

# **Deploying the VueCentric Updater Service and EHR Shortcut Using Group Policy**



**Adam Searcy  
Doug Martin  
Medsphere Systems Corporation  
2/6/2008**

**Background:**

The RPMS-EHR utilizes a repository-based update mechanism for deploying updated components to each client workstation. While this technique works well, it requires each user to possess a minimum set of permissions in order to successfully download and install each update. This set of permissions is typically embodied in the "Power User" group where members have write access to the HKEY\_CLASSES\_ROOT hive of the Windows Registry and write access to the local Program Files folder. IHS corporate policy now dictates that users have more limited permissions in an effort to preserve network security and workstation integrity. Enforcement of this policy renders the current update mechanism inoperable. As a consequence, a different mechanism had to be devised to address this problem.

The VueCentric Updater Service allows the RPMS-EHR to continue to employ a repository-based update mechanism, while eliminating the need to modify individual user permissions to allow updates to occur. This application runs in the background on each workstation under a specially created account that has all the necessary permissions to perform a successful update. The service performs all update operations on behalf of the RPMS-EHR. This process is completely transparent to the RPMS-EHR user.

**Summary:**

This document describes in detail techniques for the centralized deployment of the VueCentric Updater Service to client workstations using Group Policy. This document also shows how these same techniques can be applied in the deployment of the EHR Shortcut to the client desktop.

Note: where version numbers occur in file names, this document uses the generic notation "x.y".

**Target Audience:**

This document is intended for use by domain administrators.

**Required Elements:**

1. RPMS-EHR Patch 4
2. Orca msi Editor
3. Active Directory Users and Computers
4. Group Policy Management Console
5. Computer Management Utility

**Known Values:**

1. vcUpdaterService\_Silent\_x.y.msi and EHR\_Shortcut\_Silent\_x.y.msi (these are specially designed for unattended installation)
2. Domain Admin username and password
3. Active Directory Domain(s) or OU(s) to which the msi files will be deployed.
4. UNC path to the RPMS-EHR bin directory
5. UNC path to the msi file distribution point.

**Outline:**

- I. Install Orca
- II. Deploy the VueCentric Updater Service
  - A. Create a domain admin account for use with VueCentric Updater Service
  - B. Modify the vcUpdaterService\_Silent\_x.y.msi Properties Table using Orca
    - 1) Add line for USERNAME

- 2) Add line for PASSWORD
  - C. Deploy the vcUpdaterService\_Silent\_x.y.msi via Group Policy
  - D. Verify vcUpdaterService\_Silent\_x.y.msi deployment on Client
- III. Deploy the EHR Shortcut (optional)
- A. Modify the EHR\_Shortcut\_Silent\_x.y.msi Properties Table using Orca
    - 1) Add line for REPOSITORYPATH
  - B) Deploy the EHR\_Shortcut\_Silent\_x.y.msi via Group Policy
  - C) Verify EHR\_Shortcut\_Silent\_x.y.msi deployment on Client

**Assumptions:**

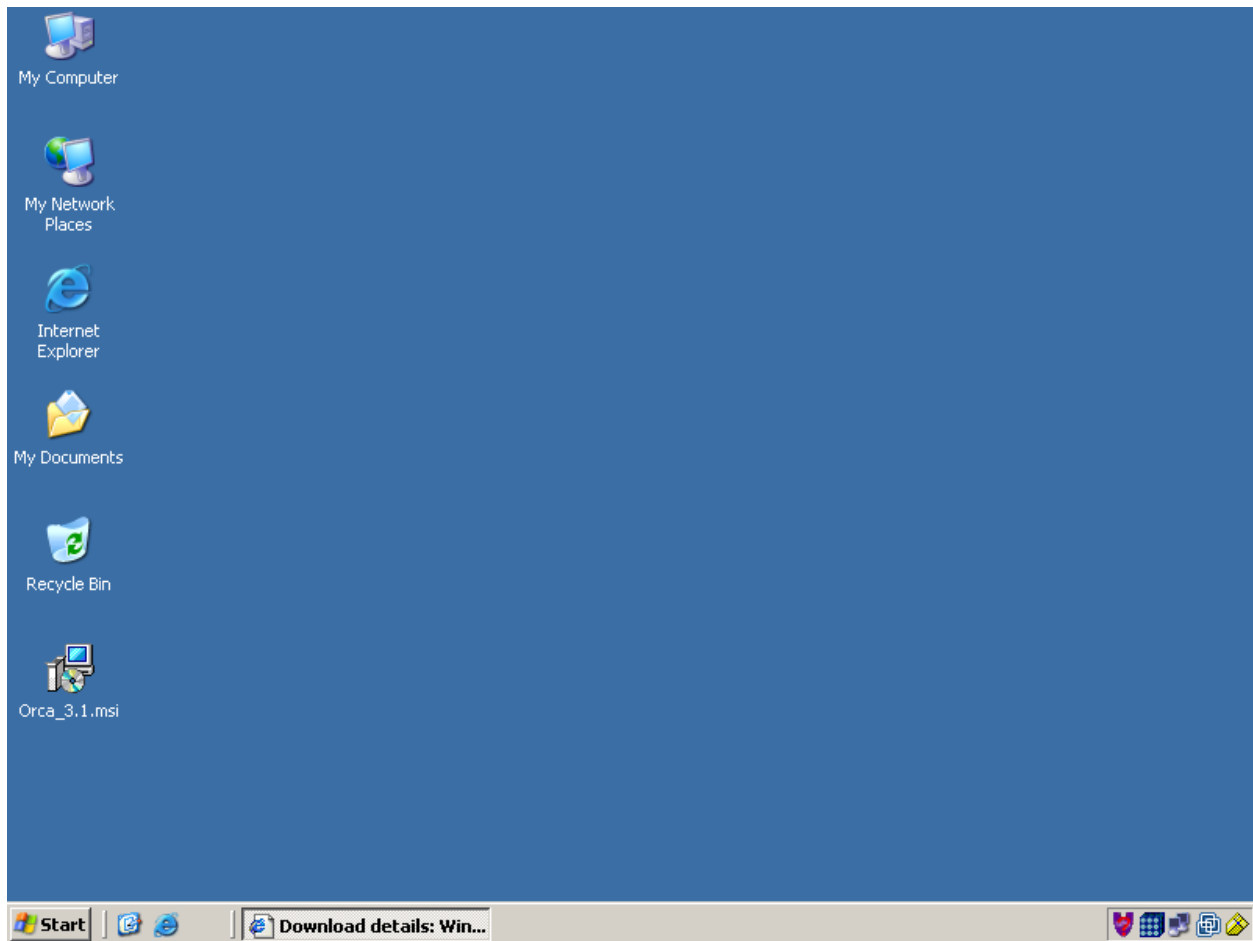
This document assumes Windows 2003 Server Edition is running as the domain controller. Adjustments may need to be made to the procedures for other operating system versions.

This document further assumes that the Group Policy Management Console has been installed and is available to the domain administrator. If this application is not available, it may be downloaded from:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&displaylang=en>

## I. Install Orca

Orca is a tool distributed with the Microsoft Platform SDK that can be used to edit Microsoft Installer (“msi”) files. In order for an msi file to be deployed via group policy, all required inputs must be imbedded within it. Orca allows the insertion of required property values into the msi so that unattended deployment can occur. Orca is provided as an msi file that may be installed on the domain administrator’s workstation.

