ASSIGNING CERTIFICATES TO DOMAIN MEMBERS VIA AUTOENROLLMENT IN A WINDOWS SERVER 2003 ACTIVE DIRECTORY DOMAIN

One of the advantages joining your machines to an Active Directory domain with an enterprise CA is that you can deploy machine certificates automatically using a process known as *autoenrollment*. The autoenrollment feature allows you to configure domain or OU based Group Policy to automatically install both a machine certificate and the CA certificate into each domain member machine's certificate store. This greatly reduces the amount of administrative overhead required to deploy certificates to your VPN clients.

There are three basic procedures involved in assigning certificates via autoenrollment:

- **Configure Group Policy to assign machine certificates**
  Group Policy is the heart of certificate of autoenrollment. Configure domain group policy to automatically issue domain member servers and workstations certificates via autoenrollment.

- **Force Group Policy update on certificate recipients**
  Group Policy refreshes every 90 minutes for domain workstations and member servers. Domain group policy refresh is forced every 16 hours for all machines in the domain. You can apply autoenrollment settings immediately using the **gpupdate** utility.

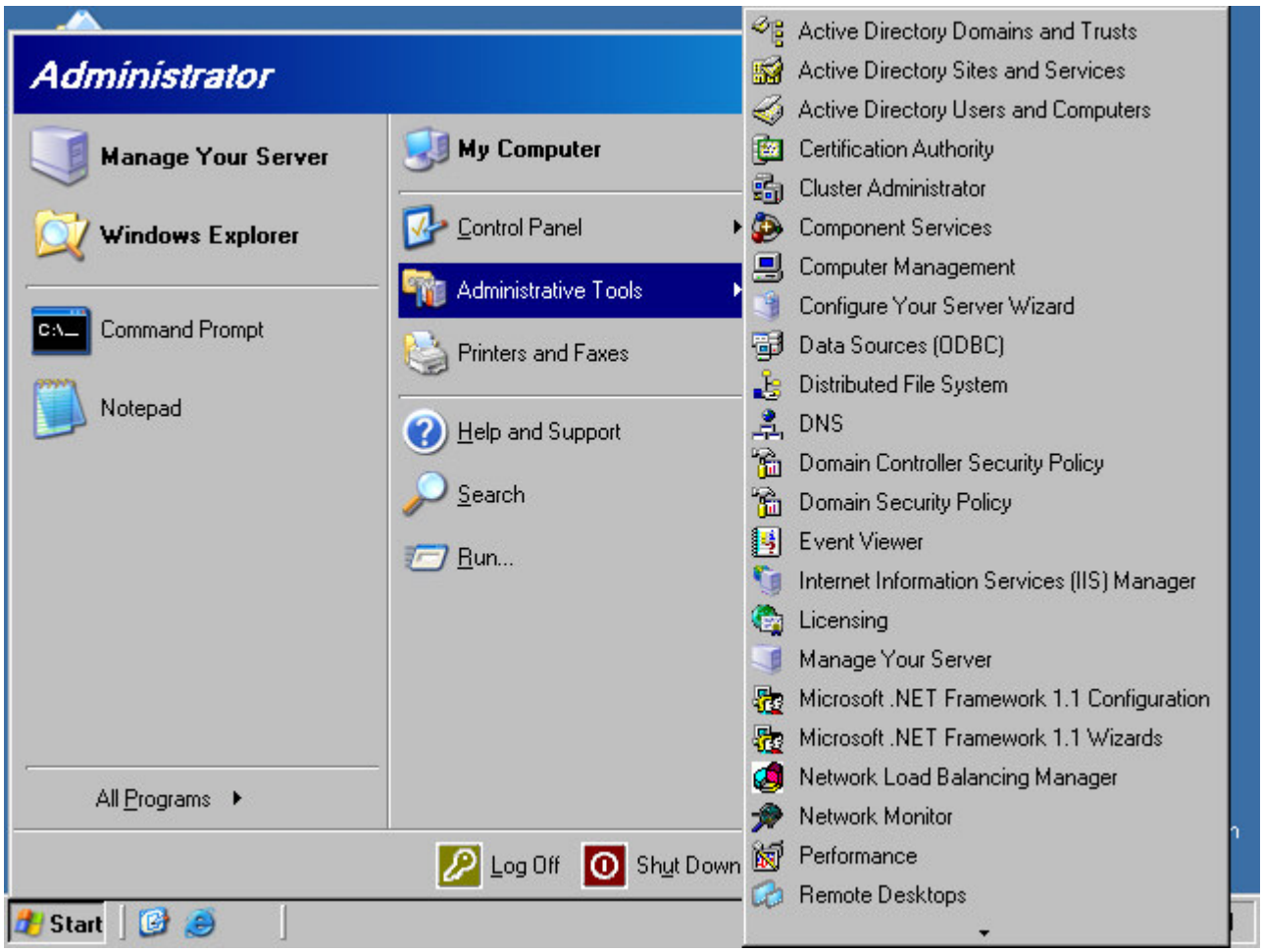
- **Automate User Certificate assignment using autoenrollment**
  If you wish to use certificate-based EAP-TLS authentication with either L2TP/IPSec or PPTP VPN connection, you can automate the issuance of User Certificates to all domain members or you can limit the scope of the certificate assignment by creating a user certificate autoenrollment policy.

Configuring Group Policy to Assign Machine Certificates

Both VPN clients and VPN servers can be issued certificates via autoenrollment. Perform the following steps to issue all domain members a machine certificate:

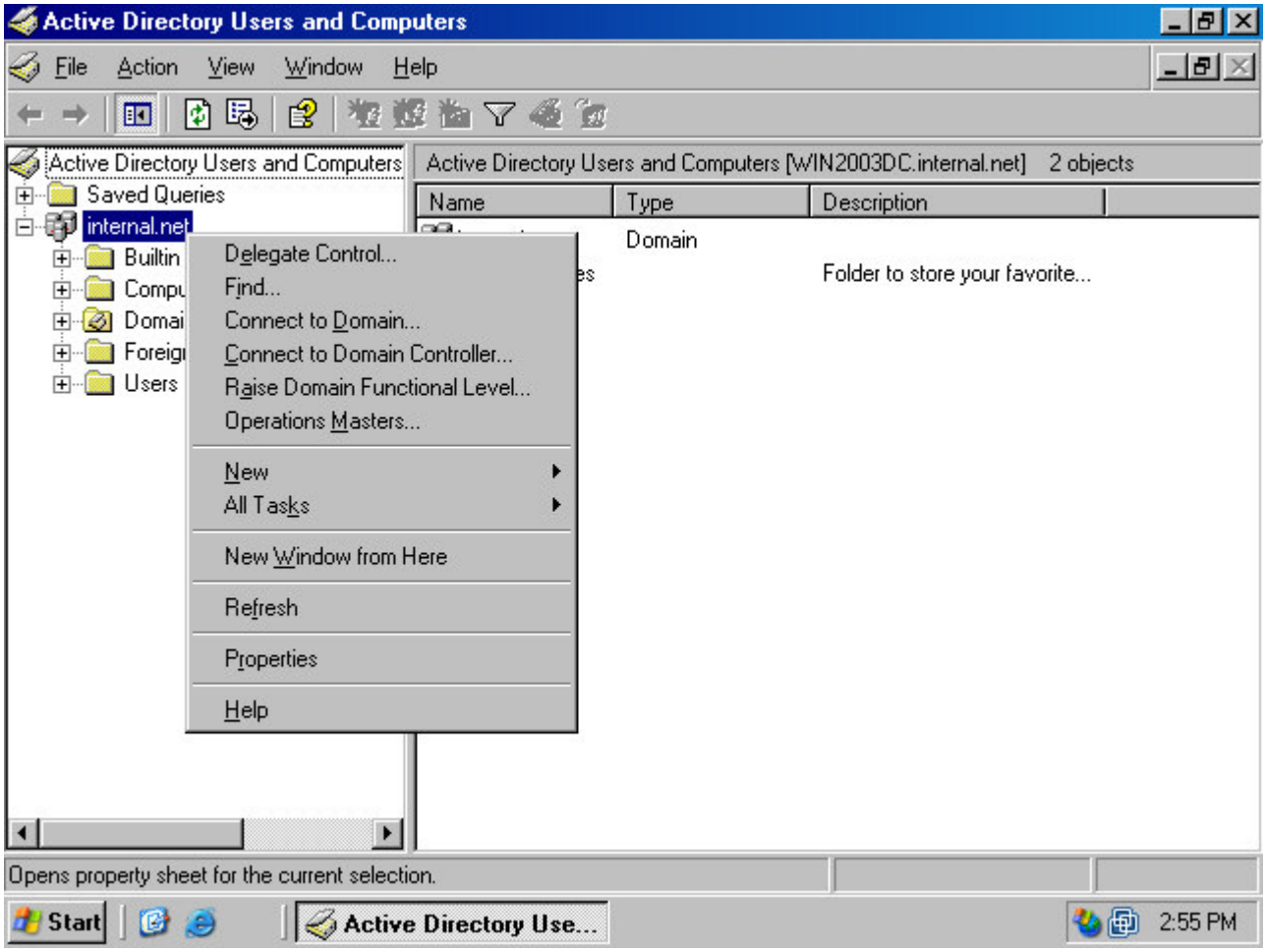
1. Click **Start** point to **Administrative Tools** and click **Active Directory Users and Computers** (figure 1).

Figure 1 (fig101)



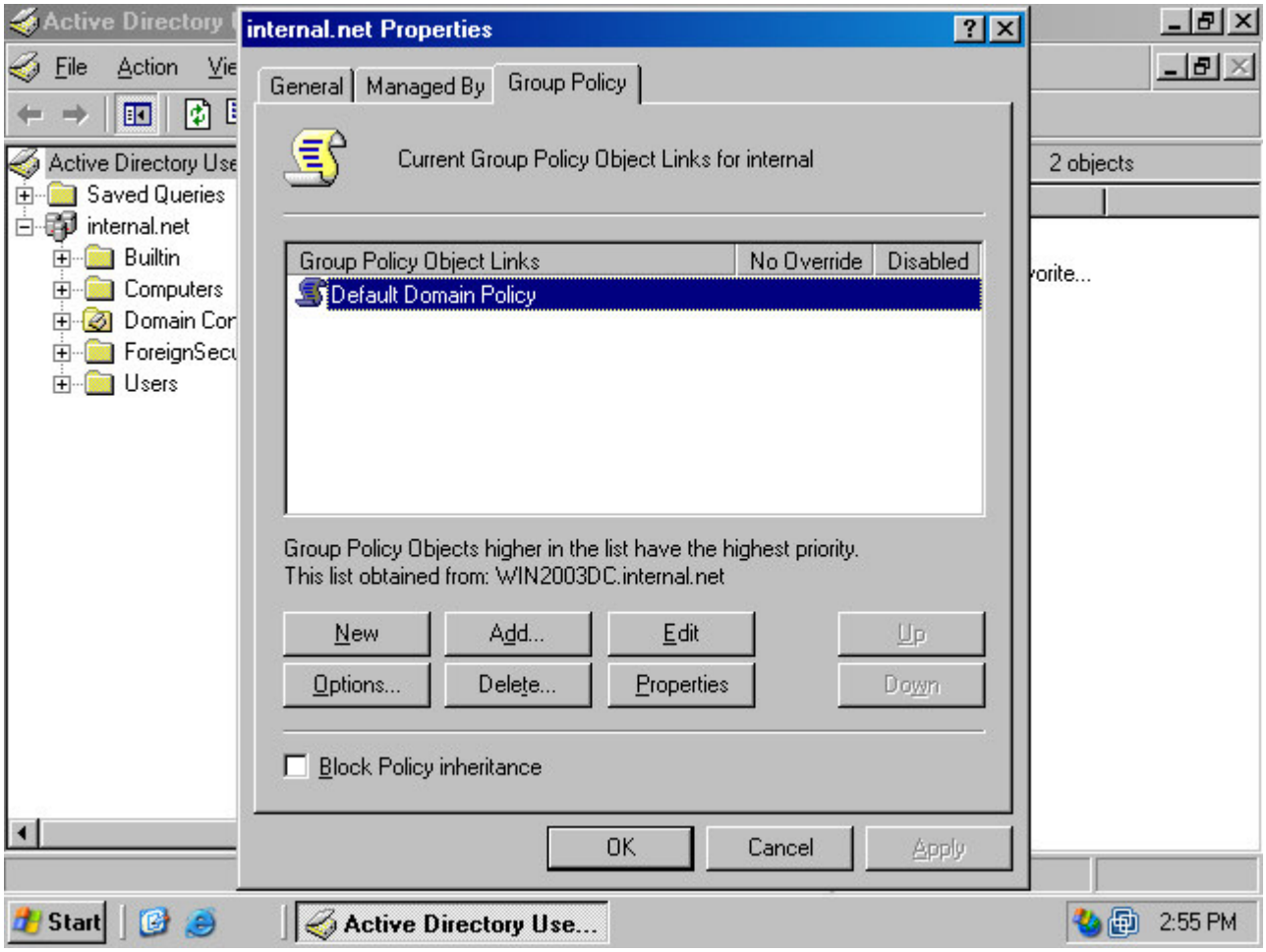
2. In the **Active Directory Users and Computer** console, right click on your domain name and click the **Properties** command (figure 2).

Figure 2 (fig102)



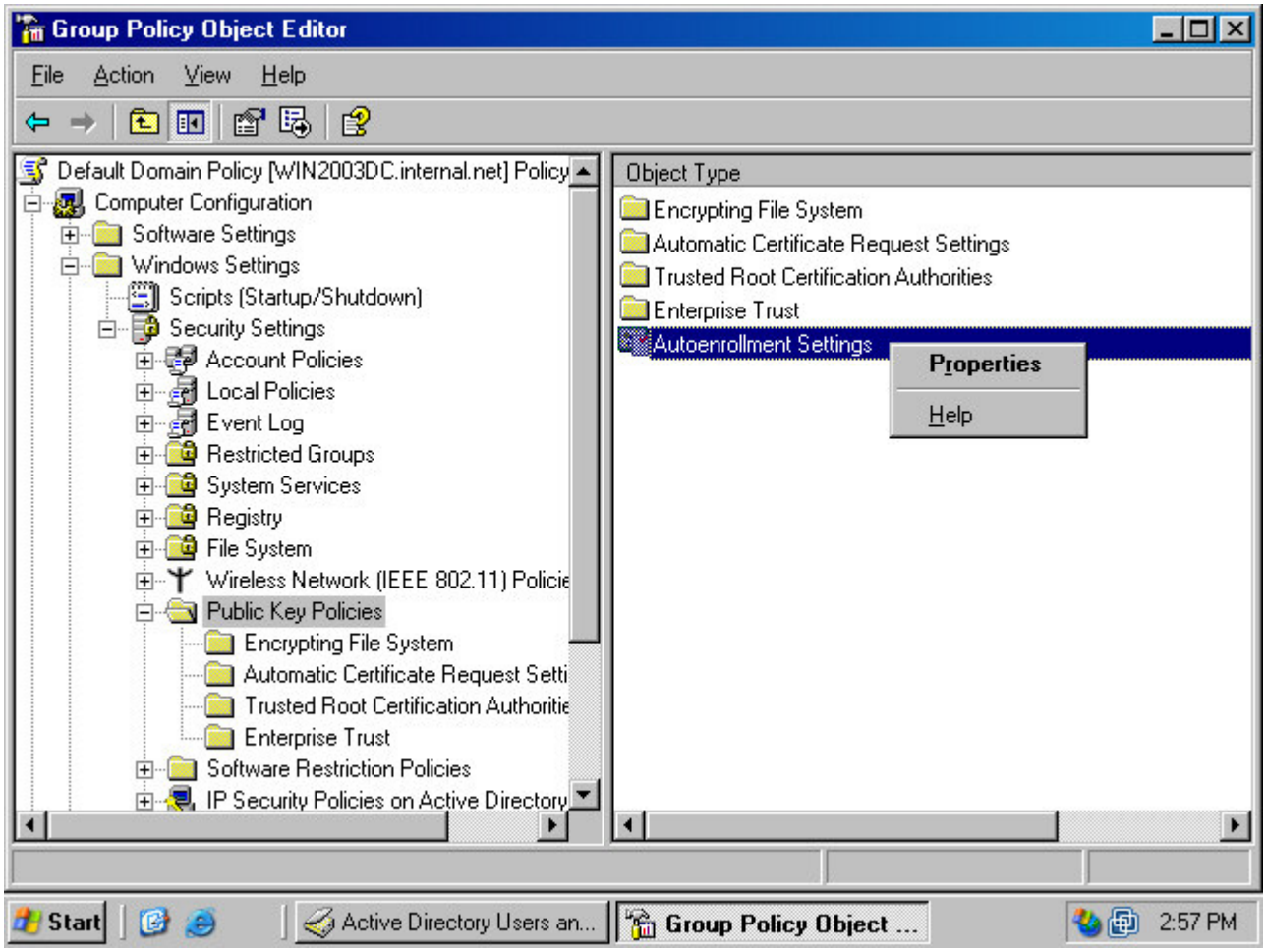
3. In the domain **Properties** dialog box, click on the **Group Policies** tab. On the **Group Policy** tab, click on the **Default Domain Policy** and click the **Edit** button (figure 3).

Figure 3 (fig103)



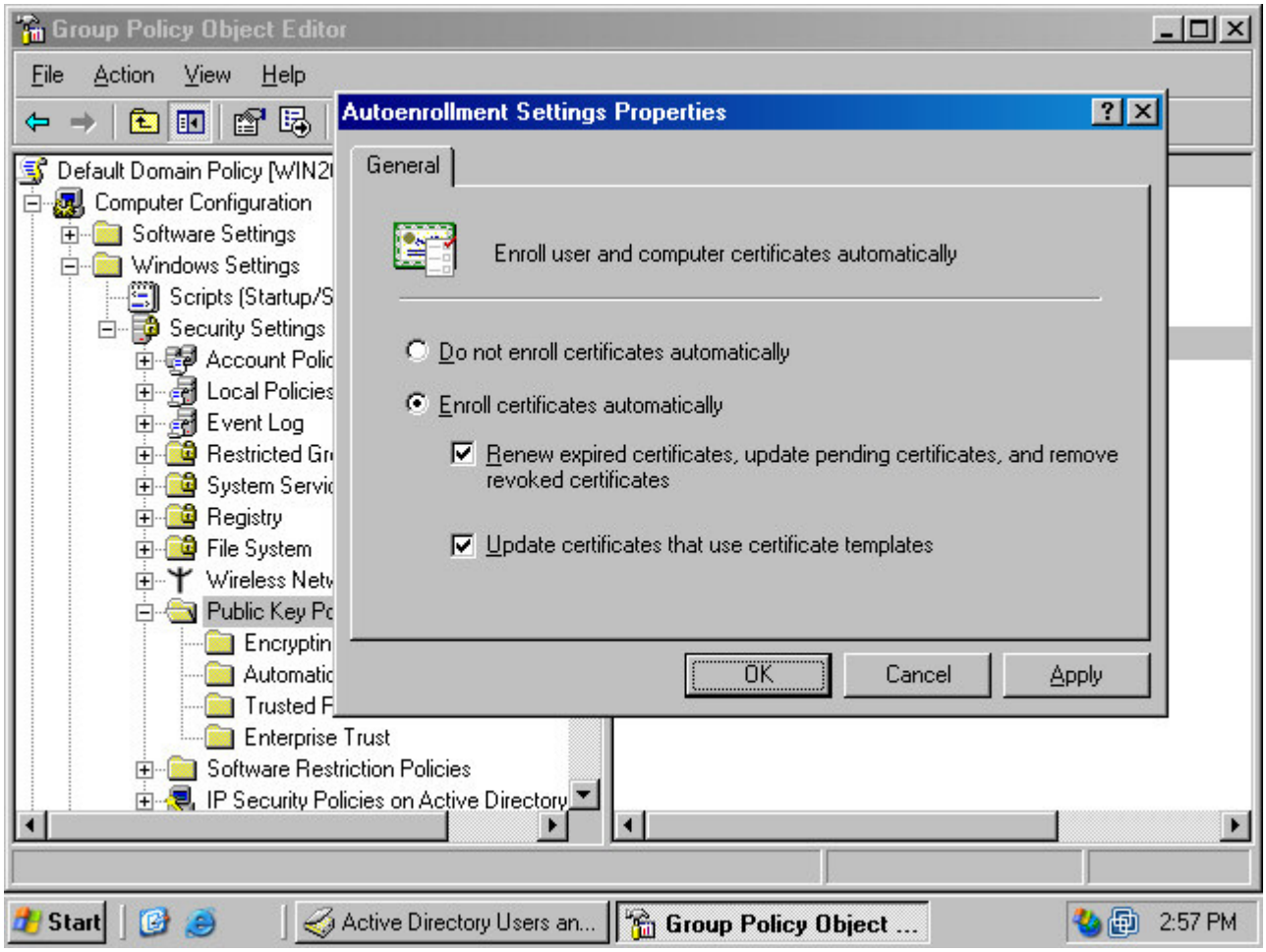
4. In the **Group Policy Object Editor** window, drill down to the **Computer Configuration\Windows Settings\Security Settings\Public Key Policies** node (figure 4). Right click the **Autoenrollment Settings** entry in the right pane of the console and click the **Properties** command.

