Microsoft NPS による 5760/3850 シリーズ WLC PEAP 認証の設定例

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[PEAP フェーズ 1：TLS-Encrypted チャネル](#)
[PEAP フェーズ 2：EAP 認証による通信](#)
[設定](#)
[ネットワーク図](#)
[設定](#)
[CLI で Converged Access WLC を設定します。](#)
[GUI で Converged Access WLC を設定します。](#)
[Microsoft Windows バージョン 2008 サーバの設定](#)
[確認](#)
[トラブルシュート](#)

概要

このドキュメントでは、Microsoft Network Policy Server（NPS）を RADIUS サーバとして使用する Cisco Converged Access ワイヤレス LAN（WLAN）導入環境で、Protected Extensible Authentication Protocol（PEAP）と Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2（MS-CHAP v2）認証を設定する方法について説明します。

前提条件

要件

このドキュメントで説明する設定を開始する前に、次の項目に関する知識があることが推奨されます。

- Microsoft Windows バージョン 2008 の基本的なインストール
- Cisco Converged Access WLAN コントローラのインストール

この設定を試す前に、次の要件が満たされていることを確認してください。

- テスト ラボで、サーバに Microsoft Windows Server バージョン 2008 オペレーティング システム（OS）がインストールされていること。
- すべてのサービス パックを更新していること。
- コントローラと Lightweight アクセス ポイント（LAP）がインストールされていること。
- 最新ソフトウェア更新が設定されていること。

注：Cisco Converged Access WLAN コントローラの最初のインストールと設定に関する情報については、『CT5760 コントローラおよび Catalyst 3850 スイッチの設定例』を参照してください。

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。

- Cisco 5760 シリーズ WLAN コントローラ バージョン 3.3.2（Next Generation Wiring Closet（NGWC））
- Cisco 3602 シリーズ LAP
- Microsoft Windows XP と Intel PROset サプリカント
- ドメイン コントローラの役割のある NPS を実行する Microsoft Windows バージョン 2008 サーバ
- Cisco Catalyst 3560 シリーズ スイッチ

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。

背景説明

PEAP では、Transport Level Security（TLS）を使用して、ワイヤレス ラップトップなど認証対象の PEAP クライアントと Microsoft NPS や任意の RADIUS サーバなどの PEAP オーセンティケータとの間に暗号化チャネルを作成します。PEAP では認証方式は指定されませんが、PEAP により提供される TLS-encrypted 暗号化チャネルで動作できる EAP-MS-CHAP v2 などの他の Extensible Authentication Protocol（EAP）認証プロトコルに対してセキュリティが付加されます。PEAP の認証プロセスは、主に 2 つのフェーズで構成されます。

PEAP フェーズ 1：TLS-Encrypted チャネル

ワイヤレス クライアントはアクセス ポイント（AP）を関連付けます。 IEEE 802.11 ベースの関連付けでは、クライアントと AP 間でセキュアなアソシエーションが確立される前に、オープン システムや共有キーによる認証が提供されます。クライアントと AP 間に IEEE 802.11 ベースのアソシエーションが確立されると、AP との TLS セッションがネゴシエートされます。

ワイヤレス クライアントと NPS の間で認証が完了すると、クライアントと NPS の間で TLS セッションがネゴシエートされます。このネゴシエーションで生成されたキーが、後続のすべての通信の暗号化に使用されます。

PEAP フェーズ 2：EAP 認証による通信

PEAP 認証プロセスの最初の段階で PEAP が作成した TLS チャネルで、EAP ネゴシエーションを含む EAP 通信が発生します。NPSはEAP-MS-CHAP v2を使用してワイヤレスクライアントを認証します。LAPとコントローラは、ワイヤレスクライアントとRADIUSサーバの間でメッセージを転送するだけです。WLC は TLS エンドポイントではないため、WLAN コントローラ（WLC）と LAP はメッセージを復号化できません。

正常な認証（ユーザが PEAP-MS-CHAP v2 でパスワードベースの有効なクレデンシャルを入力し

た場合) の RADIUS メッセージ シーケンスは次のとおりです。

1. NPS がクライアントに ID 要求メッセージ

   ```
   EAP-Request/Identity
   ```
2. クライアントが ID 応答メッセージ

   ```
   EAP-Response/Identity
   ```
3. NPS が MS-CHAP v2 チャレンジ メッセージ

   ```
   EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)
   ```
4. クライアントが MS-CHAP v2 チャレンジと応答

   ```
   EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)
   ```
5. サーバがクライアントの認証に成功すると、NPS が MS-CHAP v2 成功パケットで応答

   ```
   EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)
   ```
6. クライアントがサーバの認証に成功すると、クライアントが MS-CHAP v2 成功パケットで応答

   ```
   EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)
   ```
7. NPS が認証の成功を示す EAP-type-length-value (TLV) を送信します。

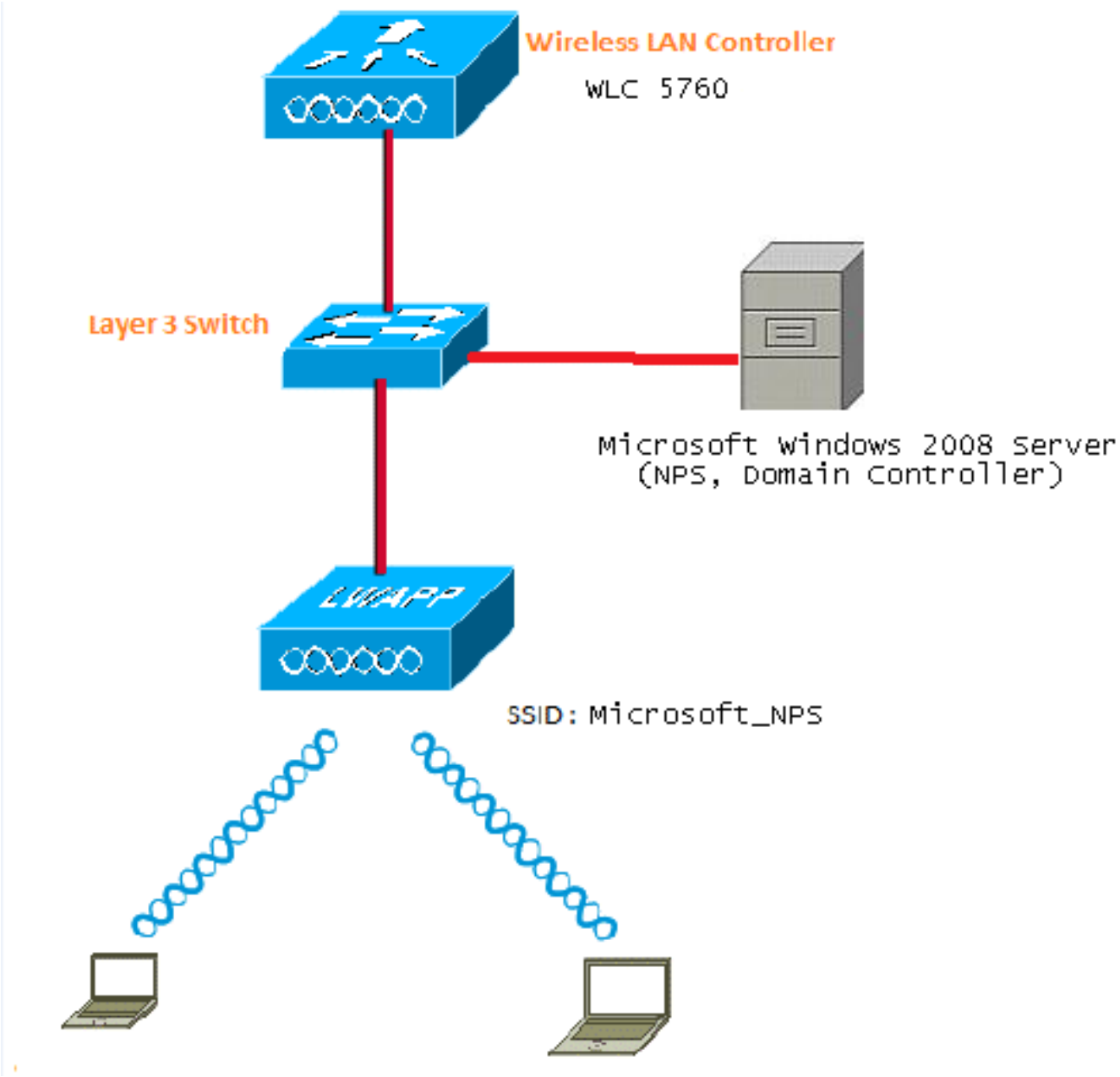
8. クライアントが EAP-TLV ステータスの成功メッセージを返します。

9. サーバが認証を完了し、EAP-Success メッセージをプレーン テキストで送信します。クライアントの分離に VLAN が展開されている場合は、このメッセージに VLAN の属性が含まれています。

設定

このセクションでは、RADIUS サーバとして Microsoft NPS を使用する Cisco Converged Access WLC の導入時に、MS-CHAP v2 認証によって PEAP を設定する方法について説明します。

ネットワーク図



この例では、Microsoft Windows バージョン 2008 サーバは次の役割を担います。

- **wireless.com ドメインのドメイン コントローラ**
- ドメイン ネーム システム（DNS）サーバ
- 認証局（CA）サーバ
- ワイヤレス ユーザ認証のための NPS
- ユーザ データベースを維持するための Active Directory（AD）

サーバは、図に示すように、レイヤ2(L2)スイッチを介して有線ネットワークに接続します。
WLCと登録されたLAPも、L2スイッチを介してネットワークに接続します。

ワイヤレス クライアントは Wi-Fi Protected Access 2（WPA2）- PEAP-MS-CHAP v2 認証を使用してワイヤレス ネットワークに接続します。

設定

このセクションで説明されている設定は 2 つの手順で完了します。

1. CLI または GUI を使用して 5760/3850 シリーズ WLC を設定します。

2. Microsoft Windows バージョン 2008 サーバで、AD 上の NPS、ドメイン コントローラ、およびユーザ アカウントを設定します。

CLI で Converged Access WLC を設定します。

要求されたクライアント VLAN の WLAN を設定し、CLI で認証方式リストにマッピングするには、次の手順を実行します。

> **注：**WLC で **dot1x system auth control が有効になっているか、または dot1X が動作しないことを確認します。**

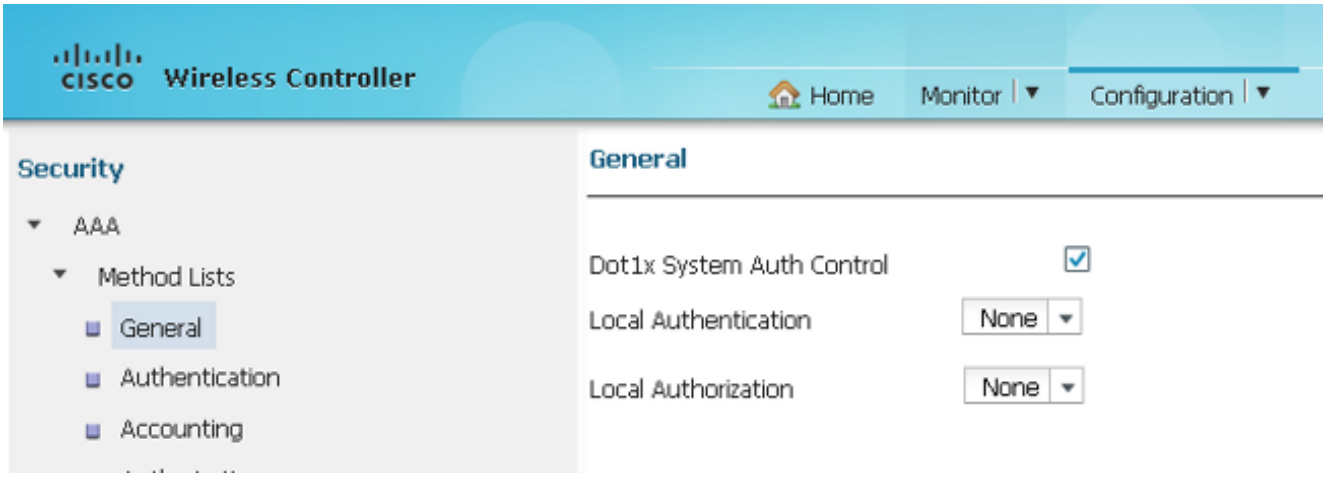
1. **AAA new model 機能を有効にします。**
2. RADIUS サーバを設定します。
3. サーバ グループにサーバを追加します。
4. 方式リストにサーバ グループをマッピングします。
5. WLAN に方式リストをマッピングします。

```
aaa new-model
!
!
aaa group server radius Microsoft_NPS
 server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPS

aaa authorization network Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
 address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 10
 key Cisco123

wlan Microsoft_NPS 8 Microsoft_NPS
 client vlan VLAN0020
 no exclusionlist
 security dot1x authentication-list Microsoft_NPS
 session-timeout 1800
 no shutdown
```

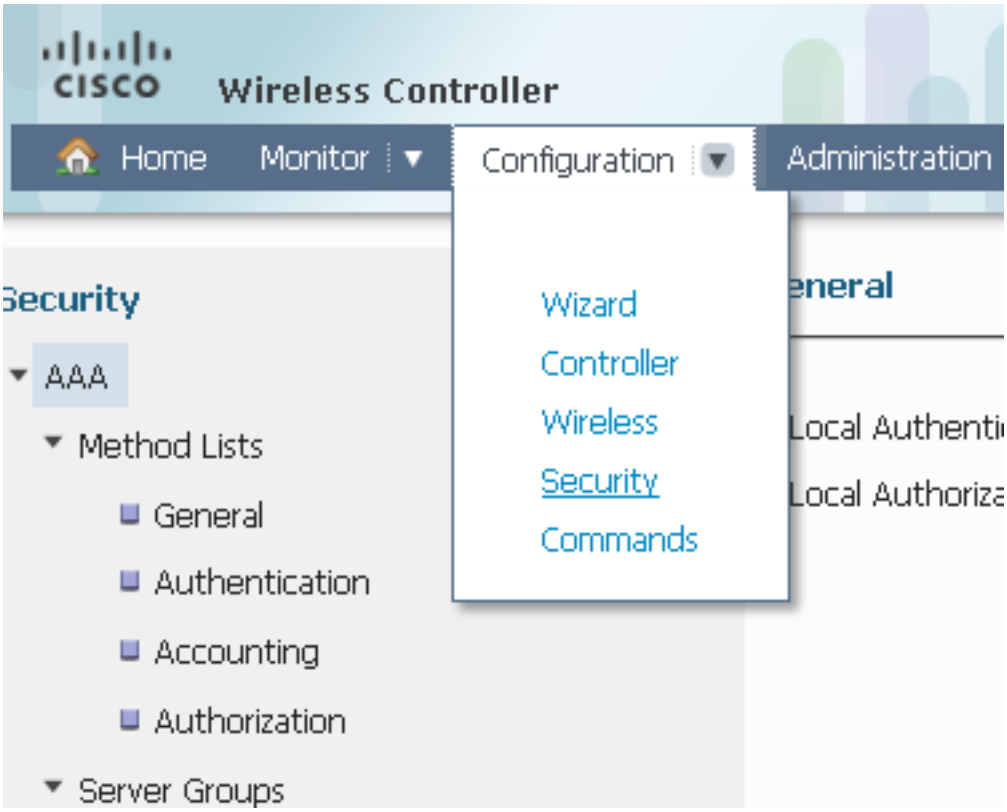
GUI で Converged Access WLC を設定します。

GUI を使用して Converged Access WLC を設定するには、次の手順を実行します。

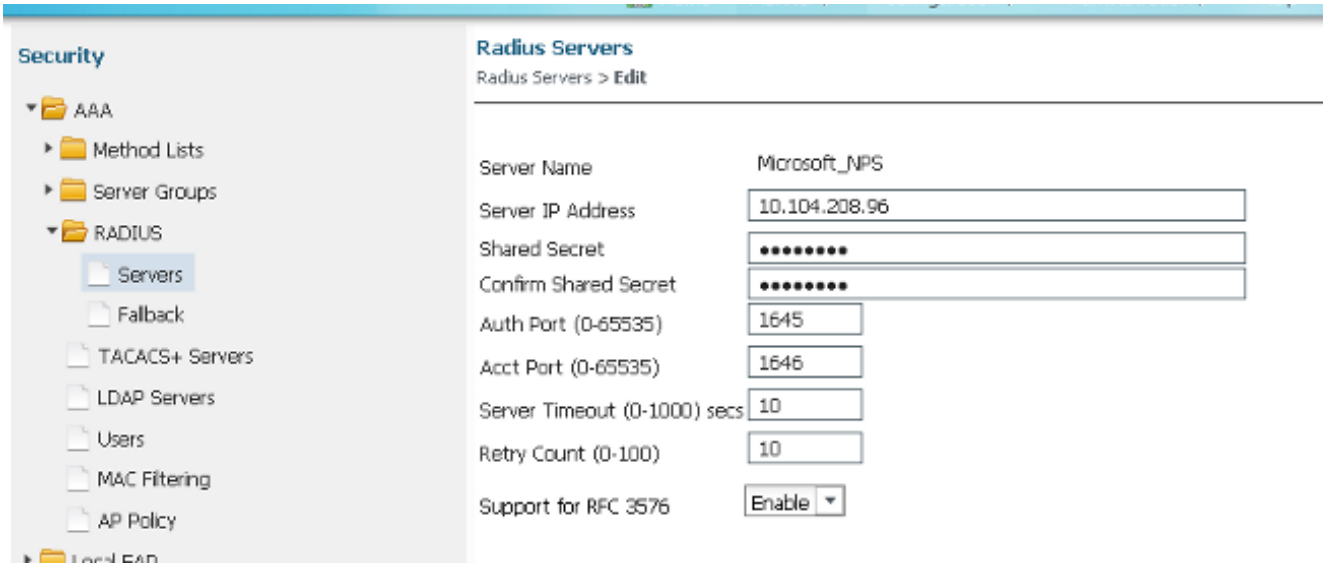
1. **dot1x system-auth-control** を有効にします。



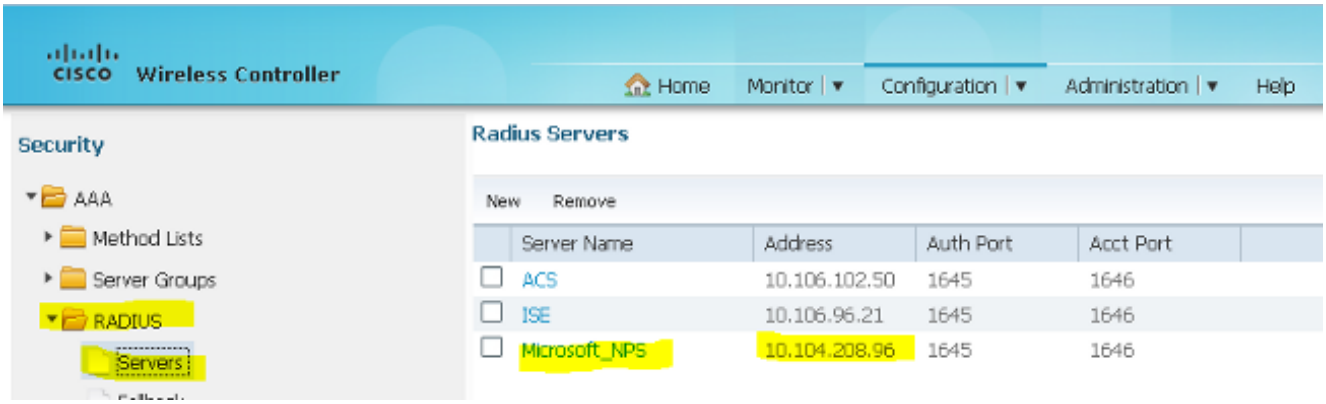
2. [Configuration] **> [Security]** > [AAA] **に移動し、RADIUS サーバを追加します。**



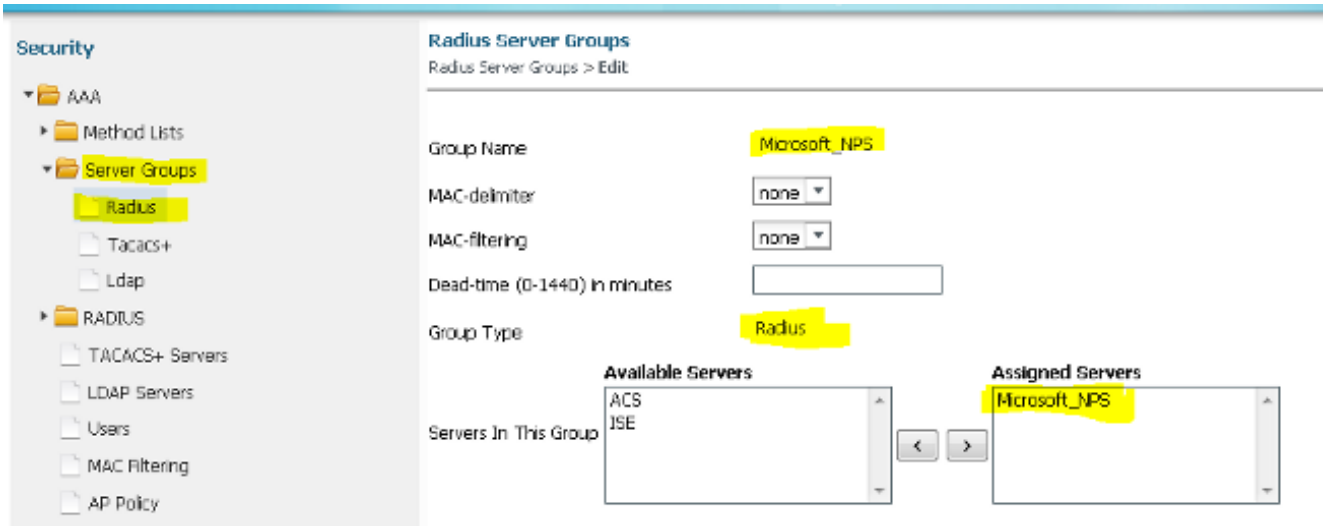
3. [RADIUS] > [Servers] に移動し、[NEW] をクリックして、共有秘密とともに RADIUS サーバの IP アドレスを更新します。共有秘密は、RADIUS サーバに設定されている共有秘密と一致する必要があります。



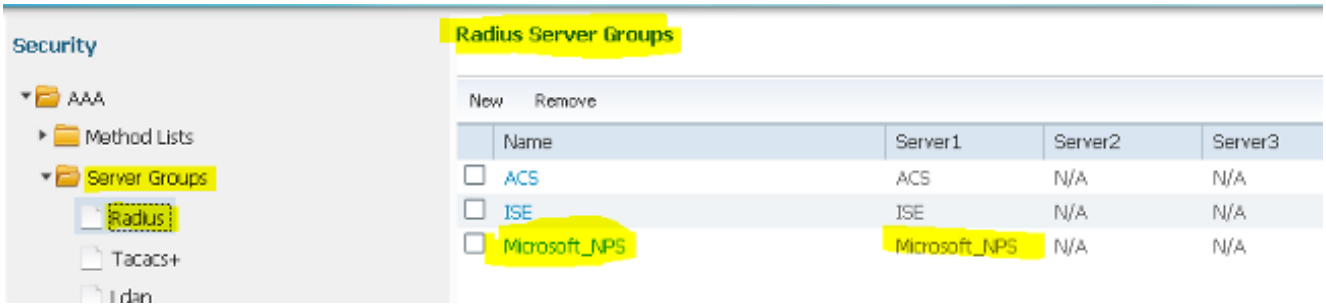
RADIUS サーバを設定した後、[Server] タブは次のように表示されます。



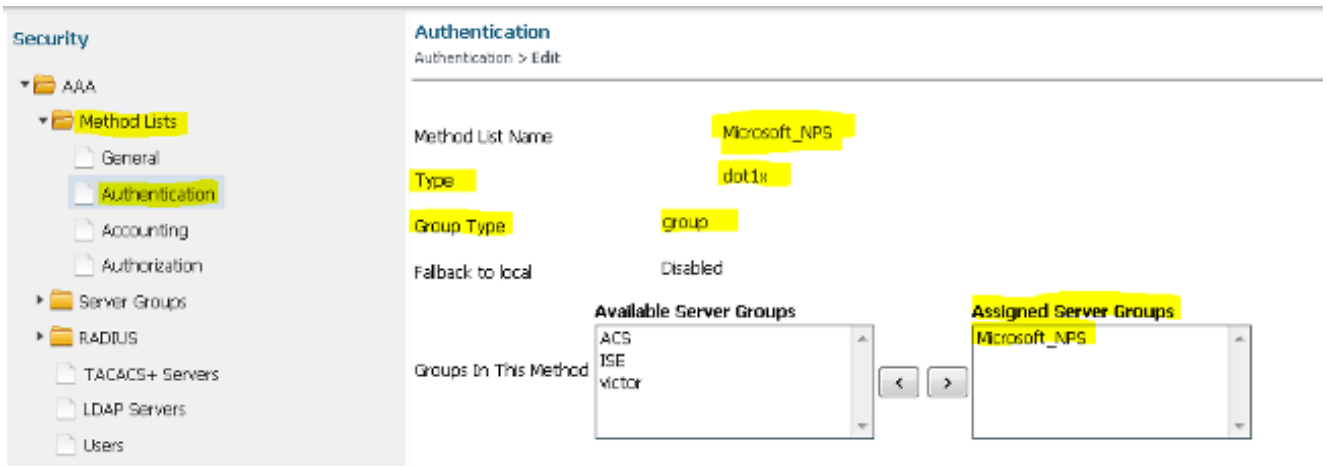
4. サーバ グループを設定し、グループ タイプに [RADIUS] を選択します。次に、前の手順で作成した RADIUS サーバを追加します。



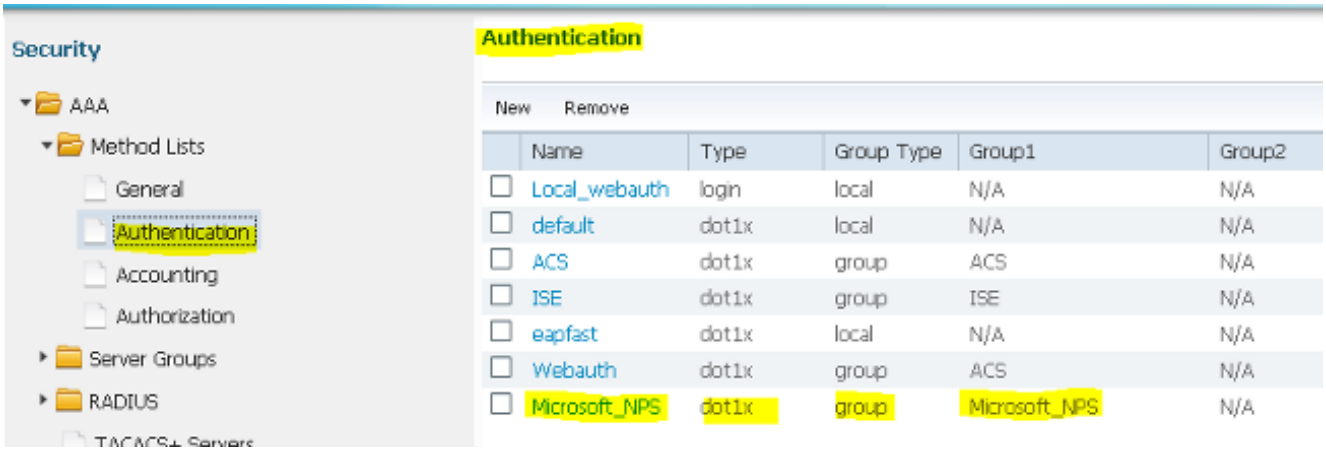
設定後、サーバ グループは次のように表示されます。



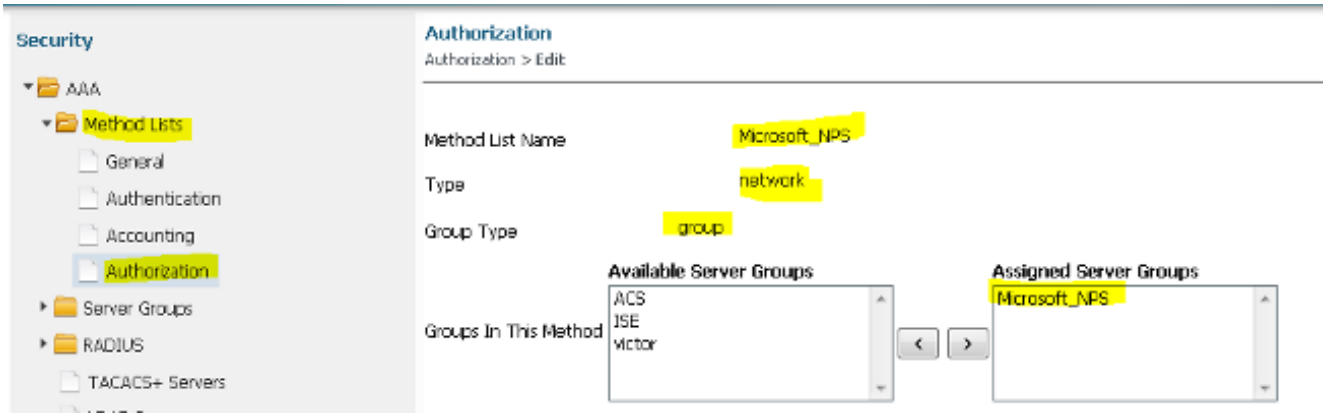
5. 認証方式リストのタイプに **[dot1x]、グループ タイプに [Group] を選択します。**次に、前の手順で設定したサーバ グループをマッピングします。



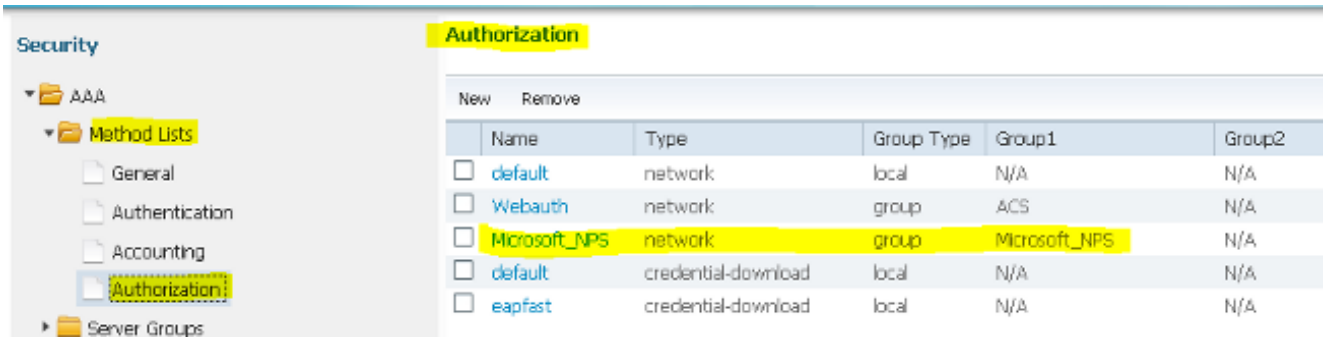
設定後、認証方式リストは次のように表示されます。



6. 許可方式リストのタイプに **[Network]、グループ タイプに [Group] を選択します。**次に、前の手順で設定したサーバ グループをマッピングします。



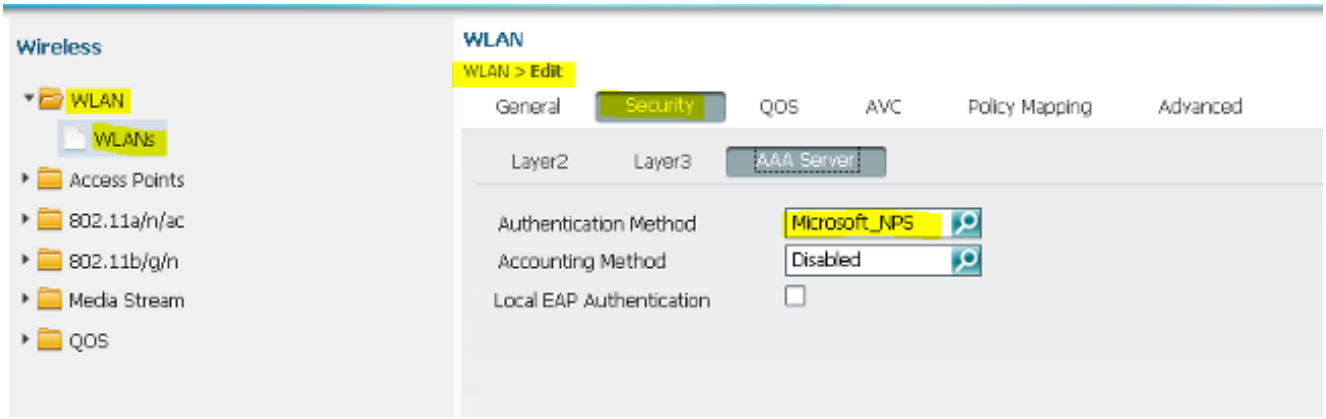
設定後、許可方式リストは次のように表示されます。



7. [Configure] > [Wireless] **に移動し、[WLAN] タブをクリックします。**ユーザが接続し、EAP 認証によって Microsoft NPS サーバで認証されるための新しい WLAN を設定します。

設定後、[Security L2] タブは次のように表示されます。

8. 前の手順で設定した方式リストをマッピングします。これにより、クライアントが正しいサーバに認証されます。



Microsoft Windows バージョン 2008 サーバの設定

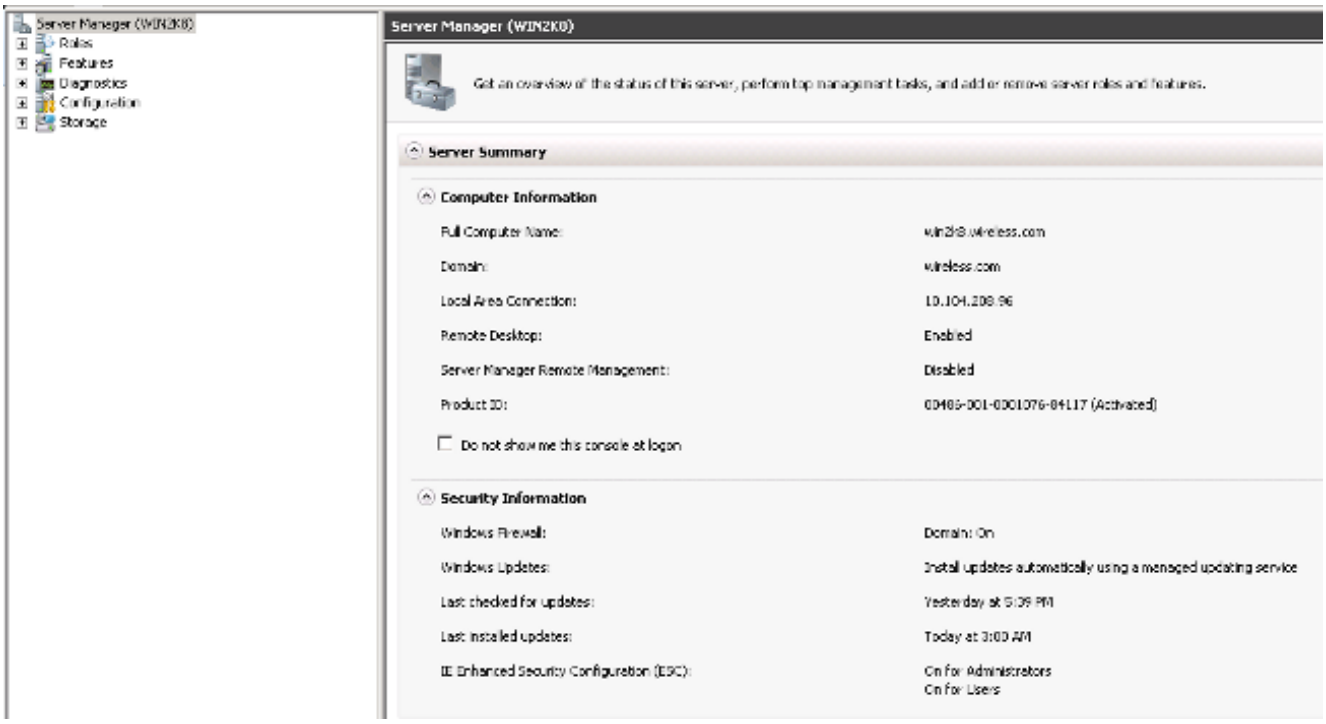
このセクションでは、Microsoft Windows バージョン 2008 サーバの完全な設定について説明します。設定は 6 つの手順で完了します。