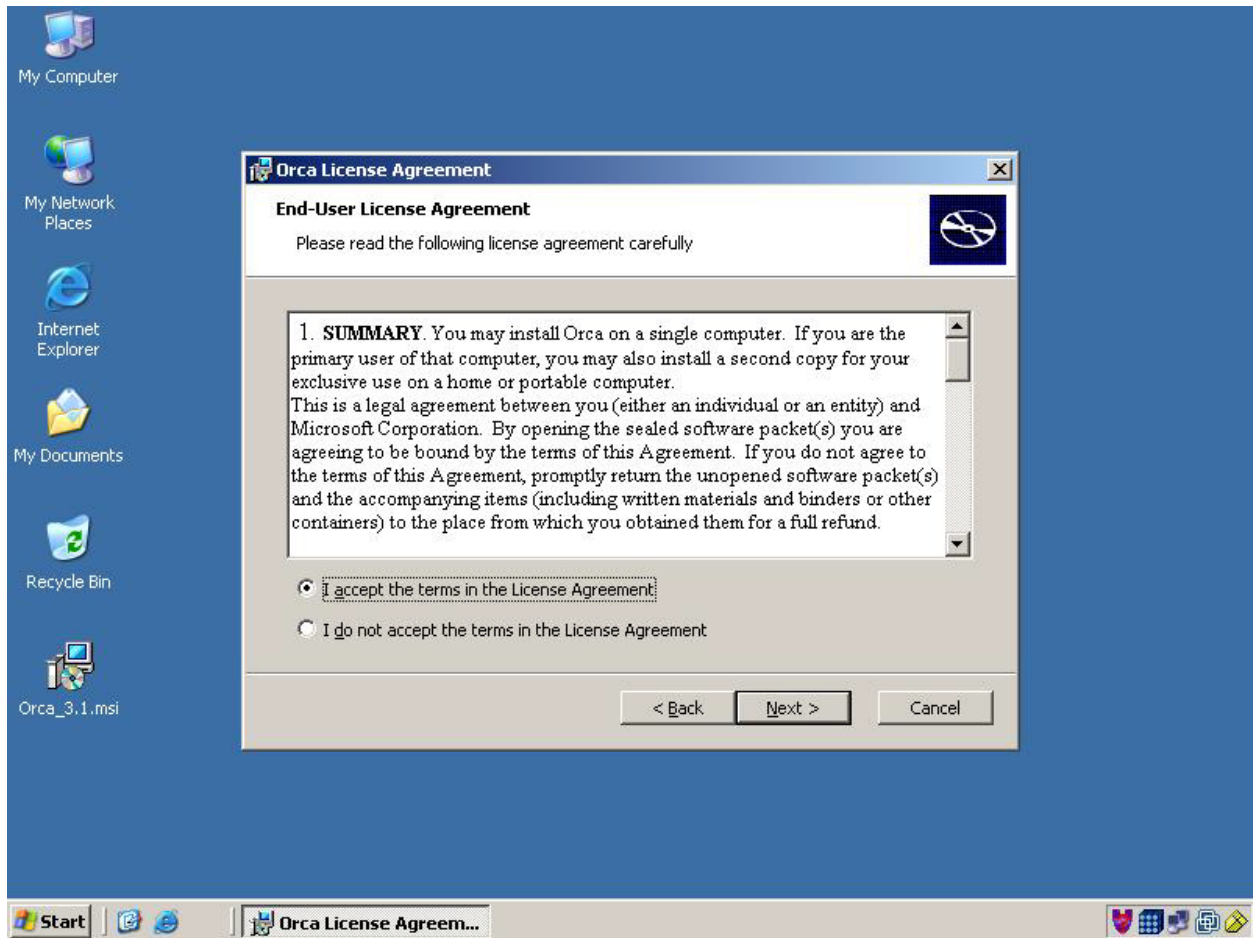


1. Save Orca locally and execute it by double-clicking on its icon.

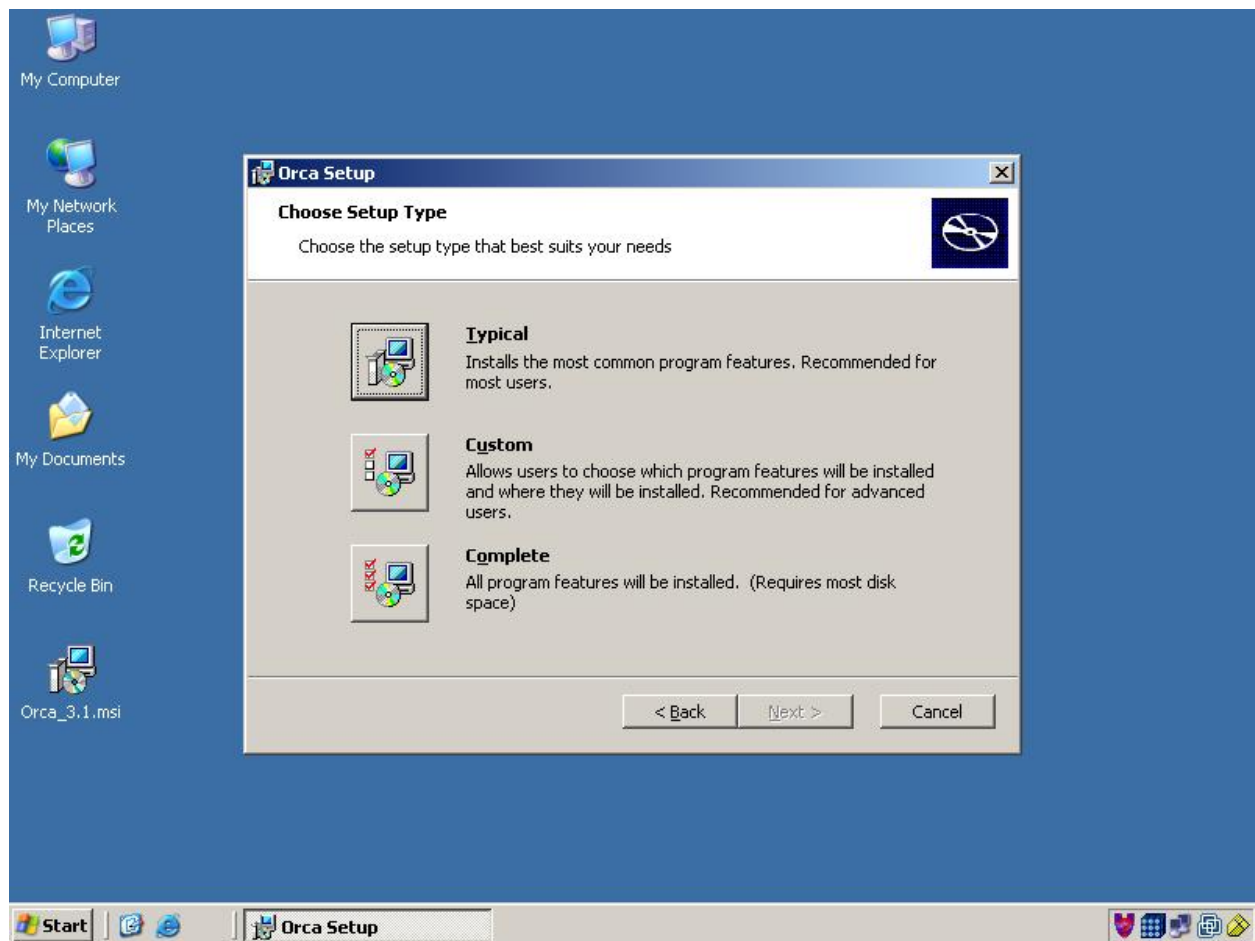




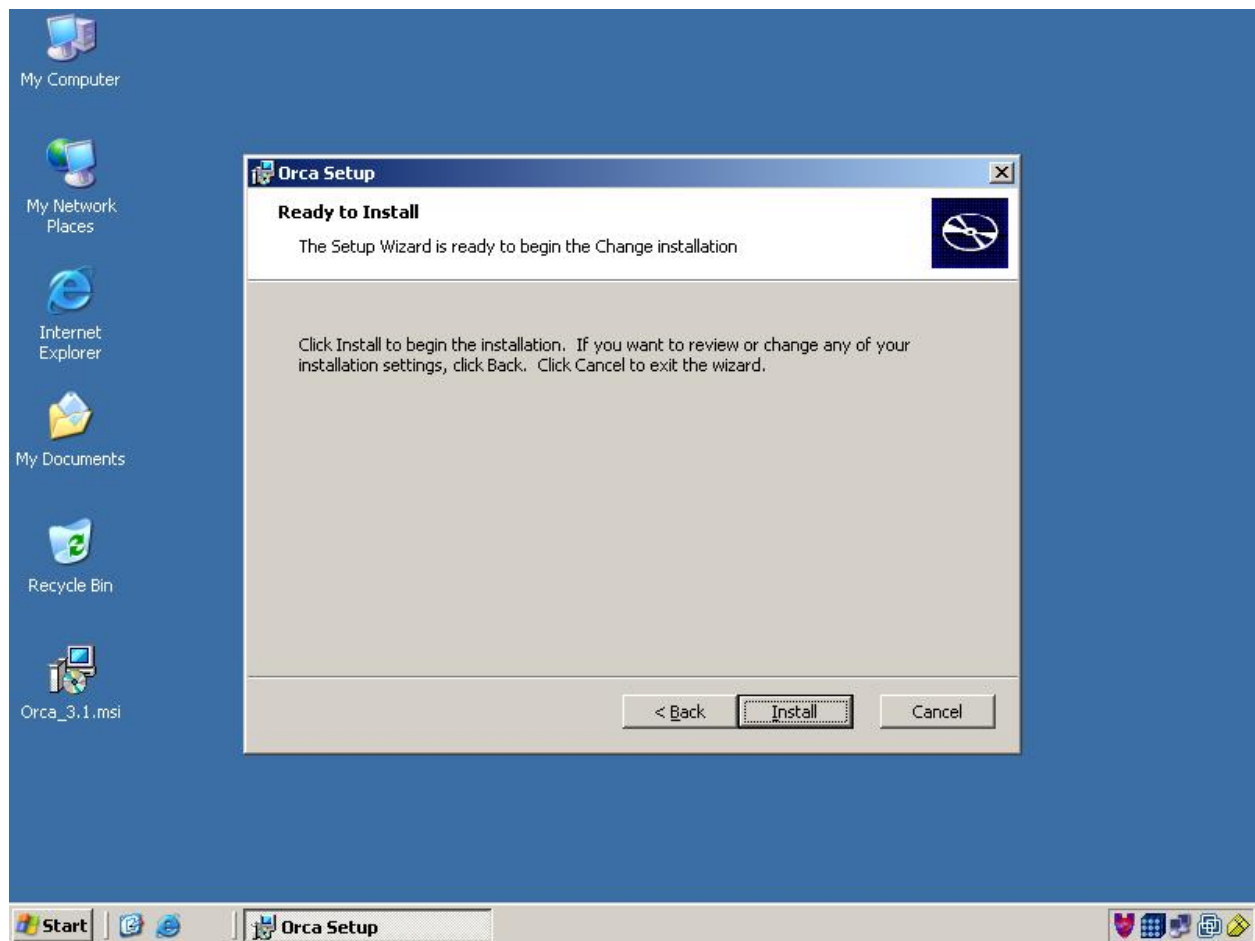
2. Click "Next".



3. Select "I accept..." and click next.



4. Click "Typical".



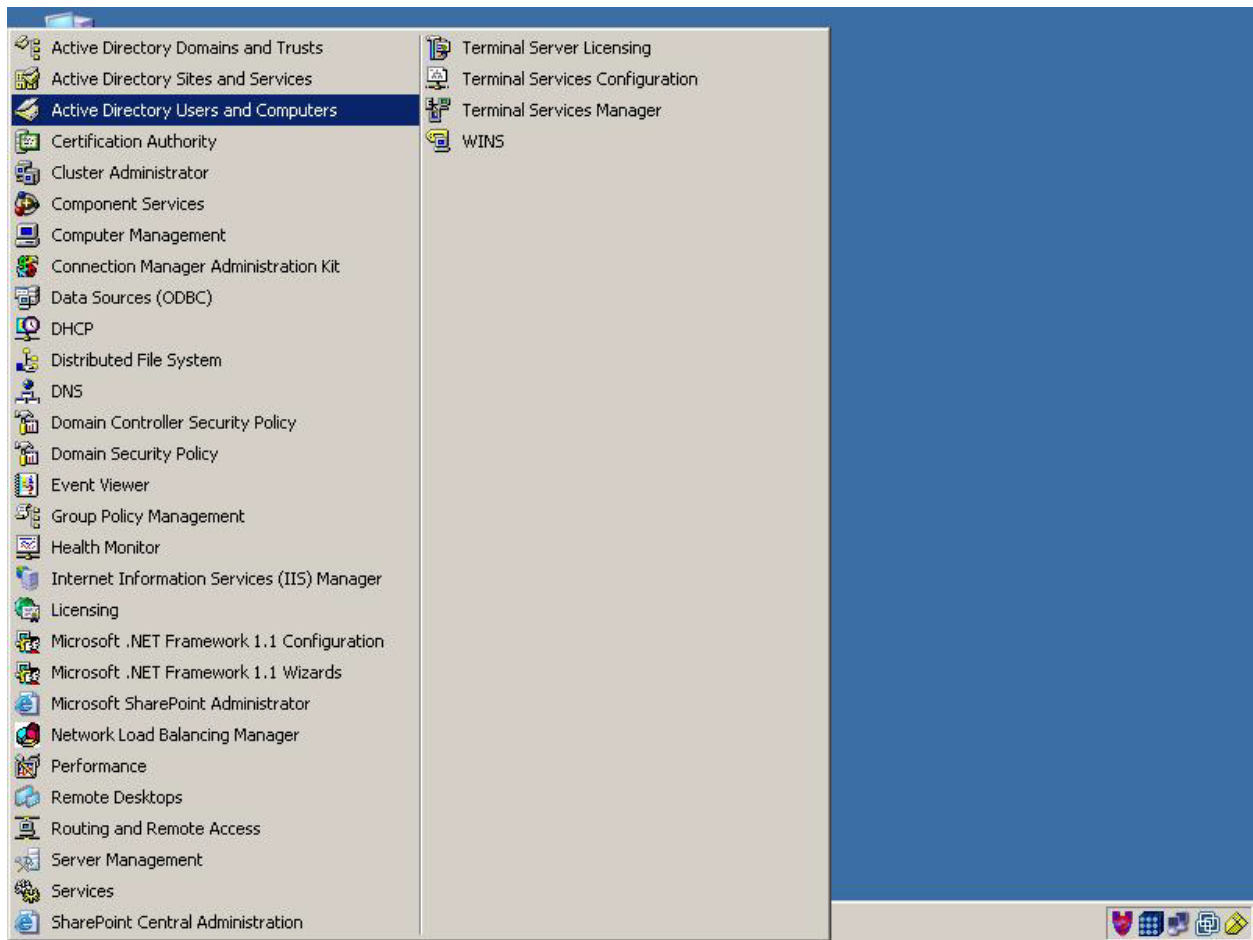
5. Click "Install".



