ワイヤレス LAN コントローラでの EAP-FAST および LDAP サーバを使用したローカル EAP 認証の設定例

内容

概要

このドキュメントでは、Wireless LAN Controller（WLC）での Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST) Local EAP 認証の設定方法を説明します。また、ユーザ クレデンシャルを受信しユーザを認証するために Lightweight Directory Access Protocol（LDAP）サーバをローカル EAP のバックエンド データベースとして設定する方法も説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア 4.2 が稼働している Cisco 4400 シリーズ WLC
- Cisco Aironet 1232AG シリーズ Lightweight アクセス ポイント（LAP）
- Microsoft Windows 2003 サーバ（ドメイン コントローラとして設定）、LDAP サーバ（認証局サーバとして設定）
- ファームウェア リリース 4.2 が稼働する Cisco Aironet 802.11a/b/g クライアント アダプタ
- ファームウェア バージョン 4.2 が稼働する Cisco Aironet Desktop Utility（ADU）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ワイヤレス LAN コントローラのローカル EAP 認証は、ワイヤレス LAN コントローラ バージョン 4.1.171.0 で導入されました。

ローカル EAP 認証方法を使用すると、ユーザとワイヤレス クライアントをコントローラでローカルに認証できます。この機能は、バックエンド システムが中断したり外部認証サーバが停止したりした場合でもワイヤレス クライアントとの接続を維持する必要があるリモート オフィスでの使用を想定して作られています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバへの依存が排除されます。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザのクレデンシャルを取得してユーザを認証します。ローカル EAP では、コントローラとワイヤレス クライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式がサポートされます。

ローカル EAP は、ユーザのクレデンシャルを取得する際にバックエンド データベースとして LDAP を使用する場合があります。

LDAP バックエンド データベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）を LDAP サーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。

LDAP バックエンド データベースでは次のローカル EAP 方式がサポートされています。

- EAP-FAST/GTC

- EAP-TLS
- PEAPv1/GTC

LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、**平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます**。たとえば、Microsoft Active Directory は、平文のパスワードを返さないため、サポートされません。平文のパスワードを返すように LDAP サーバを設定できない場合、LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 はサポートされません。

注：コントローラにRADIUSサーバが設定されている場合、コントローラは最初にRADIUSサーバを使用してワイヤレスクライアントの認証を試みます。ローカル EAP が試されるのは、RADIUS サーバがタイムアウトしたため、または RADIUS サーバが設定されていないために、RADIUS サーバが検出されない場合のみです。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番目の RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番目の RADIUS サーバを試行し、次に 4 番目の RADIUS サーバ、その次にローカル EAP を試行します。

この例では、WLC のローカル EAP 方式として EAP-FAST を使用します。この WLC は LDAP バックエンド データベースにワイヤレス クライアントのユーザ クレデンシャルを照会するように設定されています。

設定

このドキュメントでは、クライアント側とサーバ側の両方で証明書を使用する EAP-FAST を使用します。このため、**Microsoft 認証局（CA）**サーバを使用してクライアントとサーバの証明書が生成されます。

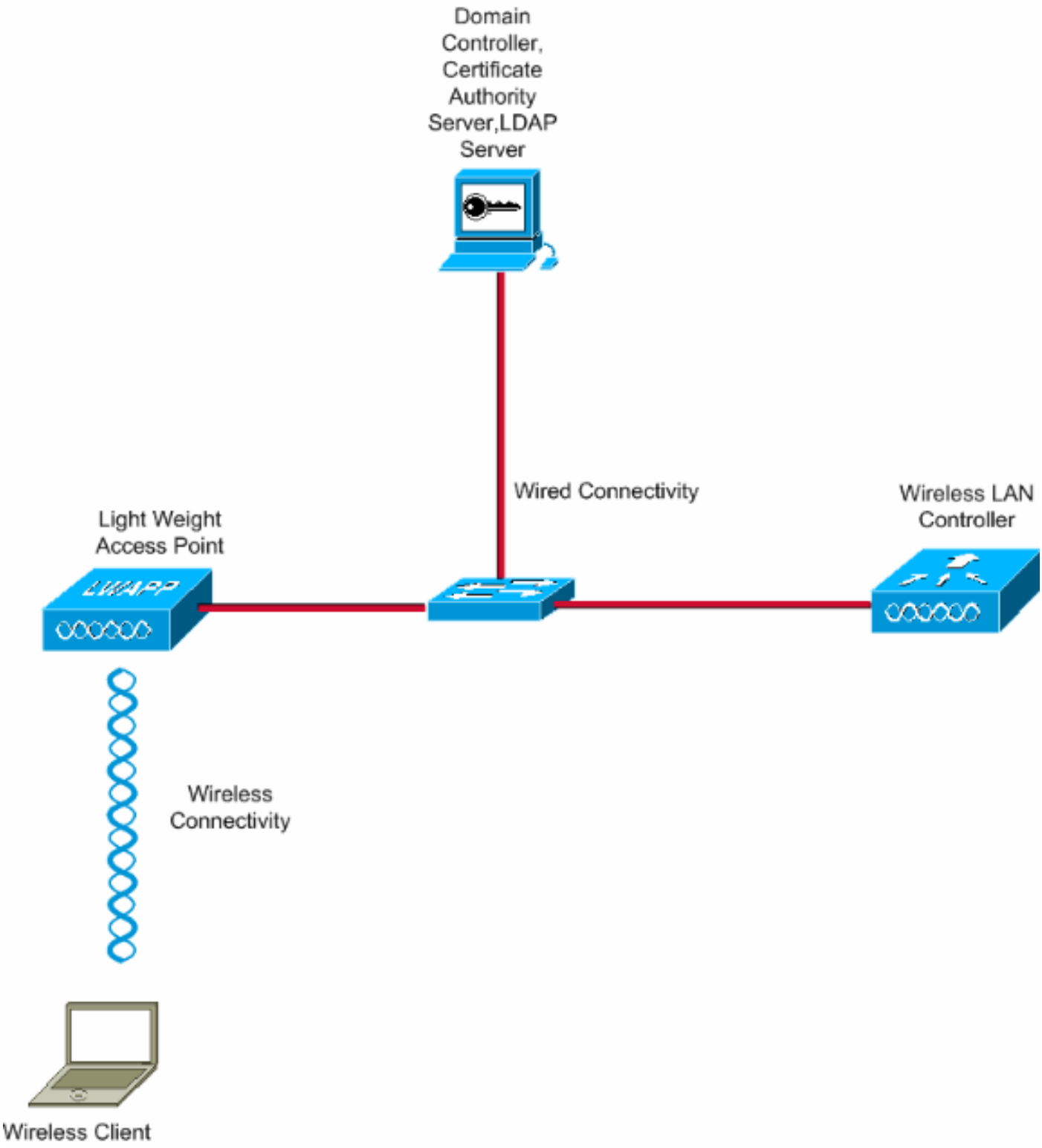
ユーザ クレデンシャルは LDAP サーバに保存されるので、クレデンシャルの検証が正常に完了するとコントローラはユーザ クレデンシャルを取得するため LDAP サーバに対して照会を実行し、ワイヤレス クライアントを認証します。

このドキュメントは次の設定がすでに完了していることを前提としています。

- LAP が WLC に登録されている。必要な登録手順の詳細については、『Lightweight アクセス ポイント（LAP）の無線 LAN コントローラ（WLC）への登録』を参照してください。
- DHCP サーバがワイヤレス クライアントに IP アドレスを割り当てるように設定されている。
- Microsoft Windows 2003 サーバがドメイン コントローラおよび CA サーバとして設定されている。この例ではドメインとして **wireless.com** を使用します。Windows 2003 サーバをドメイン コントローラとして設定する方法の詳細については、『ドメイン コントローラとしての Windows 2003 の設定』を参照してください。Windows 2003 サーバをエンタープライズ CA サーバとして設定するには、『Microsoft Windows 2003 サーバのインストールと認証局（CA）サーバとしての設定』を参照してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

この設定を実装するには、次の作業を実行します。

- WLC でのローカル EAP 認証方式としての EAP-FAST の設定
- LDAP サーバの設定
- ワイヤレス クライアントの設定

WLC でのローカル EAP 認証方式としての EAP-FAST の設定

前述したように、このドキュメントではクライアント側とサーバ側の両方で証明書を使用する EAP-FAST をローカル EAP 認証方式として使用します。最初に次の証明書をサーバ（この場合は WLC）とクライアントにダウンロードしてインストールします。

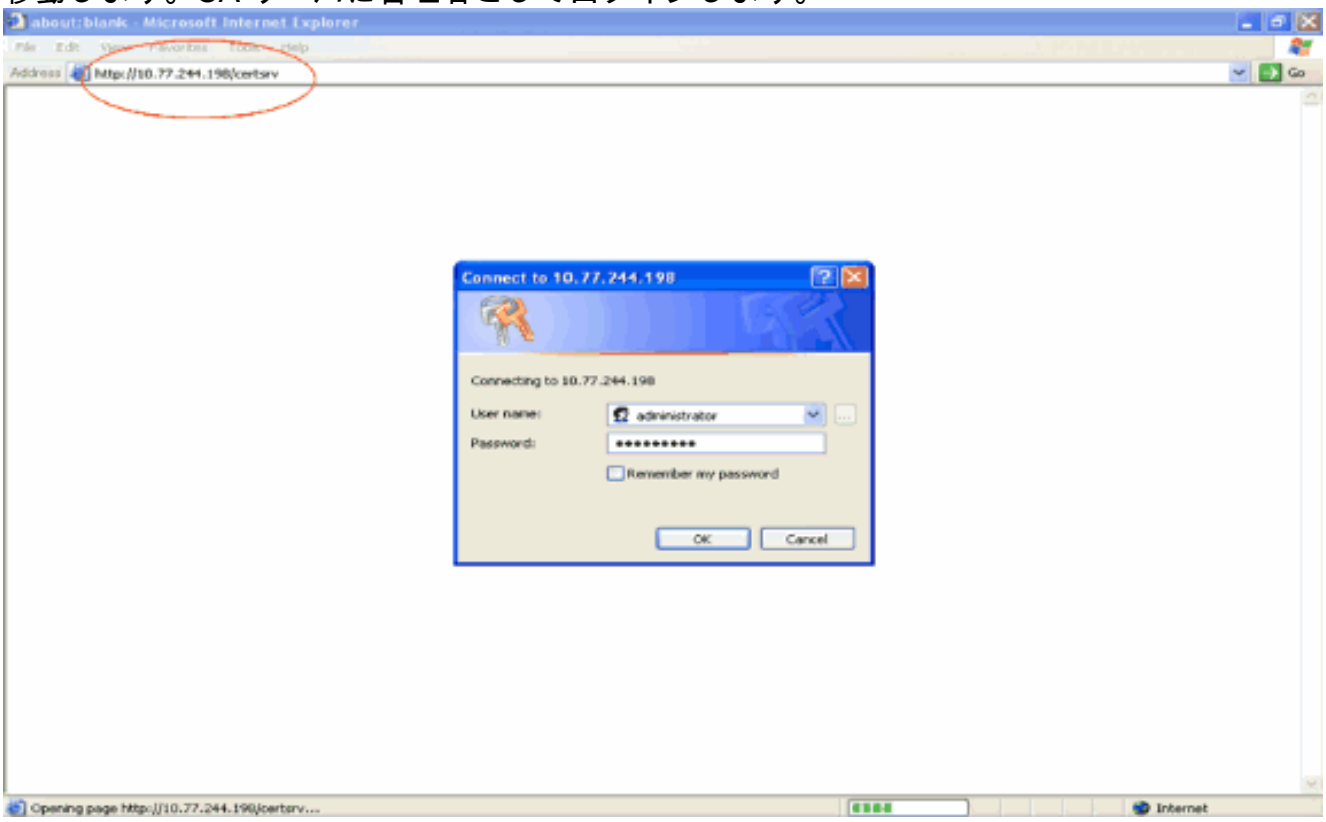
WLC とクライアントでそれぞれ CA サーバからこれらの証明書をダウンロードする必要があります。

- デバイス証明書（WLC とクライアントそれぞれに 1 つずつ）
- 公開キー インフラストラクチャ（PKI）のルート証明書（WLC）と CA 証明書（クライアント）

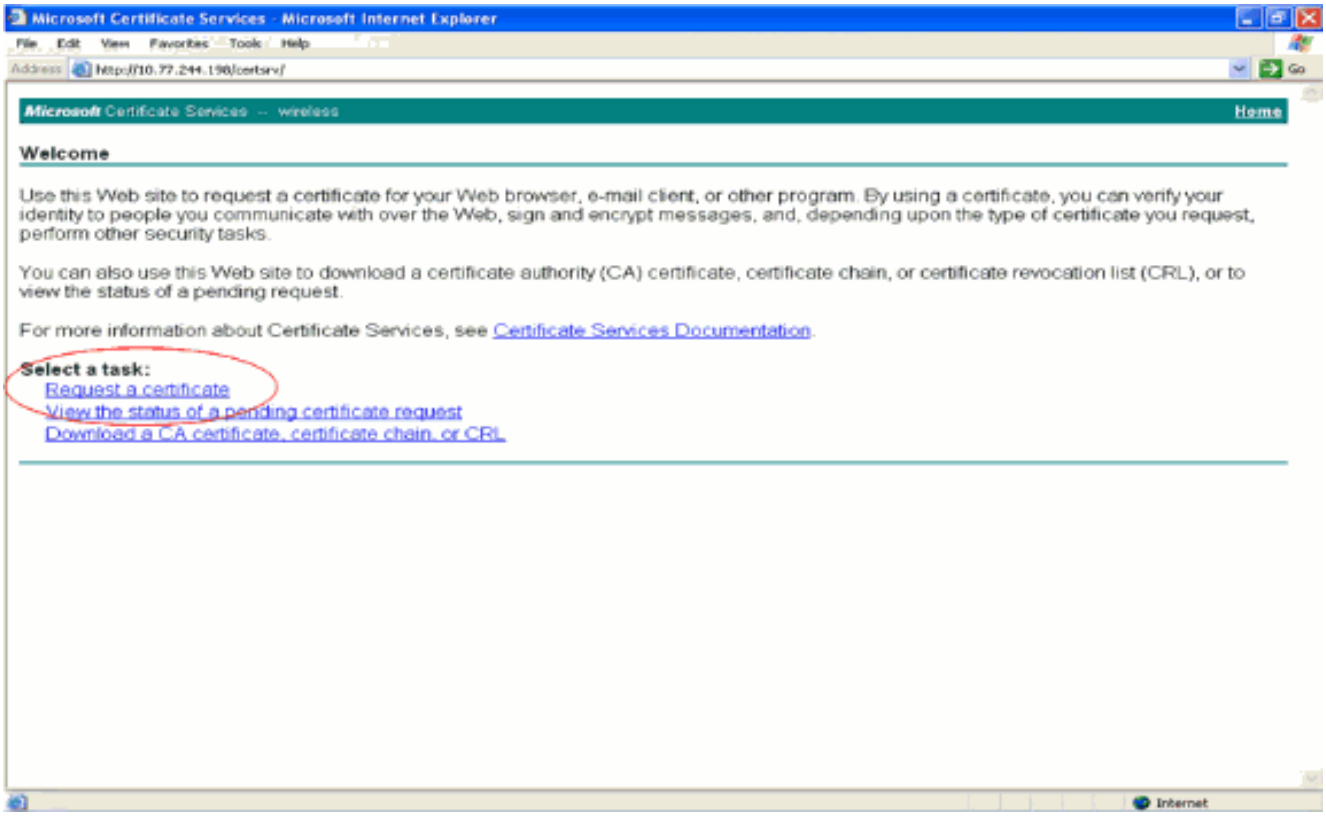
WLC のデバイス証明書の生成

CA サーバから WLC のデバイス証明書を生成するには、次の手順を実行します。このデバイス証明書は、WLC がクライアントを認証するときに使用します。

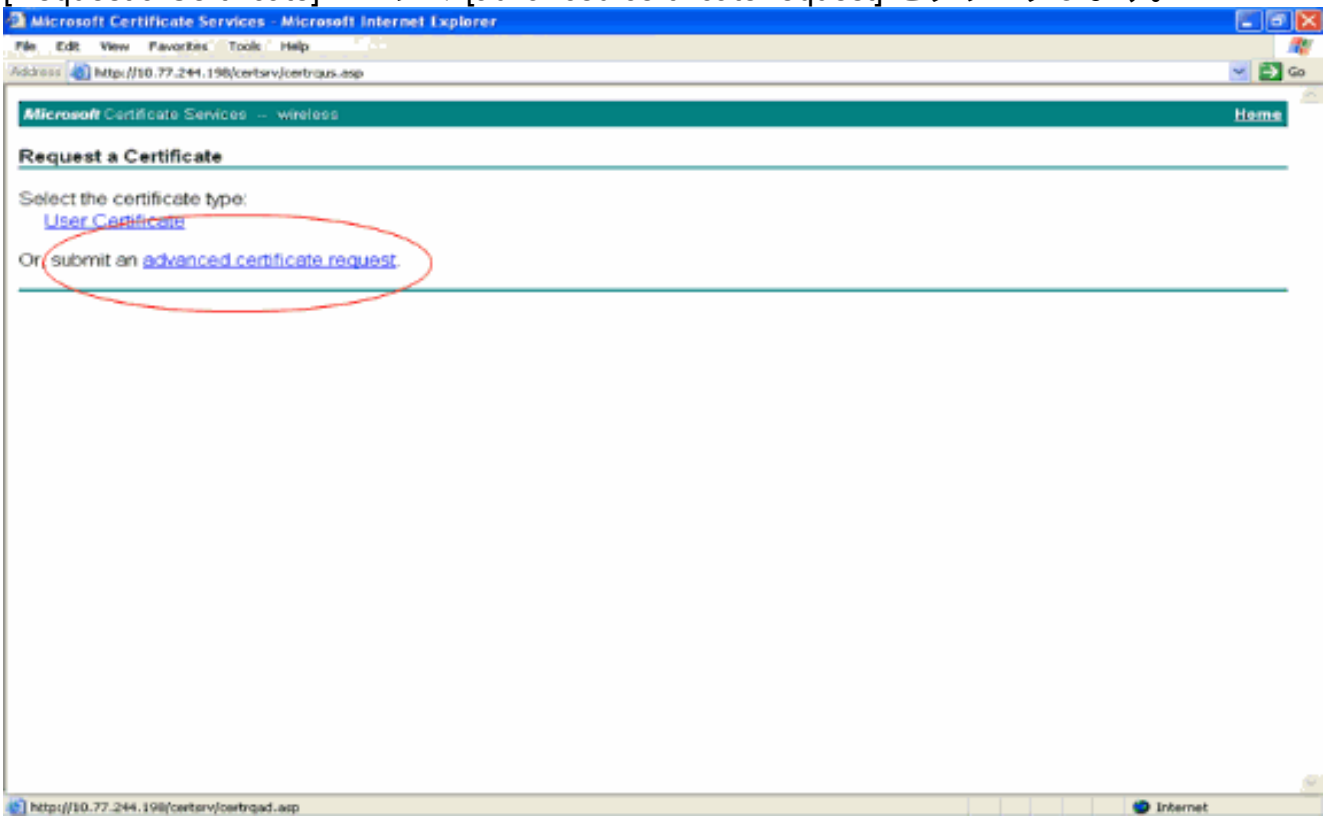
1. CA サーバにネットワーク接続している PC で、**http://<CA サーバの IP アドレス>/certsrv** に移動します。CA サーバに管理者としてログインします。



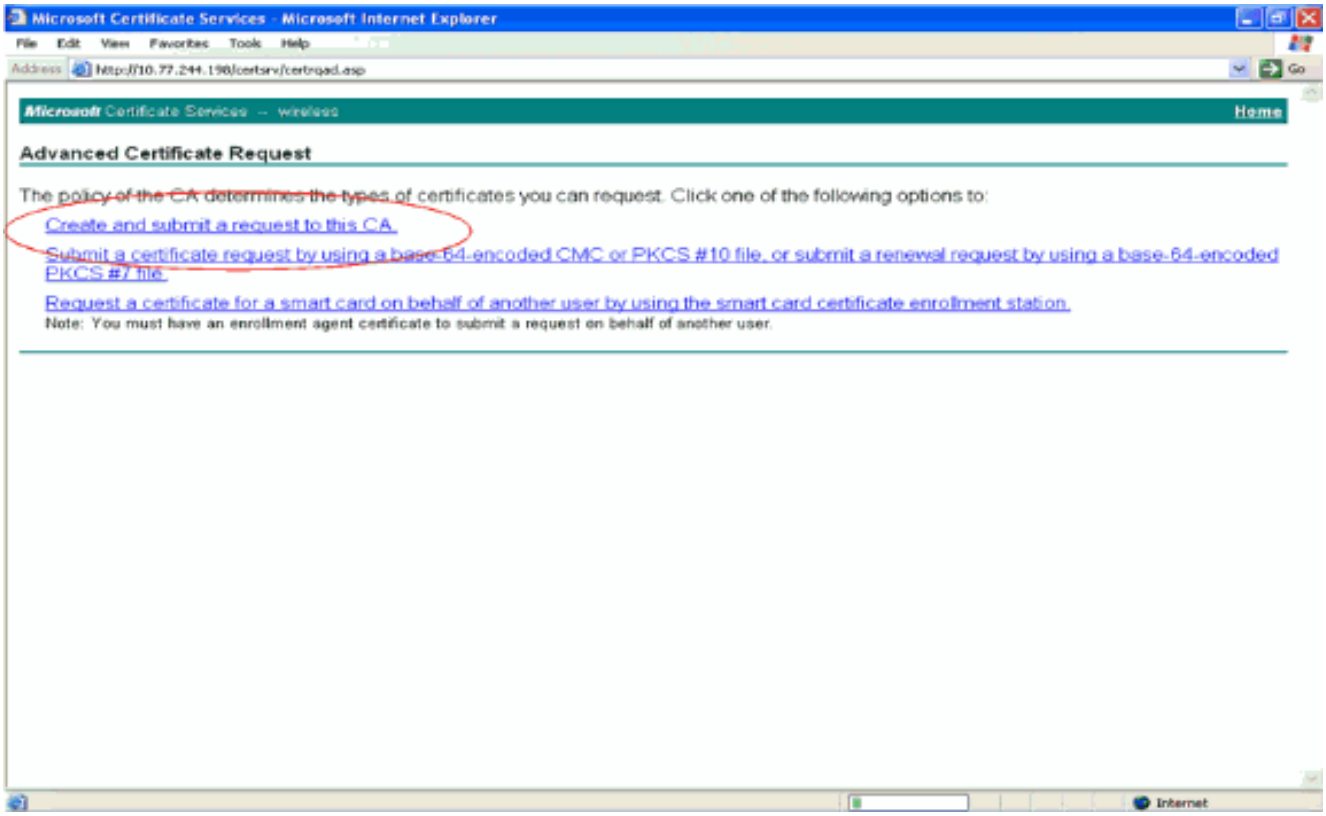
2. [Request a certificate] を選択します。



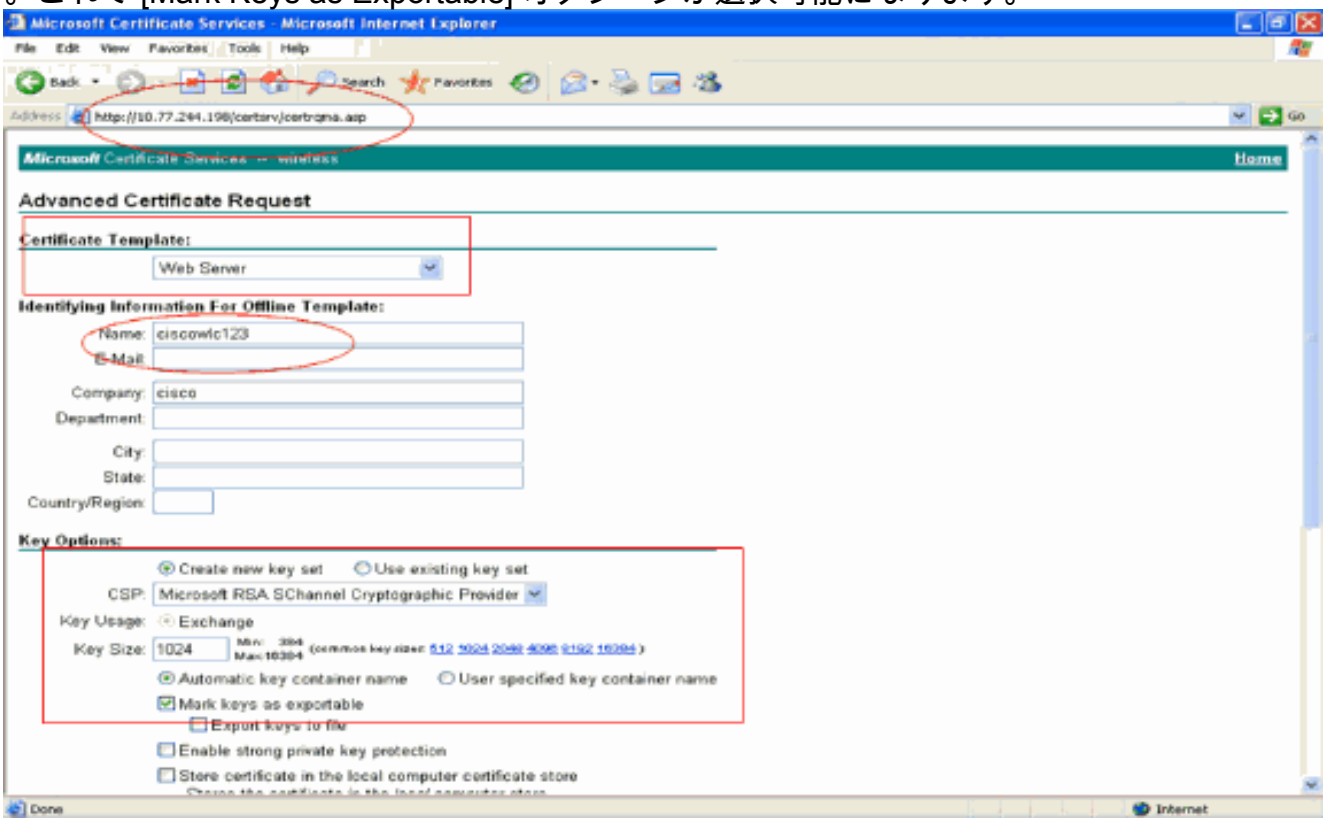
3. [Request a Certificate] ページで [advanced certificate request] をクリックします。



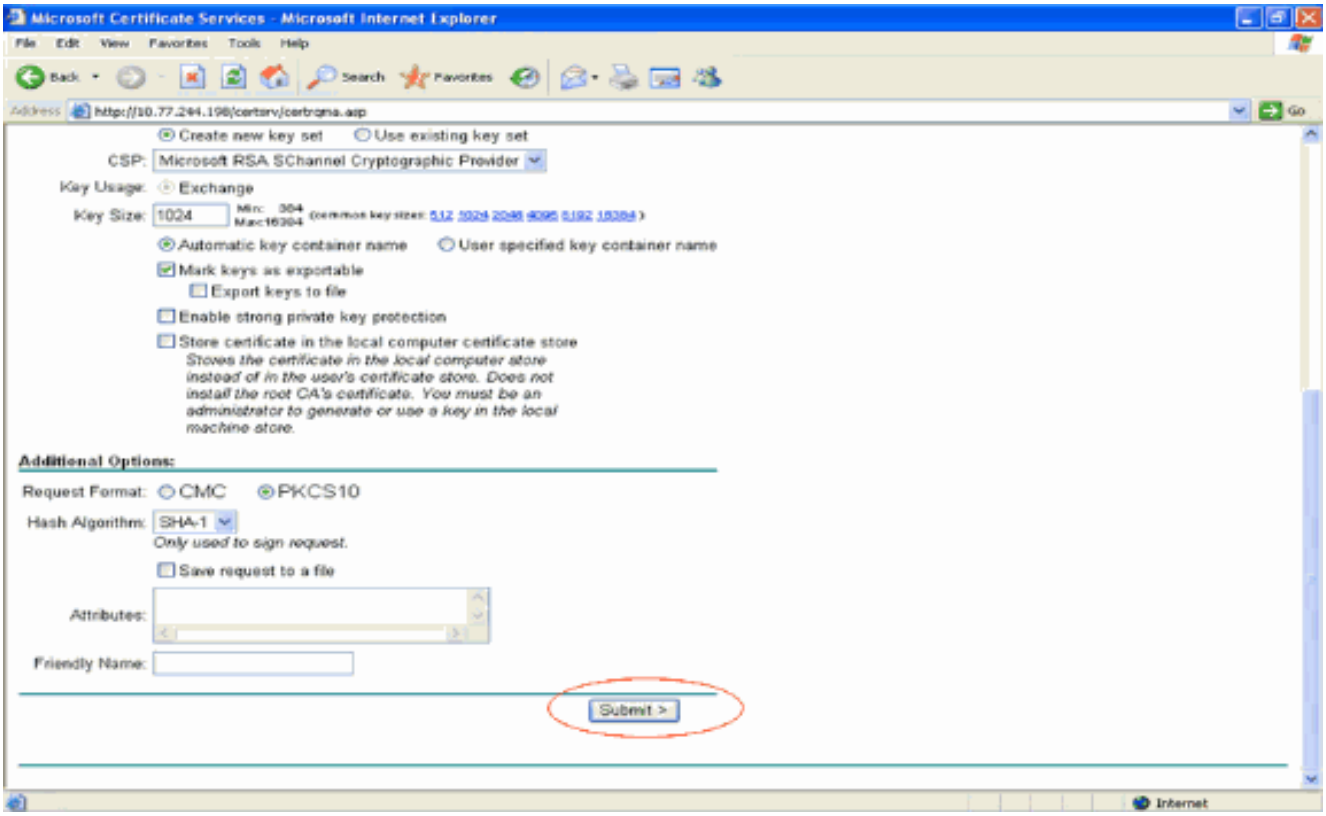
4. [Advanced Certificate Request] ページで [Create and submit a request to this CA] をクリックします。[Advanced Certificate Request] フォームが表示されます。



5. [Advanced Certificate Request] フォームの [Certificate Template] で [Web Server] を選択します。次に、このデバイス証明書の名前を指定します。この例では証明書名 ciscowlc123 を使用します。要件に基づいてその他の識別情報を入力します。
6. [Key Options] セクションで [Mark Keys as Exportable] オプションを選択します。場合によっては、Web サーバ テンプレートを選択するときにこのオプションがグレー表示になっており、このオプションを有効または無効にできないことがあります。このような場合はブラウザ メニューで [Back] をクリックして前のページに戻ってからこのページに再度進みます。これで [Mark Keys as Exportable] オプションが選択可能になります。

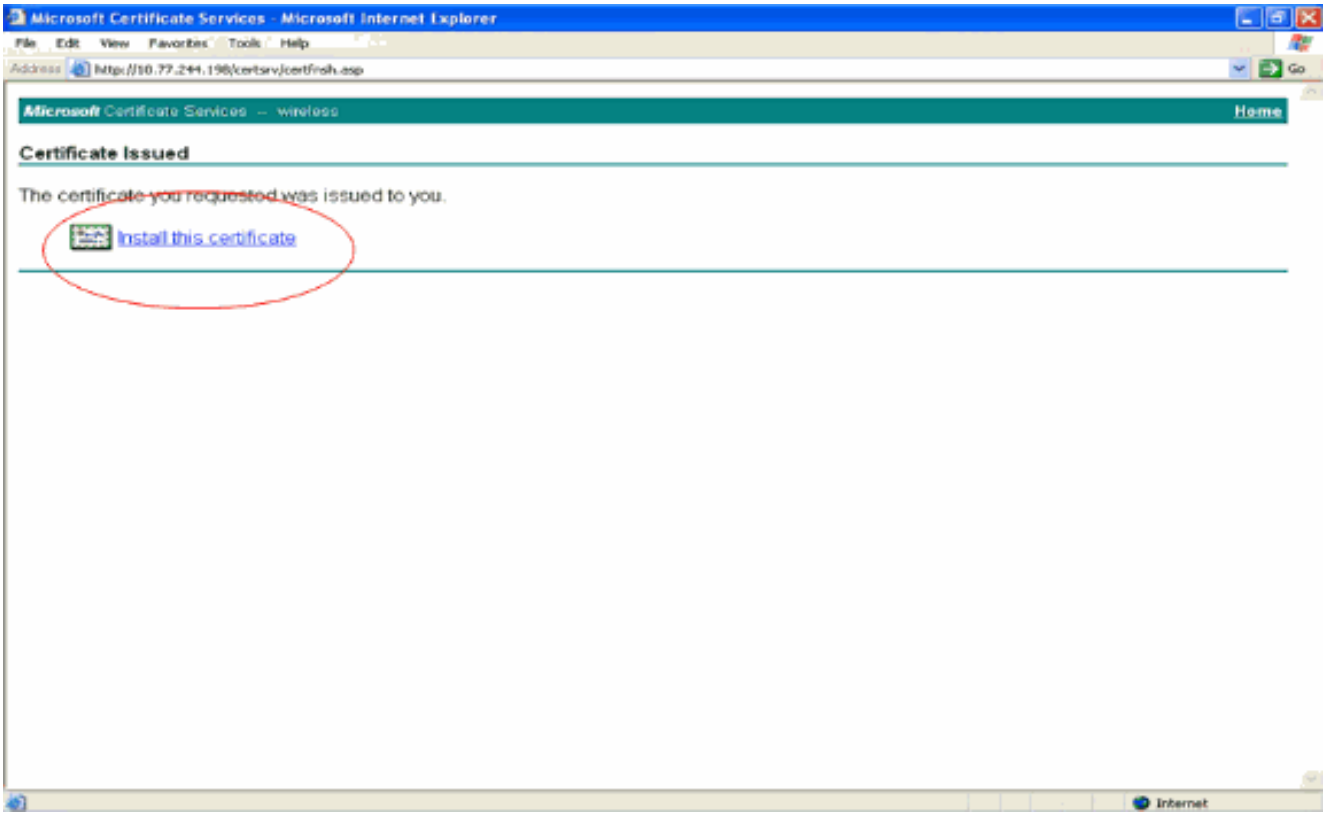


7. その他の必須フィールドをすべて設定して [Submit] をクリックします。

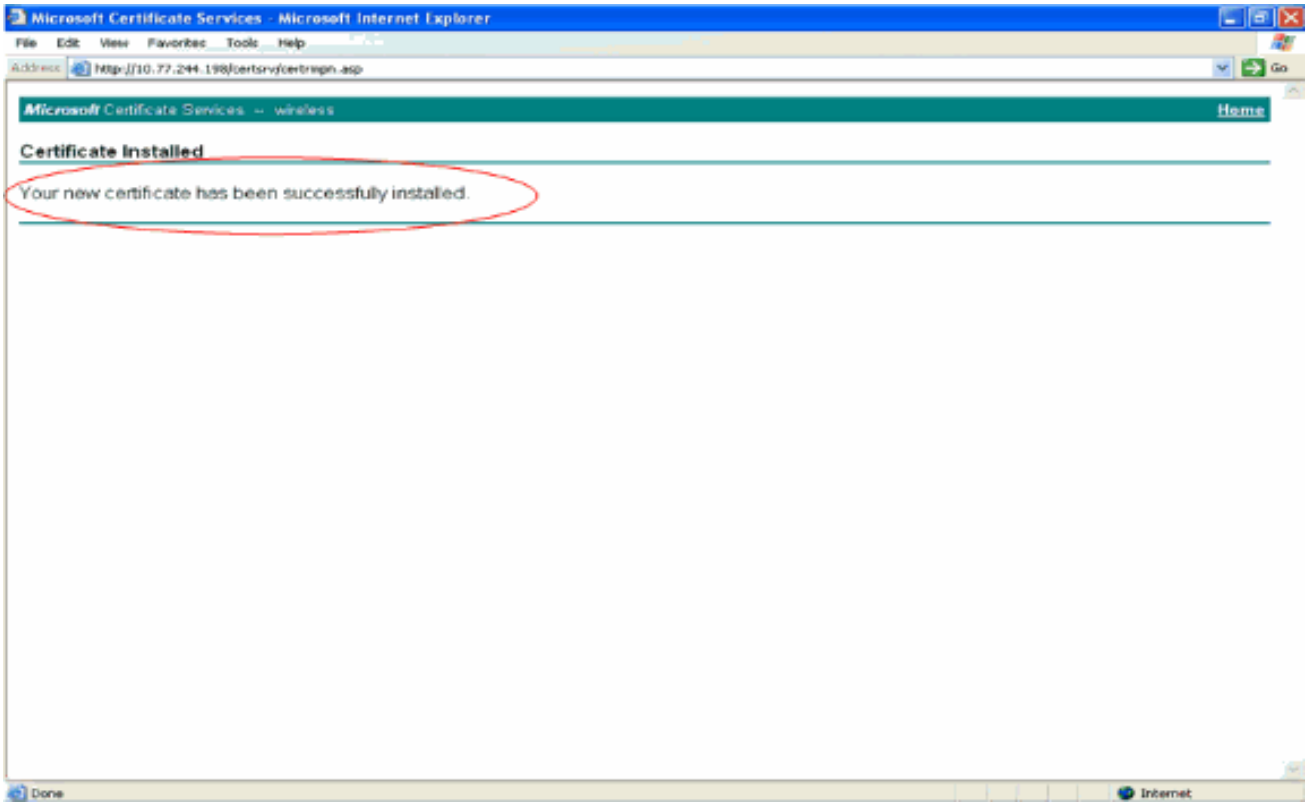


8. 証明書要求プロセスを許可するため、次に表示されるウィンドウで [Yes] をクリックします。

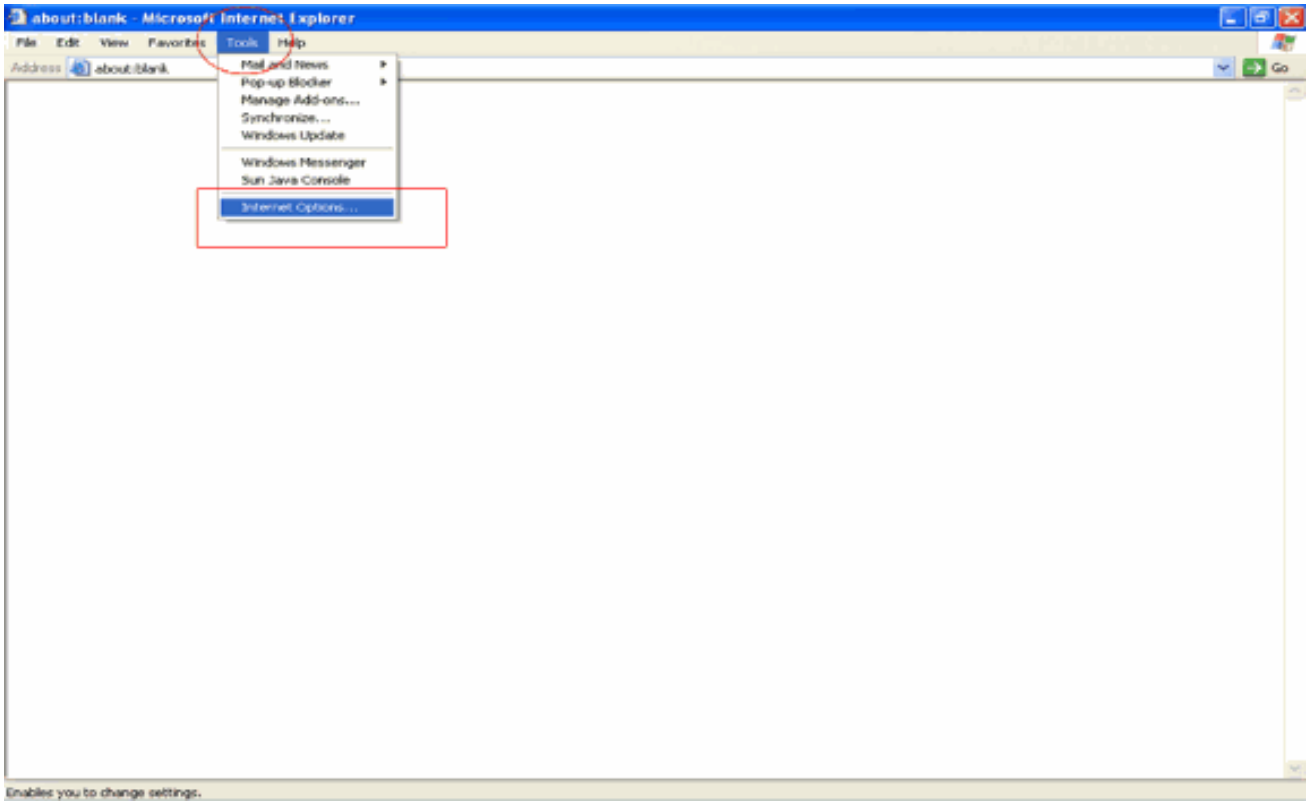
9. [Certificate Issued] ウィンドウが表示され、証明書要求プロセスが正常に完了したことが示されます。次に、発行された証明書をこの PC の証明書ストアにインストールします。[Install this certificate] をクリックします。