Figure 4 (fig104)



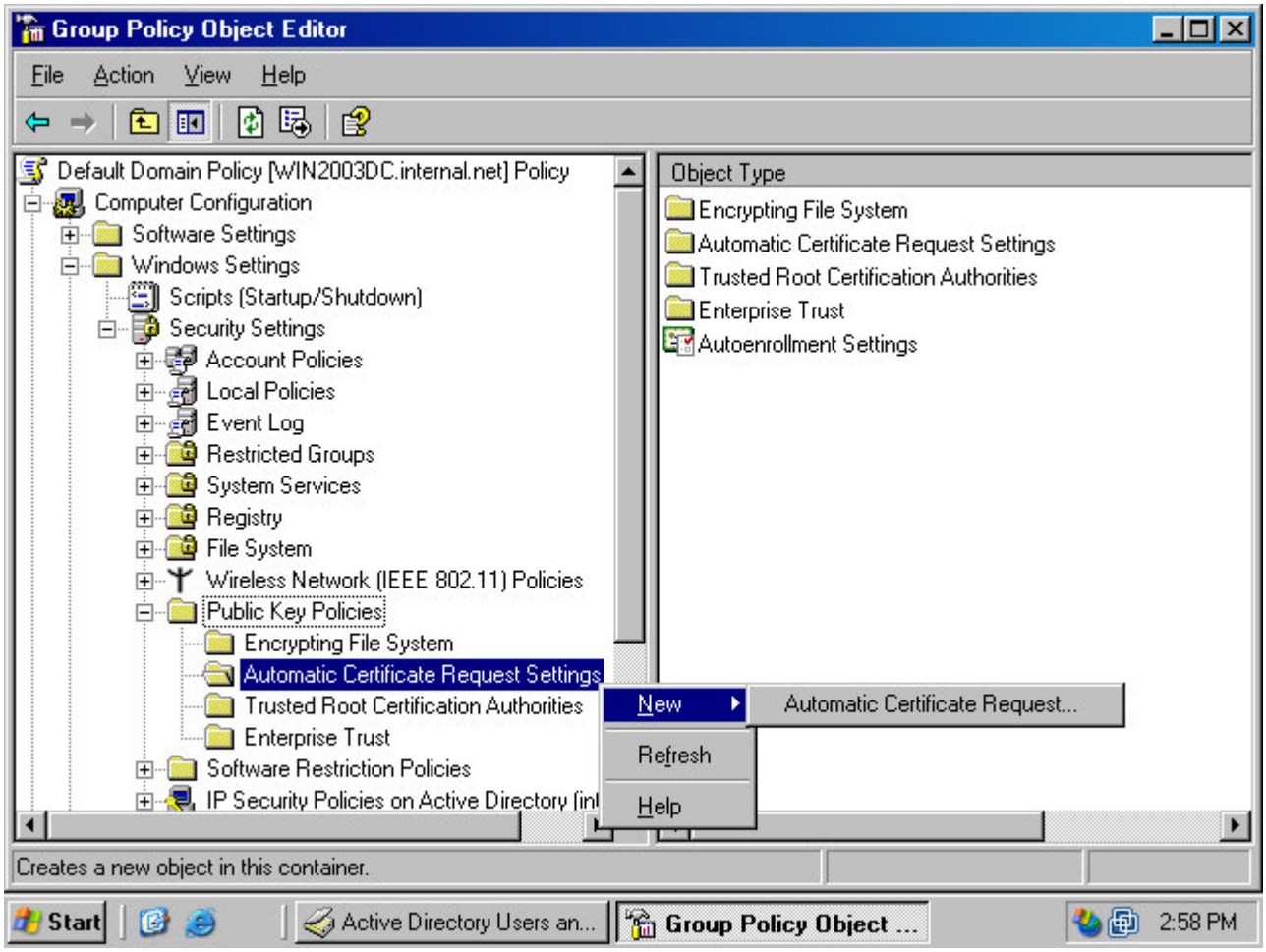
5. In the **Autoenrollment Settings Properties** dialog box (figure 5), select the **Enroll certificates automatically** option. Confirm that both **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates** checkboxes are checked. Click **Apply** and then click **OK**.

Figure 5 (fig105)



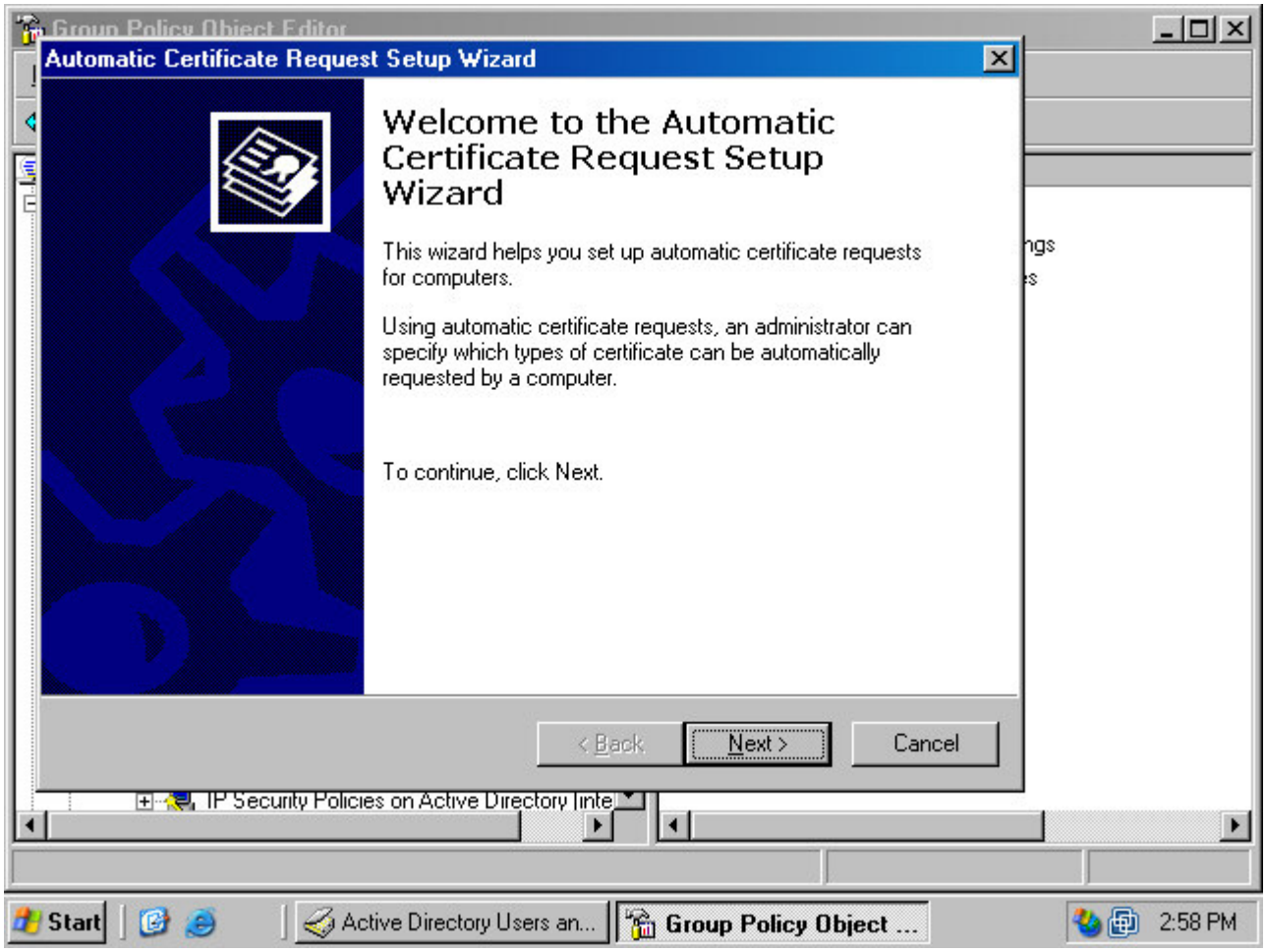
6. The next step sets up domain Group Policy to automatically issue machine certificates to domain members. Click on the **Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request Settings** node in the left pane of the console, then right click it. Point to **New** and click on the **Automatic Certificate Request** command (figure 6)

Figure 6 (fig106)



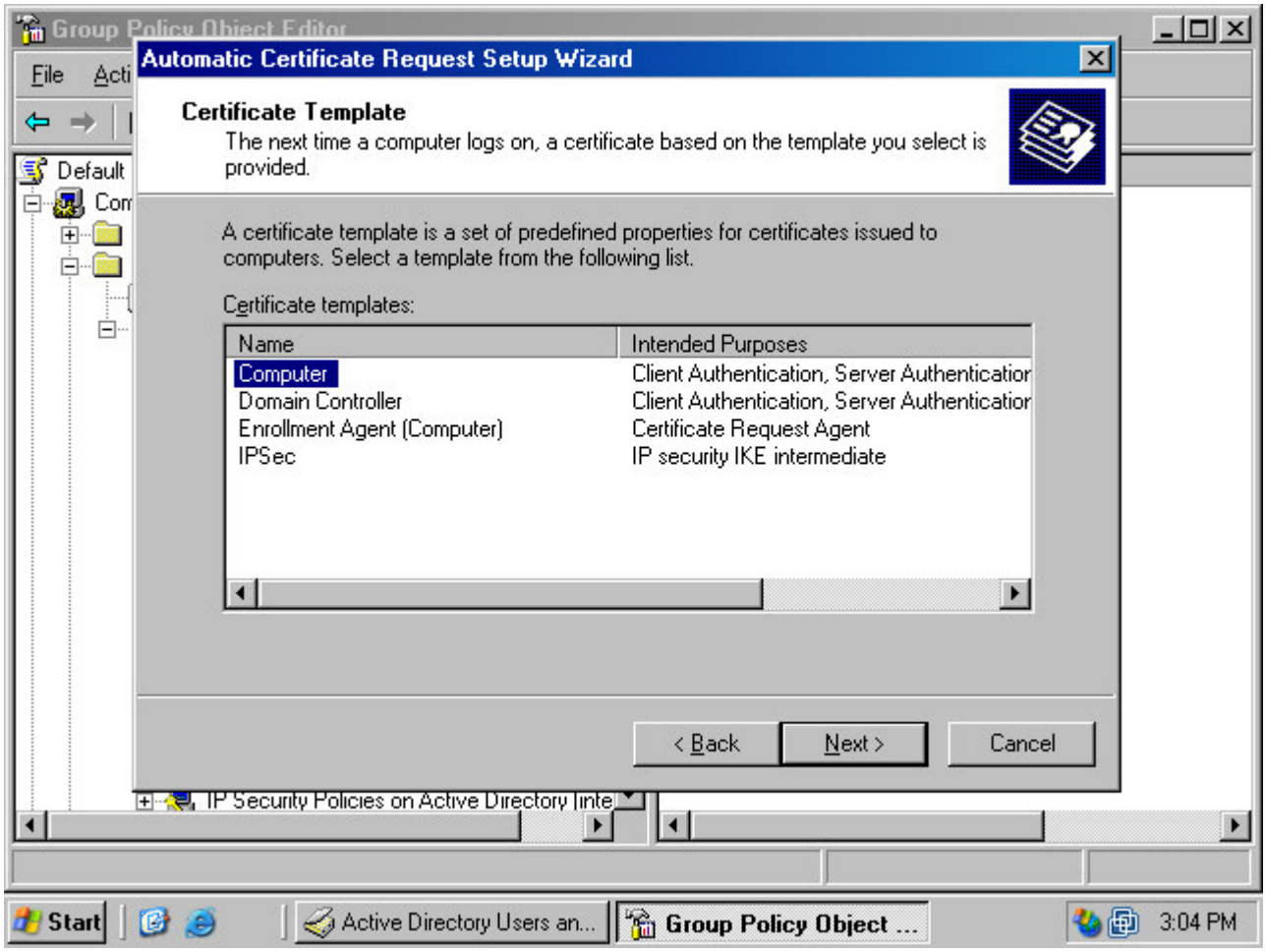
7. Click **Next** on the **Welcome to the Automatic Certificate Request Setup Wizard** page (figure 7).

Figure 7 (fig107)



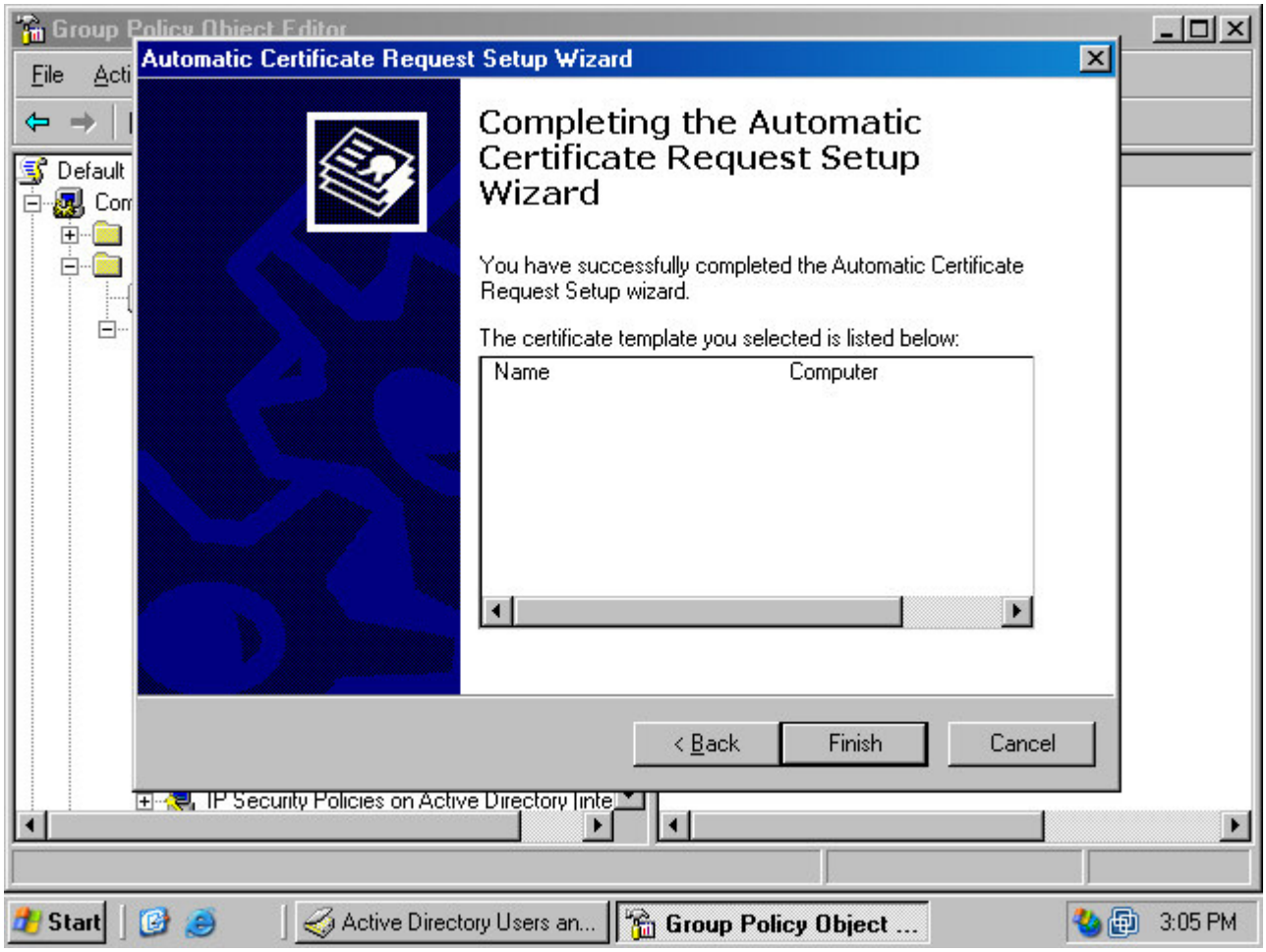
8. On the **Certificate Template** page, click on the **Computer** template in the list of **Certificate Templates**. Click **Next** (figure 8).

Figure 8 (fig108)



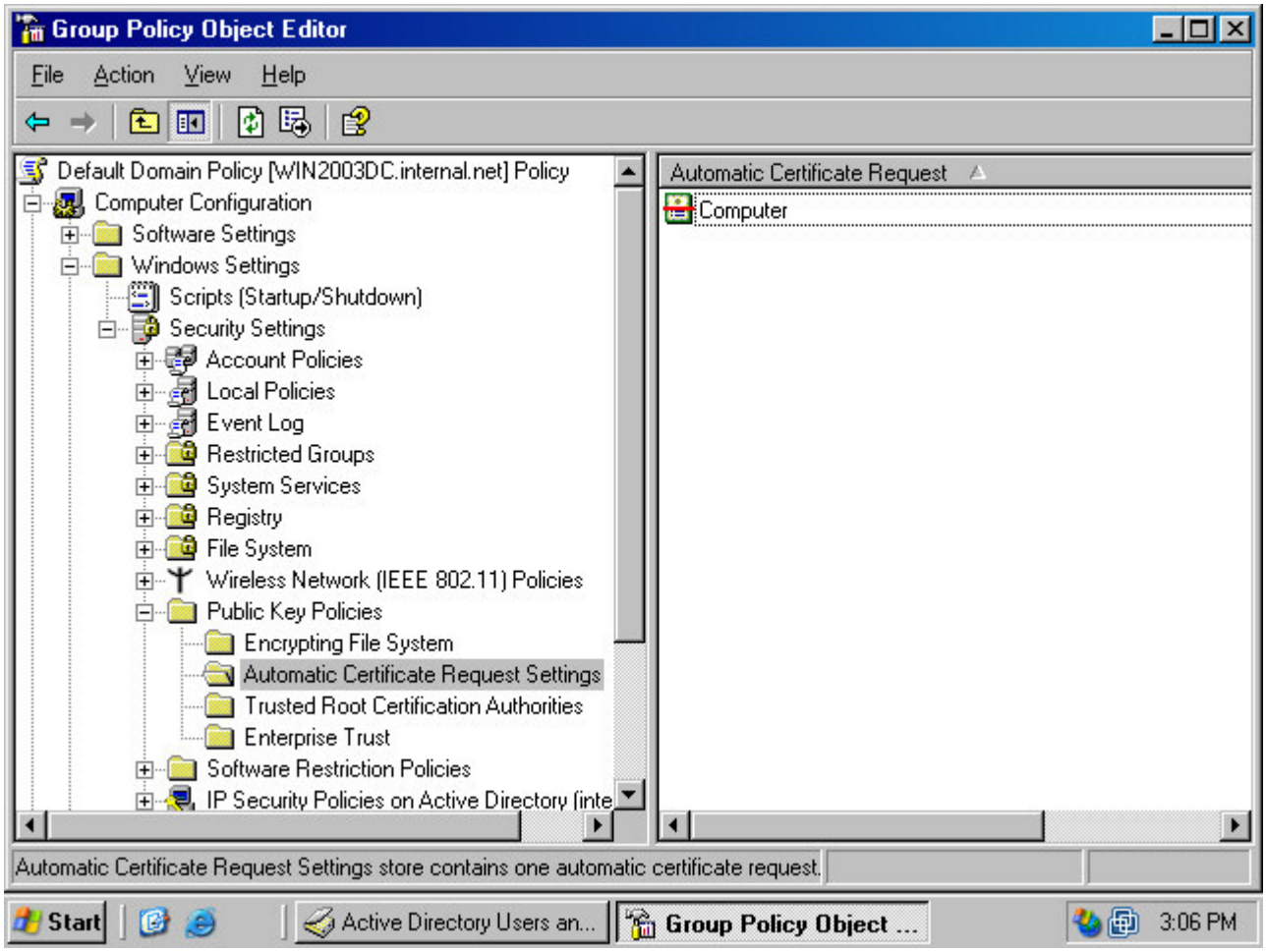
9. Click **Finish** on the **Completing the Automatic Certificate Request Setup Wizard** page (figure 9).

Figure 9 (fig109)



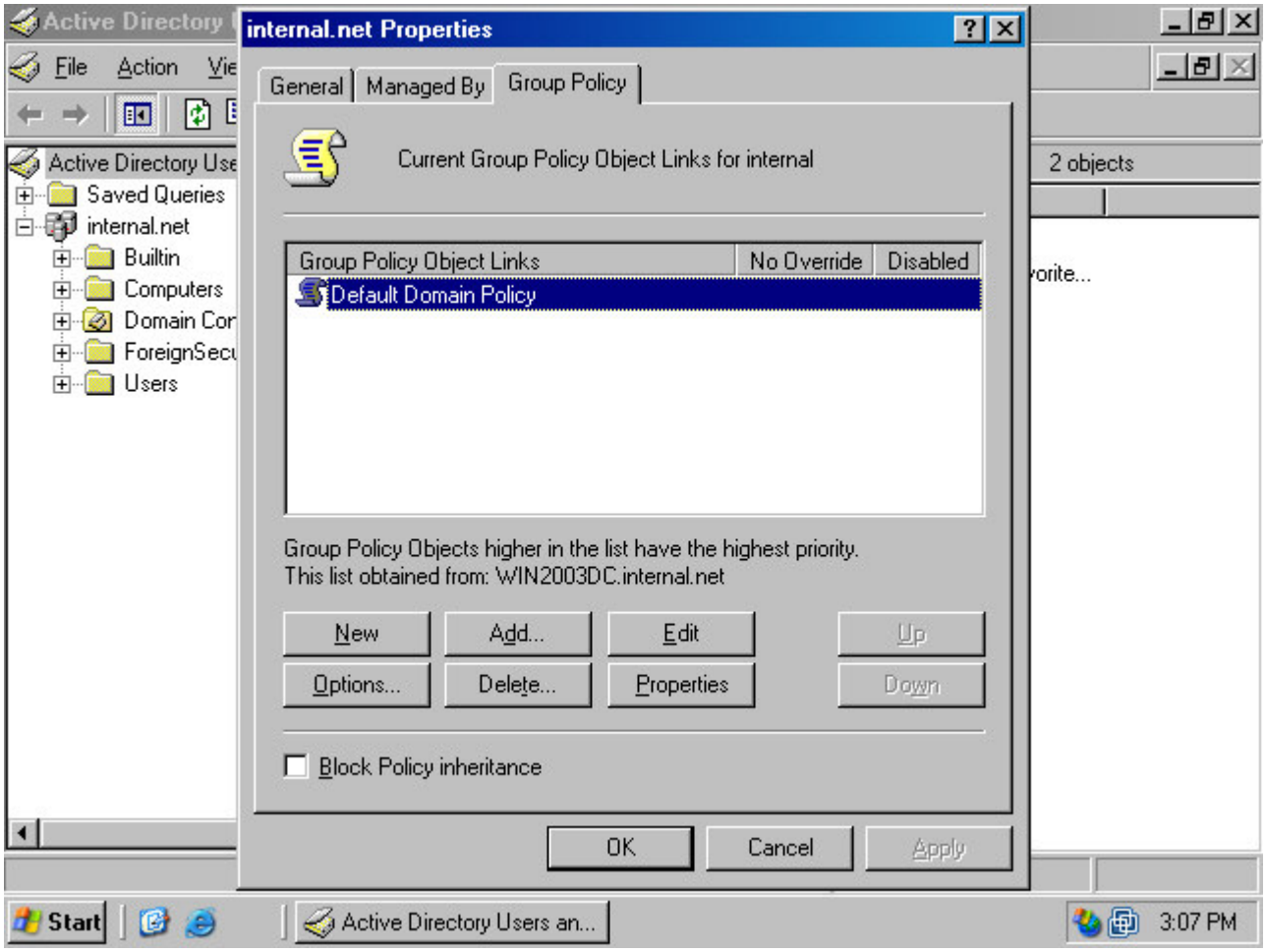
10. You should not see the **Computer** certificate template in the right pane of the console (figure 10). Close the **Group Policy Object Editor** console.

