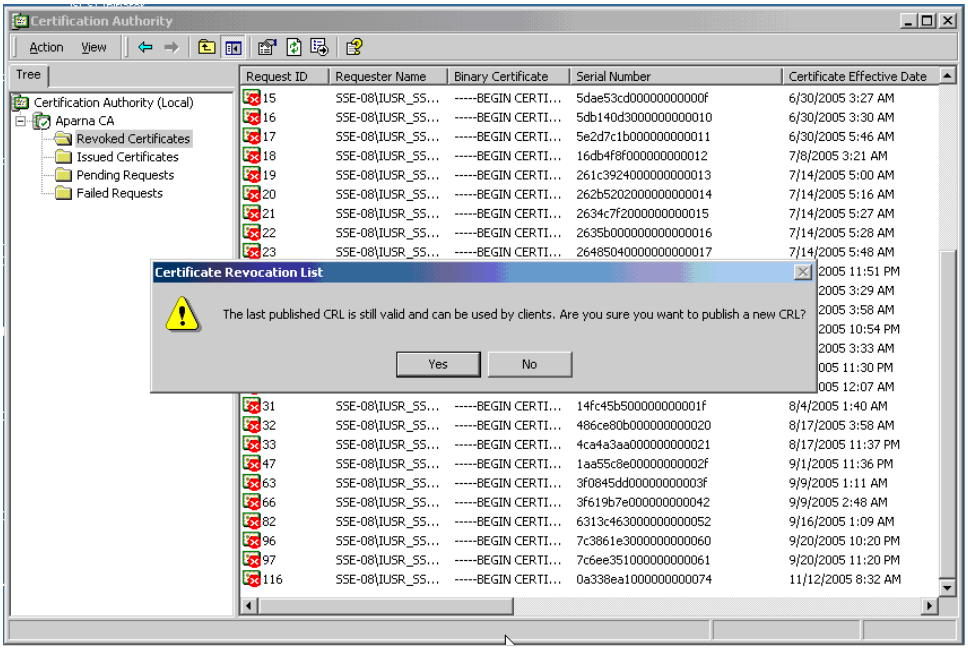
CRL の生成および公開

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。

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



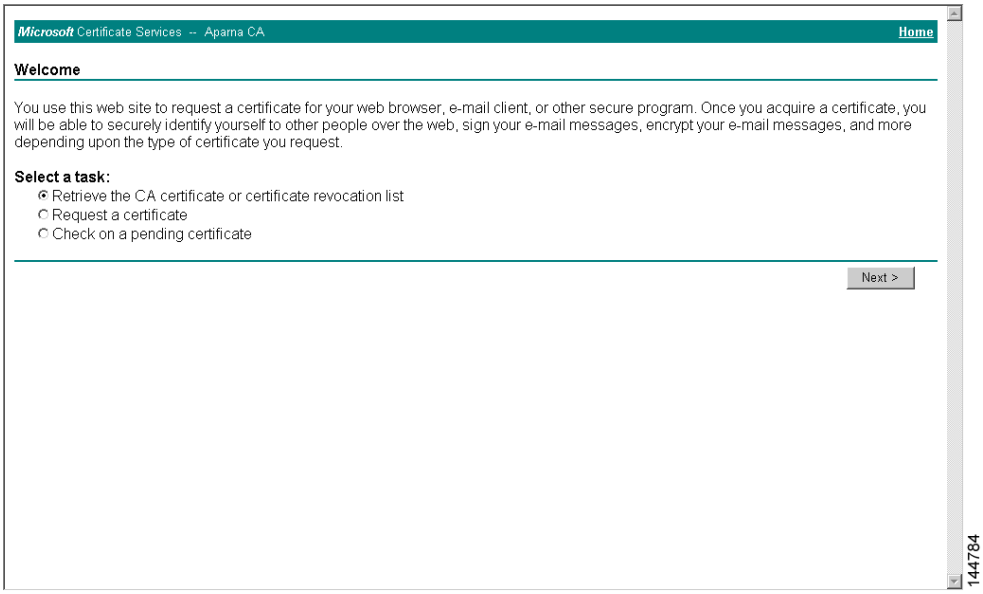
ステップ 2　[Certificate Revocation List] ダイアログボックスで [Yes] をクリックし、最新の CRL を公開します。