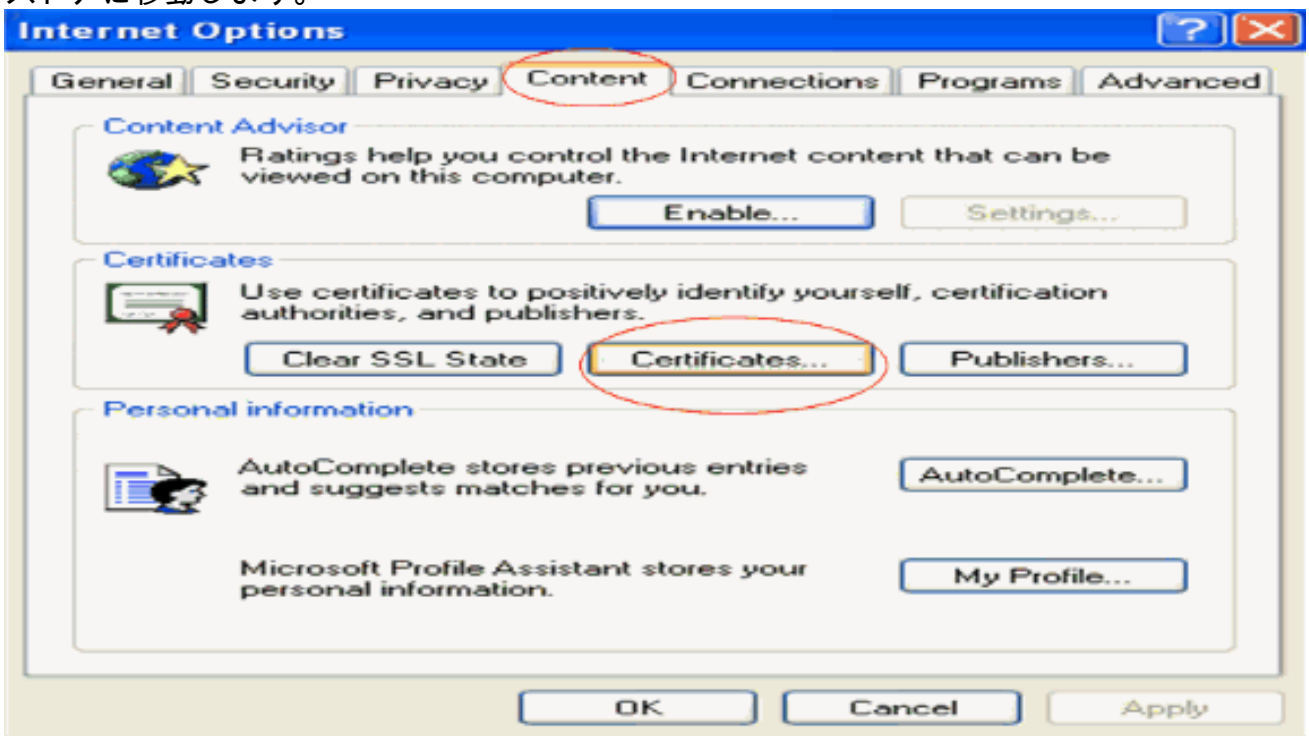
10. CA サーバへの要求が生成された PC に新しい証明書が正常にインストールされました。



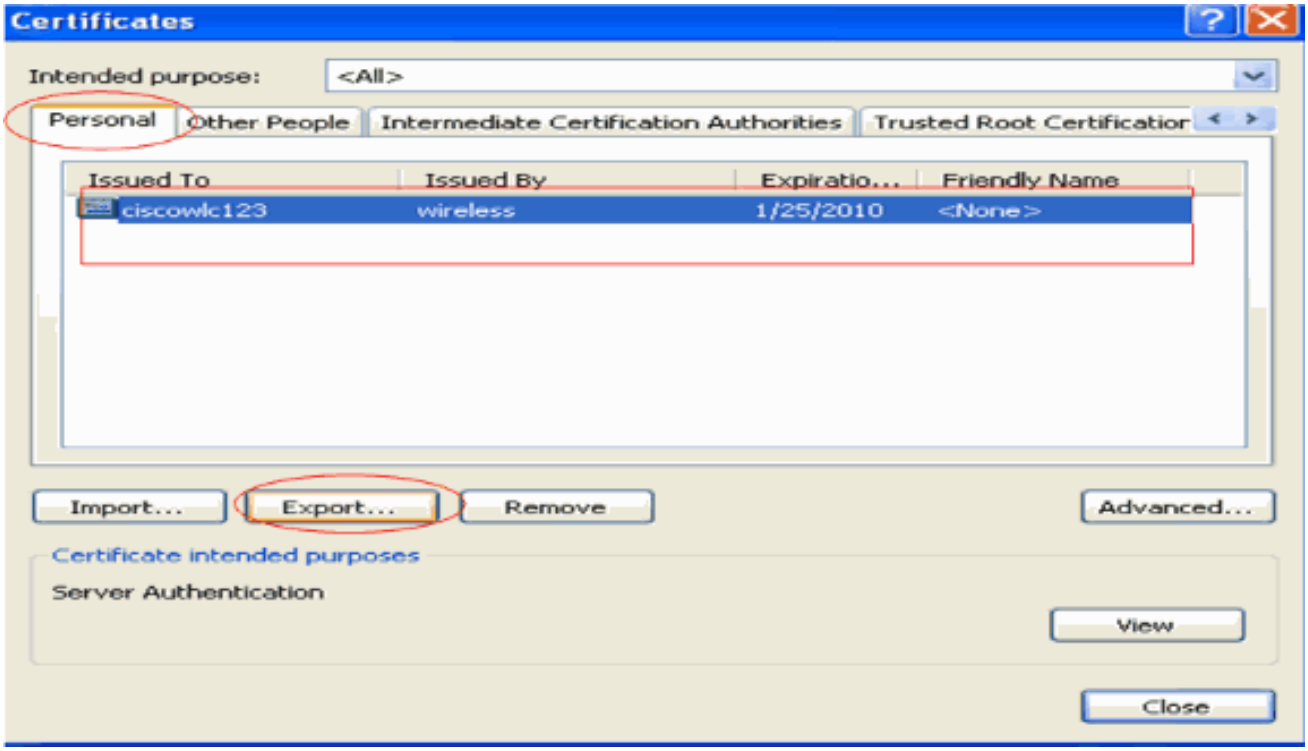
11. 次に、証明書ストアからこの証明書をファイルとしてハードディスクにエクスポートします。この証明書ファイルは後で WLC に証明書をダウンロードするために使用されます。証明書ストアから証明書をエクスポートするには、Internet Explorer ブラウザを開いて [Tools] > [Internet Options] をクリックします。



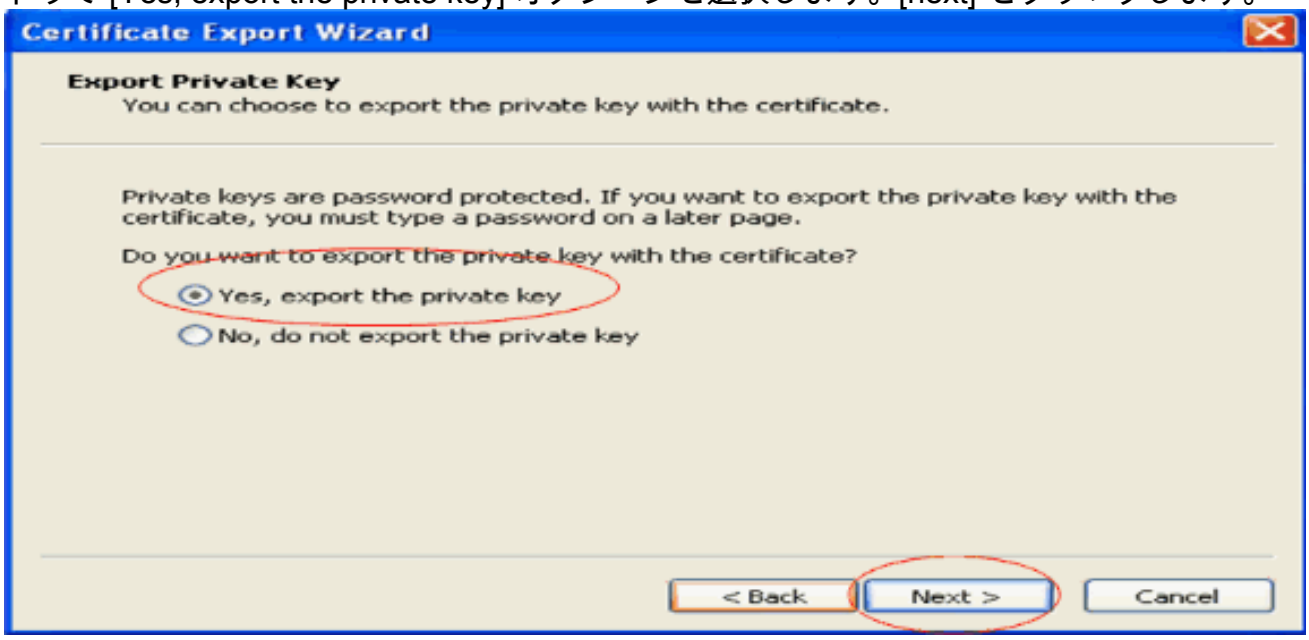
12. [Content] > [Certificates] をクリックし、証明書がデフォルトでインストールされる証明書ストアに移動します。



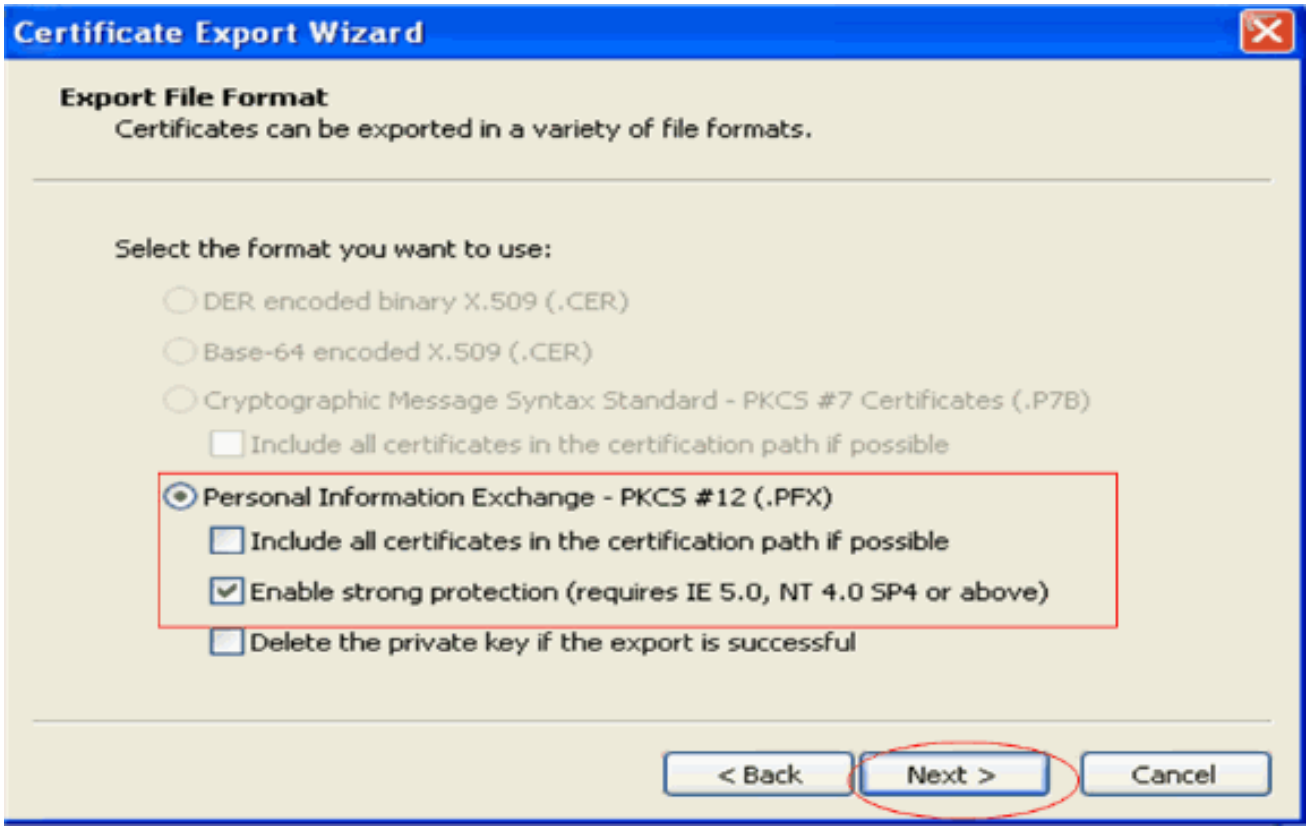
13. デバイス証明書は通常 [Personal] 証明書リストにインストールされます。新たにインストールした証明書がこのリストに表示されます。証明書を選択して [Export] をクリックします。



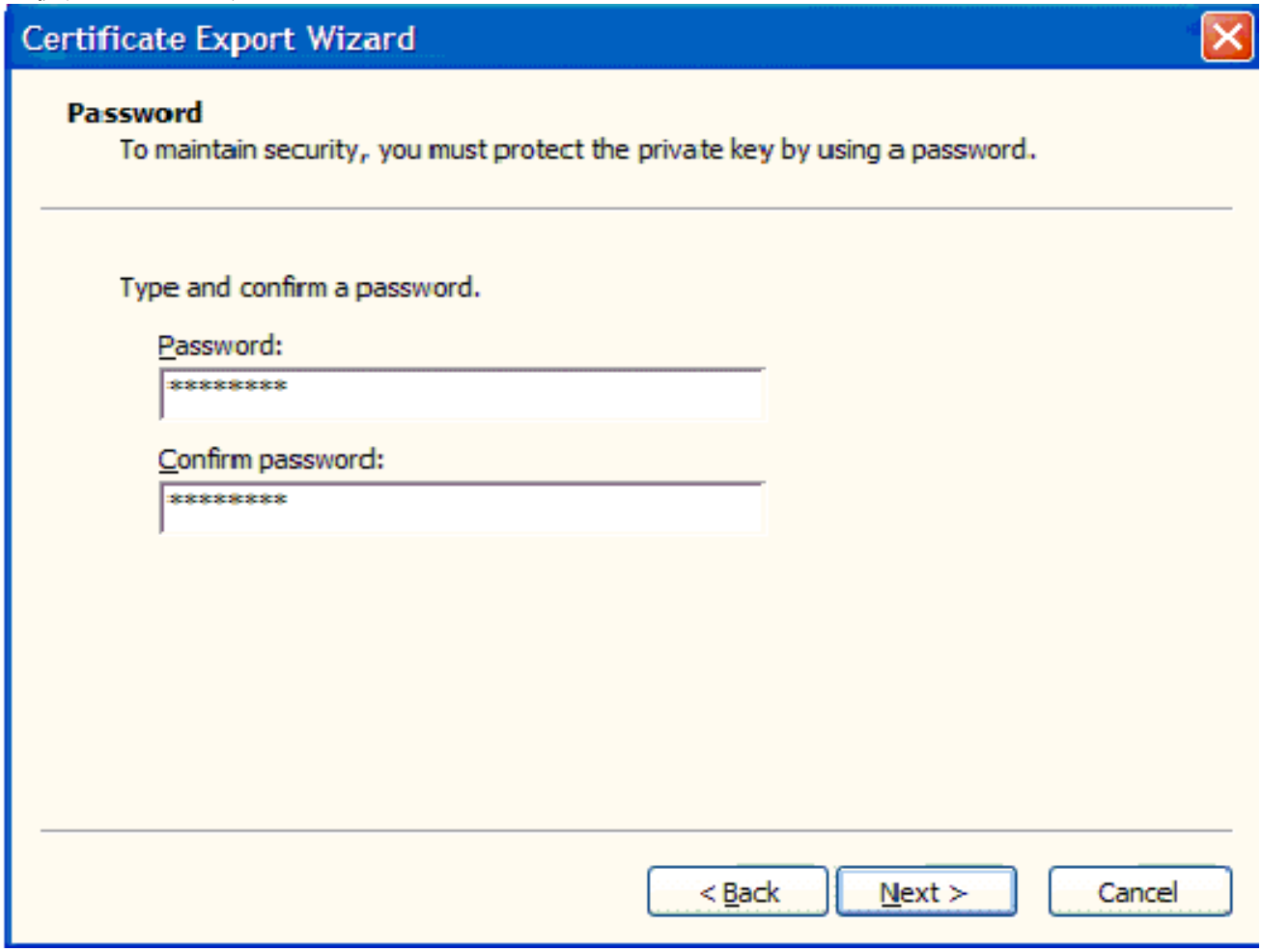
14. 次に表示されるウィンドウで [Next] をクリックします。[Certificate Export Wizard] ウィンドウで [Yes, export the private key] オプションを選択します。[next] をクリックします。



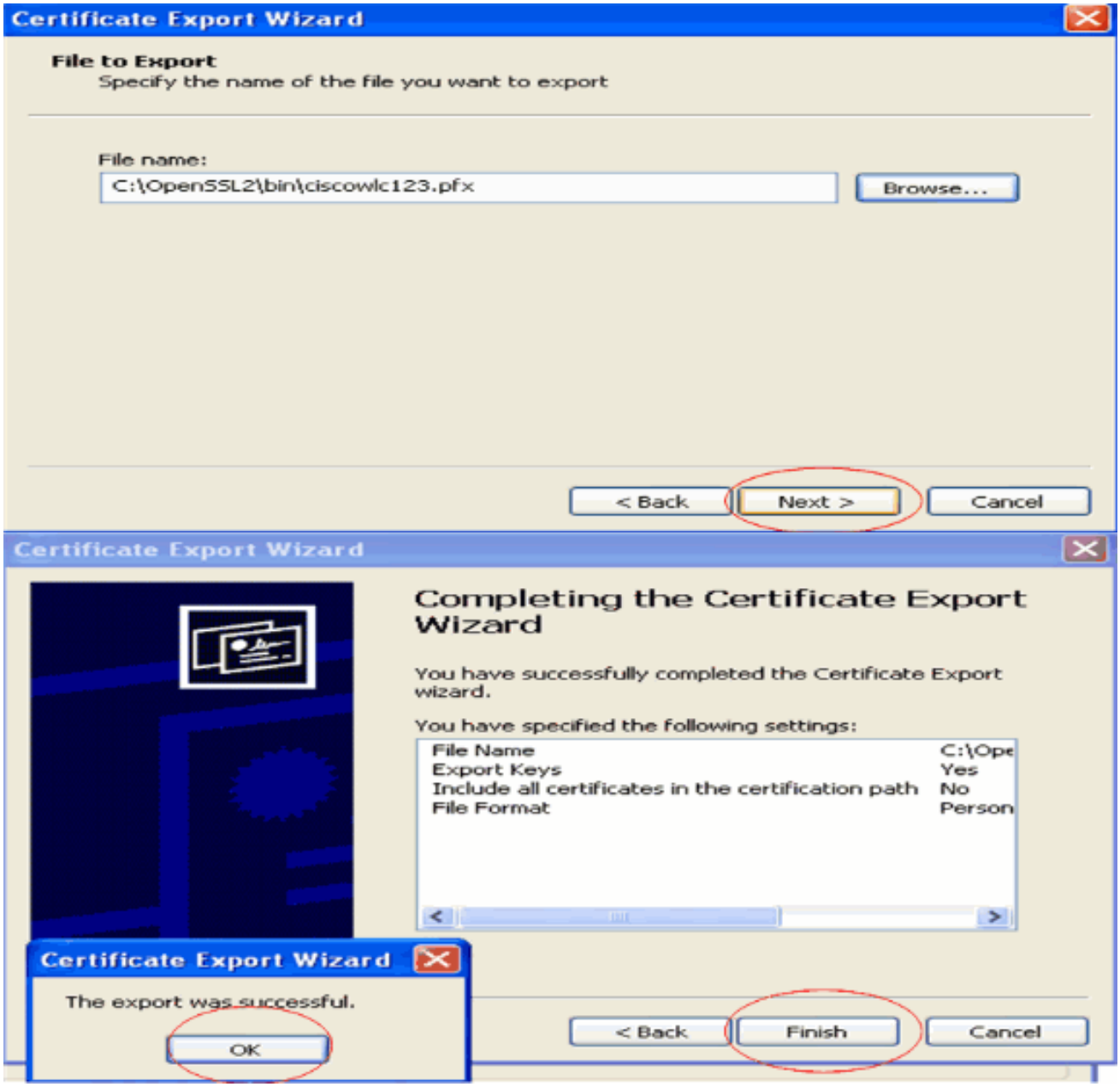
15. エクスポート ファイル フォーマットとして [.PFX] を選択し、[Enable strong protection] オプションを選択します。[next] をクリックします。



16. [Password] ウィンドウにパスワードを入力します。この例では、パスワードとして **cisco** を使用しています。



17. 証明書ファイル（.PFX ファイル）をハード ディスクに保存します。[Next] をクリックしてエクスポート プロセスを完了します。



WLC へのデバイス証明書のダウンロード

WLC デバイス証明書が .PFX ファイルとして作成されました。次に、このファイルをコントローラにダウンロードします。Cisco WLC は PEM フォーマットの証明書だけを受け入れます。したがって、最初に openSSL プログラムを使用して .PFX または PKCS12 フォーマットのファイルを PEM ファイルに変換する必要があります。

openSSL プログラムを使用した PFX 証明書から PEM フォーマットへの変換

証明書を PEM フォーマットに変換する openSSL がインストールされている PC に証明書をコピーできます。openSSL プログラムの bin フォルダで openssl.exe ファイルの次のコマンドを入力します。

注：openSSLはOpenSSL Webサイトからダウンロードできます。

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
```

```
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco
```

証明書ファイルが PEM フォーマットに変換されます。次に、PEM フォーマットのデバイス証明書を WLC にダウンロードします。

注：その前に、PEMファイルのダウンロード元となるPCにTFTPサーバソフトウェアが必要です。この PC は WLC に接続している必要があります。TFTP サーバの現行ベース ディレクトリが、PEM ファイルが保存されるロケーションとして指定されている必要があります。

WLC への変換後の PEM フォーマット デバイス証明書のダウンロード

この例では、WLC の CLI を使用したダウンロード プロセスについて説明します。

1. コントローラの CLI にログインします。
2. **transfer download datatype eapdevcert** コマンドを入力します。
3. **transfer download serverip 10.77.244.196 コマンドを入力します。**10.77.244.196 が TFTP サーバの IP アドレスです。
4. **transfer download filename ciscowlc.pem コマンドを入力します。**ciscowlc123.pem はこの例で使用されるファイル名です。
5. 証明書のパスワードを設定するため **transfer download certpassword** コマンドを入力します。
6. **transfer download start** コマンドを入力して更新後の設定を確認します。現在の設定を確認してダウンロード プロセスを開始するプロンプトが表示されたら、**y** と答えます。このダウンロード コマンドの出力例を次に示します。

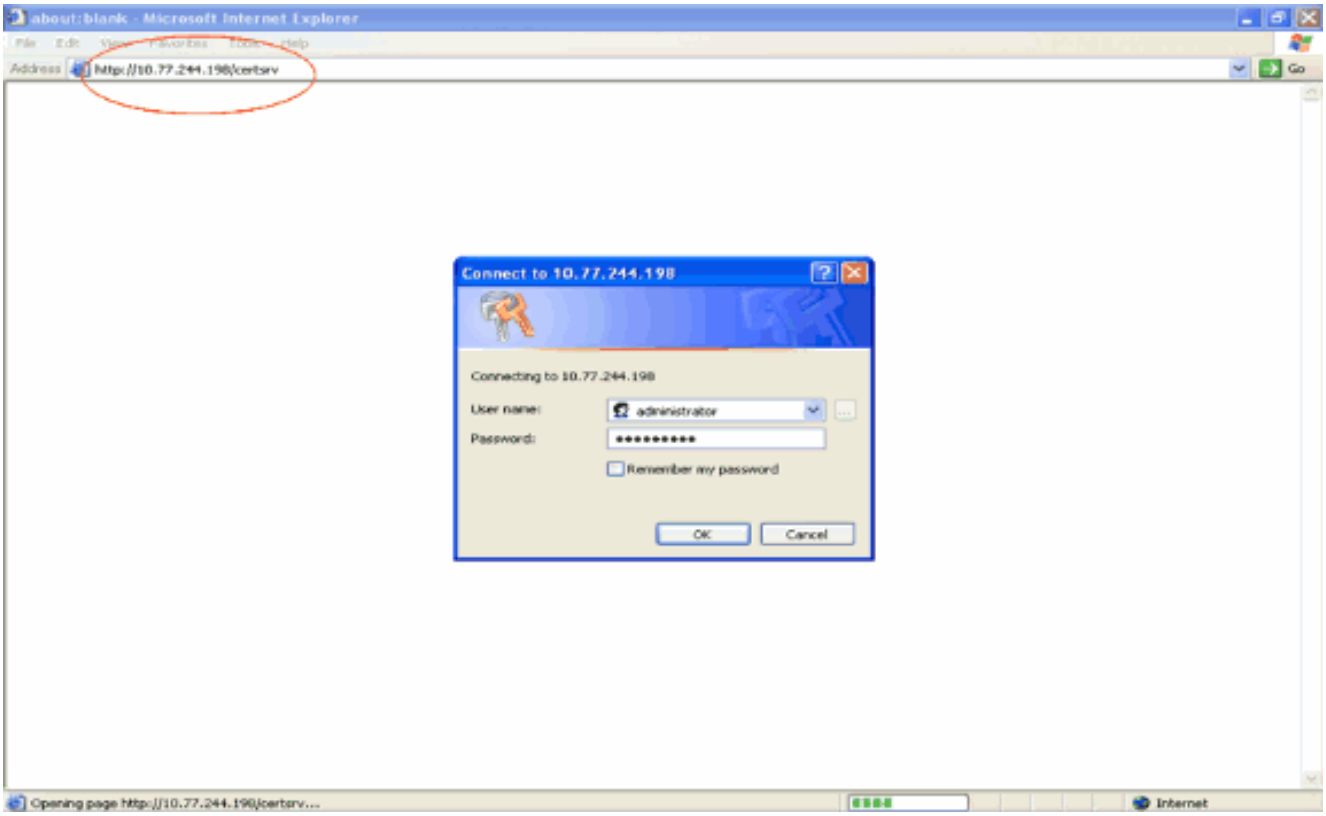
```
(Cisco Controller) >transfer download start

Mode............................................ TFTP
Data Type....................................... Vendor Dev Cert
TFTP Server IP.................................. 10.77.244.196
TFTP Packet Timeout............................. 6
TFTP Max Retries................................ 10
TFTP Path.......................................
TFTP Filename................................... ciscowlc.pem