Figure 10 (fig110)



11. Close **OK** in the domain **Properties** dialog box (figure 11).

Figure 11 (fig111)



12. Close the **Active Directory Users and Computers** console.

Forcing Group Policy Updates for Certificate Recipients

Group Policy changes won't take place immediately unless you force them. There are two ways you can force Group Policy changes to be applied immediately:

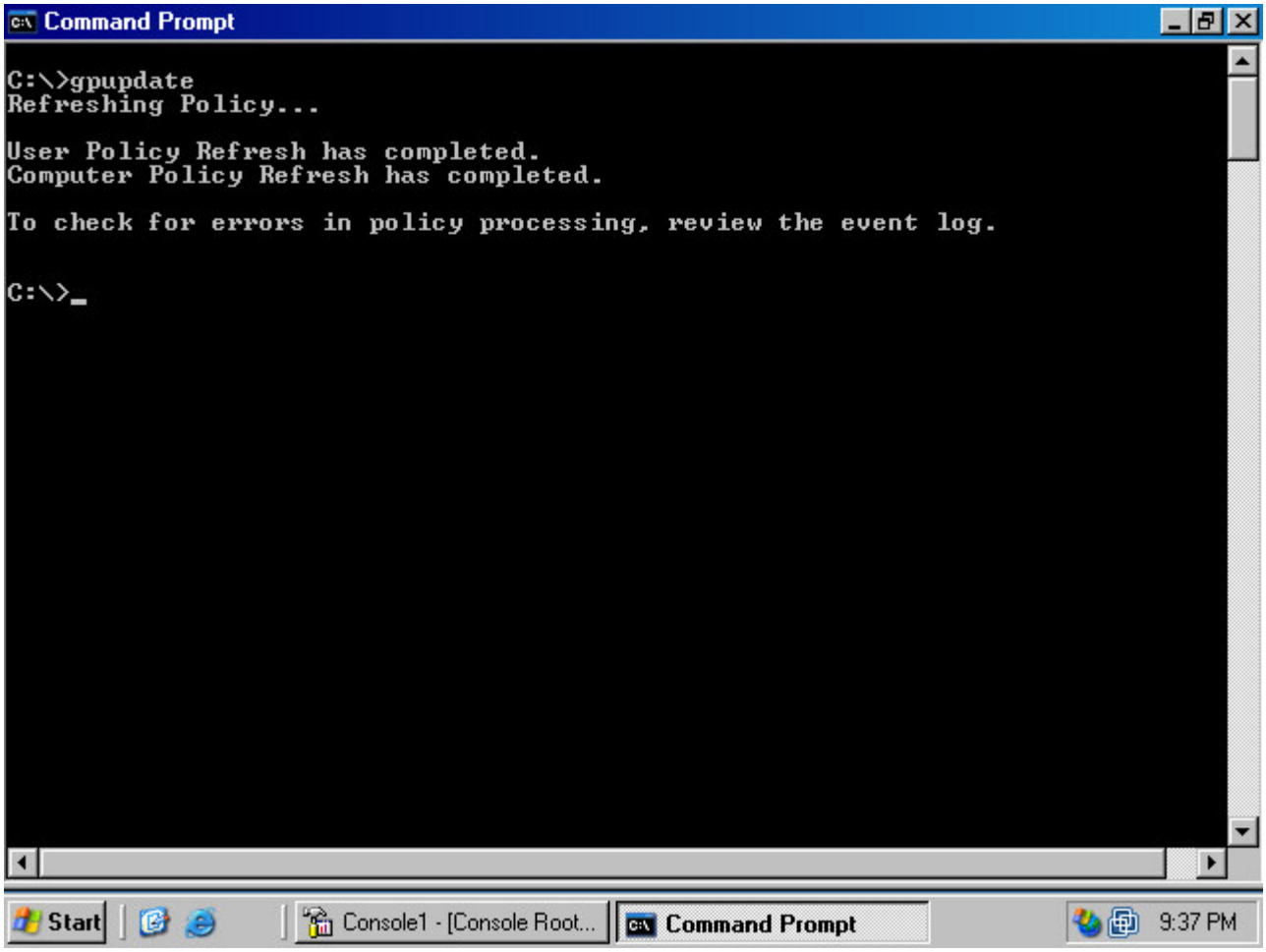
- **The *gpupdate* or *secedit* command**
  The **gpupdate** command is available only Windows XP and Windows Server 2003 machines. Use the **secedit** command on Windows 2000 computers.

- **The Windows XP or Windows Server 2003 Certificates MMC standalone snap-in**
  The Windows XP and Windows Server 2003 **Certificates** standalone snap-in allows you to use the graphic interface to immediately update Group Policy on the VPN client.

Perform the following steps to refresh Group Policy on the VPN client using the **gpupdate** or **secedit** commands:

1. Click **Start** then click the **Run** command on a Windows Server 2003 or Windows XP VPN client.
2. At the command prompt, type **gpupdate** and press ENTER. You will see what appears in figure 12. No errors will appear in the **Command Prompt** window. You can check for errors in the **Event Viewer**.

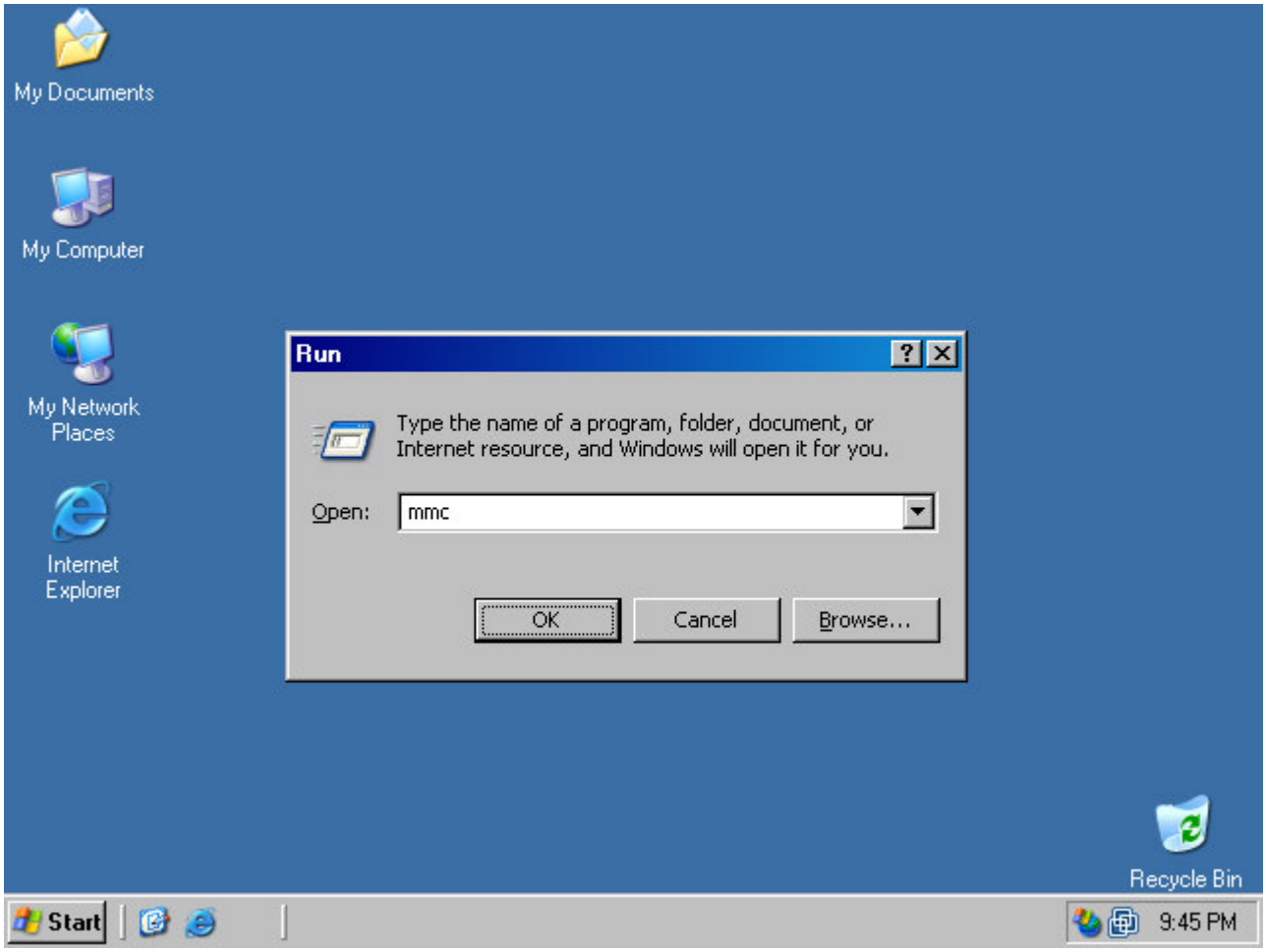
Figure 12 (fig112)



You need to confirm that the domain member VPN client received its certificate during the Group Policy update. Perform the following steps to refresh Group Policy on the VPN client using the **Windows Server 2003** or **Windows XP Certificates** MMC standalone snap-in:

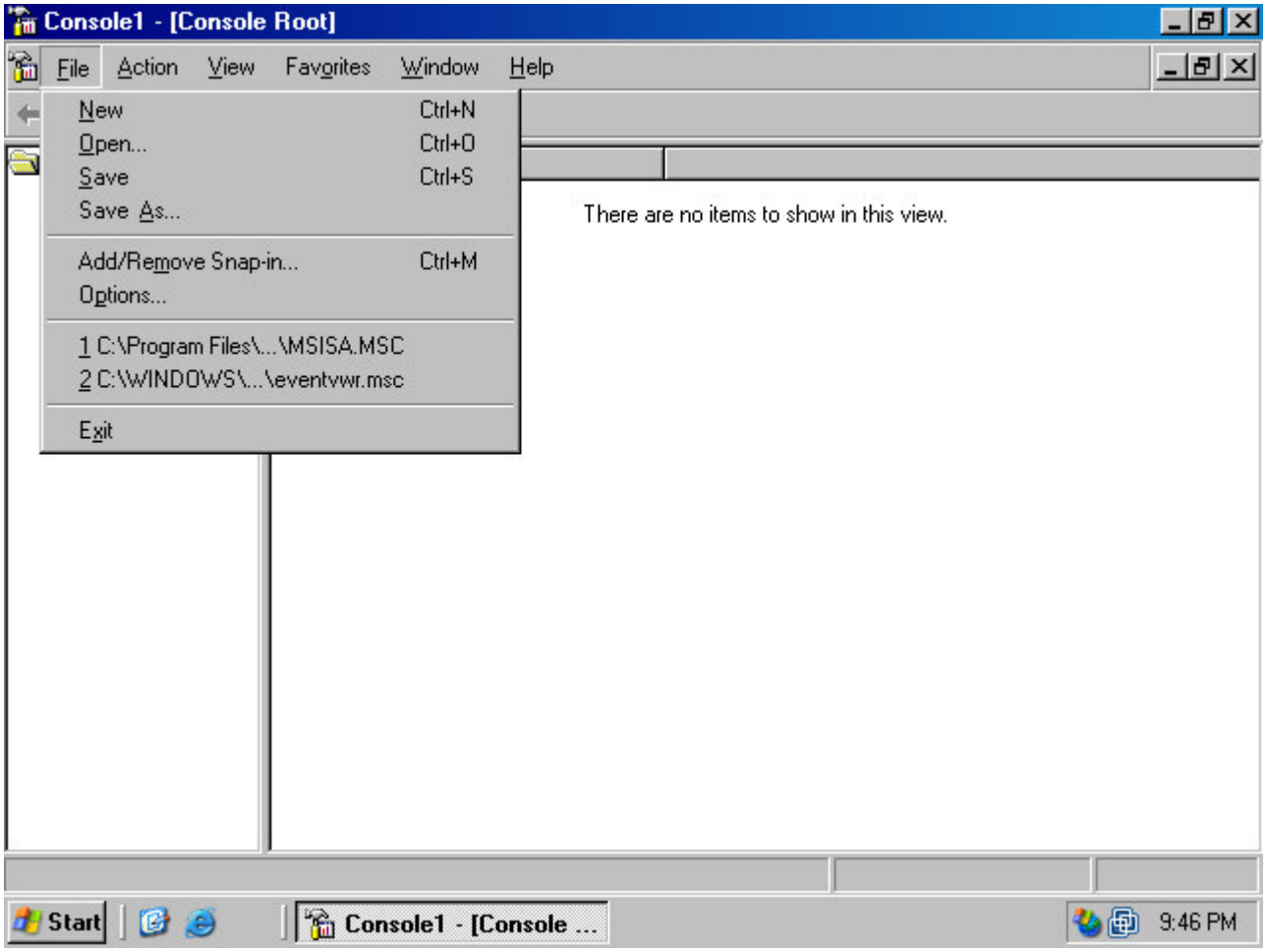
1. Click **Start**, and then click the **Run** command. Type **mmc** in the **Open** text box and click **OK**.

Figure 13 (fig113)



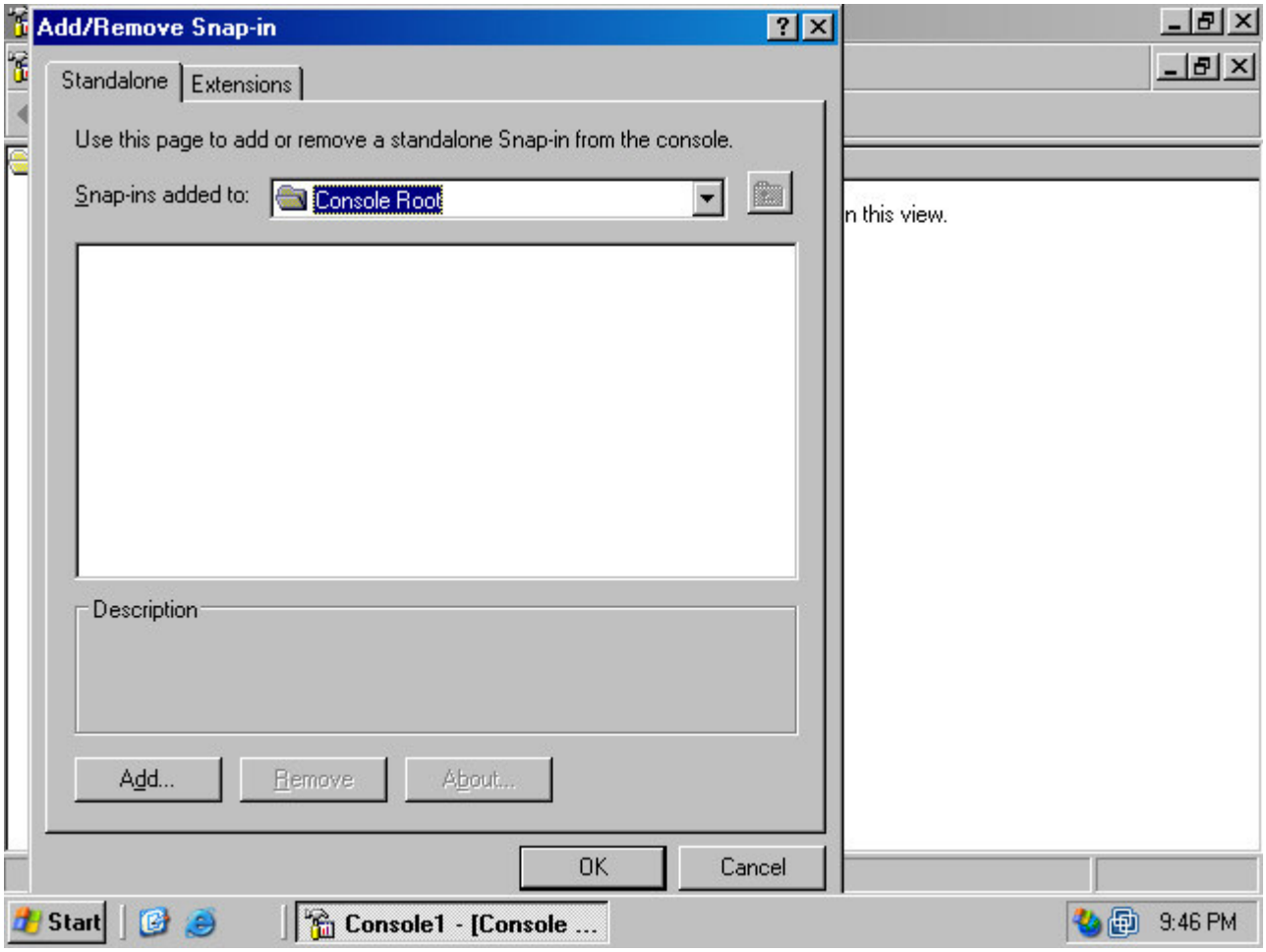
2. In the **Console1** window, click the **File** menu and then click the **Add/Remove Snap-in** command (figure 14).

Figure 14 (fig 114)



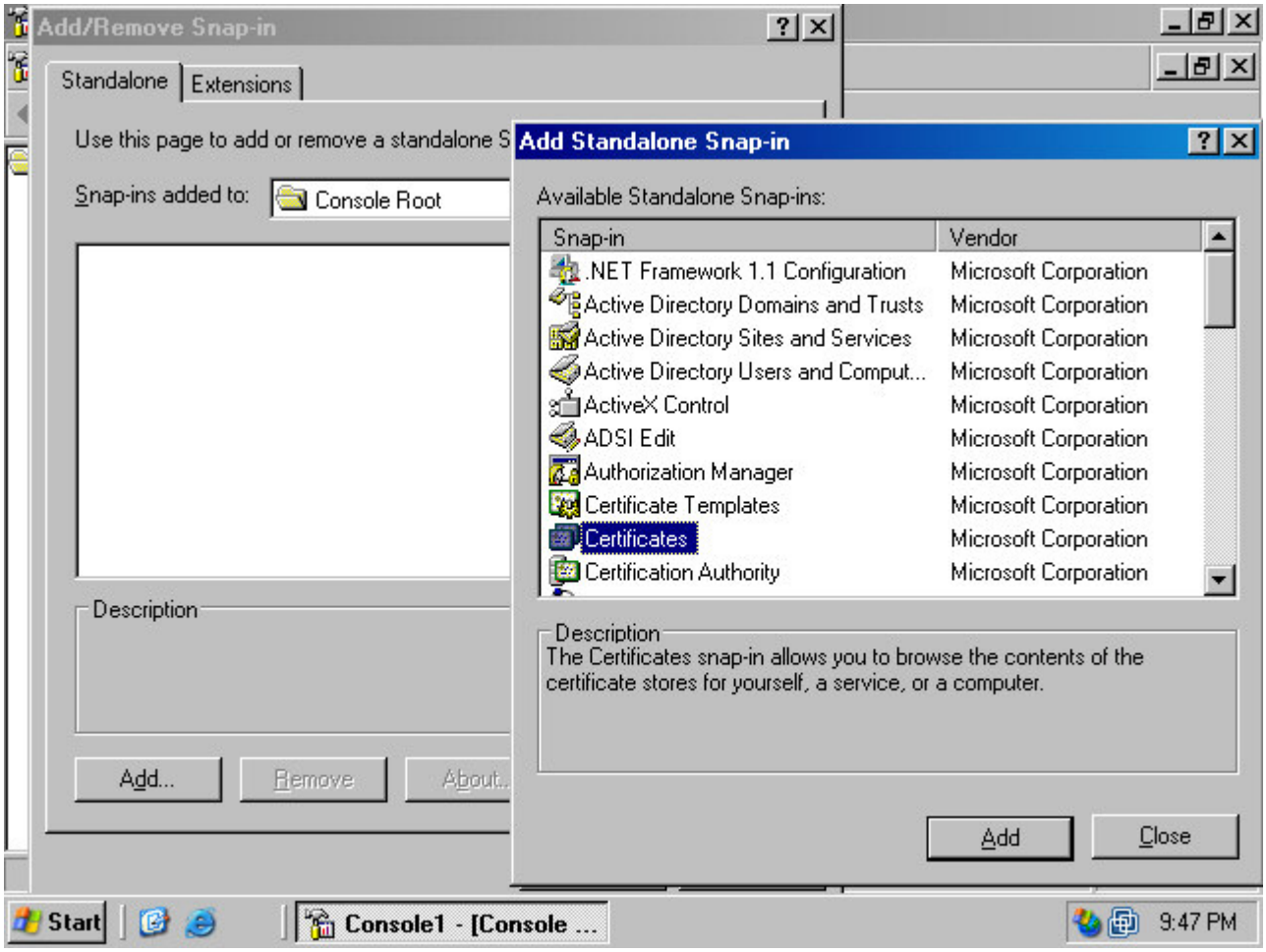
3. In the **Add/Remove Snap-in** dialog box, click the **Add** button (figure 15).