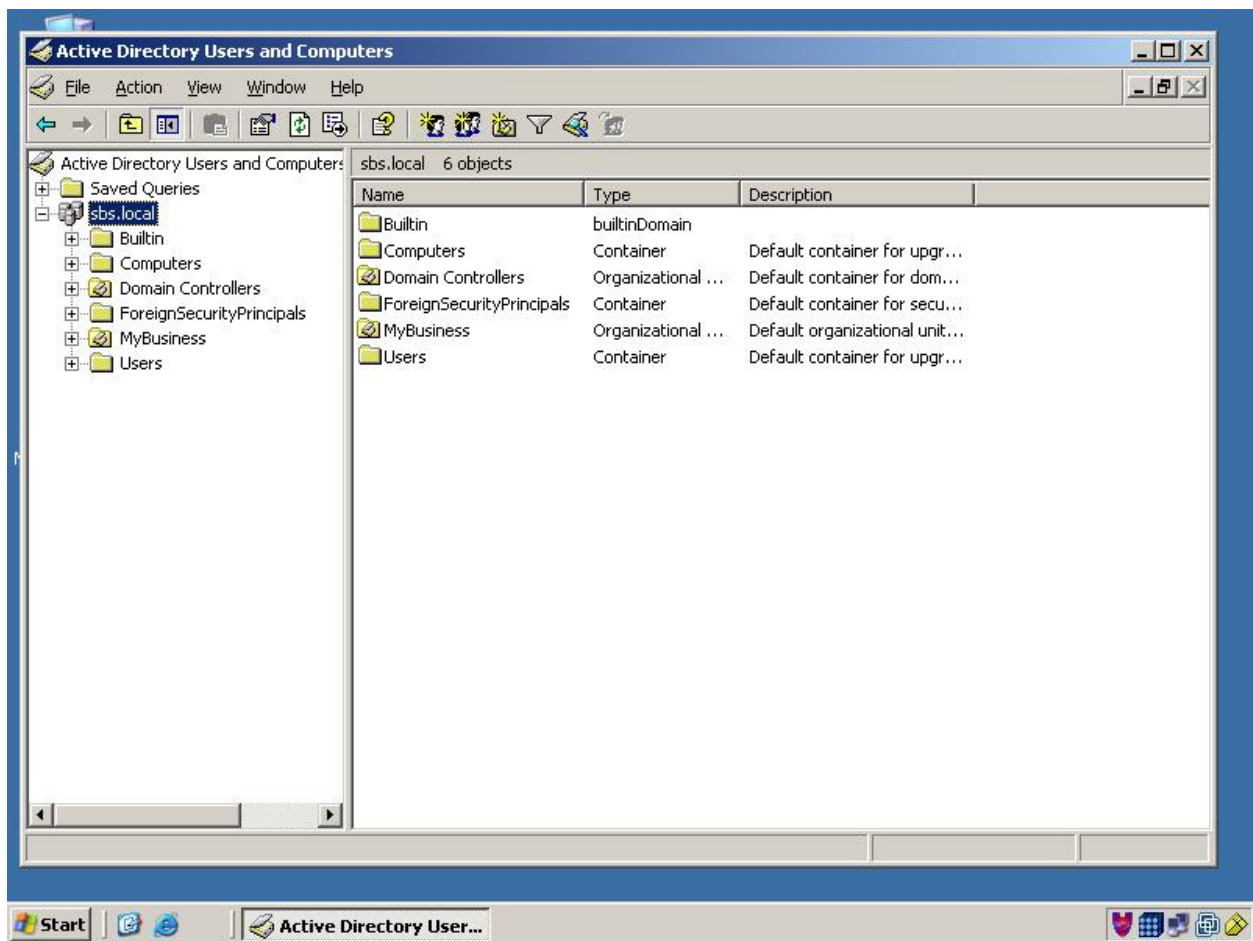
6. Click "Finish". Orca is now installed.

## II. Deploy the VueCentric Updater Service

### A. Create a service account for use with VueCentric Updater Service



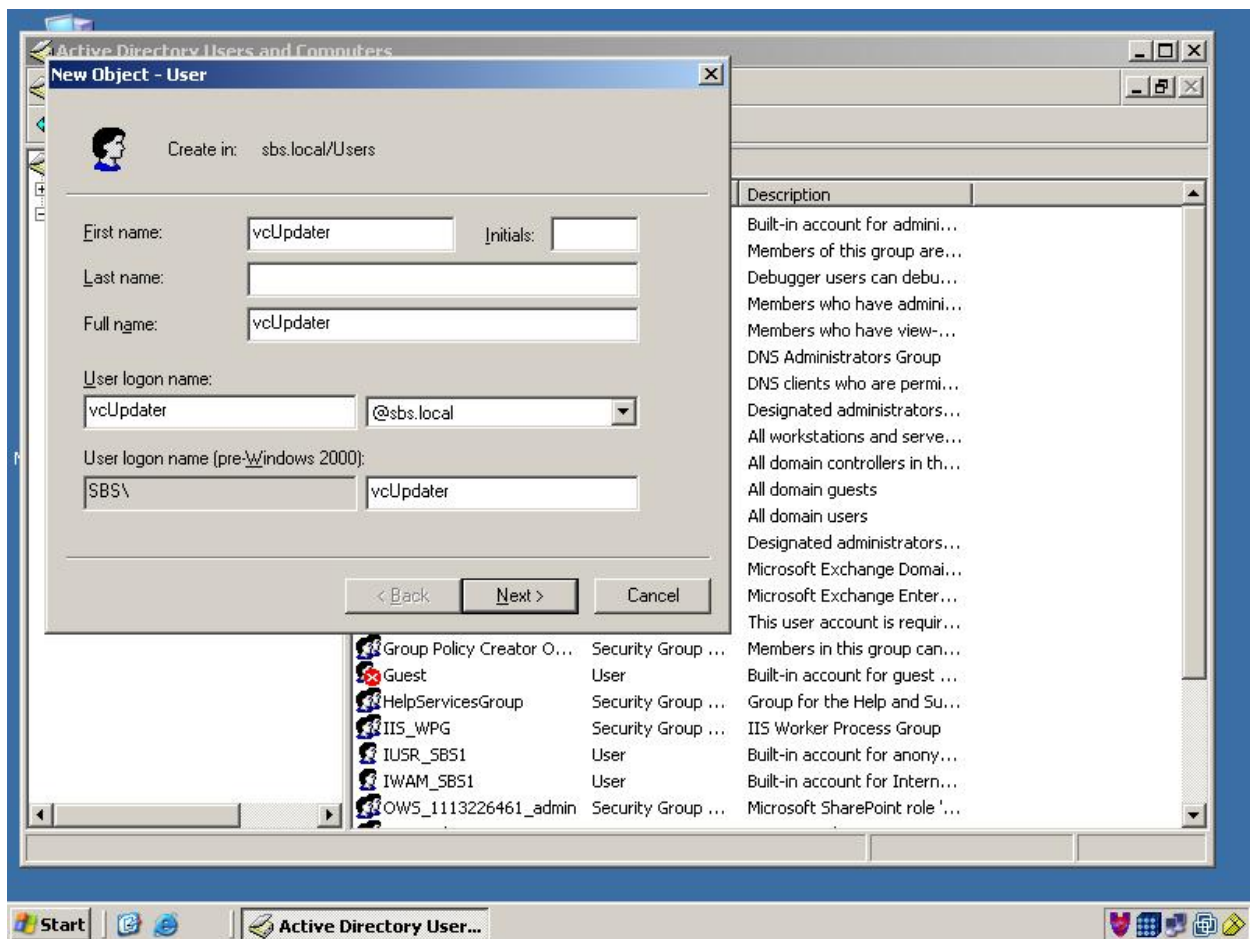
#### 1. Open Active Directory Users and Computers



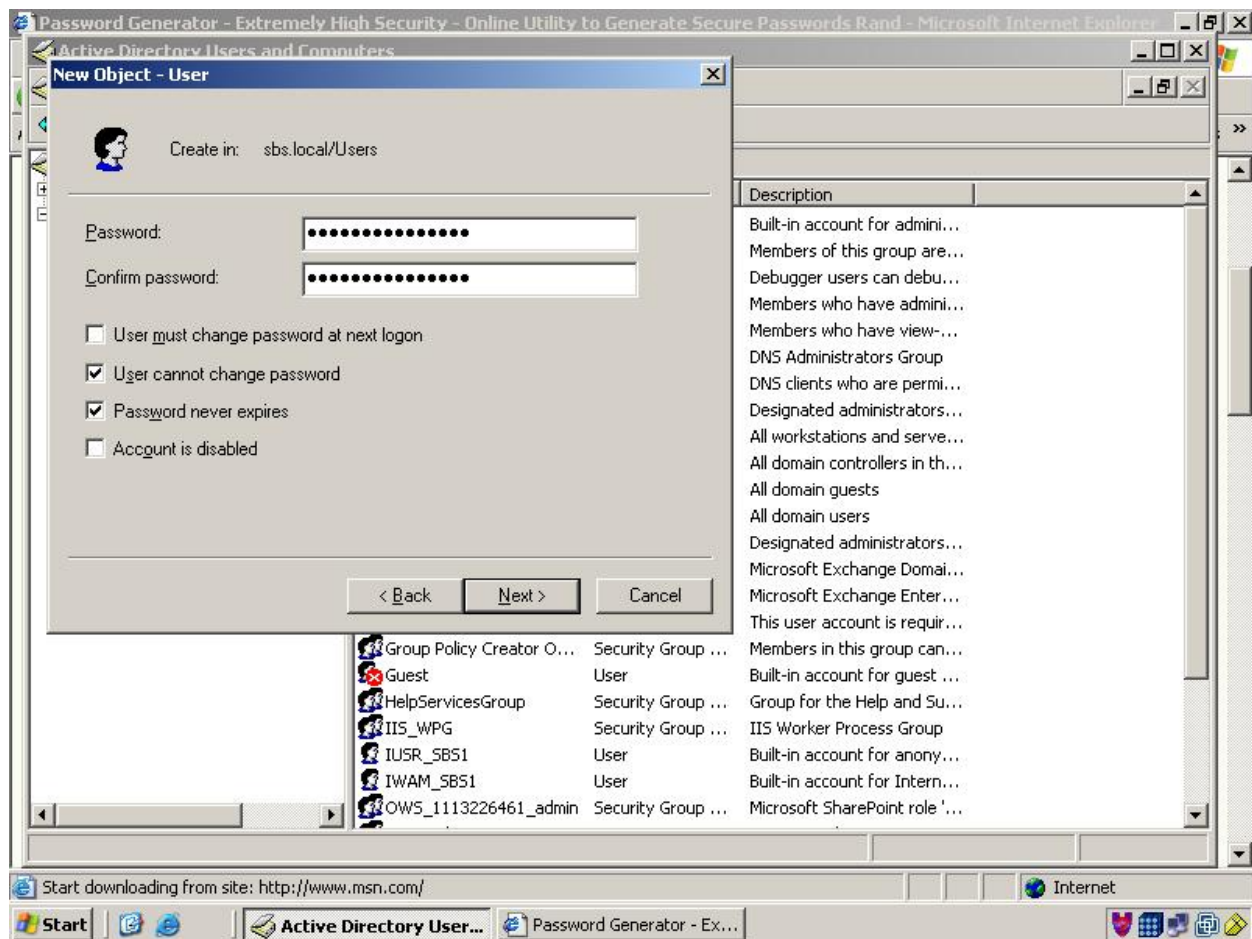
2. Right click on the OU where you want to create the service account.