This may take some time.
Are you sure you want to start? (y/N) y
TFTP EAP CA cert transfer starting.
Certificate installed.
Reboot the switch to use the new certificate.
Enter the reset system command to reboot the controller.
     The controller is now loaded with the device certificate.
```

7. **reset system** コマンドを入力してコントローラをリブートします。これで、コントローラにデバイス証明書がロードされました。

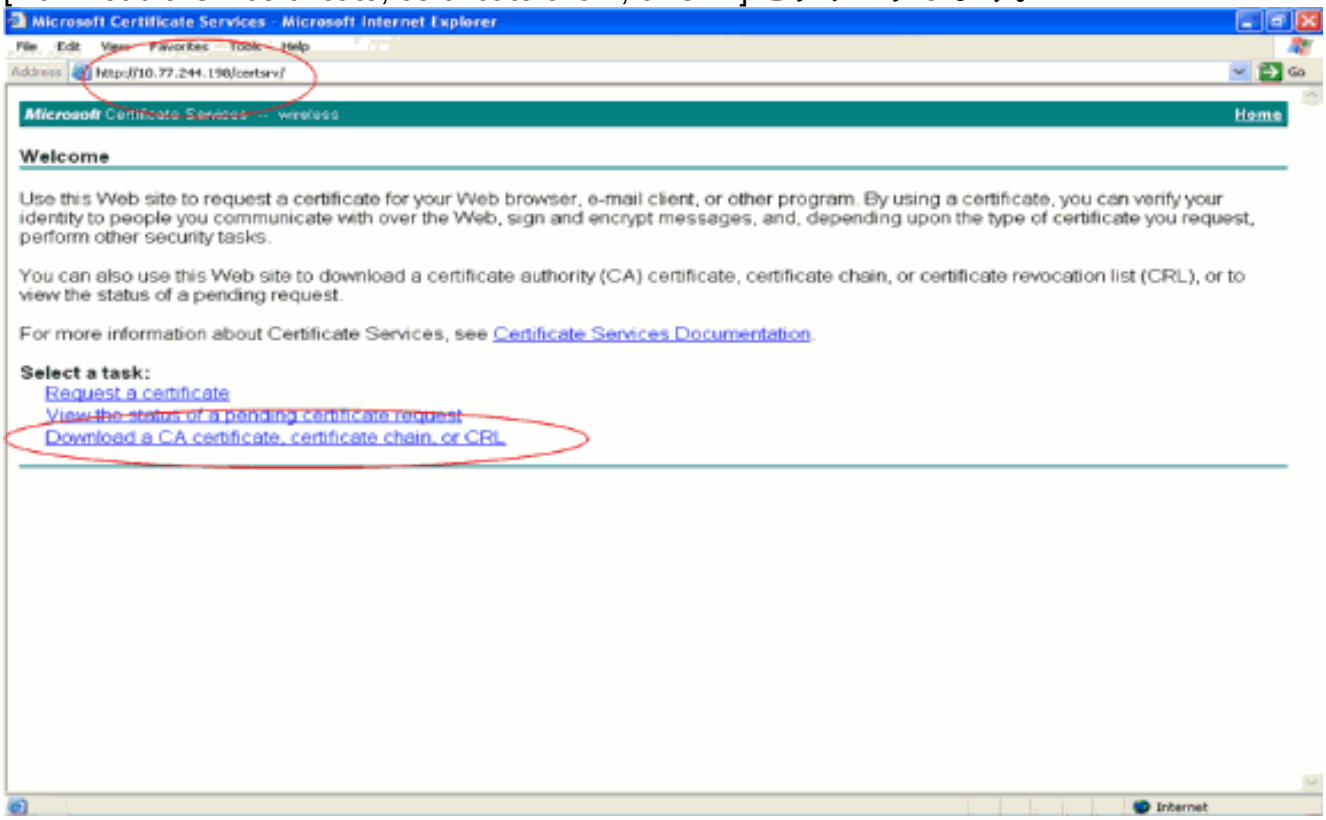
WLC への PKI のルート証明書のインストール

デバイス証明書が WLC にインストールされました。次に、PKI のルート証明書を CA サーバから WLC にインストールします。次のステップを実行します。

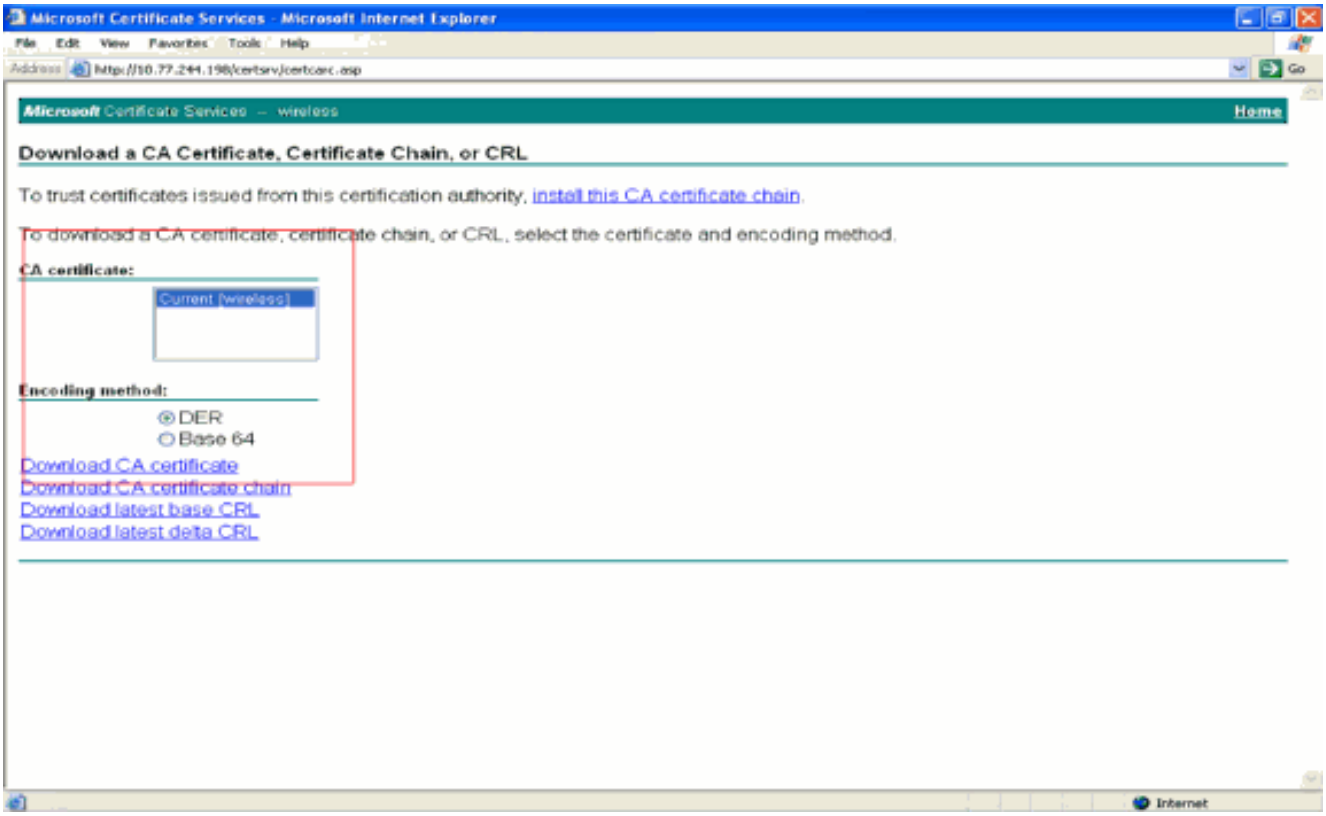
1. CA サーバにネットワーク接続している PC で、**http://<CA サーバの IP アドレス>/certsrv** に移動します。CAサーバの管理者としてログインします。



2. [Download a CA certificate, certificate chain, or CRL] をクリックします。



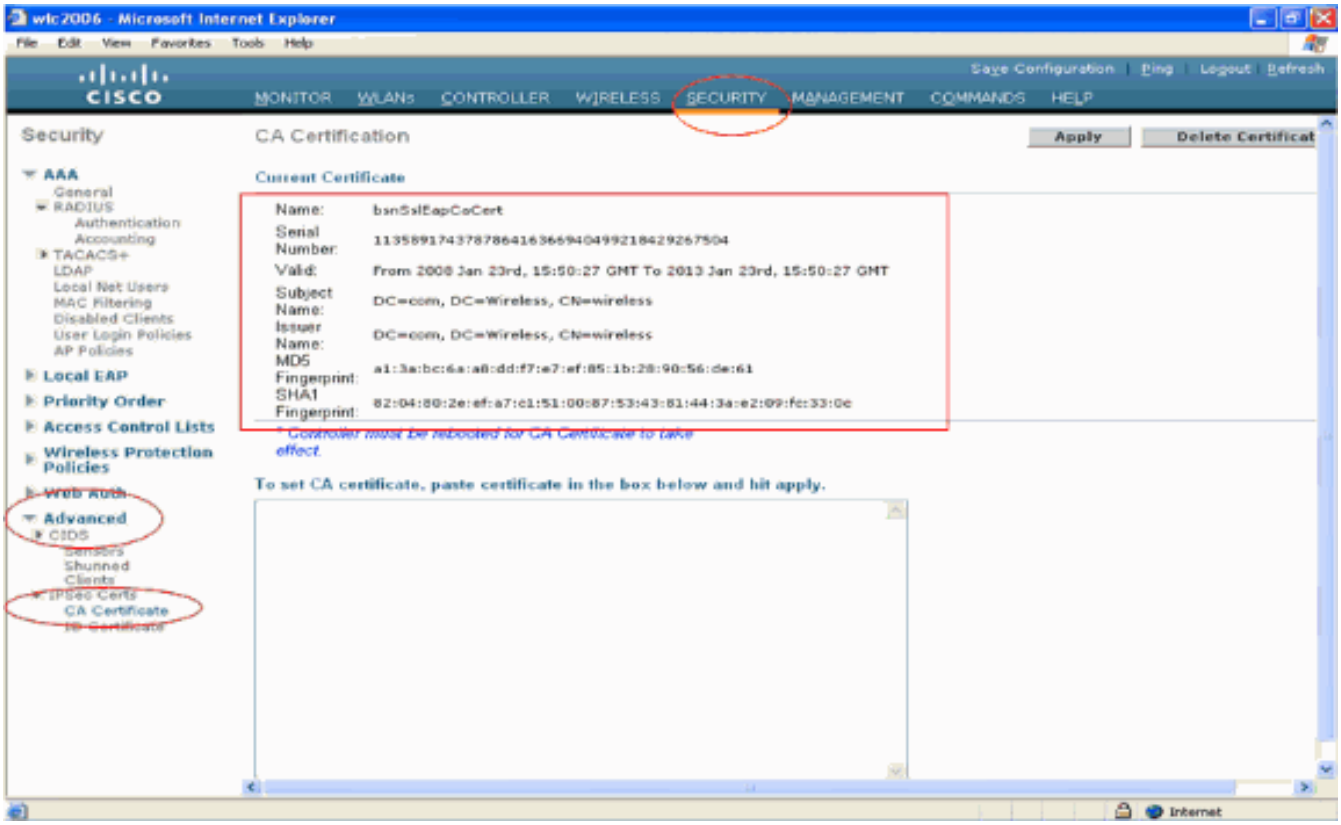
3. 表示されるページで、[CA certificate] ボックスに CA サーバで使用可能な現行の CA 証明書が表示されることを確認します。[Encoding method] で [DER] を選択し、[Download CA certificate] をクリックします。



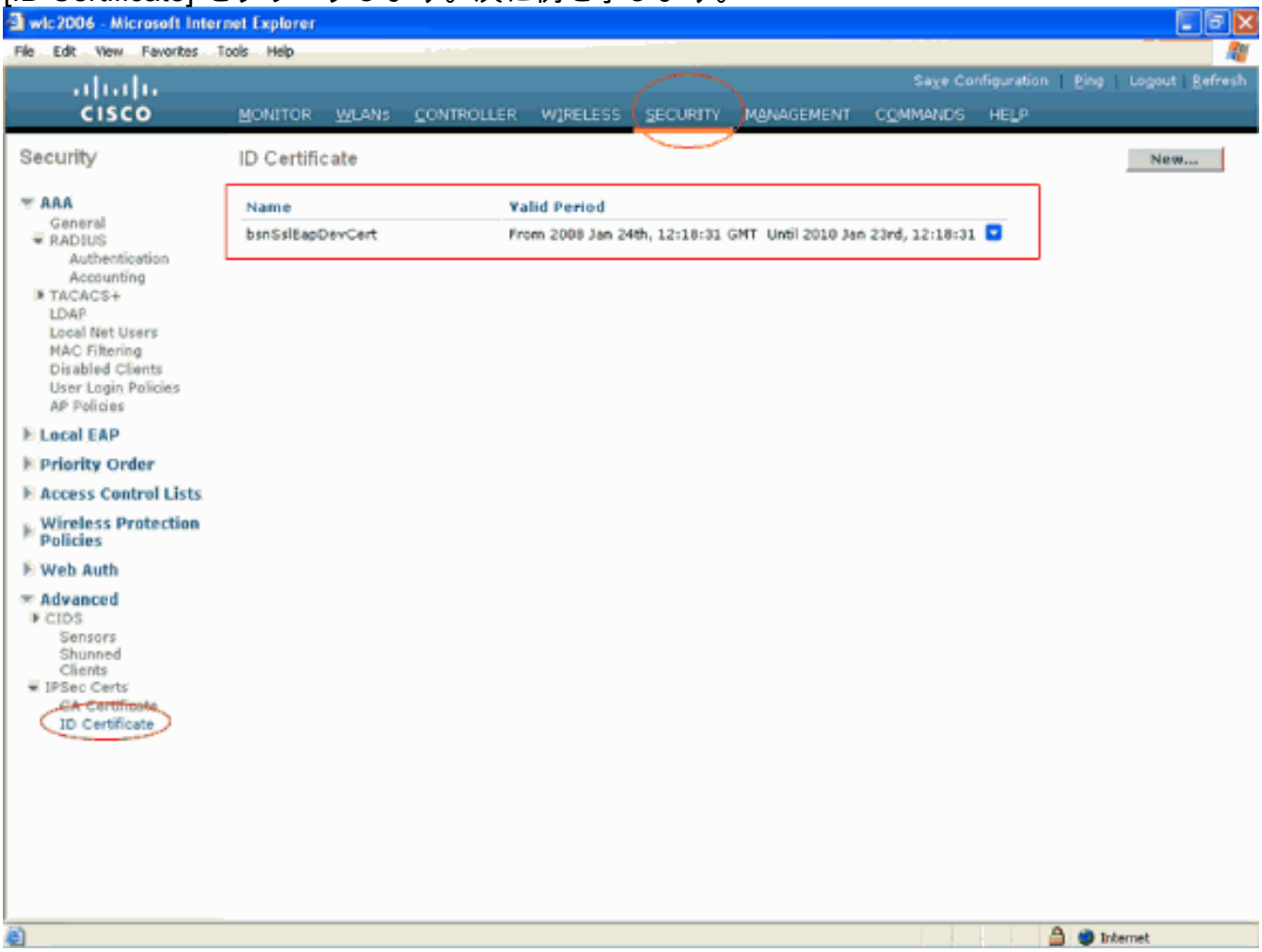
4. 証明書を .cer ファイルとして保存します。この例ではファイル名として **certnew.cer** が使用されています。
5. 次に .cer ファイルを PEM フォーマットに変換してコントローラにダウンロードします。以下の手順を実行するには、「WLC へのデバイス証明書のダウンロード」と同じ手順を使用しますが、次の点を変更します。openSSL の「-in」には **certnew.cer** ファイルを指定し、「-out」には **certnew.pem** ファイルを指定します。このプロセスでは PEM パスフレーズとインポート パスワードは不要です。**.cer** ファイルを **.pem** ファイルに変換する openSSL コマンドは次のとおりです。**x509 -in certnew.cer -inform DER -out certnew.pem -outform PEM**「WLC への変換後の PEM フォーマット デバイス証明書のダウンロード」のステップ 2 で証明書を WLC にダウンロードするコマンドは次のとおりです。(Cisco Controller)**>transfer download datatype eapcacert**WLC にダウンロードするファイルは **certnew.pem** です。

WLC に証明書がインストールされたかどうかをコントローラ GUI から次のように確認できます。

- WLC GUI で [Security] をクリックします。[Security] ページの左側に表示されるタスクから [Advanced] > [IPSec Certs] をクリックします。インストールされている CA 証明書を表示するため [CA Certificate] をクリックします。次に例を示します。



- デバイス証明書が WLC にインストールされているかどうかを確認するには、WLC GUI で [Security] をクリックします。[Security] ページの左側に表示されるタスクから [Advanced] > [IPSec Certs] をクリックします。インストールされているデバイス証明書を表示するため [ID Certificate] をクリックします。次に例を示します。

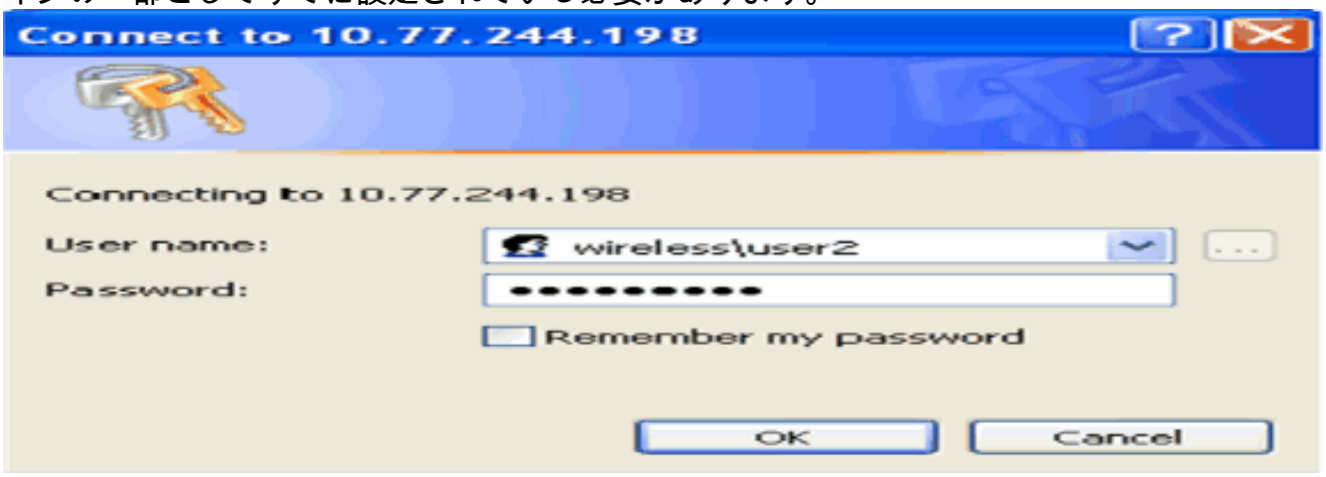


クライアントのデバイス証明書の生成

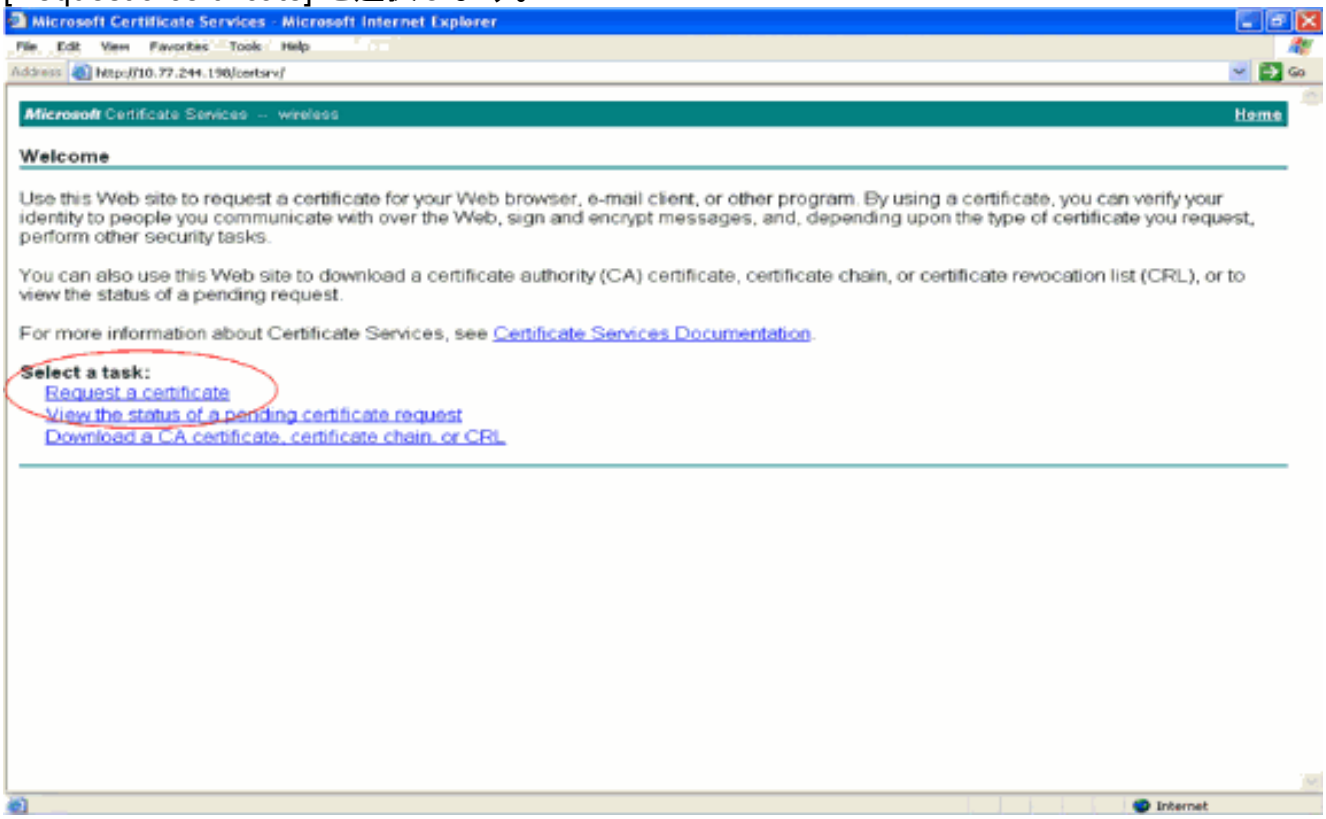
デバイス証明書と CA 証明書が WLC にインストールされました。次に、クライアントに対してこれらの証明書を生成します。

クライアントのデバイス証明書を生成するには、次の手順を実行します。この証明書は、クライアントが WLC への認証を行うときに使用されます。このドキュメントでは、Windows XP Professional クライアントの証明書を生成する手順を説明します。

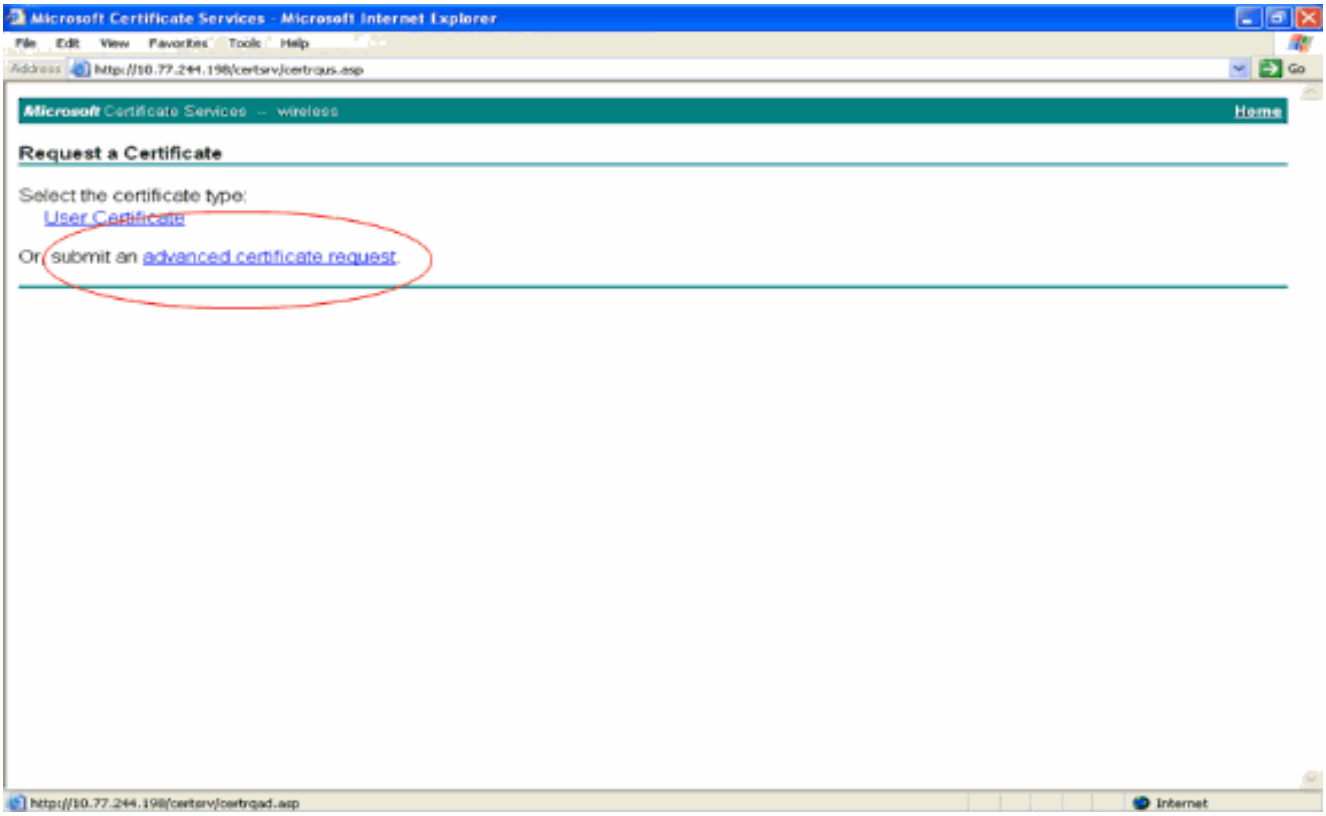
1. 証明書をインストールする必要があるクライアントで **http://<CA サーバの IP アドレス>/certsrv** に移動します。CA サーバにドメイン名\ユーザ名として ログインします。ユーザ名はこの XP マシンを使用しているユーザの名前であり、このユーザは CA サーバと同じドメインの一部としてすでに設定されている必要があります。



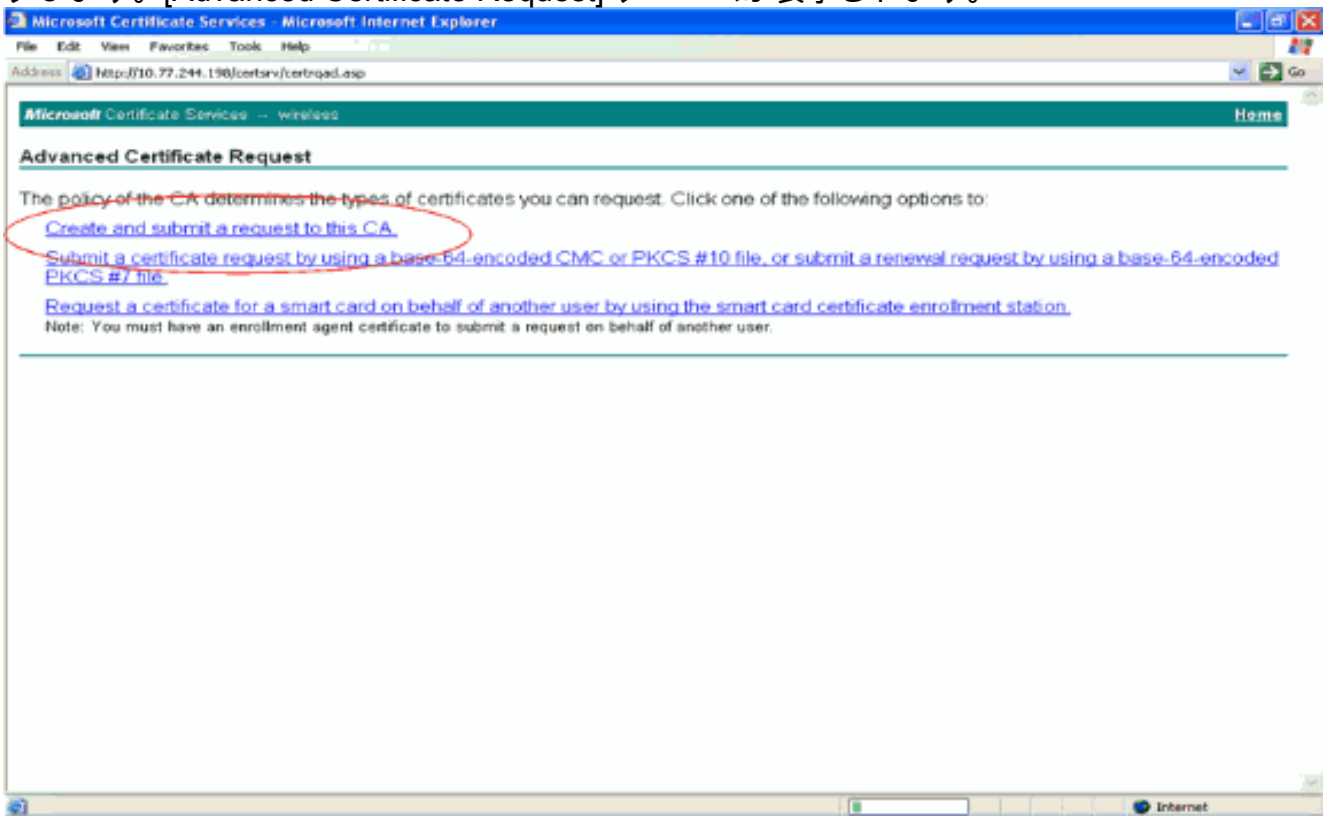
2. [Request a certificate] を選択します。



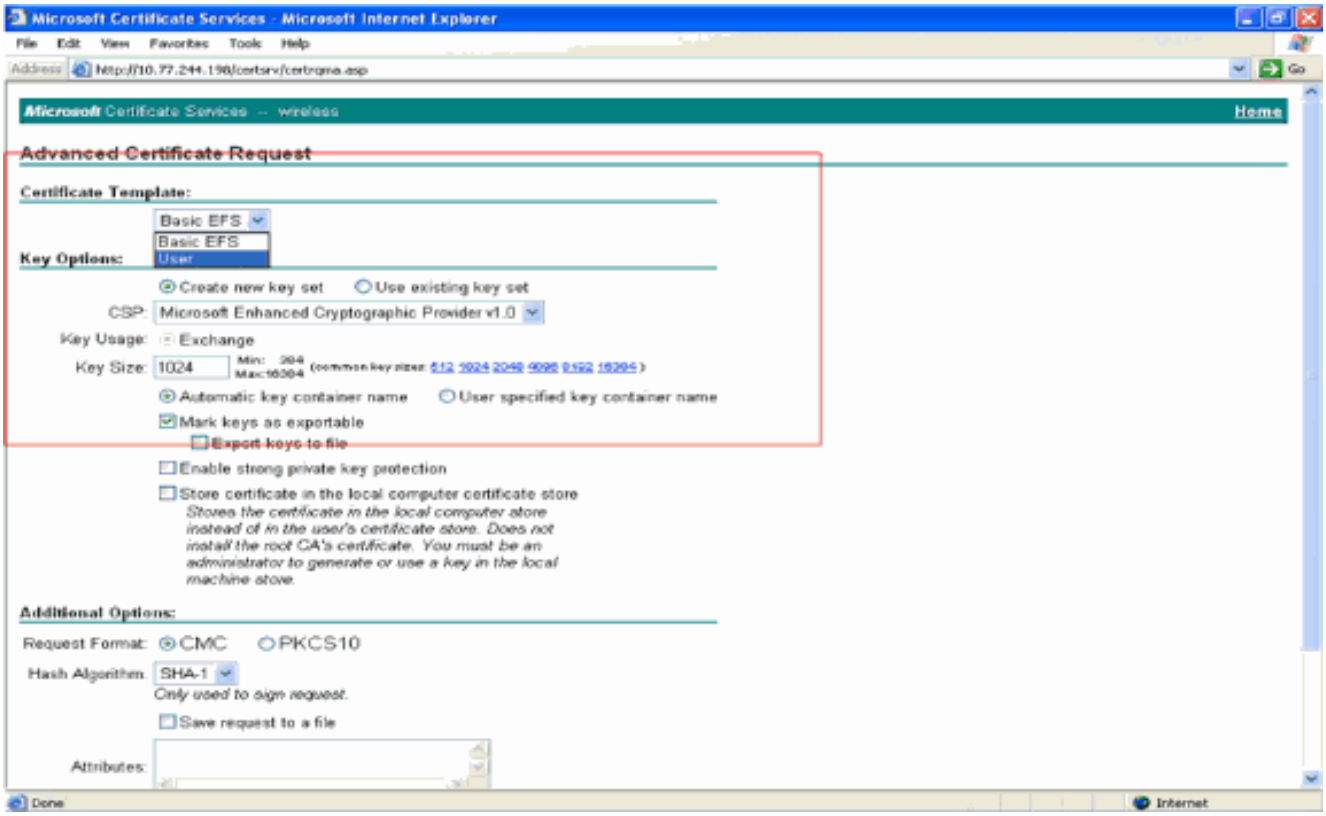
3. [Request a Certificate] ページで [advanced certificate request] をクリックします。



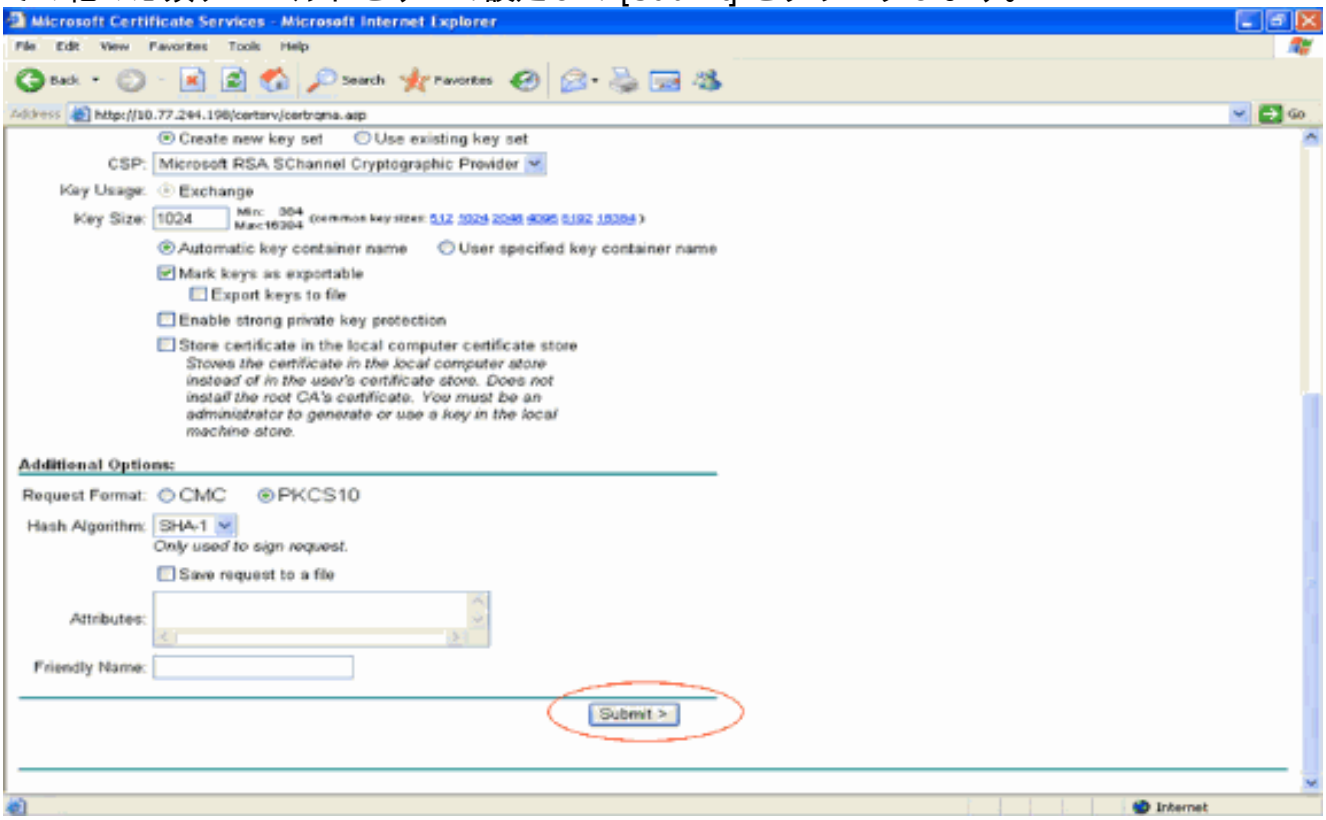
4. [Advanced Certificate Request] ページで [Create and submit a request to this CA] をクリックします。[Advanced Certificate Request] フォームが表示されます。



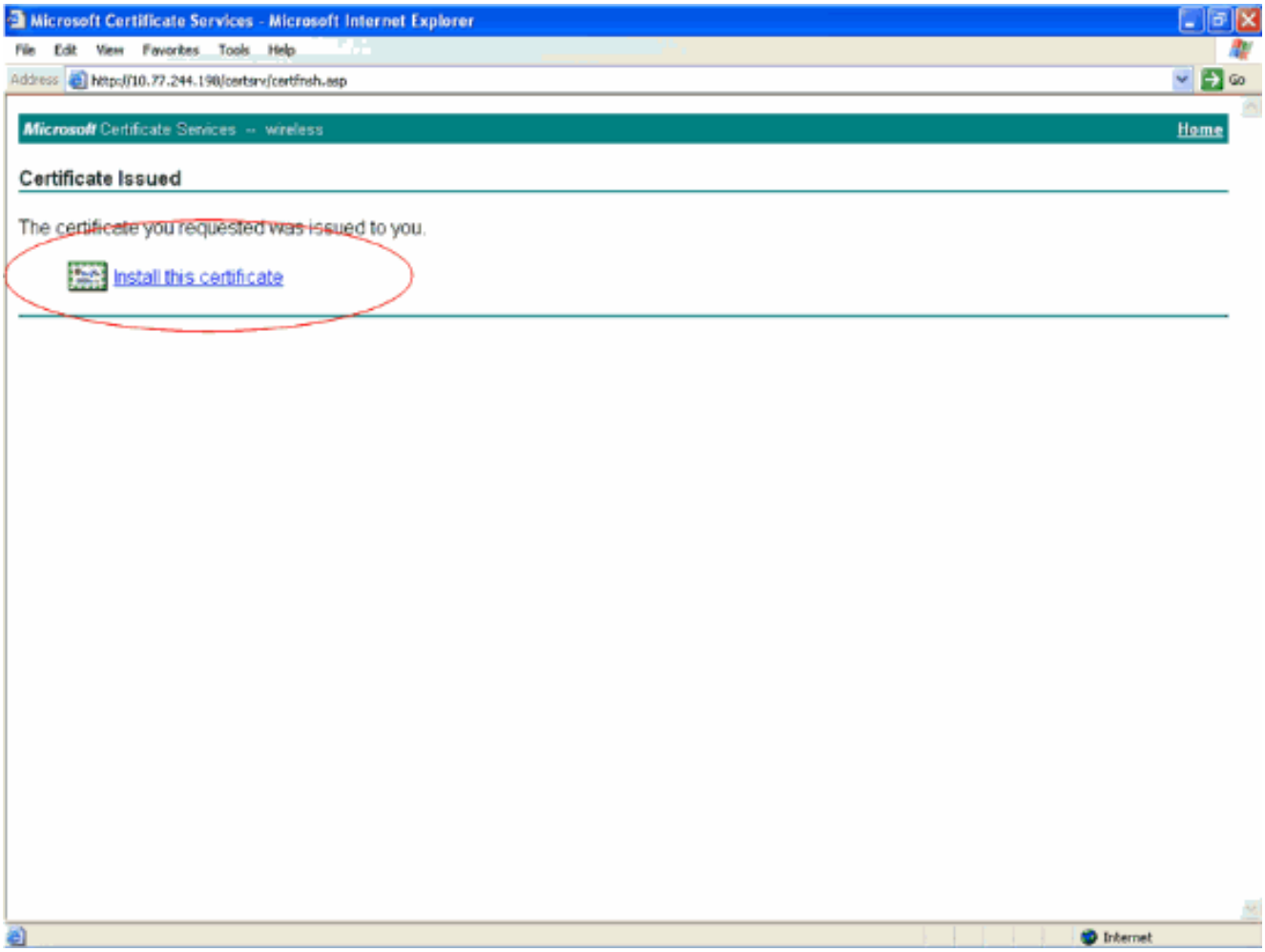
5. [Advanced Certificate Request] フォームの [Certificate Template] ドロップダウン メニューから [User] を選択します。[Key Options] セクションで次のパラメータを選択します。[Key Size] フィールドにキー サイズを入力します。この例では **1024** を使用しています。[Mark Keys as Exportable] オプションにチェックマークを付けます。



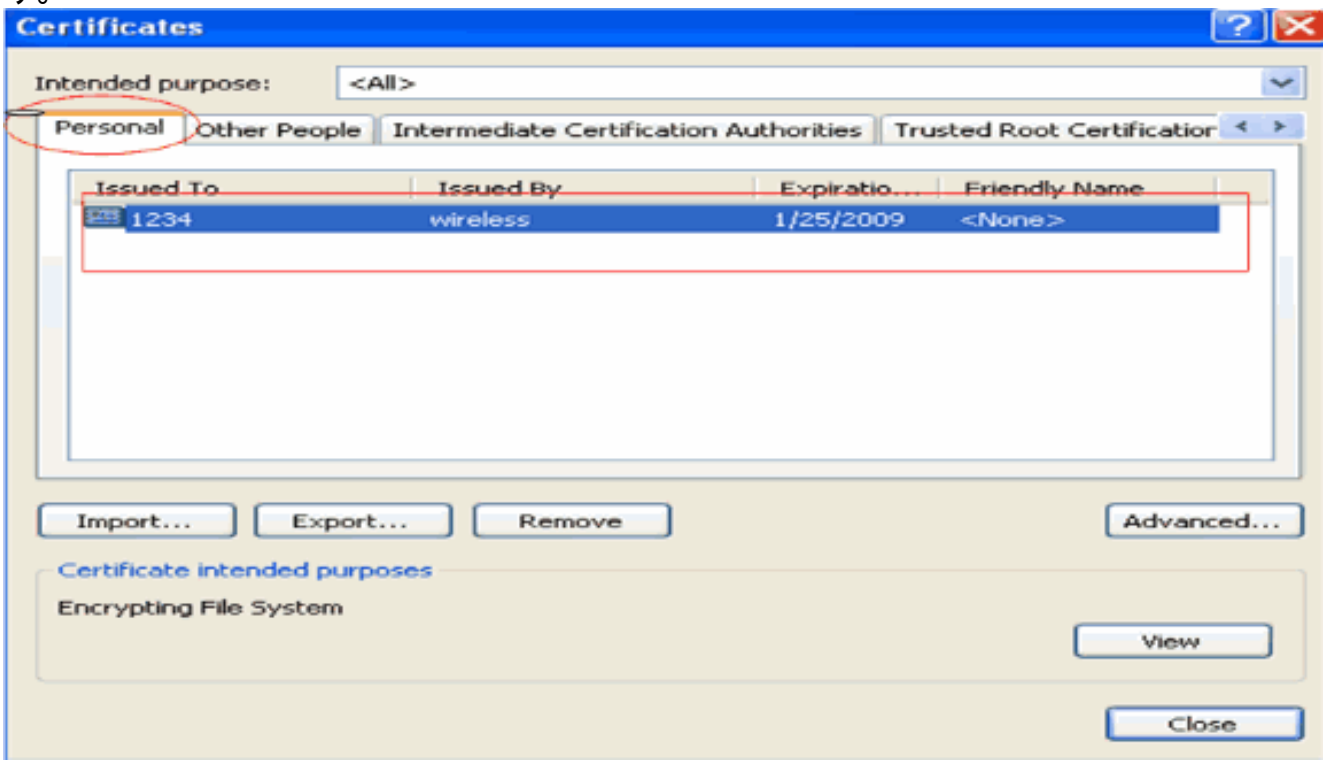
6. その他の必須フィールドをすべて設定して [Submit] をクリックします。



7. 要求に基づいてクライアントのデバイス証明書が生成されます。[Install the certificate] をクリックして証明書を証明書ストアにインストールします。



8. クライアントの IE ブラウザの [Tools] > [Internet Options] > [Content] > [Certificates] にある [Personal] 証明書リストに、インストールしたクライアントのデバイス証明書が表示されます。

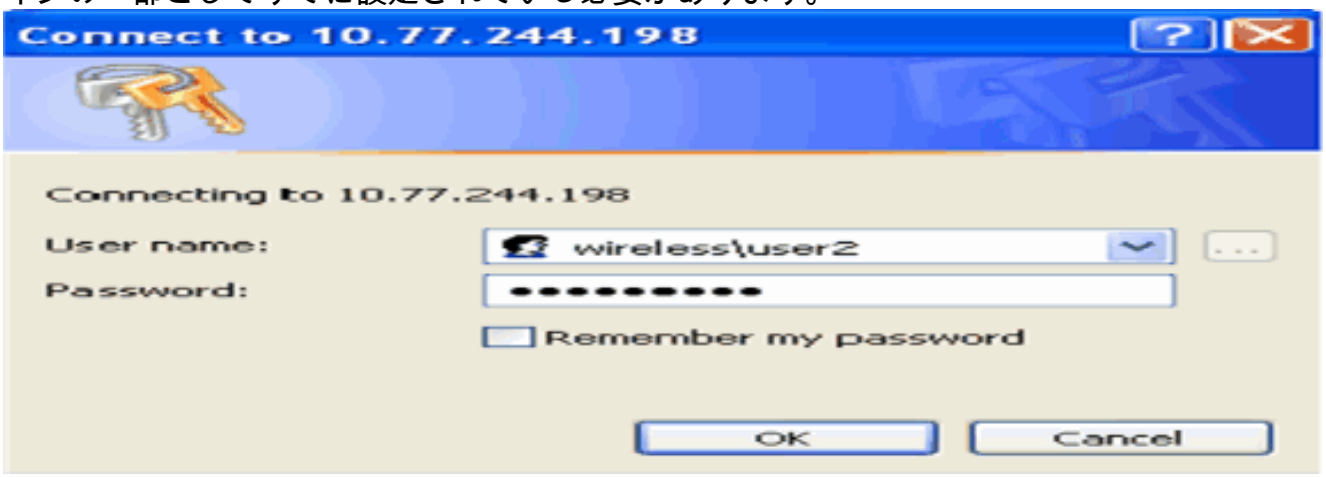


クライアントのデバイス証明書がクライアントにインストールされました。

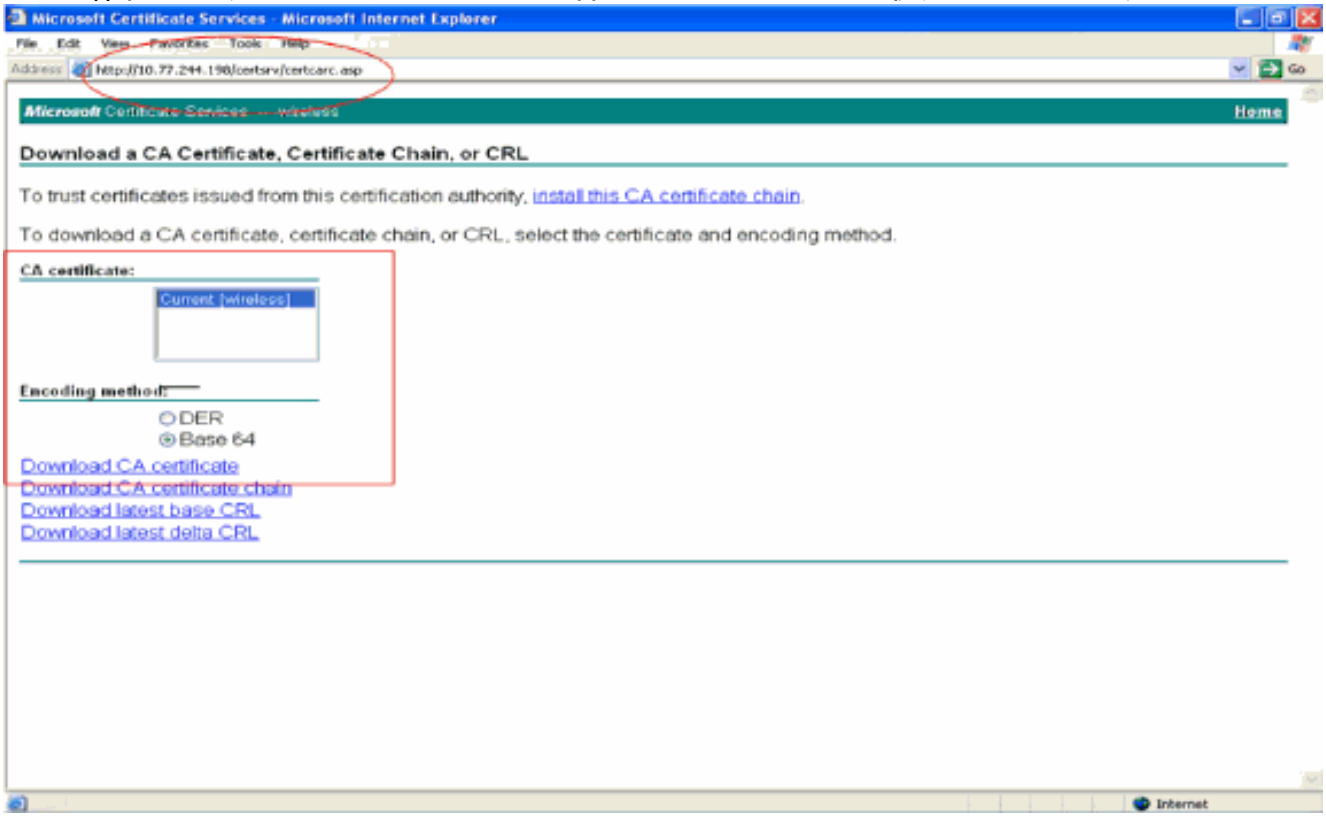
クライアントのルート CA 証明書の生成

次に、クライアントの CA 証明書を生成します。クライアント PC で次の手順を実行します。

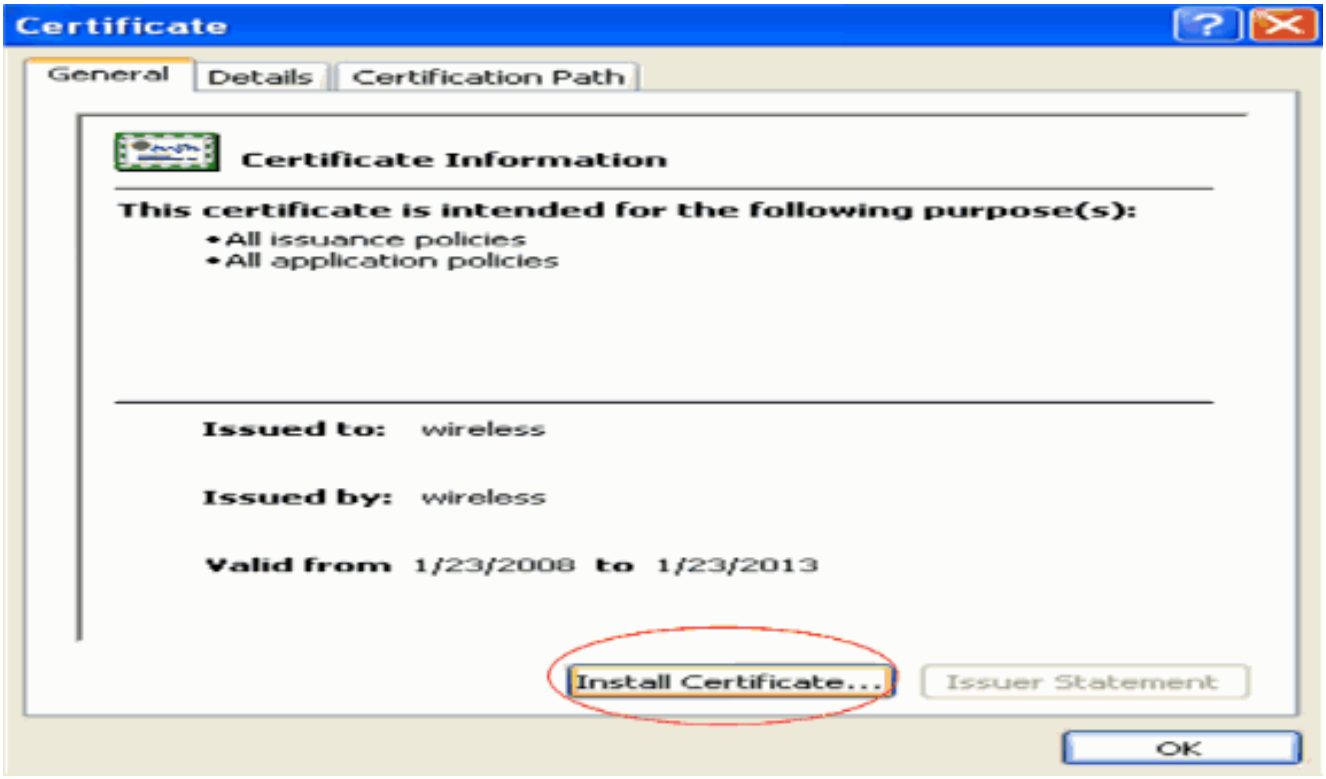