Figure 15 (fig115)



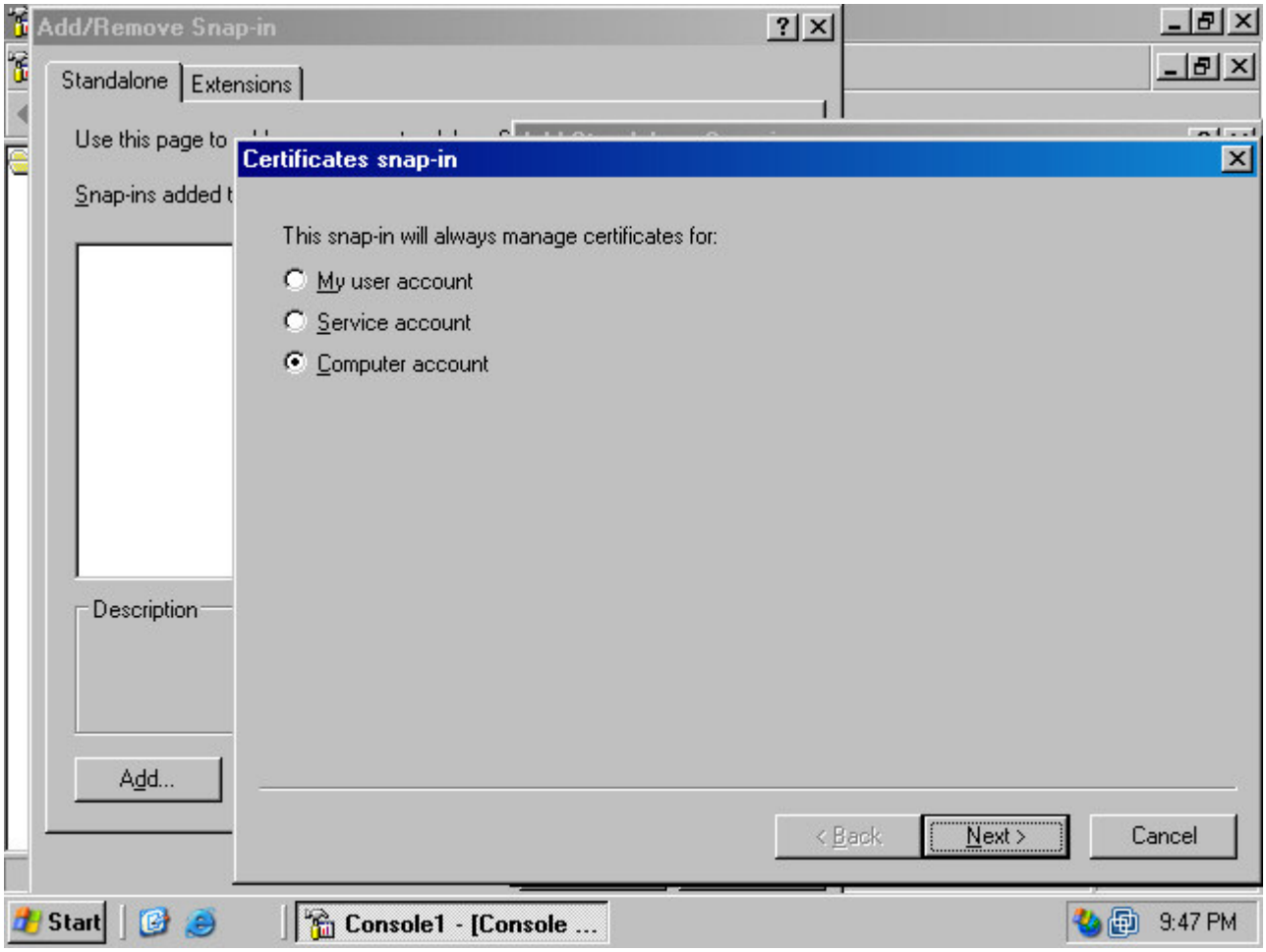
4. In the **Add Standalone Snap-in** dialog box, click the **Certificates** snap-in in the list of **Available Standalone Snap-ins** (figure 16). Click **Add**.

Figure 16 (fig116)



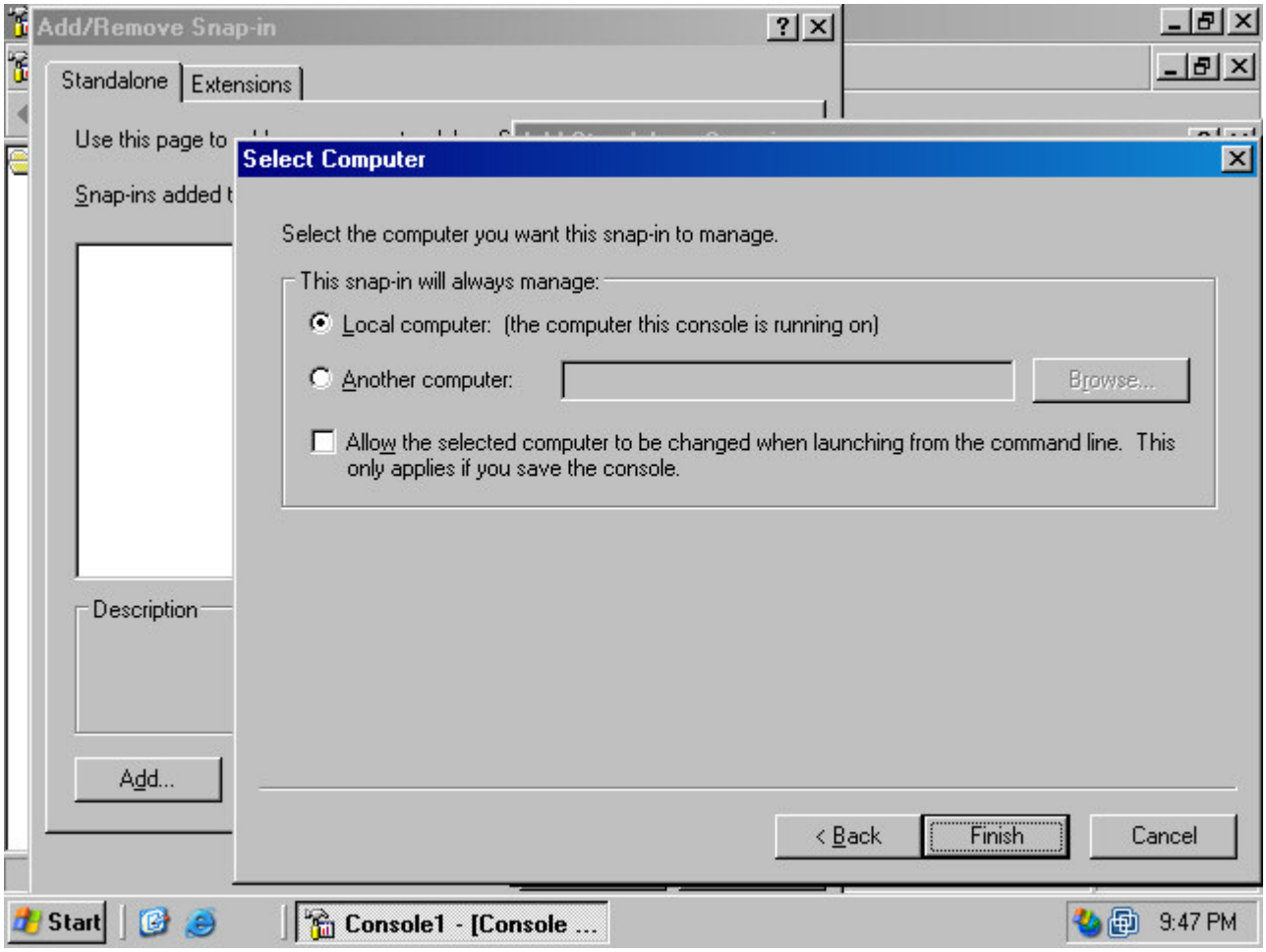
5. Select the **Computer account** option on the **Certificates snap-in** page (figure 17).

Figure 17 (fig117)



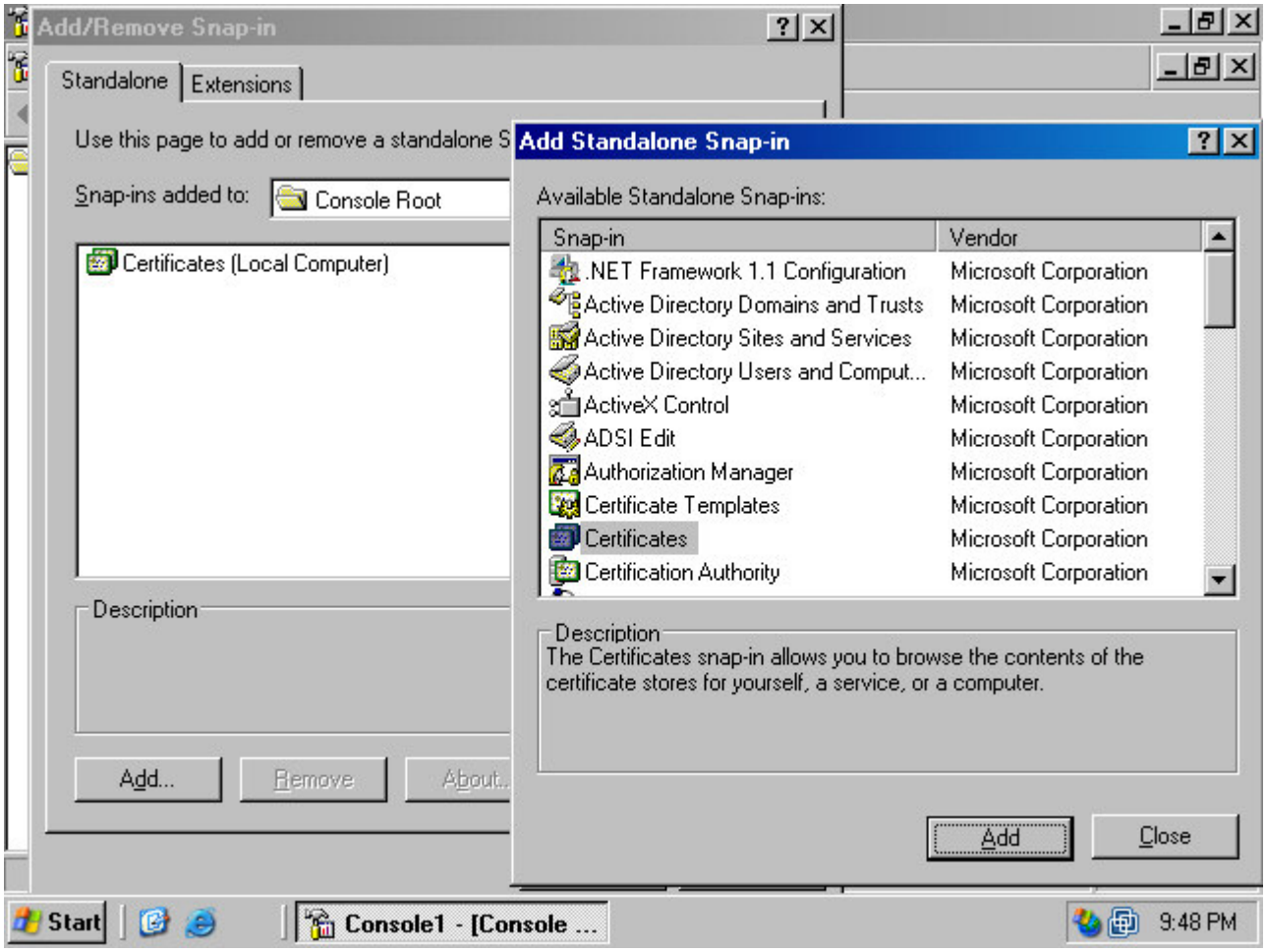
6. Select **Local computer: (the computer this console is running on)** on the **Select Computer** page. Click **Finish** (figure 18).

Figure 18 (fig118)



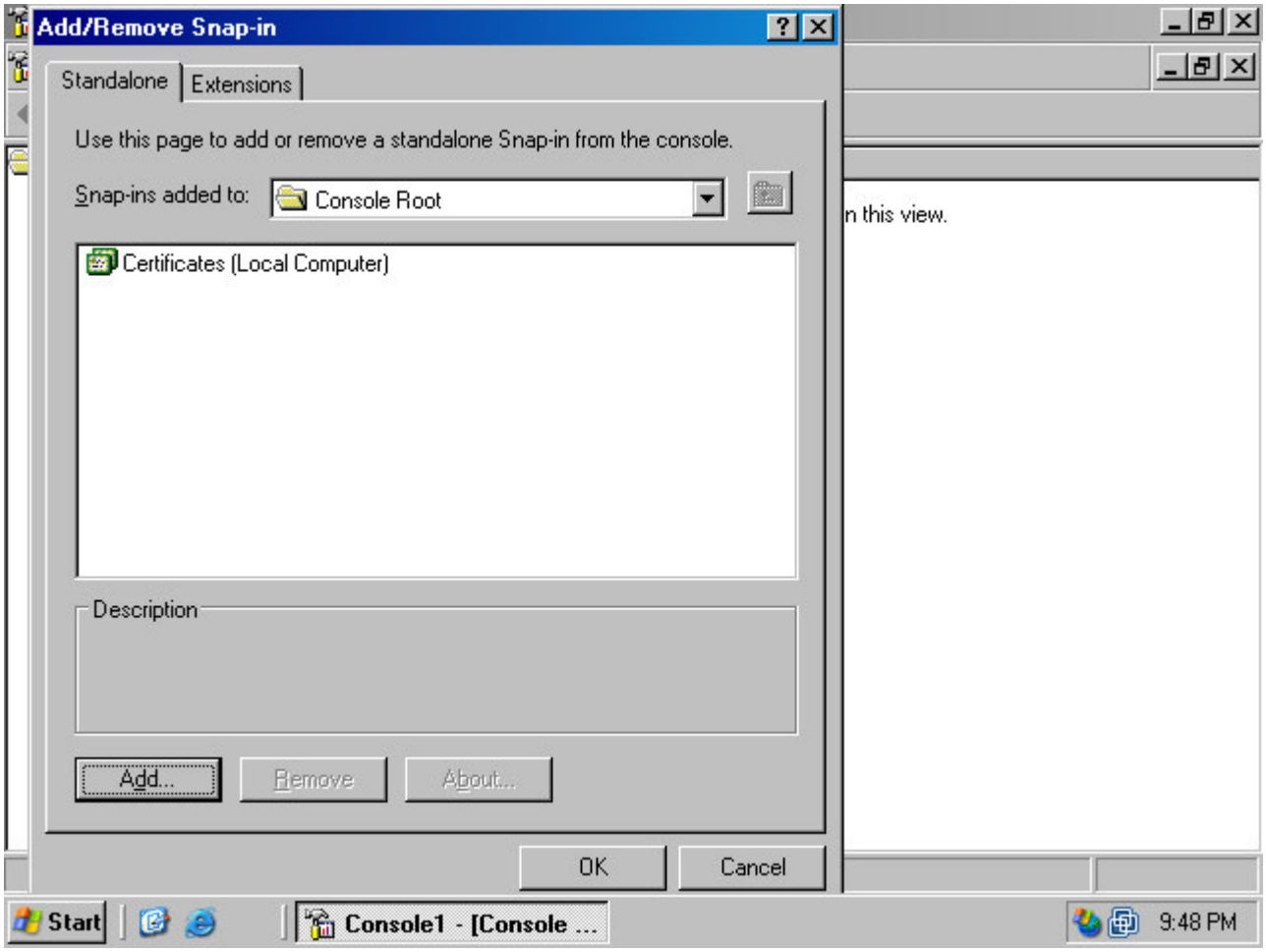
7. Click **Close** in the **Add Standalone Snap-in** dialog box (figure 19)

Figure 19 (fig119)



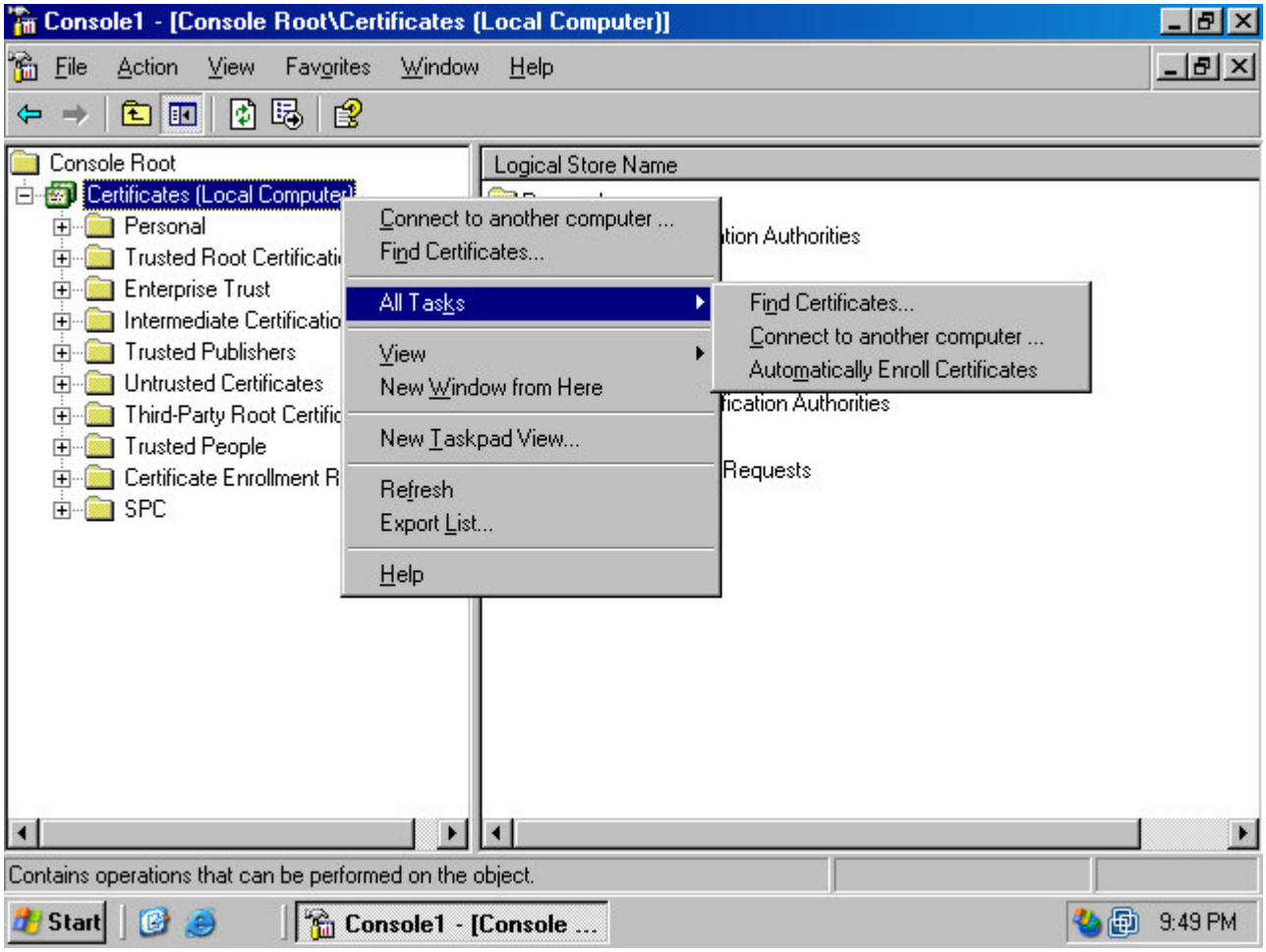
8. Click **OK** in the **Add/Remove Snap-in** dialog box (figure 20).

Figure 20 (fig120)



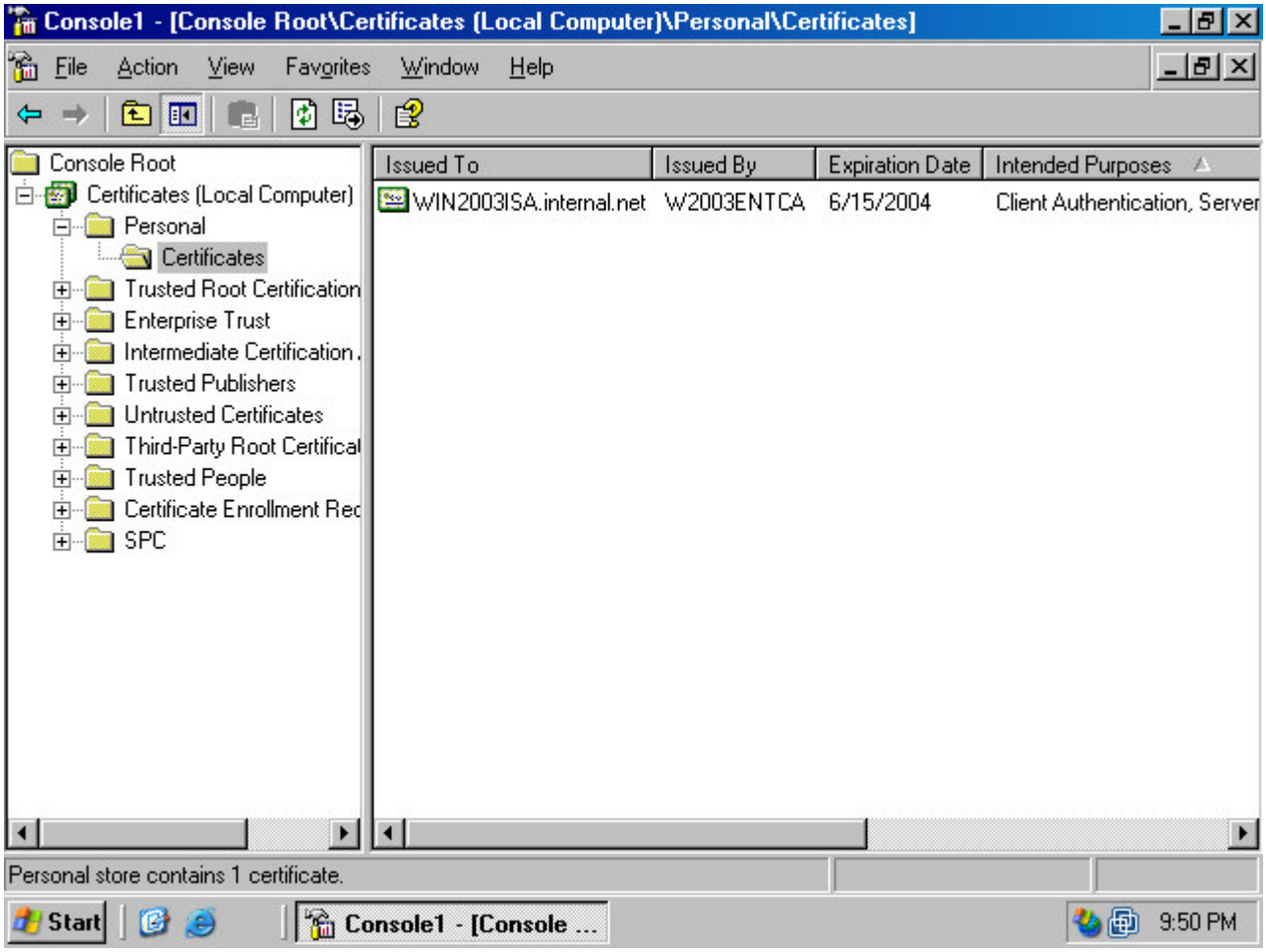
9. Click on the **Certificates (Local Computer)** node in the left pane of the console, and then right click the same node. Point to **All Tasks** and click on **Automatically Enroll Certificates** (figure 21).