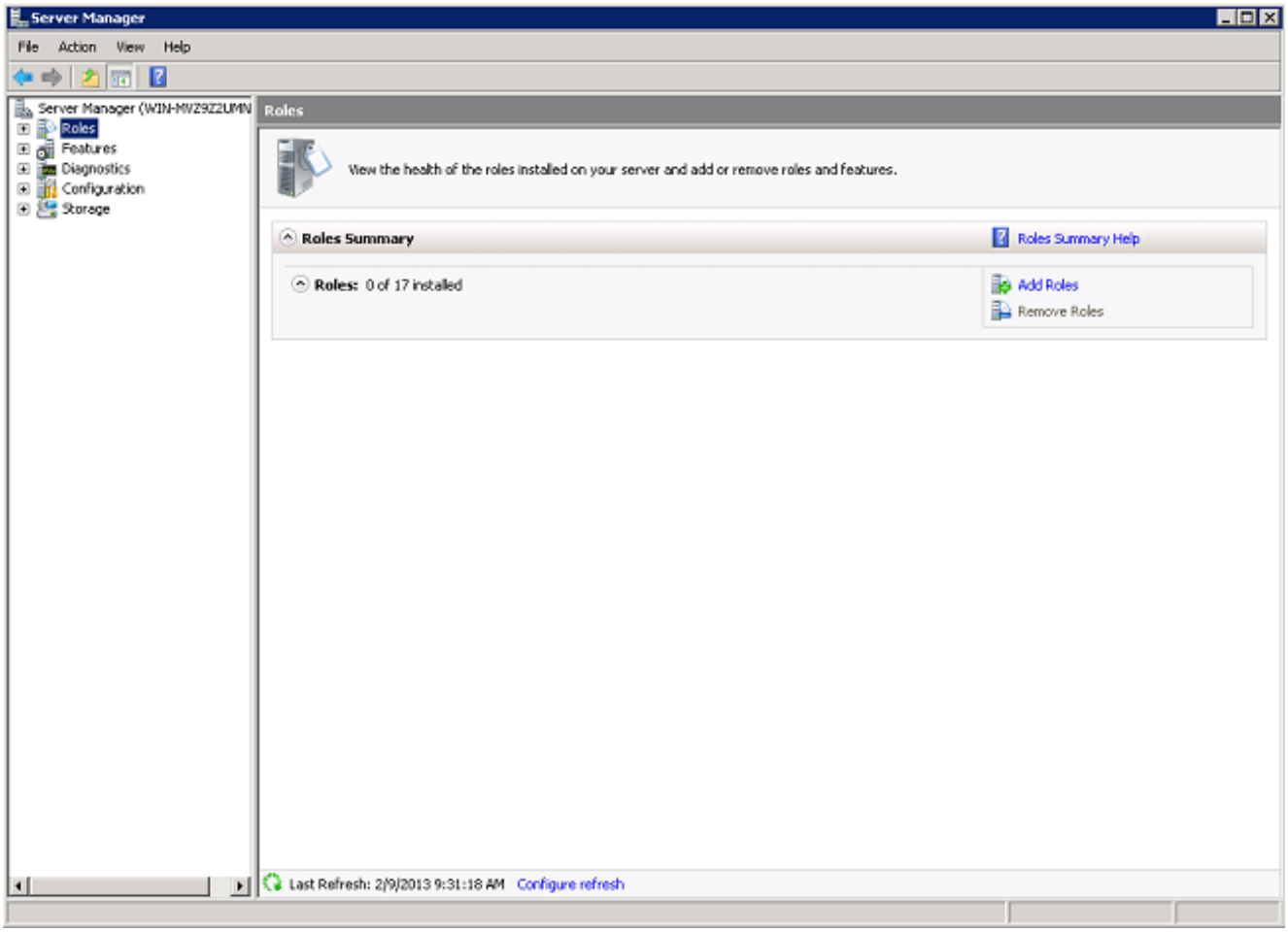
1. サーバをドメイン コントローラとして設定する
2. CA サーバとしてサーバをインストールして設定する
3. NPS をインストールする
4. 証明書をインストールする
5. PEAP 認証のために NPS を設定する
6. ユーザを AD に追加する

ドメイン コントローラとしての Microsoft Windows 2008 Server の設定

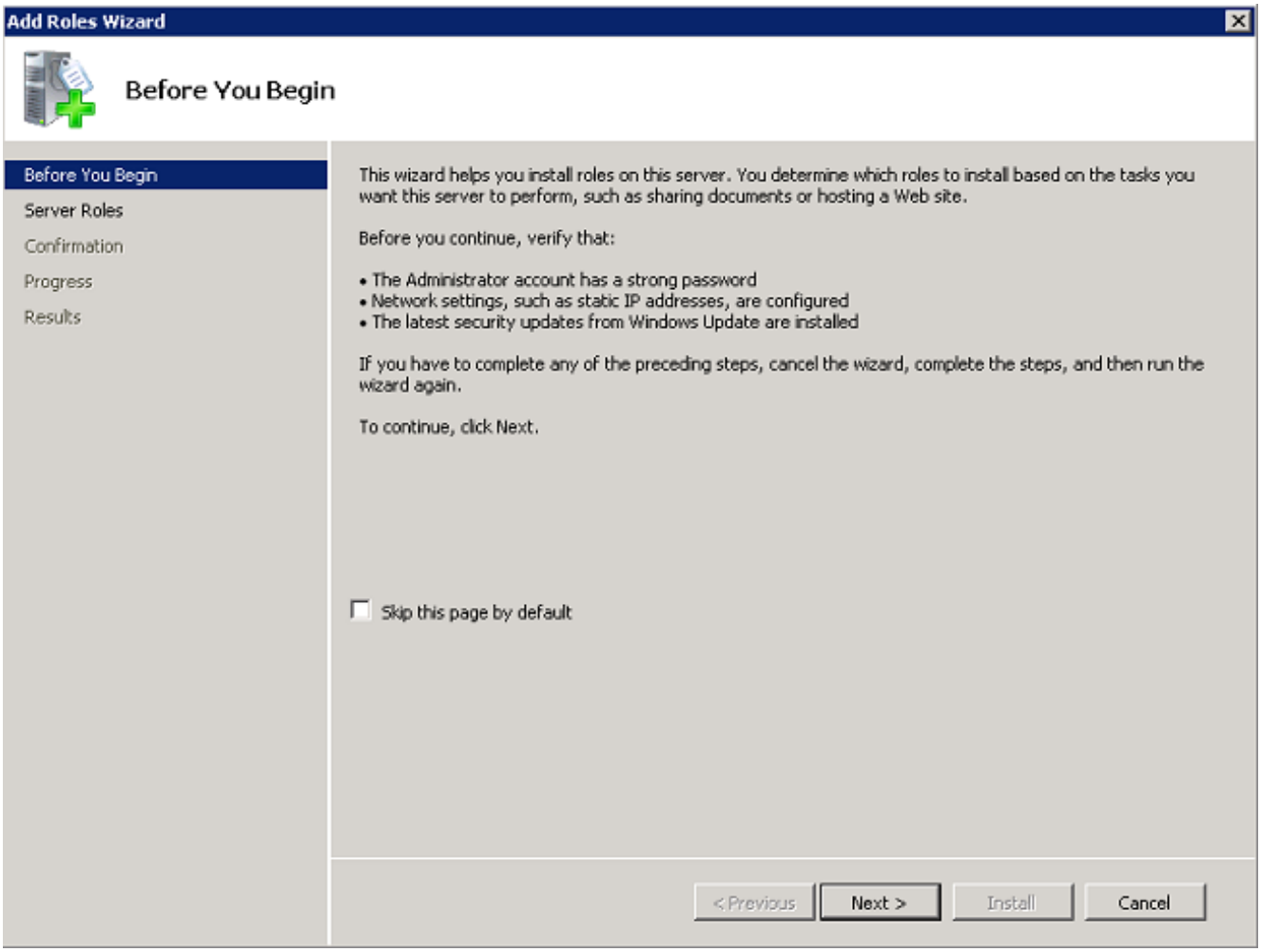
Microsoft Windows バージョン 2008 サーバをドメイン コントローラとして設定するには、次の手順を実行します。

1. [Start] > **[Server Manager] > [Roles] > [Add Roles]** に移動します。

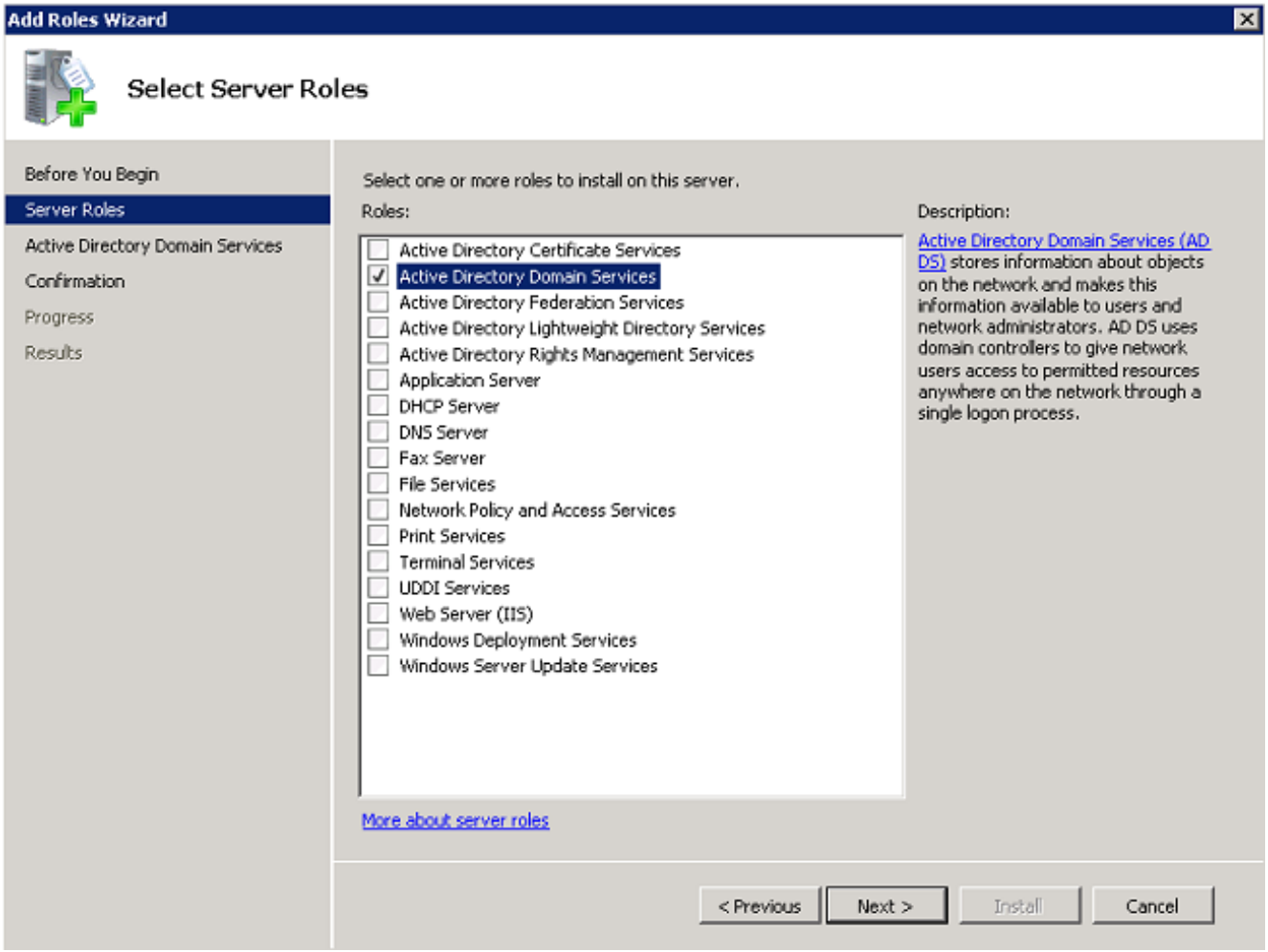




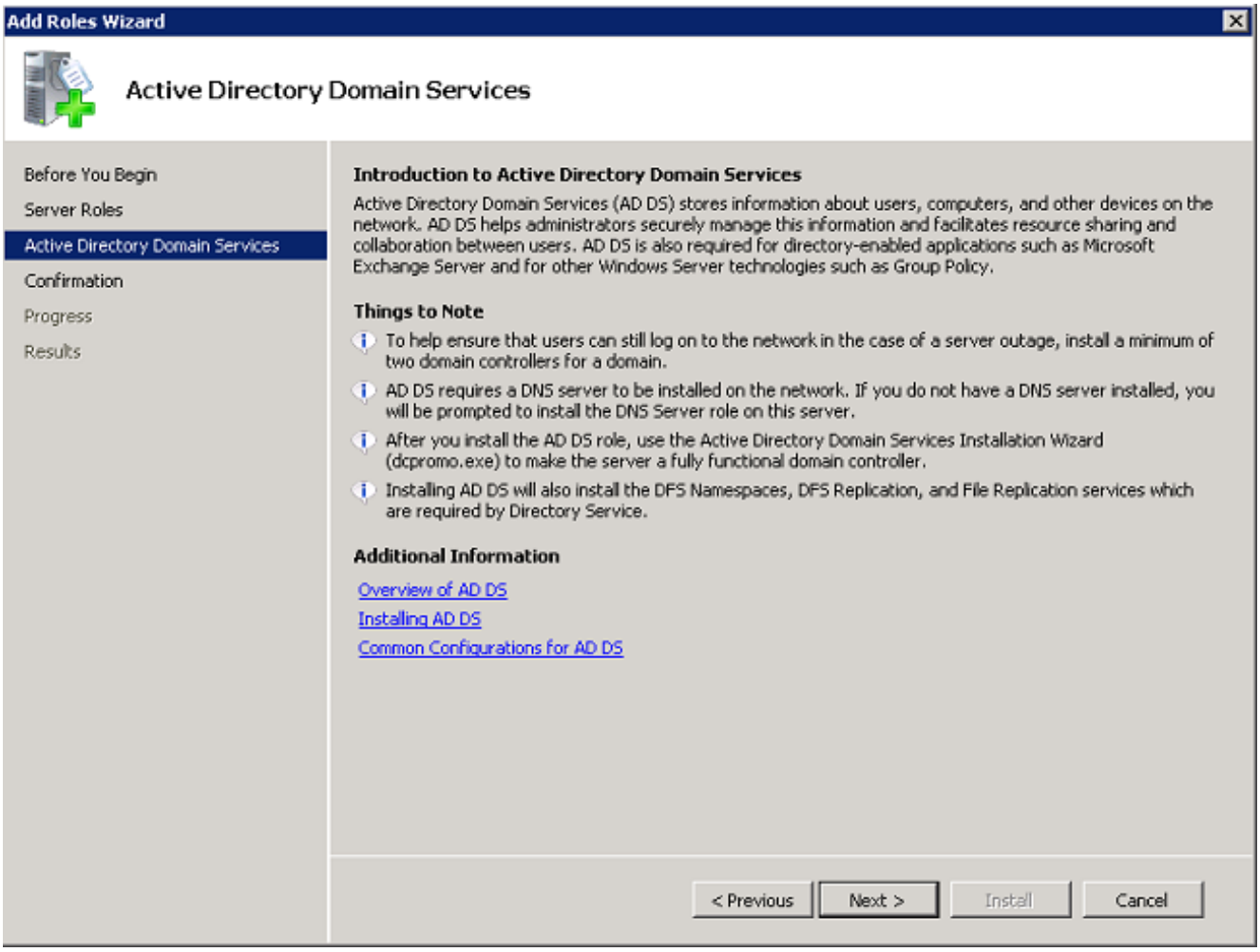
2. [next] をクリックします。



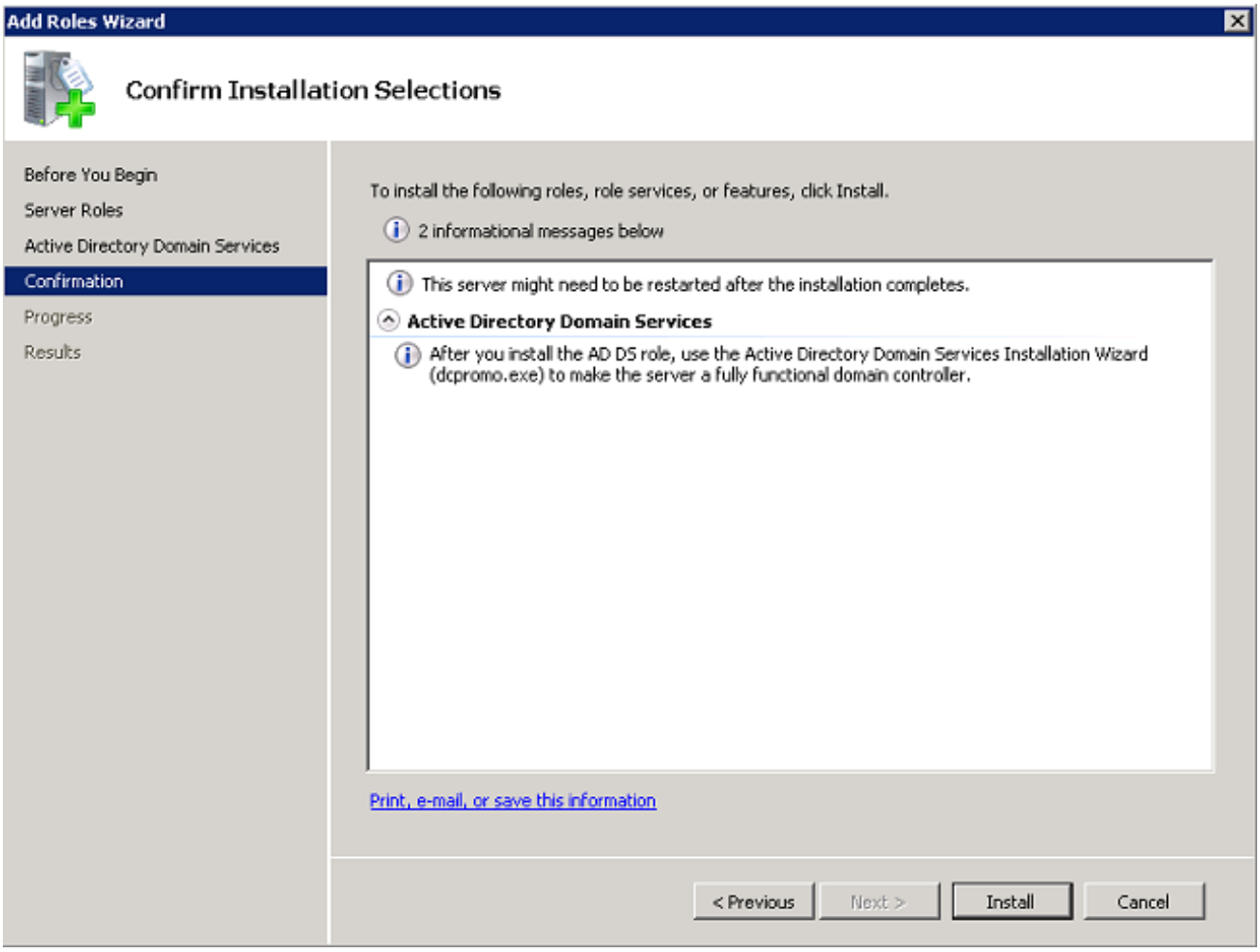
3. [Active Directory Domain Services] チェックボックスをオンにし、[Next] をクリックします。



4. 「Introduction to Active Directory Domain Services」に目を通し、[Next] をクリックします。

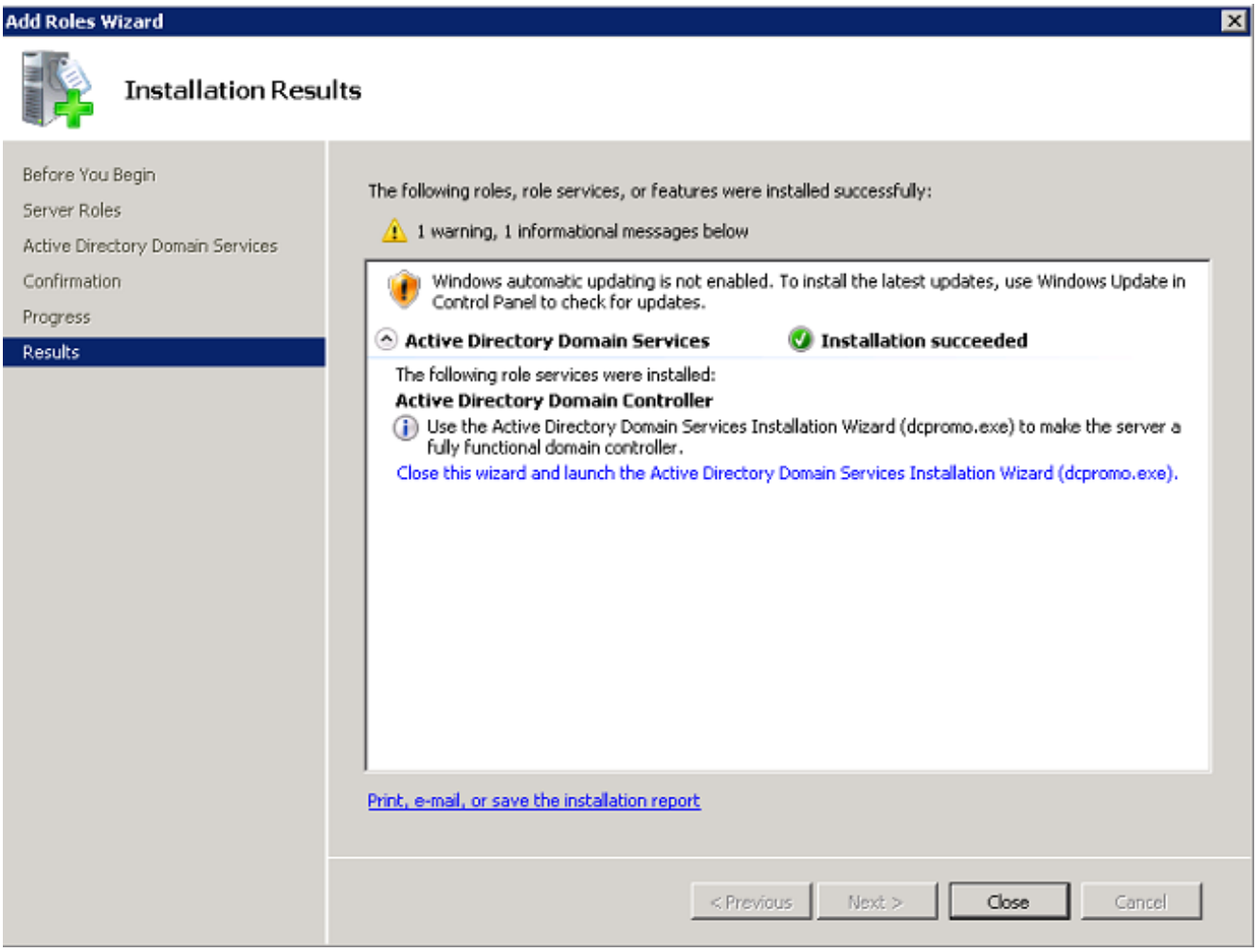


5. [Install] をクリックしてインストール プロセスを開始します。

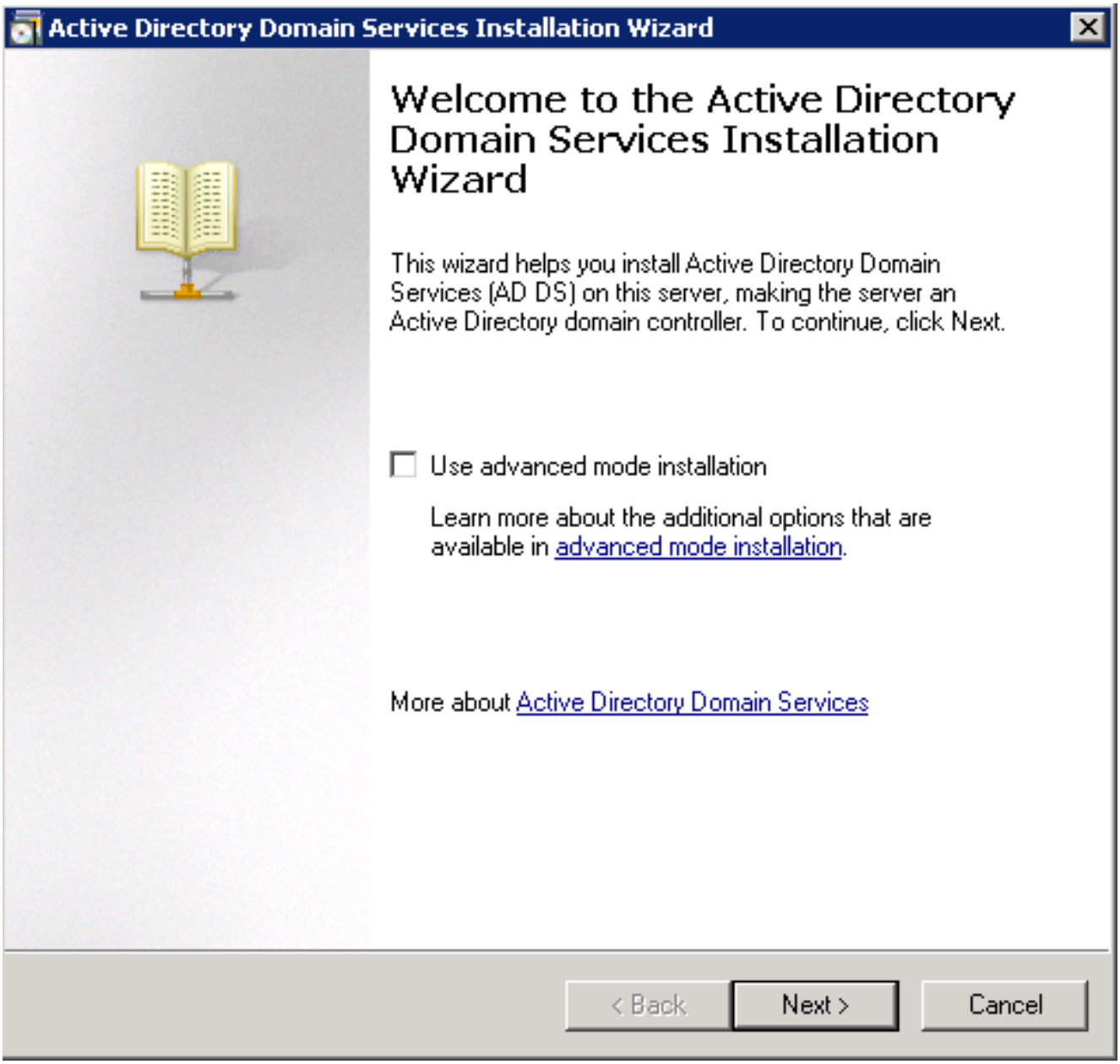


インストールが進んで完了します。

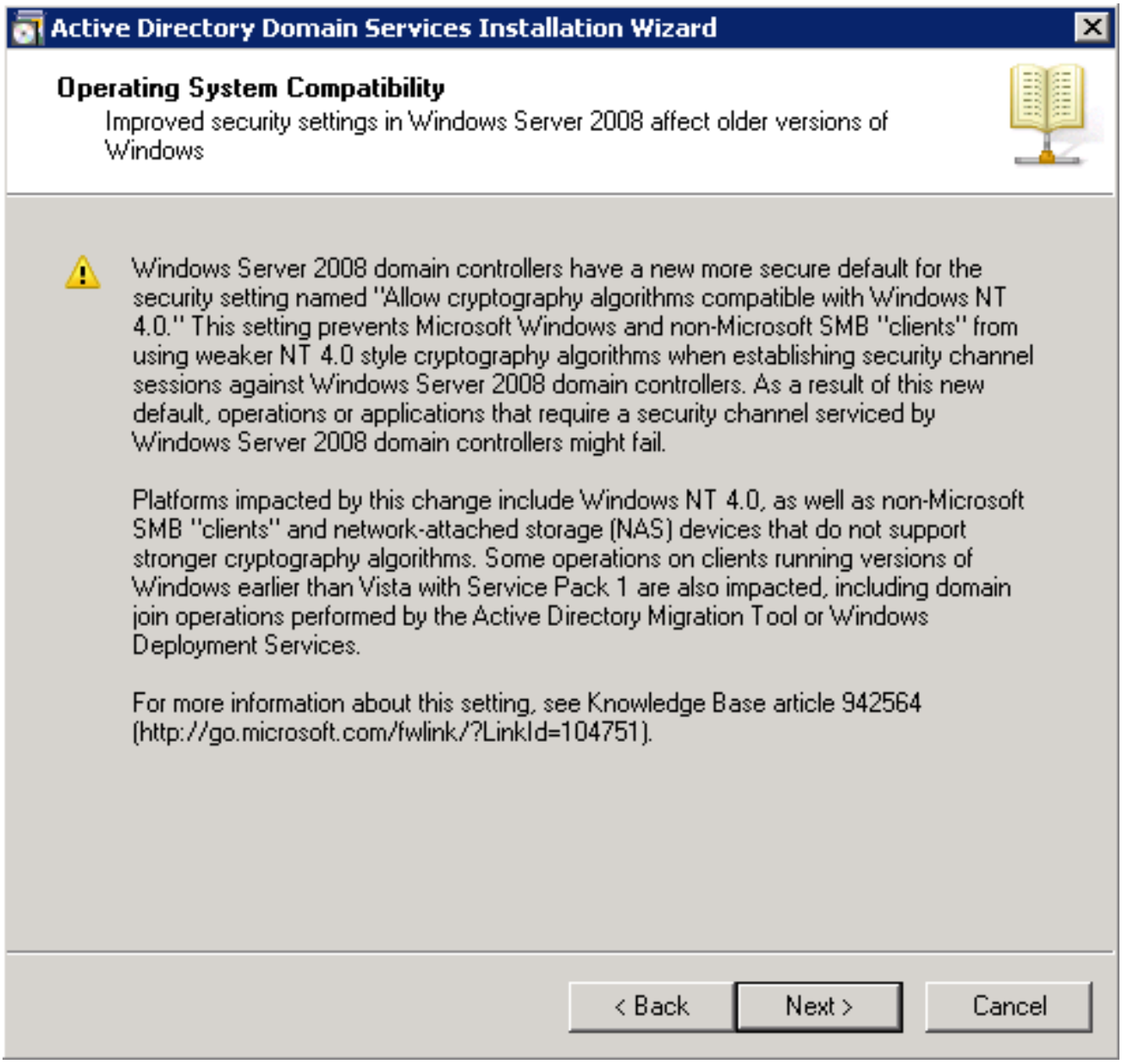
6. [Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)] をクリックしてインストールと設定を続けます。



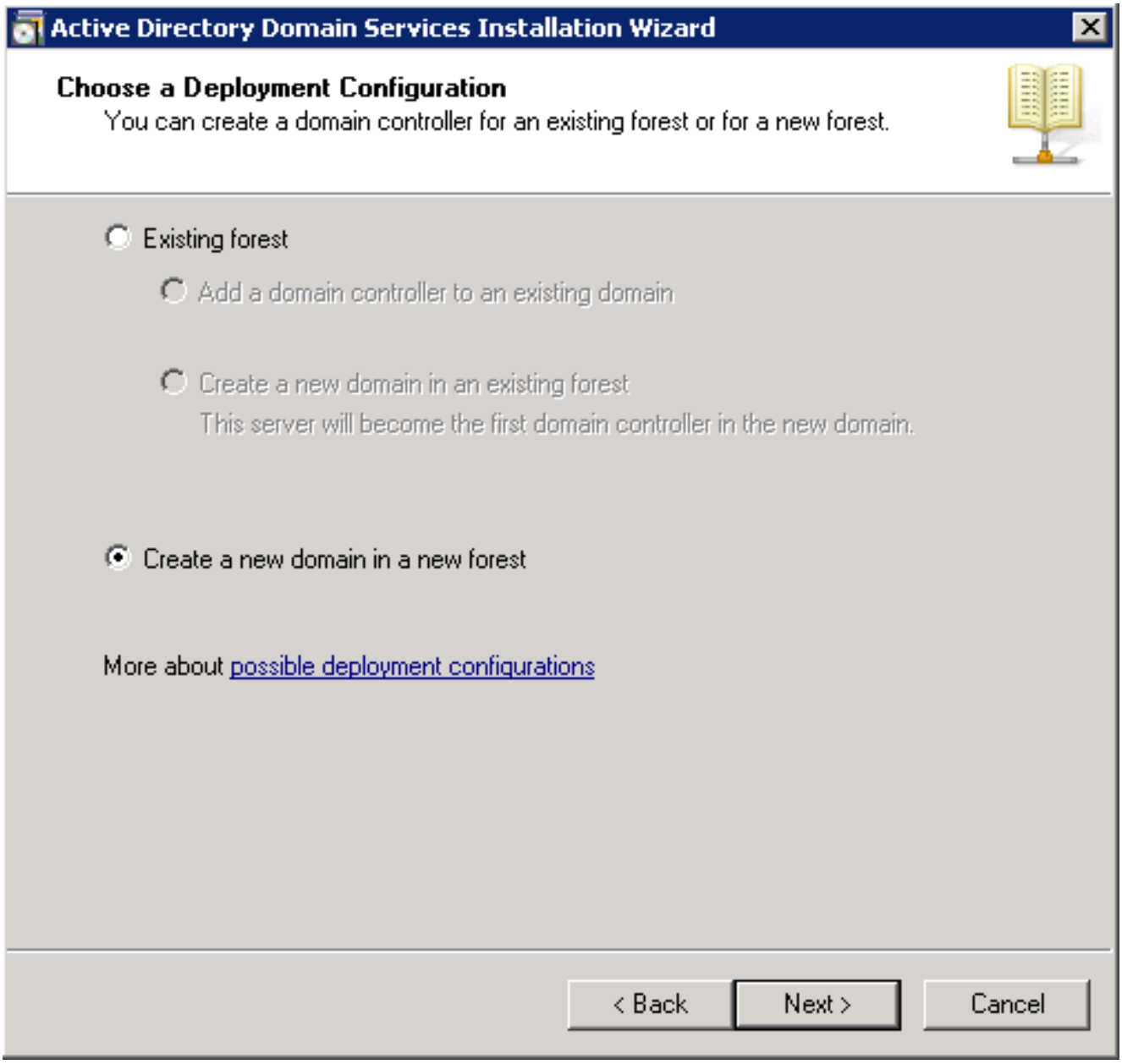
7. [Next] をクリックすると、[Active Directory Domain Services Installation Wizard] が実行されます。



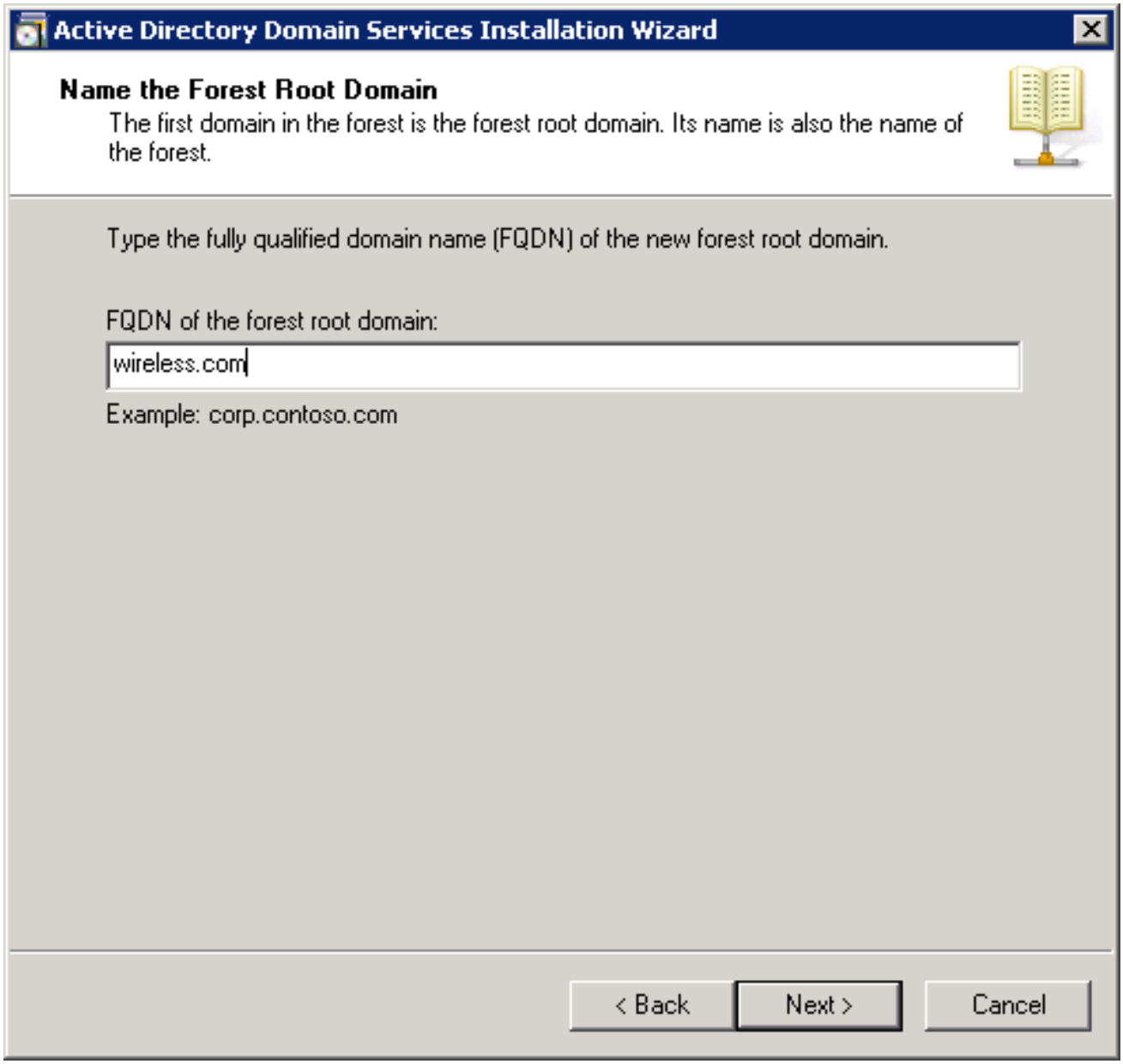
8. 「Operating System Compatibility」の情報に目を通し、[Next] をクリックします。