1. 証明書をインストールする必要があるクライアントで **http://<CA サーバの IP アドレス>/certsrv** に移動します。CA サーバにドメイン名\ユーザ名としてログインします。ユーザ名はこの XP マシンを使用しているユーザの名前であり、このユーザは CA サーバと同じドメインの一部としてすでに設定されている必要があります。



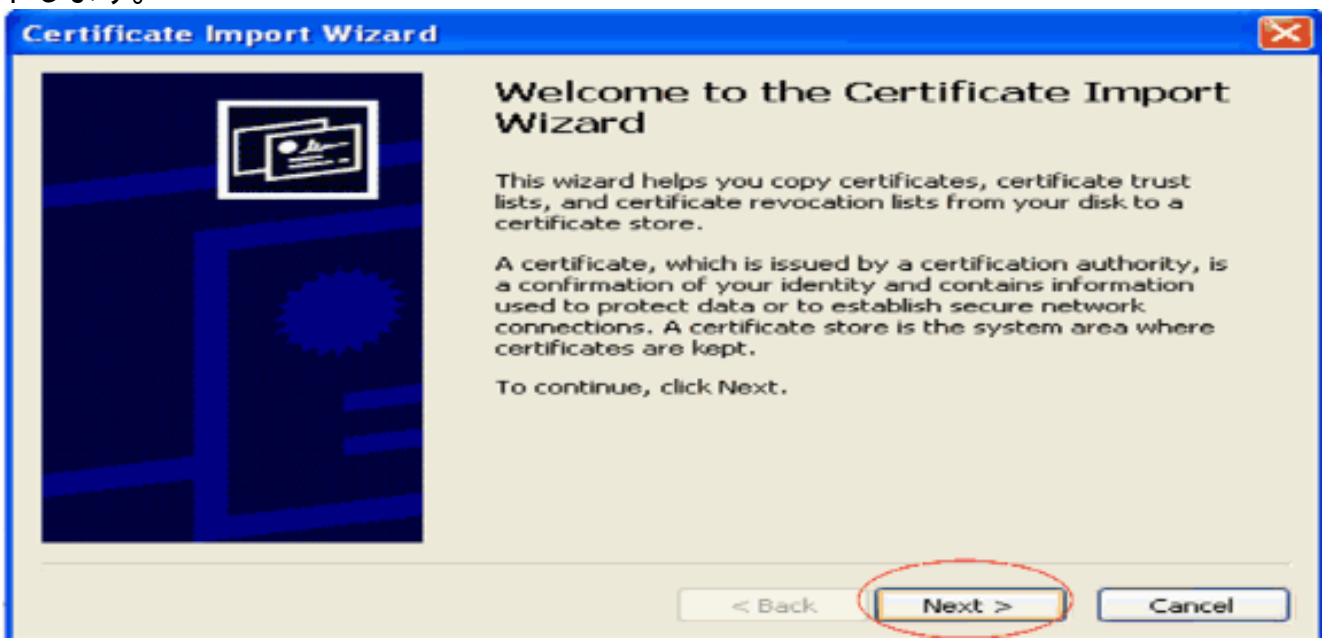
2. 表示されるページで、[CA certificate] ボックスに CA サーバで使用可能な現行の CA 証明書が表示されることを確認します。エンコード方式として [Base 64] を選択します。次に [Download CA certificate] をクリックし、ファイルを **.cer** ファイルとしてクライアントの PC に保存します。この例ではファイル名として **rootca.cer** が使用されています。



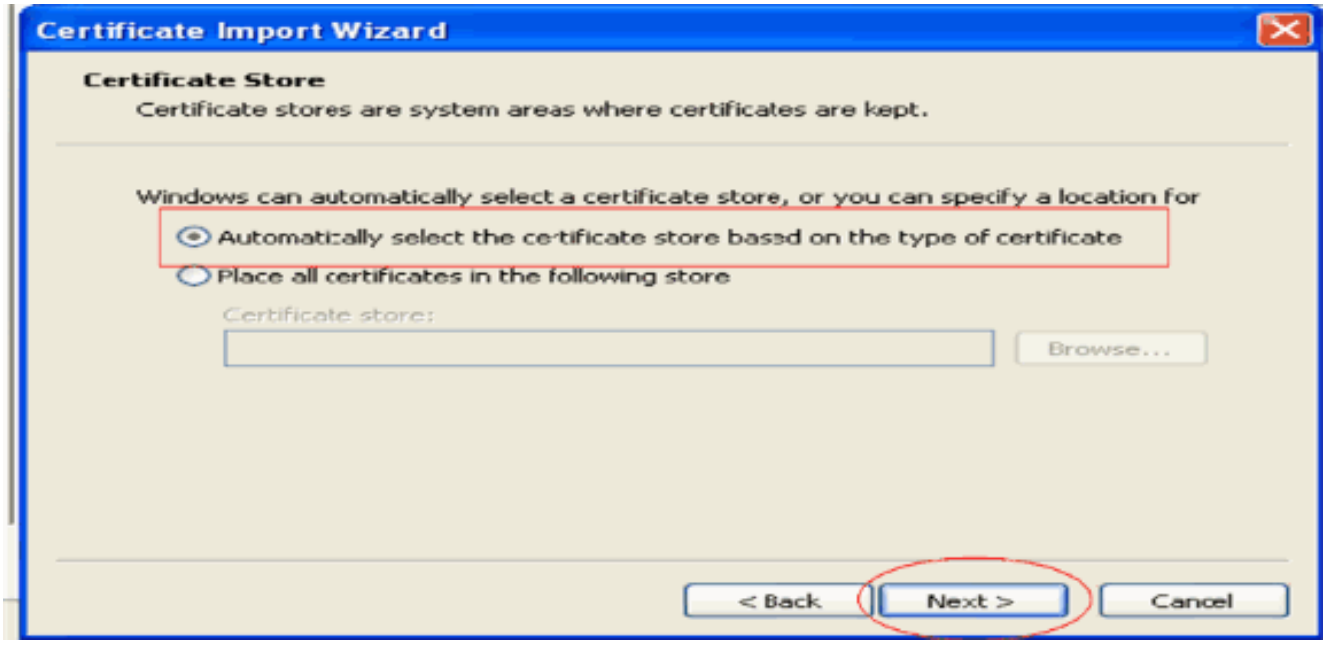
3. 次に、.cer フォーマットで保存した CA 証明書をクライアントの証明書ストアにインストールします。rootca.cer ファイルをダブルクリックして [Install Certificate] をクリックします。



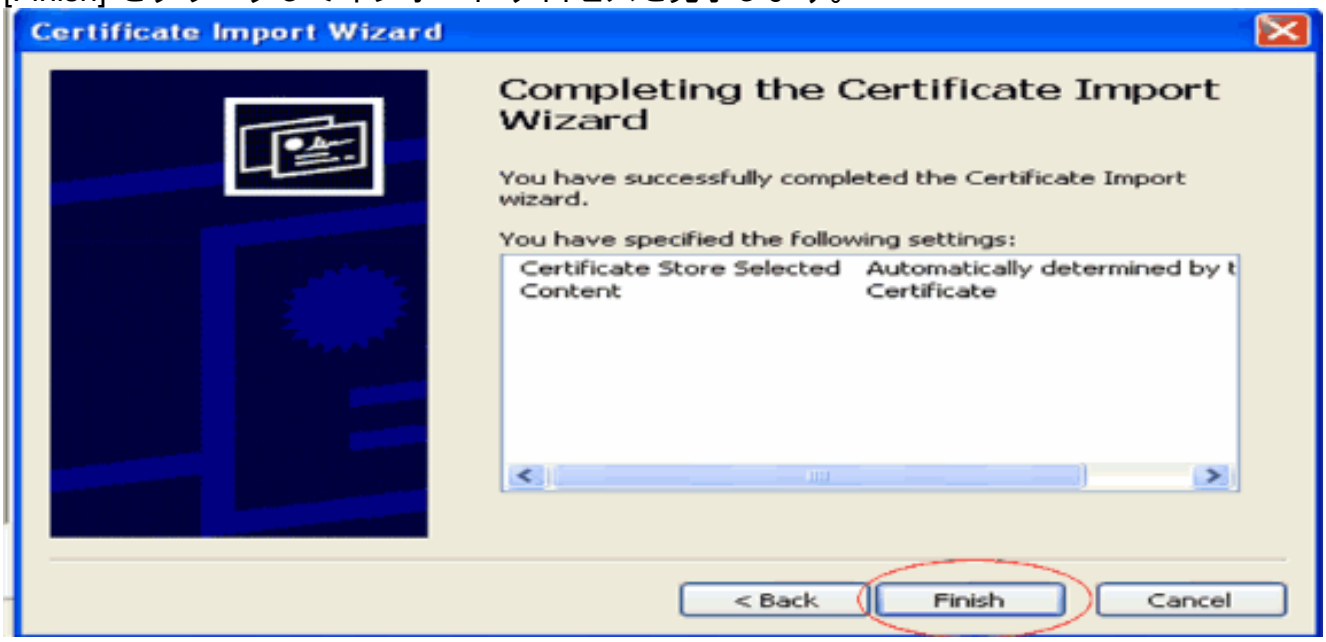
4. [Next] をクリックしてクライアントのハード ディスクから証明書ストアに証明書をインポートします。



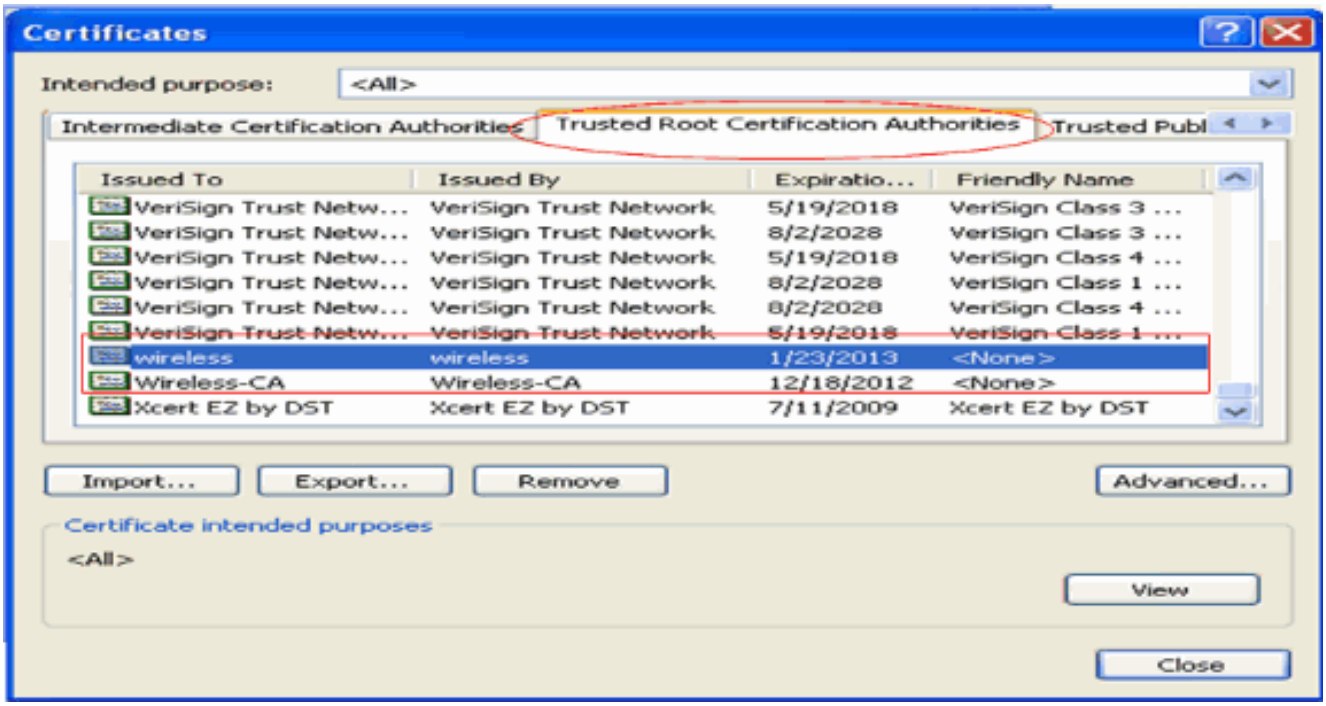
5. [Automatically select the certificate store based on the type of the certificate] を選択し、[Next] をクリックします。



6. [Finish] をクリックしてインポート プロセスを完了します。



7. デフォルトでは、CA 証明書はクライアントの IE ブラウザの [Tools] > [Internet Options] > [Content] > [Certificates] の [Trusted Root Certification Authorities] リストにインストールされます。次に例を示します。

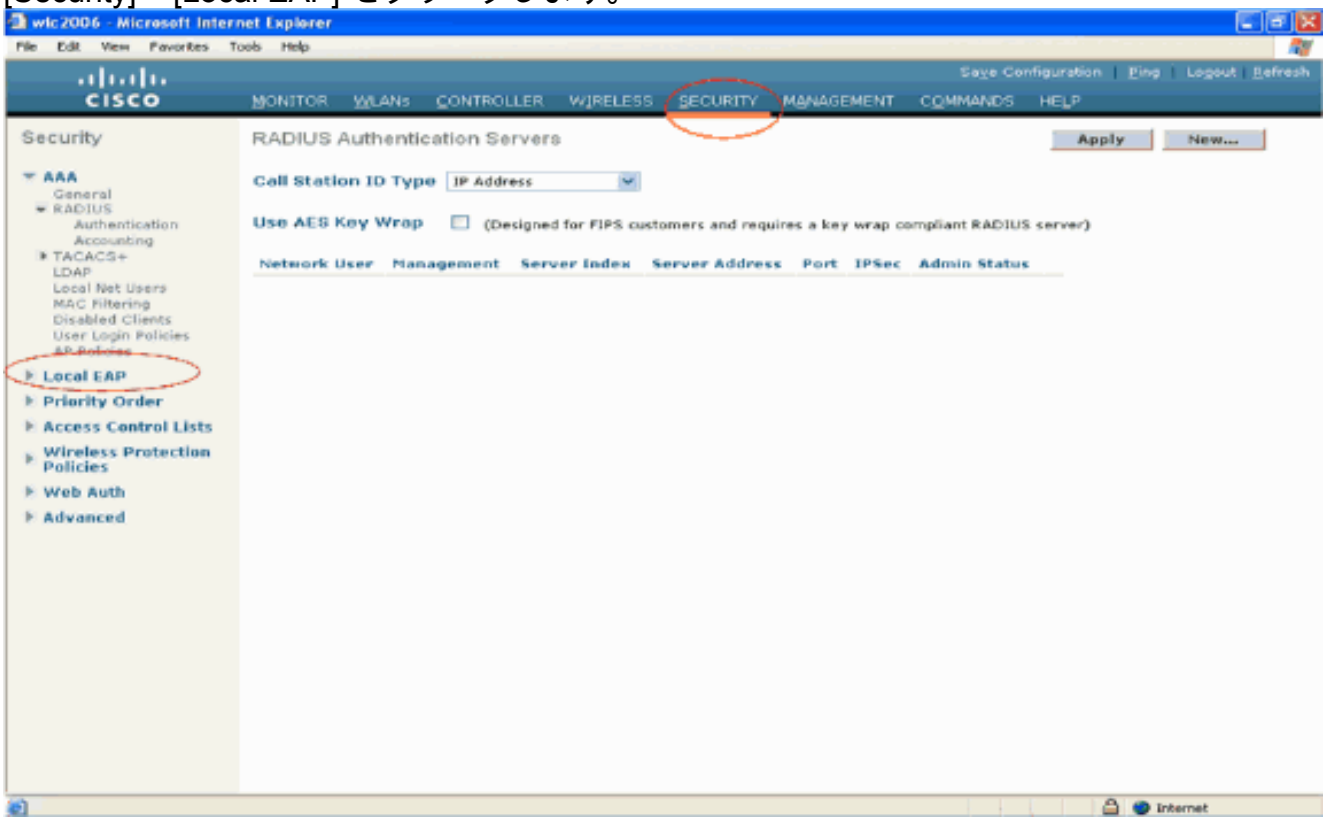


EAP-FAST ローカル EAP 認証に必要なすべての証明書が WLC とクライアントにインストールされます。次に WLC でローカル EAP 認証を設定します。

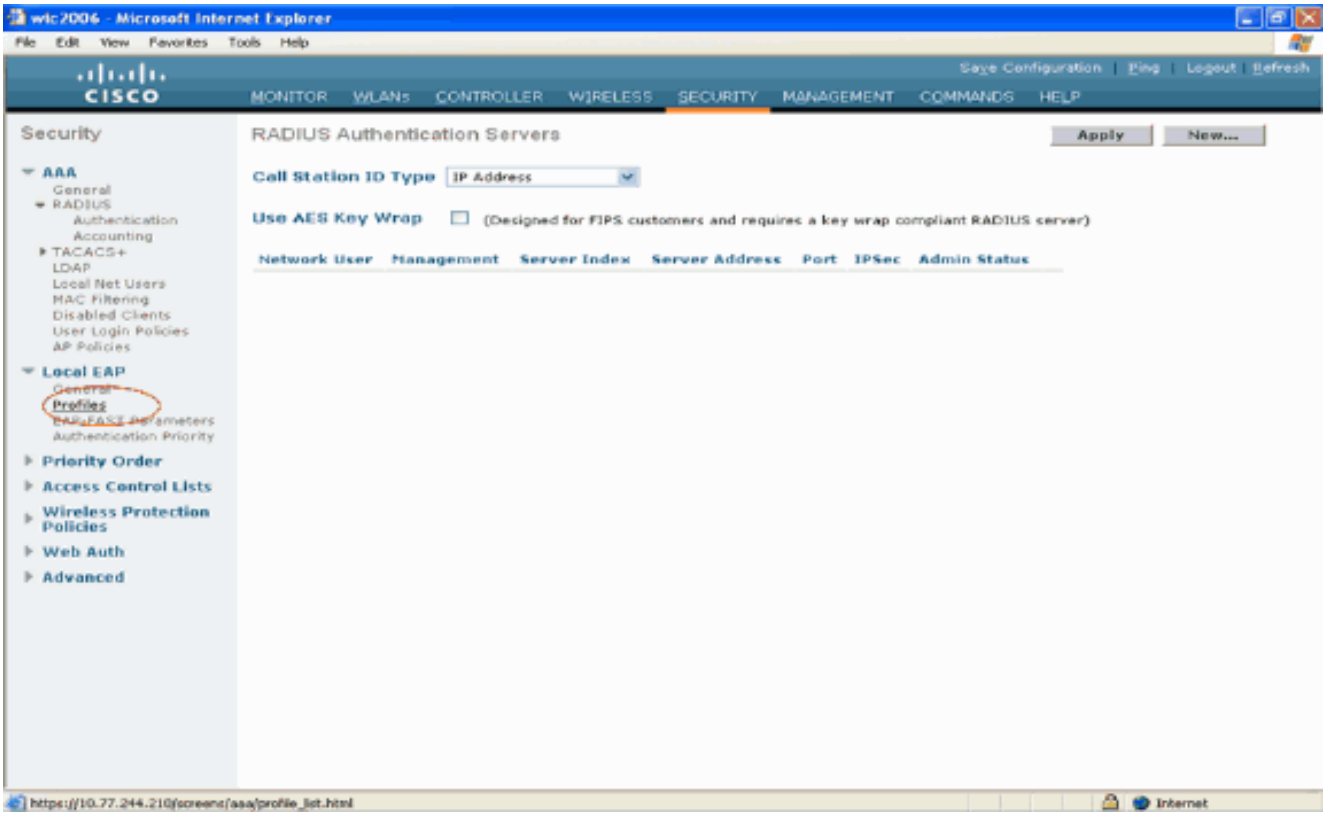
WLC でのローカル EAP の設定

WLC でローカル EAP 認証を設定するため、**WLC GUI モード**で次の手順を実行します。

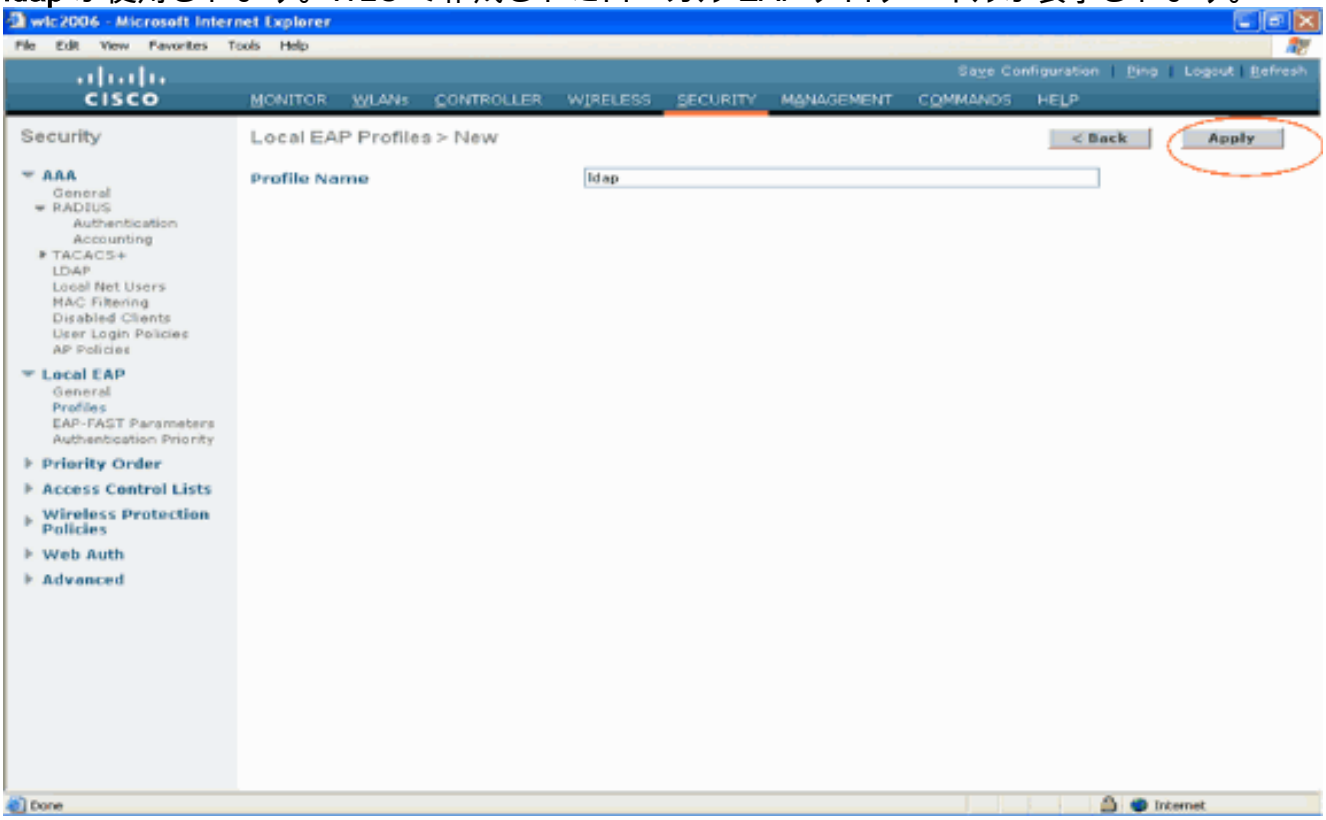
1. [Security] > [Local EAP] をクリックします。



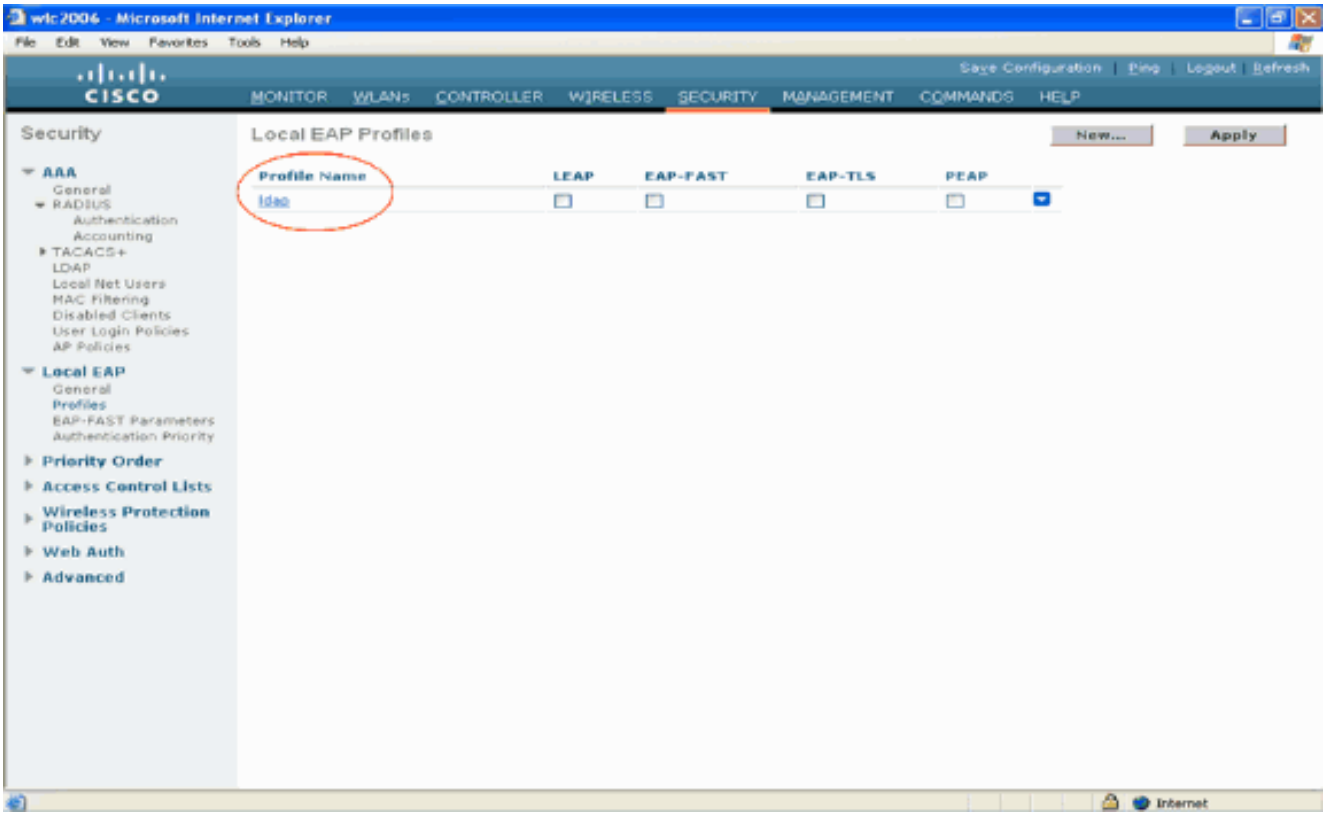
2. ローカル EAP プロファイルを設定するため [Local EAP] の [Profiles] をクリックします。



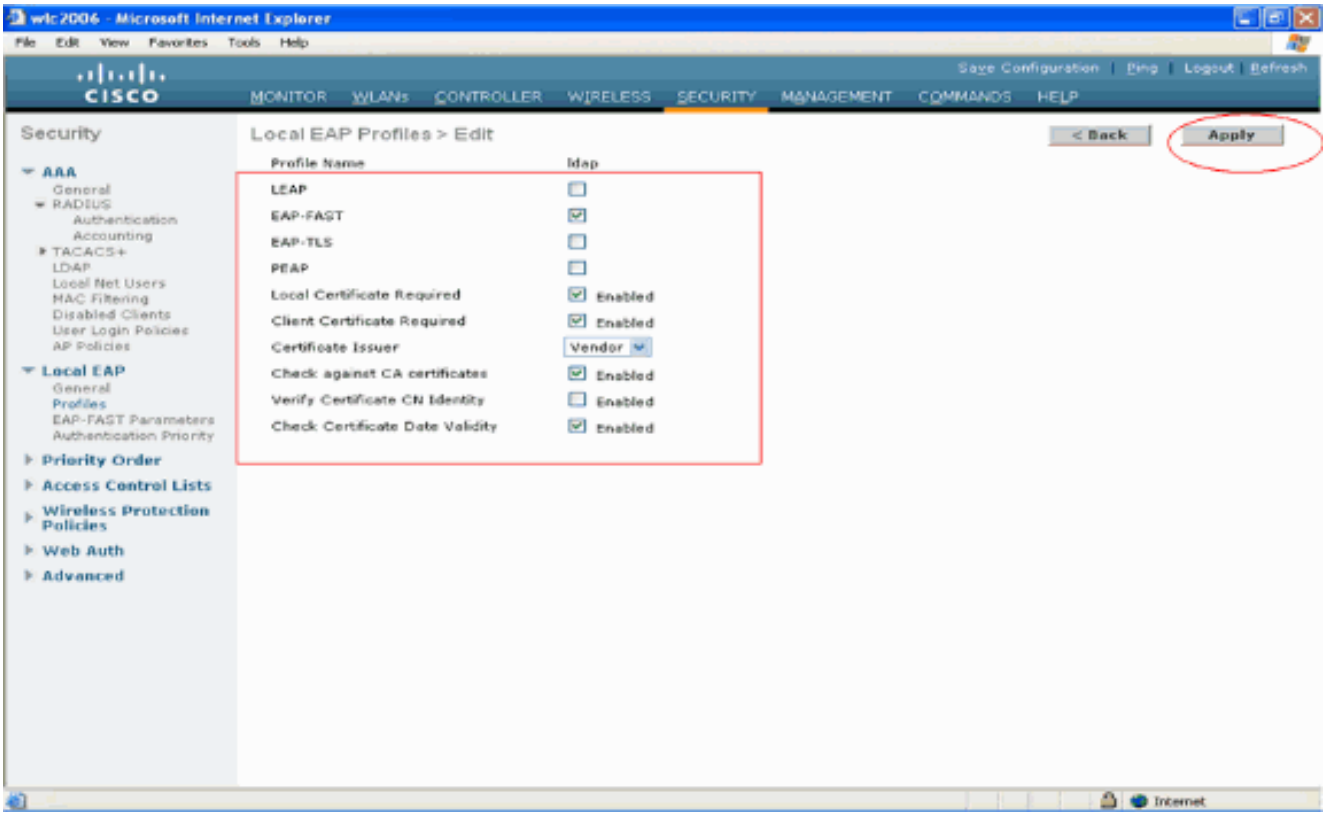
3. [New] をクリックして新しいローカル EAP プロファイルを作成します。
4. このプロファイルの名前を設定して [Apply] をクリックします。この例ではプロファイル名 **ldap** が使用されます。WLC で作成されたローカル EAP プロファイルが表示されます。



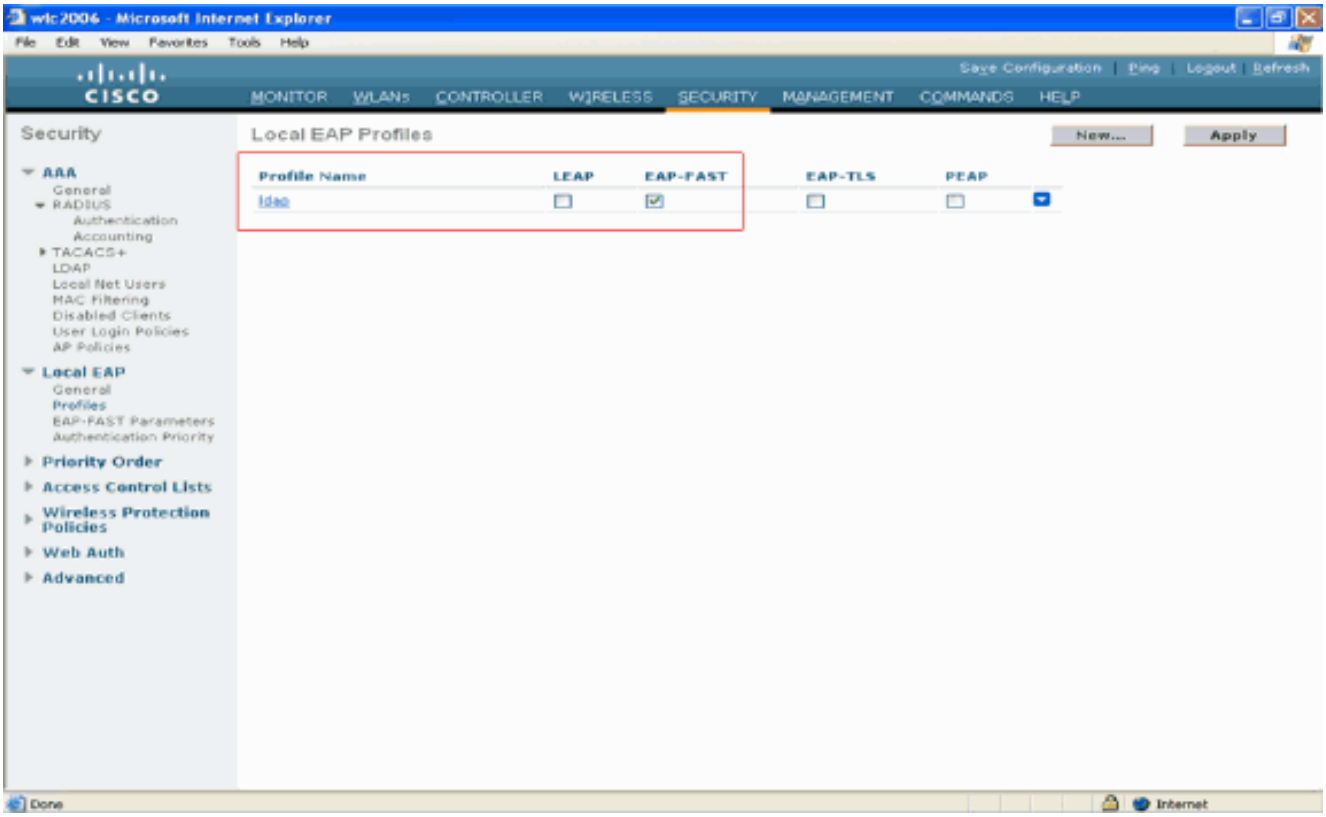
5. [Local EAP Profiles] ページの [Profile Name] フィールドに表示される、作成した **ldap** プロファイルをクリックします。[Local EAP Profiles > Edit] ページが表示されます。



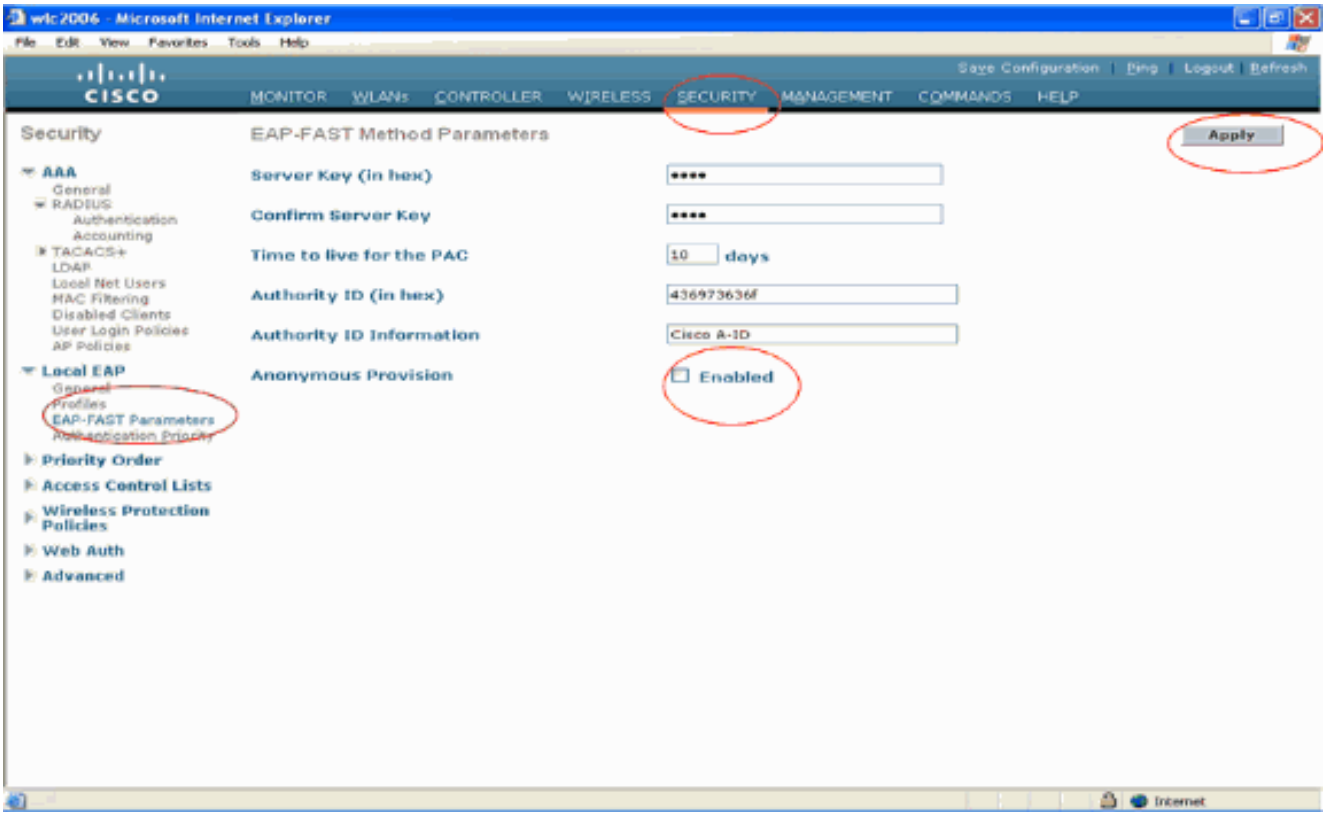
6. [Local EAP Profiles > Edit] ページでこのプロファイル固有のパラメータを設定します。ローカル EAP 認証方式として [EAP-FAST] を選択します。[Local Certificate Required] と [Client Certificate Required] の横のチェックボックスにチェックマークを付けます。このドキュメントではサードパーティ CA サーバを使用するため、[Certificate Issuer] で [Vendor] を選択します。[Check against CA certificates] の横のチェックボックスにチェックマークを付け、クライアントから受け取る証明書をコントローラの CA 証明書と照合して検証するように設定します。受信する証明書の通常名（CN）をコントローラの CA 証明書の CN と照合して検証する場合は、[Verify Certificate CN Identity] チェックボックスにチェックマークを付けます。デフォルト設定は「無効」です。コントローラで受信するデバイス証明書が有効であり有効期限切れではないことを検証できるようにするため、[Check Certificate Date Validity] チェックボックスにチェックマークを付けます。**注：証明書**の日付の妥当性は、コントローラに設定されている現在のUTC(GMT)時間と照合してチェックされます。時間帯オフセットは無視されます。[Apply] をクリックします。



7. EAP-FAST 認証を使用するローカル EAP プロファイルが WLC に作成されます。



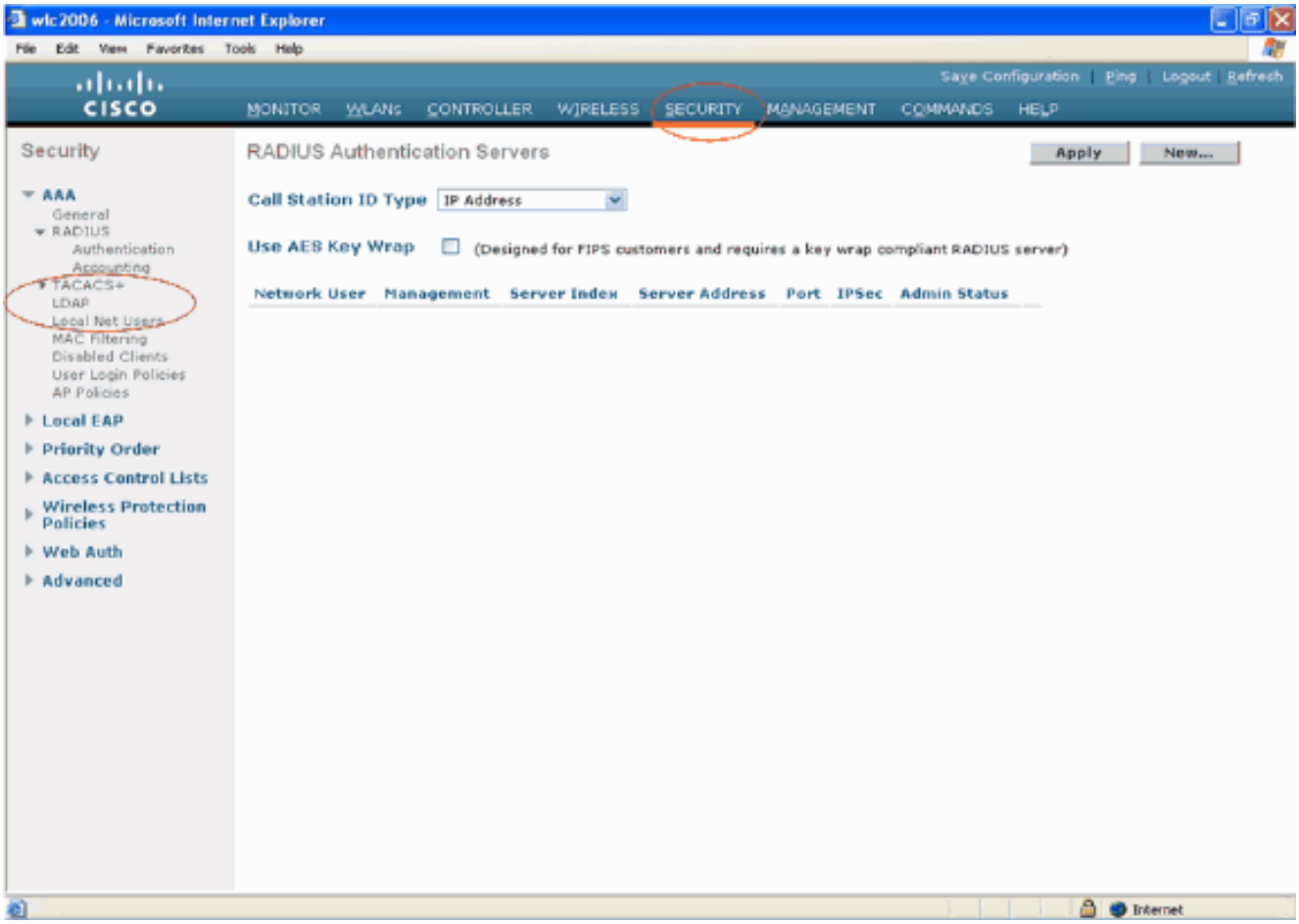
8. 次に、WLC で EAP-FAST 固有のパラメータを設定します。[WLC Security] ページで [Local EAP] > [EAP-FAST Parameters] をクリックし、[EAP-FAST Method Parameters] ページに進みます。この例では証明書を使用した EAP-FAST について説明するため、[Anonymous Provision] チェックボックスのチェックマークを外します。他のパラメータはすべてデフォルトのままにします。[Apply] をクリックします。



WLC での LDAP サーバの詳細の設定

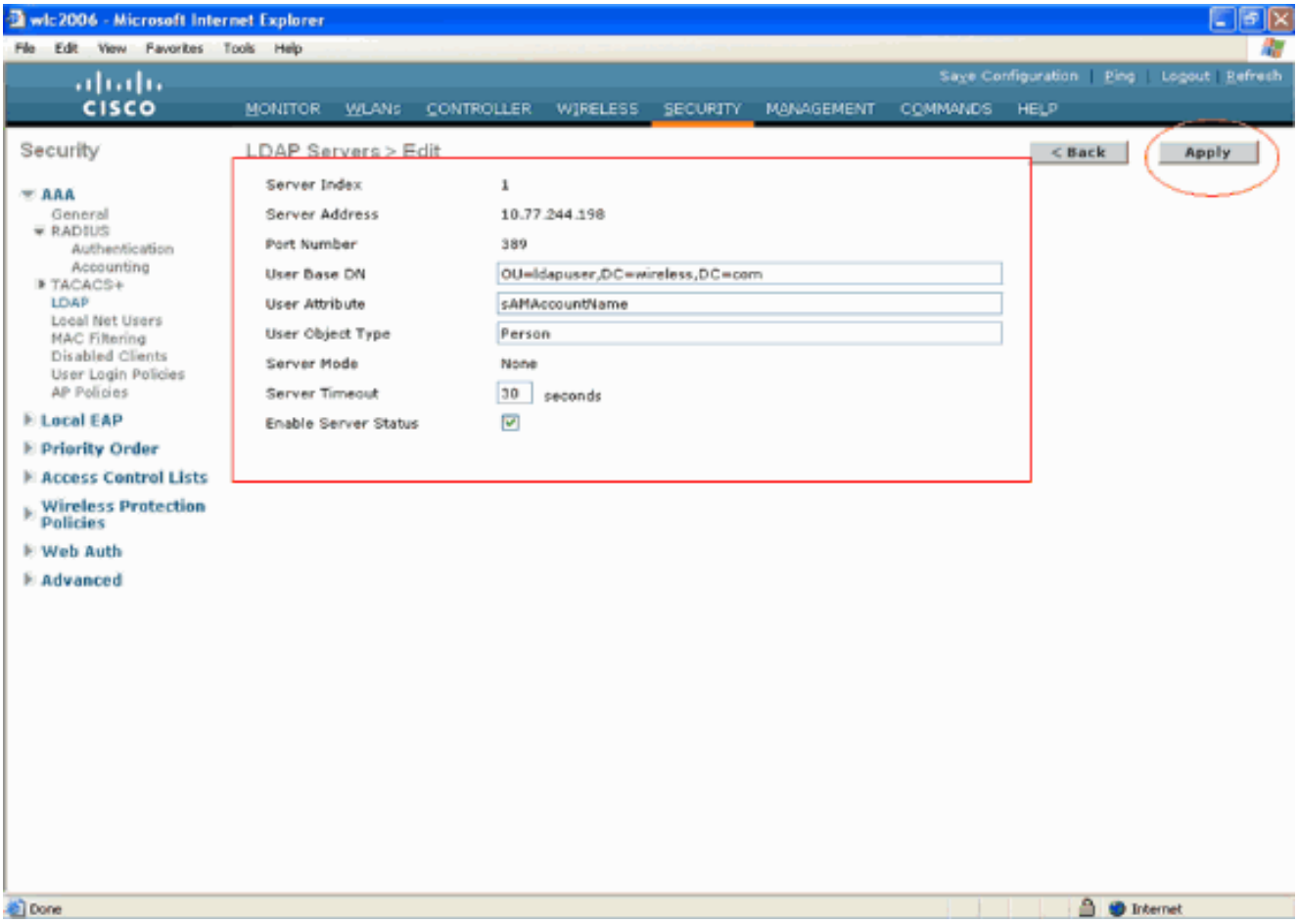
WLC にはローカル EAP プロファイルと関連情報が設定されたので、次に WLC で LDAP サーバの詳細を設定します。WLC で次の手順を実行します。

1. WLC の [Security] ページの左側にあるタスク ペインで [AAA] > [LDAP] を選択し、LDAP サーバ設定ページに進みます。LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers] > [New] ページが表示されます。



2. [LDAP Servers Edit] ページで LDAP サーバの詳細（LDAP サーバの IP アドレス、ポート番号、サーバ有効化ステータスなど）を指定します。[Server Index (Priority)] ドロップダウンボックスから番号を選択し、その他の設定済みの LDAP サーバト関連したこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目のサーバへの接続を試行する、というようになります。[Server IP Address] フィールドに LDAP サーバの IP アドレスを入力します。[Port Number] フィールドに LDAP サーバの TCP ポート番号を入力します。有効な範囲は 1 ~ 65535 で、デフォルト値は 389 です。[User Base DN] フィールドに、すべてのユーザの一覧を含む LDAP サーバ内のサブツリーの Distinguished Name（DN; 識別名）を入力します。たとえば、ou=organizational unit、.ou=next organizational unit、o=corporation.com のようになります。ユーザを含むツリーがベース DN である場合、o=corporation.com または dc=corporation, dc=com と入力します。