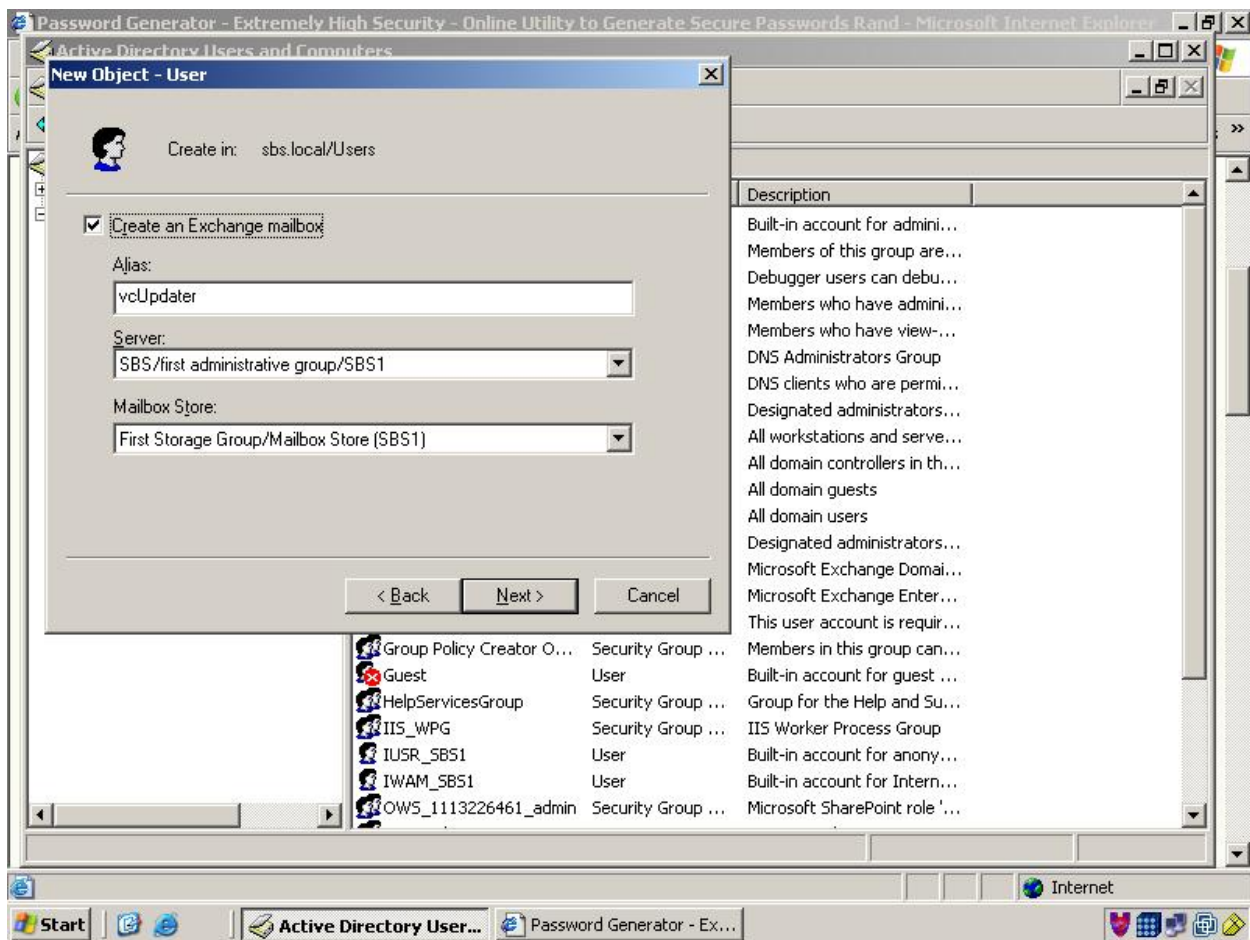




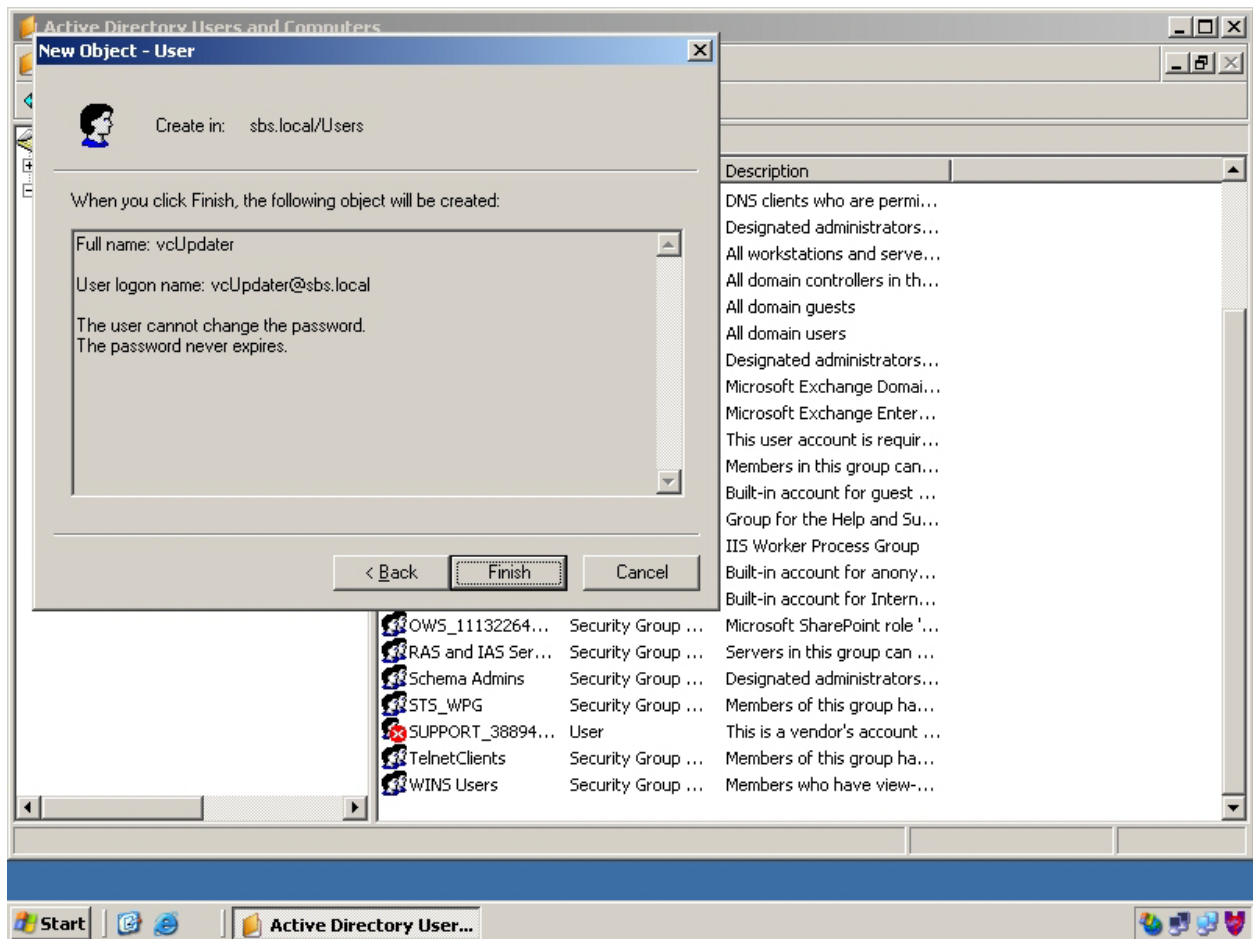
4. Enter the name of the service account you would like to use, then click “Next”.



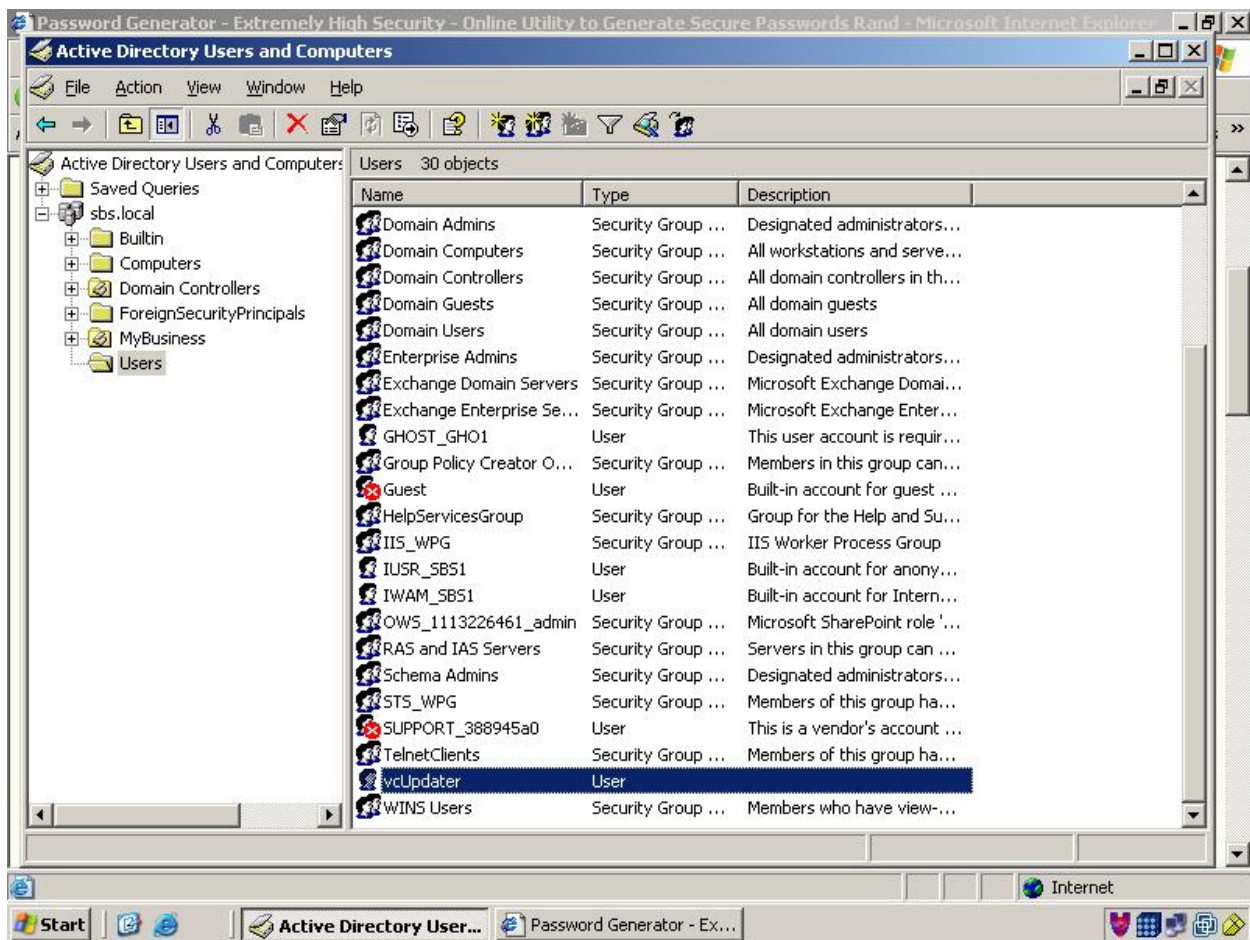
5. Create a complex password and enter into the fields. Check/uncheck the options as shown. *It is extremely important to set the password options as shown.* Then click “Next”.