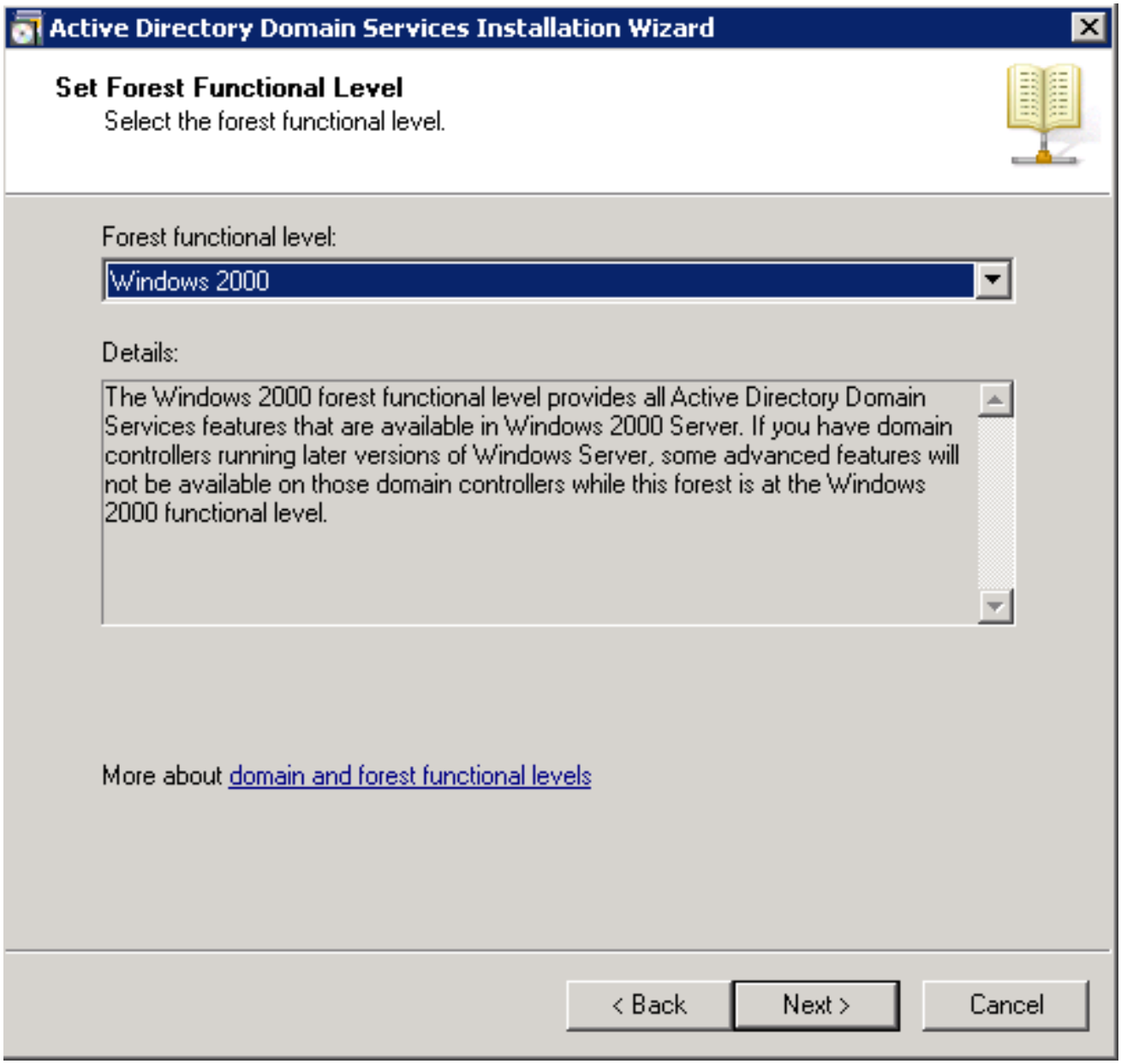
9. [Create a new domain in a new forest] オプション ボタンをクリックし、[Next] をクリックして新しいドメインを作成します。



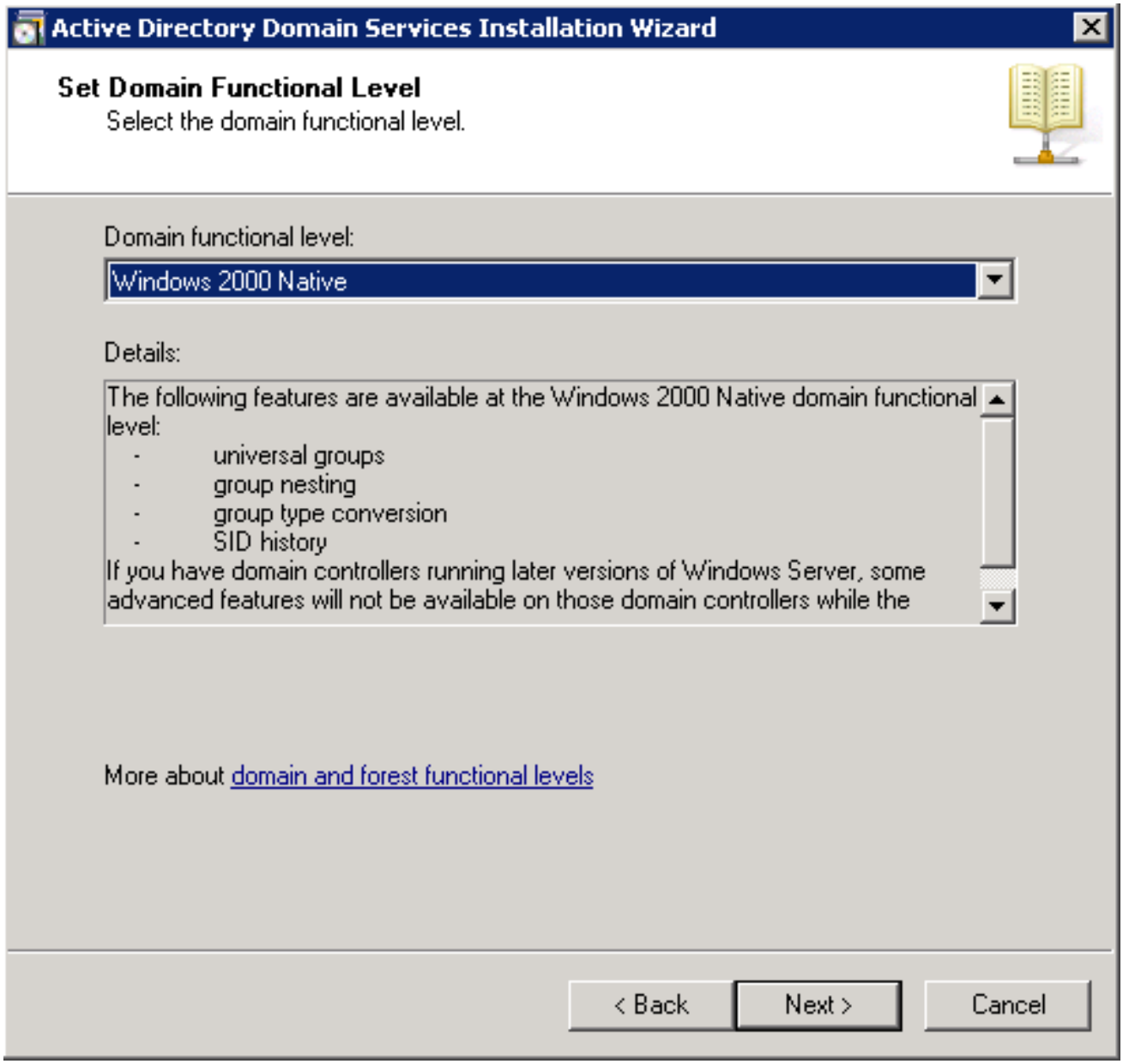
10. 新しいドメインの完全な DNS 名（この例では **wireless.com**）を入力し、[Next] をクリックします。



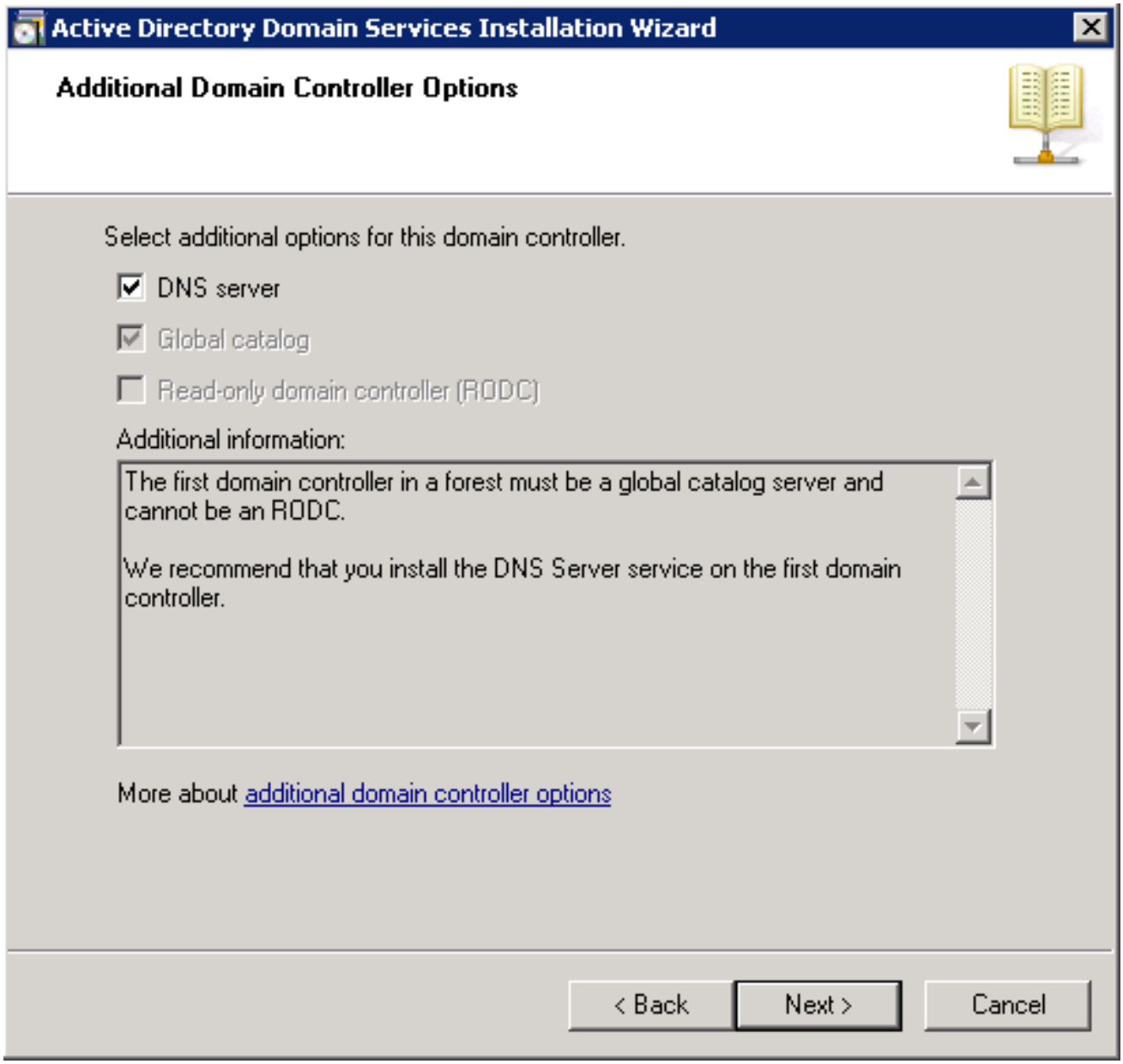
11. ドメインの [Forest functional level] を選択し、[Next] をクリックします。



12. ドメインの [Domain functional level] **を選択し、[Next] をクリックします。**

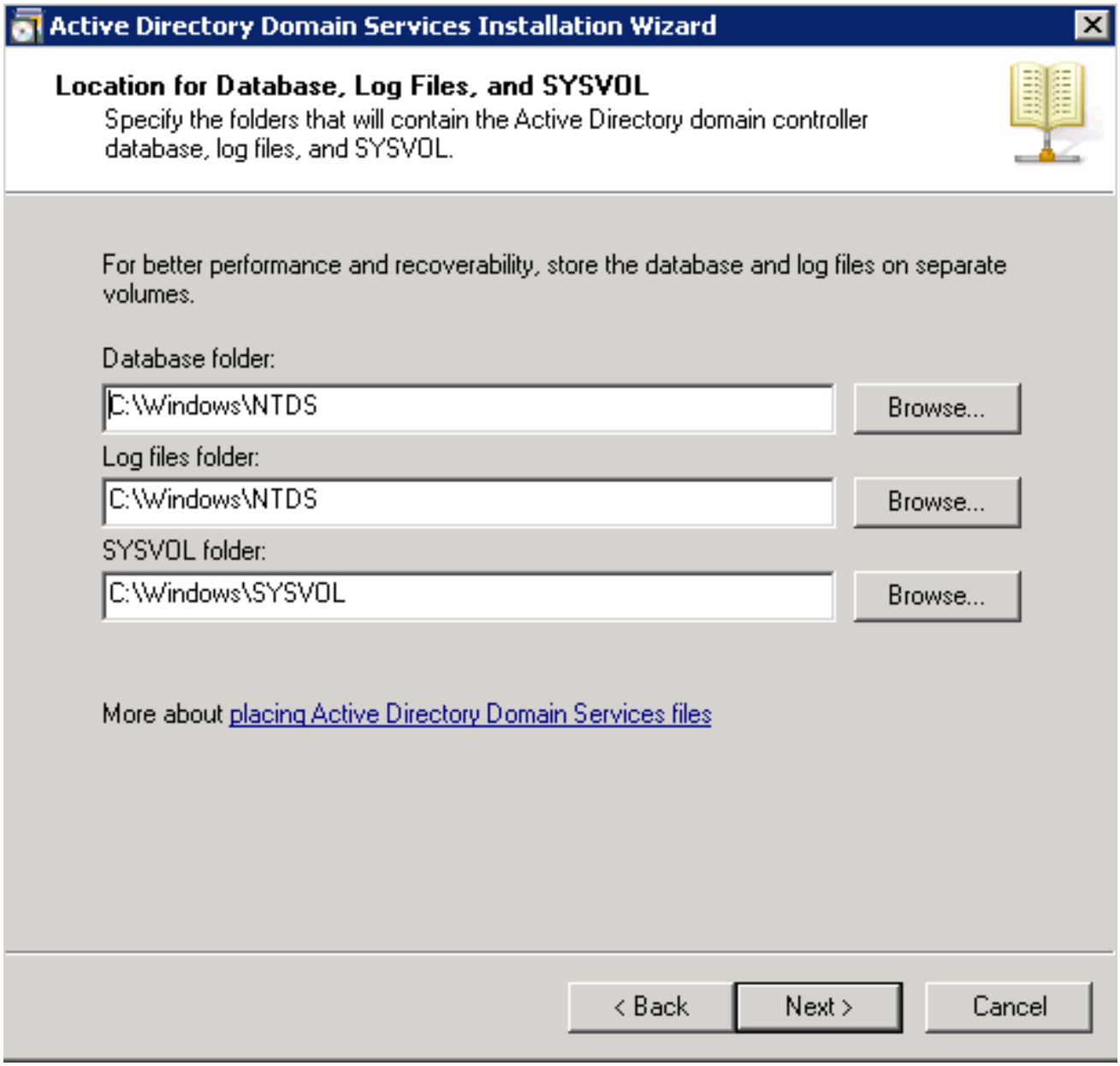


13. [DNS server] **チェックボックスをオンにし、[Next] をクリックします。**

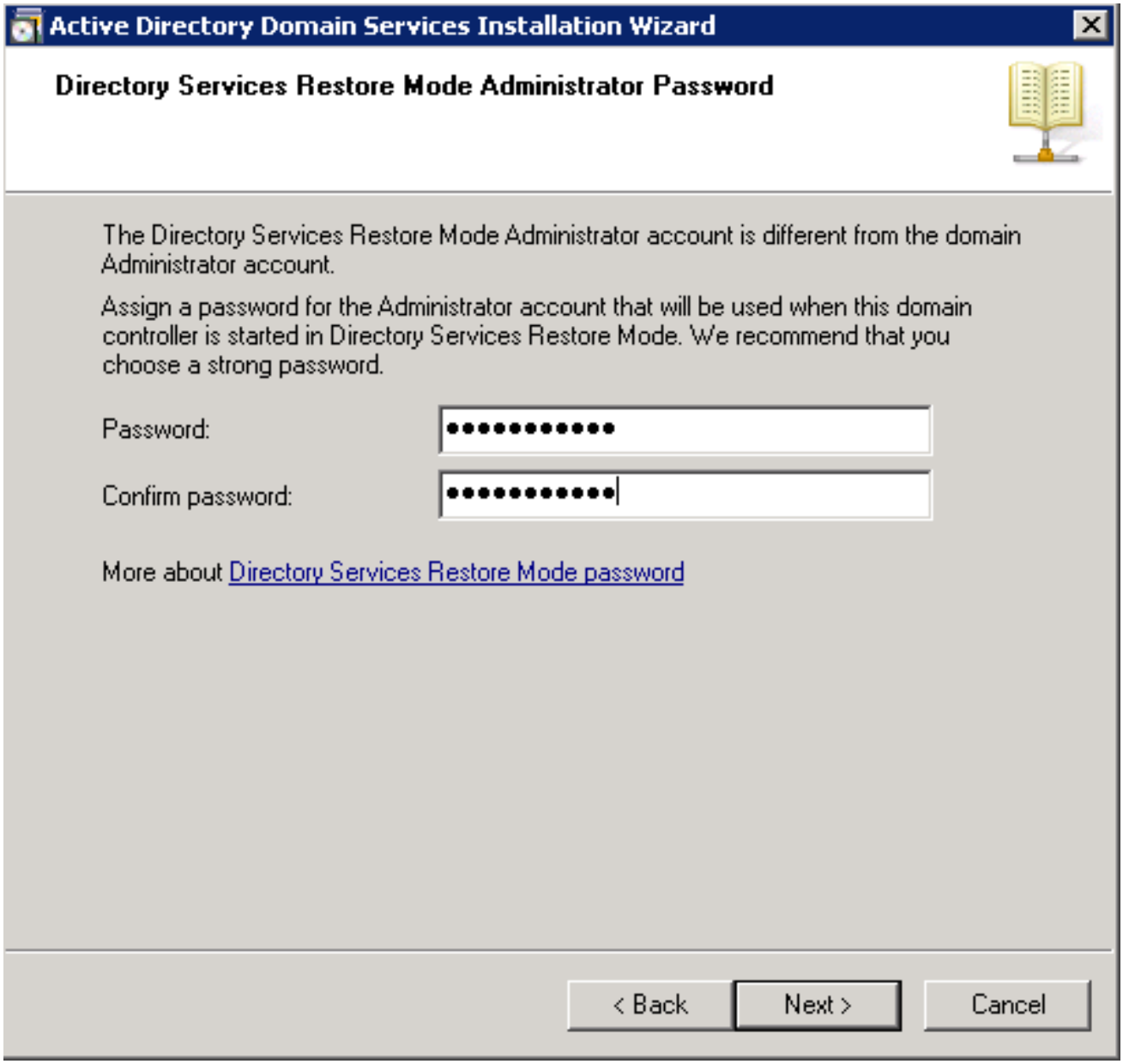


14. [Active Directory Domain Services Installation Wizard] ポップアップ ウィンドウが表示されたら、[Yes] をクリックして、ドメインの DNS に新しいゾーンを作成します。

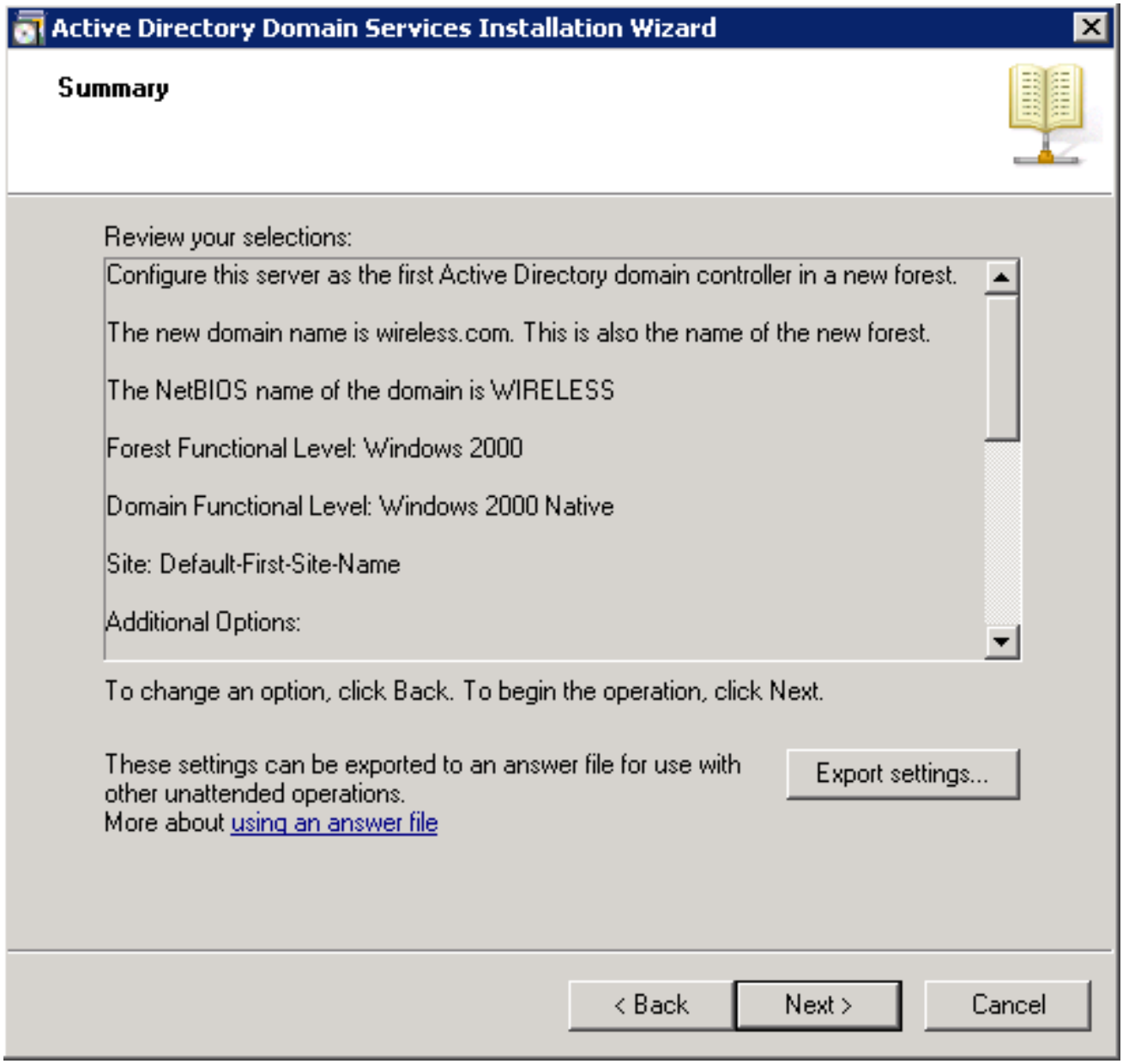
15. AD がファイル格納に使用するフォルダを選択して、[Next] をクリックします。



16. 管理者パスワードを入力し、[Next] をクリックします。

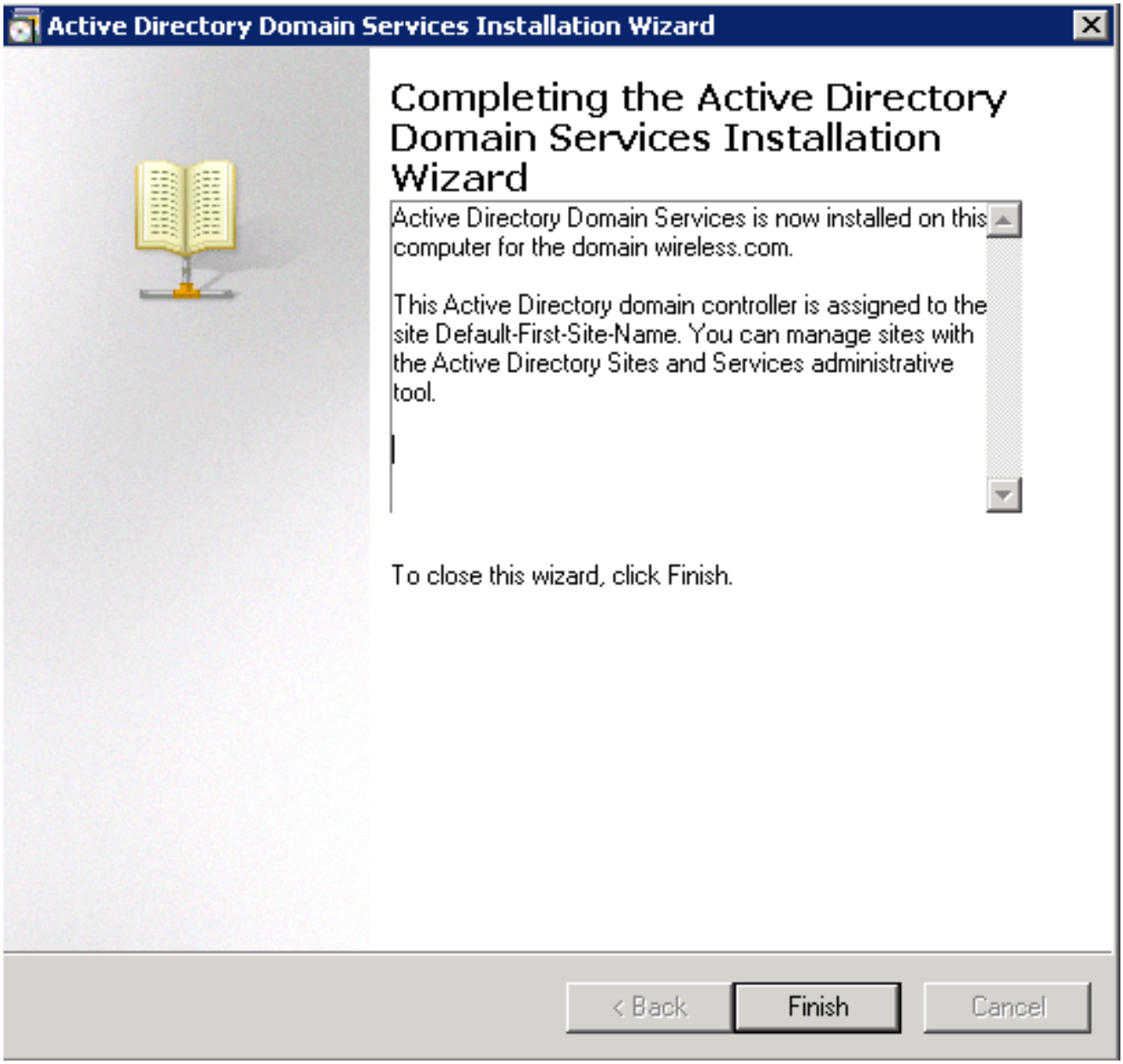


17. 選択内容を確認し、[Next] をクリックします。

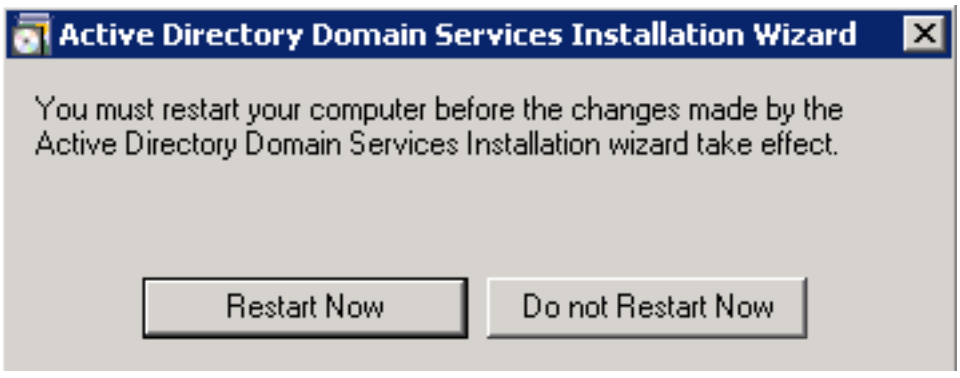


インストールが続行されます。

18. [Finish] をクリックしてウィザードを終了します。



19. 変更を反映するためにサーバを再起動します。

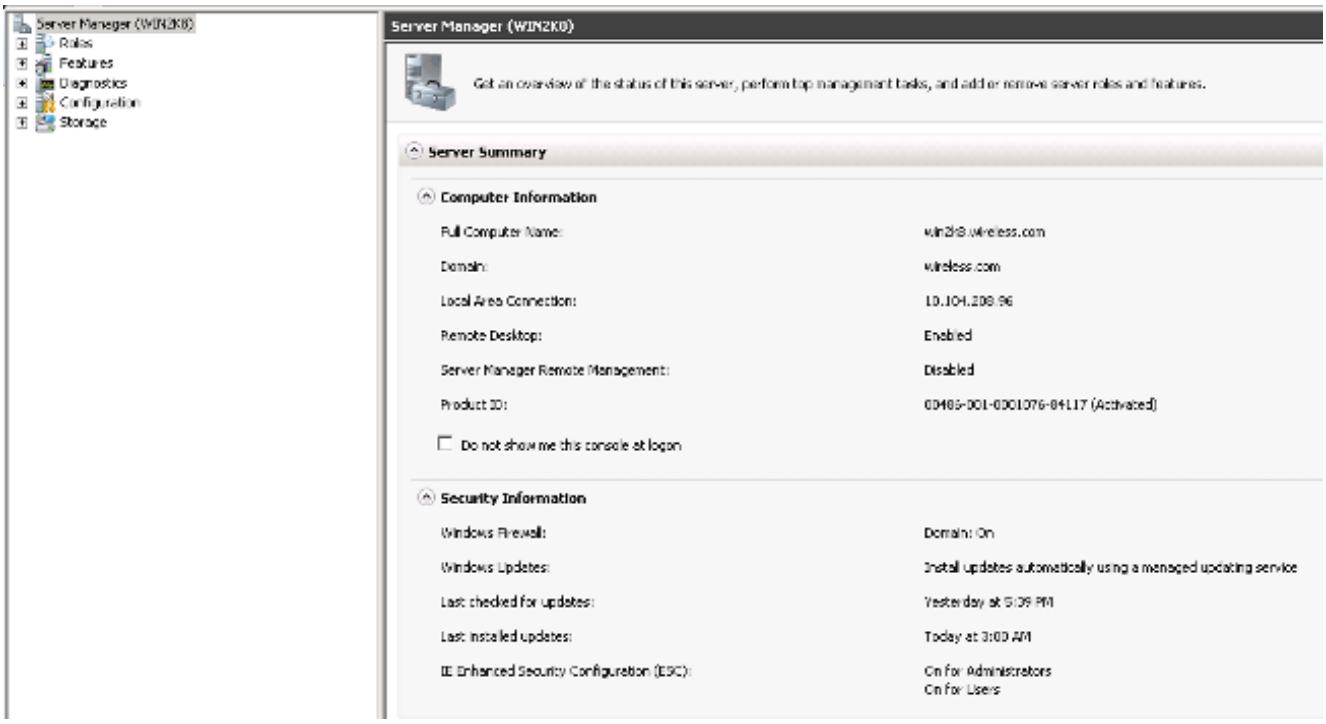


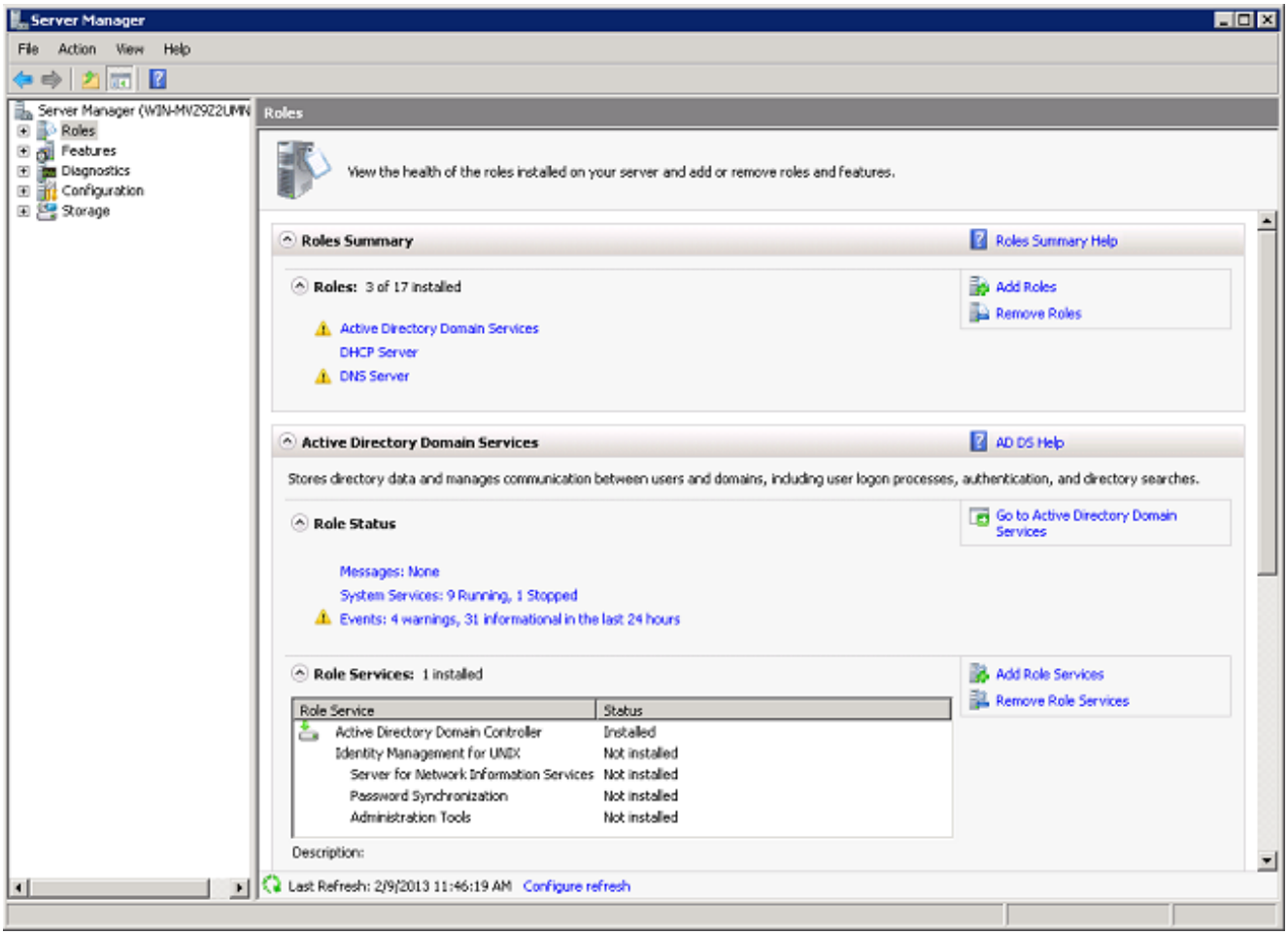
Microsoft Windows バージョン 2008 サーバの CA サーバとしてのインストールと設定

EAP-MS-CHAP v2 を使用する PEAP は、サーバにある証明書に基づいて RADIUS サーバの検証を行います。また、サーバ証明書は、クライアント コンピュータが信頼するパブリック CA によって発行する必要があります。つまり、パブリック CA 証明書は、クライアント コンピュータの証明書ストアの [Trusted Root Certification Authority] フォルダにすでに存在しています。

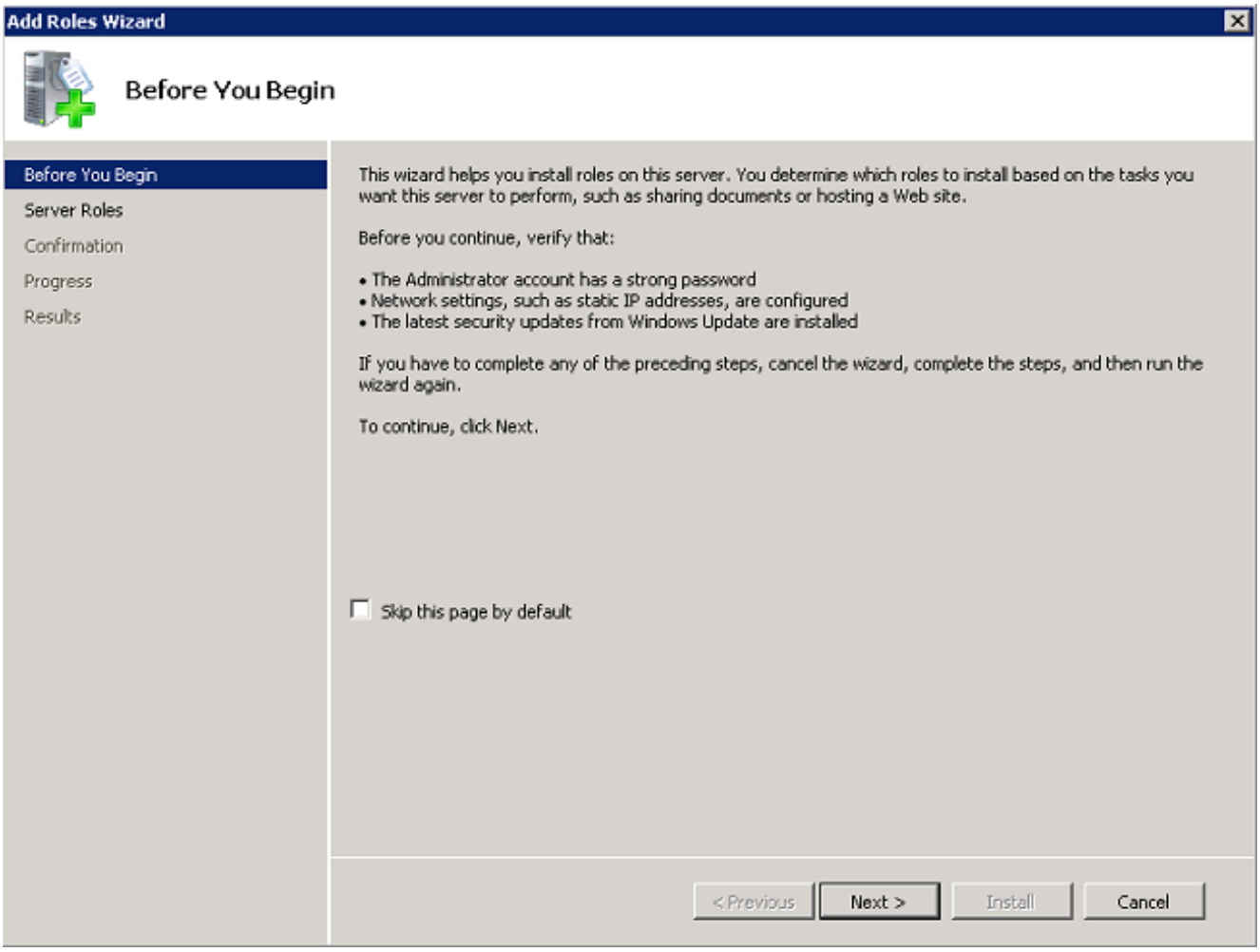
証明書を NPS に発行する CA サーバとして Microsoft Windows バージョン 2008 サーバを設定するには、次の手順を実行します。