この例ではユーザは組織単位（OU）**ldapuser** に含まれています。この組織単位は **Wireless.com** ドメインの一部として作成されています。ユーザ ベース DN は、ユーザ情報（EAP-FAST 認証方式に基づくユーザ クレデンシャル）が保存されている場所のフル パスを指し示している必要があります。この例ではユーザはベース DN OU=ldapuser, DC=Wireless, DC=com に含まれています。OU とユーザ設定の詳細については、このドキュメントの「[ドメイン コントローラでのユーザの作成]」で説明します。[User Attribute] フィールドに、ユーザ名を含むユーザ レコード内の属性の名前を入力します。[User Object Type] フィールドに、レコードをユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには複数の objectType 属性の値が含まれています。そのユーザに一意の値と、他のオブジェクト タイプと共有する値があります。**注：これら**の2つのフィールドの値は、Windows 2003サポートツールの一部として提供されているLDAPブラウザユーティリティを使用して、ディレクトリサーバから取得できます。**この Microsoft LDAP ブラウザ ツールは LDP と呼ばれます。**このツールを使用して、特定ユーザの [User Base DN]、[User Attribute]、および [User Object Type] フィールドの値を確認できます。LDP を使用したユーザ固有属性の確認の詳細については、この

ドキュメントの「Using LDP to Identify the User Attributes」を参照してください。すべての LDAP トランザクションでセキュア TLS トンネルを使用するように設定するには、[Server Mode] ドロップダウン ボックスから [Secure] を選択します。それ以外の場合はデフォルト設定である [None] を選択します。[Server Timeout] フィールドに再送信の間隔（秒数）を入力します。有効な範囲は 2 ~ 30 秒で、デフォルト値は 2 秒です。[Enable Server Status] チェックボックスにチェックマークを付けてこの LDAP サーバを有効にします。無効にする場合はチェックマークを外します。デフォルト値は [disabled] です。[Apply] をクリックして、変更を確定します。上記の情報を使用した設定の例を次に示します。

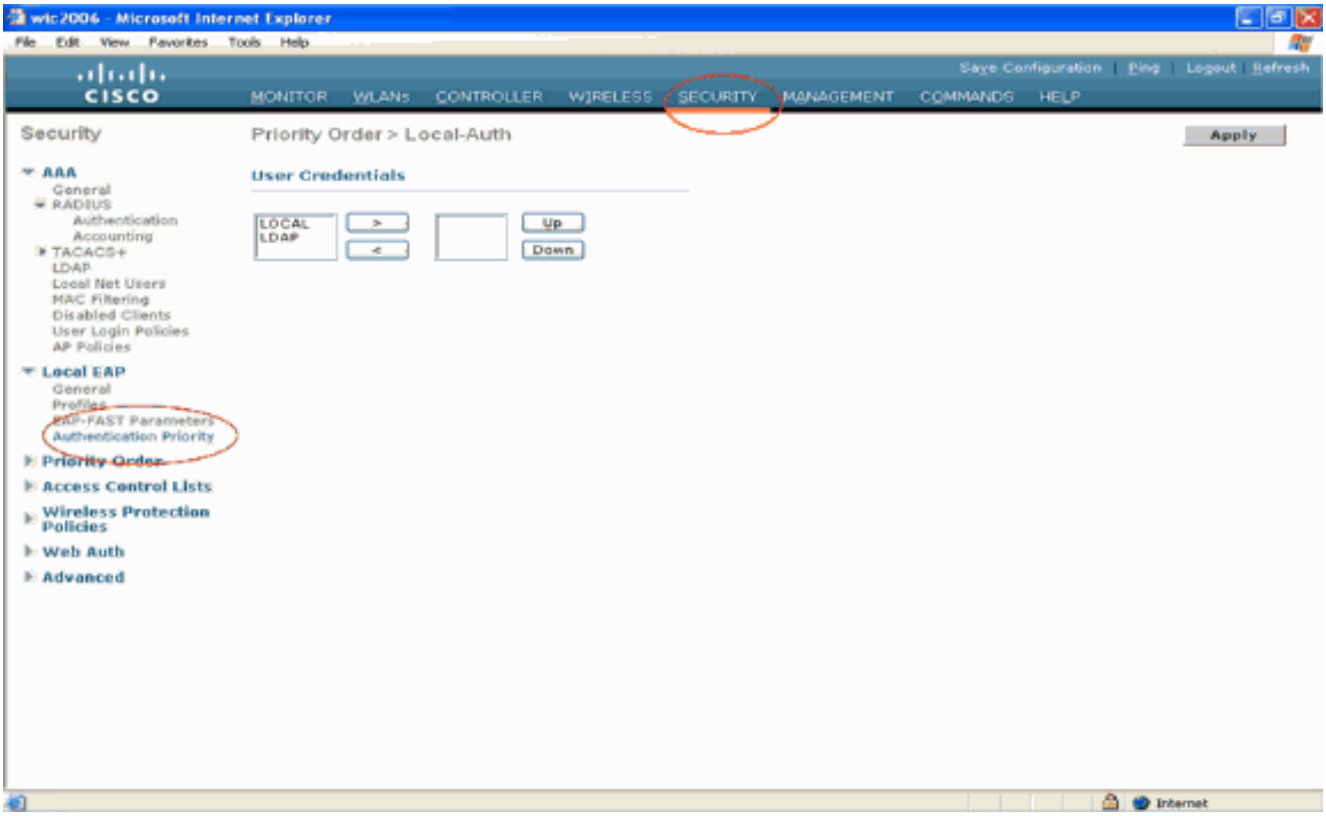


WLC で LDAP サーバの詳細が設定されました。次に、WLC が他のデータベースよりも前に LDAP データベースでユーザ クレデンシャルを最初に検索するようにするため、LDAP を優先バックエンド データベースとして設定します。

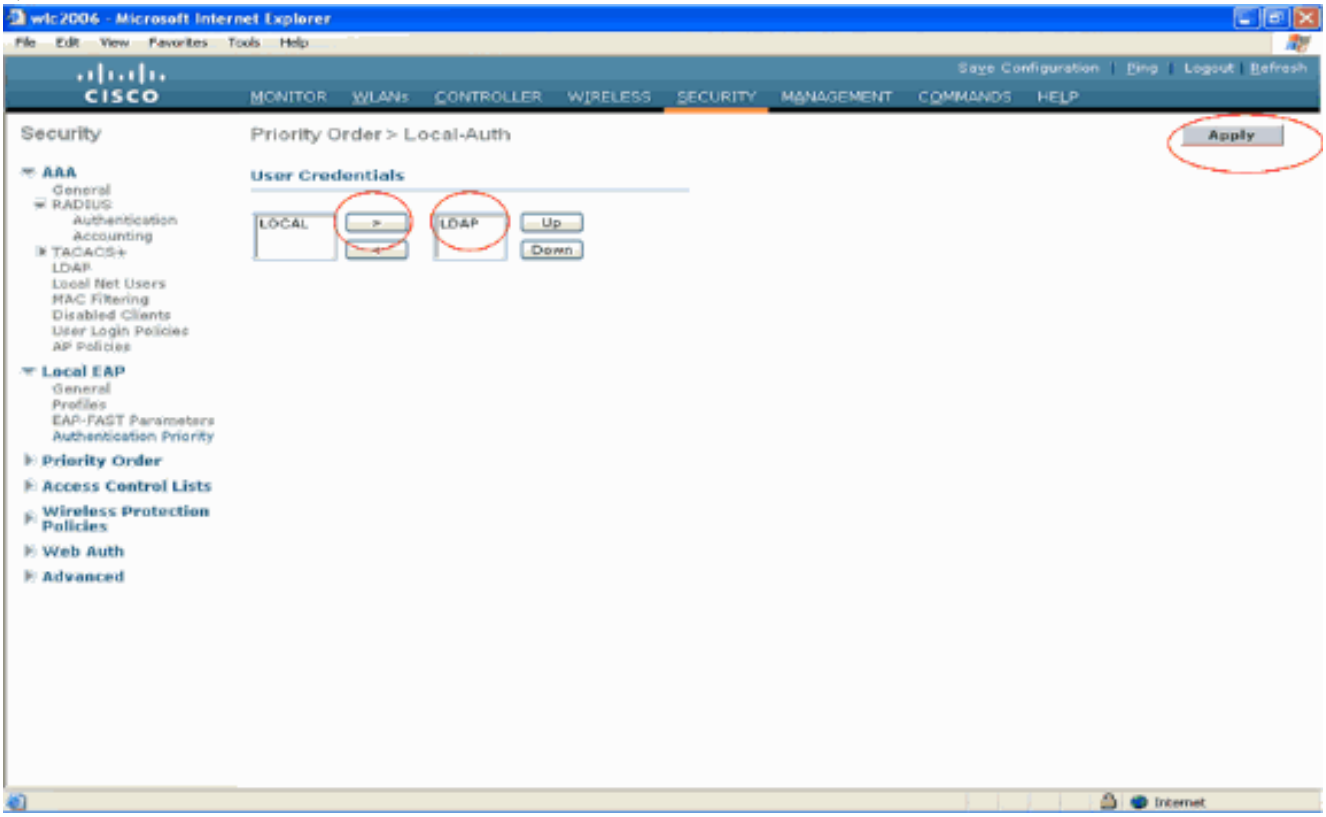
優先バックエンド データベースとしての LDAP の設定

LDAP を優先バックエンド データベースとして設定するには WLC で次の手順を実行します。

1. [Security] ページで [Local EAP] > [Authentication Priority] をクリックします。[Priority Order > Local-Auth] ページに、ユーザ クレデンシャルを保存できる 2 つのデータベース（ローカルと LDAP）が表示されます。LDAPを優先データベースにするには、左側のユーザクレデンシャルボックスから**LDAP**を選択し、**>**ボタンをクリックして、LDAPを右側の優先順ボックスに移動します。



2. この例では、左側のボックスで[LDAP]が選択され、[>]ボタンが選択されていることを明確に示しています。この結果、LDAP は優先順位を決定する右側のボックスに移動します。LDAP データベースが認証優先データベースとして選択されました。[Apply] をクリックします。



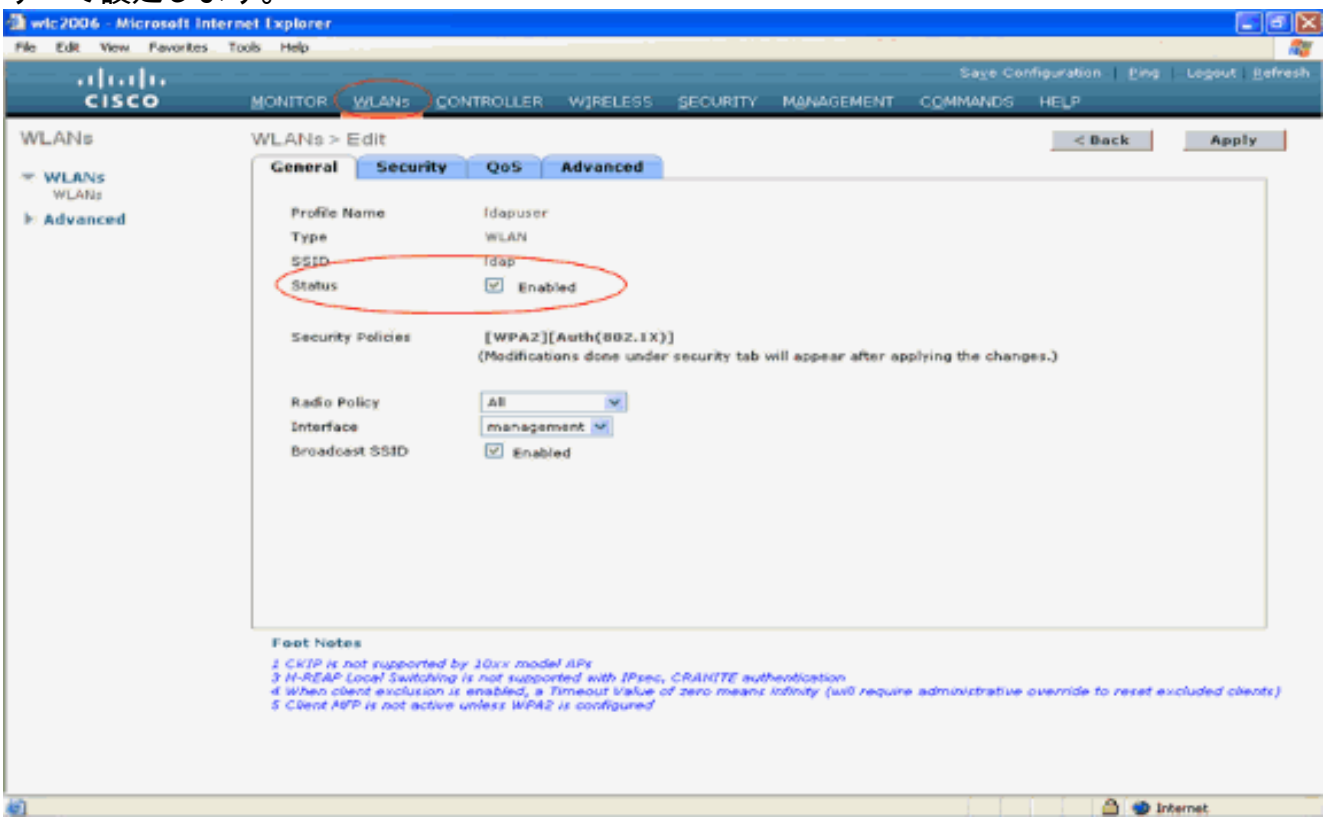
注：LDAPとLOCALの両方が右側の[User Credentials]ボックスに表示され、LDAPが上に、LOCALが下に表示されている場合、ローカルEAPはLDAPバックエンドデータベースを使用してクライアントの認証を試み、LDAPサーバに到達できない場合はローカルユーザデータベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が最上位にある場合、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われま

せん。

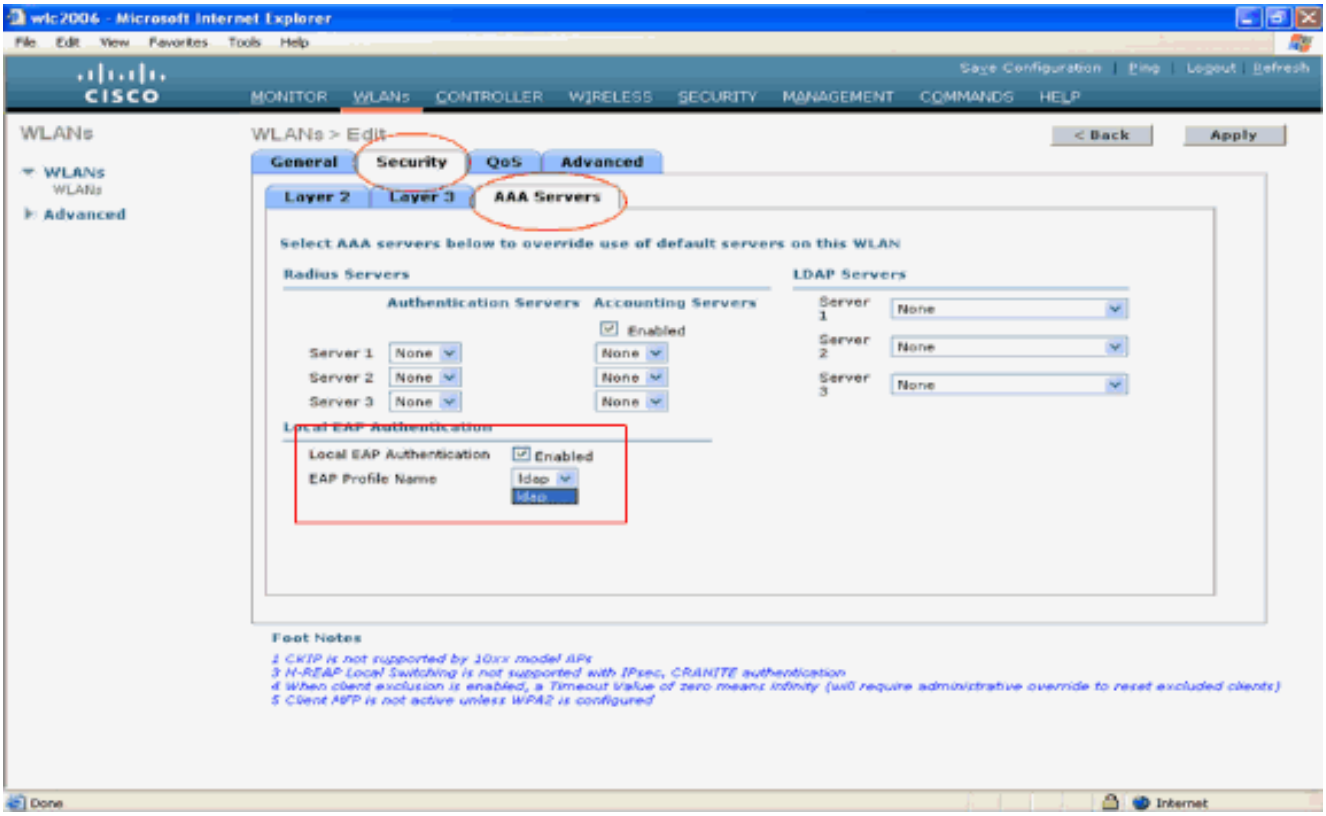
WLC でのローカル EAP 認証を使用する WLAN の設定

WLC で最後に行う操作は、バックエンド データベースとして LDAP を使用し、認証方式としてローカル EAP を使用する WLAN の設定です。次のステップを実行します。

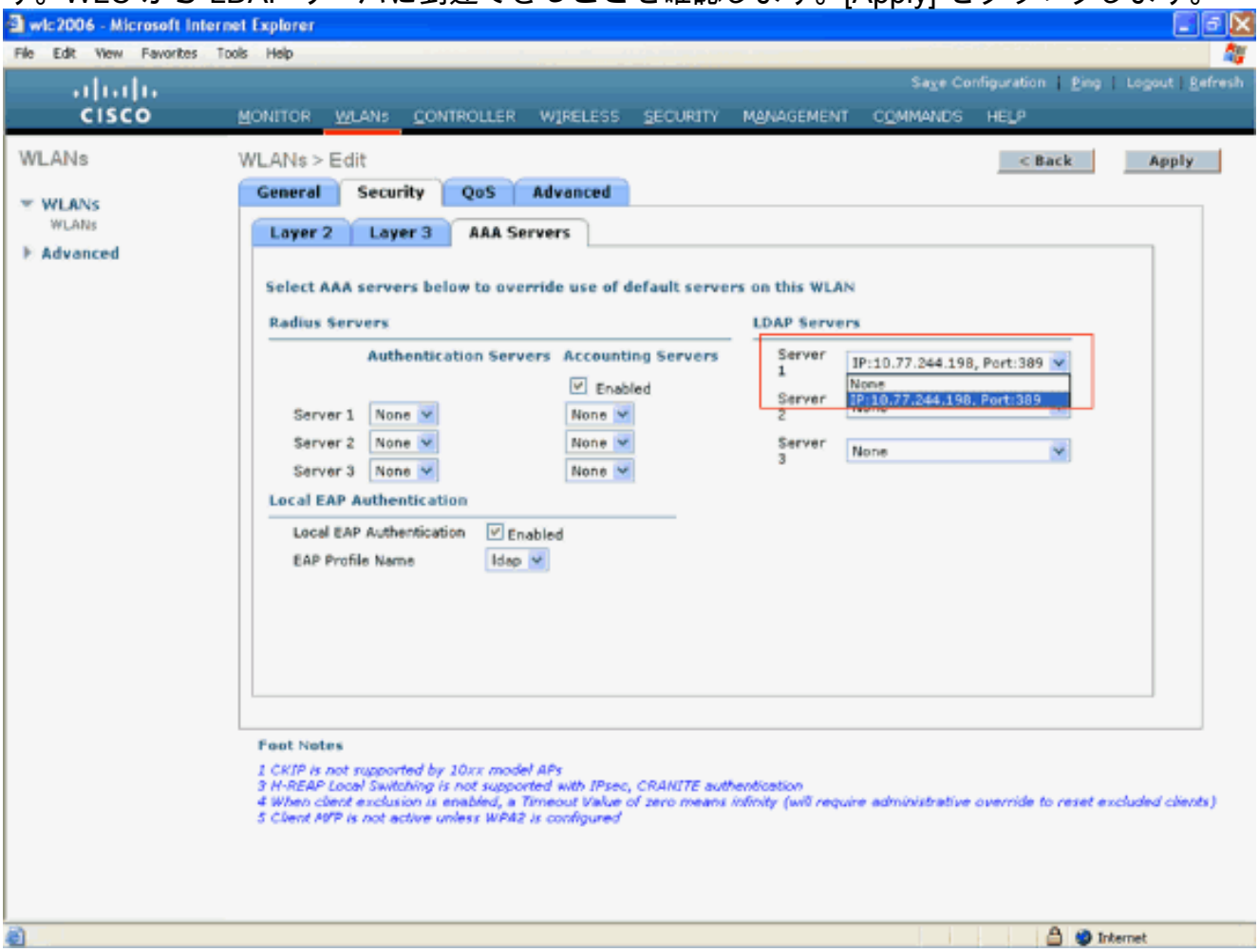
1. コントローラのメイン メニューで [WLANs] をクリックし、[WLANs] 設定ページに移動します。[WLANs] ページで [New] をクリックし、新しい WLAN を作成します。この例では新しい WLAN **ldap** を作成します。[Apply] をクリックします。次に、[WLANs > Edit] ページで WLAN パラメータを設定します。
2. WLAN 編集ページでこの WLAN の [Status] を有効にします。その他の必要なパラメータをすべて設定します。



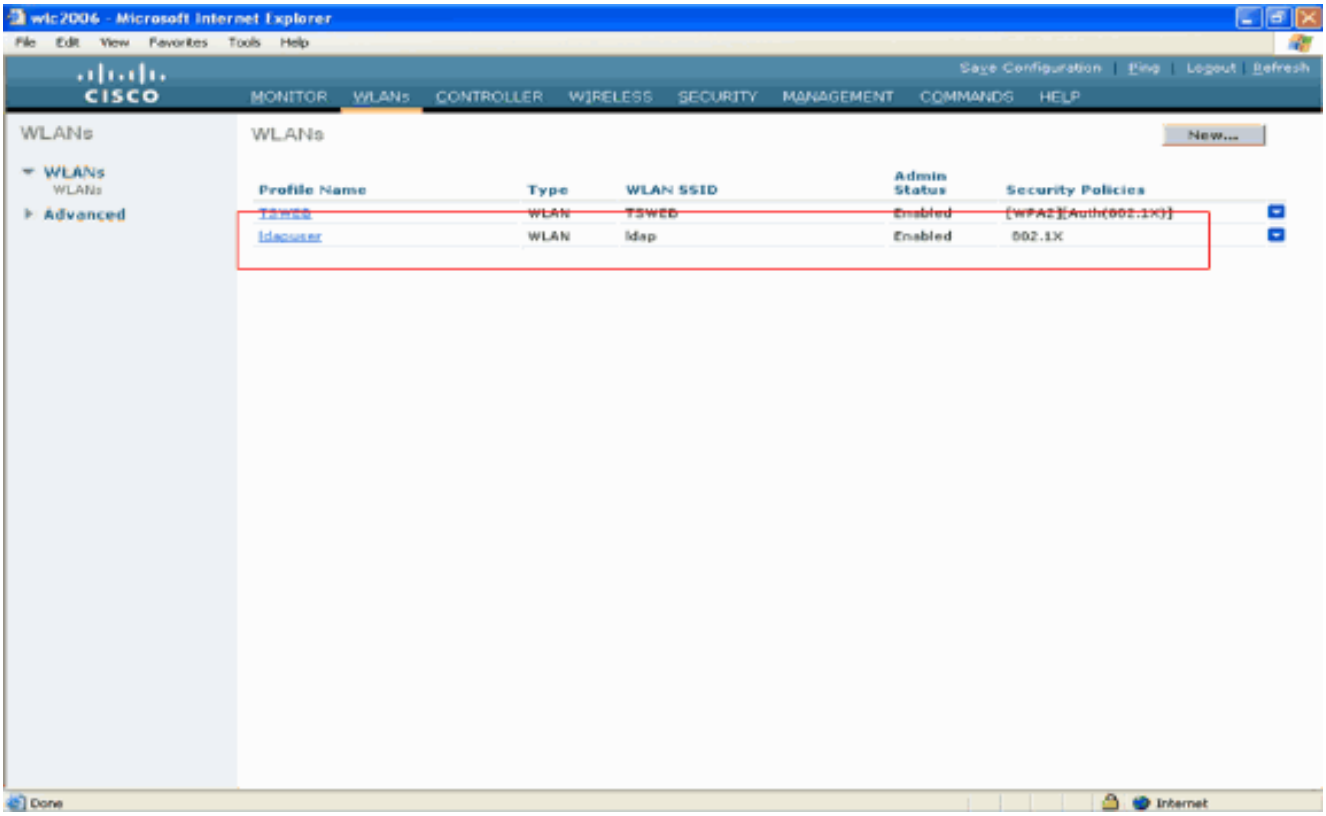
3. [Security] をクリックして、この WLAN のセキュリティ関連パラメータを設定します。この例ではレイヤ 2 セキュリティ 802.1x と 104 ビット ダイナミック WEP が使用されています。**注：このド**キュメントでは、例として802.1xとダイナミックWEPを使用します。実際にはより安全な認証方式（WPA/ WPA2 など）を使用することを推奨します。
4. WLAN セキュリティ設定ページで [AAA servers] タブをクリックします。[AAA Servers] ページで [Local EAP Authentication] を有効にし、[EAP Profile Name] パラメータのドロップダウン ボックスから [ldap] を選択します。これは、この例で作成したローカル EAP プロファイルです。



5. ドロップダウン ボックスから LDAP サーバ（WLC で以前に設定されたサーバ）を選択します。WLC から LDAP サーバに到達できることを確認します。[Apply] をクリックします。



6. WLC で新しい WLAN **ldap** が設定されました。この WLAN はローカル EAP 認証（この場合は EAP-FAST）を使用してクライアントを認証し、クライアント クレデンシャルの検証のために LDAP バックエンド データベースを照会します。



LDAP サーバの設定

WLC でローカル EAP が設定されました。次に、バックエンド データベースとして機能する LDAP サーバが、証明書検証が正常に完了した後でワイヤレス クライアントを認証するように設定します。

LDAP サーバ設定手順の最初のステップとして、LDAP サーバでユーザ データベースを作成します。これにより、WLC はユーザ認証時にこのデータベースを照会できます。

ドメイン コントローラでのユーザの作成

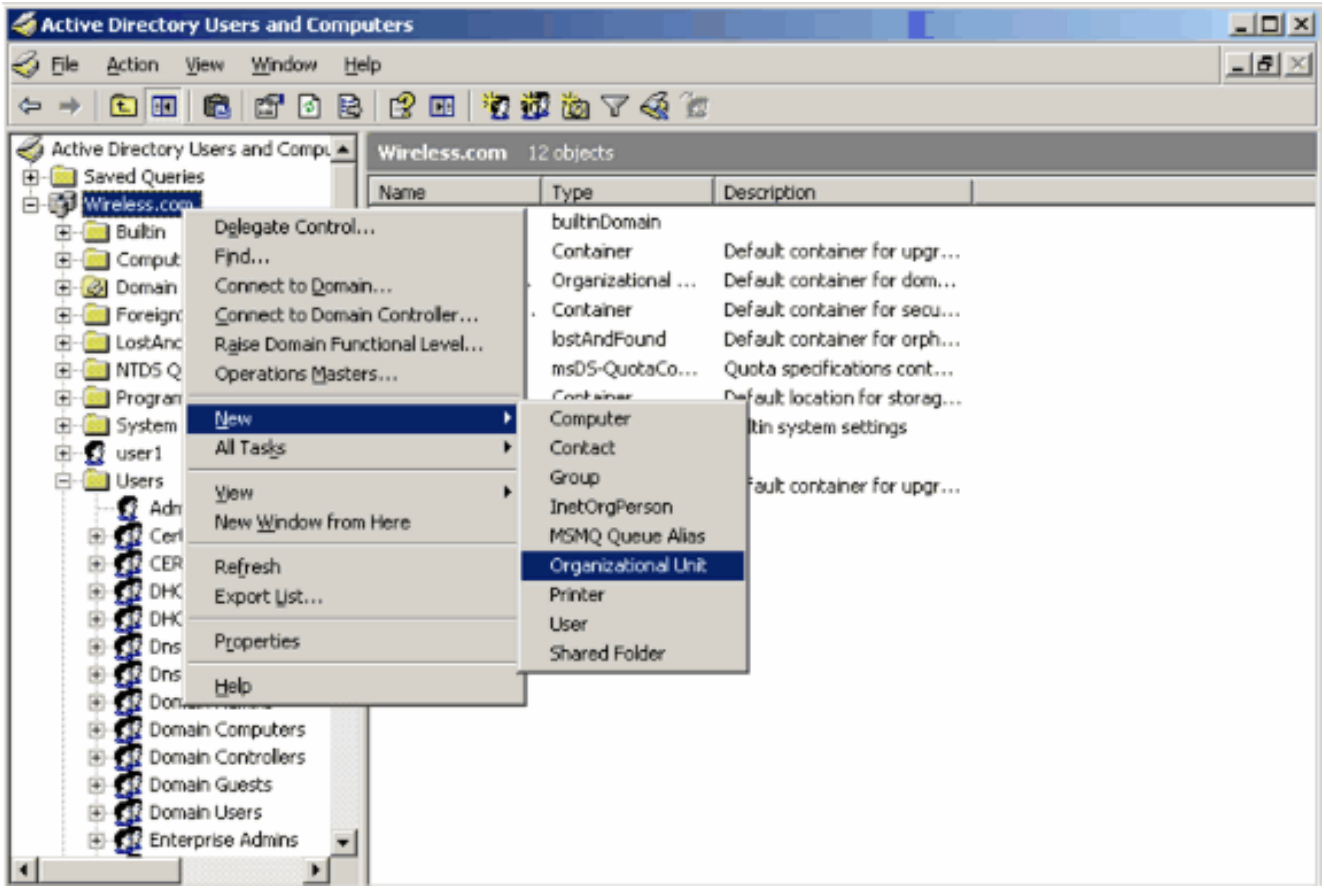
この例では新しい OU **ldapuser** が作成され、この OU の中にユーザ **user2** が作成されました。このユーザに対して LDAP アクセスを設定することで、WLC はユーザ認証でこの LDAP データベースを照会できます。

この例で使用するドメインは **wireless.com** です。