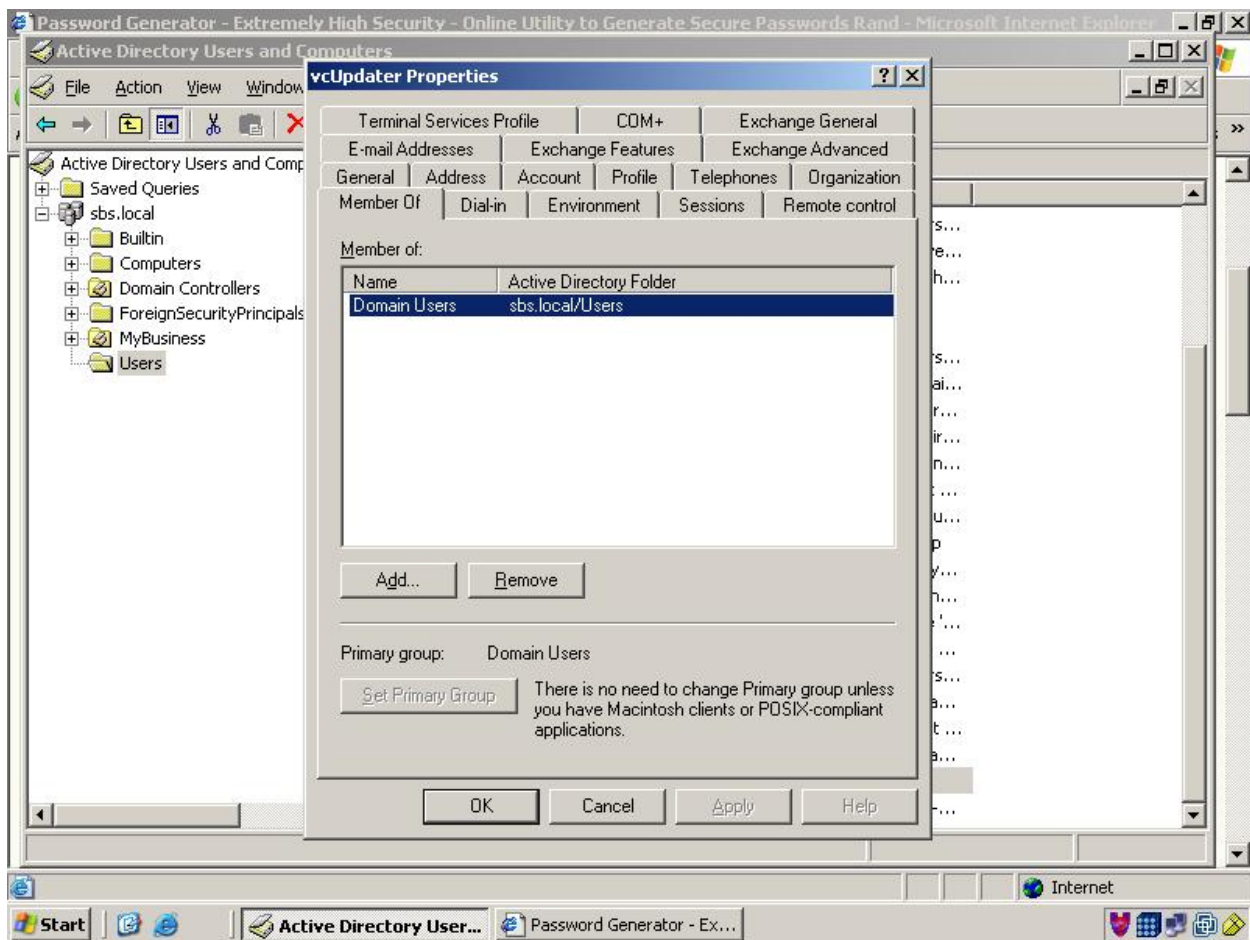
6. The creation of a mailbox is not required. Uncheck the "Create an Exchange mailbox" checkbox and click "Next".



7. Click "Finish".

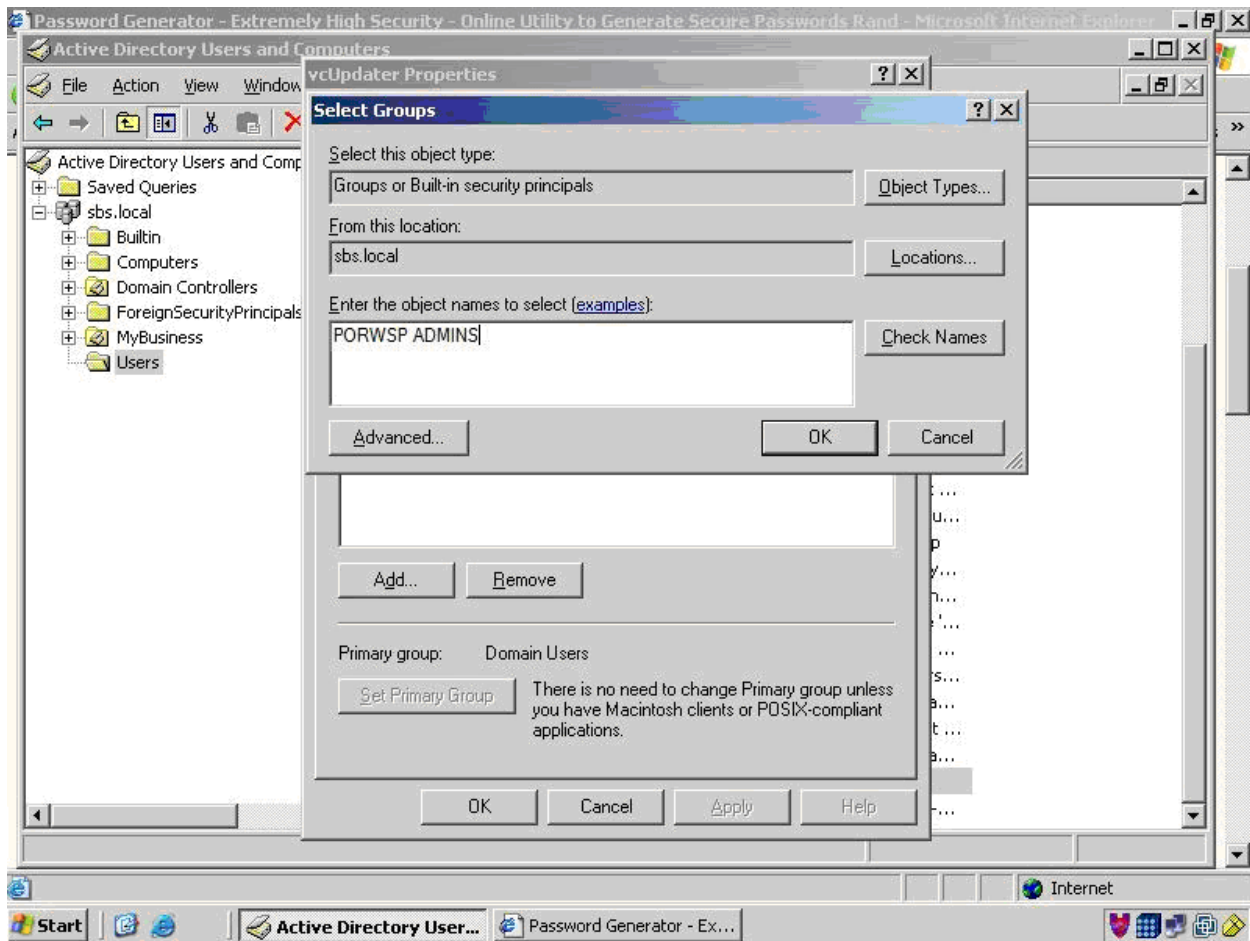


8. Locate and double-click the vcUpdater account in the right pane. Select the "Member of" tab from the properties dialog that appears.