1. [Start] > **[Server Manager] > [Roles] > [Add Roles]** に移動します。

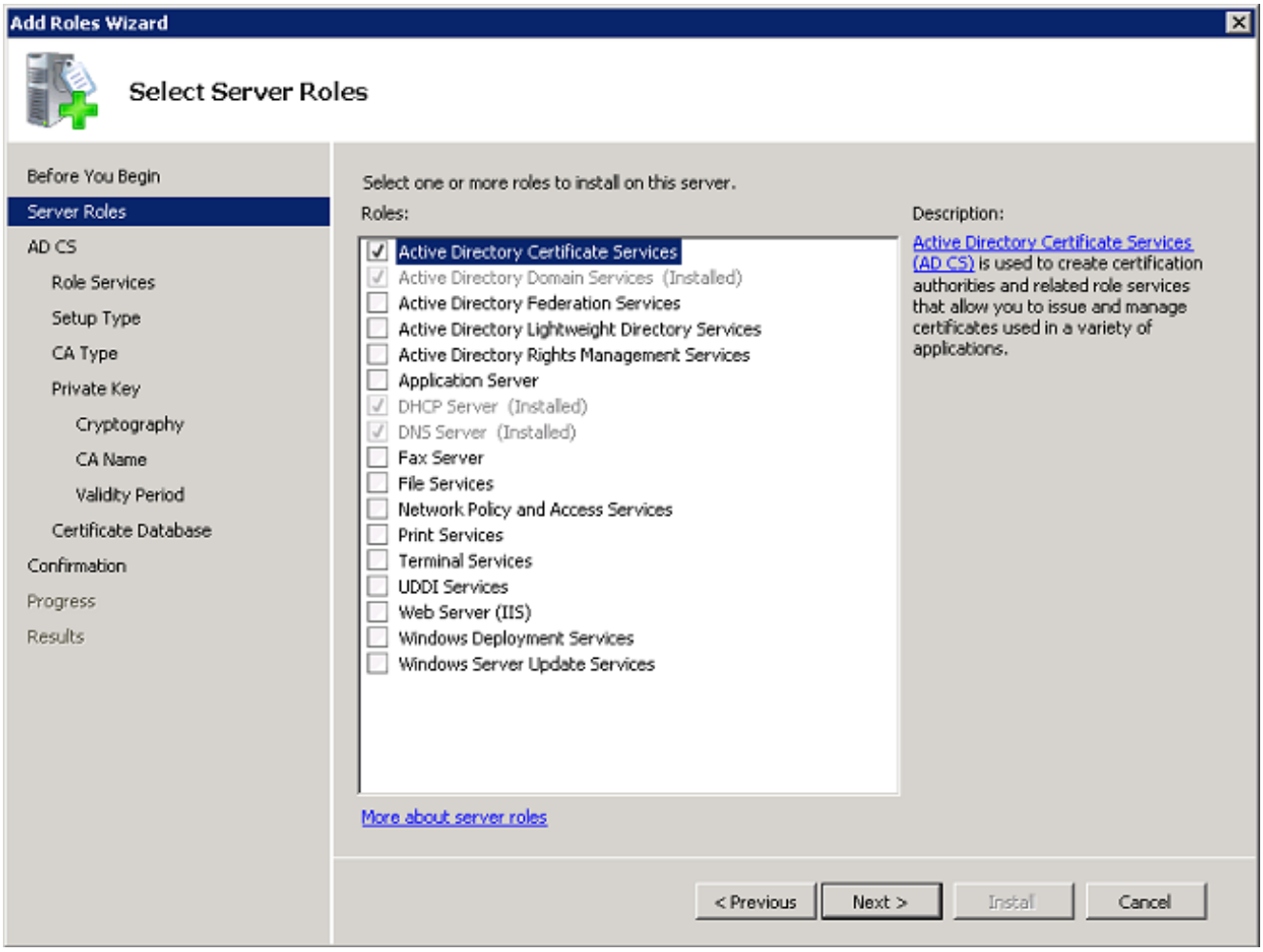




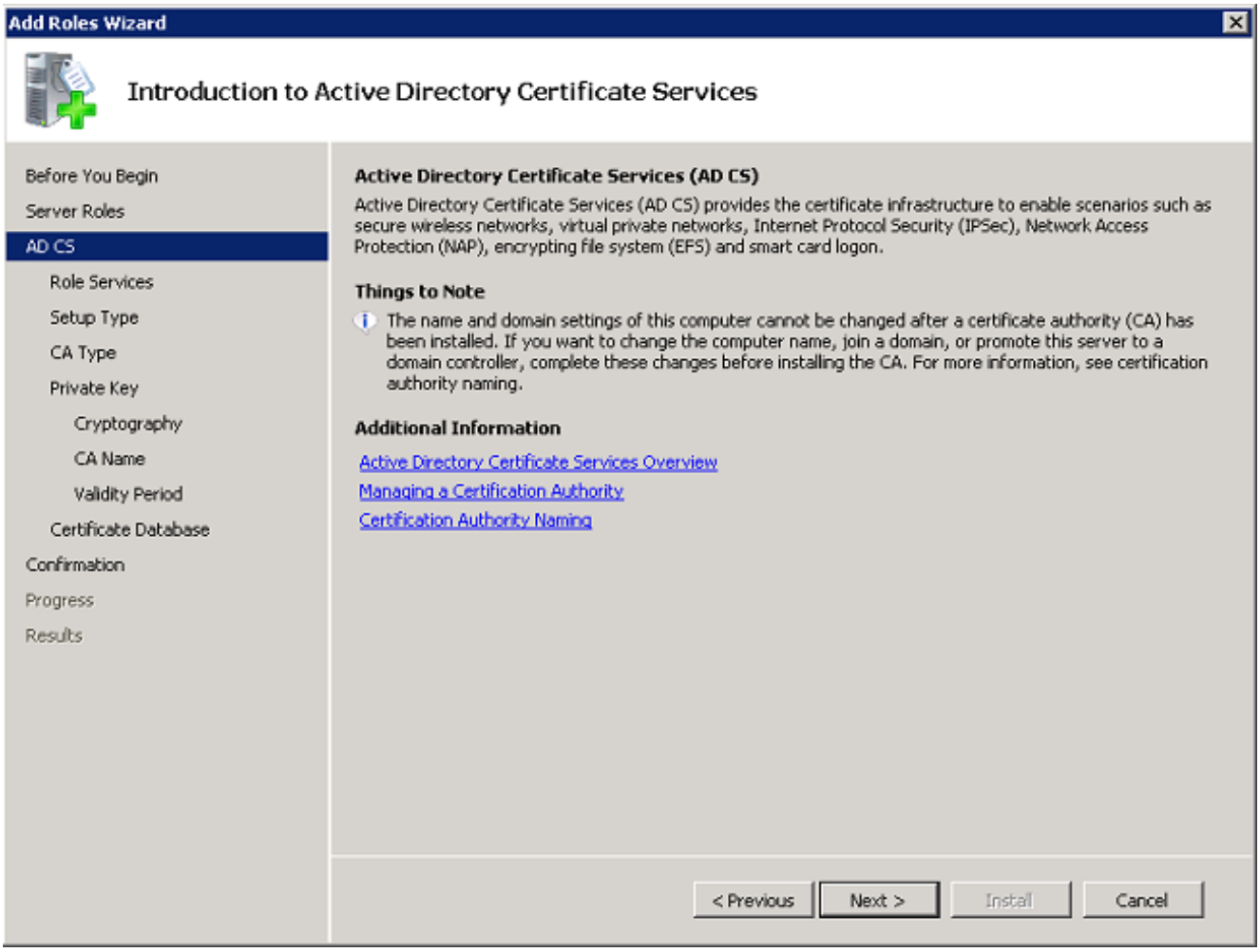
2. [next] をクリックします。



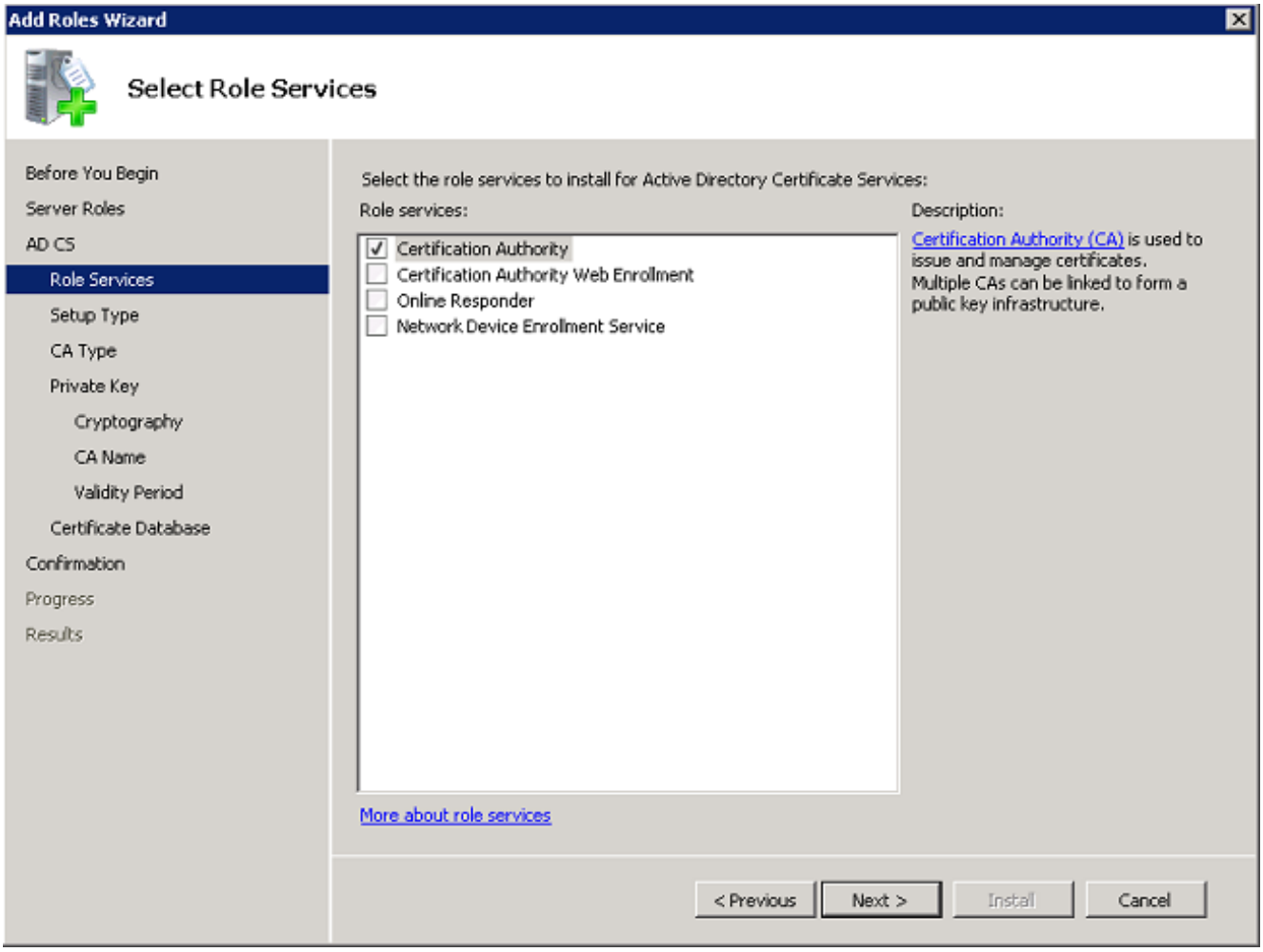
3. [Active Directory Certificate Services] チェックボックスをオンにし、[Next] をクリックします。



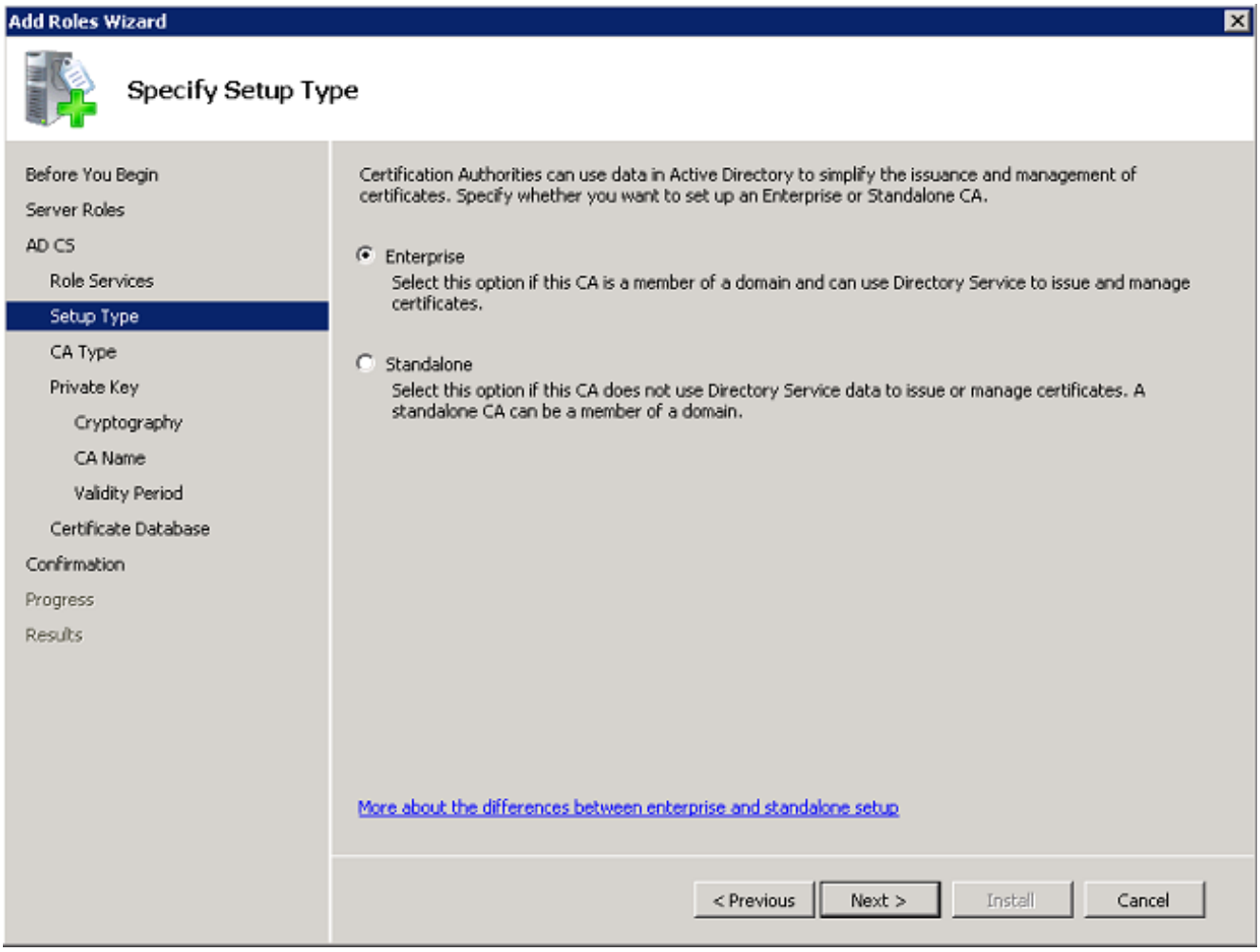
4. 「Introduction to Active Directory Certificate Services」に目を通し、[Next] をクリックします。



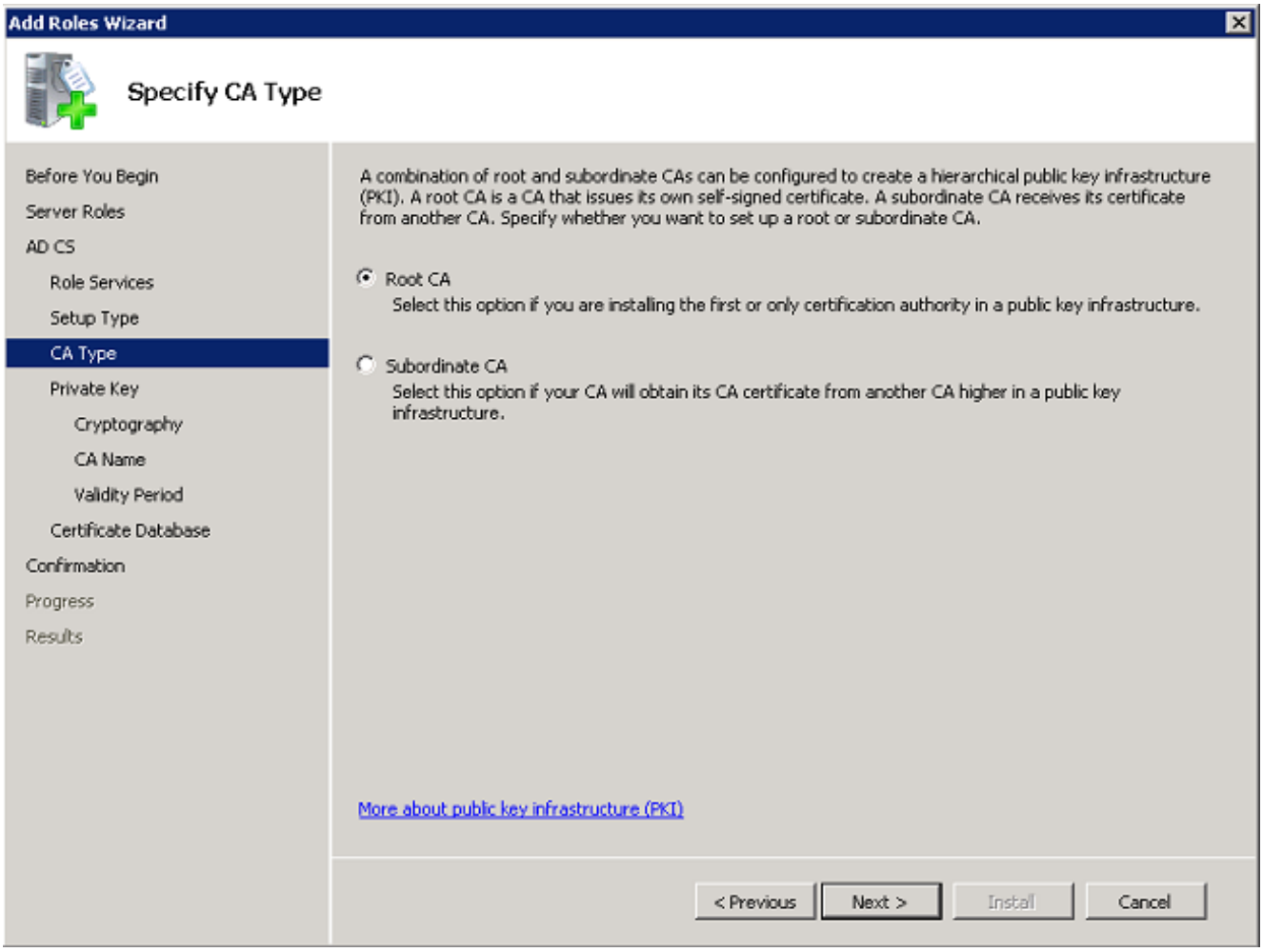
5. [Certificate Authority] チェックボックスをオンにし、[Next] をクリックします。



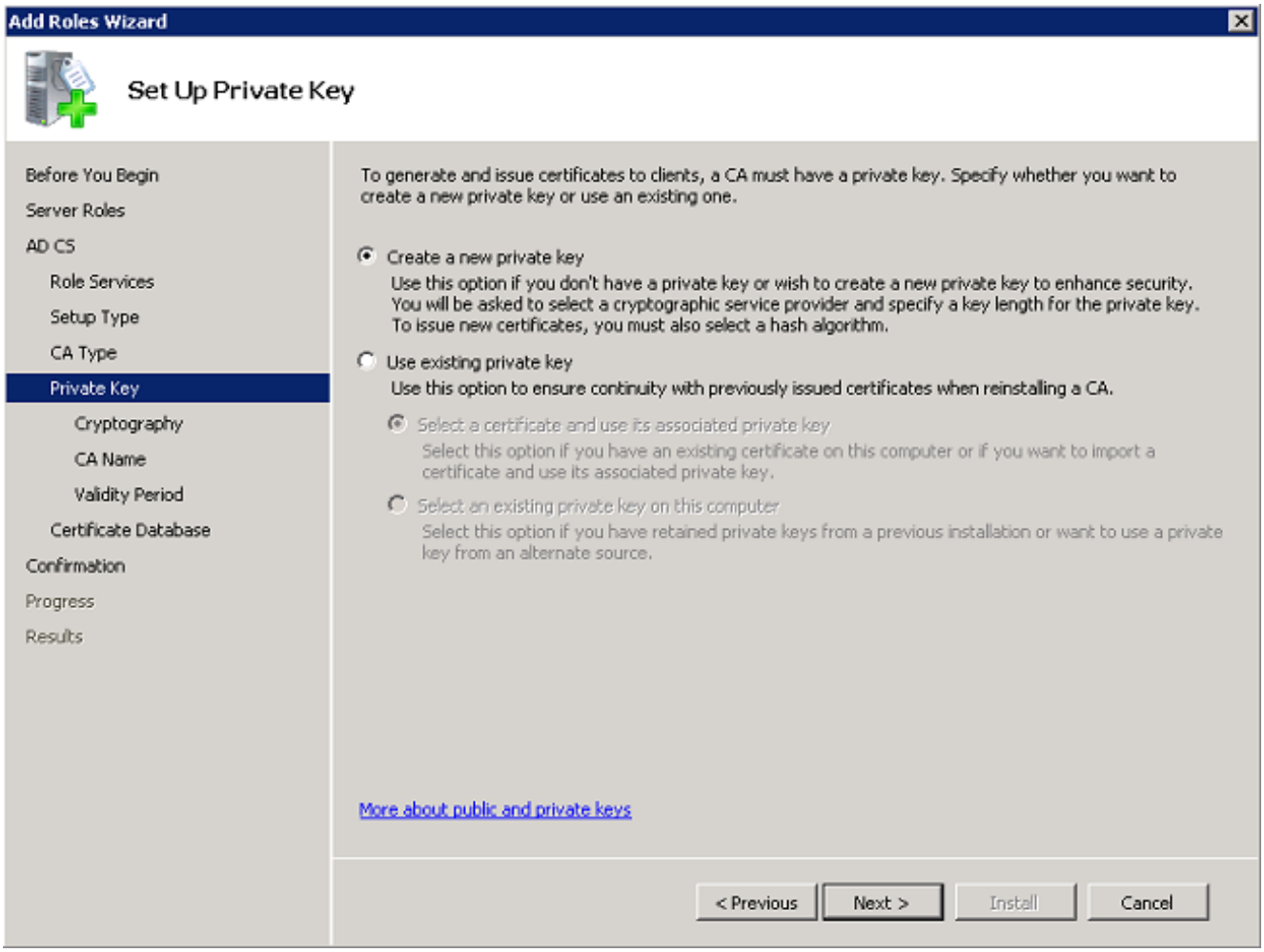
6. [Enterprise] **オプション ボタンをクリックし、[Next] をクリックします。**



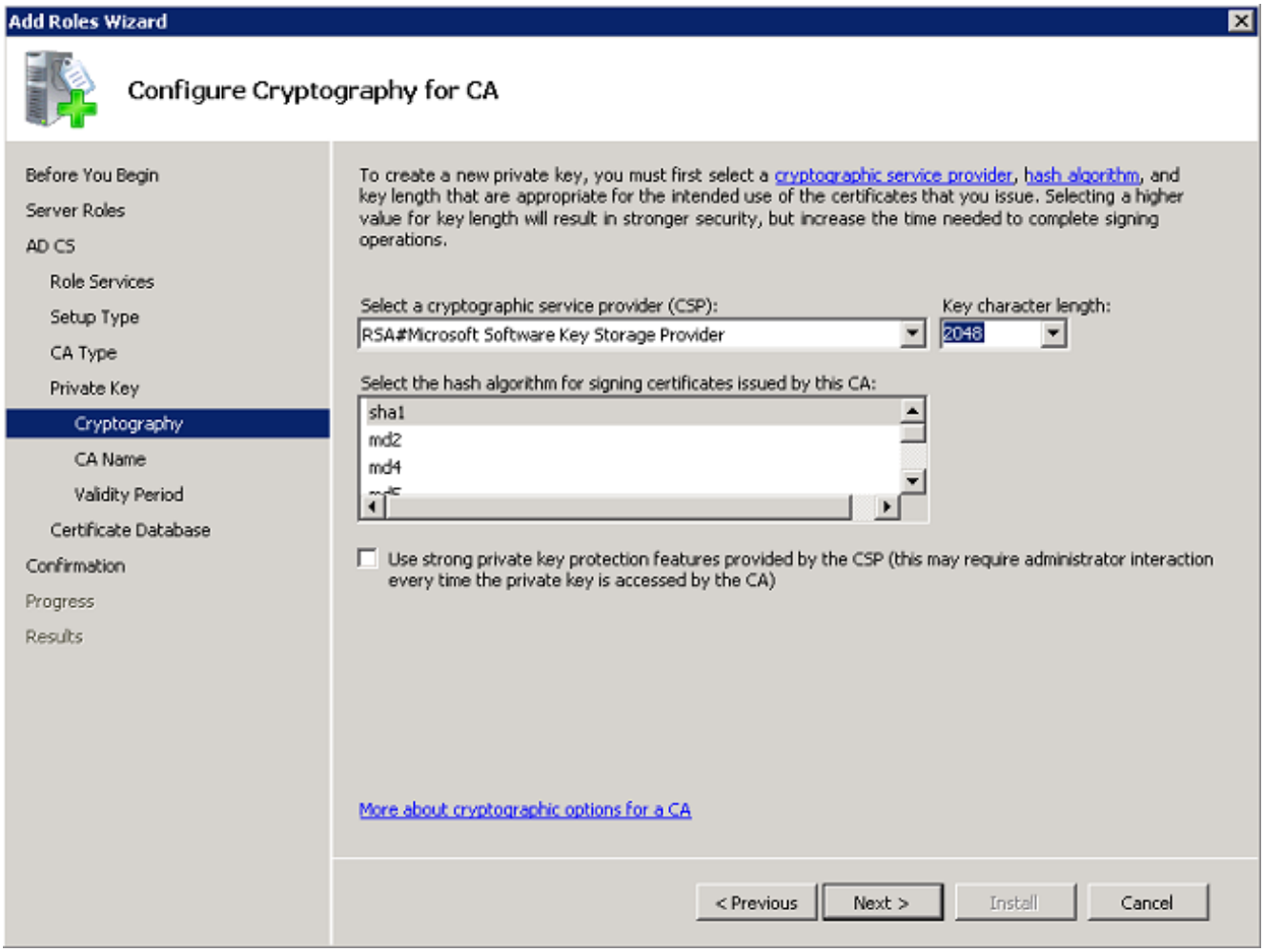
7. [Root CA] **オプション ボタンをクリックし、[Next] をクリックします。**



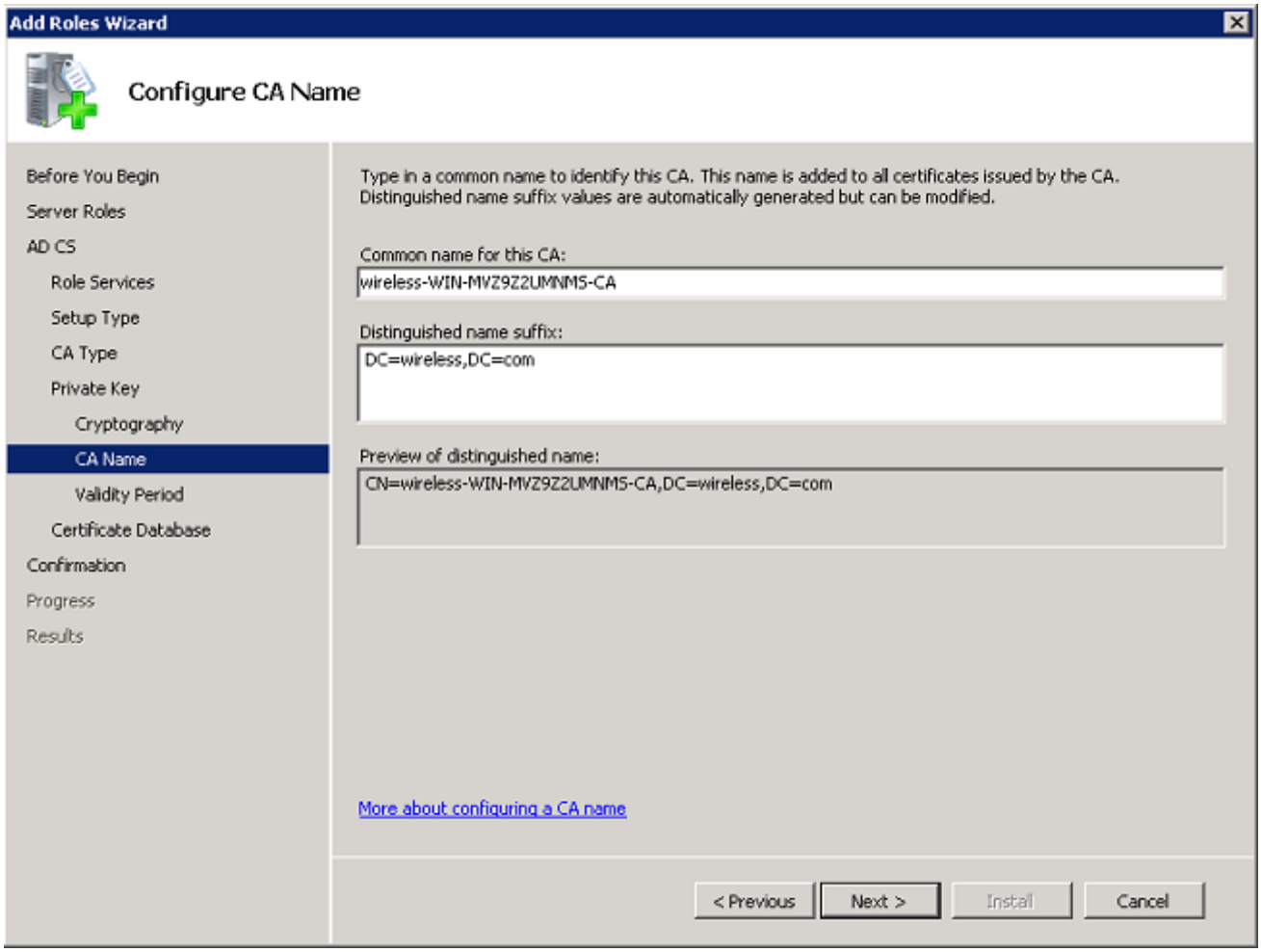
8. [Create a new private key]**オプションボタンをクリックし、**[**Next**]をクリック**します。**



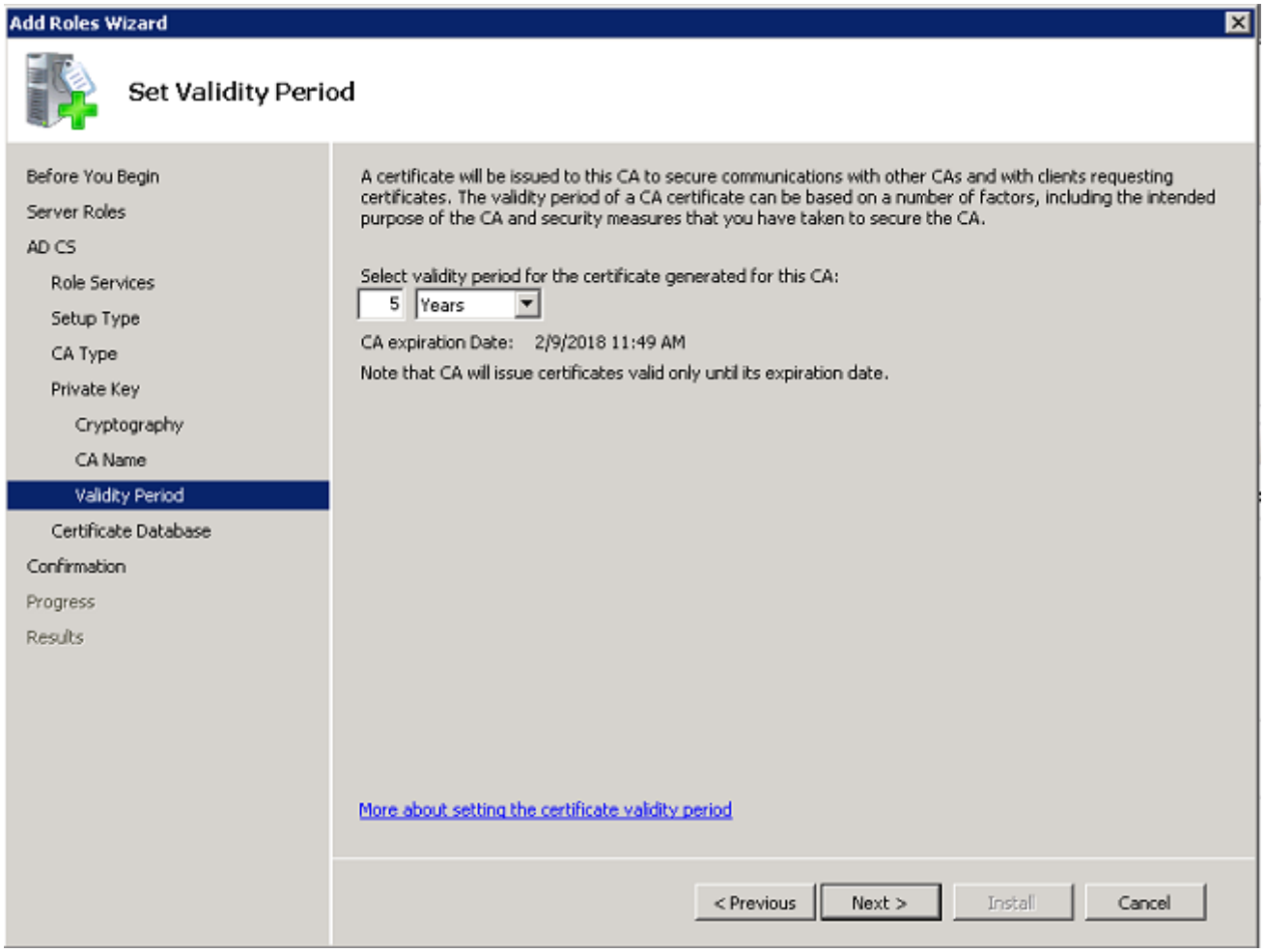
9. [Configuring Cryptography for CA] ウィンドウで [Next] をクリックします。



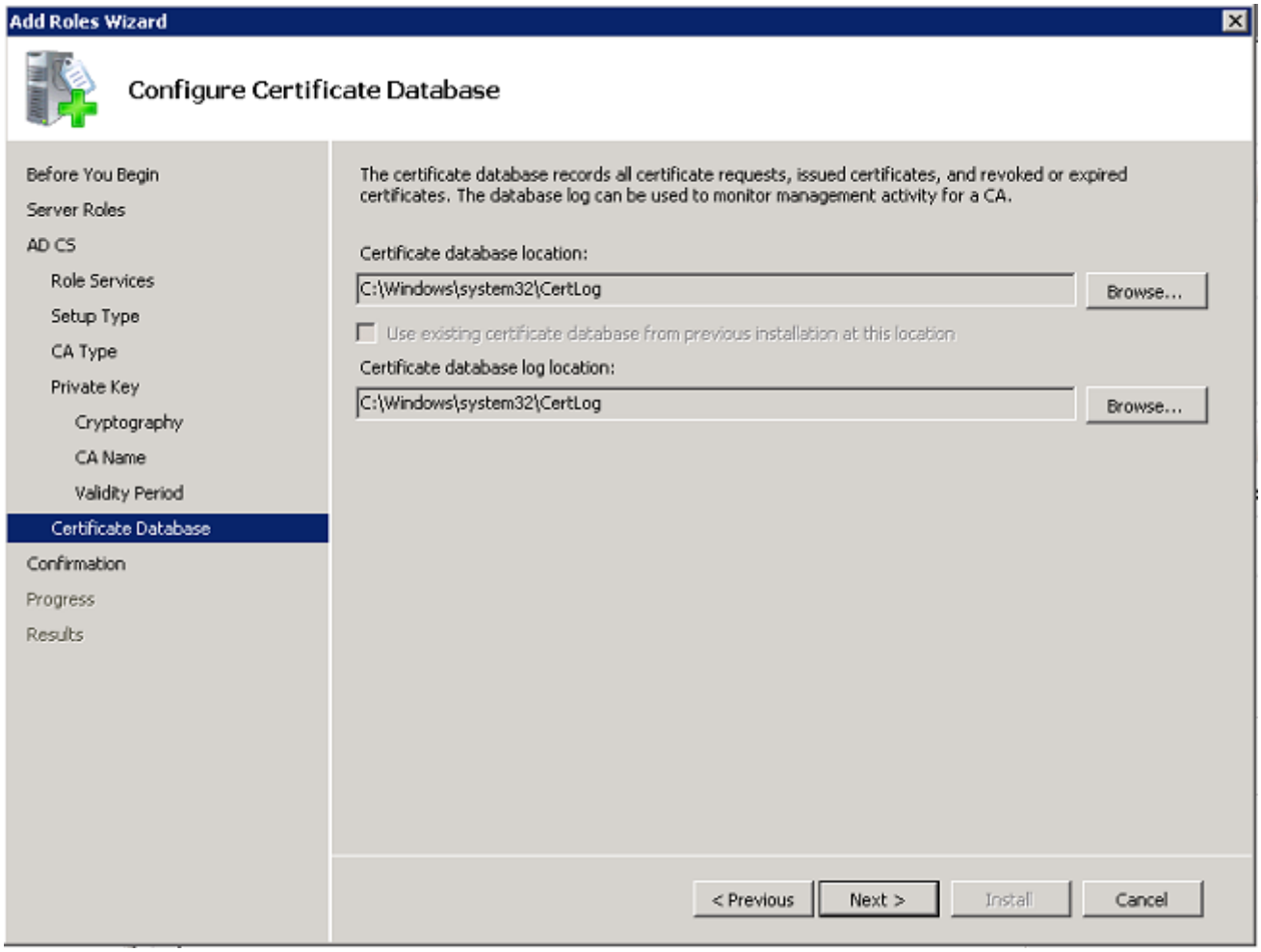
10. [Common name for this CA] のデフォルトの名前を承認したら、[Next] をクリックします。