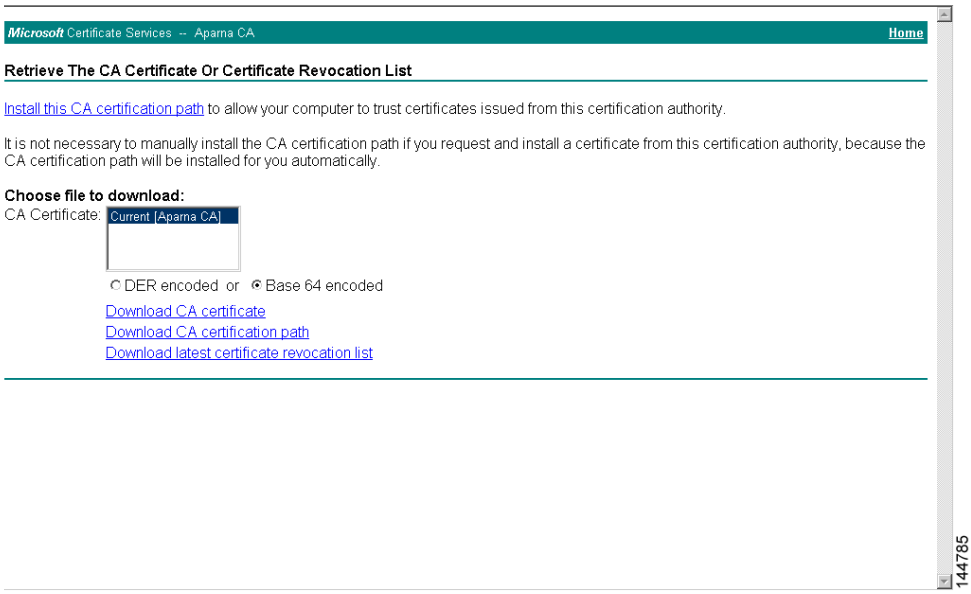
CRL のダウンロード

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。

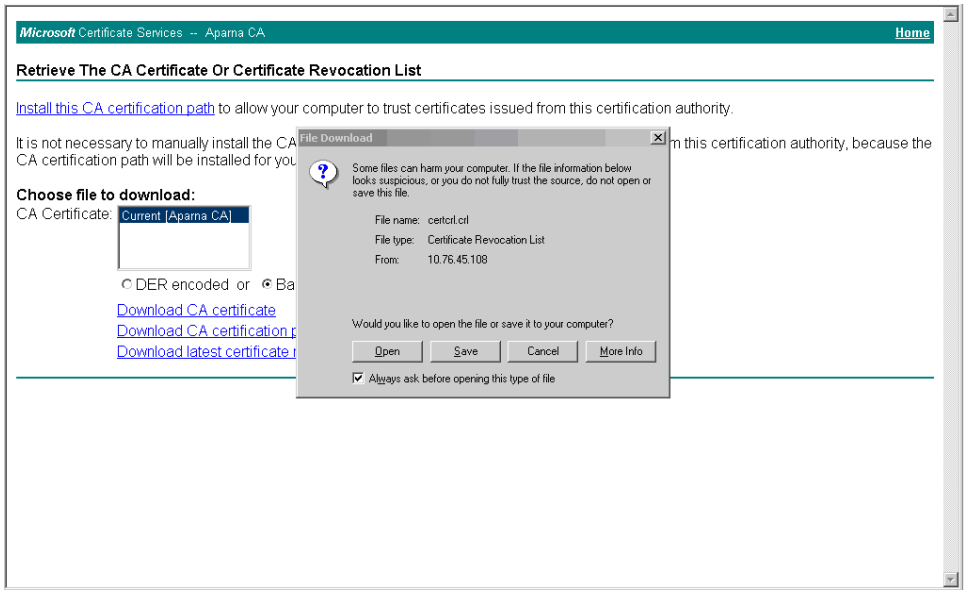
ステップ 1　Microsoft Certificate Services Web インターフェイス上の [Request the CA certificate or certificate revocation list] オプション ボタンを選択し、[Next] ボタンをクリックします。