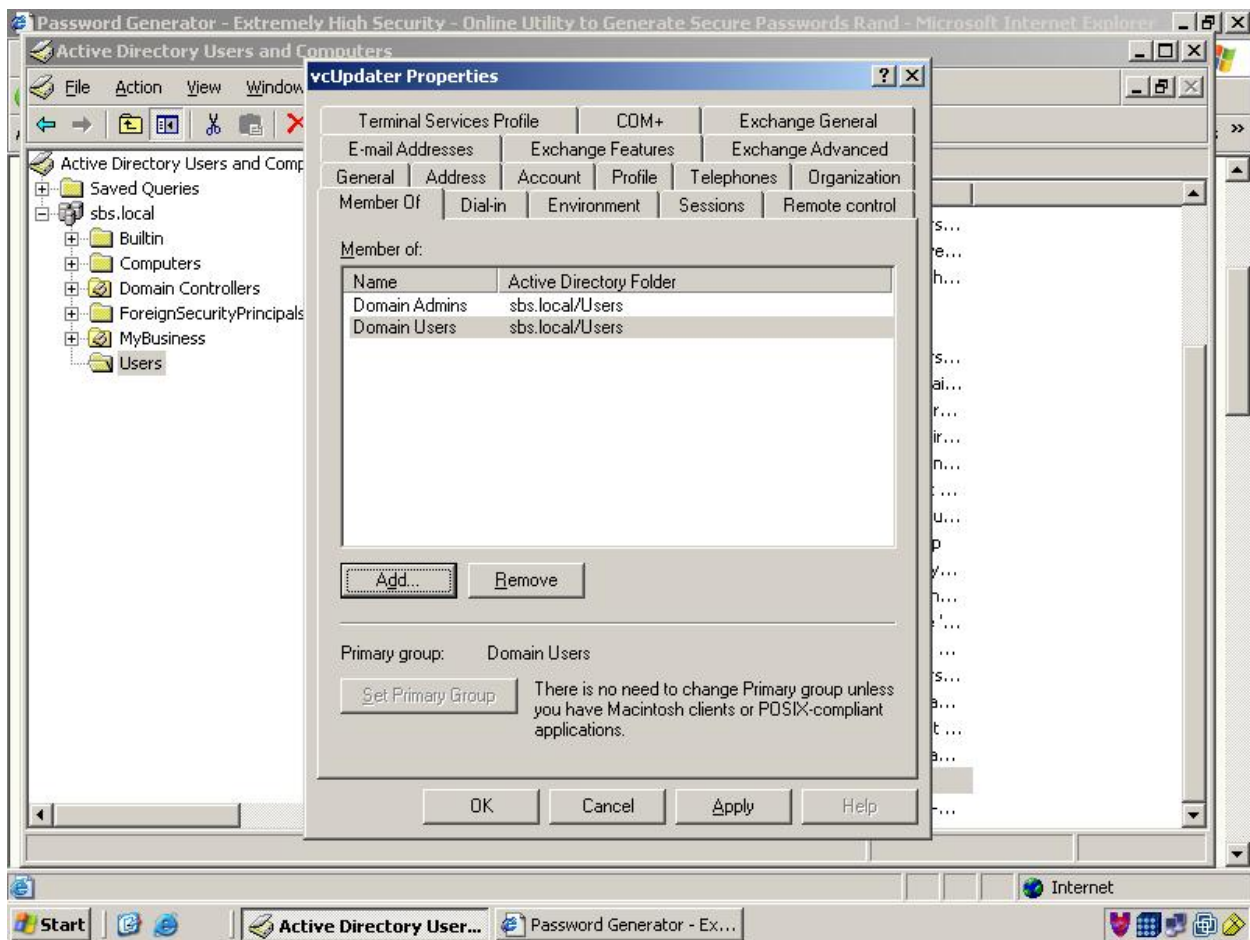


9. Click "Add".



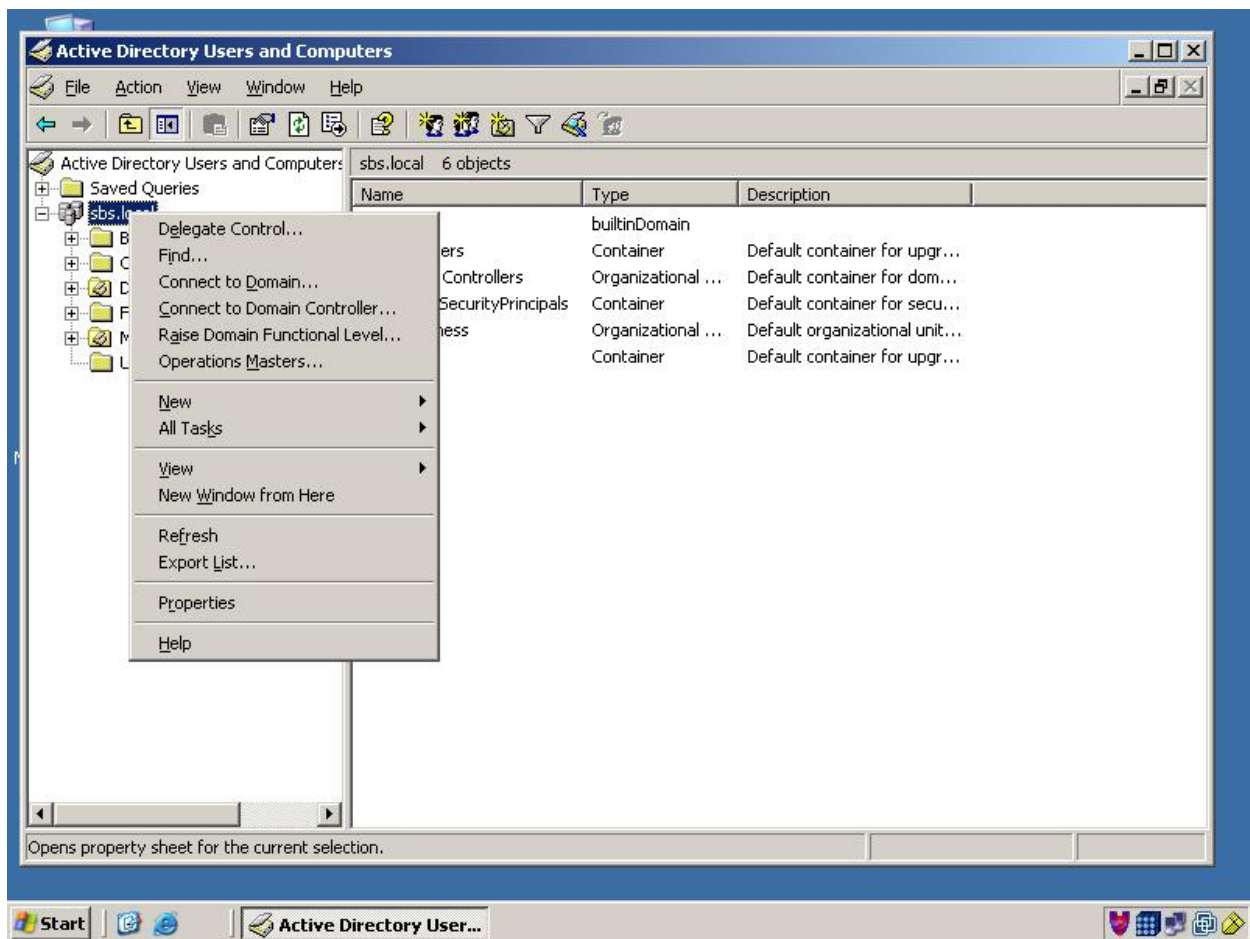


10. Enter the security group for this account and click "OK". **Note: sites will have different administrative security groups defined. The vcUpdater account must be a local admin on the workstations. The site administrator should put the account into a local admin group that has the necessary rights to perform updates.**

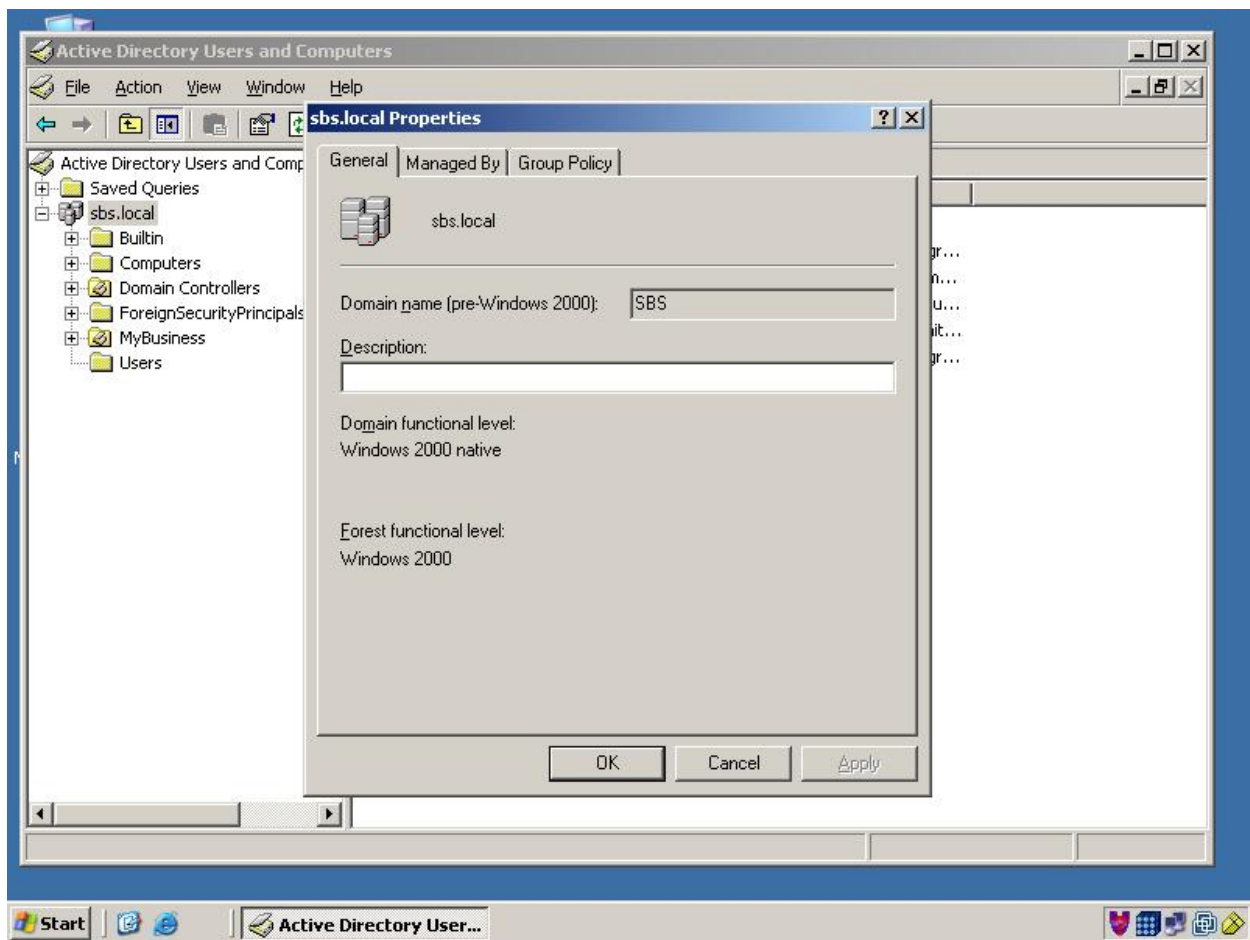


11. Click "OK".

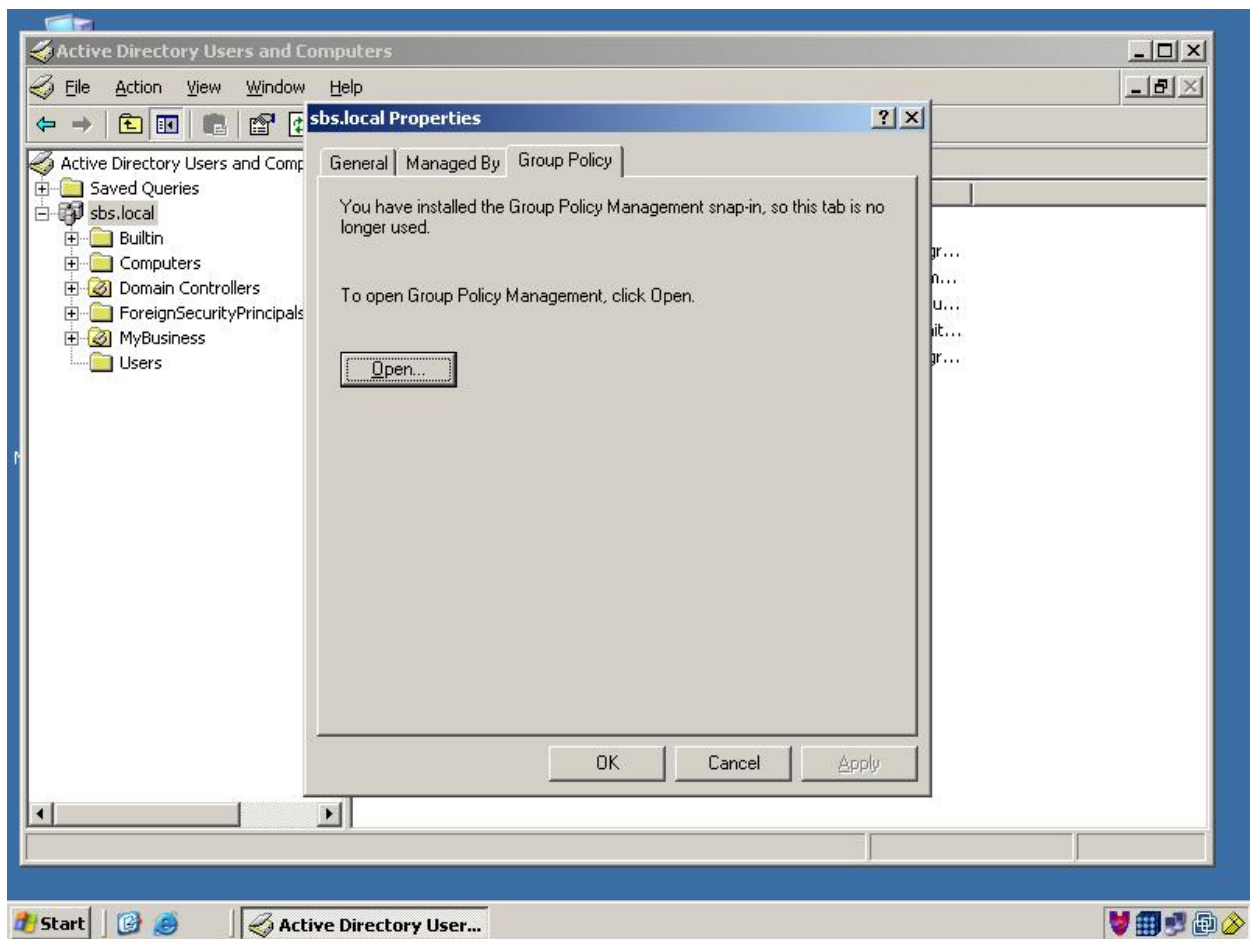




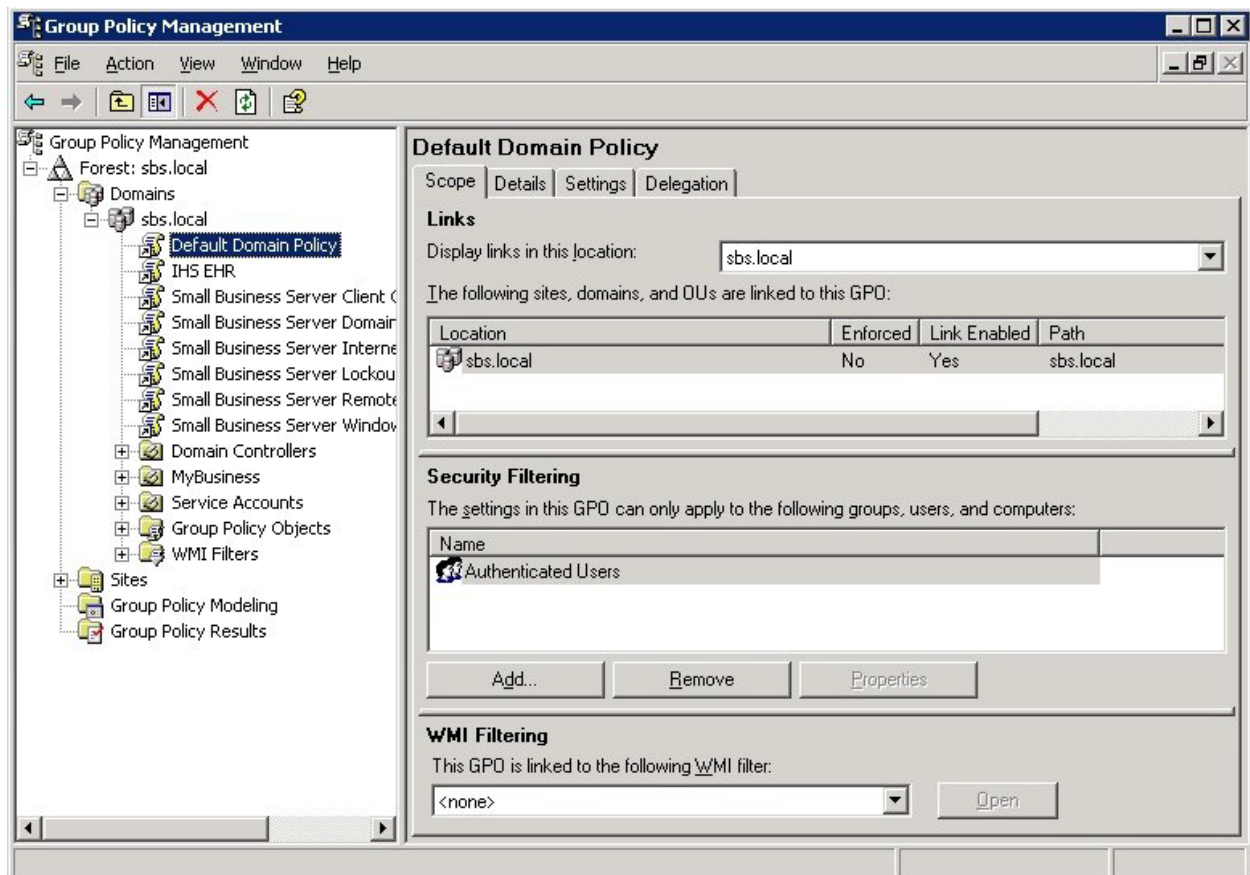
12. Next, the newly created account must be granted permission to run as a service and to prevent it from interactive logins. Right-click on the domain or OU to which the account belongs and select properties.