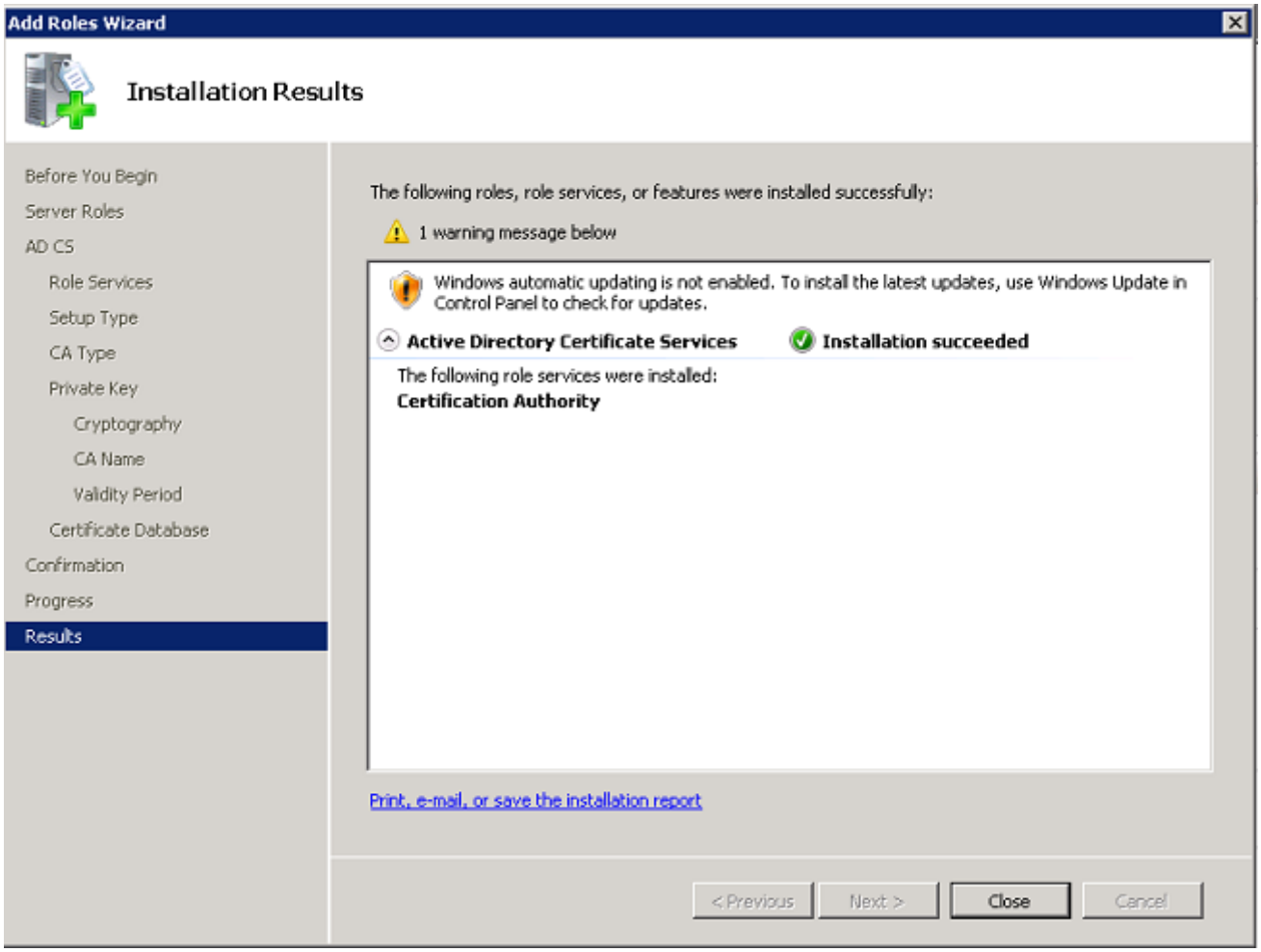
11. CA 証明書の有効期間を選択し、[Next] をクリックします。



12. [Certificate database location] のデフォルトの場所を承認したら、[Next] をクリックします。



13. 設定を見直し、[Install] をクリックして [Active Directory Certificate Services] を開始します。



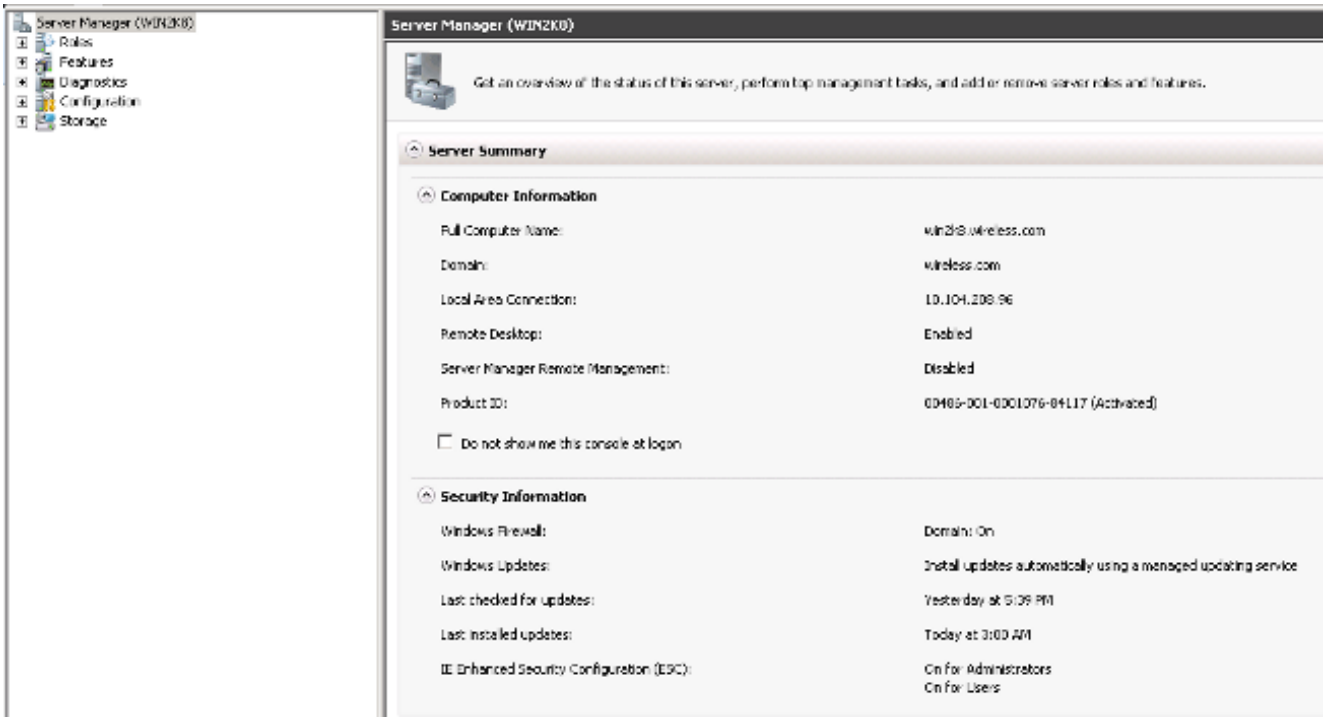
14. インストールが完了したら、[Close] をクリックします。

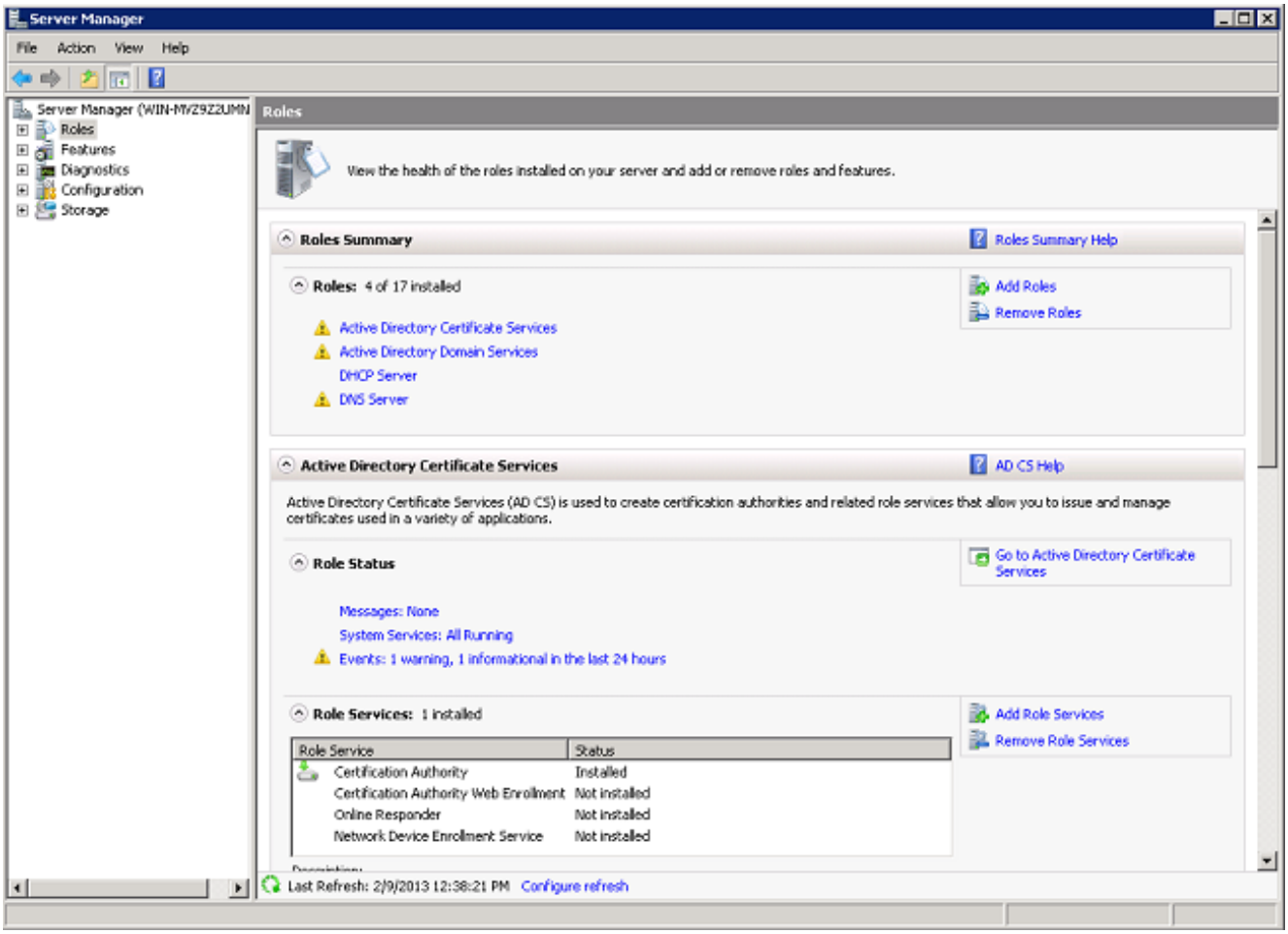
Microsoft Windows バージョン 2008 サーバへの NPS のインストール

> **注**：このセクションで説明した設定により、NPS が RADIUS サーバとして使用され、PEAP 認証でワイヤレス クライアントを認証します。

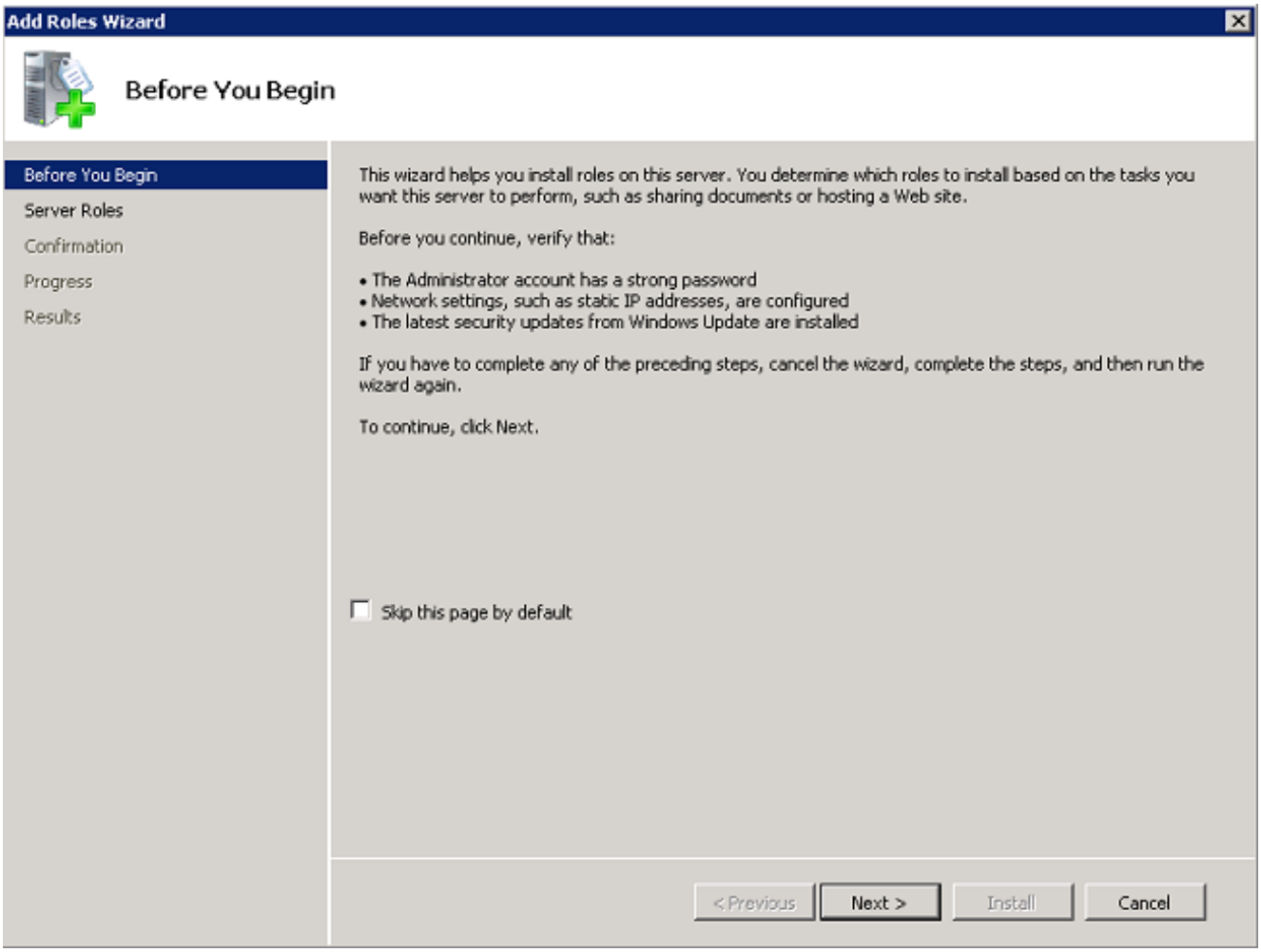
Microsoft Windows バージョン 2008 サーバで NPS をインストールして設定するには、次の手順を実行します。

1. [Start] **> [Server Manager] > [Roles] > [Add Roles]** に移動します。

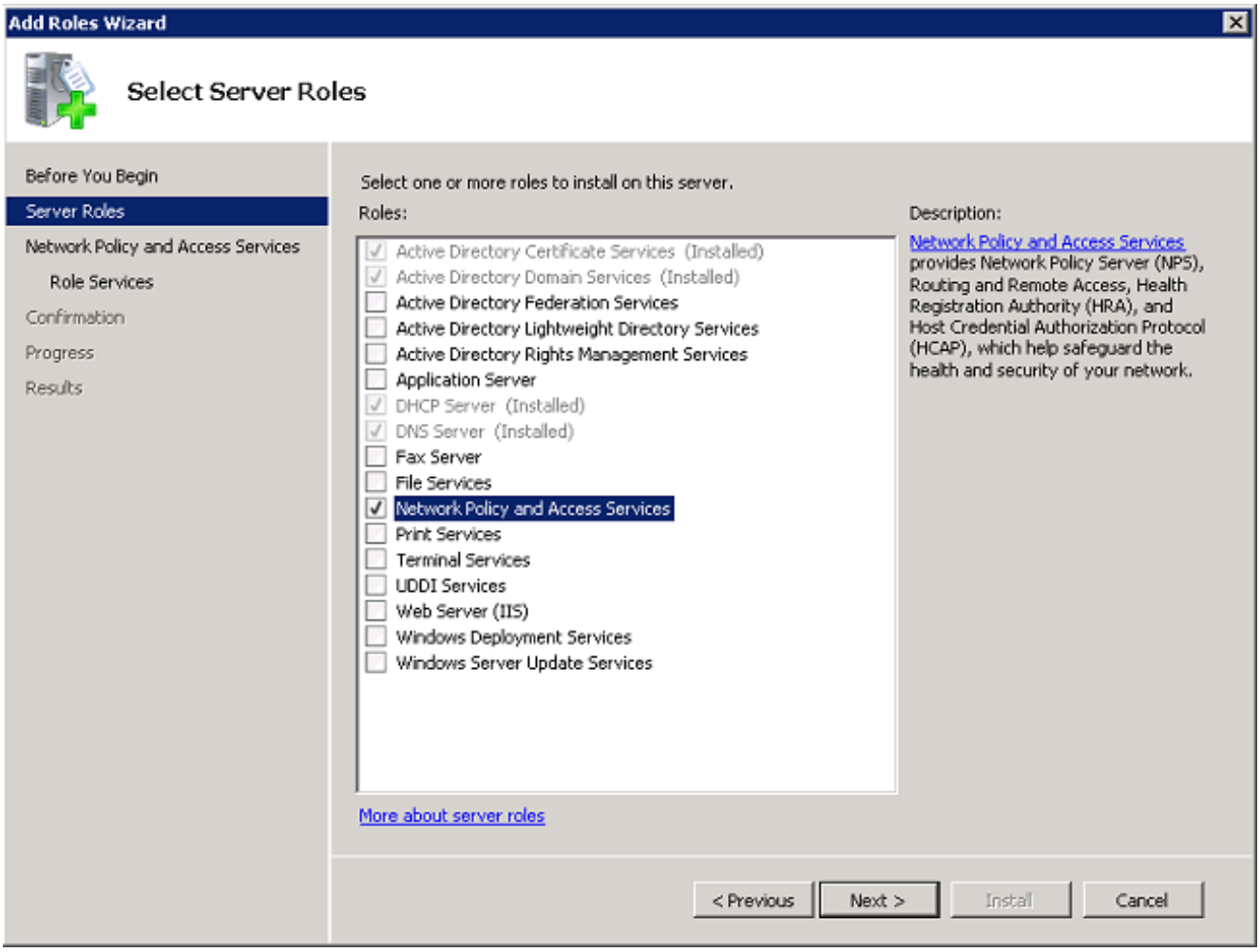




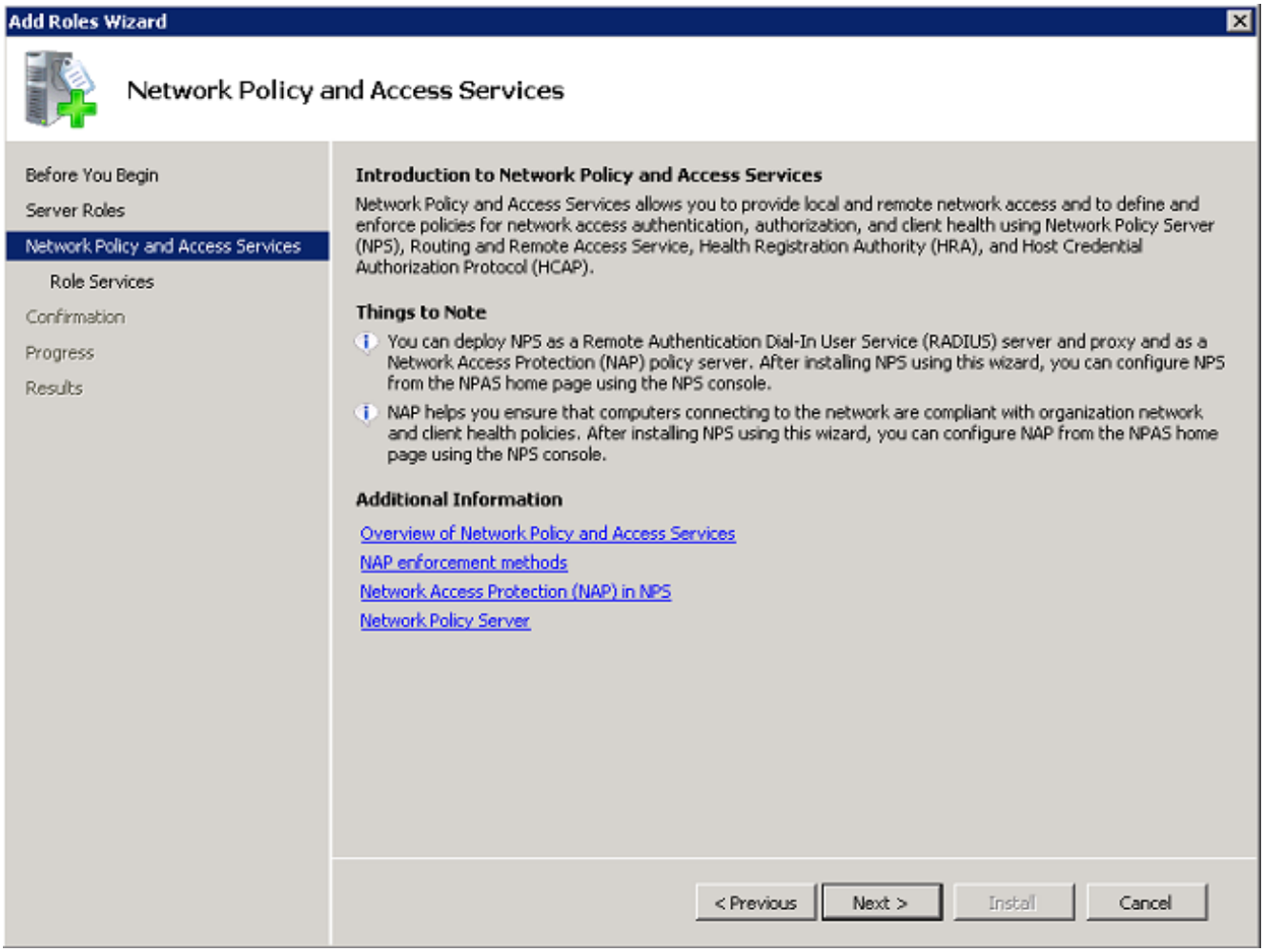
2. [next] をクリックします。



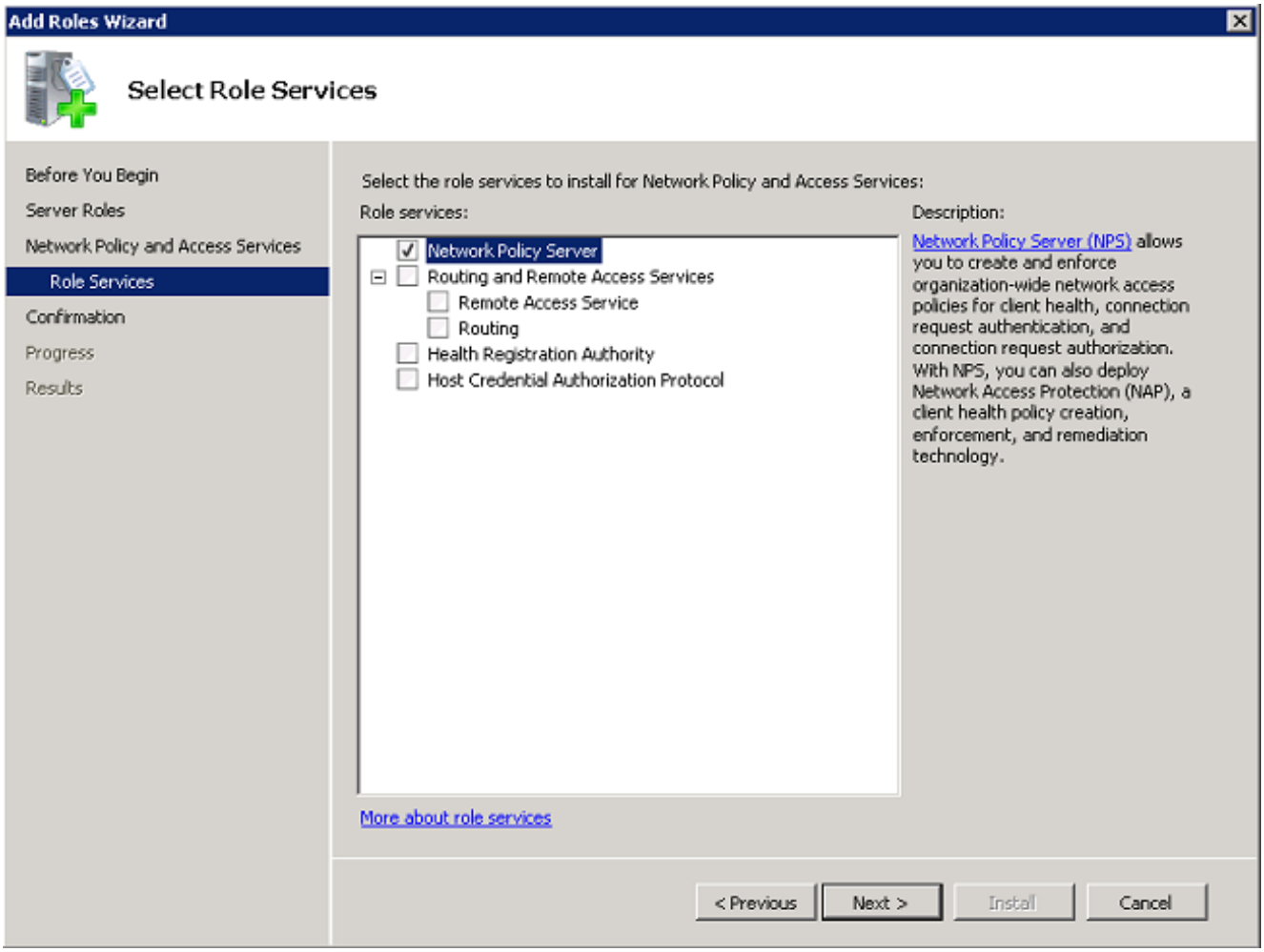
3. [Network Policy and Access Services] **チェックボックスをオンにし、[Next] をクリックします。**



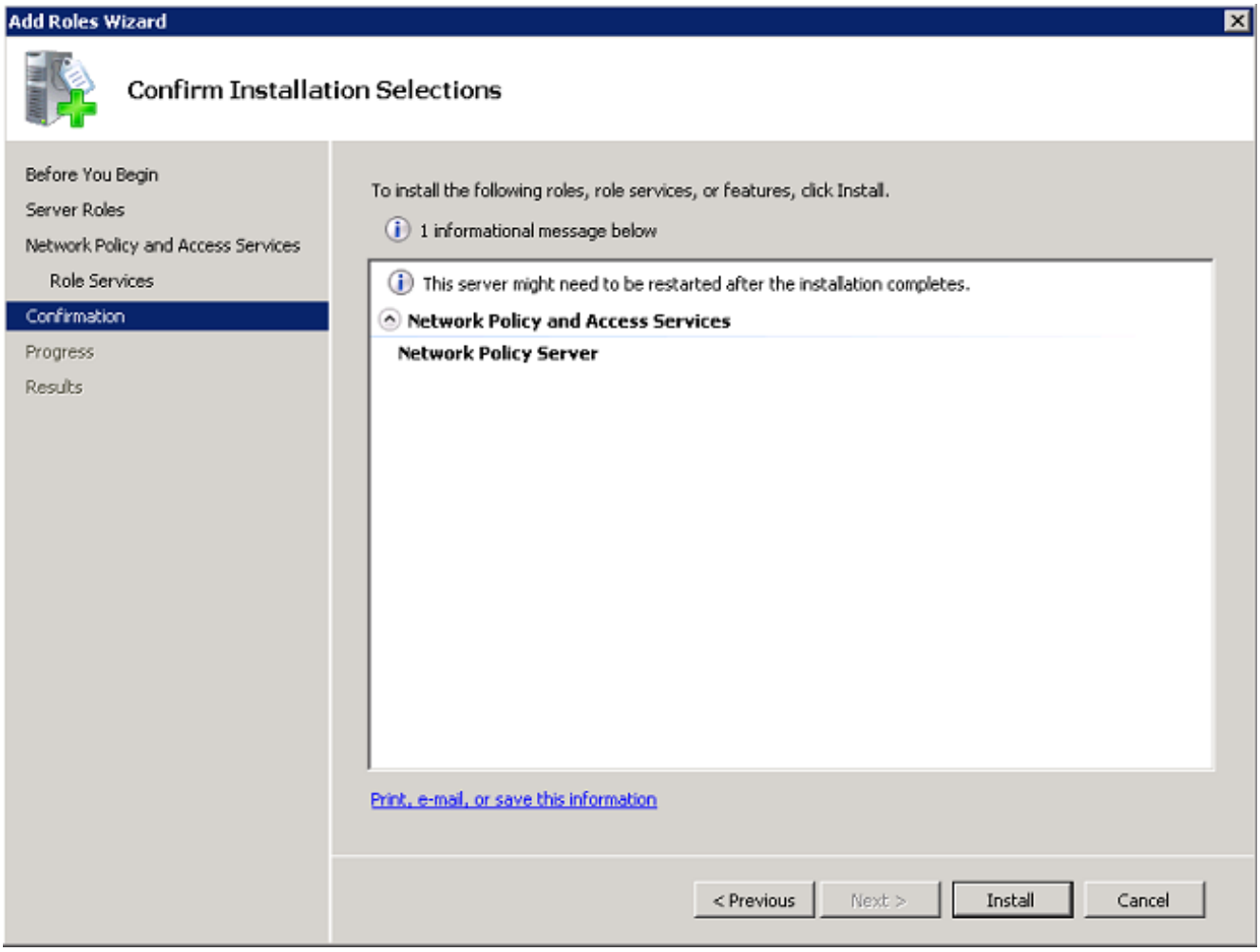
4. 「Introduction to Network Policy and Access Services」に目を通し、[Next] をクリックします。



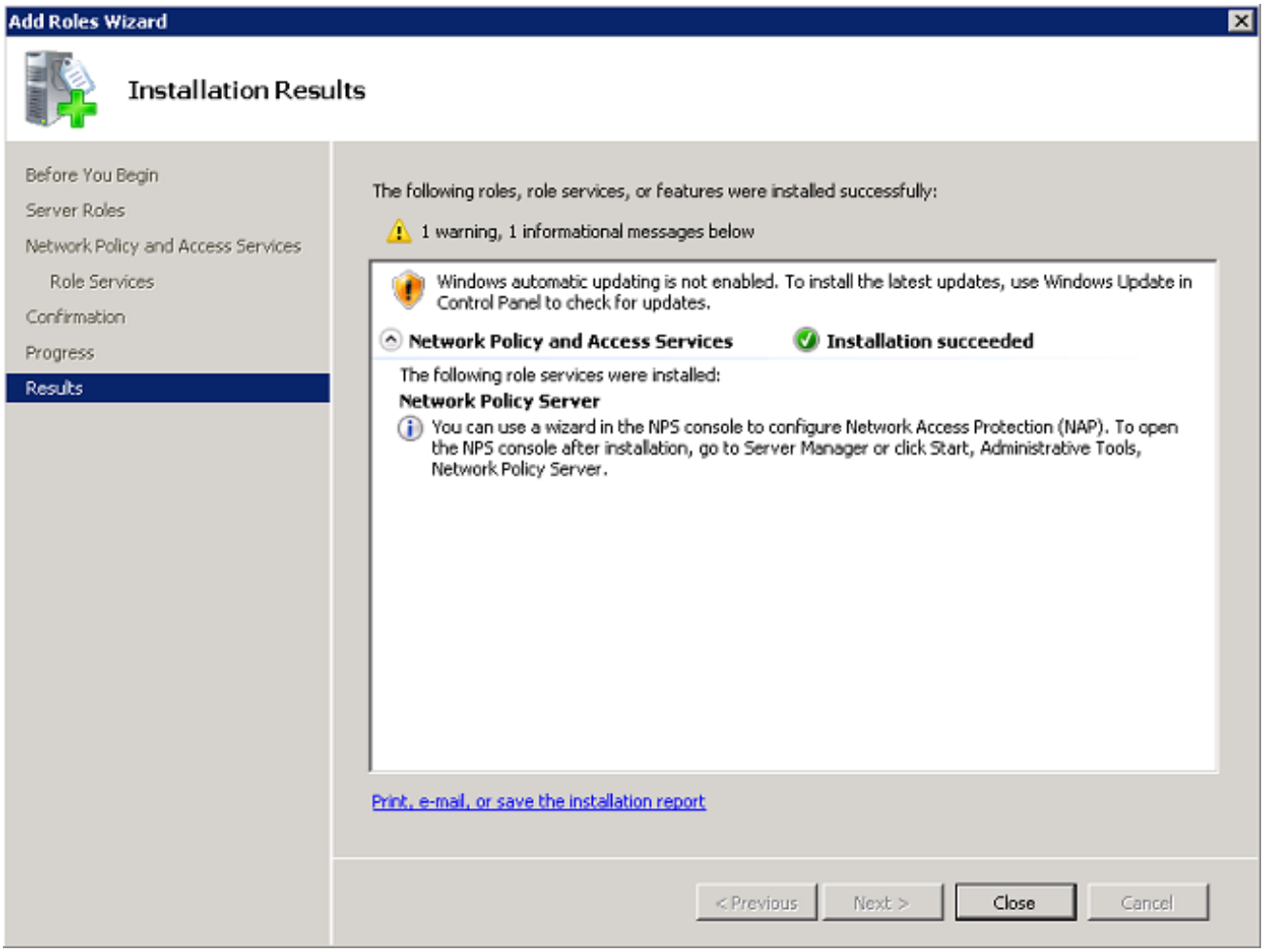
5. [ネットワークポリ**シーサーバー]チェックボックス**をオンにし、[次へ]**をクリックします。**