Figure 21 (fig121)



10. You will see the computer certificate in the right pane of the console (figure 22)

Figure 22 (fig122)



Automate User Certificate Assignment with Autoenrollment

You can assign user certificates *if* for Windows XP and Windows Server 2003 VPN clients. You need to perform the following procedures to use autoenrollment to assign user certificates to VPN Windows XP and Windows Server 2003 clients:

- **Configure an email address for the User Account**
  The user account must have an email address associated with it. User certificate autoenrollment will not work if the account does not have an email address.

- **Create a Custom User Template for User Certificate Autoenrollment**
  The user certificate issued via autoenrollment is based on a user certificate template derived from the built-in user certificate template. You copy the built-in user certificate template and customize it later if you wish.

- **Configure the enterprise CA to assign User Certificates Using the Customer User Template**
  The enterprise CA is configured to be aware of the custom User Certificate. Once the CA is aware of the certificate, the CA can issue the certificate via Group Policy.

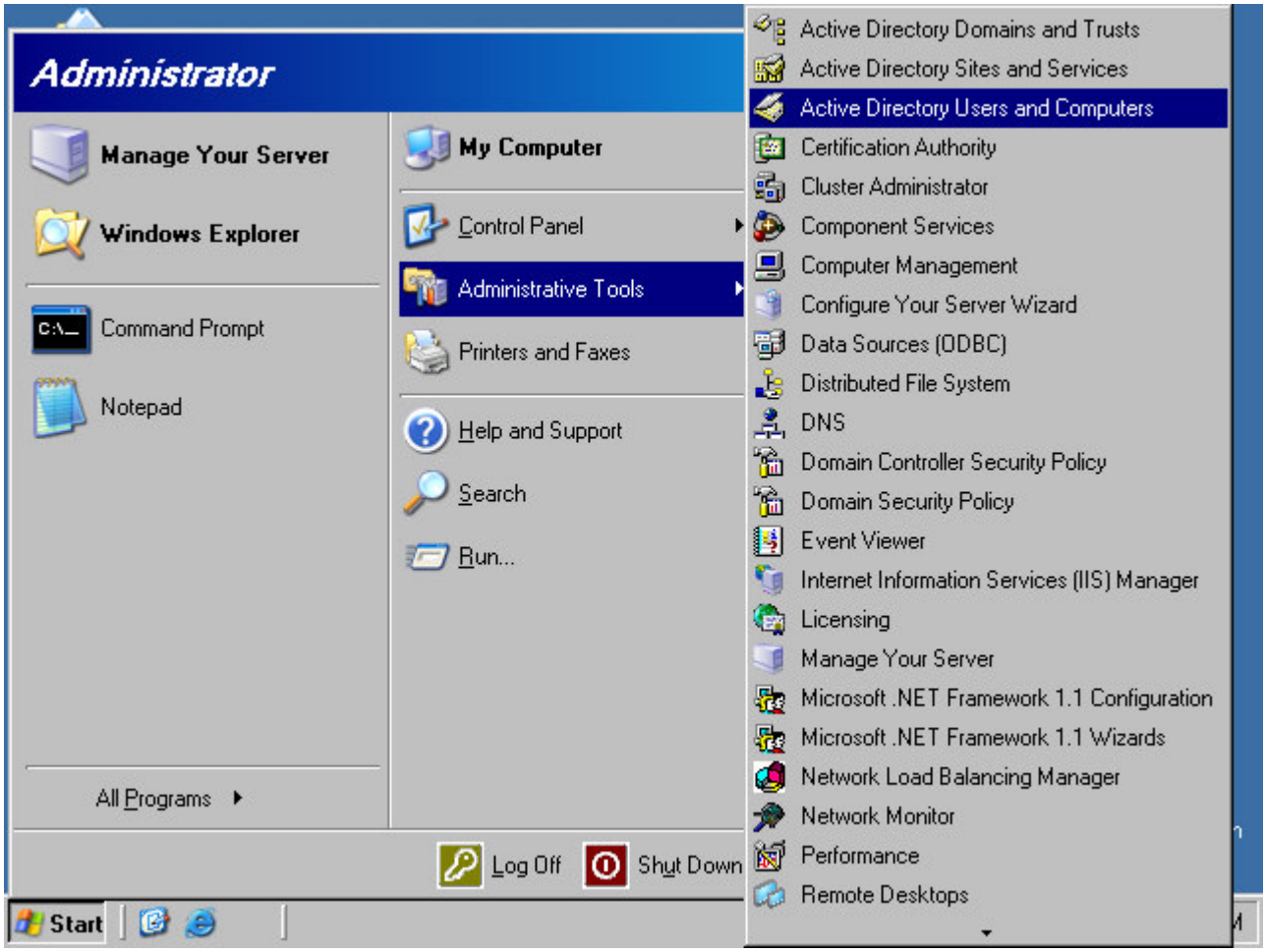
- **Configure autoenrollment in Group Policy**
  The last step is to configure user certificate autoenrollment in domain Group Policy. Only Windows XP and Windows Server 2003 clients receive user certificates via Group Policy (you can still assign user certificates to Windows 2000 and downlevel Windows clients, but you will need to use methods *other than* autoenrollment).

Configuring an Email Address for the User Account

Perform the following steps to configure an email address for the user account:

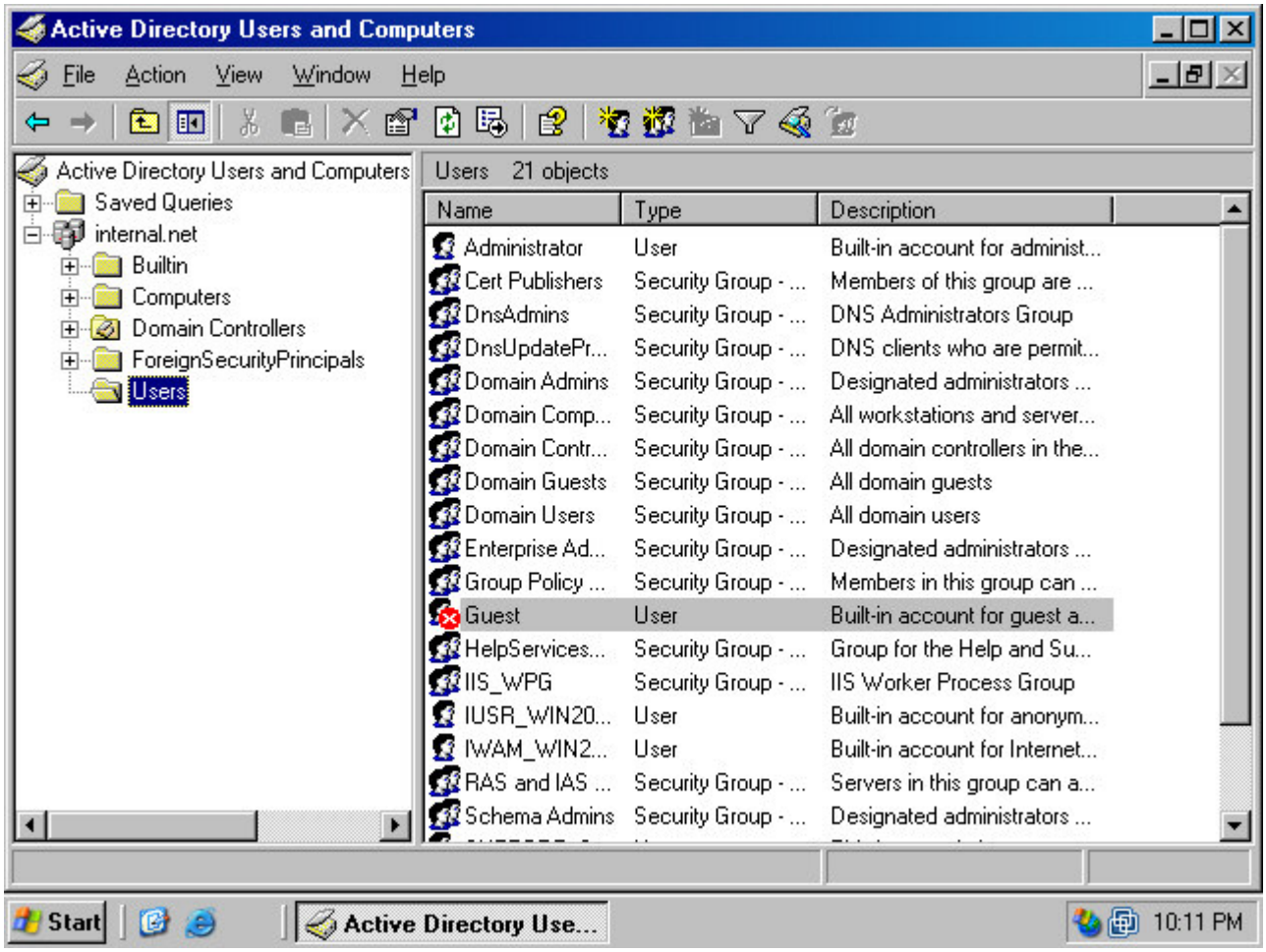
1. Click **Start** and point to **Administrative Tools**. Click on **Active Directory Users and Computers** (figure 23).

Figure 23 (fig123)



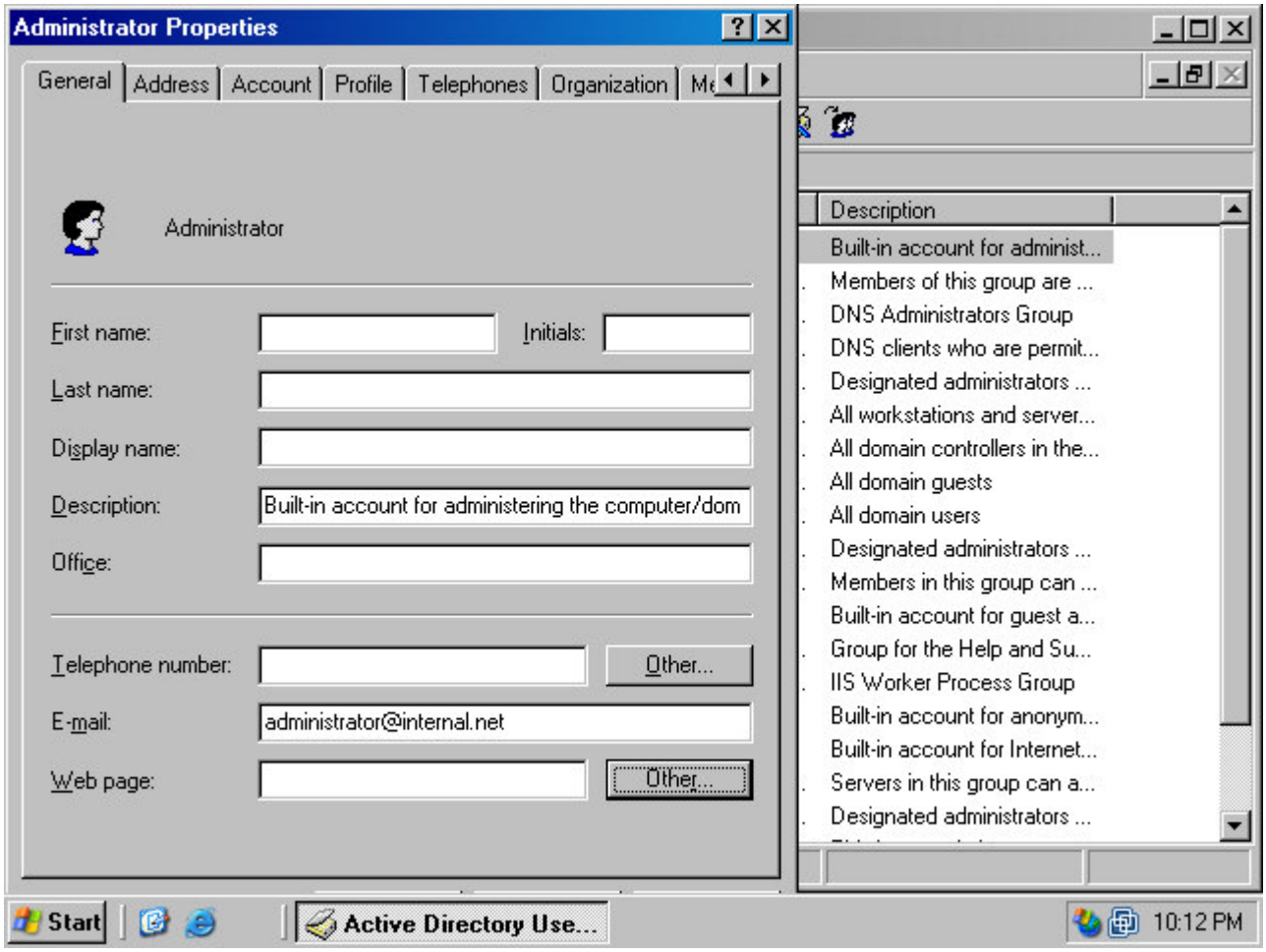
2. In the **Active Directory Users and Computers** console (figure 24), expand your domain name and click on the **Users** node. Double click on a user account in the right pane of the console (figure 24).

Figure 24 (fig 124)



3. On the **General** tab in the user account **Properties** dialog box, enter an email address in the **E-mail** text box (figure 25). This email address is required to create the required entries in the email address fields of the user certificate issued to the user via autoenrollment.

Figure 25 (fig126)

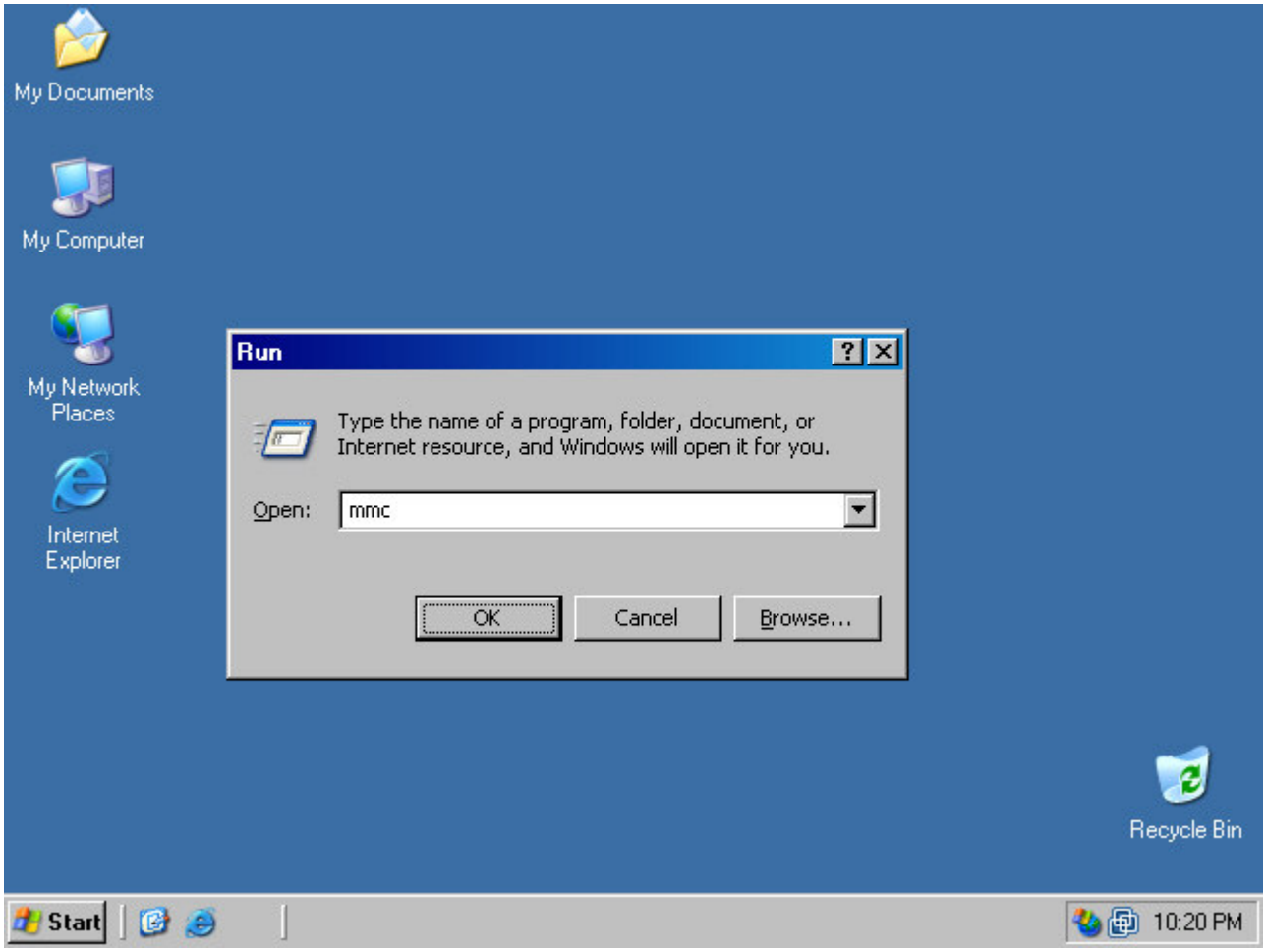


Creating the New User Certificate Template

The next step is to create a new User Certificate template that will be issued to domain users via Group Policy. Perform the following steps to create the new user template:

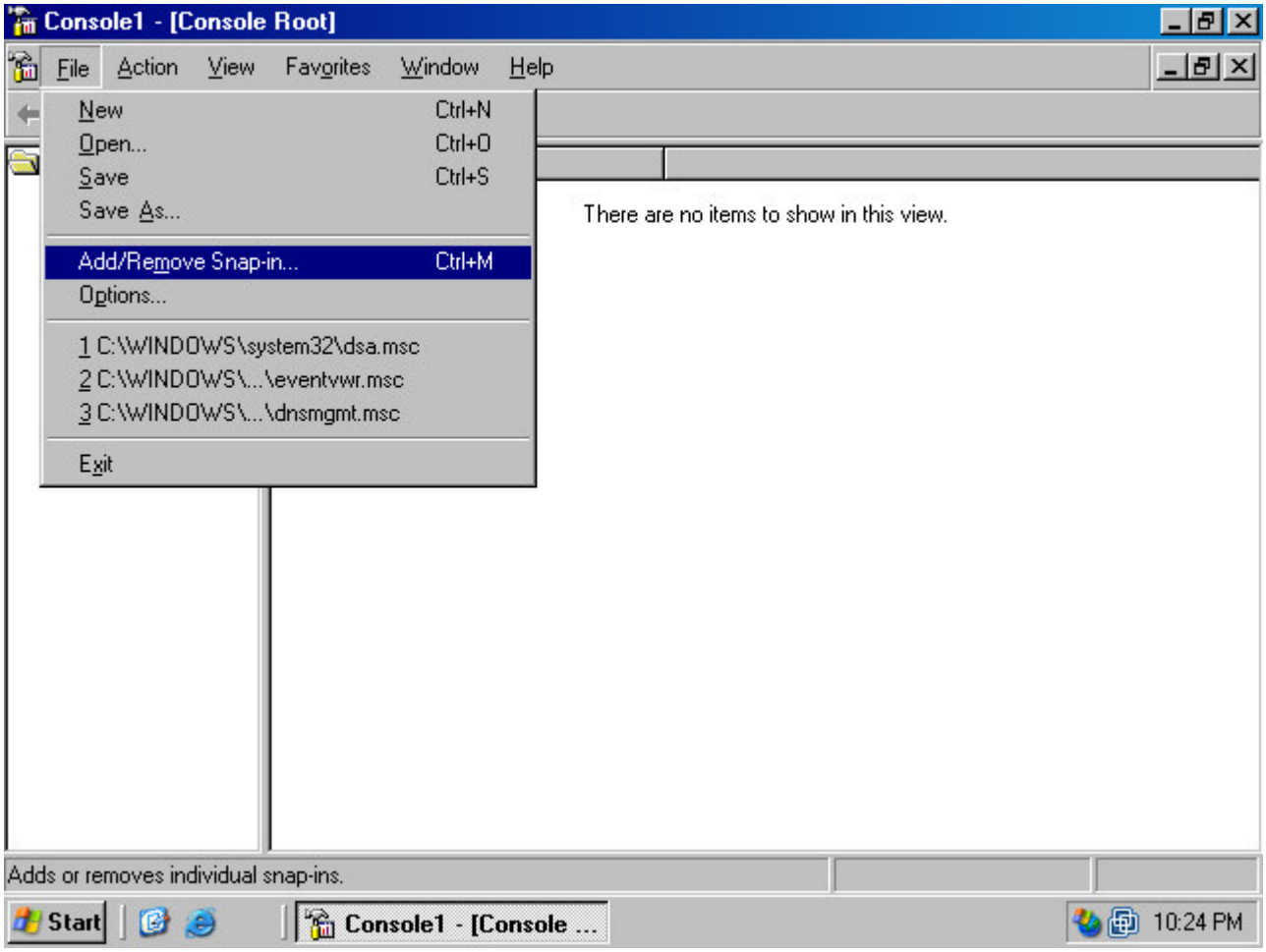
1. Click **Start** and click the **Run** command. Type **mmc** in the **Open** text box and click **OK** (figure 26).