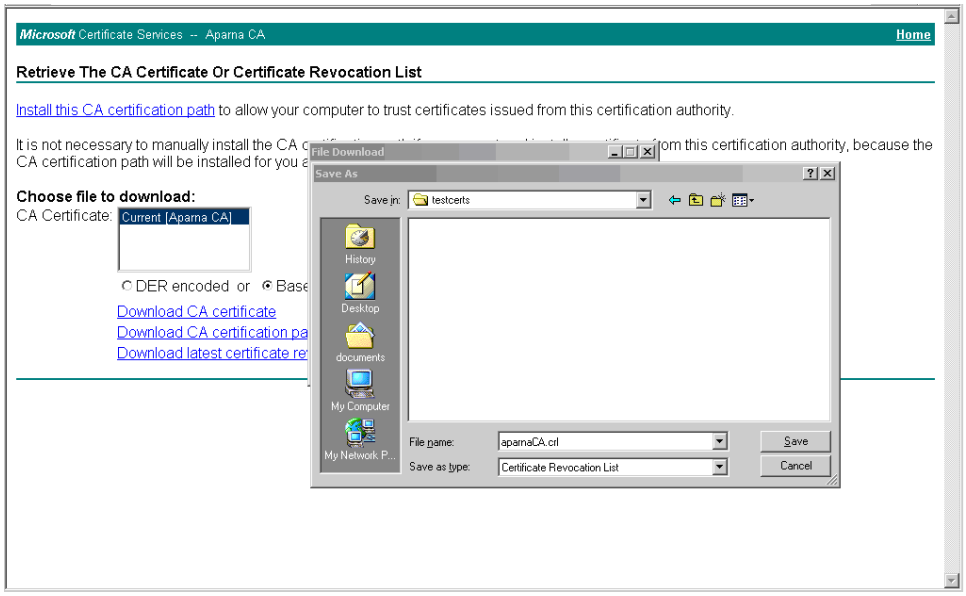
ステップ 2　[Download latest certificate revocation list] リンクをクリックします。



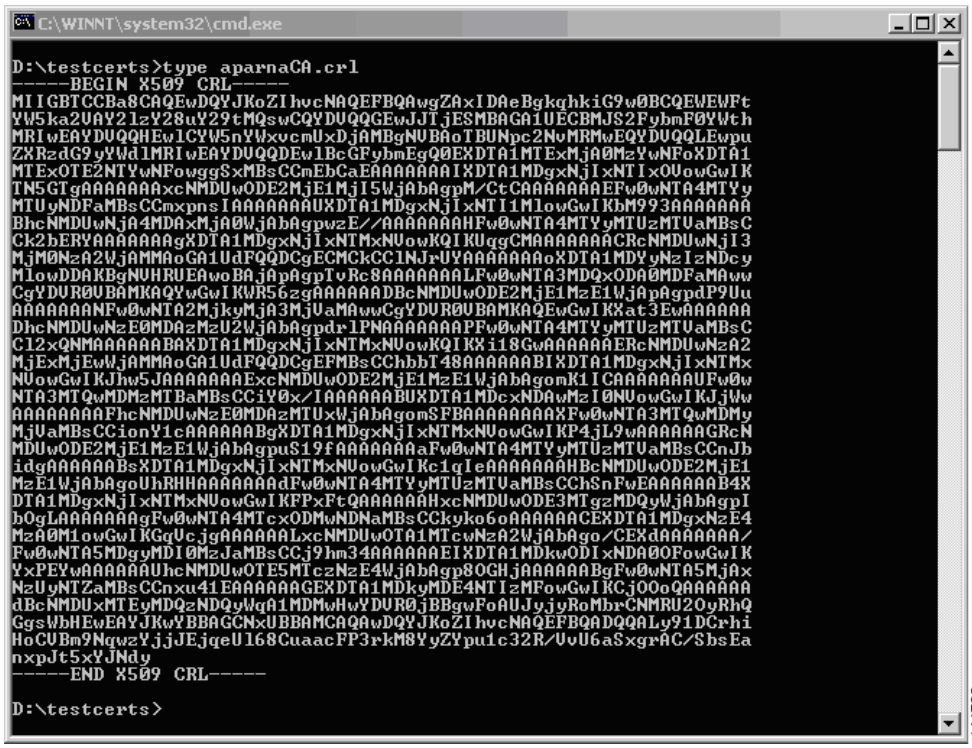
ステップ 3　[File Download] ダイアログボックスで、[Save] をクリックします。



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。



ステップ 5　Microsoft Windows の **type** コマンドを使用して、CRL を表示します。



CRL のインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

ステップ 1　CRL ファイルを MDS スイッチのブートフラッシュにコピーします。

```
Vegas-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl
```

ステップ 2　CRL を設定します。

```
Vegas-1# config terminal
Vegas-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Vegas-1(config)#
```

ステップ 3　CRL の内容を表示します。

```
Vegas-1(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: 52A802300000000000009
        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 0:33:56 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 0:32:45 2005 GMT
    Serial Number: 2635B000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 26485040000000000017
        Revocation Date: Jul 14 0:32:25 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
```

(注)　失効しているスイッチのアイデンティティ証明書（シリアル番号 0A338EA1000000000074）は、最後にリストされます。

最大限度

表 6-1 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。

表 6-1　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
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

表 6-2 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。

表 6-2　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	512
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