6. 確認事項を見直し、[Install] をクリックします。



インストールが完了すると、次のような画面が表示されます。

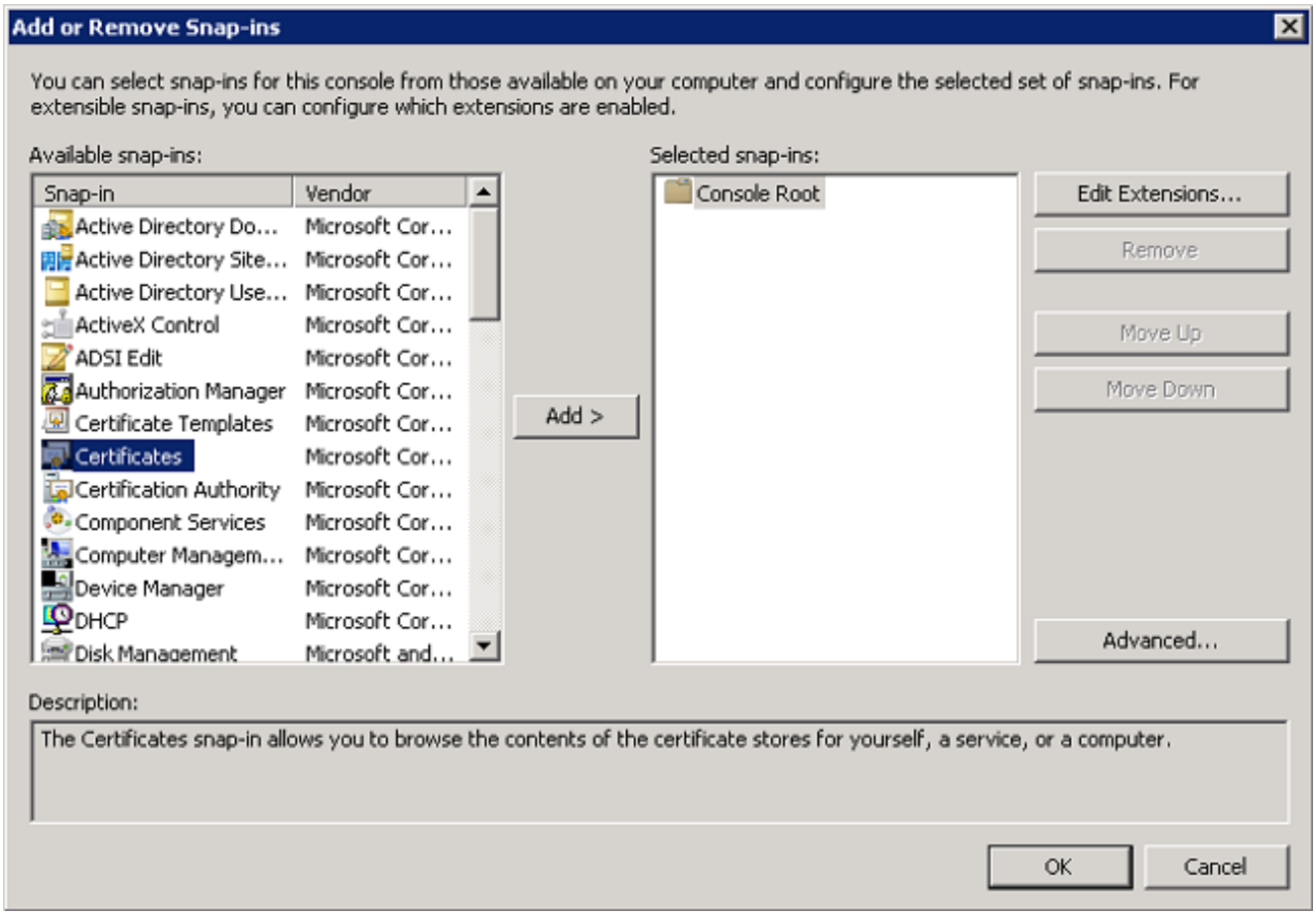


7. [Close] をクリックします。

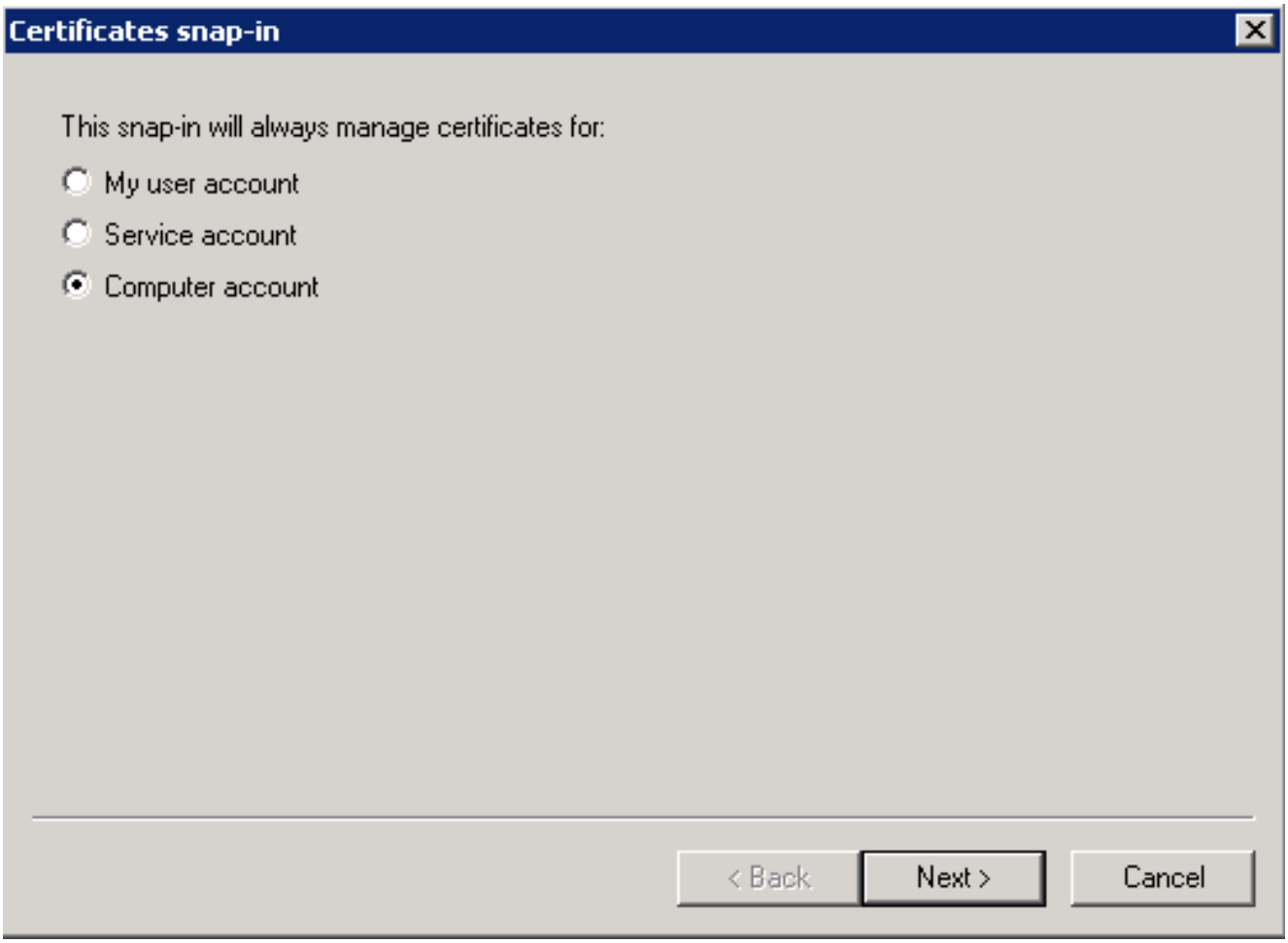
証明書のインストール

コンピュータ証明書を NPS にインストールするには、次の手順を実行します。

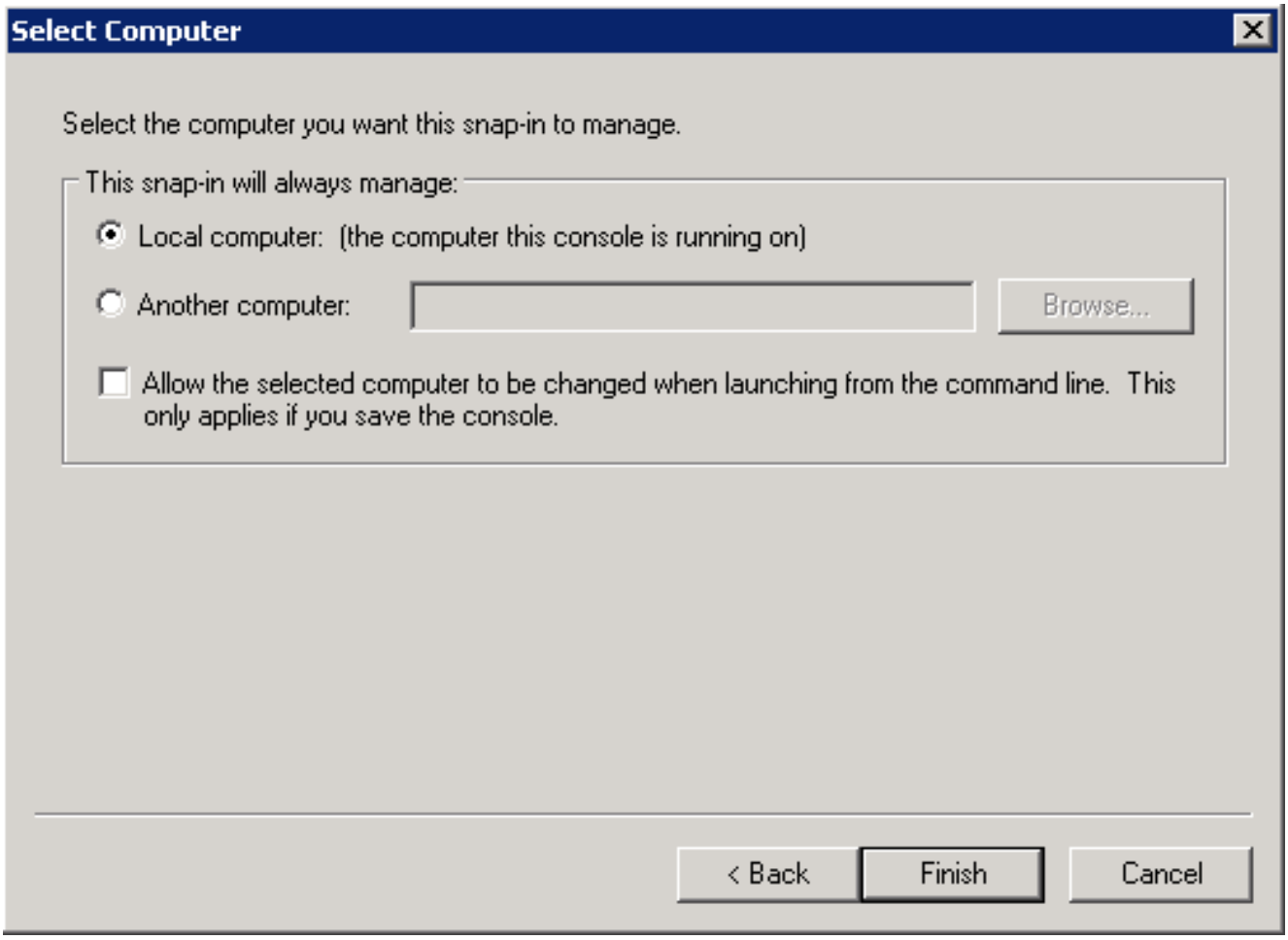
1. [Start] をクリックして Microsoft 管理コンソール（MMC）を開始し、Enter キーを押します。
2. [File] > [Add/Remove Snap-in] に移動します。
3. [Certificates] **を選択して、[Add] をクリックします。**



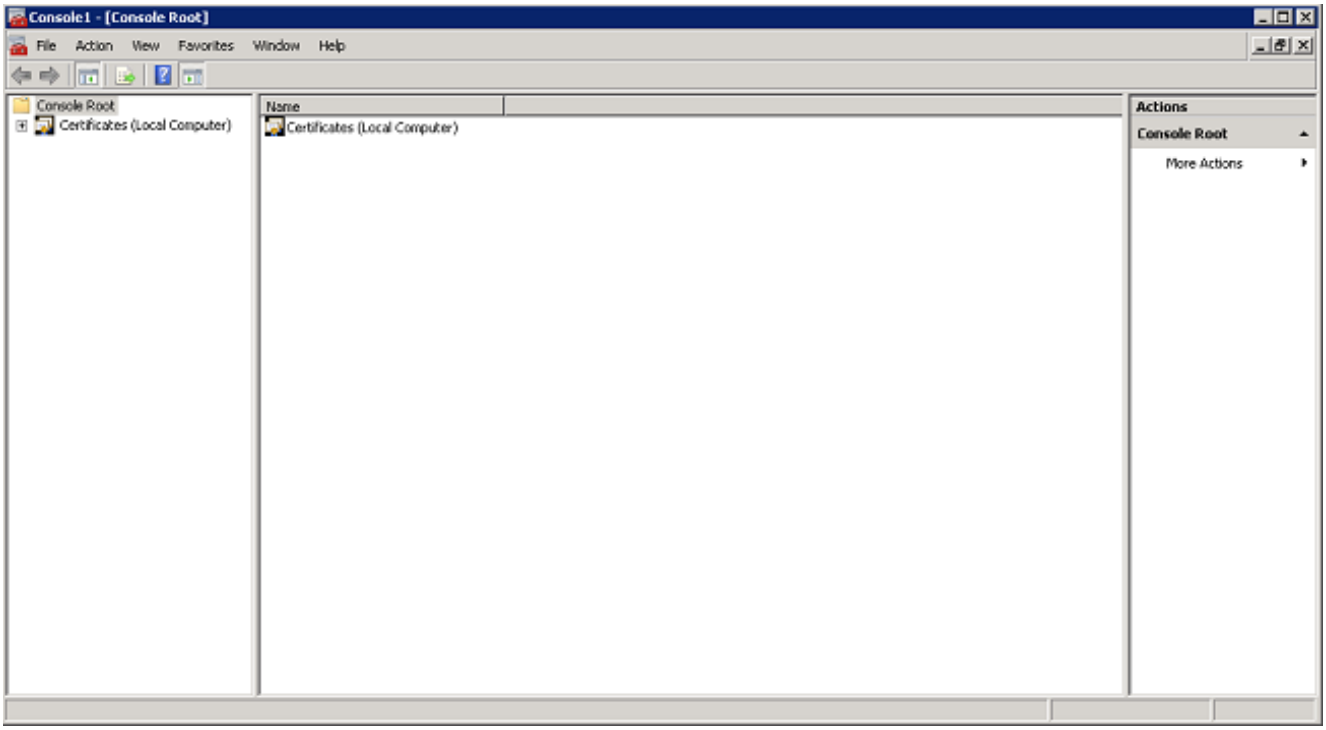
4. [Computer account] **オプション ボタンをクリックし、[Next] をクリックします。**



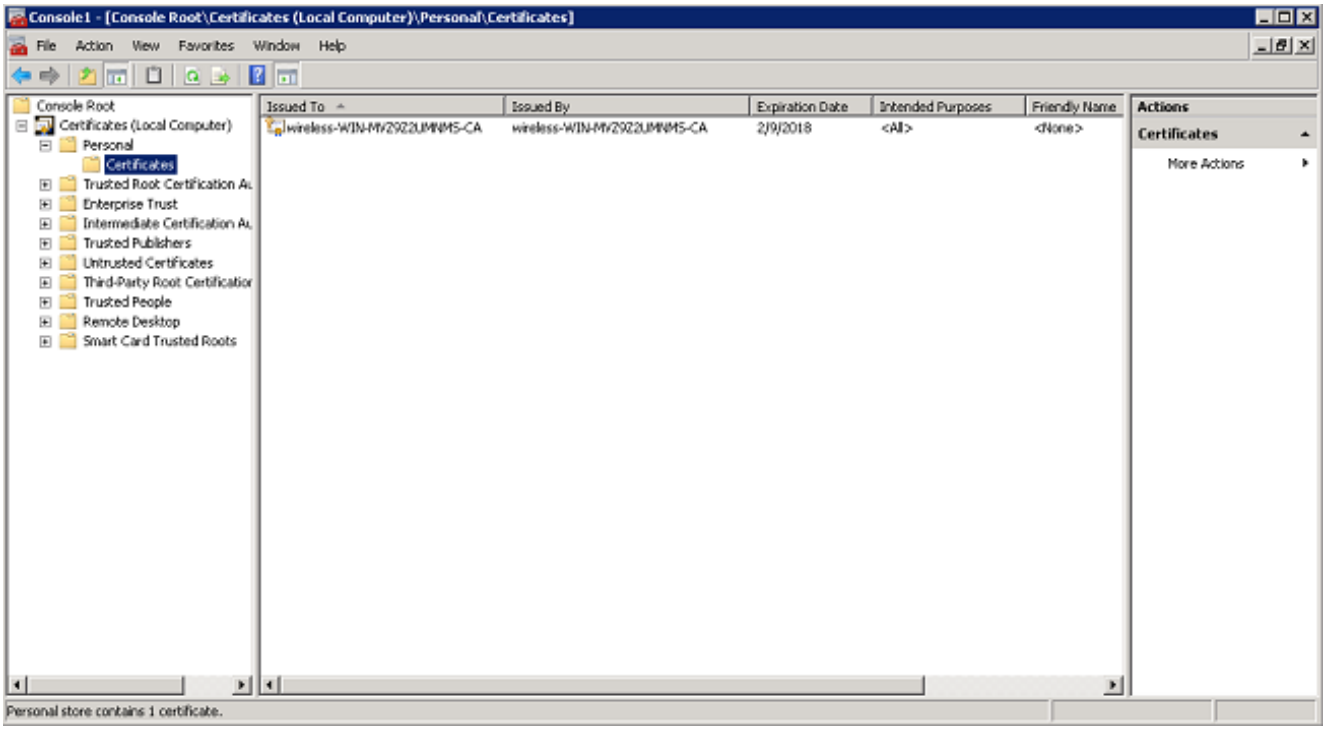
5. [ローカルコンピュータ]ラジオボタンをクリックし、[完了]をクリックします。



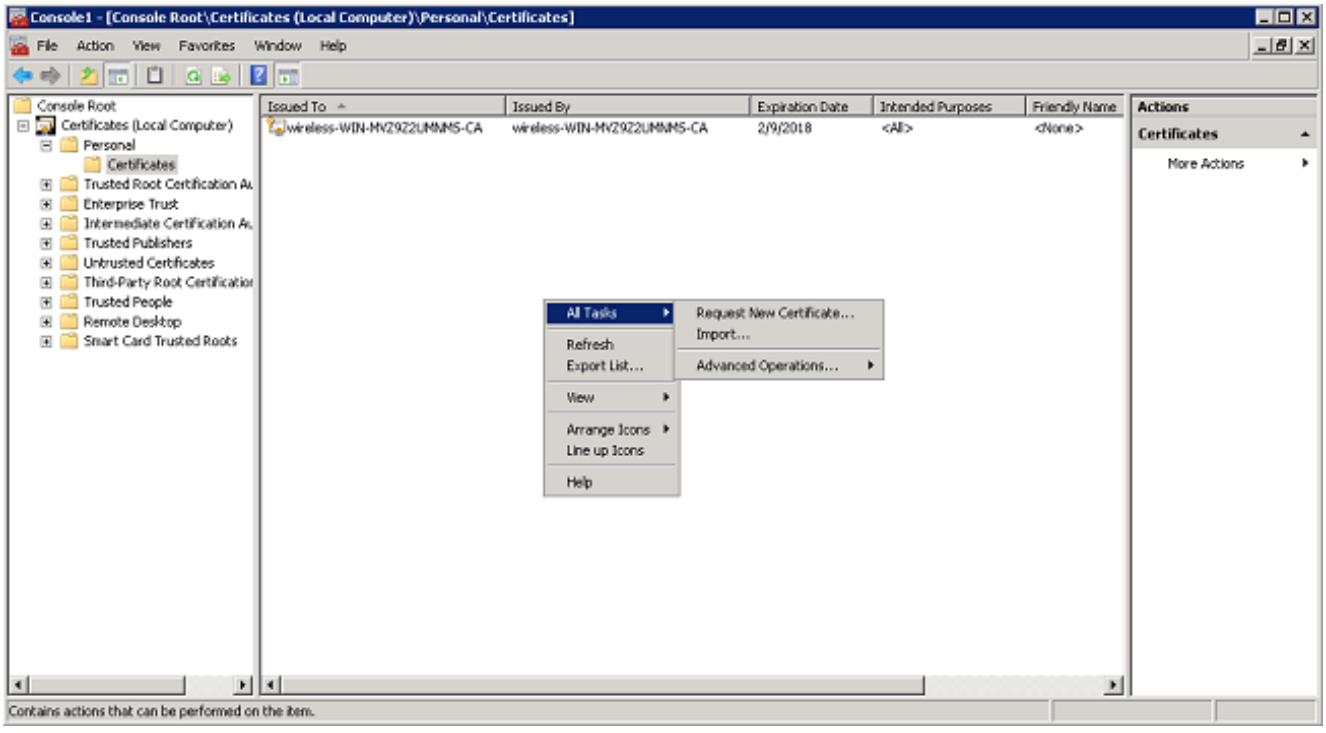
6. [OK] をクリックして MMC に戻ります。



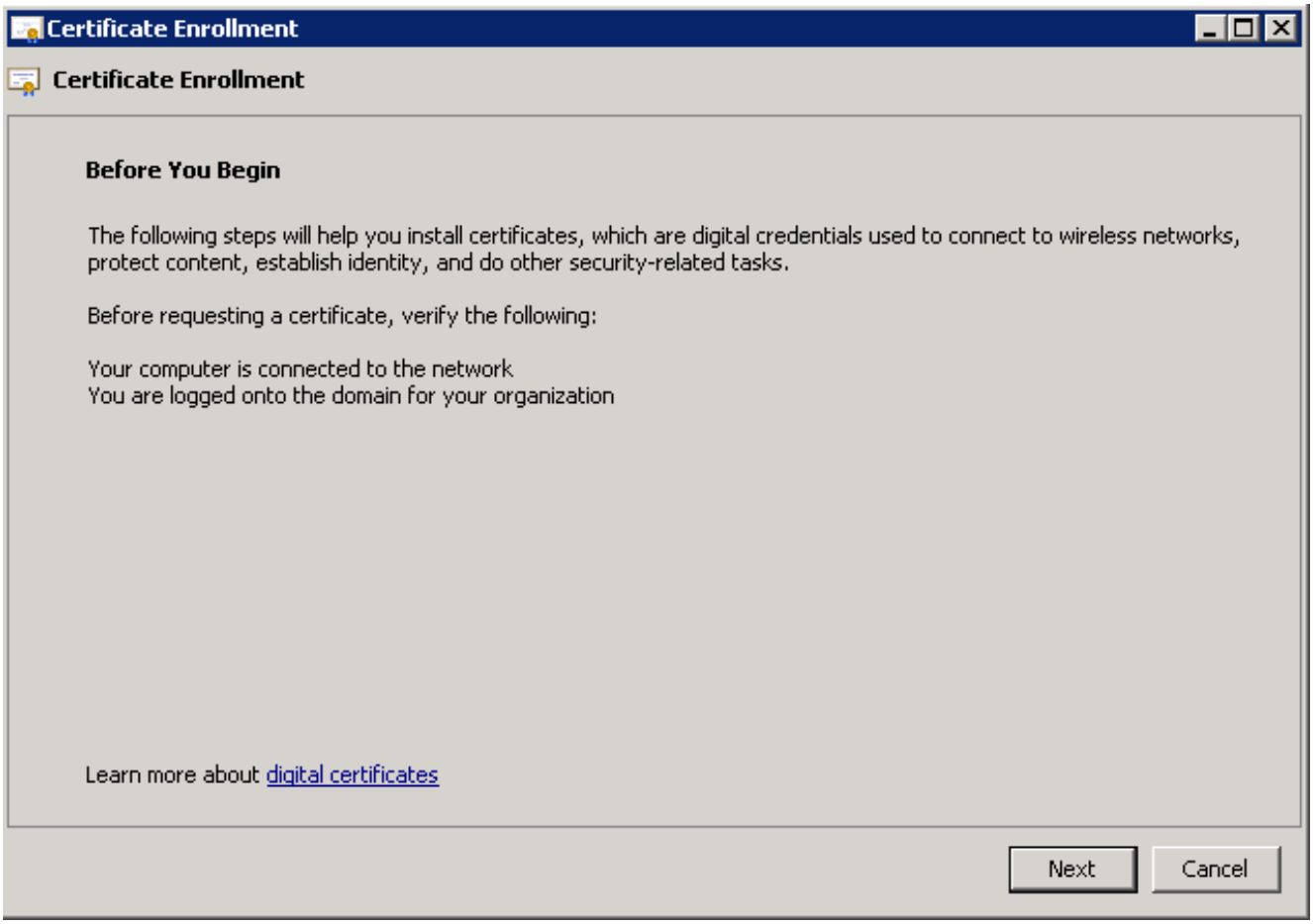
7. [Certificates (Local Computer)] と [Personal] フォルダを展開し、[Certificates] をクリックします。



8. CA 証明書の空白領域を右クリックし、[All Tasks] > [Request New Certificate] を選択します。

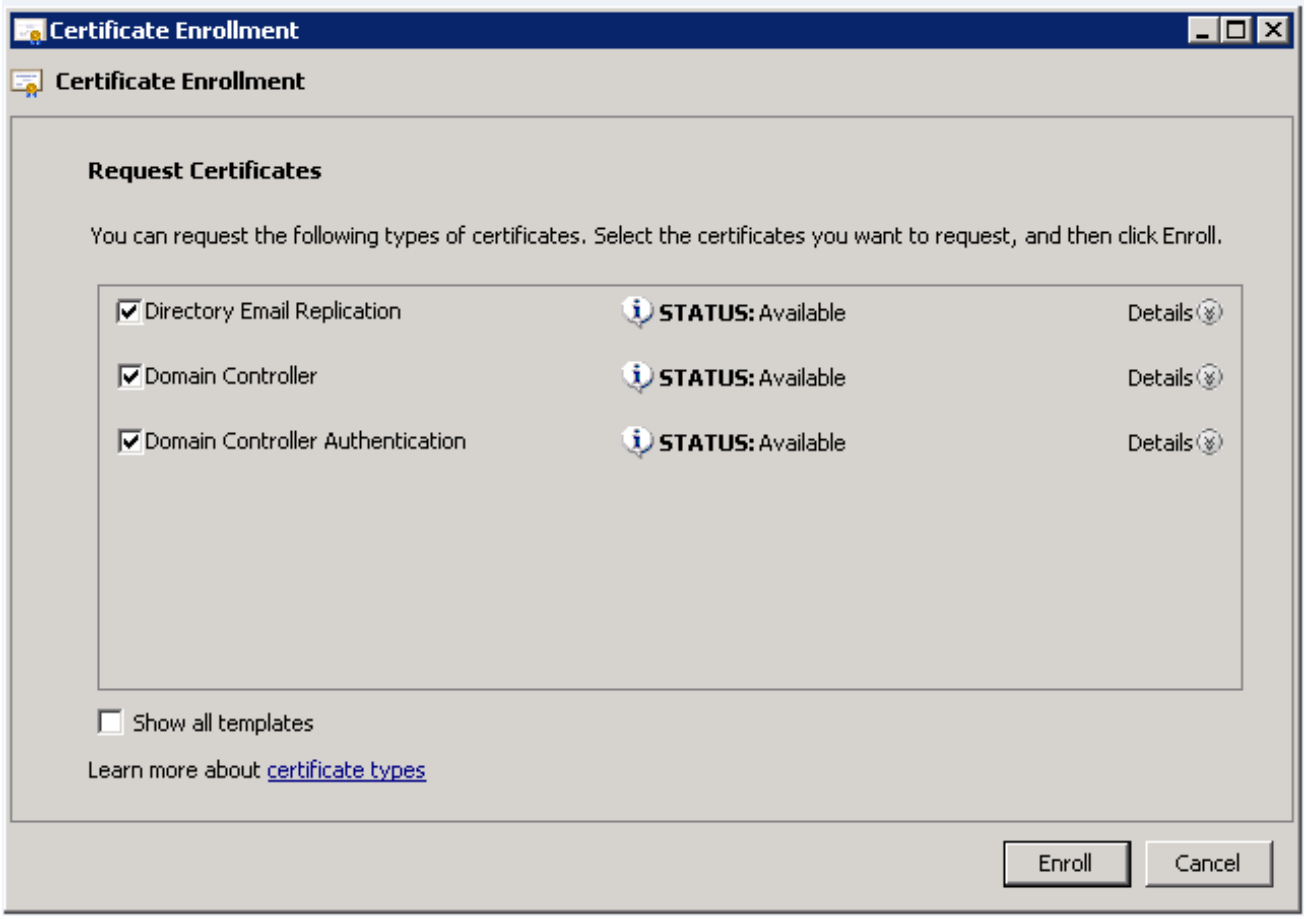


9. [next] をクリックします。

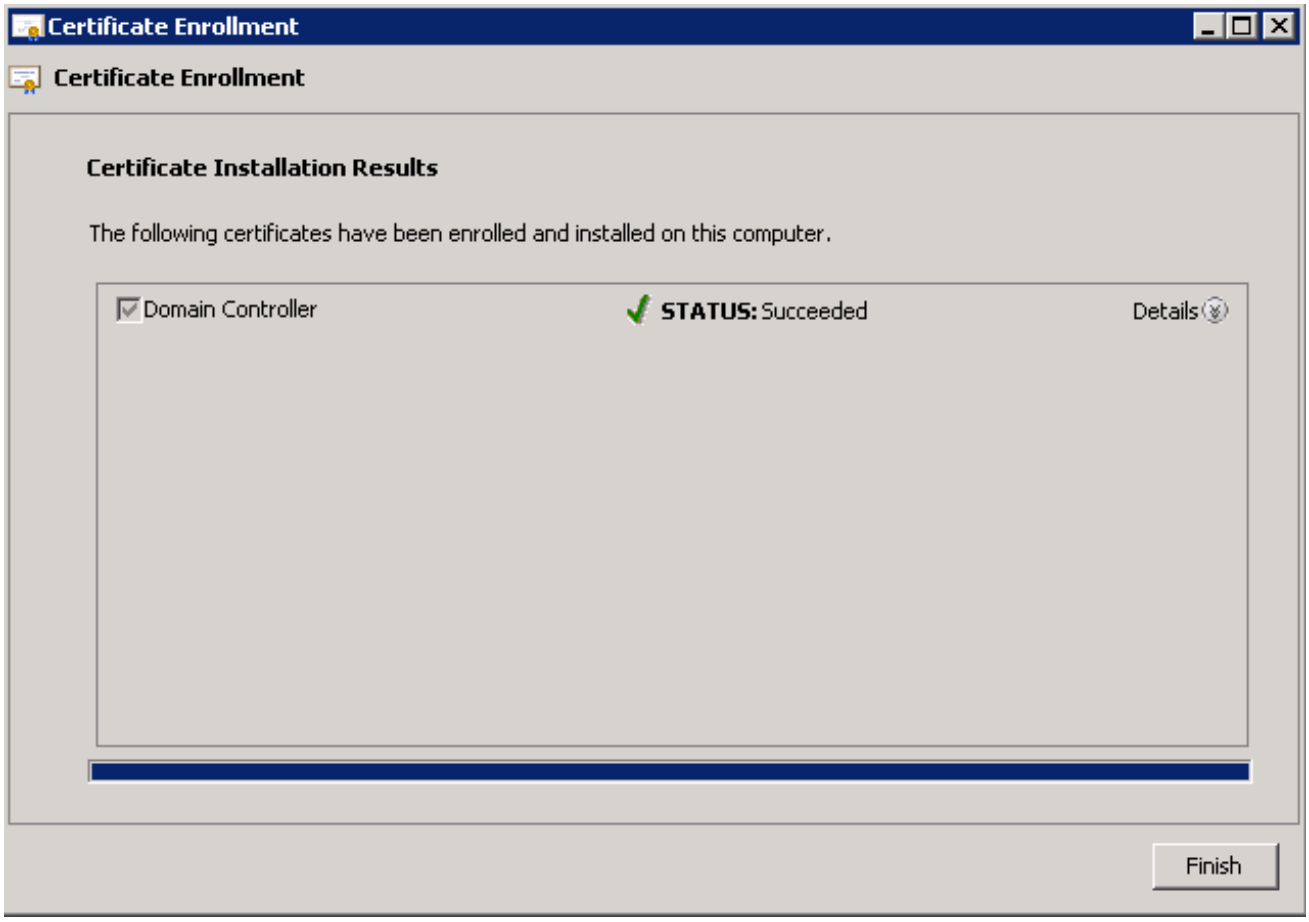


10. [Domain Controller] **チェックボックスをオンにし、[Enroll] をクリックします。**

    注：EAP 証明書のエラーが原因でクライアント認証に失敗したら、[Enroll] をクリックする前に、この [Certificate Enrollment] **ページで、チェックボックスがすべてオンになっていることを確認します。**証明書は通常、3 つ作成されます。

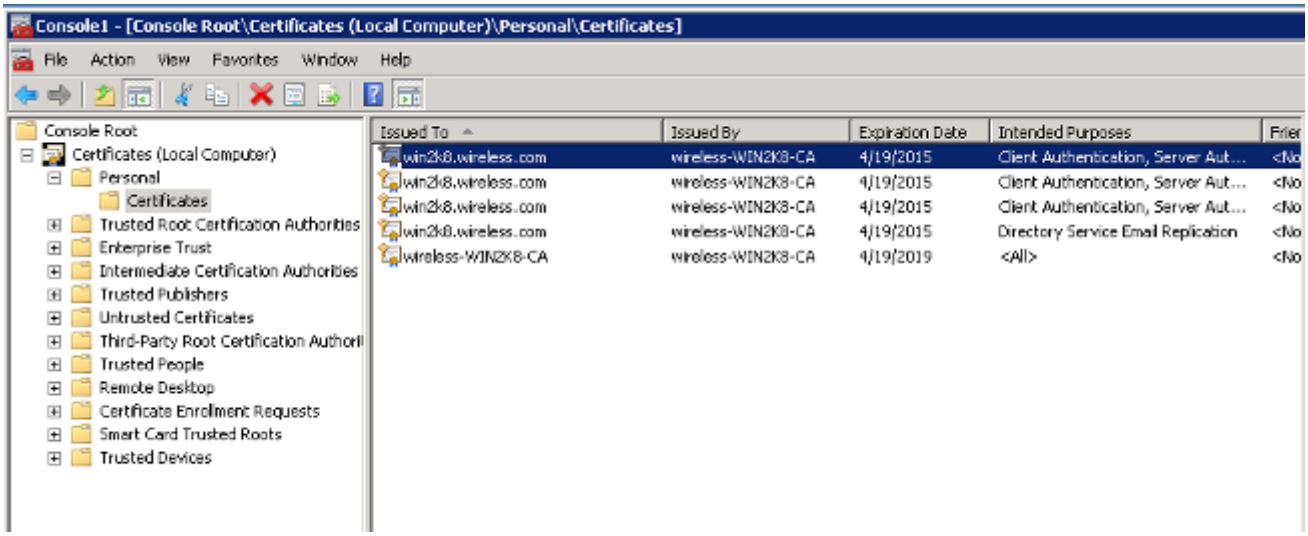


11. 証明書がインストールされたら、[Finish] をクリックします。



これで、NPS 証明書がインストールされました。

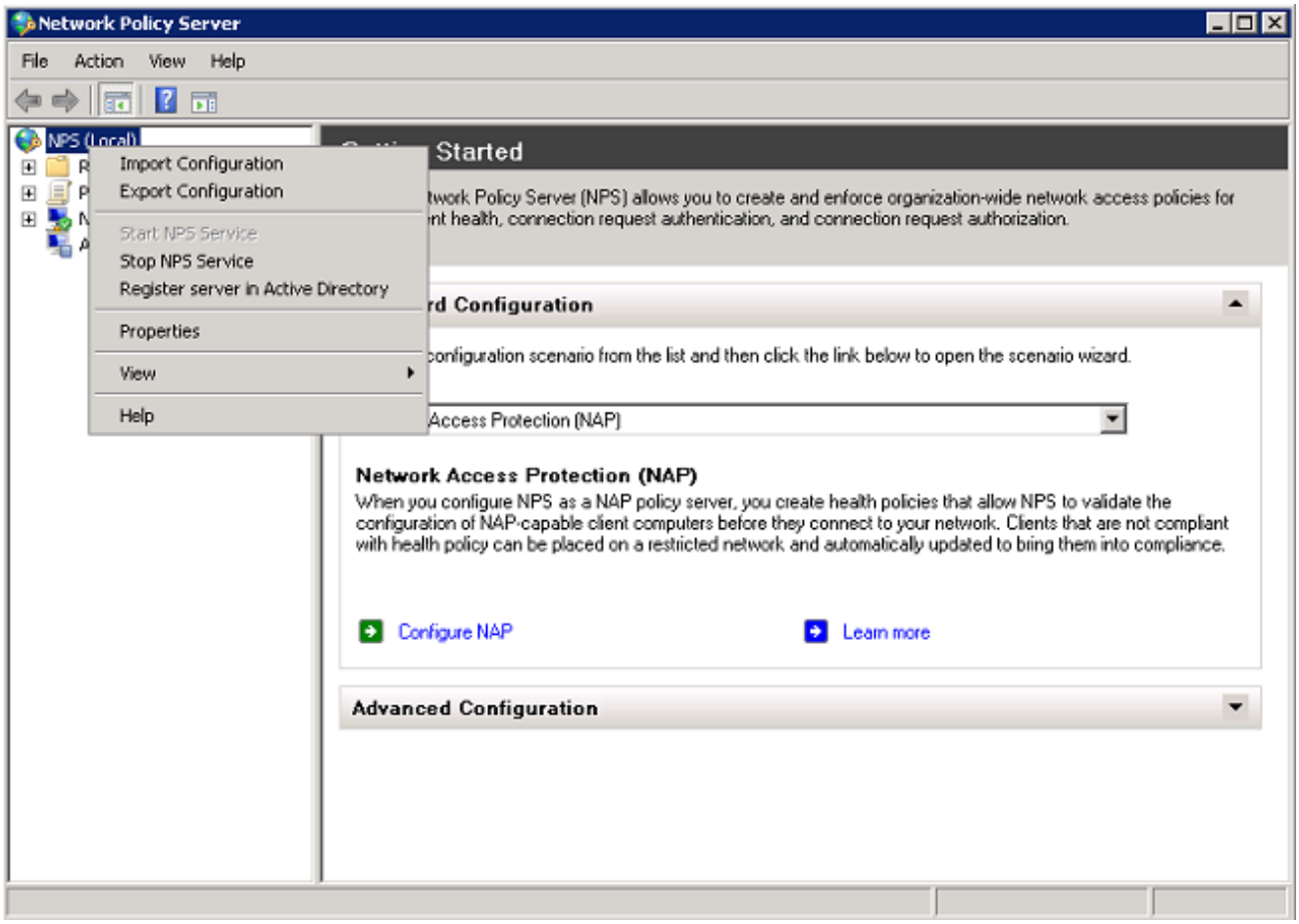
12. 証明書の [Intended Purposes] 列に [Client Authentication, Server Authentication] **が表示されていることを確認します。**



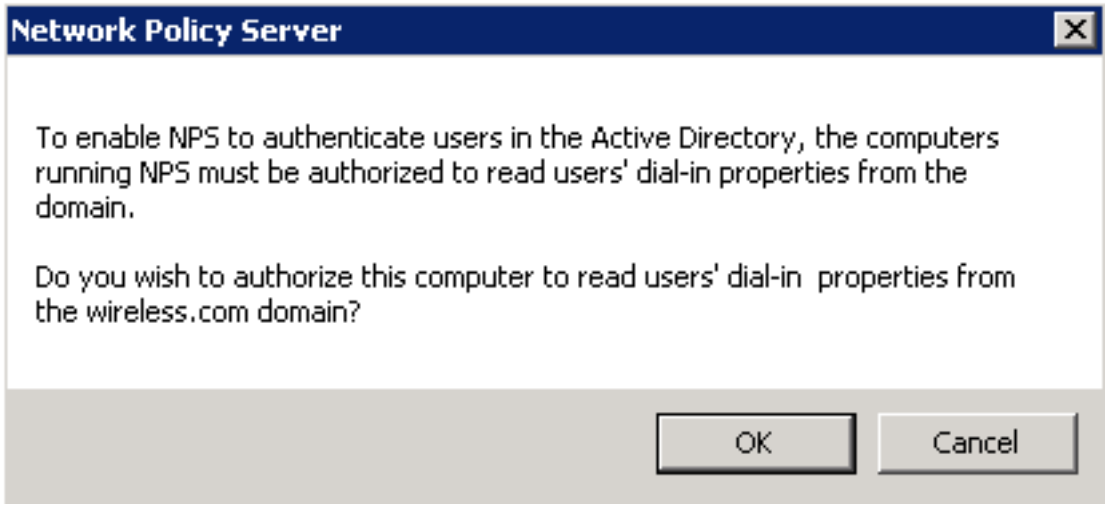
PEAP-MS-CHAP v2 認証のネットワーク ポリシー サーバ サービスの設定