Figure 26 (figure 127)



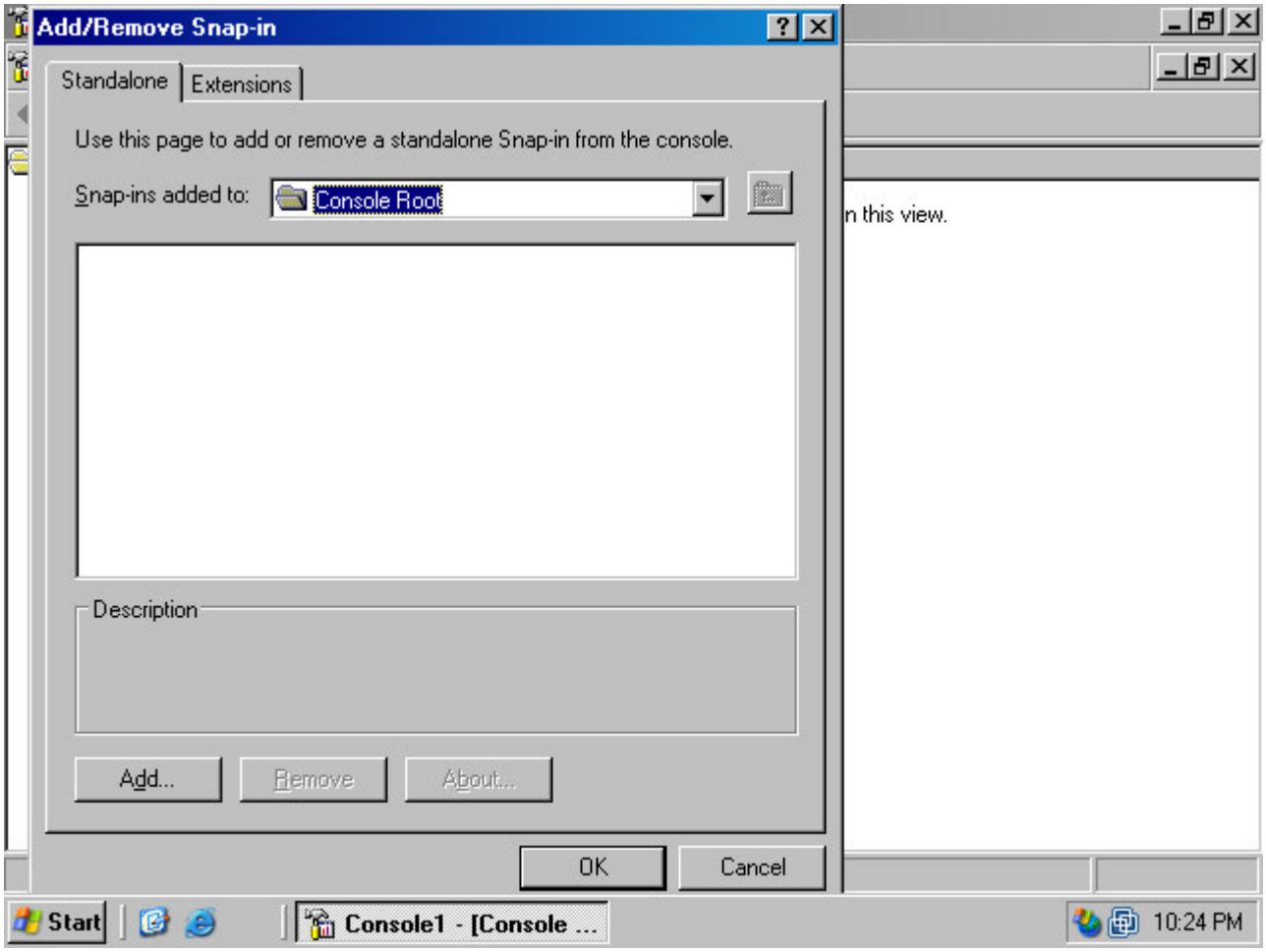
2. Click the **File** menu in the **Console1** window. Click the **Add/Remove Snap-in** command (figure 27).

Figure 27 (figure 128)



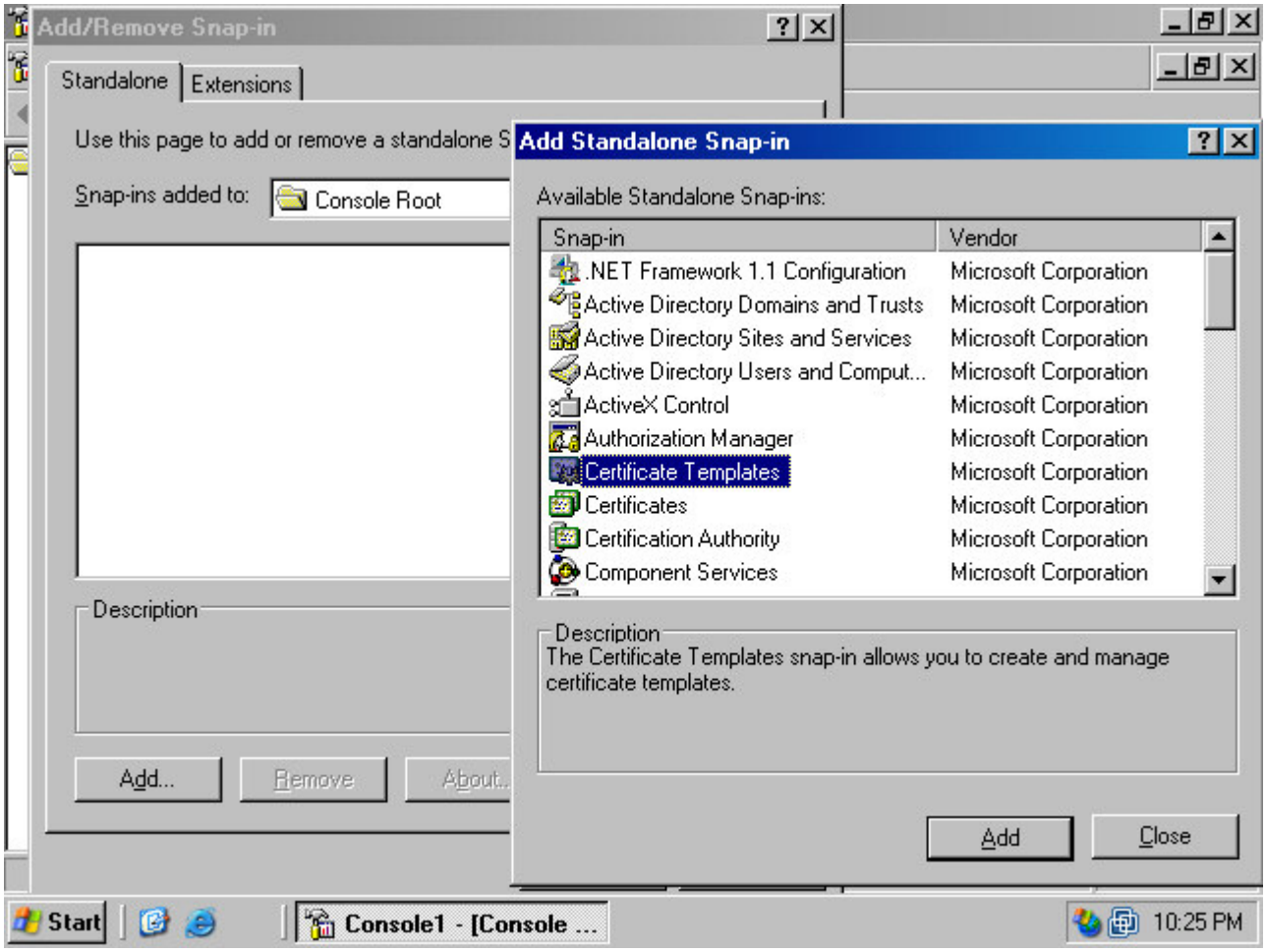
3. Click the **Add** button in the **Add/Remove Snap-in** dialog box (figure 28).

Figure 28 (figure 129)



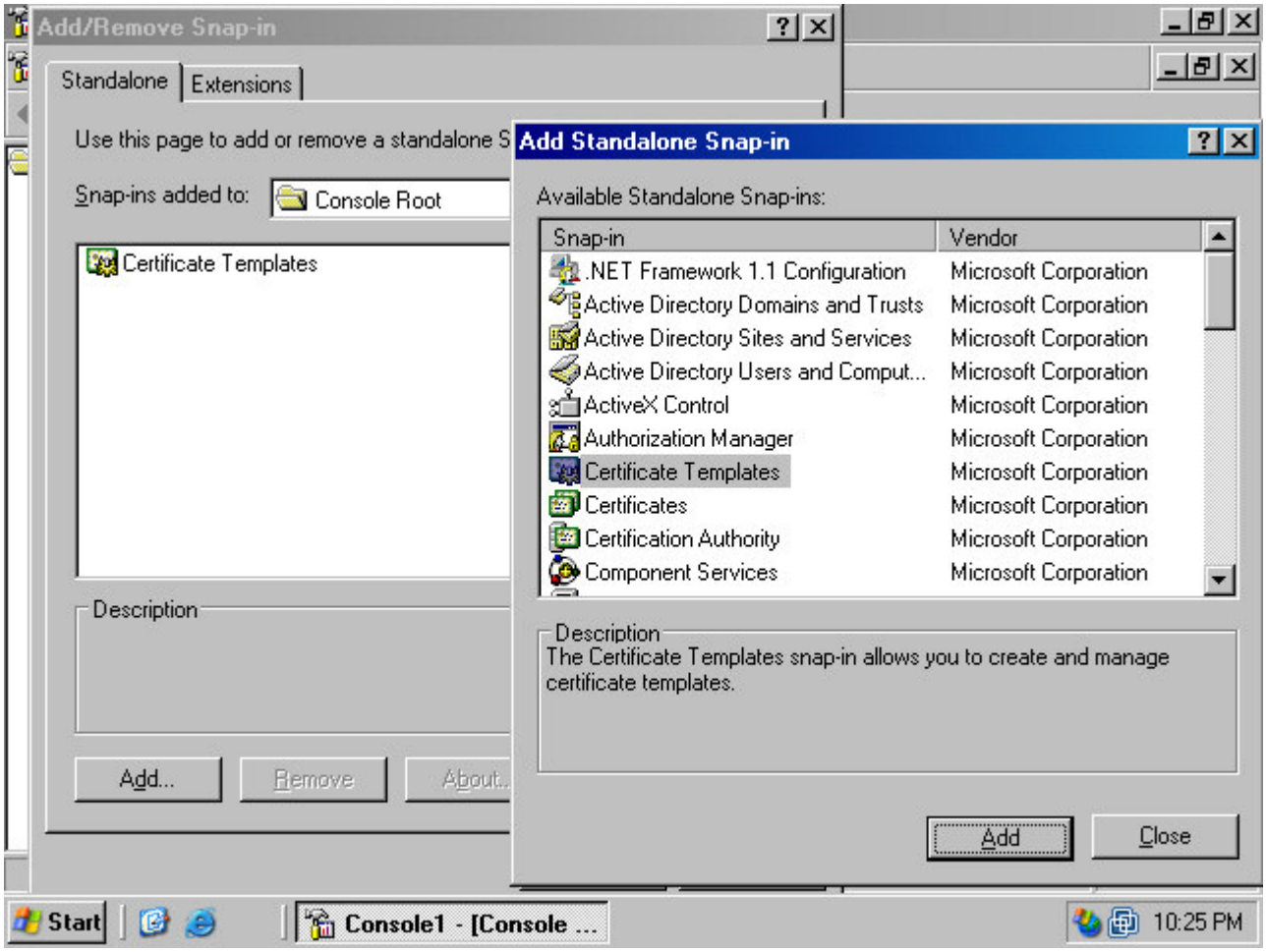
4. Select the **Certificate Template** entry in the list of the **Available Standalone Snap-ins** on the **Add Standalone Snap-in** dialog box. Click the **Add** button (figure 29).

Figure 29 (fig130)



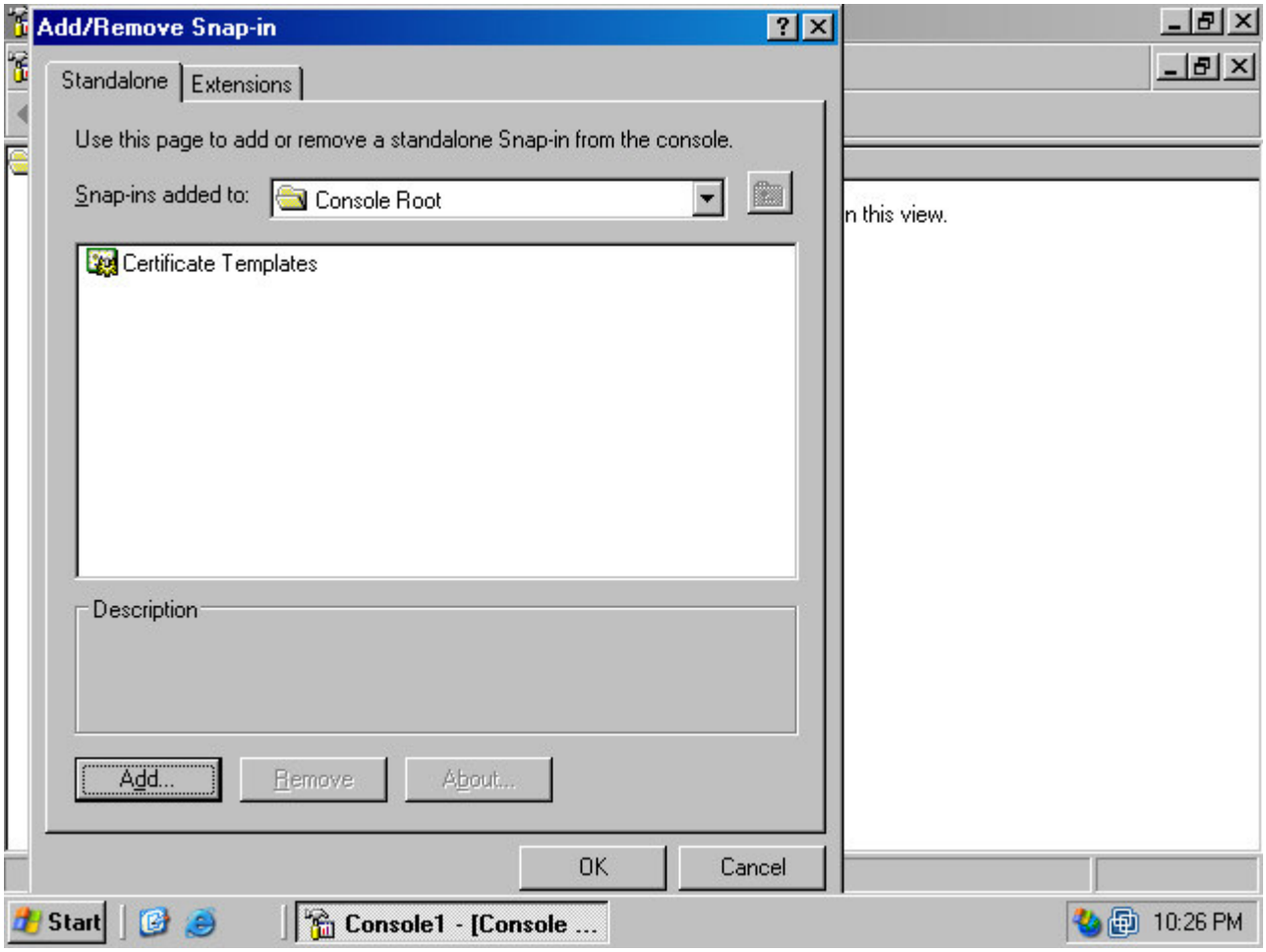
5. Notice that the **Certificate Templates** snap in appears in the **Add/Remove Snap-in** dialog box (on the left side of figure 30). Click **Close** on the **Add Standalone Snap-in** dialog box.

Figure 30 (fig131)



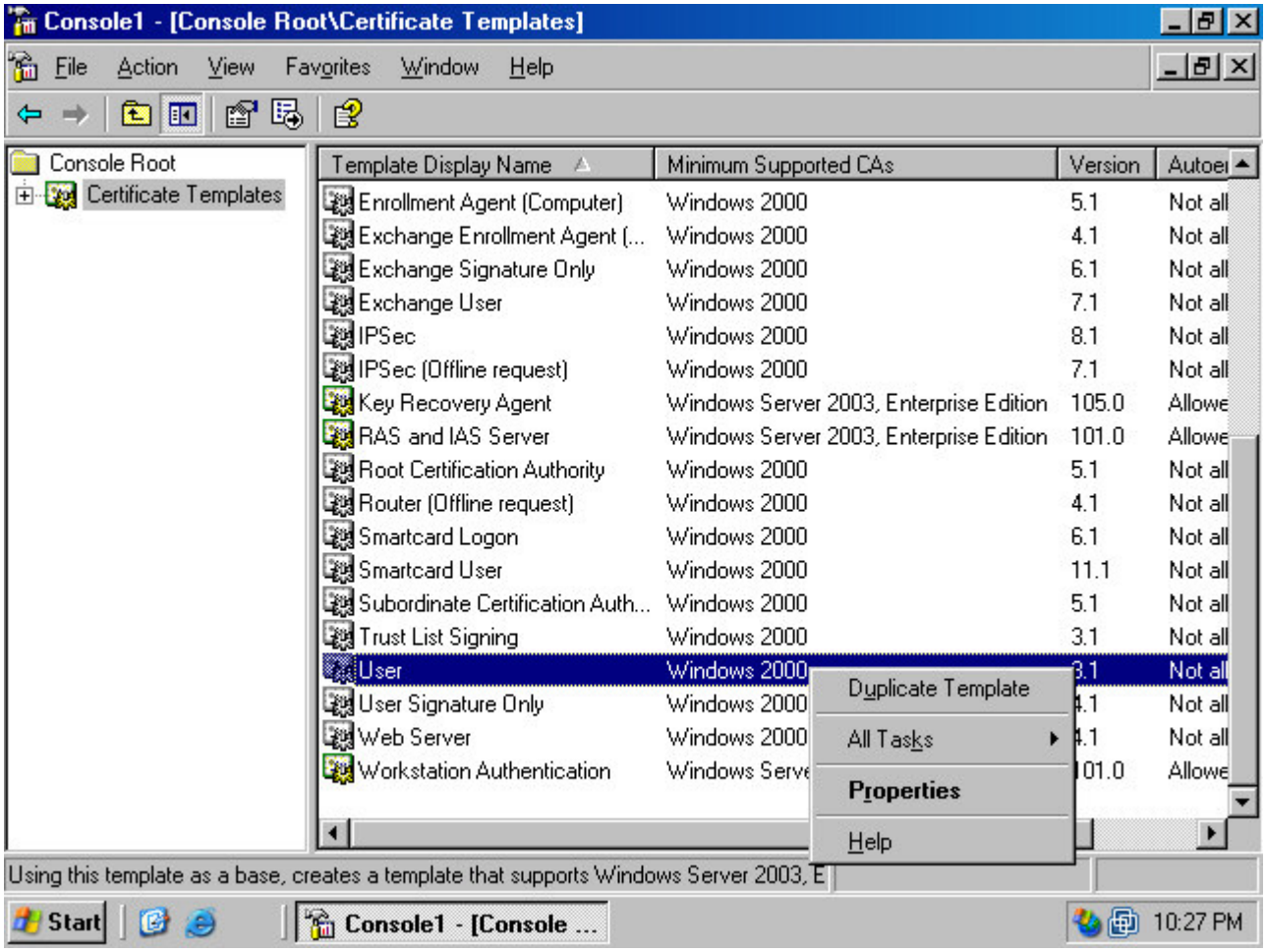
6. Click **OK** in the **Add/Remove Snap-in** dialog box (figure 31).