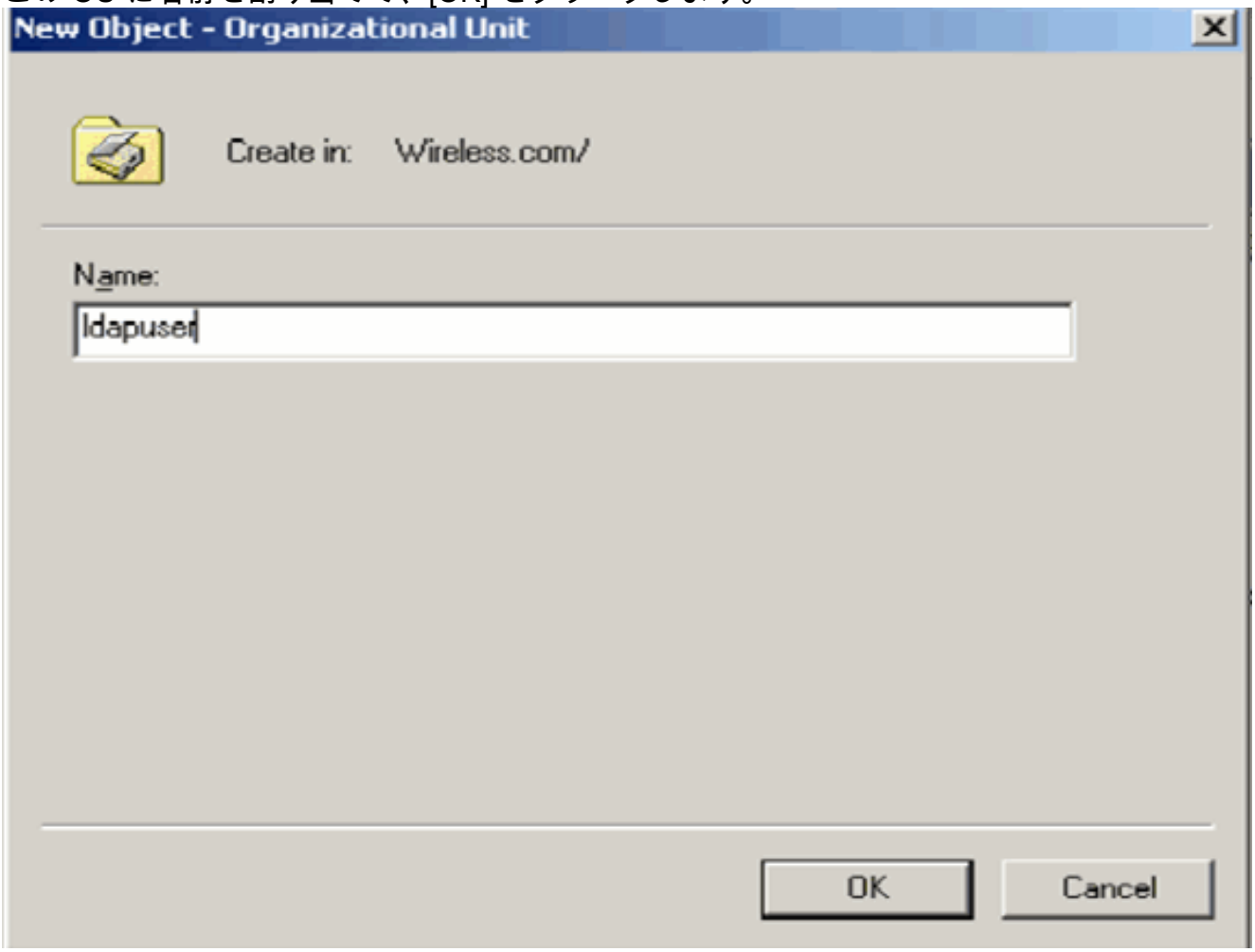
OU でのユーザ データベースの作成

この項では、ドメインに新しい OU を作成し、この OU の中に新しいユーザを作成する手順を説明します。

1. ドメイン コントローラで [Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] をクリックし、[Active Directory Users and Computers] 管理コンソールを起動します。
2. 新しい OU を作成するため、ドメイン名（この例では wireless.com）を右クリックし、コンテキスト メニューから [New] > [Organizational Unit] を選択します。

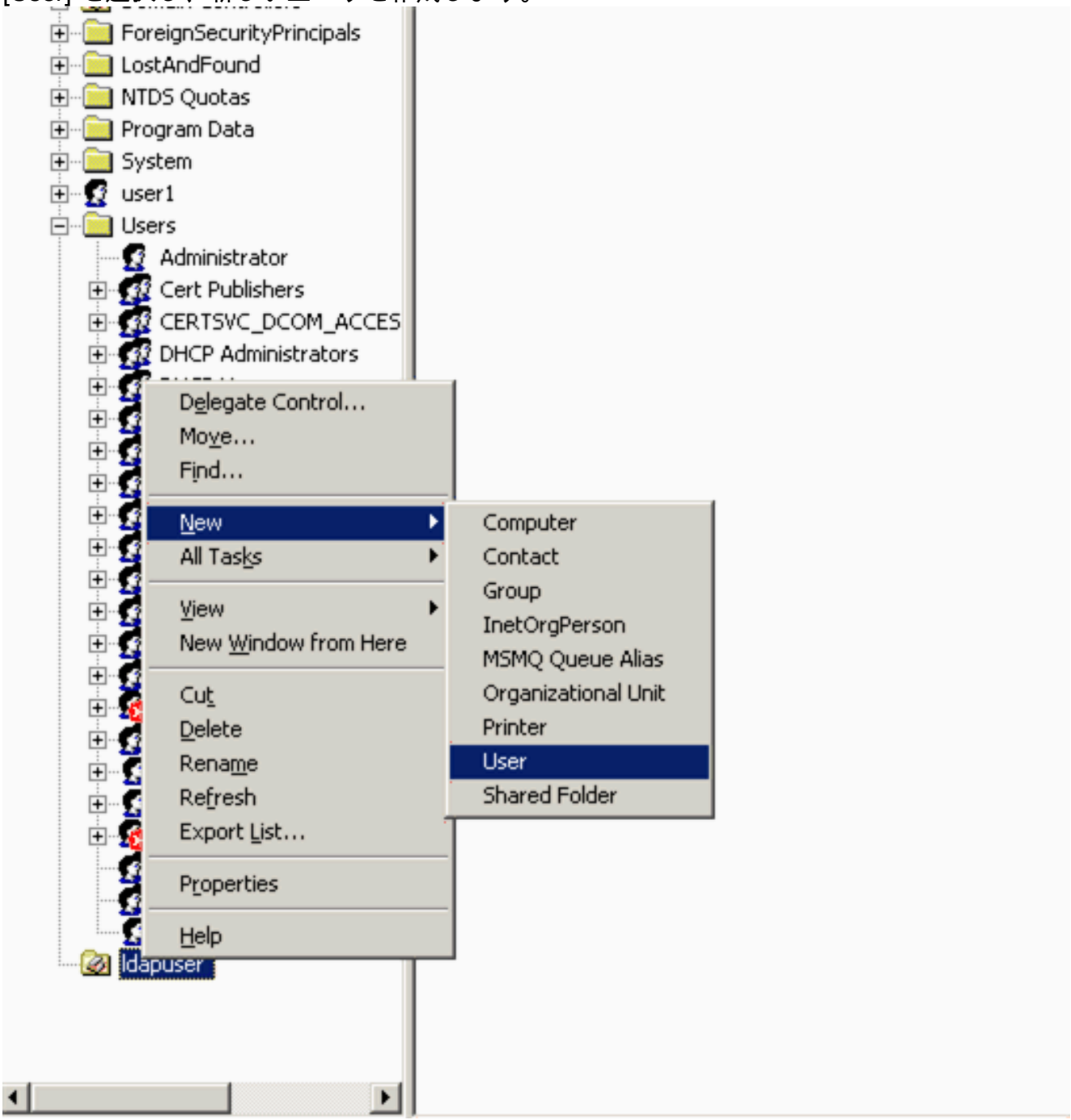


3. この OU に名前を割り当てて、[OK] をクリックします。

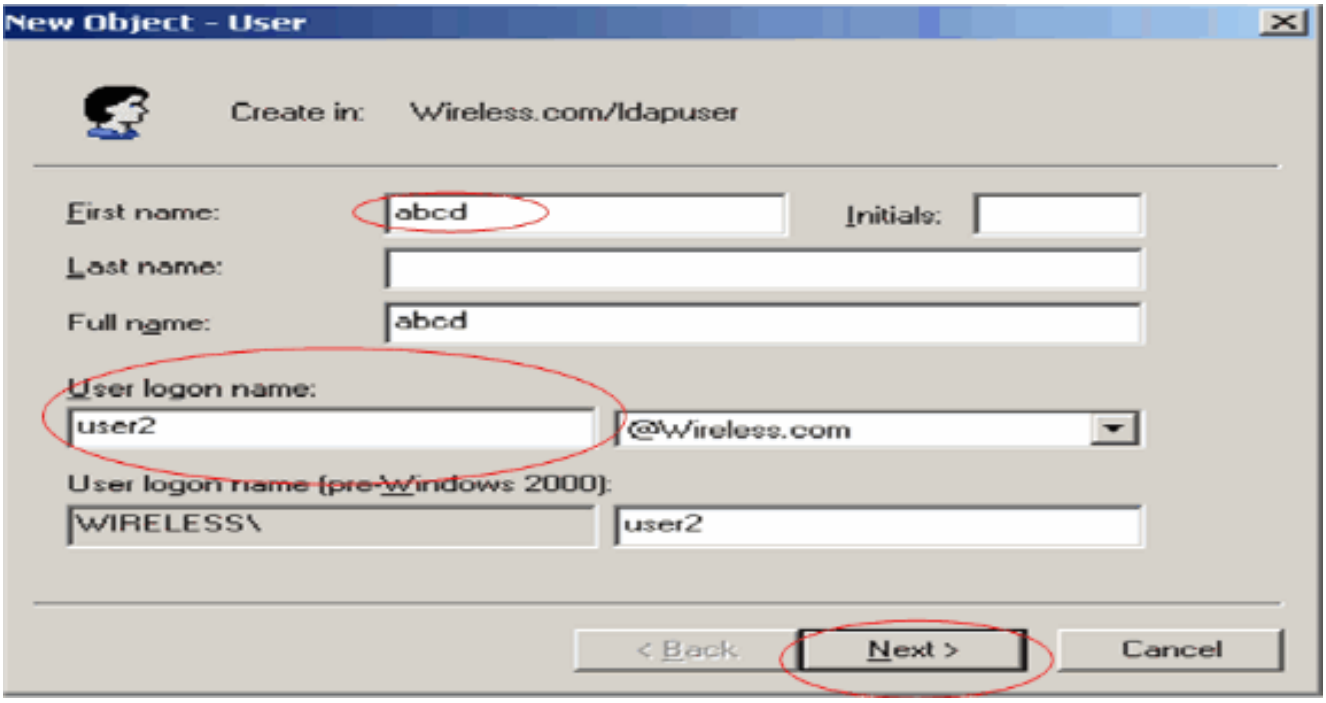


LDAP サーバに新しい OU **ldapuser** が作成されました。次にこの OU の中にユーザ **user2** を作成します。これを行うには、次の手順を実行します。

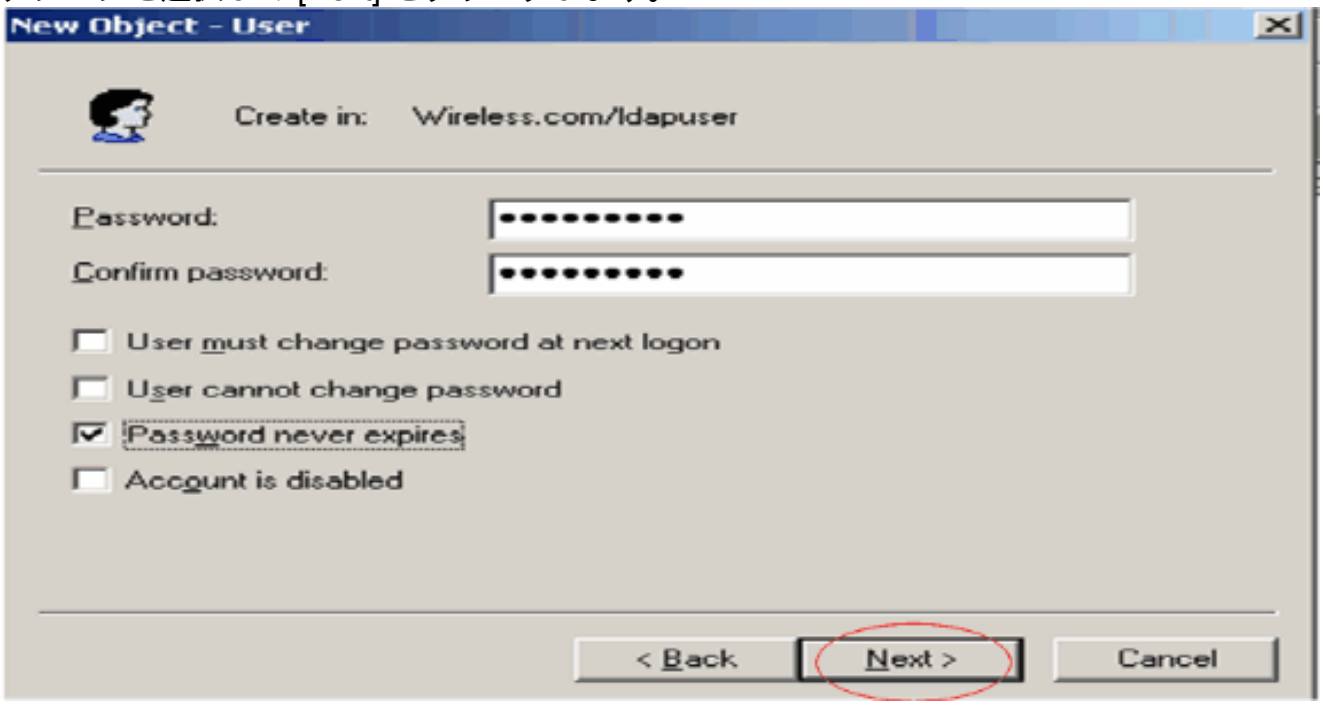
1. 作成した新しい OU 上で右クリックします。表示されるコンテキスト メニューから [New] > [User] を選択し、新しいユーザを作成します。



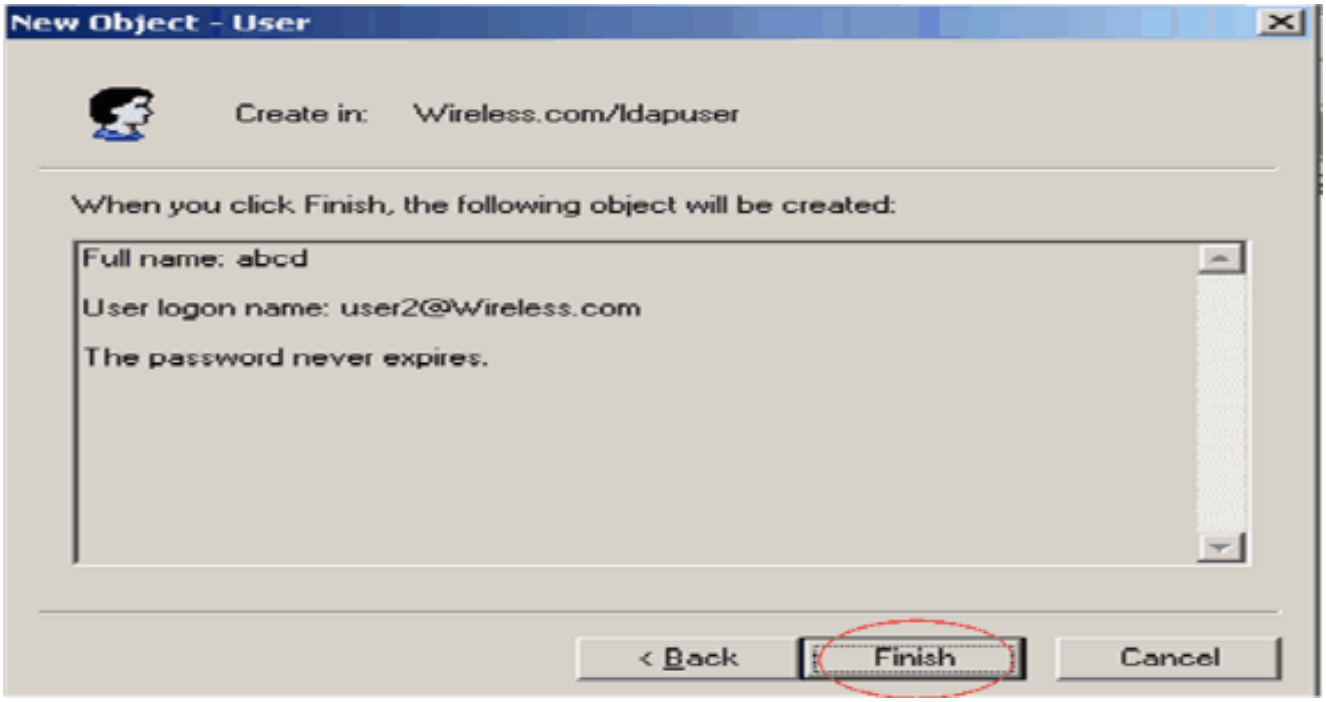
2. 次の例に示すように、ユーザ設定ページで必須フィールドに情報を入力します。次の例では [User logon name] に **user2** が設定されています。これは、クライアント認証時に LDAP データベースで検証されるユーザ名です。次の例では [First name] と [Last name] に **abcd** が設定されています。[next] をクリックします。



3. パスワードを入力し、確認のためのパスワードを入力します。[Password never expires] オプションを選択して [Next] をクリックします。



4. [Finish] をクリックします。新しいユーザ **user2** が OU **ldapuser** に作成されます。このユーザのクレデンシャルを次に示します。ユーザ名：**user2**パスワード：**Laptop123**



これで OU の中にユーザが作成されました。次に、このユーザの LDAP アクセスを設定します。

ユーザの LDAP アクセスの設定

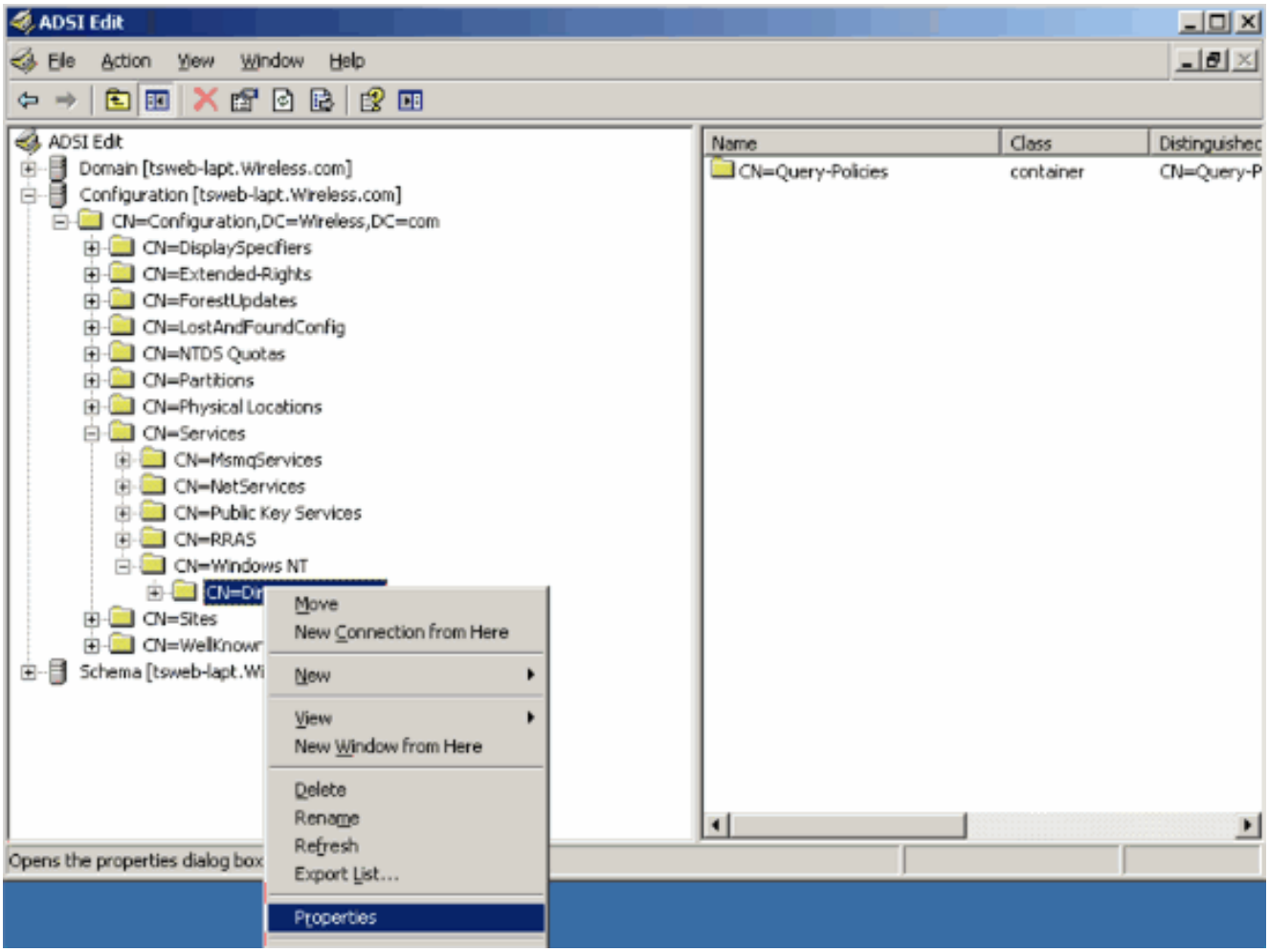
ユーザの LDAP アクセスを設定するには、ここで説明する手順を実行します。

Windows 2003 サーバでの匿名バインド機能の有効化

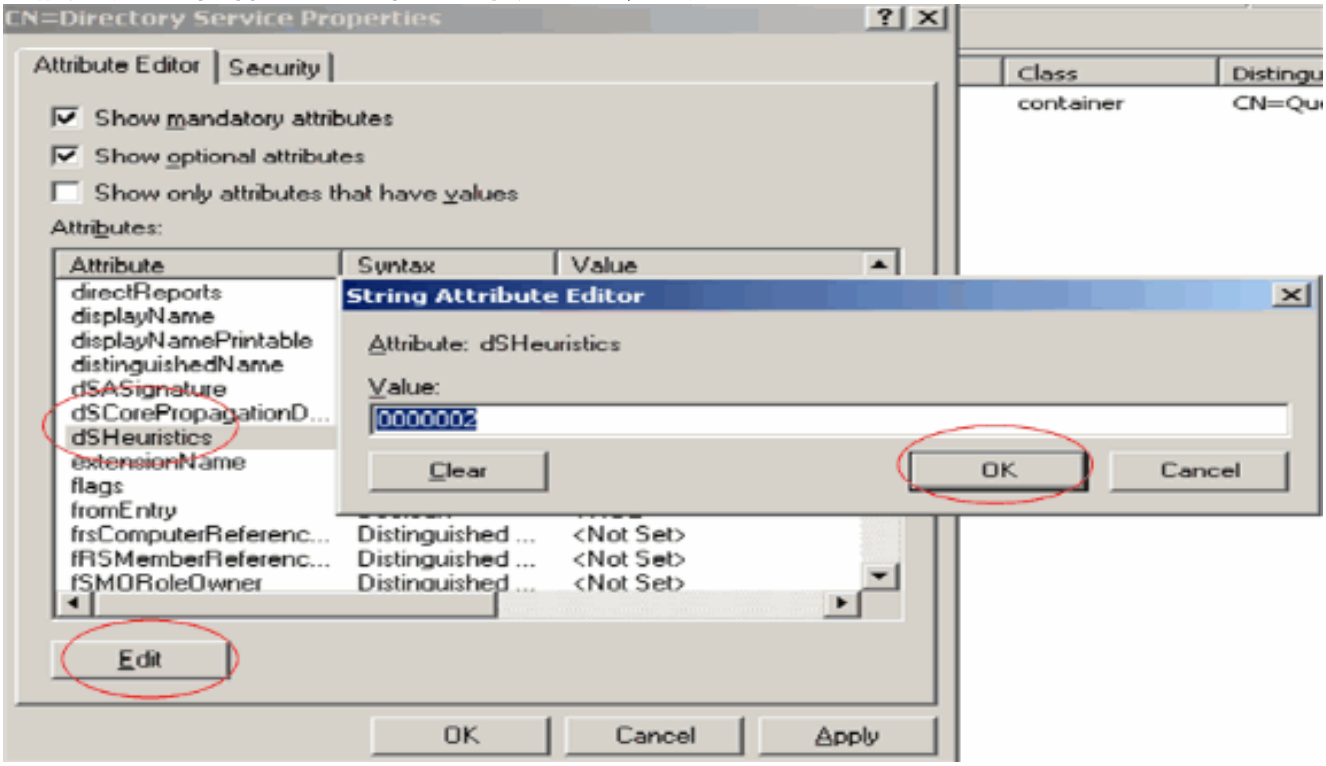
すべてのサードパーティ アプリケーションが LDAP で Windows 2003 AD にアクセスできるようにするには、Windows 2003 で匿名バインド機能が有効になっている必要があります。デフォルトでは、Windows 2003 ドメイン コントローラでは匿名 LDAP 操作は許可されていません。

匿名バインド機能を有効にするには、次の手順を実行します。

1. [Start] > [Run] > [Type] にADSI Edit.mscと入力して、**ADSI Edit**ツールを起動します。このツールは、Windows 2003 サポート ツールの 1 つです。
2. [ADSI Edit] ウィンドウでルート ドメイン（ Configuration [tsweb-lapt.Wireless.com] ）を展開します。[CN=Services] > [CN=Windows NT] > [CN=Directory Service] を展開します。[CN=Directory Service] コンテナを右クリックし、コンテキスト メニューから [Properties] を選択します。



3. [CN=Directory Service Properties] ウィンドウで [Attribute] フィールドの下にある [dsHeuristics] 属性をクリックし、[Edit] を選択します。この属性の [String Attribute Editor] ウィンドウに値 **0000002** を入力して [Apply] をクリックし、[OK] をクリックします。Windows 2003 サーバで匿名バインド機能が有効になりました。**注：最後の**（7番目の）文字は、LDAPサービスにバインドする方法を制御するものです。7 番目の文字が「0」または 7 番目の文字がない場合は、匿名 LDAP 操作が無効になっています。**7 番目の文字を「2」に設定すると匿名バインド機能が有効になります。**

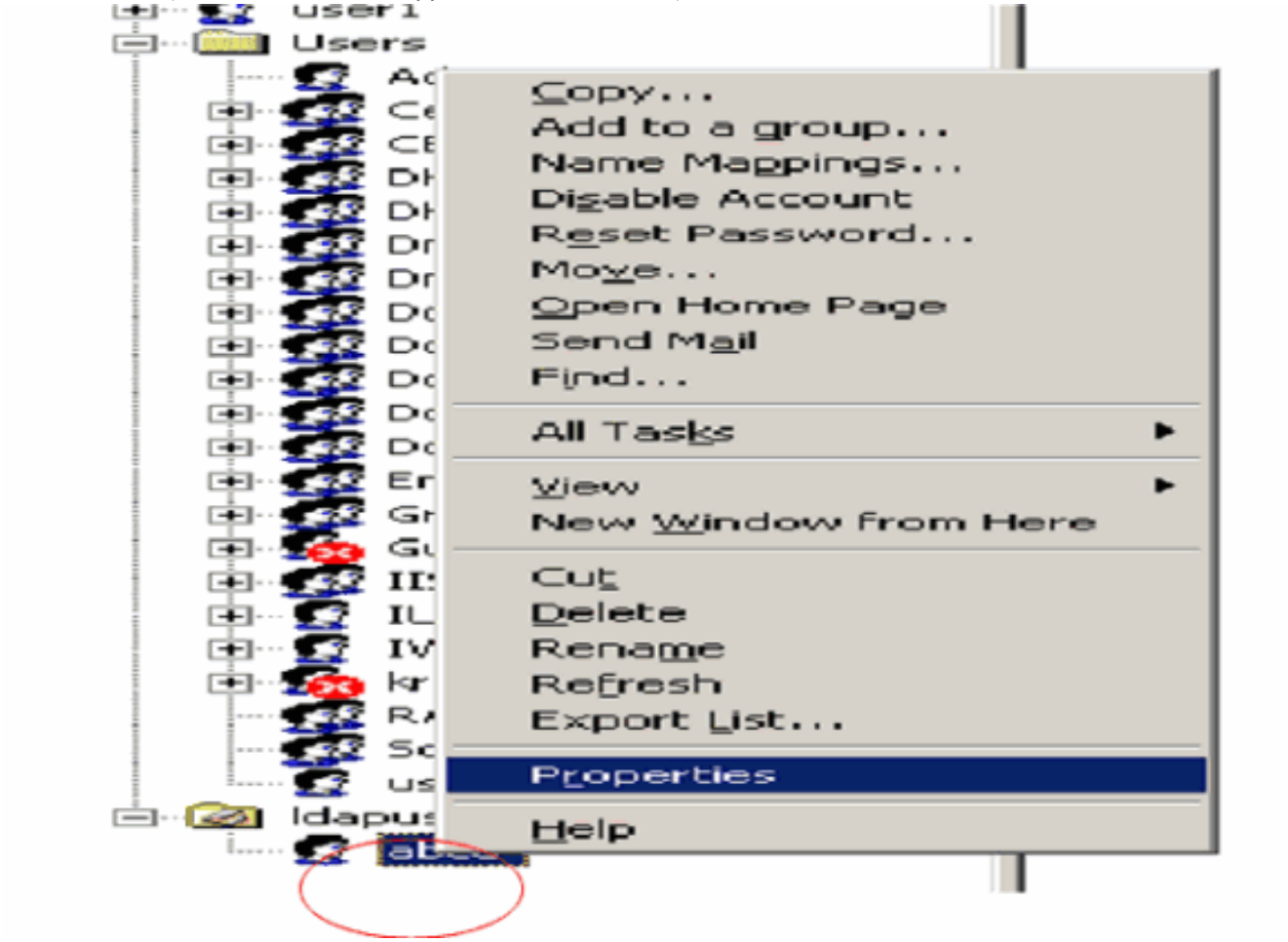


注：この属性に既に値が含まれている場合は、左側から7番目の文字のみを変更してください。匿名バインドを有効にするために変更が必要なのはこの文字だけです。たとえば現行値が「0010000」の場合は「0010002」に変更する必要があります。現在の値が7文字未満の場合は、使用していない場所にゼロを入力する必要があります。「001」は「0010002」になります。

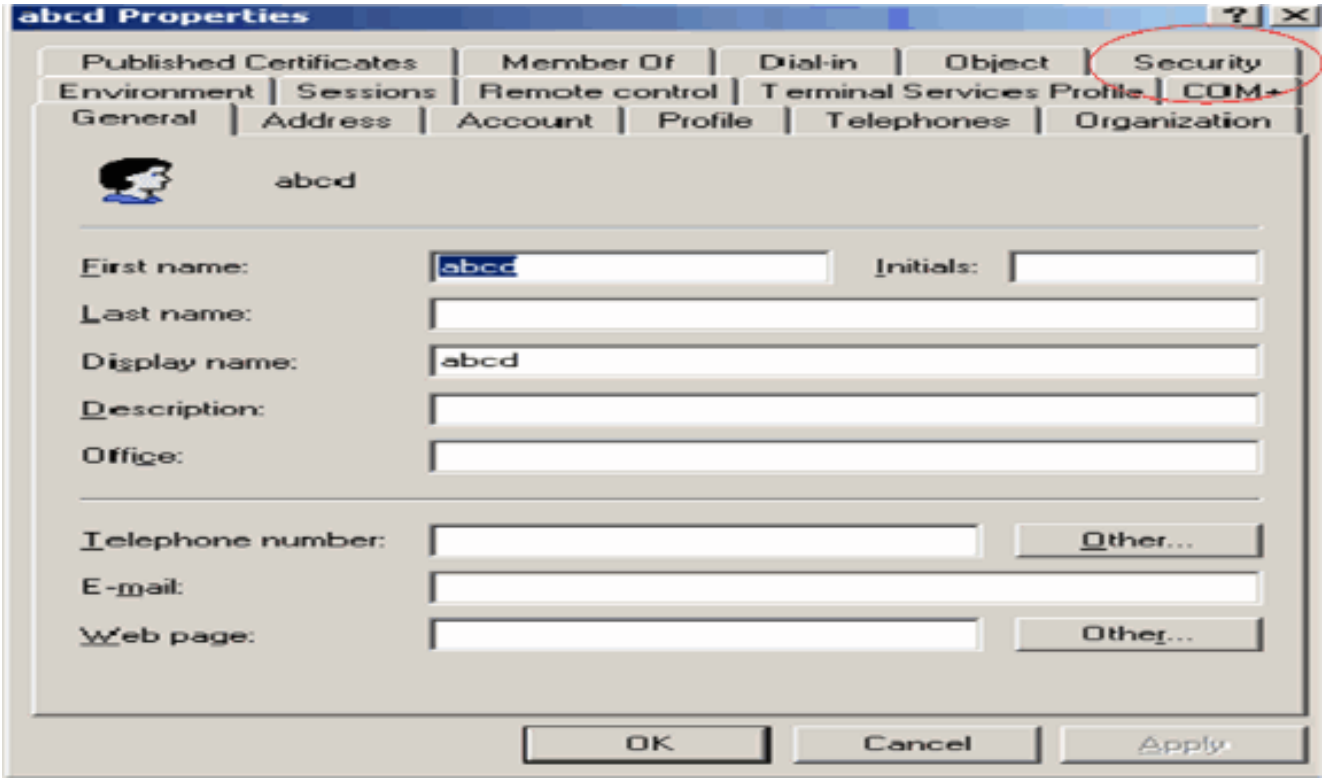
ユーザ「user2」への ANONYMOUS LOGON アクセス権限の付与

次に、ANONYMOUS LOGON アクセス権限をユーザ user2 に付与します。これを行うには、次の手順を実行します。

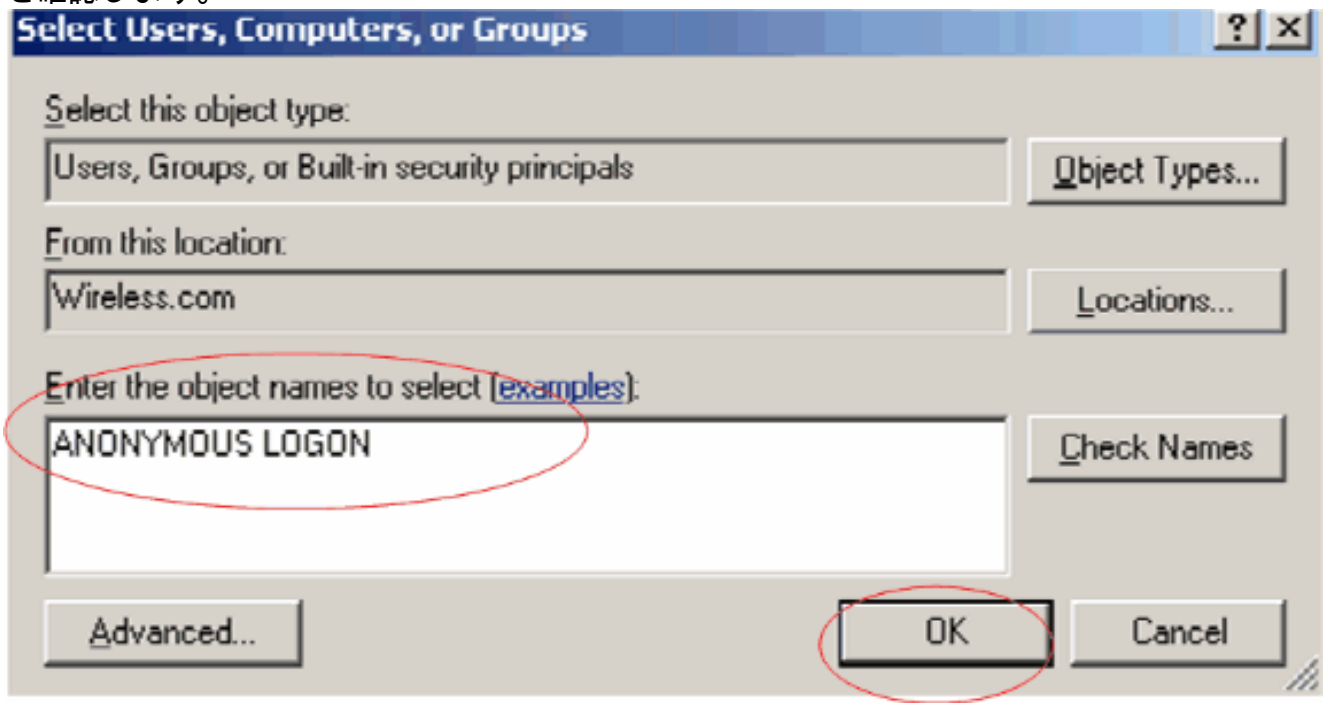
1. [Active Directory Users and Computers] を開きます。
2. [View Advanced Features] にチェックマークが付いていることを確認します。
3. ユーザ user2 にナビゲートして右クリックします。コンテキスト メニューから [Properties] を選択します。このユーザの名前は「abcd」です。



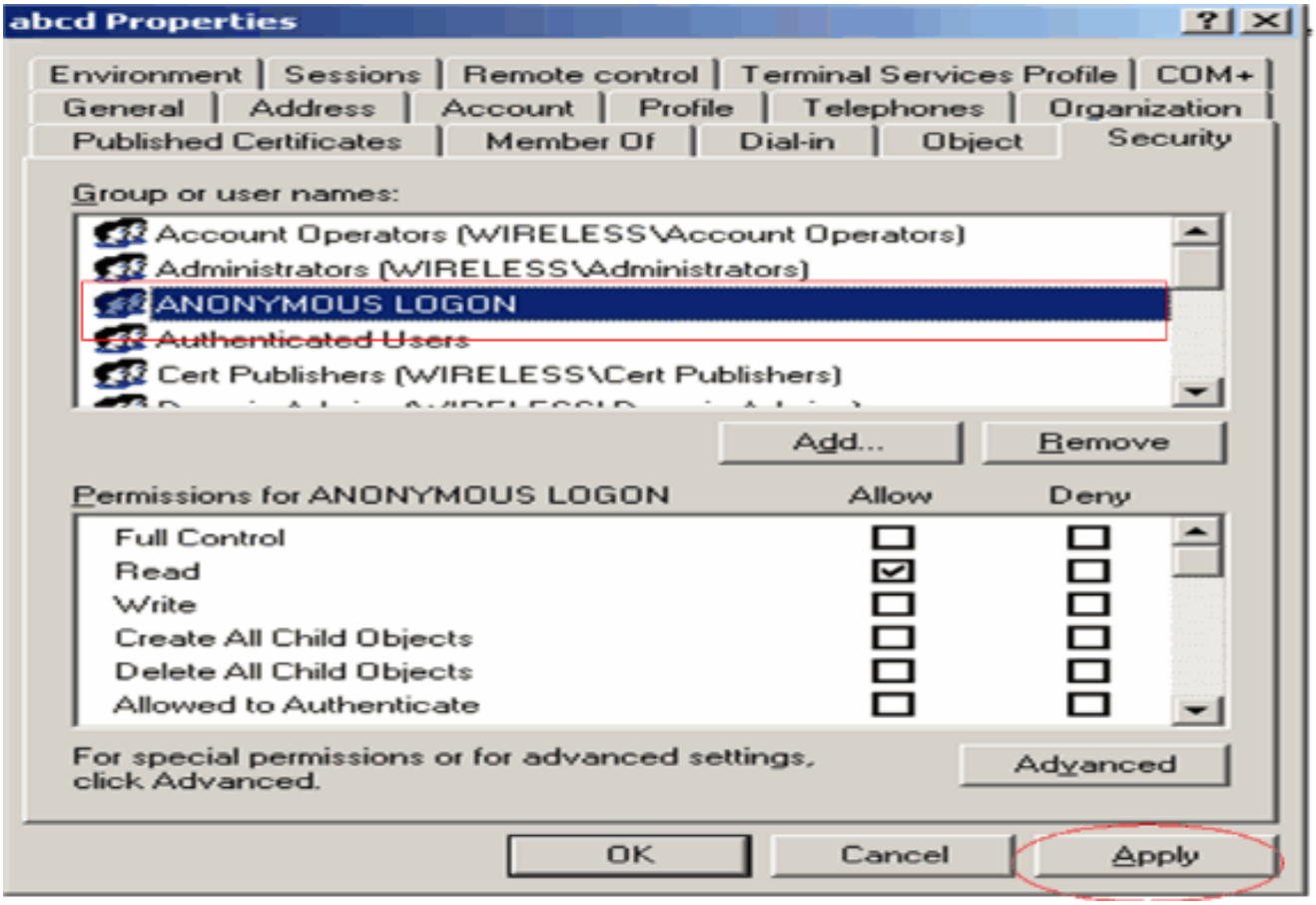
4. [abcd Properties] ウィンドウの [Security] に移動します。



5. 表示されるウィンドウで [Add] をクリックします。
6. [Enter the object names to select] ボックスに **ANONYMOUS LOGON** と入力し、ダイアログを確認します。



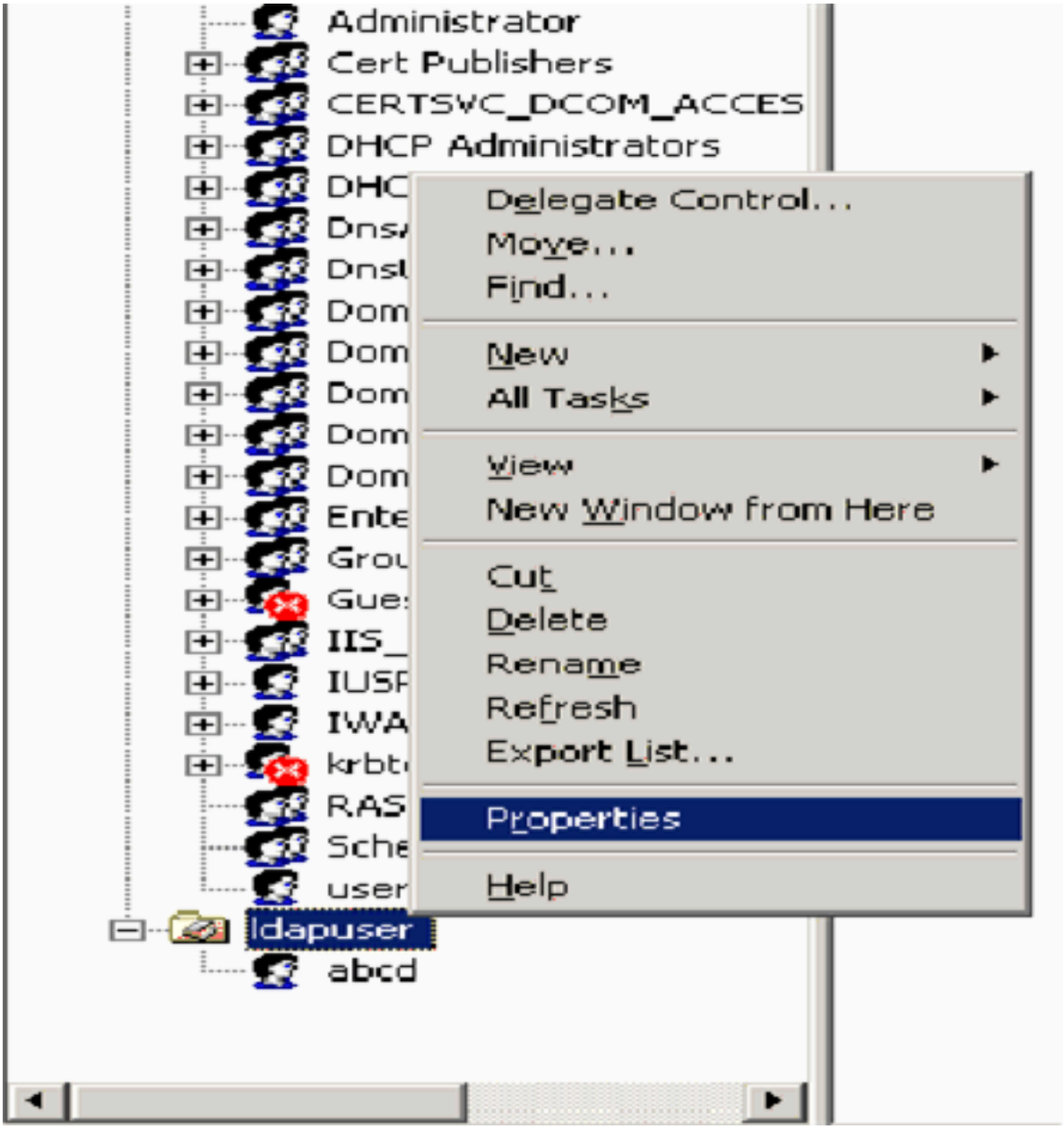
7. ACL で **ANONYMOUS LOGON** がユーザの一部のプロパティ セットにアクセスできることがわかります。[OK] をクリックします。ANONYMOUS LOGON アクセス権限がこのユーザに付与されます。



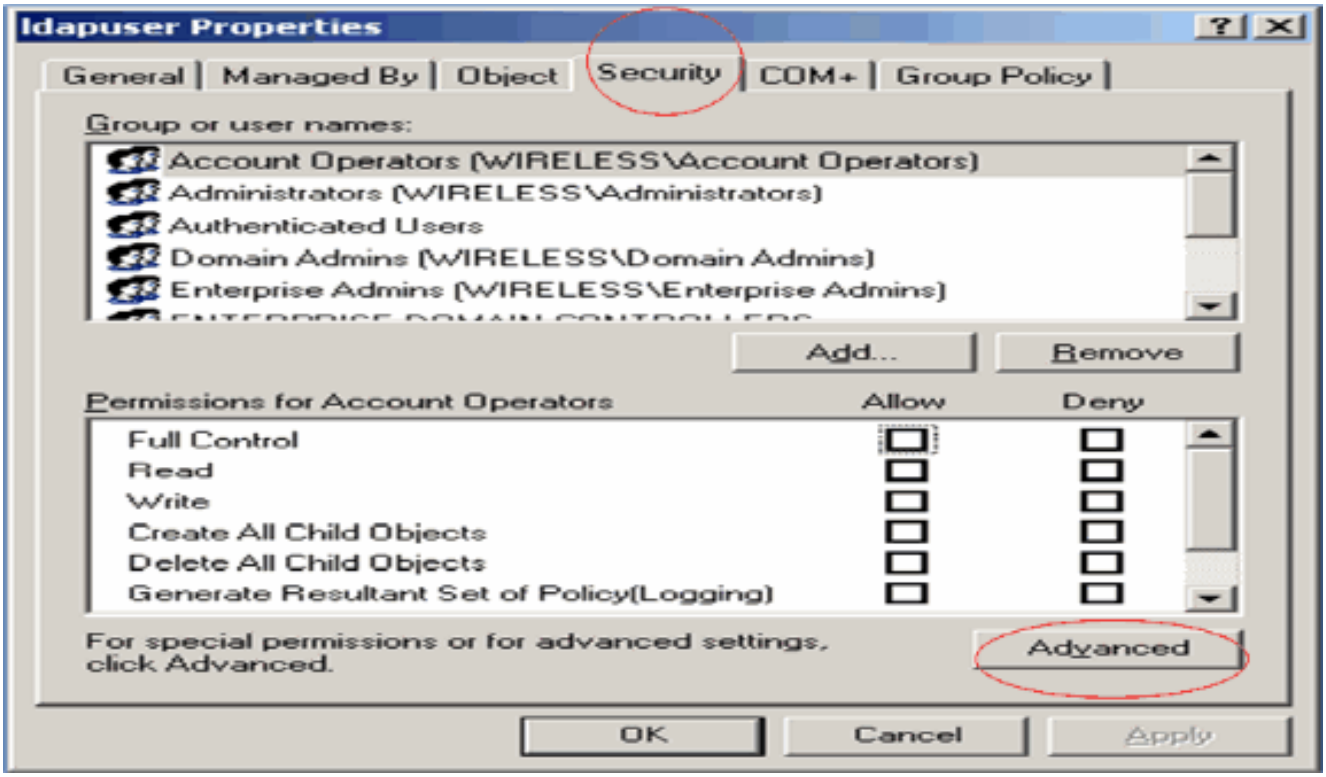
OU での List Contents 権限の付与

次に、ユーザが含まれている OU で **ANONYMOUS LOGON** に **List Contents** 権限を付与します。この例では OU「ldapuser」にユーザ「user2」が含まれています。これを行うには、次の手順を実行します。

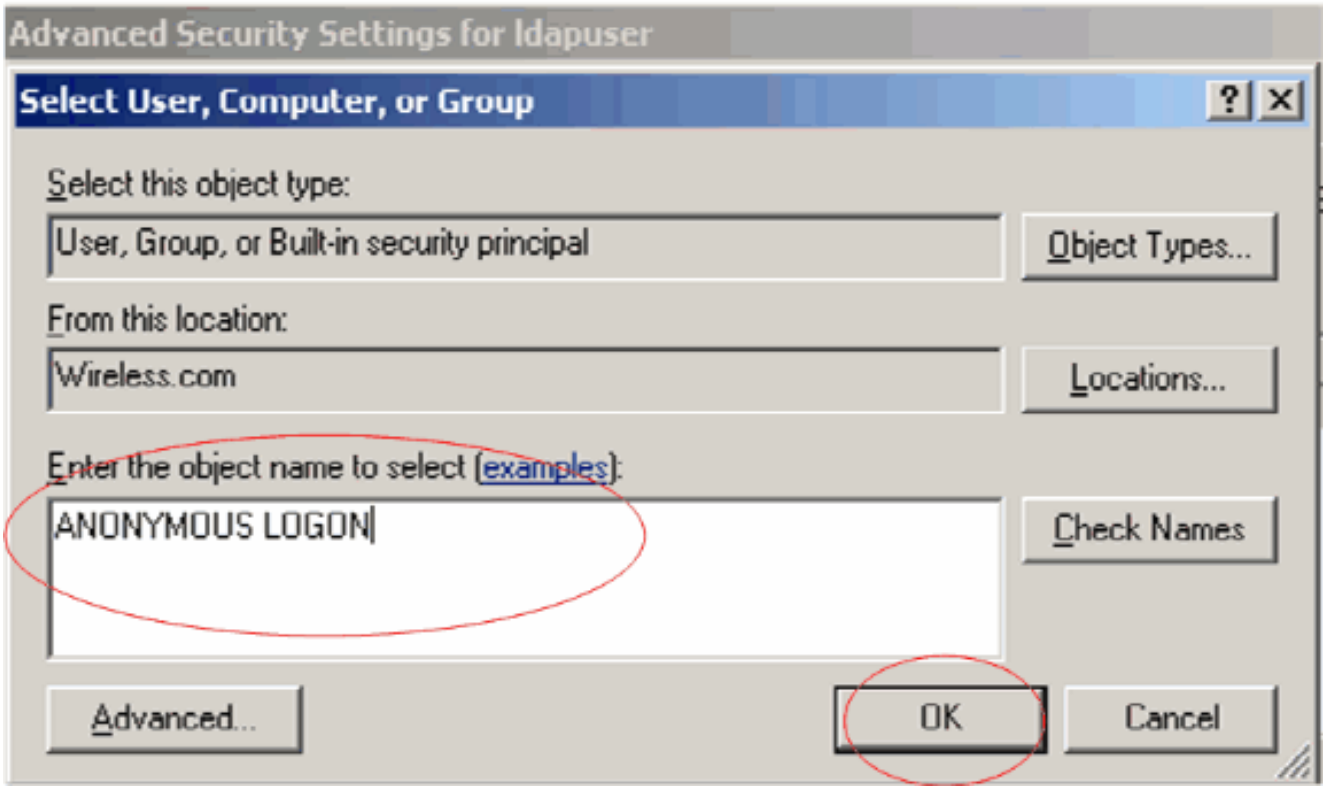
1. [Active Directory Users and Computers] で OU **ldapuser** を右クリックして [Properties] を選択します。



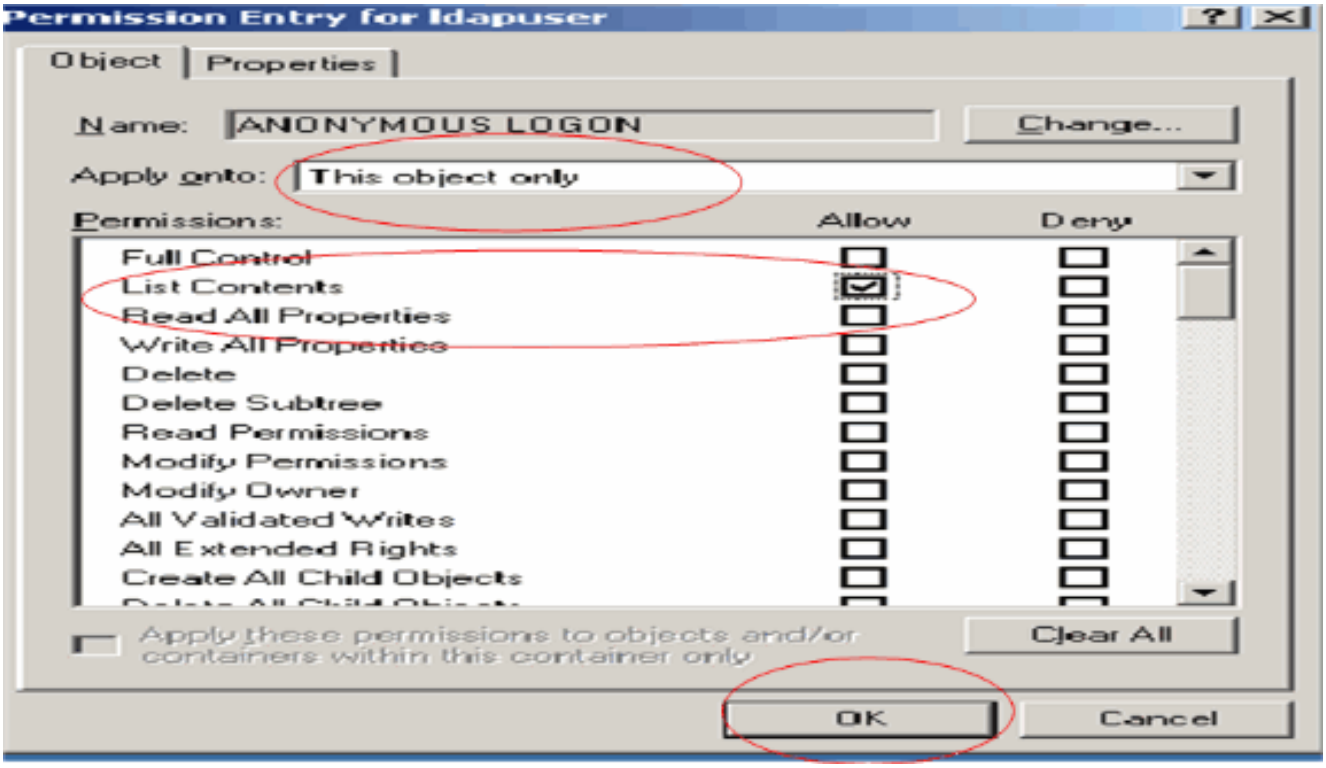
2. [Security] をクリックし、次に [Advanced] をクリックします。



3. [Add] をクリックします。表示されるダイアログに ANONYMOUS LOGON と入力します。



4. ダイアログの内容を確認します。新しいダイアログ ウィンドウが表示されます。