認証用に NPS を設定するには、次の手順を実行します。

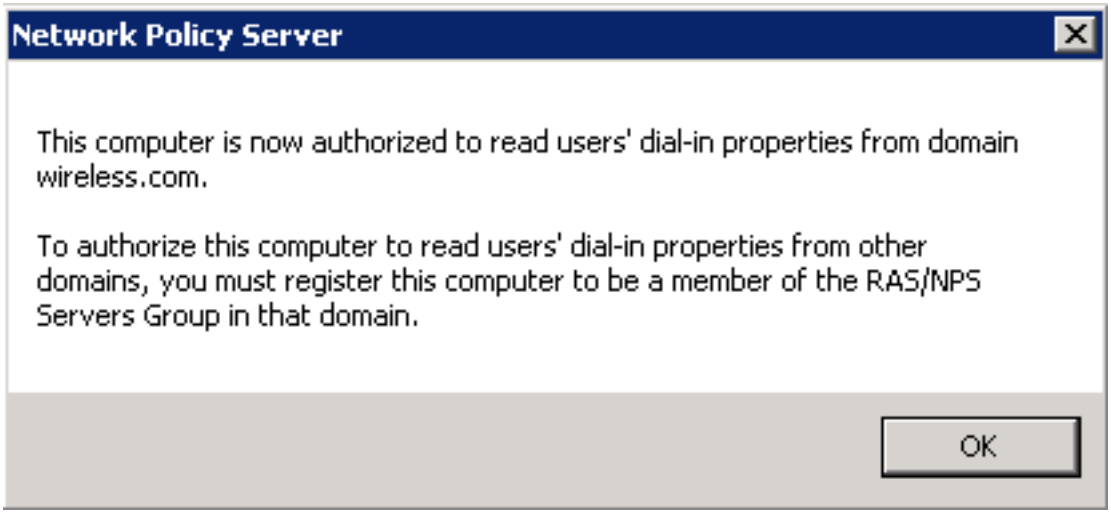
1. [Start] > [Administrative Tools] > **[Network Policy Server]** に移動します。
2. [NPS (Local)] **を右クリックし、[Register server in Active Directory] を選択します。**



3. [OK] をクリックします。

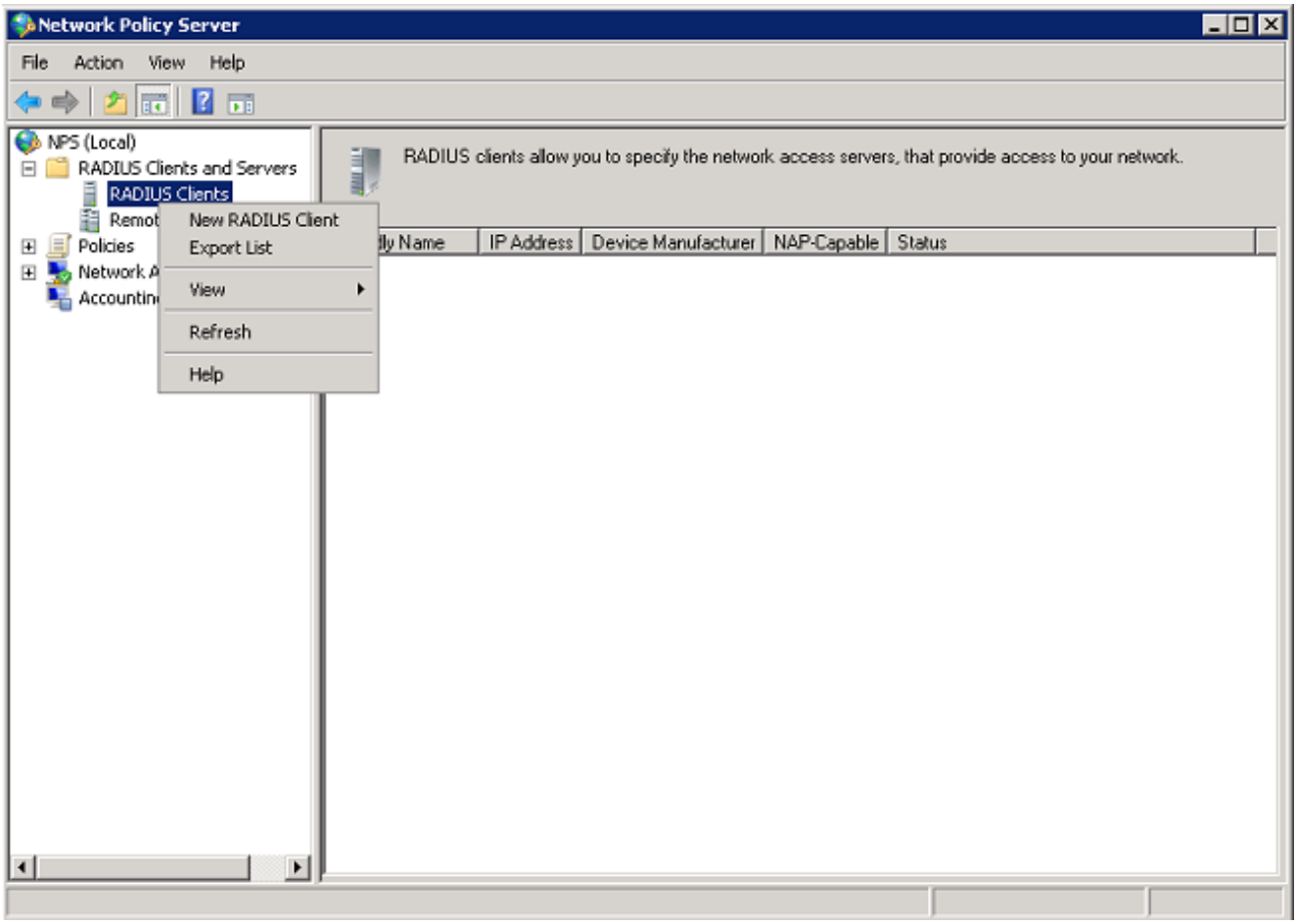


4. [OK] をクリックします。



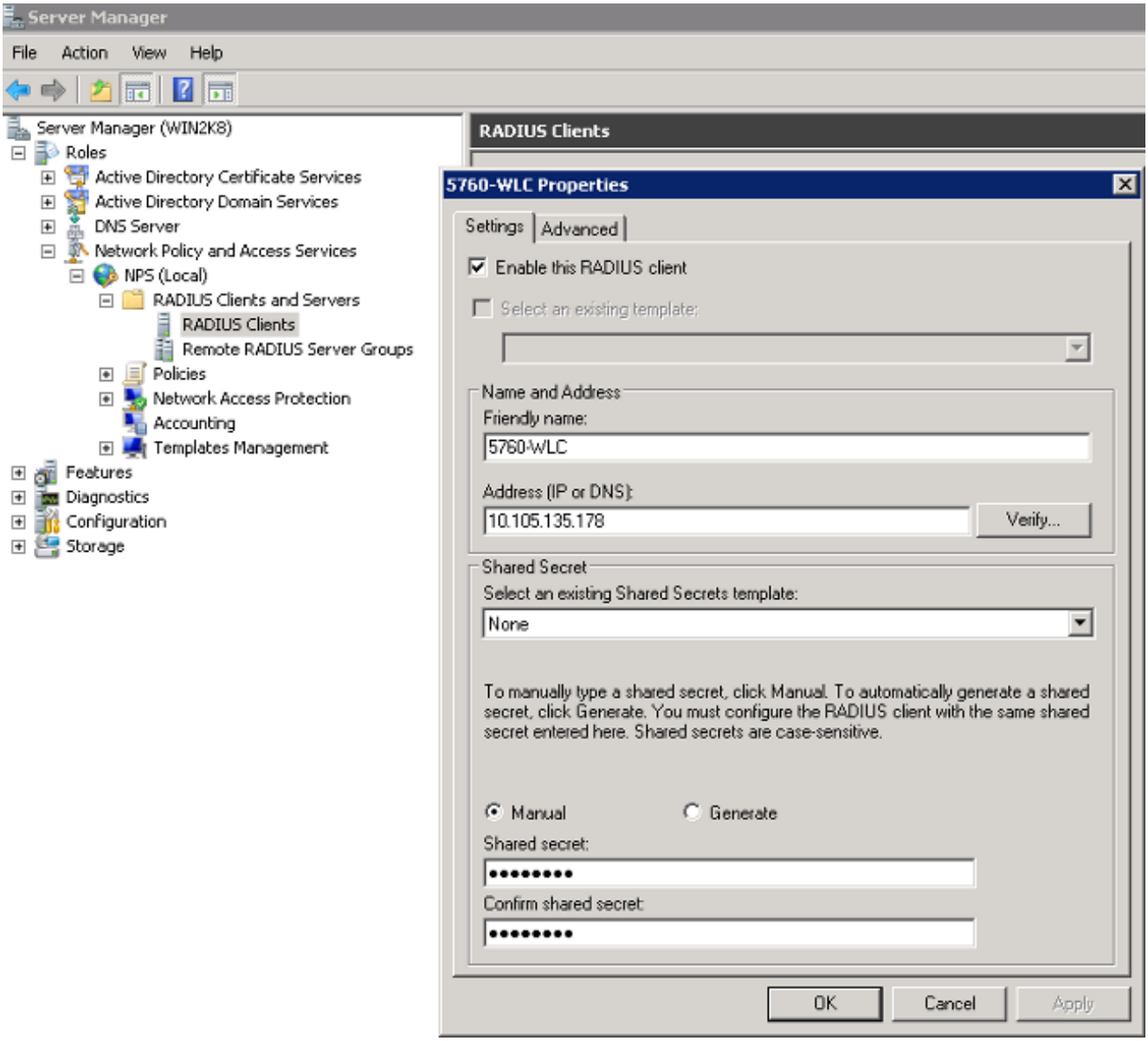
5. NPS の認証、許可、アカウンティング（AAA）クライアントとして WLC を追加します。

6. [RADIUS Clients and Servers] を展開します。[RADIUS Clients] **を右クリックし、[New RADIUS Client]** を選択します。

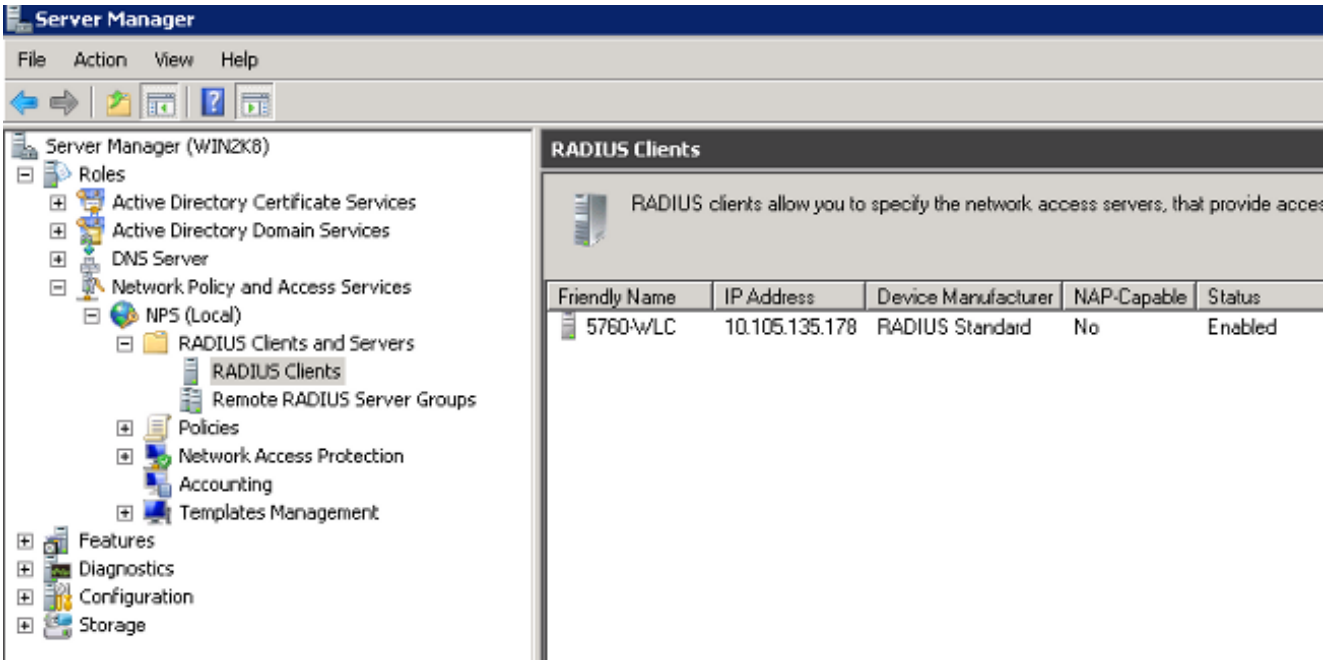


7. 名前（この例では WLC）、WLC の管理 IP アドレス（この例では 10.105.135.178）、共有秘密を入力します。

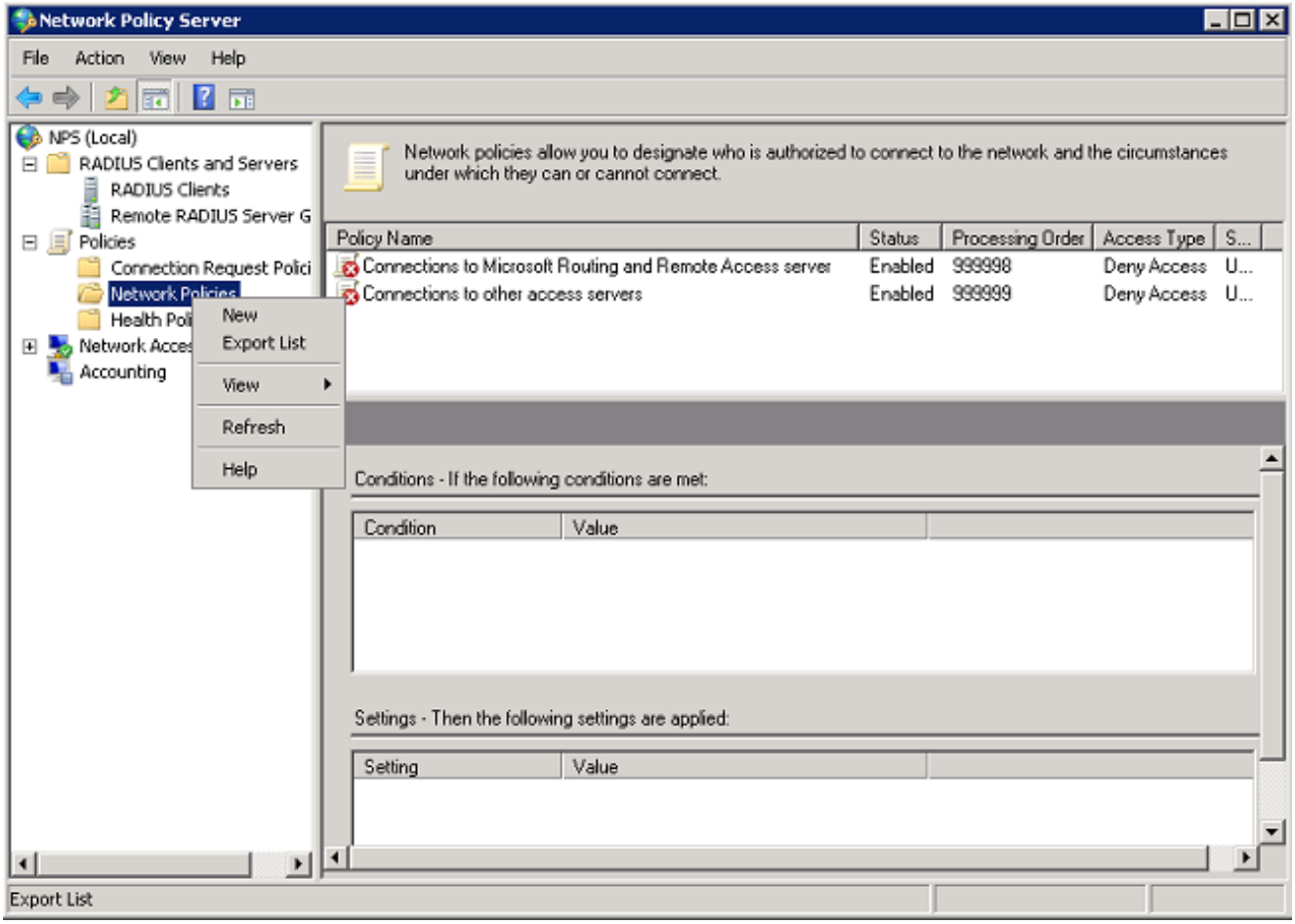
   注：WLC の設定には同じ共有秘密を使用します。



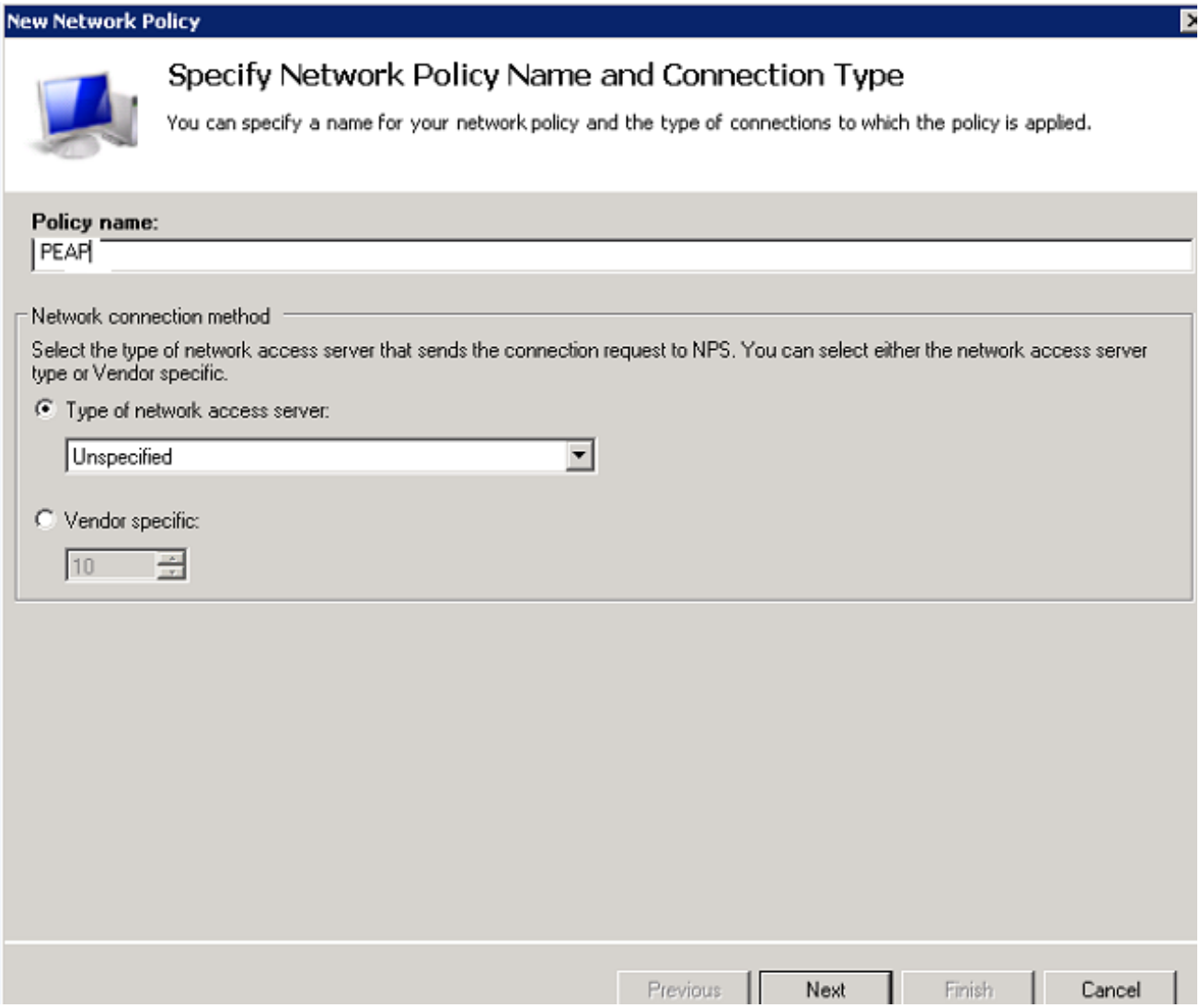
8. [OK] をクリックして前の画面に戻ります。



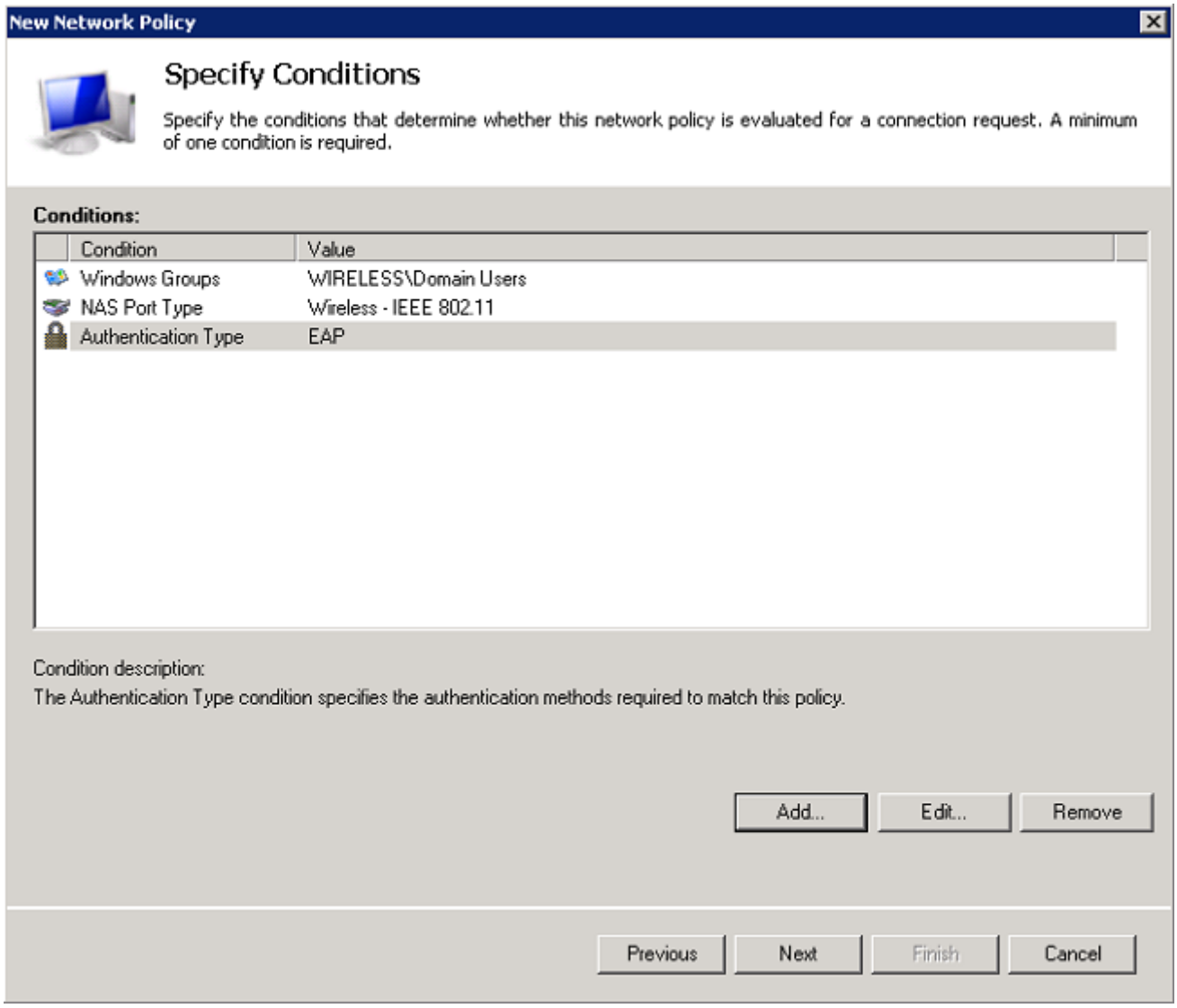
9. 新しいネットワーク ポリシーをワイヤレス ユーザ用に作成します。[Policies] を展開して [Network Policies] を右クリックし、[New] を選択します。



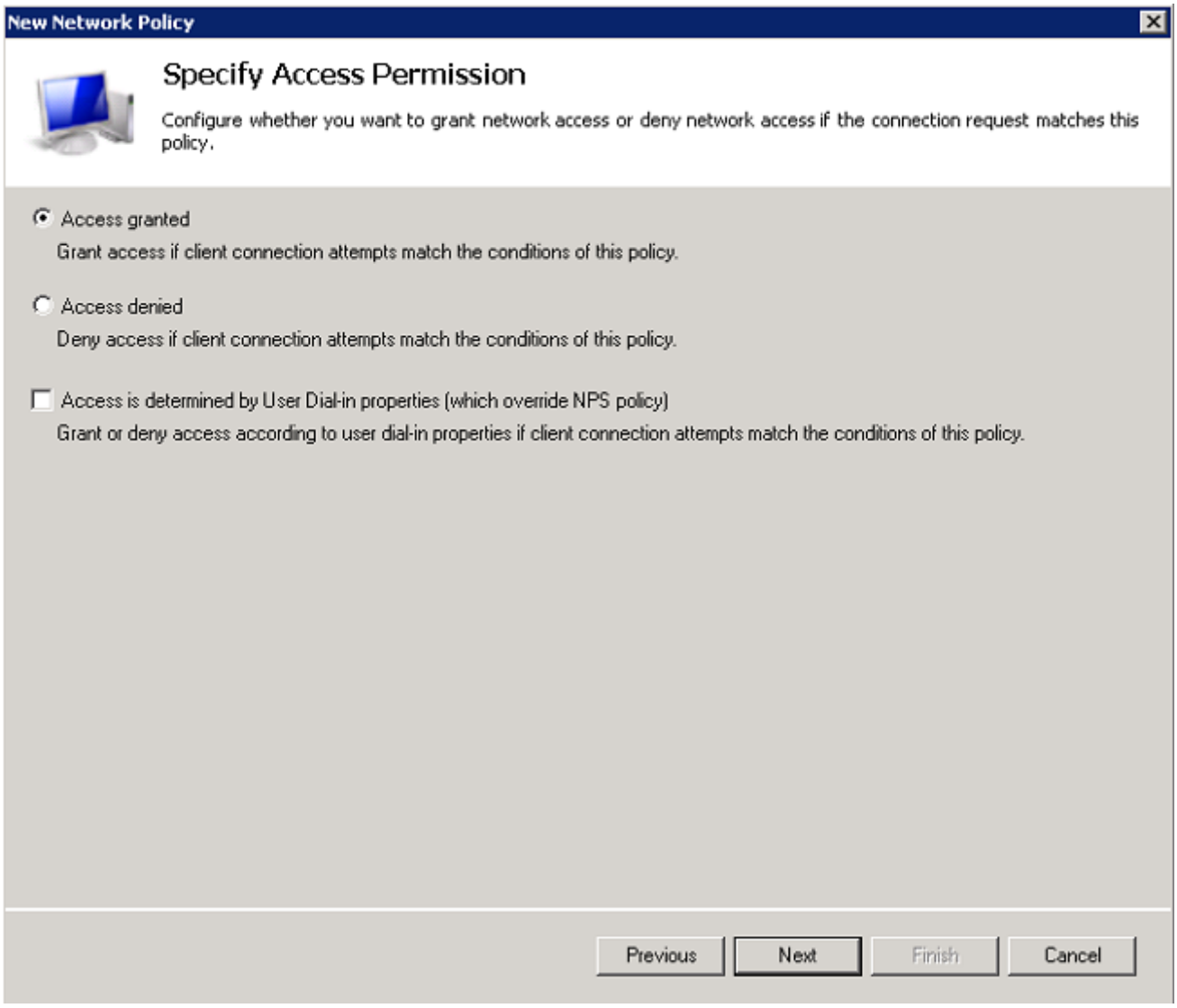
10. このルールのポリシー名（この例では **PEAP**）を入力し、**[Next] をクリックします。**



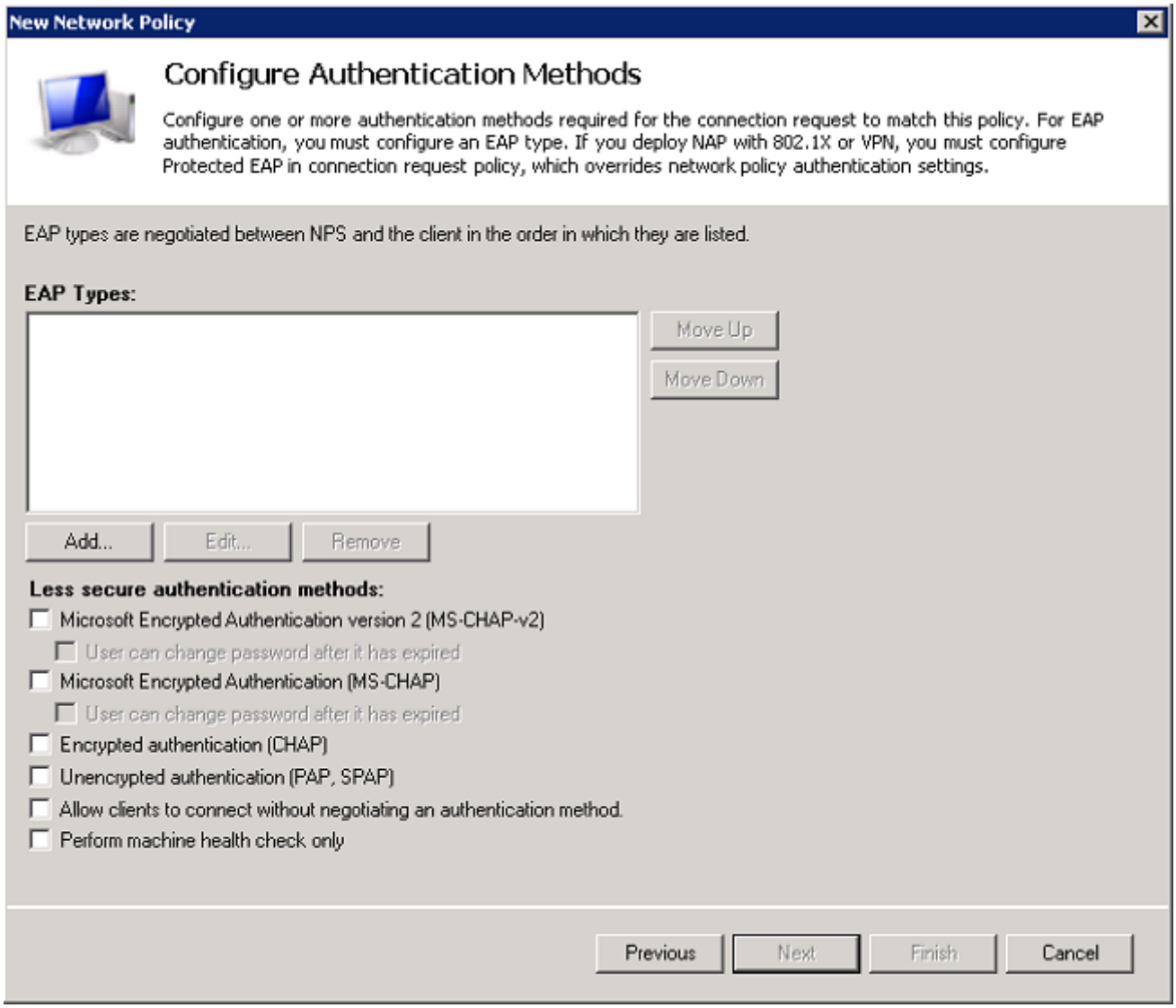
11. このポリシーをワイヤレス ドメイン ユーザのみに許可するように設定するには、次の 3 つの条件を追加し、[Next] をクリックします。



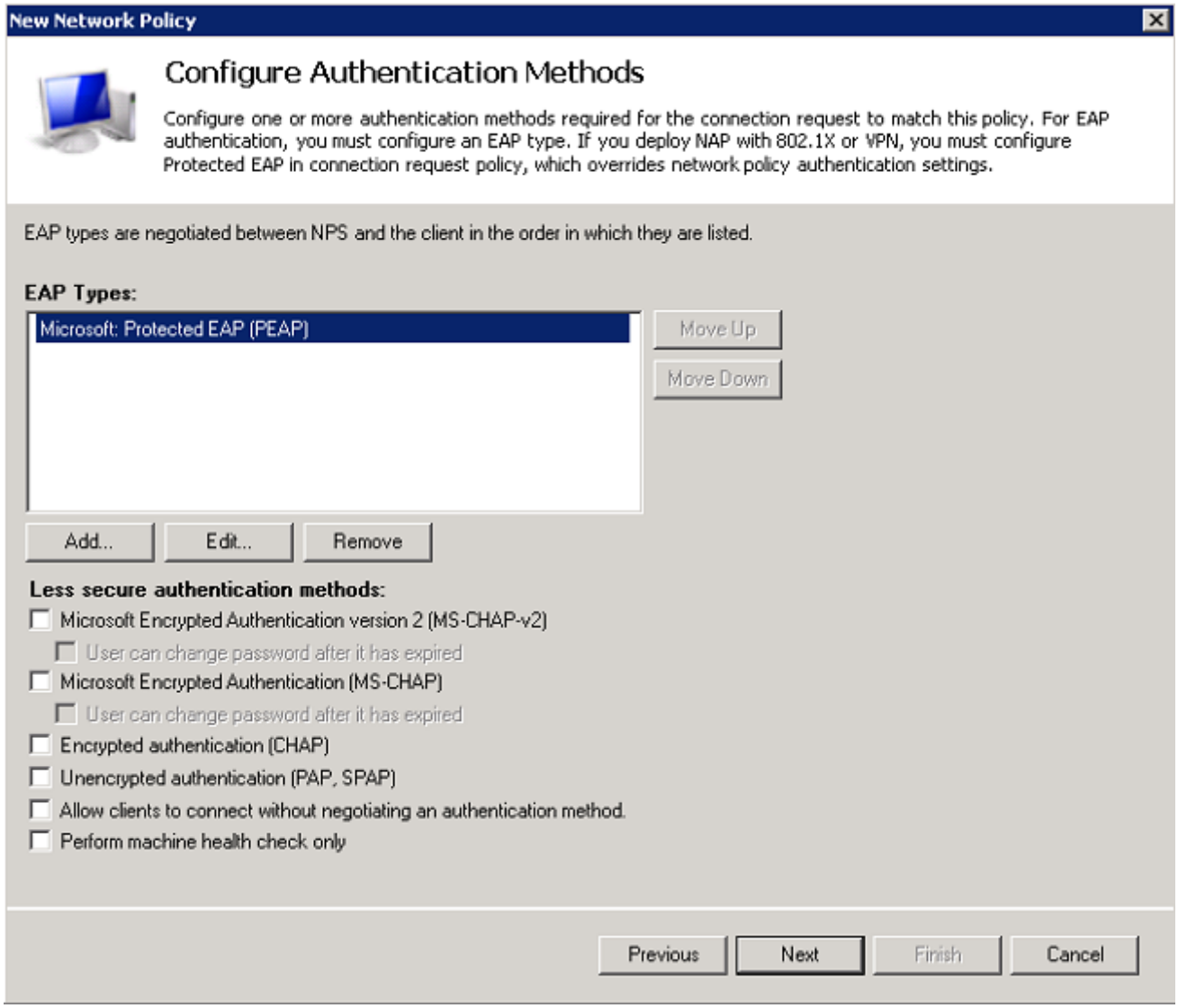
12. [Access granted] **オプション ボタンをクリックし、このポリシーに一致する接続試行を許可して、[Next] をクリックします。**



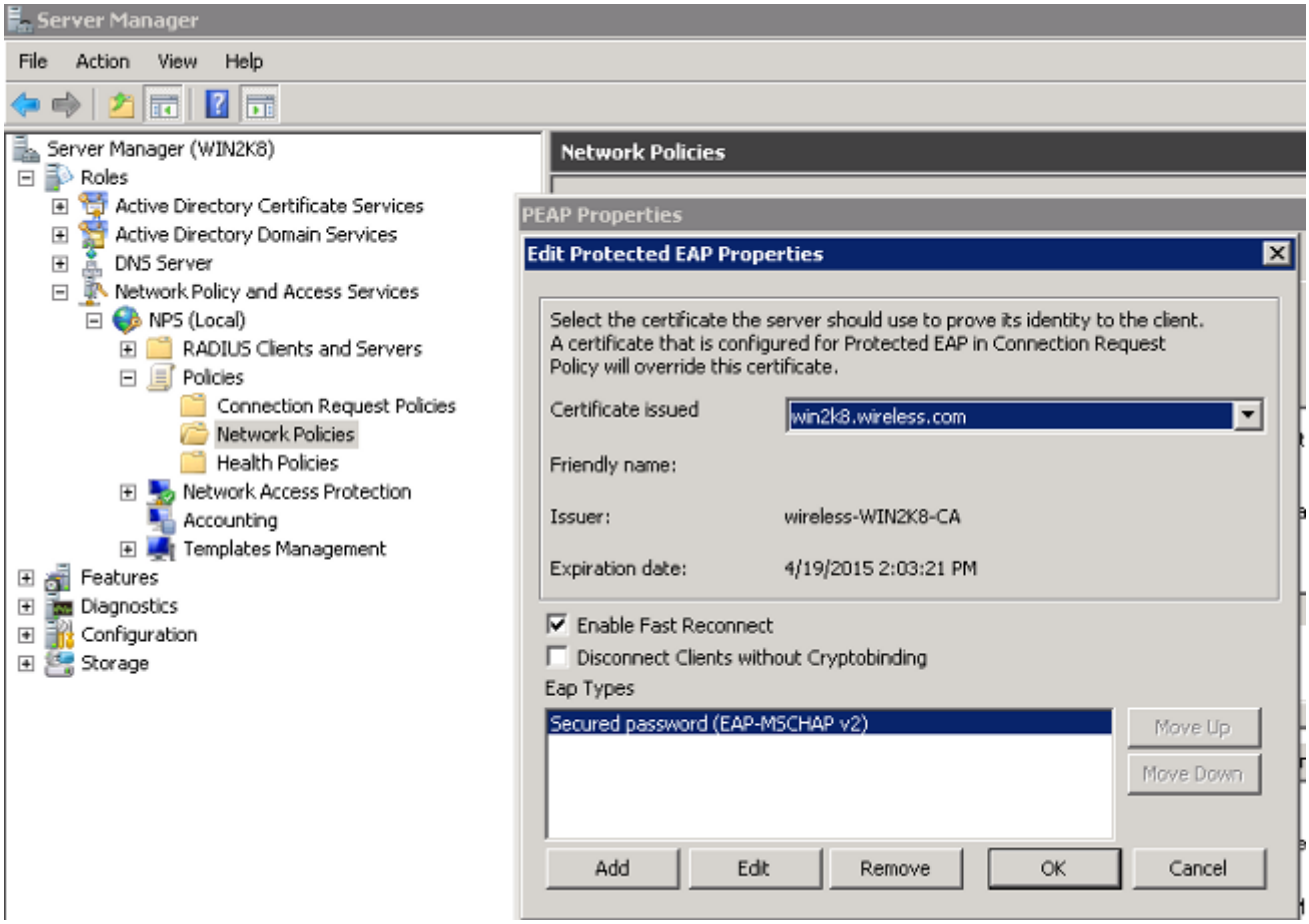
13. [Less secure authentication methods] はすべて無効にします。