Figure 31 (fig132)



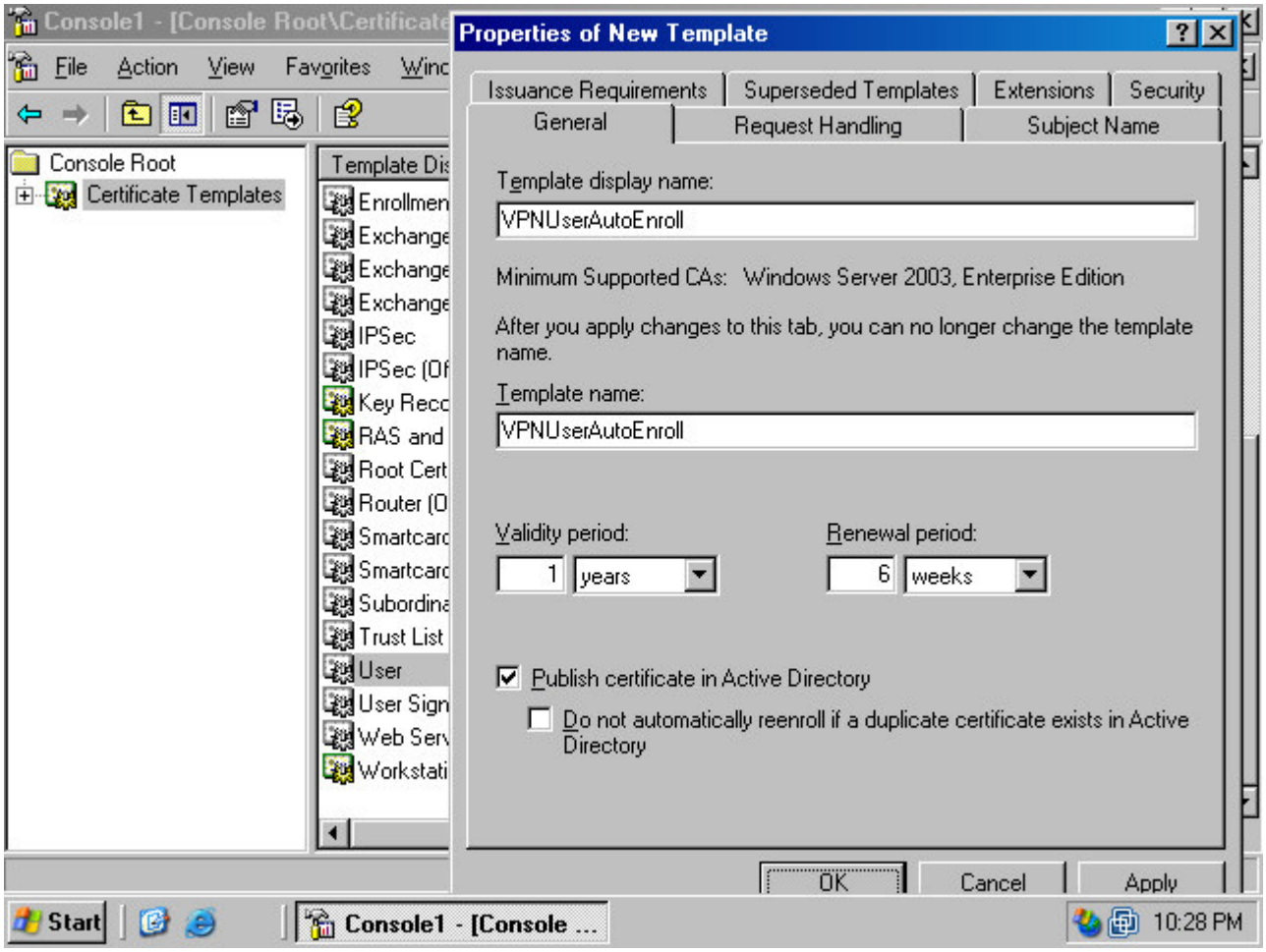
7. Click on the **Certificate Templates** node in the left pane of the console (figure 32). Right click on the **User** certificate template in the right pane of the console and click the **Duplicate Template** command.

Figure 32 (fig133)



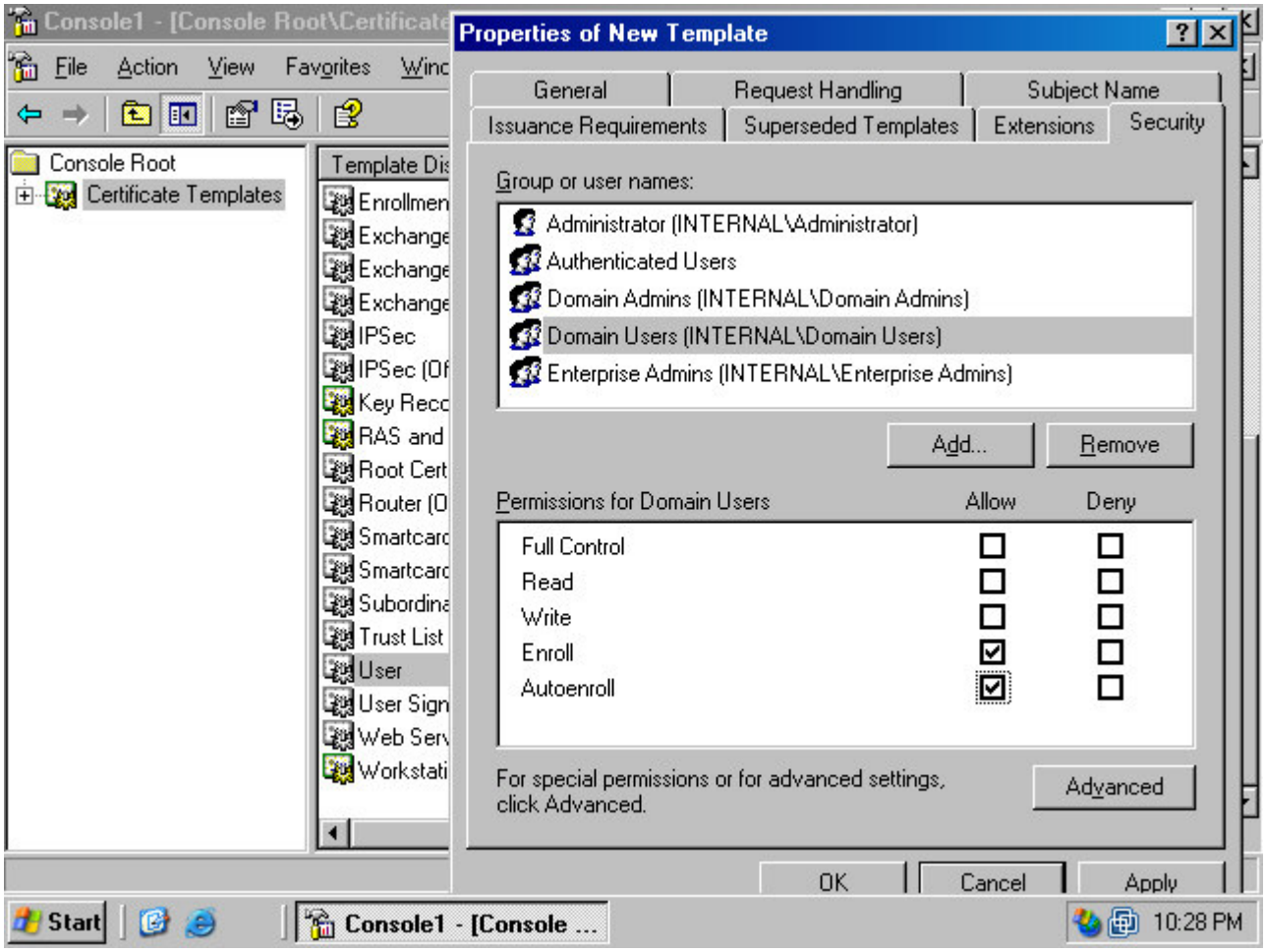
8. On the **Properties of the New Template** dialog box, click on the **General** tab. Type in a name for the new template in the **Template display name** text box. We suggest you use **VPNUserAutoEnroll** (figure 33).

Figure 33 (fig134)



9. Click on the **Security** tab in the **Properties of New Template** dialog box. Select the group you want to allow access to the template. In this example we will assign user certificates to all members of the **Domain Users** group. You may wish to be more selective and allow a specific group access to a user certificate via autoenrollment. If so, you must create a group for the VPN users and place the user accounts into that group. Then use the **Add** button (figure 35) to add the VPN users group permissions to autoenroll for user certificates. Enable both the **Enroll** and **Autoenroll Allow** checkboxes.

Figure 35 (fig135)



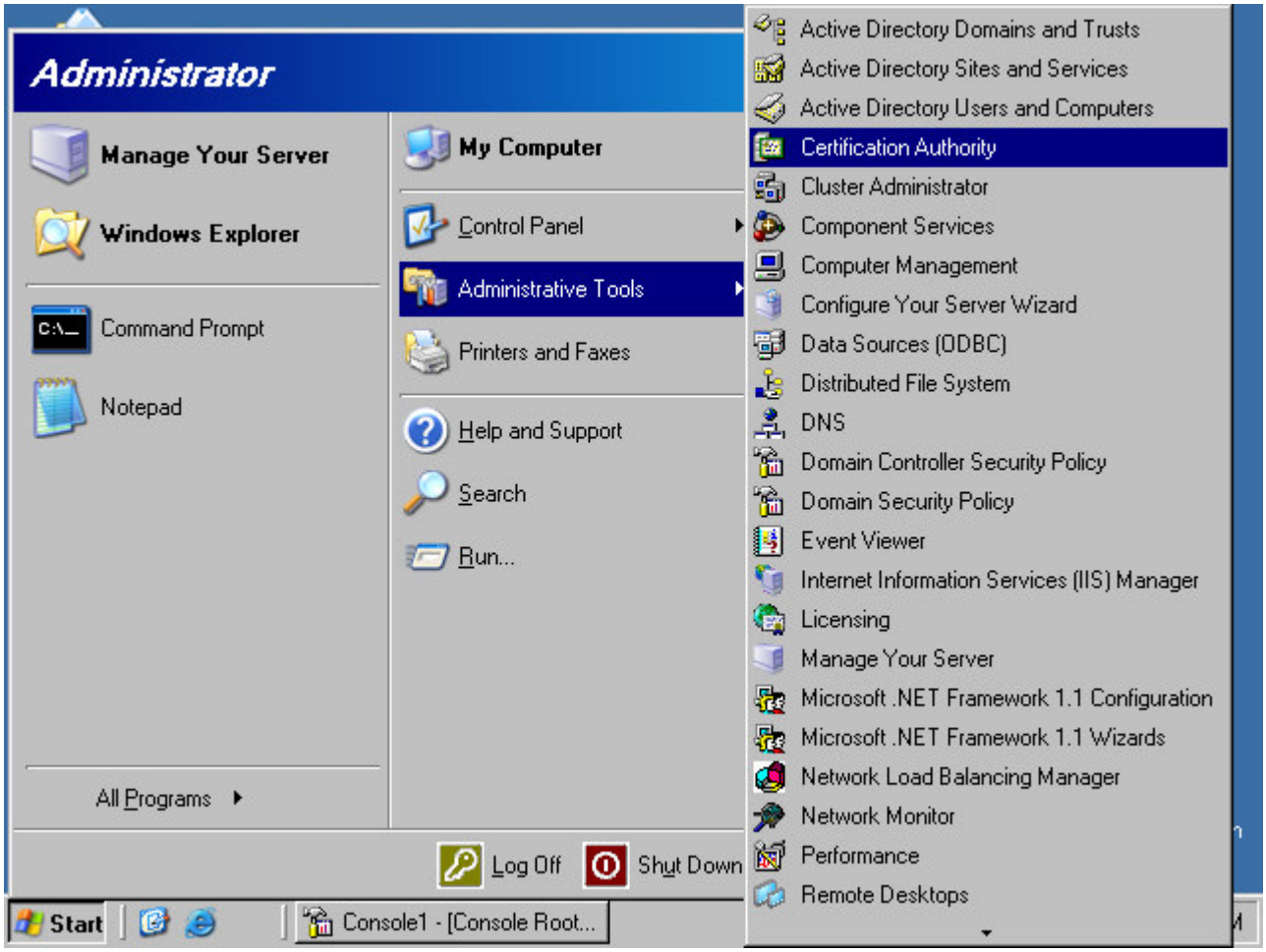
10. Click **Apply** and then click **OK** in the **Properties of New Template** dialog box.

Configuring the Enterprise CA to Assign Certificates Based on the New User Template

Perform the following steps to configure the enterprise CA to assign user certificates using the new template:

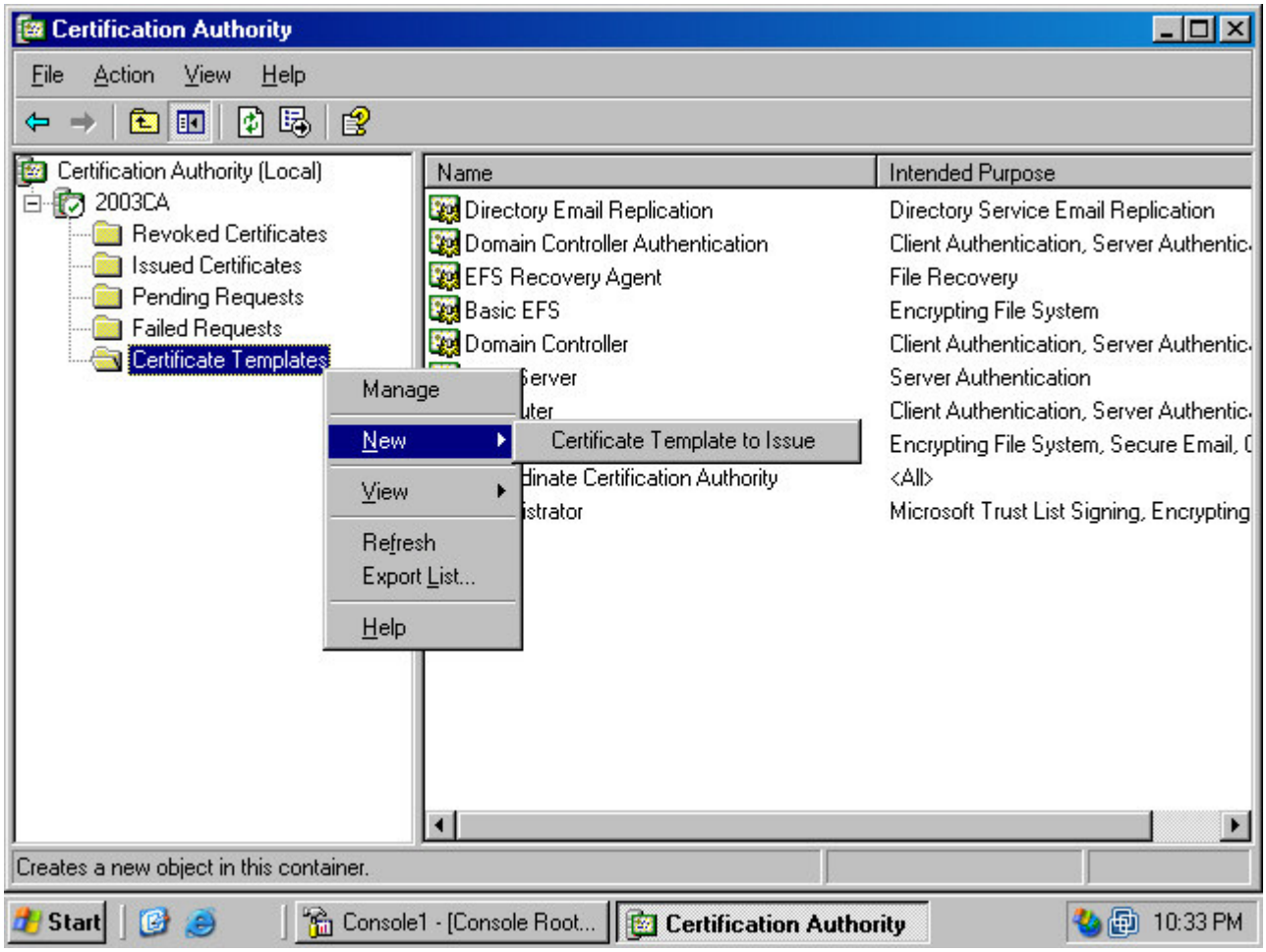
1. Click **Start** and point to **Administrative Tools**. Click on the **Certification Authority** command (figure 36).

Figure 36 (fig136)



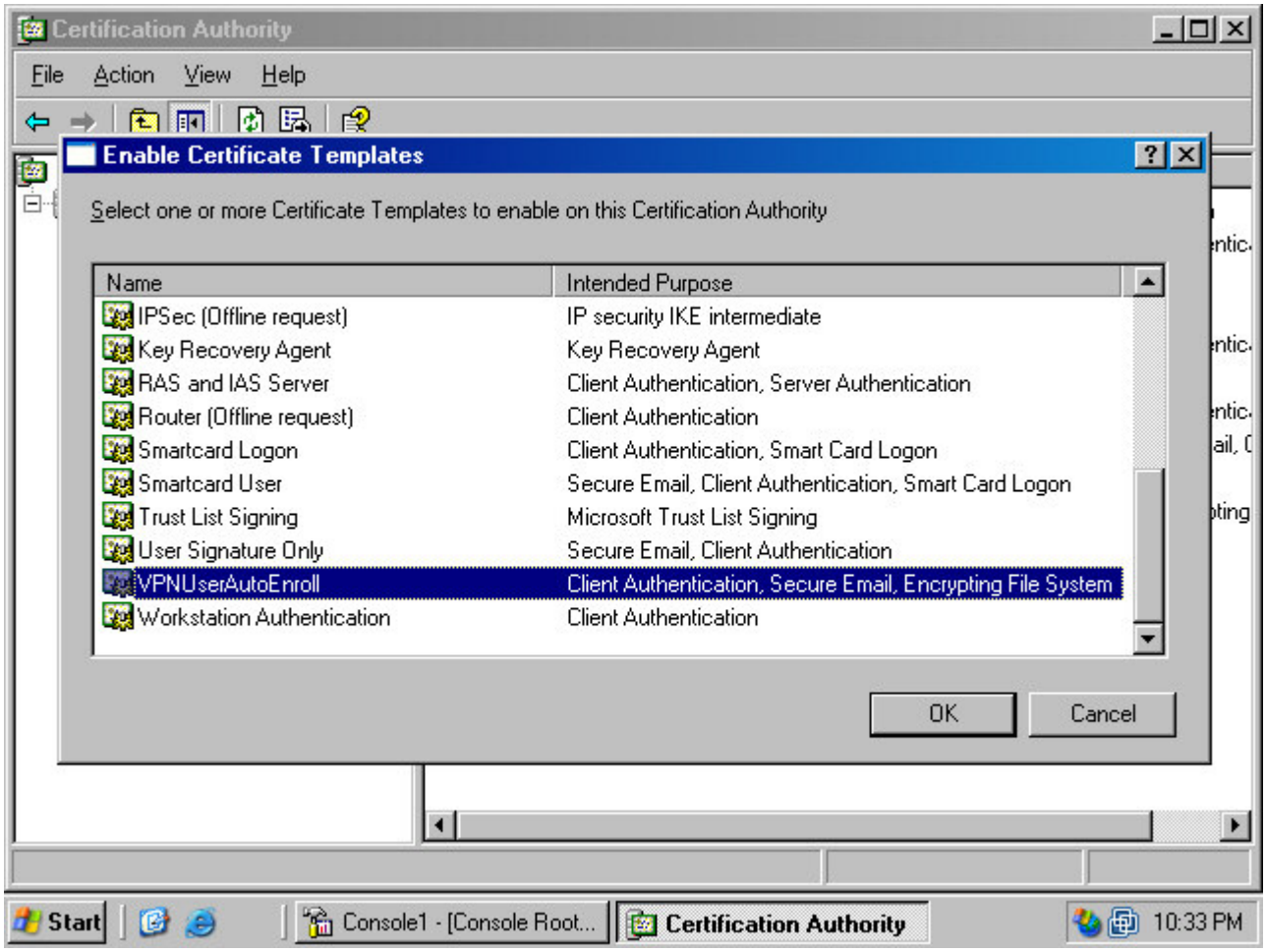
2. In the **Certification Authority** console (figure 37), select the **Certificate Templates** node in the left pane of the console, then right click on it. Point to **New** and click the **Certificate Template to Issue** command.

Figure 37 (fig137)



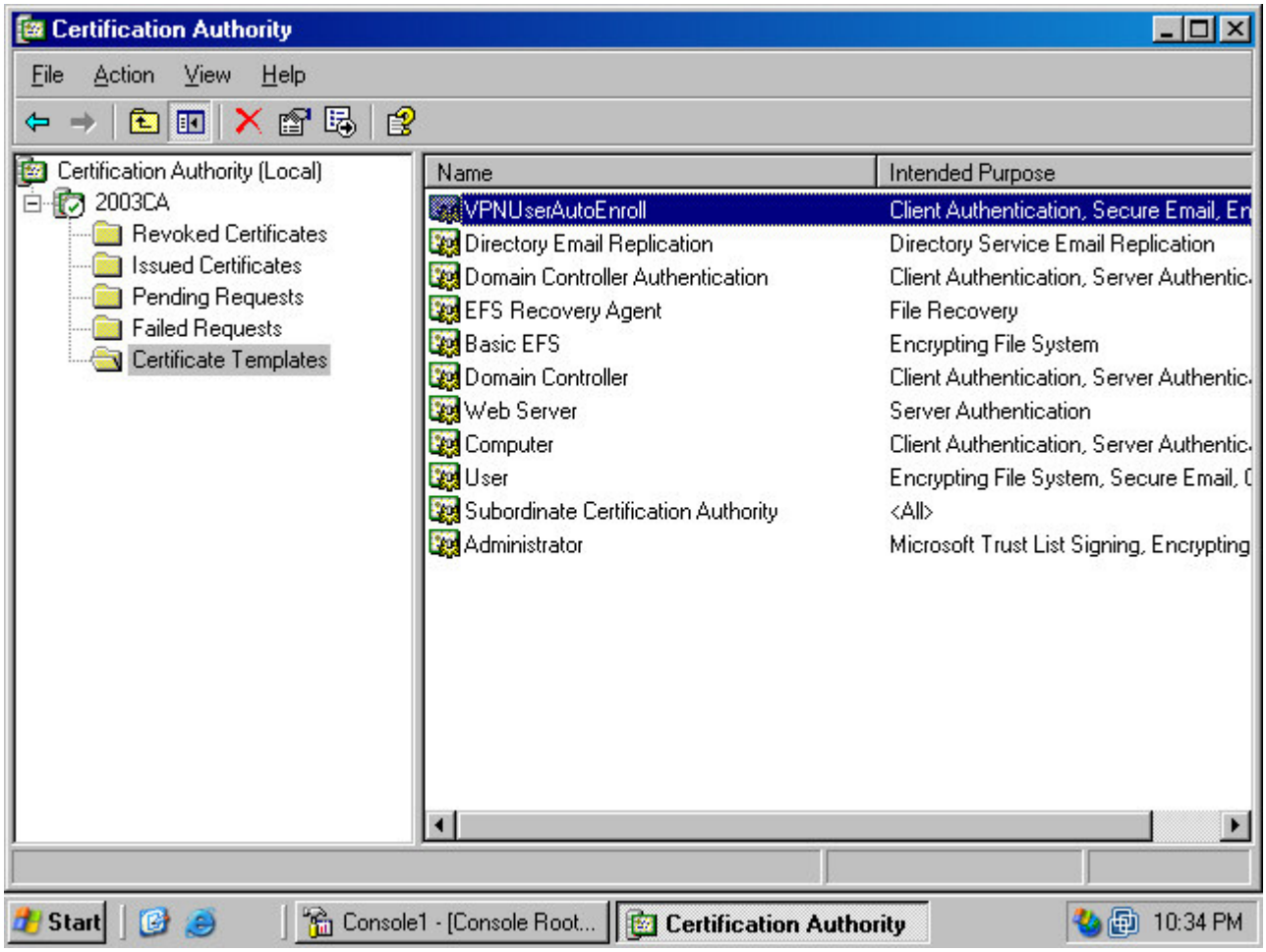
3. Select the **VPNUserAutoEnroll** entry in the **Enable Certificate Templates** dialog box (figure 38). Click **OK**.