5. [Apply onto] ドロップダウン ボックスで [This object only] を選択し、[List Contents] の [Allow] チェックボックスにチェックマークを付けます。

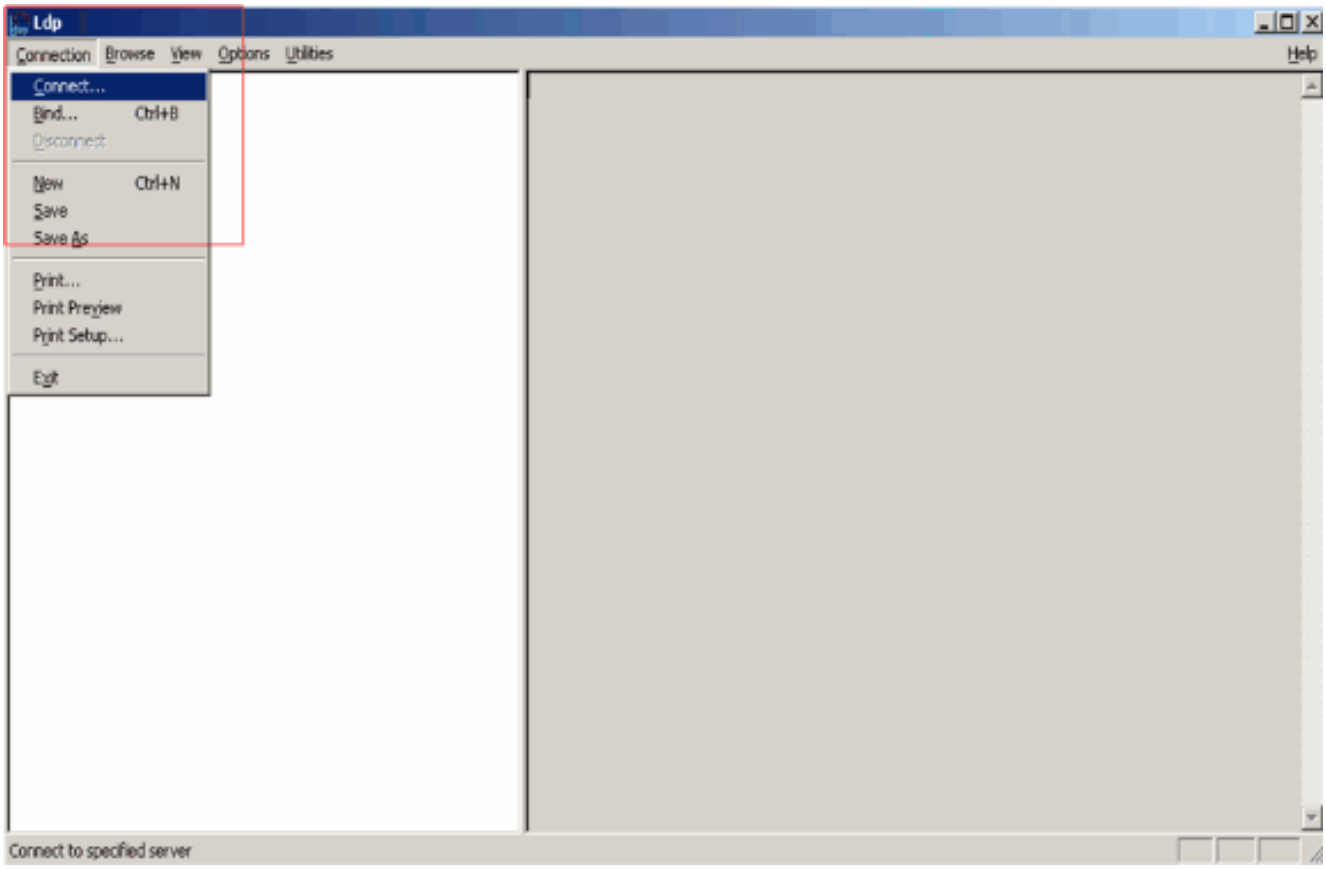


LDP を使用したユーザ属性の確認

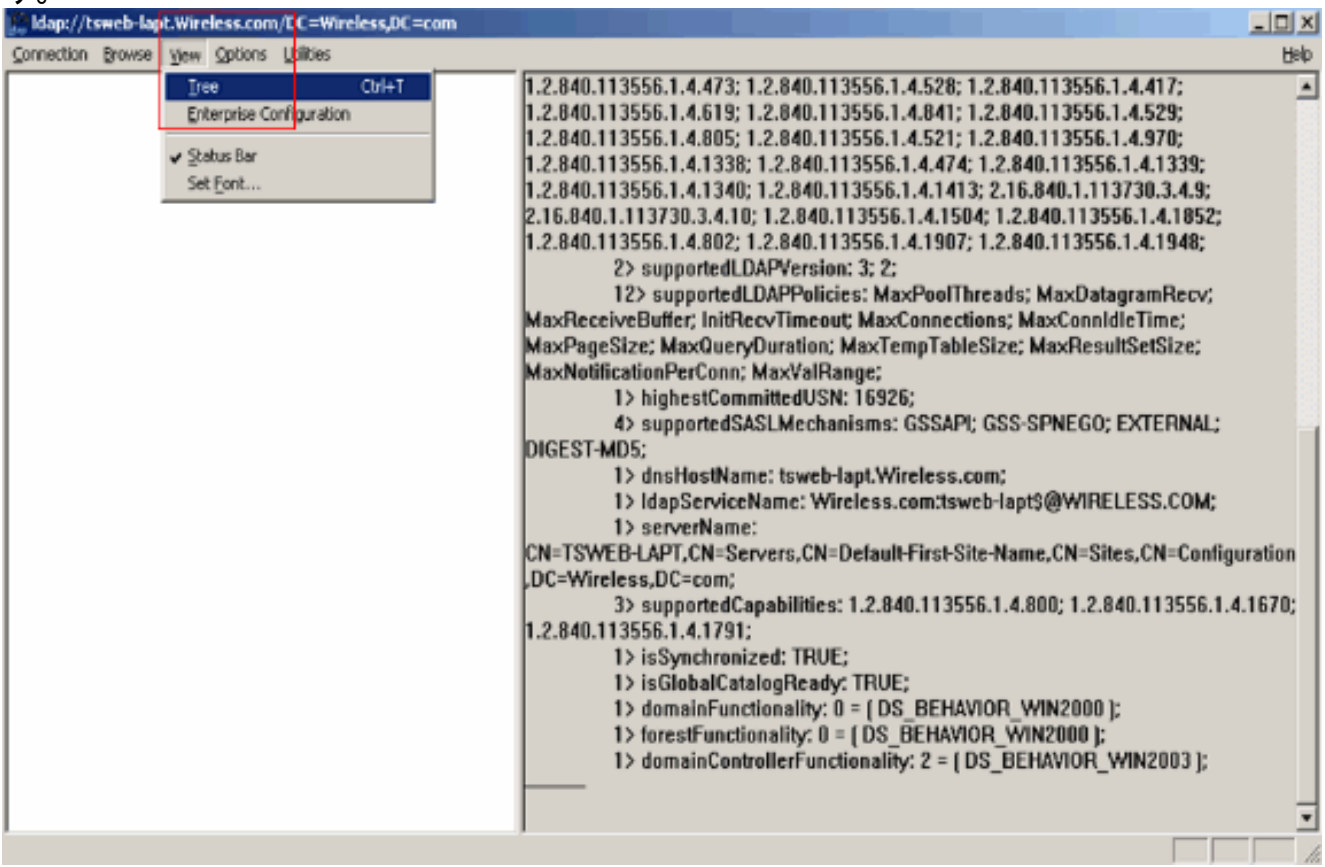
この GUI ツールは、ユーザがすべての LDAP 互換ディレクトリ（Active Directory など）に対して操作（接続、バインド、変更、追加、削除など）を実行できるようにする LDAP クライアントです。LDP では、Active Directory に格納されているオブジェクトとそのメタデータ（セキュリティ記述子やレプリケーション メタデータなど）を表示できます。

LDP GUI ツールは、製品 CD から Windows Server 2003 Support Tools をインストールするとインストールされます。この項では、LDP ユーティリティを使用してユーザ **user2** に関連付けられている特定の属性を確認する方法について説明します。一部の属性は、WLC で LDAP サーバ設定パラメータ（ユーザ属性タイプ、ユーザ オブジェクトタイプなど）の値を入力するときに使用されます。

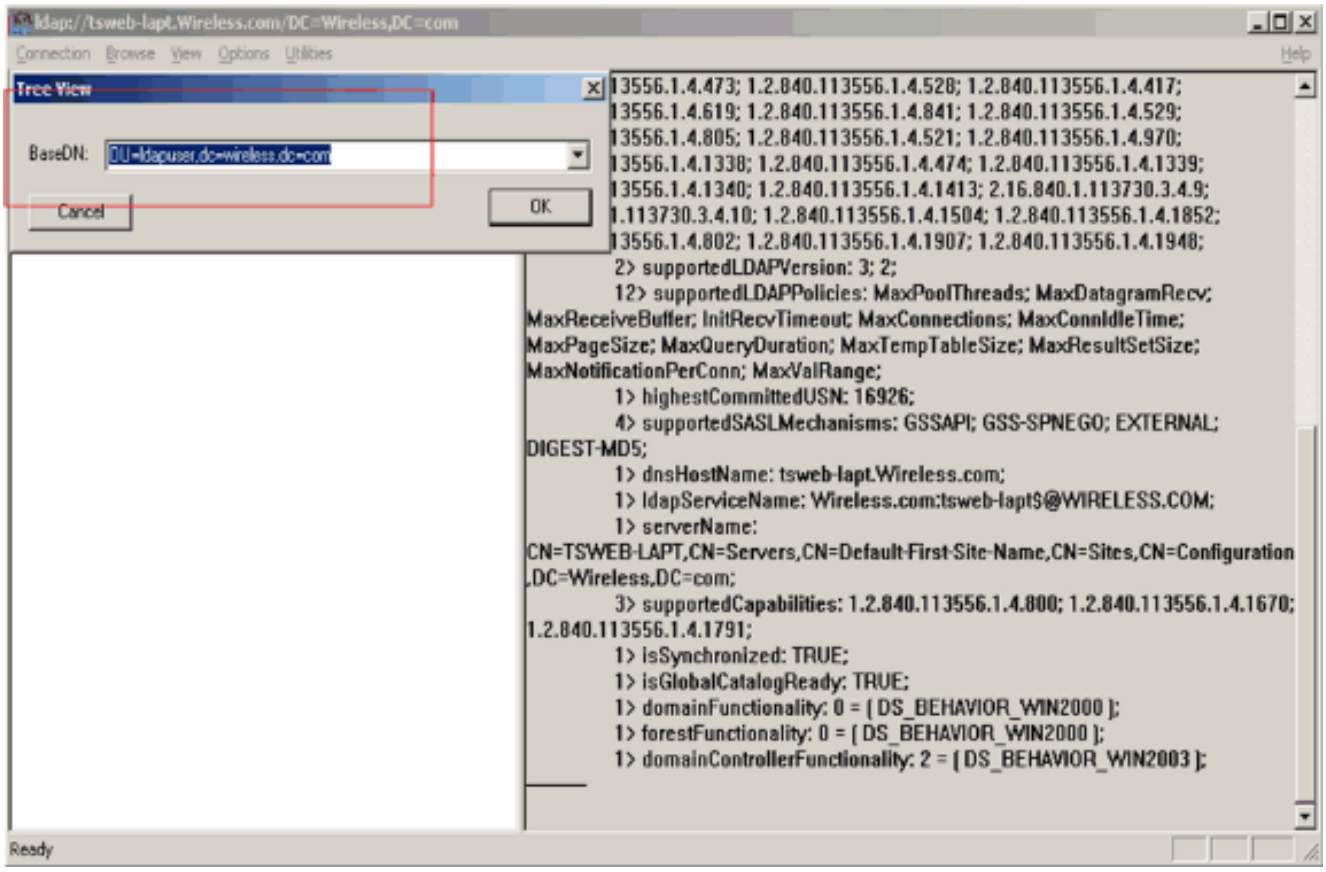
1. Windows 2003 サーバ（同じ LDAP サーバ上でも）で [Start] > [Run] をクリックし、**LDP** と入力して、LDP ブラウザにアクセスします。
2. LDP メイン ウィンドウで [Connection] > [Connect] をクリックし、LDAP サーバの IP アドレスを入力して LDAP サーバに接続します。



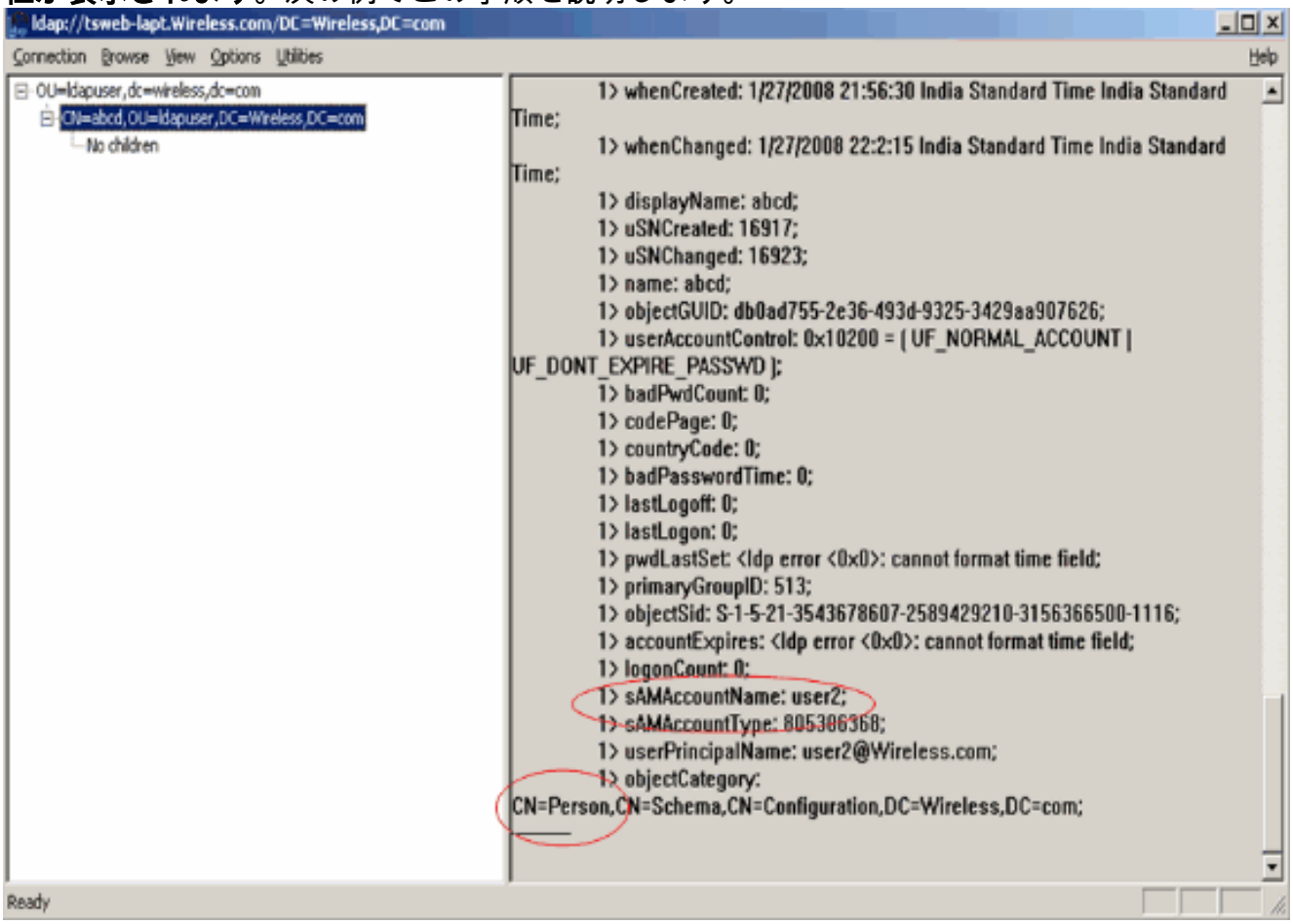
3. LDAP サーバに接続したら、メイン メニューから [View] を選択して [Tree] をクリックします。



4. 表示される [Tree View] ウィンドウで、ユーザの BaseDN を入力します。この例では、**user2 はドメイン Wireless.com の OU「ldapuser」に含まれています。**したがってユーザ **user2** の BaseDN は **OU=ldapuser, dc=wireless, dc=com** となります。[OK] をクリックします。



5. LDP ブラウザの左側に、指定した BaseDN（**OU=ldapuser, dc=wireless, dc=com**）の下にツリー全体が表示されます。ツリーを展開してユーザ **user2** を見つけます。このユーザは、ユーザの名前を表す CN 値で識別されます。この例では **CN=abcd** です。[CN=abcd] をダブルクリックします。LDP ブラウザの右側のペインに、**user2 に関連付けられているすべての属性が表示されます**。次の例でこの手順を説明します。



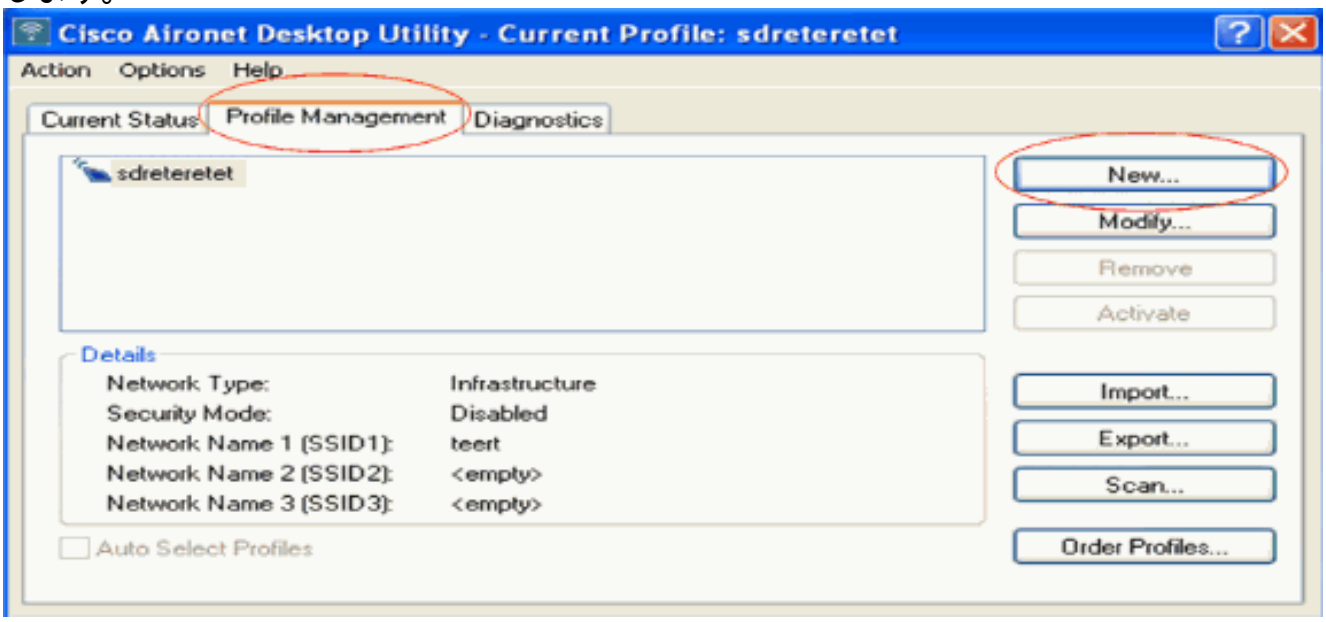
この例の右側にある円で囲まれたフィールドに注目してください。

6. このドキュメントの「WLC での LDAP サーバの詳細の設定」で説明するように、[User Attribute] フィールドには、ユーザ レコードでユーザ名を含む属性の名前を入力します。この LDP 出力では、**sAMAccountName** がユーザ名「user2」を含む属性です。したがって、WLC の [User Attribute] フィールドに対応する [sAMAccountName] 属性を入力します。
7. [User Object Type] フィールドに、レコードをユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには複数の objectType 属性の値が含まれています。そのユーザに一意の値と、他のオブジェクト タイプと共有する値があります。LDP 出力の **CN=Person** は、このレコードをユーザとして示す値の 1 つです。したがって WLC で [User Object Type] 属性に **Person** を指定します。

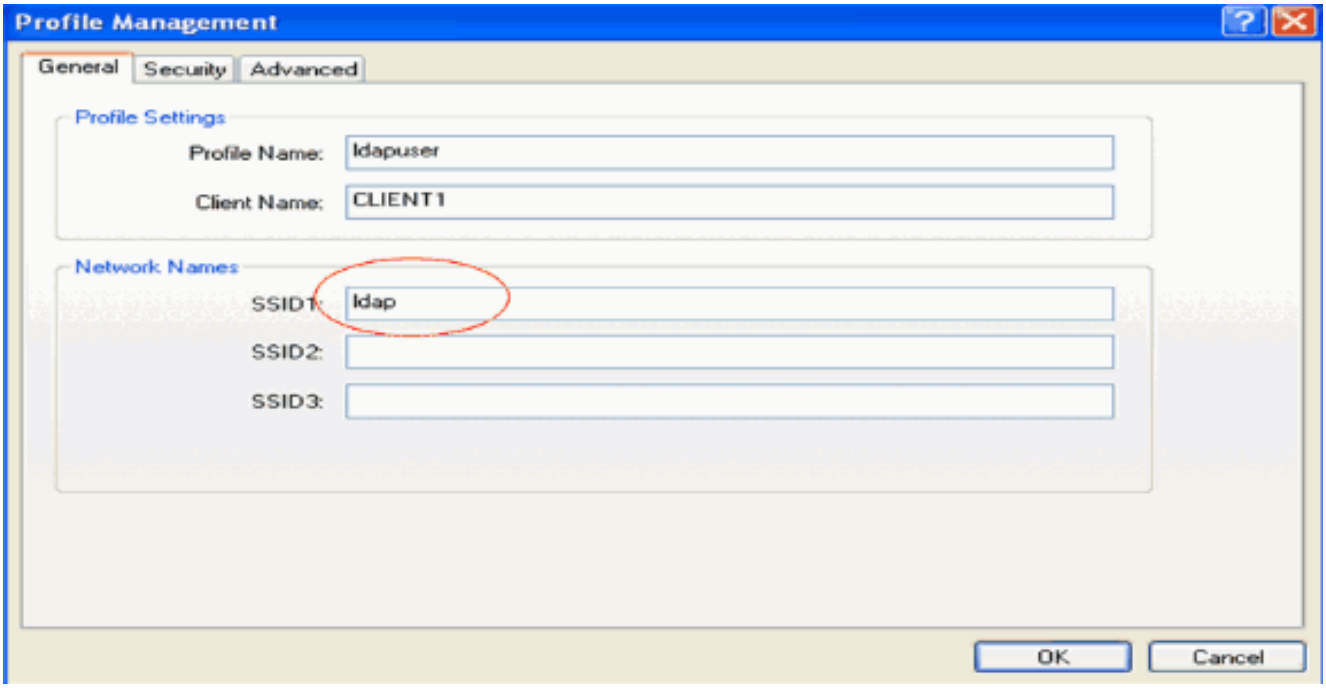
ワイヤレス クライアントの設定

最後に、クライアント証明書とサーバ証明書を使用する EAP-FAST 認証を実行するようにワイヤレス クライアントを設定します。これを行うには、次の手順を実行します。

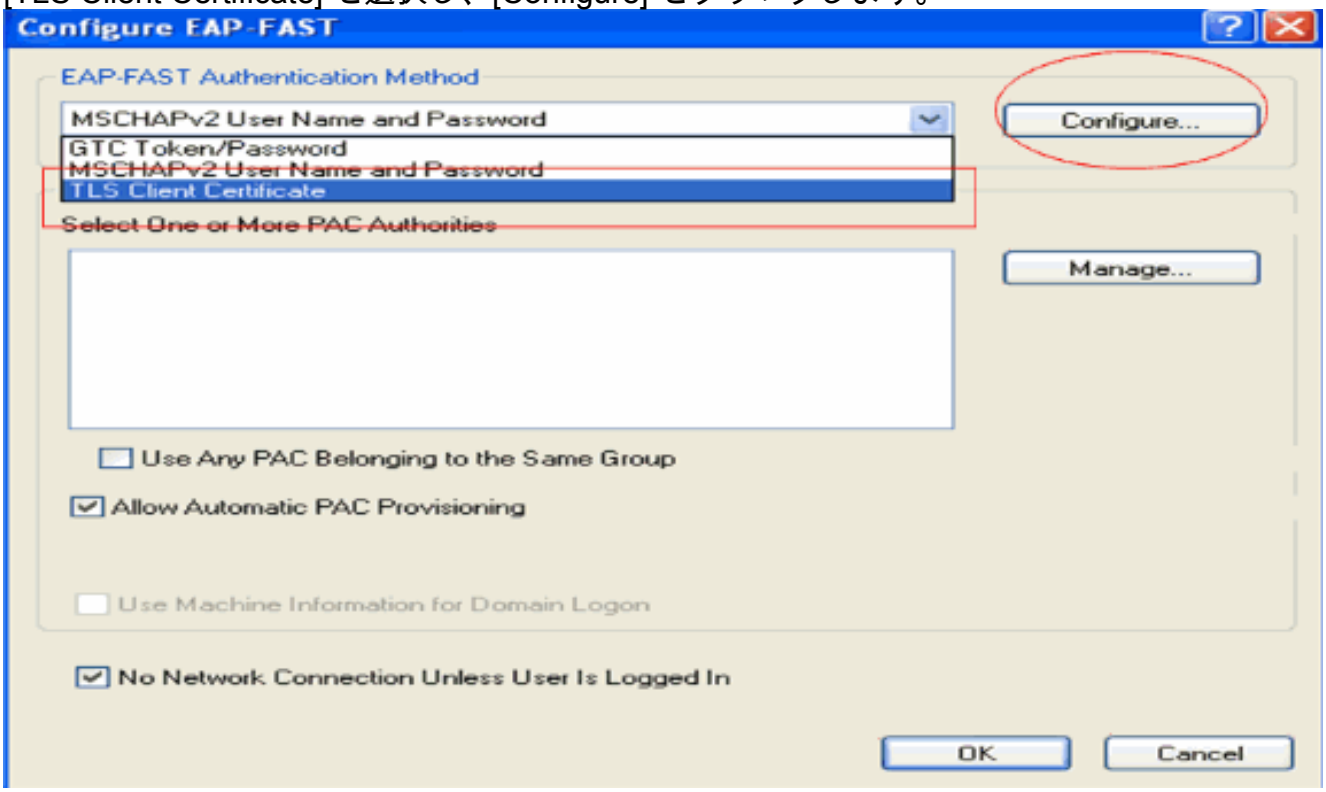
1. **Cisco Aironet Desktop Utility**（ADU）を起動します。ADU のメイン ウィンドウで [Profile Management] > [New] をクリックし、新しいワイヤレス クライアント プロファイルを作成します。



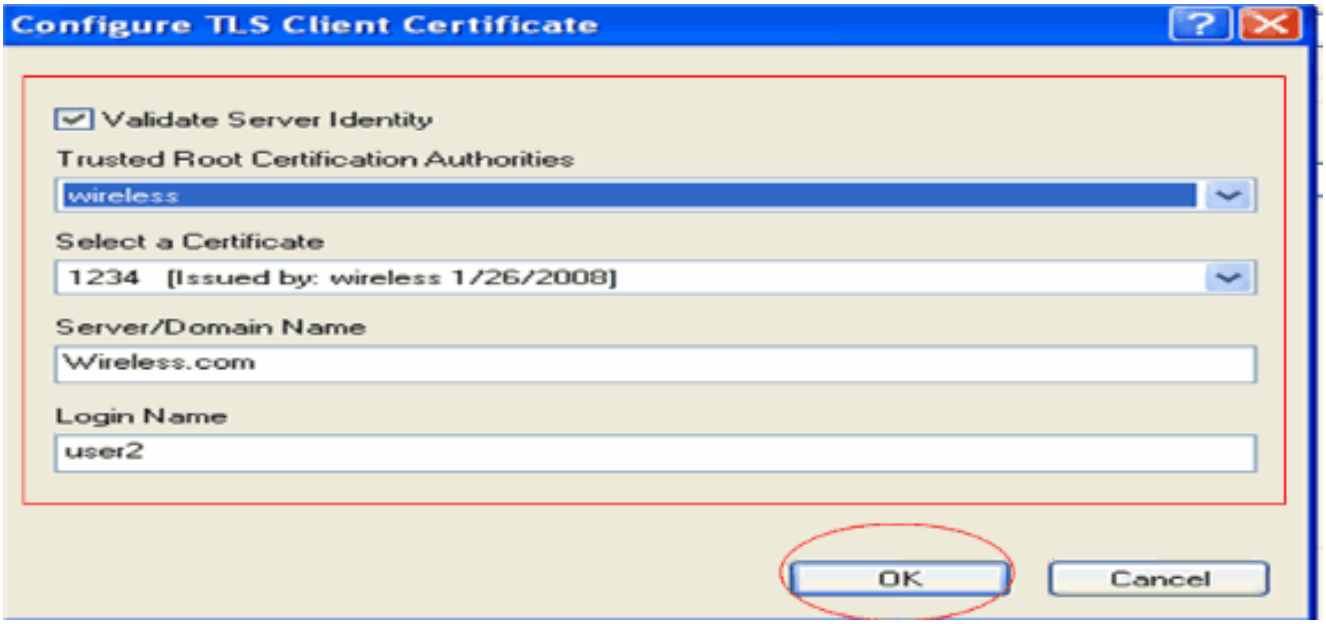
2. プロファイル名を指定し、このプロファイルに SSID 名を割り当てます。この SSID 名は WLC で設定されている SSID 名と同じでなければなりません。この例では SSID 名は **ldap** です。



3. [Security] タブをクリックし、レイヤ 2 セキュリティとして [802.1x/EAP] を選択します。EAP メソッドとして [EAP-FAST] を選択し、[Configure] をクリックします。
4. EAP-FAST 設定ページの [EAP-FAST Authentication Method] ドロップダウン ボックスから [TLS Client Certificate] を選択し、[Configure] をクリックします。



5. TLS クライアント証明書設定ウィンドウで次の操作を実行します。[Validate Server Identity] チェックボックスにチェックマークを付け、[Trusted Root Certification Authority] でクライアントにインストールされている CA 証明書（このドキュメントの「**クライアントのルート CA 証明書の生成**」を参照）を選択します。クライアント証明書として、クライアントにインストールされているデバイス証明書（このドキュメントの「クライアントのデバイス証明書の生成」を参照）を選択します。[OK] をクリックします。次の例でこの手順を説明します。



ワイヤレス クライアント プロファイルが作成されます。

確認

設定が正しく機能するかどうかを確認するには、次の手順を実行します。

1. ADU で **ldap** SSID をアクティブにします。
2. 次に表示されるウィンドウで、必要に応じて [Yes] または [OK] をクリックします。ADU に、クライアントの認証と関連付けを適切に行うための手順がすべて表示されます。

ここでは、設定が正常に機能しているかどうかを確認します。WLC CLI モードを使用します。

- WLC が LDAP サーバと通信してユーザを検出できるようにするため、WLC CLI から **debug aaa ldap enable** コマンドを指定します。次の例に、正常な通信 LDAP プロセスを示します。
  注：このセクションの出力の一部は、スペースの問題により2行目に移動されています。
  (Cisco Controller) **>debug aaa ldap enable**

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

上記のデバッグ出力で強調表示されている情報から、WLC で指定されているユーザ属性を使用して WLC が LDAP サーバに対して照会を実行し、LDAP プロセスが正常に完了したことがわかります。

- ローカル EAP 認証が正常に完了したかどうかを確認するには、WLC CLI から **debug aaa local-auth eap method events enable** コマンドを指定します。以下が一例です。(Cisco Controller) **>debug aaa local-auth eap method events enable**