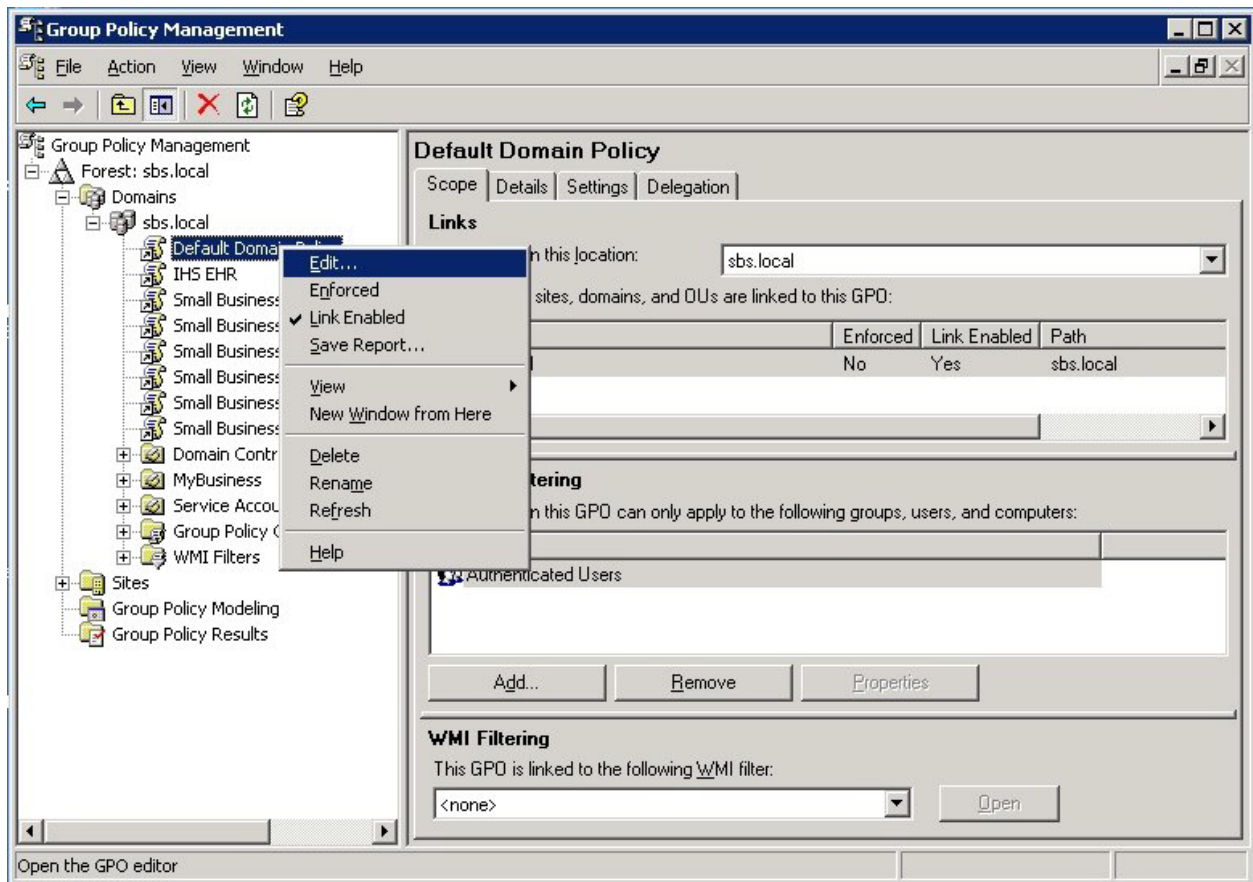
13. Click on the "Group Policy" tab.



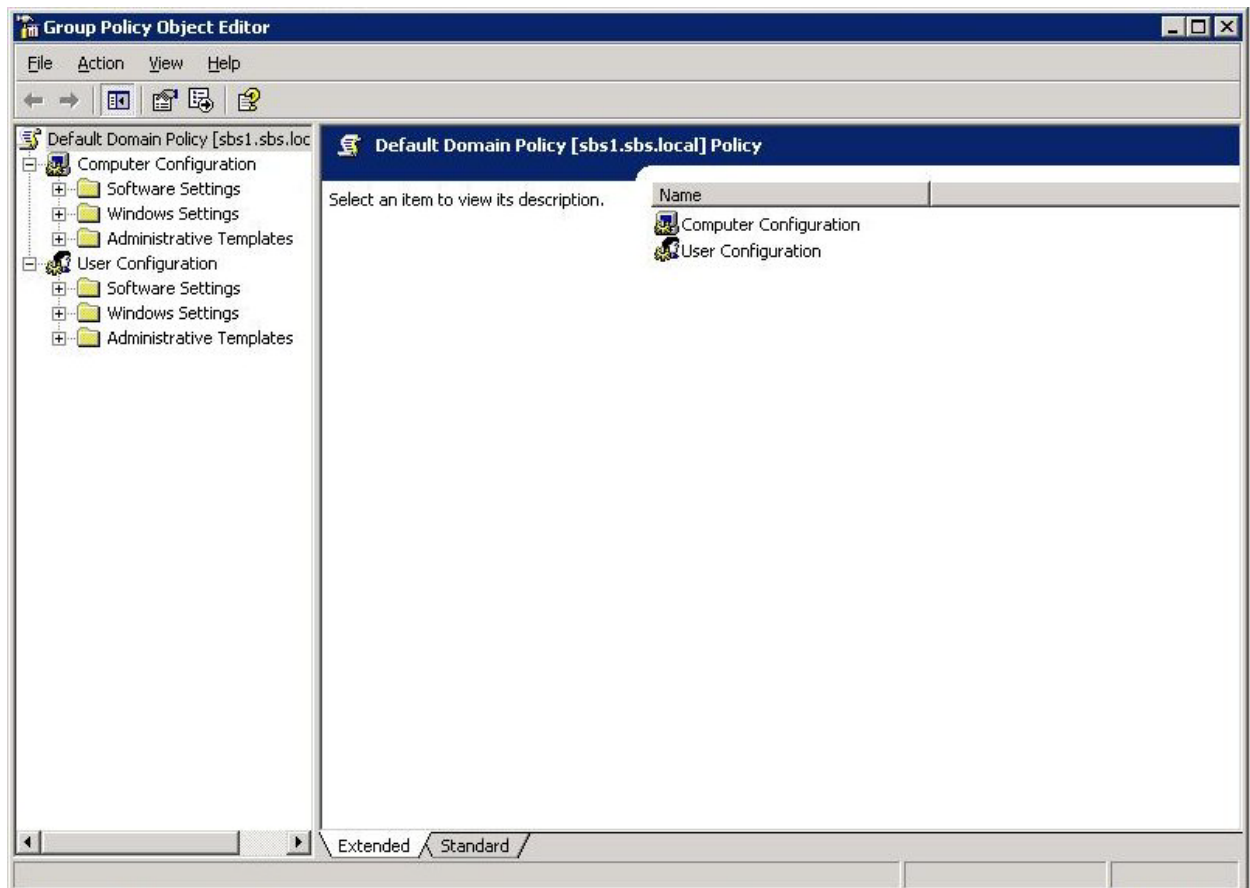
14. Click "Open".



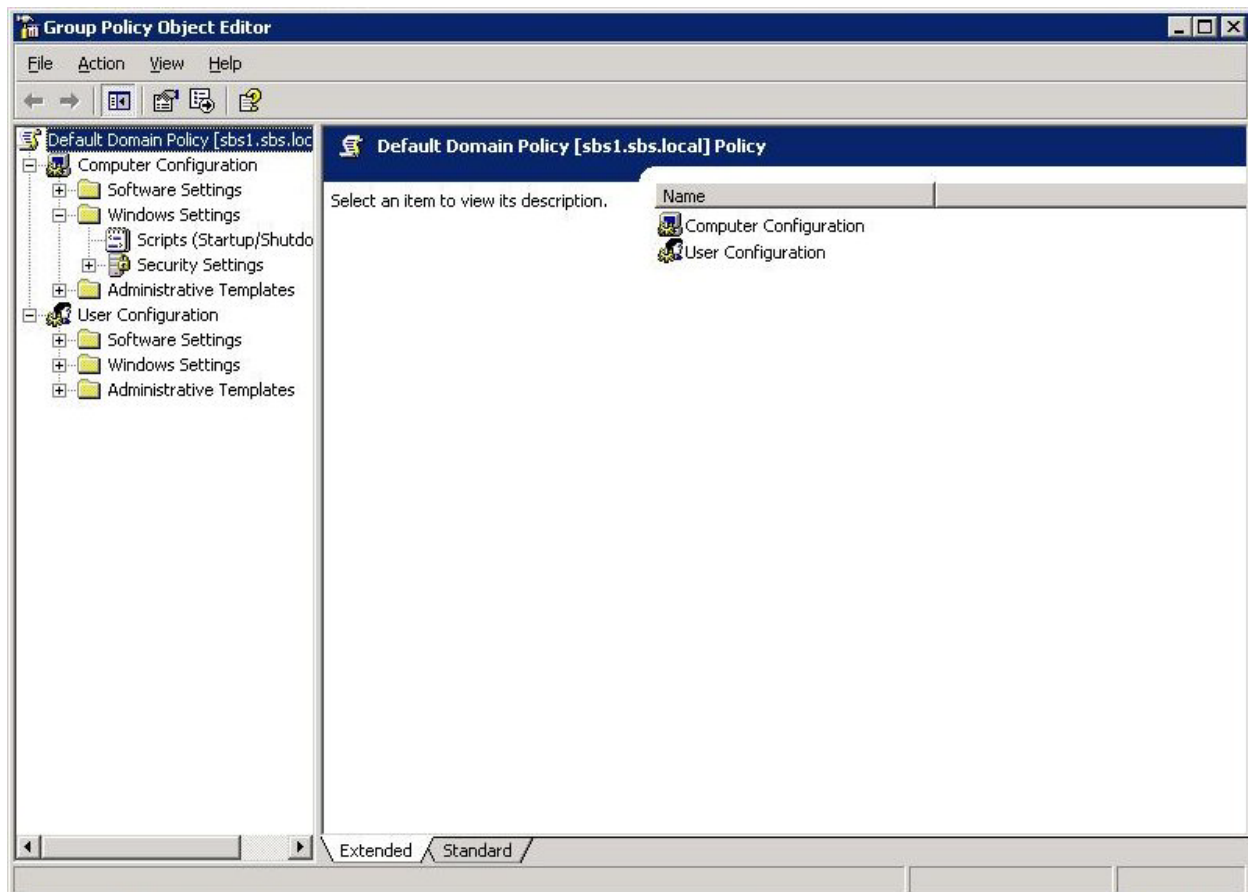
15. Expand the domain node by clicking on the + to the left. Click the appropriate domain policy to select it. Close any informational dialogs that may appear. **Note: Sites can use group policies already in place or call OIT to request a GPO to be created for them.**