Figure 38 (fig138)



4. The **VPNUserAutoEnroll** certificate template appears in the right pane of the **Certification Authority** console (figure 39).

Figure 39 (fig139)



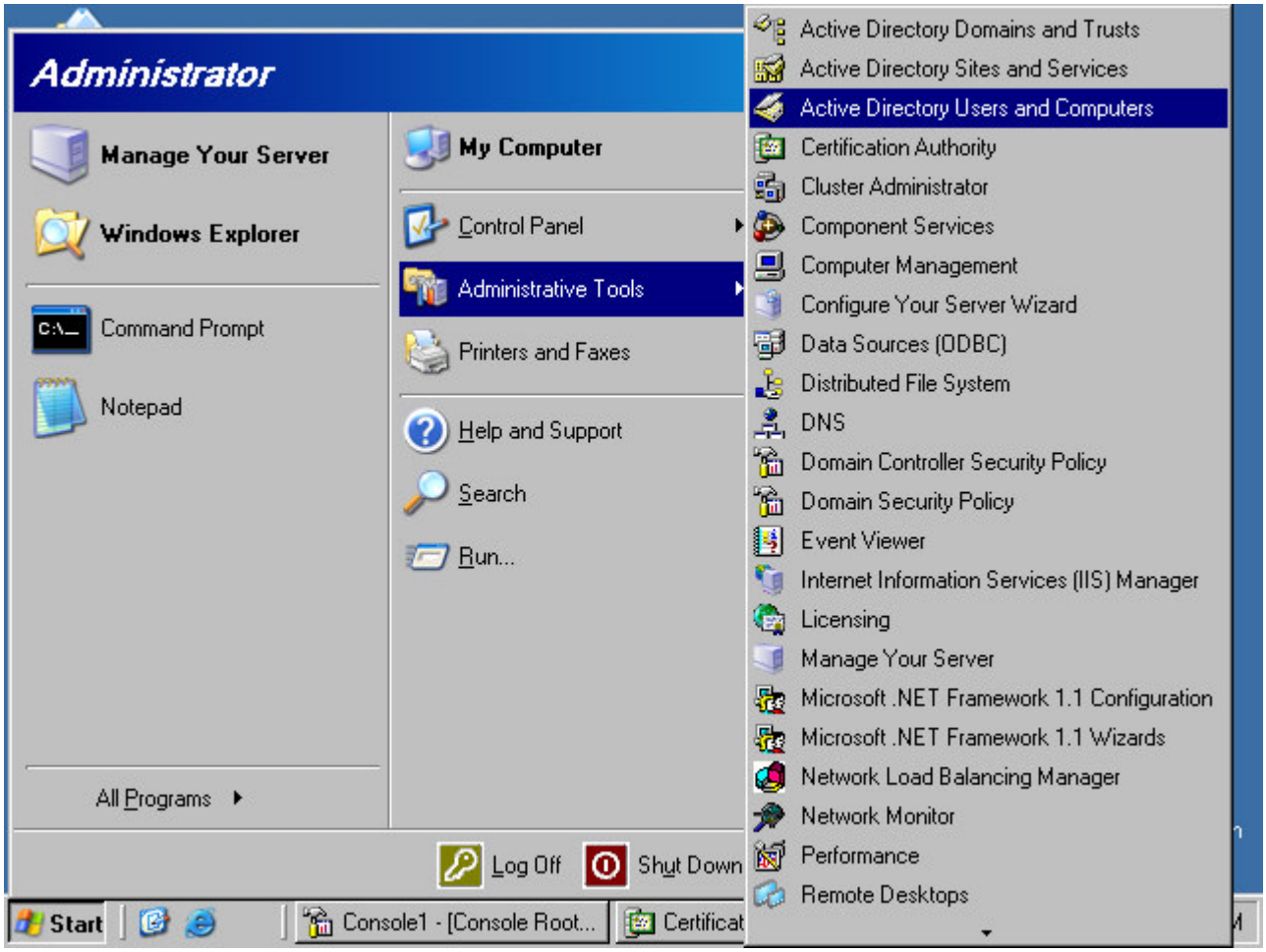
5. Close the **Certification Authority** console.

Configuring Autoenrollment via Group Policy

Perform the following steps to configure autoenrollment in Group Policy:

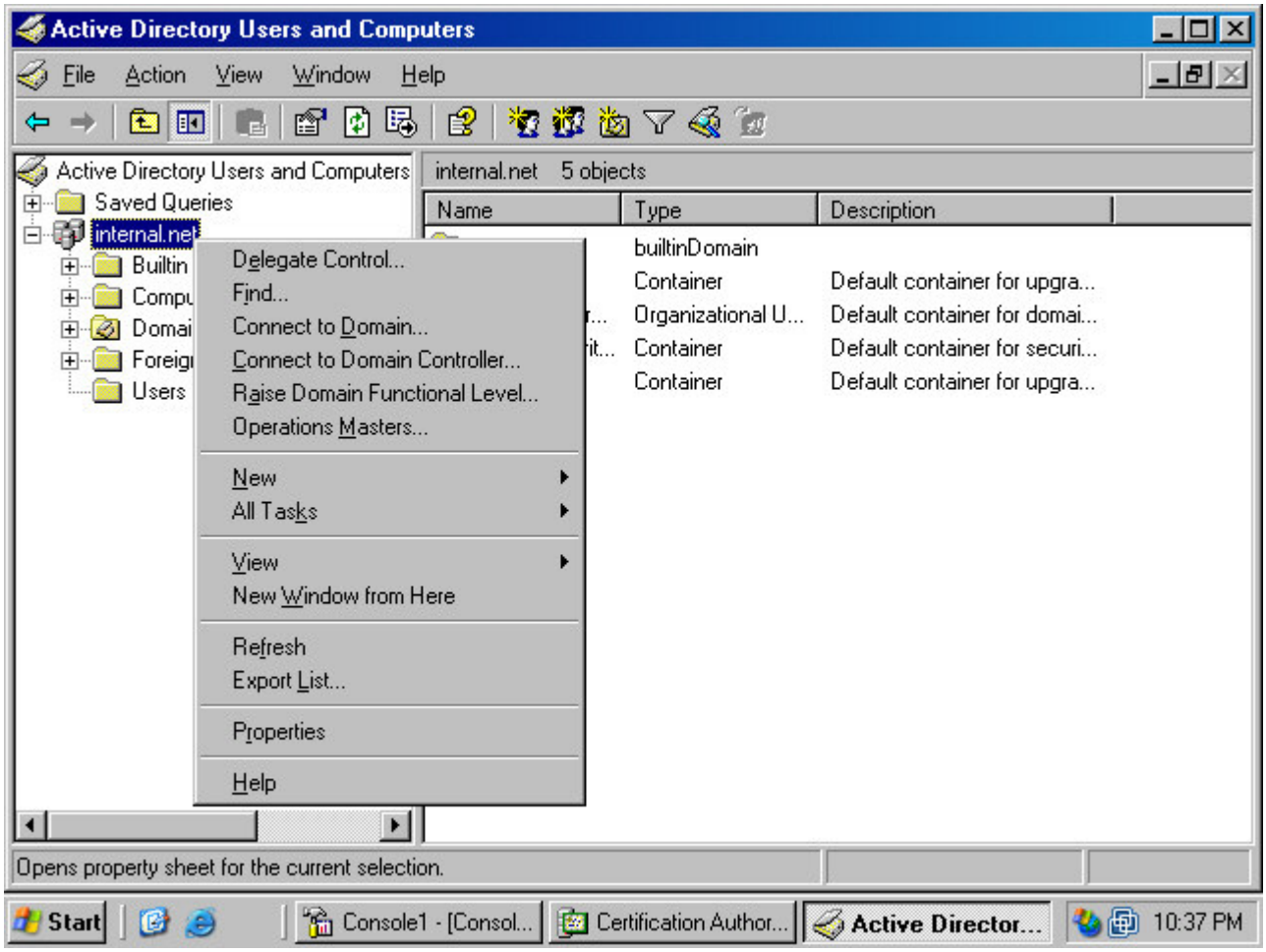
1. Click **Start** and point to **Administrative Tools**. Click on **Active Directory Users and Computers** (figure 40).

Figure 40 (fig140)



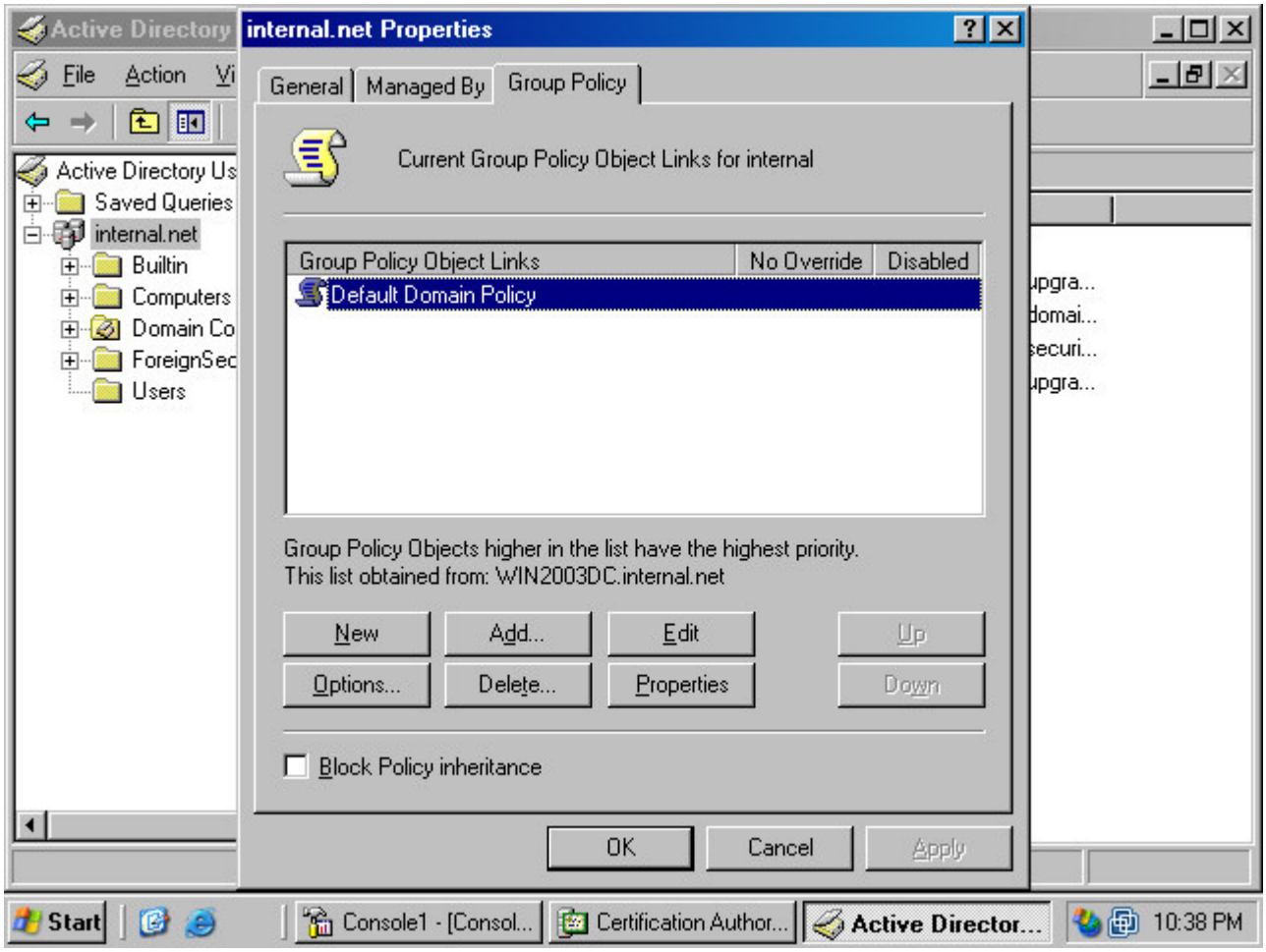
2. In the **Active Directory Users and Computers** console, right click on your domain name and click on the **Properties** command (figure 41).

Figure 41 (fig141)



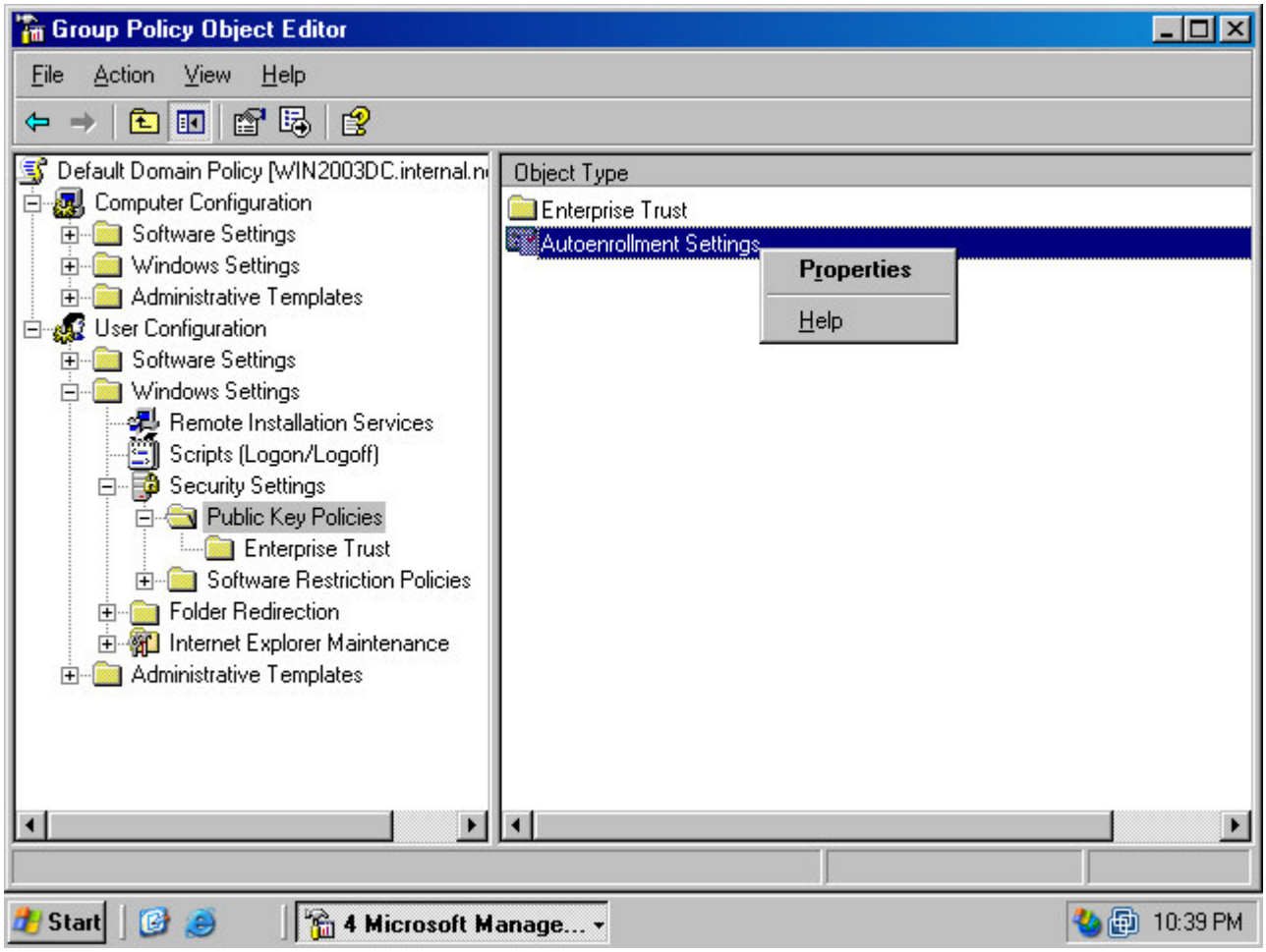
3. In the domain **Properties** dialog box, click on the **Group Policy** tab. On the **Group Policy** tab, click on the **Default Domain Policy** entry and click the **Edit** button (figure 42).

Figure 42 (fig142)



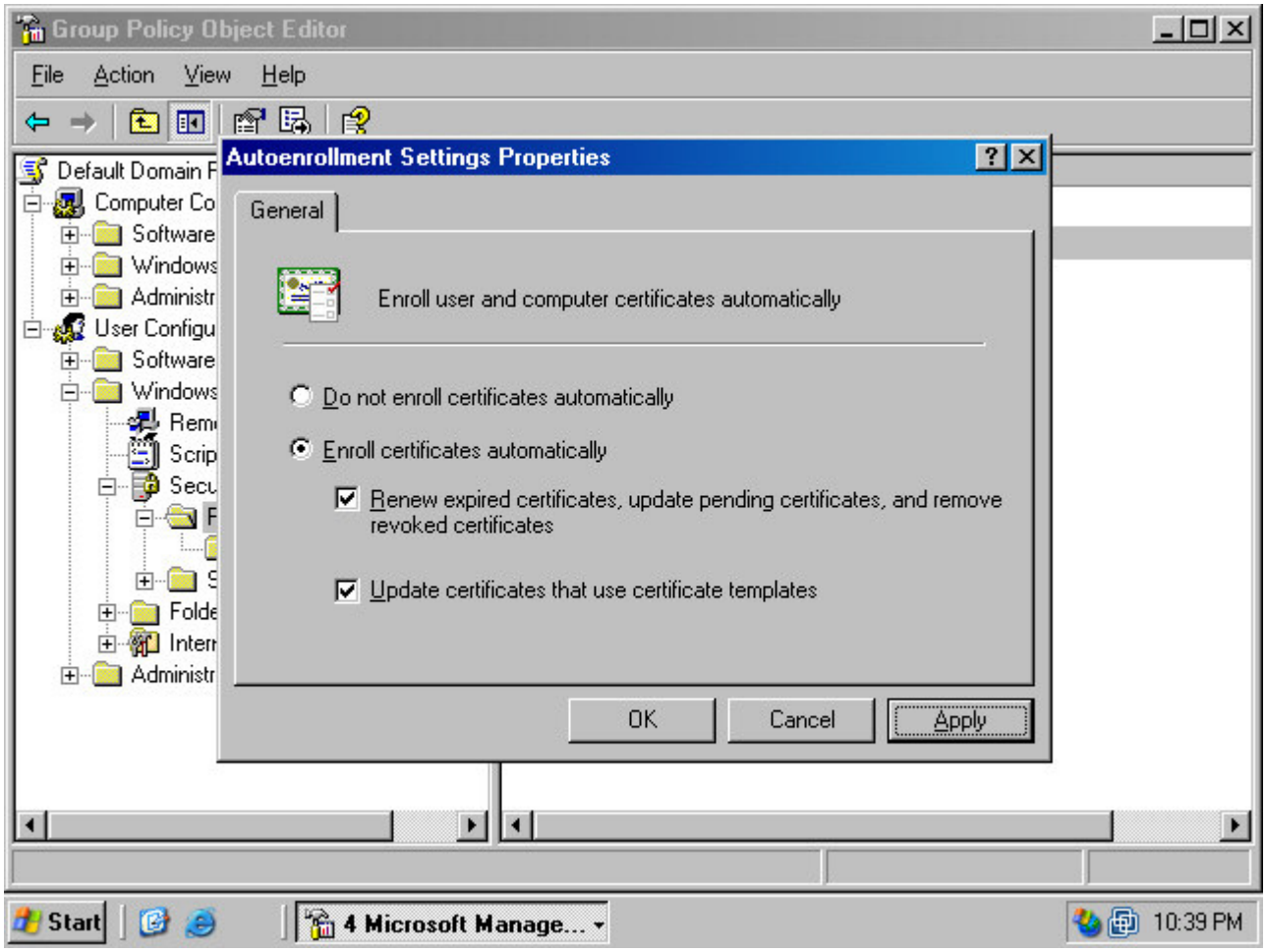
4. In the **Group Policy Object Editor** window, click on the **User Configuration\Windows Settings\Security Settings\Public Key Policies** node in the left pane of the console. Right click on the **Autoenrollment Settings** entry in the right pane of the console and click the **Properties** command (figure 43).

Figure 43 (fig143)



5. In the **Autoenrollment Settings Properties** dialog box (figure 44), select the **Enroll certificates automatically** option. Put a checkmark in the **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates** checkboxes.

Figure 44 (fig144)



Windows XP and Windows Server 2003 users will now automatically receive user certificates when they log onto the domain. These user certificates can be used as log on credentials by PPTP and L2TP/IPSec clients. Please refer to ISA Server 2000 VPN Deployment Kit document **Configuring the VPN Client and Server to Support Certificate-Based PPTP EAP-TLS Authentication**

****

Thank for choosing PLANET Products.

Best Regards,

PLANET Tech SupportTeam