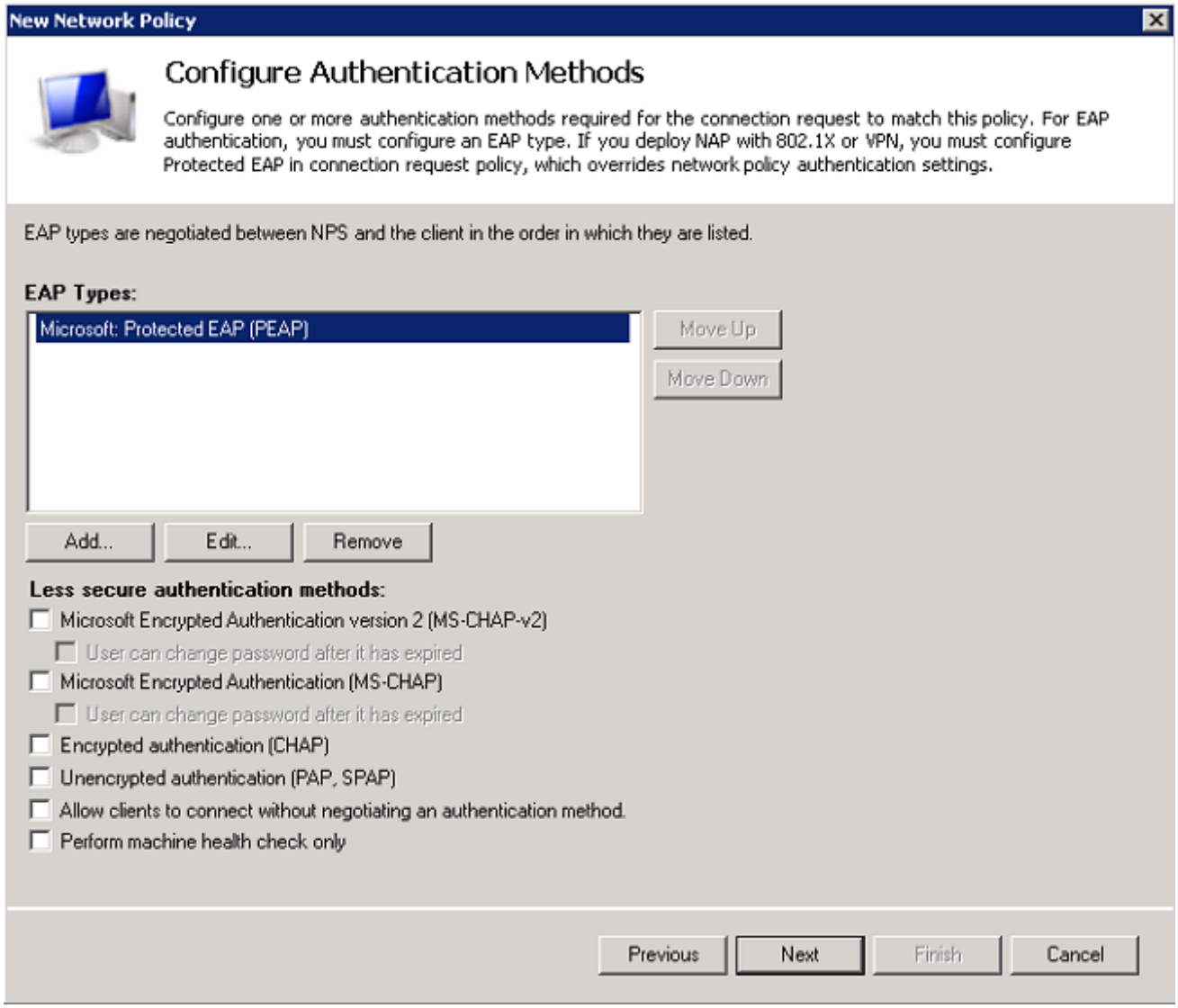
14. [Add] をクリックし、[EAP Type] に **[Microsoft:Protected EAP (PEAP)]** を選択したら、[OK] をクリックして PEAP を有効にします。



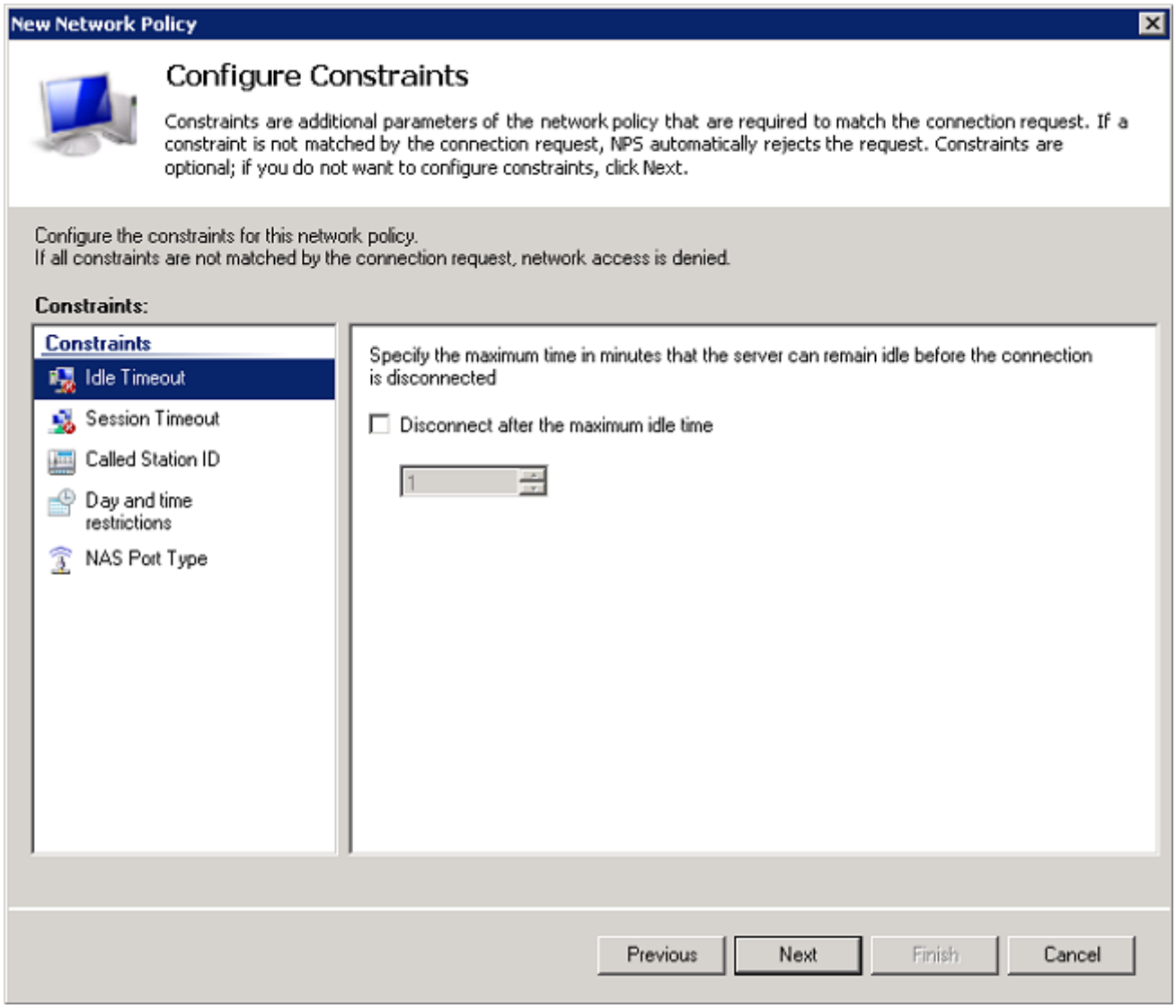
15. [Microsoft:**EAP (PEAP)] を選択し、[Edit] をクリックします。**以前作成したドメイン コントローラ証明書が [Certificate issued] ドロップダウン リストで選択されていることを確認し、[OK] をクリックします。



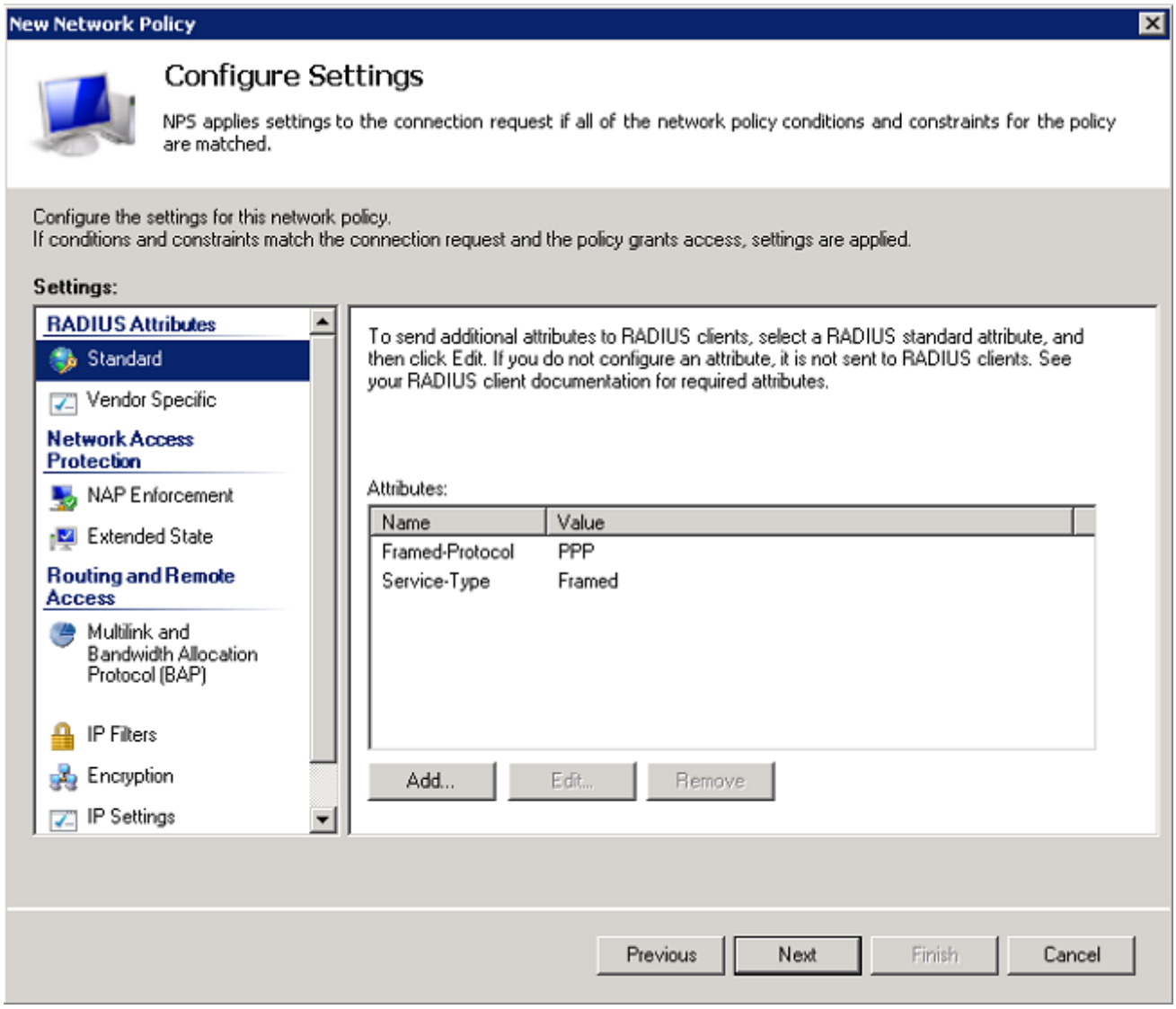
16. [next] をクリックします。



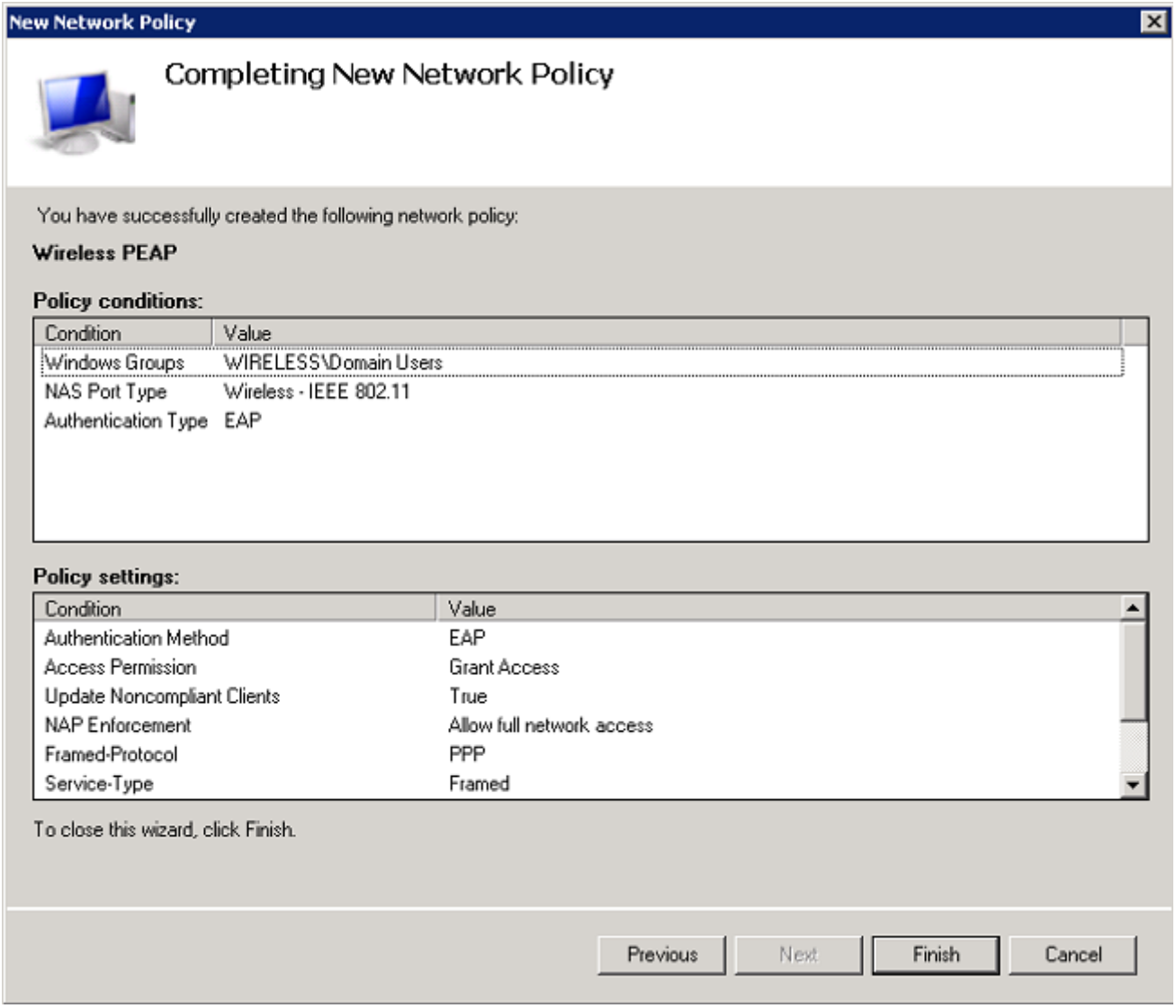
17. [next] をクリックします。



18. [next] をクリックします。



19. [Finish] をクリックします。



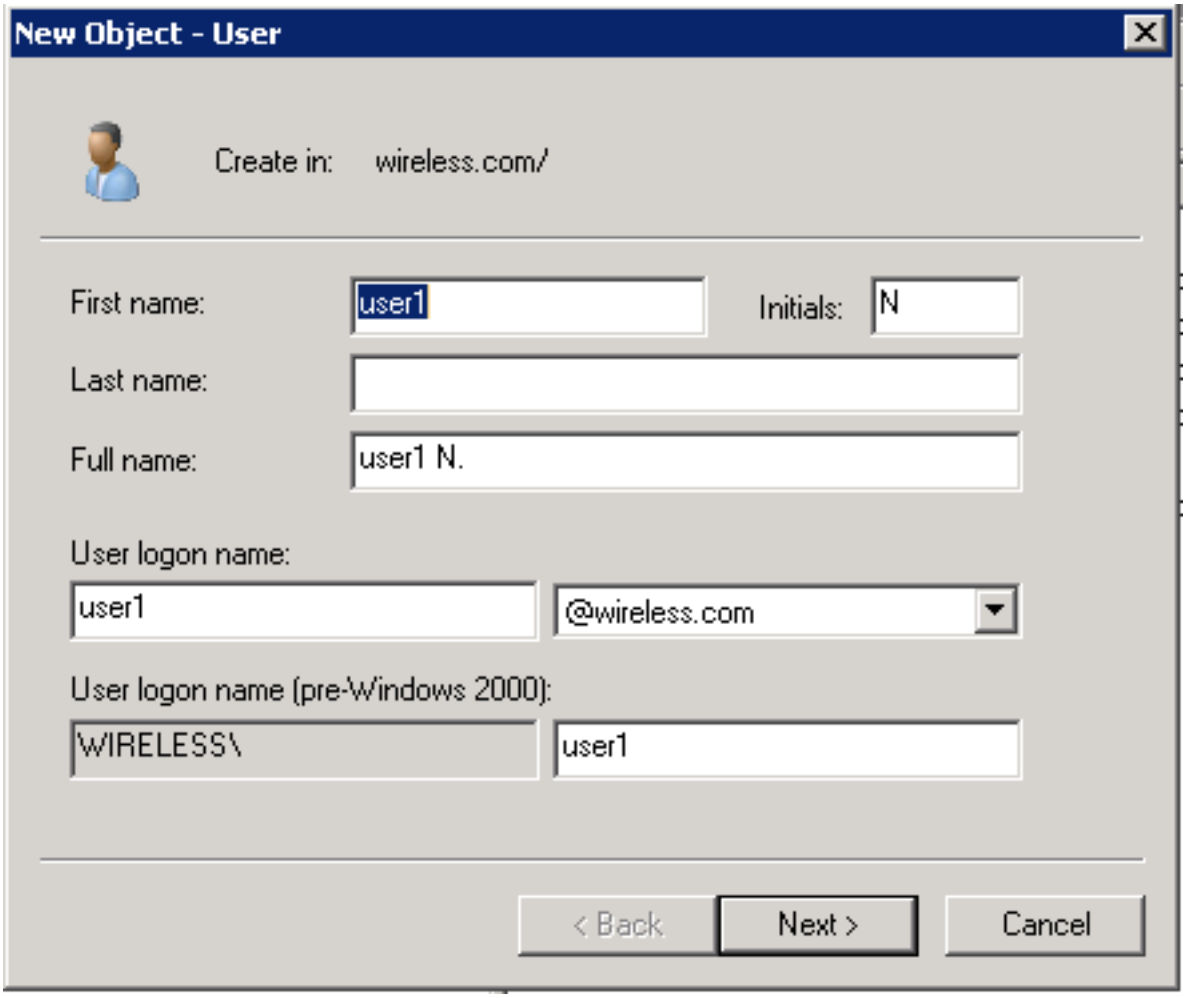
注：場合によっては、PEAP プロファイルまたはポリシーを許可するために、NPS で [Connection Request Policies] **を設定する必要があります。**

Active Directory へのユーザの追加

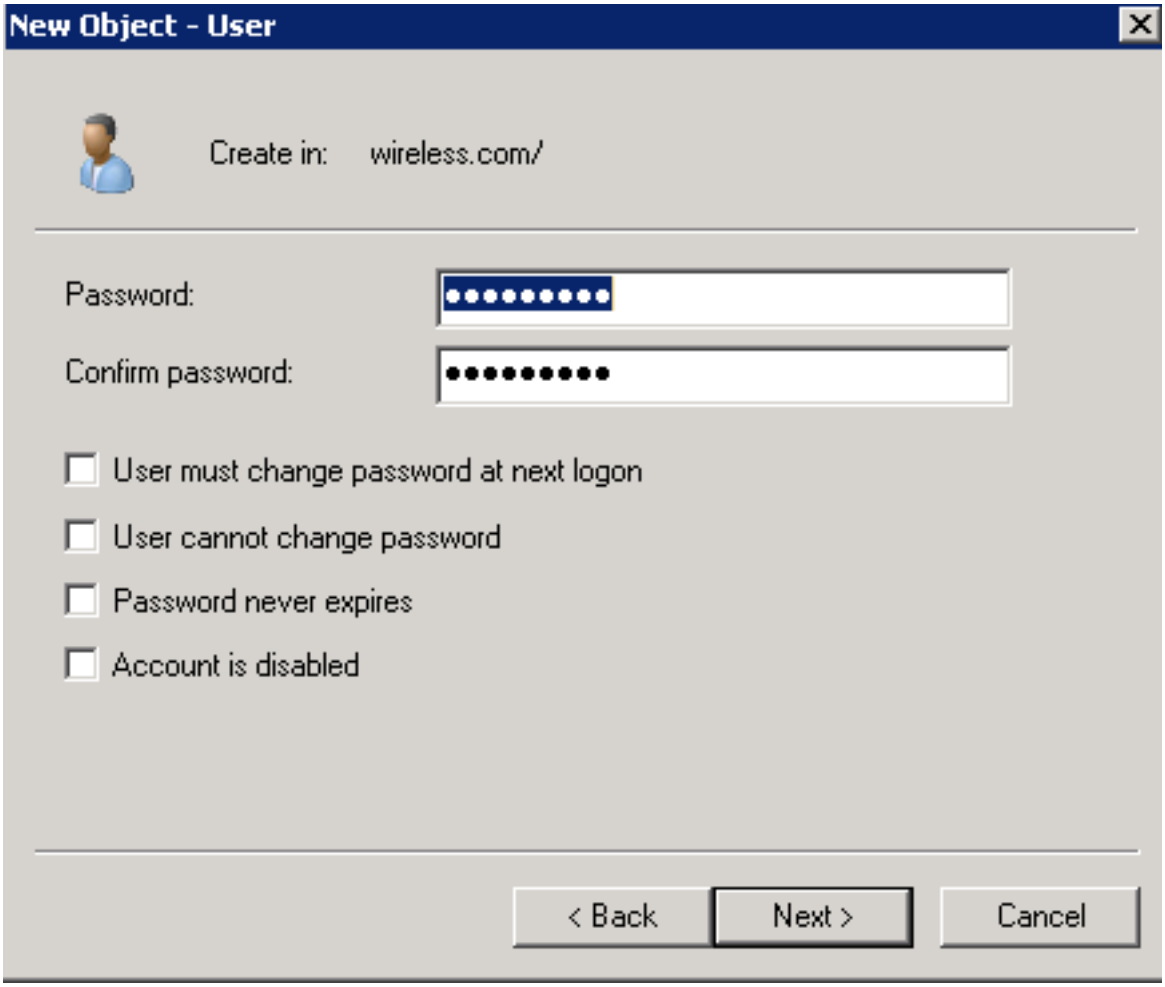
注：この例では、ユーザ データベースが AD で維持されています。

AD データベースにユーザを追加するには、次の手順を実行します。

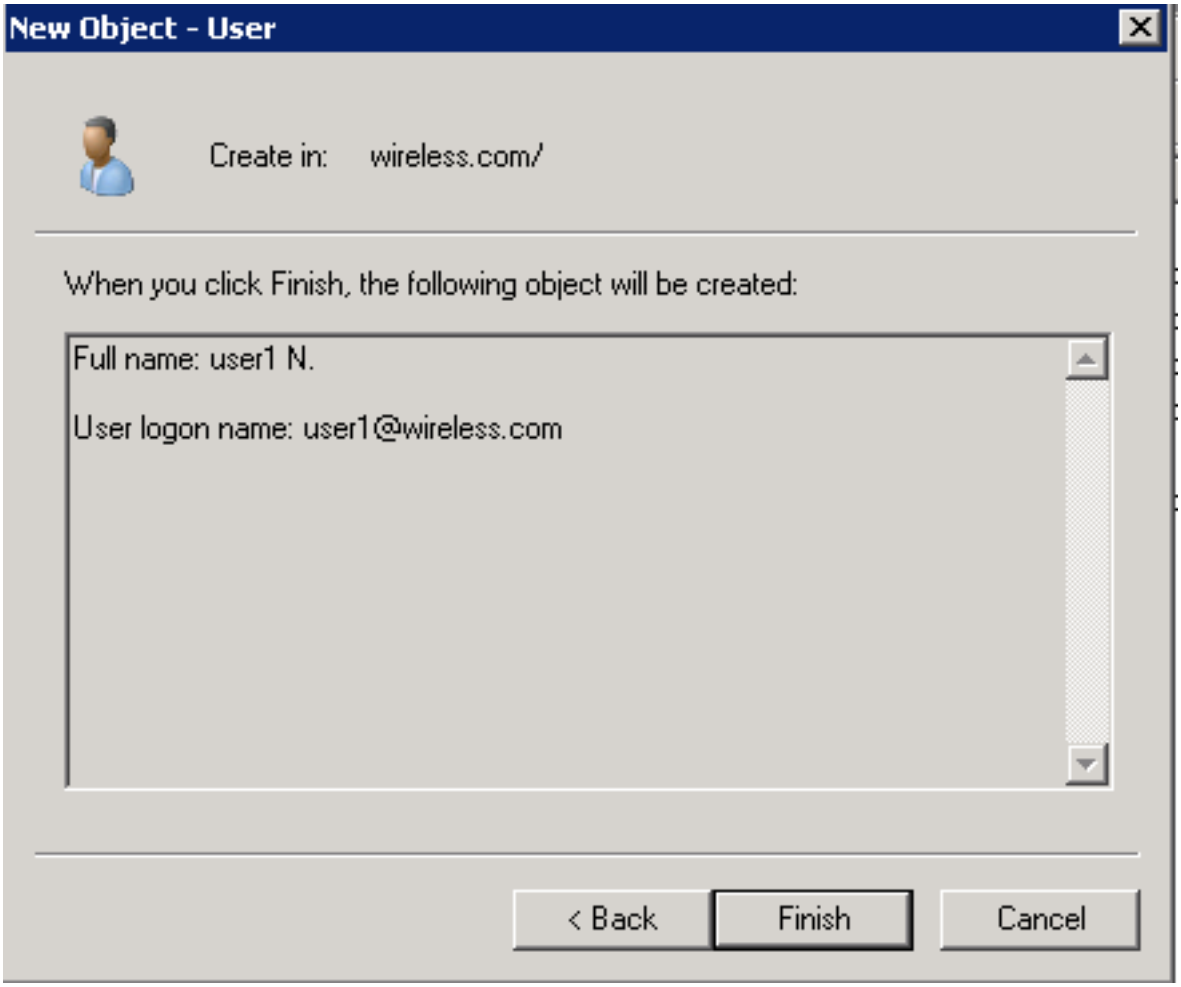
1. [Start] > [Administrative Tools] > [Active Directory Users and Computers] に移動します。
2. [Active Directory Users and Computers] のコンソール ツリーでドメインを展開し、[Users] > [New] の順に右クリックし、[User] を選択します。
3. [New Object - User] ダイアログボックスで、ワイヤレス ユーザの名前を入力します。この例では、[First Name] フィールドに **[Client1]、[User logon name] フィールドに [Client1] という名前を使用しています。**[next] をクリックします。



4. [New Object - User] ダイアログボックスで、[Password] フィールドと [Confirm password] フィールドに任意のパスワードを入力します。[User must change password at next logon] チェック ボックスをオフにして、[Next] をクリックします。



5. [New Object - User] ダイアログボックスで [Finish] をクリックします。

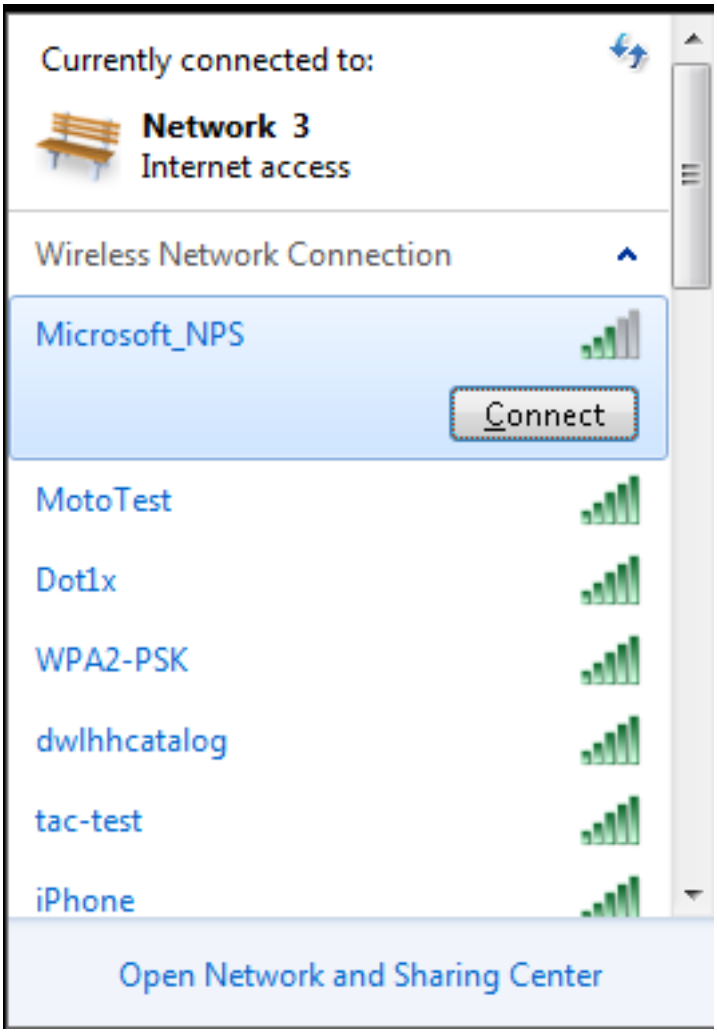


6. 追加のユーザ アカウントを作成するには、手順 2 ~ 4 を繰り返します。

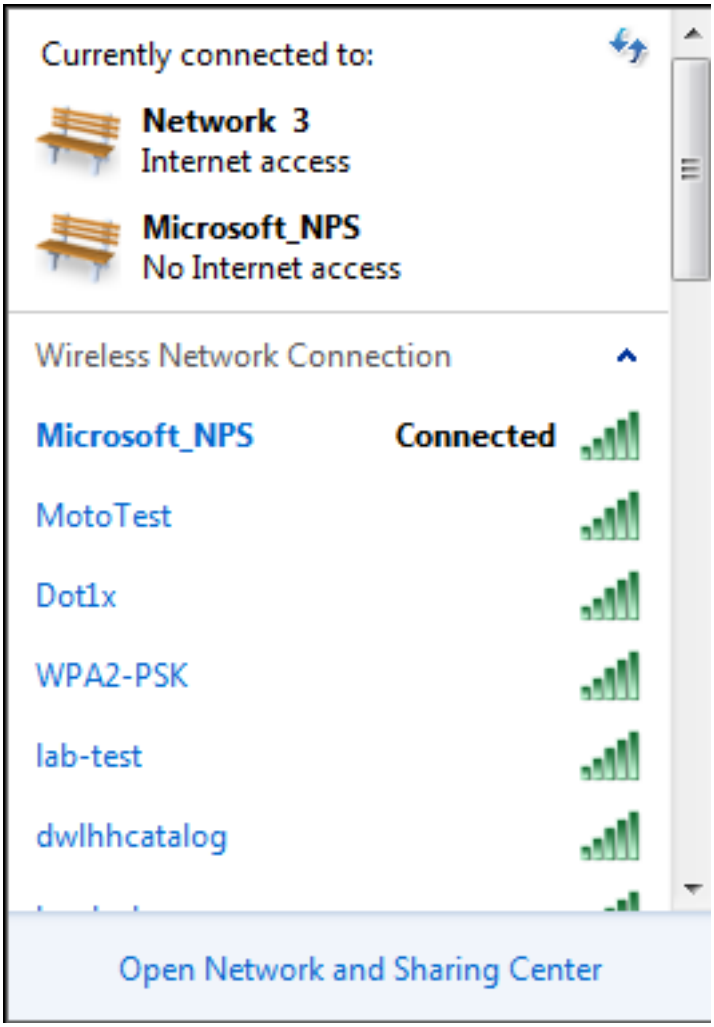
確認

設定を確認するには、次の手順を実行します。

1. クライアント マシンのサービス セット ID (SSID) を検索します。



2. クライアントが正常に接続されていることを確認します。



トラブルシュート

> **注**：無線の問題のトラブルシューティングを行う際はトレースを使用することを推奨します。トレースは循環バッファに保存されているため、プロセッサに負荷はかかりません。

L2 auth logs を取得するには、次のトレースを有効にします。

- set trace group-wireless-secure level debug
- set trace group-wireless-secure filter mac 0017.7C2F.B69A

dot1X AAA events を取得するには、次のトレースを有効にします。

- set trace wcm-dot1x aaa level debug
- set trace wcm-dot1x aaa filter mac 0017.7C2F.B69A

DHCP events を受信するには、次のトレースを有効にします。

- set trace dhcp events level debug
- set trace dhcp events filter mac 0017.7C2F.B69A

トレースを無効にして、バッファをクリアするには、次のトレースを有効にします。

- set trace control sys-filtered-traces clear
- set trace wcm-dot1x aaa level default
- set trace wcm-dot1x aaa filter none

- set trace group-wireless-secure level default
- set trace group-wireless-secure filter none

トレースを表示するには、show trace sys-filtered-traces コマンドを入力します。

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
 1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy:  Created MSCB
 Just AccessVLAN = 0 and SessionTimeout  is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN  name VLAN0020 and VLAN ID  20

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
 to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
 Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
 override for station  0017.7c2f.b69a  - vapId 8, site 'test',
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
 Interface Policy for station  0017.7c2f.b69a  - vlan 20,
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a     Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,
 applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a          ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):
 130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
 length 20 for mobile  0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
 PMKIDsfrom mobile  0017.7c2f.b69a


[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a Change state to AUTHCHECK
 (2) last state START (0)

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD
 (3) last state AUTHCHECK (2)


[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq
 (apf_80211.c:6272) Changing state for mobile  0017.7c2f.b69a  on AP
 1caa.076f.9e10  from Associated to Associated

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating
 authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth
 timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
 to authenticate client 4975000000003e uid 40
```

```
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: Session Start from
 wireless client

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client
 4975000000003e, uid 40, capwap id 7ae8c000000013,Flag 0, Audit-Session ID
 0a6987b25357e2ff00000028, method list Microsoft_NPS, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a
 (method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028),  policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3]  - client iif_id: 4975000000003E, session ID:
 0a6987b25357e2ff00000028 for 0017.7c2f.b69a


[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting RX_REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting AUTH_START for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending EAPOL packet
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Platform changed src mac  of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending out EAPOL packet
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] EAPOL packet sent to client 0x22000025


[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): Authen method=SERVER_GROUP
 Microsoft_NPS
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Queuing an EAPOL pkt on Authenticator Q
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting EAPOL_EAP for 0x22000025
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply
 GET_CHALLENGE_RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication
 status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3]
 Posting EAP_REQ for 0x22000025
```

次に、EAP 出力の残りの部分を示します。

```
[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen
 method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
```

DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): **protocol reply PASS for Authentication**
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): **Return Authentication status=PASS**
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO: [0017.7c2f.b69a, Ca3] **Received an EAP Succe**ss

[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a **Starting key exchange with mobile - data forwarding is disable**d
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: **Sending EAPOL message to mobile, WLAN=8 AP WLAN=8**
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL message (len 121) from mobile
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: **Received EAPOL-Key from mobile**
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: **Received EAPOL-key in PTK_START state (msg 2)** from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: **Sending EAPOL message to mobile, WLAN=8 AP WLAN=8**
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL message (len 99) from mobile
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: **Received EAPOL-Key from mobile**
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: **Received EAPOL-key in PTKINITNEGOTIATING state (msg 4) from mobile**
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete - updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMs1xStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a **Change state to L2AUTHCOMPLETE (**4) last state 8021X_REQD (3)

[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPOFFER notify setup address **20.20.20.5 mask 255.255.255.0**

[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a **Change state to RUN (20) last state DHCP_REQD (7)**