```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
(436973636f000000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Start

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 1 ...

Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 1 complete

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required
```

```
Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....................................................................

.....................................................................

.....................................................................

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Sent provisioning Server Hello

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate handshake

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 2 ...

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 2 complete.

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate Verify handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Sign certificate verify succeeded (compare)

.....................................................................

.....................................................................

.....................................................................

.....................................................................
.
```

- debug aaa local-auth db enable コマンドも非常に便利です。以下が一例です。(Cisco Controller) >debug aaa local-auth db enable

```
Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request
```

```
Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser'

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 2) to EAP subsys

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8


.....................................................................................

.....................................................................................

.....................................................................................

.....................................................................................


Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 12) to EAP subsys

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- WLC にインストールされており ローカル認証に使用される証明書を確認するには、WLC CLI から **show local-auth certificates** コマンドを実行します。以下が一例です。(Cisco Controller) **>show local-auth certificates**

```
Certificates available for Local EAP authentication:


Certificate issuer ............................. vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123
```

```
     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT


Certificate issuer ............................. cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

            Not installed.
```

- CLI モードで WLC のローカル認証設定を確認するには、**show local-auth config** コマンドを実行します。以下が一例です。(Cisco Controller) **>show local-auth config**

```
User credentials database search order:

    Primary ..................................... LDAP


Timer:

    Active timeout .............................. 300


Configured EAP profiles:

    Name ........................................ ldapuser

      Certificate issuer ....................... vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ........................... fast

      Configured on WLANs ....................... 2


EAP Method configuration:

    EAP-FAST:
```

```
--More-- or (q)uit

      Server key ................................. <hidden>

      TTL for the PAC ............................ 10

      Anonymous provision allowed ................ No

      ..............................................

      ..............................................

      Authority Information ...................... Cisco A-ID
```

トラブルシュート

設定のトラブルシューティングを行うには、次のコマンドを使用できます。

- debug aaa local-auth eap method events enable
- debug aaa all enable
- debug dot1x packet enable

関連情報

- ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認証の設定例
- Microsoft Internet Authentication Service（IAS）を使用した Unified Wireless Network での PEAP
- ACS と Active Directory グループのマッピングに基づく WLC を使用したダイナミック VLAN 割り当ての設定例
- Cisco Wireless LAN Controller コンフィギュレーション ガイド - セキュリティ ソリューションの設定
- Cisco Wireless LAN Controller コンフィギュレーション ガイド - コントローラ ソフトウェアと設定の管理
- EAP 認証と WLAN コントローラ（WLC）の設定例
- Wireless LAN Controller（WLC）の設計と機能に関する FAQ
- EAP-FAST 認証を使用する Cisco Secure Services Client
- Wireless LAN Controller（WLC）に関する FAQ
- Wireless LAN Controller（WLC）のエラー メッセージとシステム メッセージに関する FAQ
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。