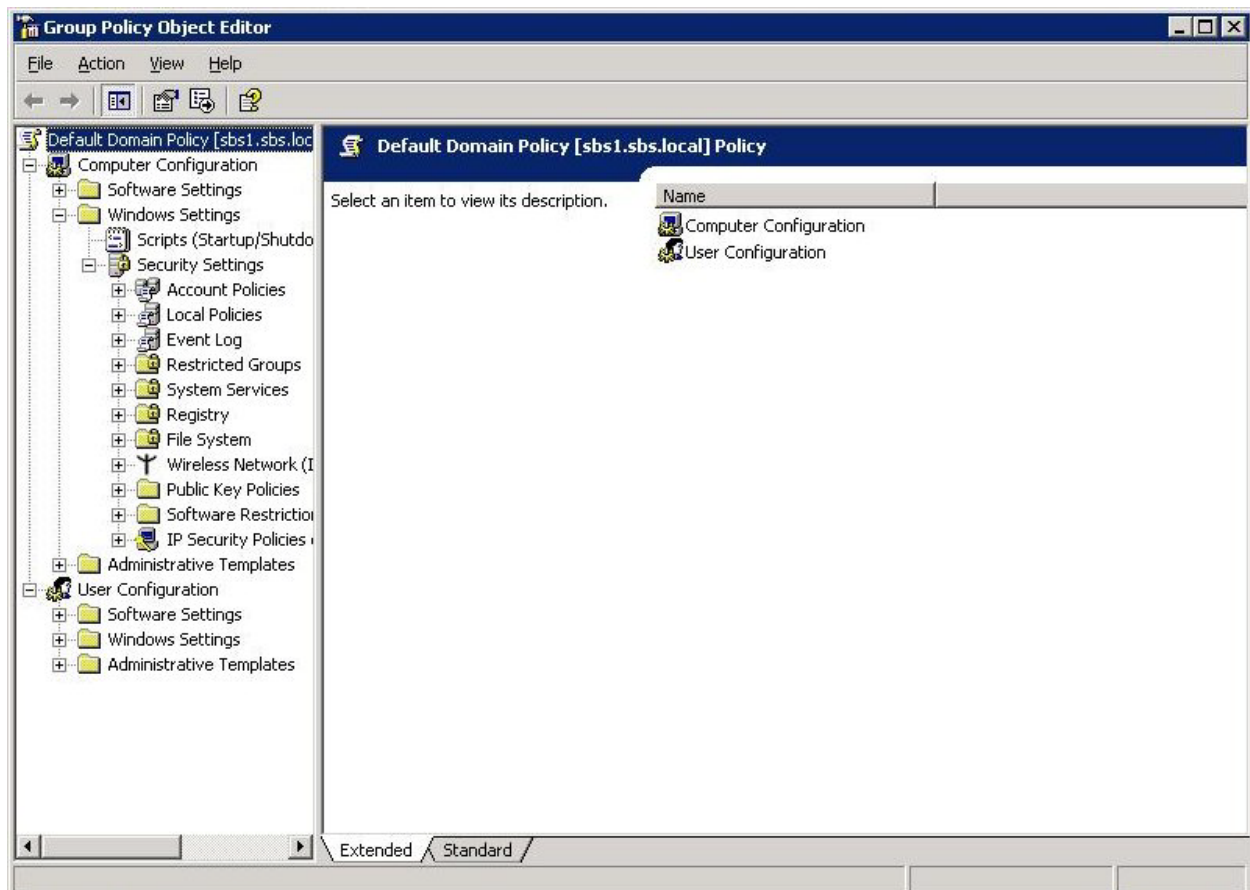
16. Right-click the entry and select “Edit” from the popup menu. Dismiss any informational dialogs that may appear.



17. Under Computer Configuration, click the + to the left of the Windows Settings node to expand it.

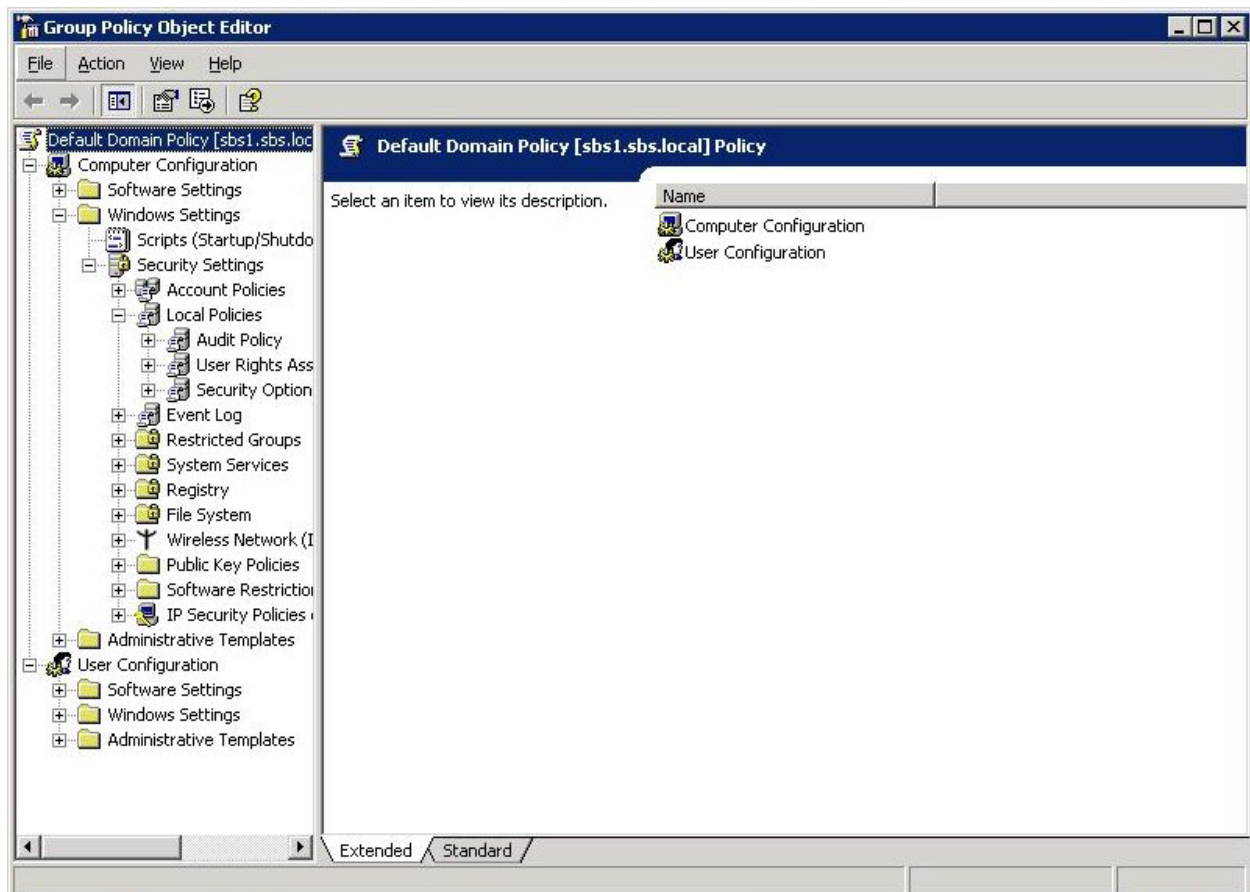


18. Click the + to the left of the Security Settings node to expand it.

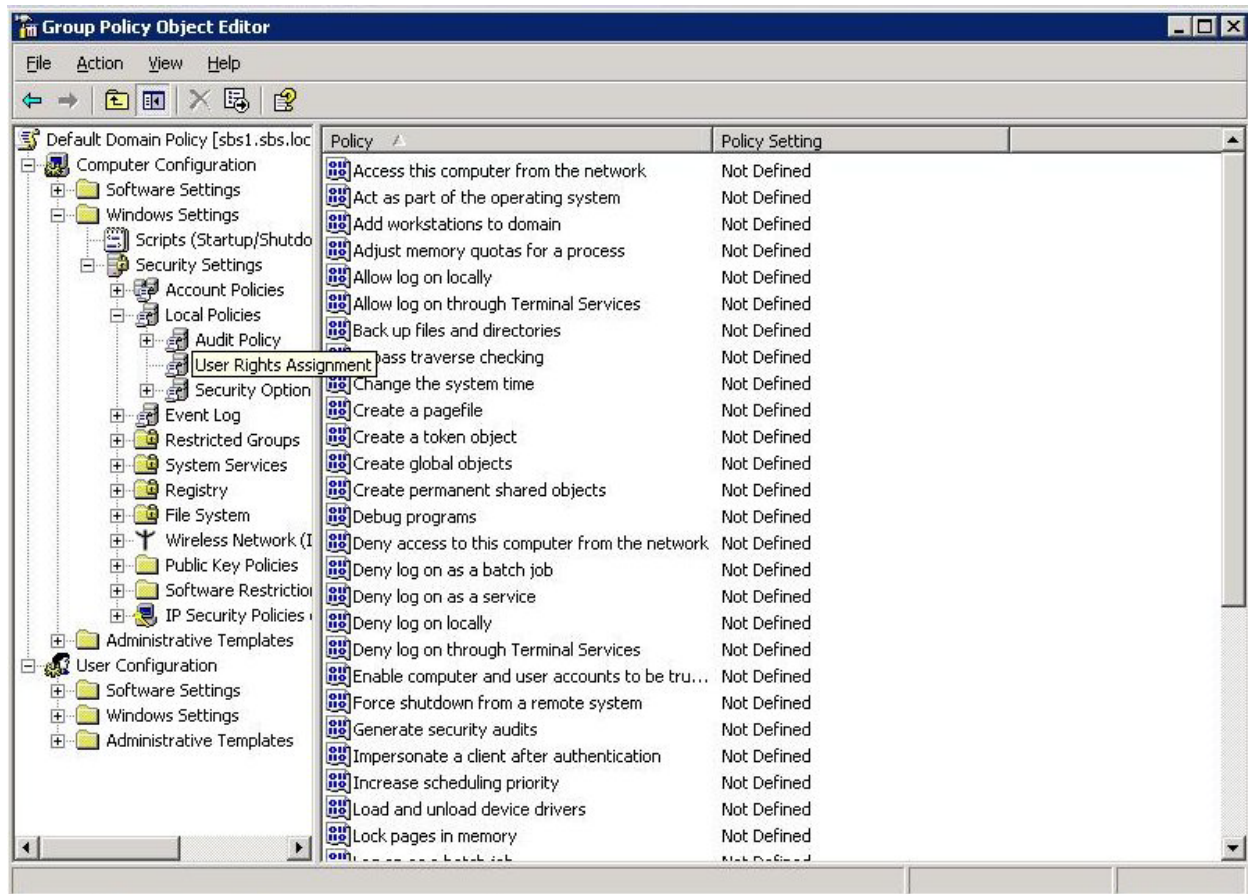


19. Click the + to the left of the Local Policies node to expand it.

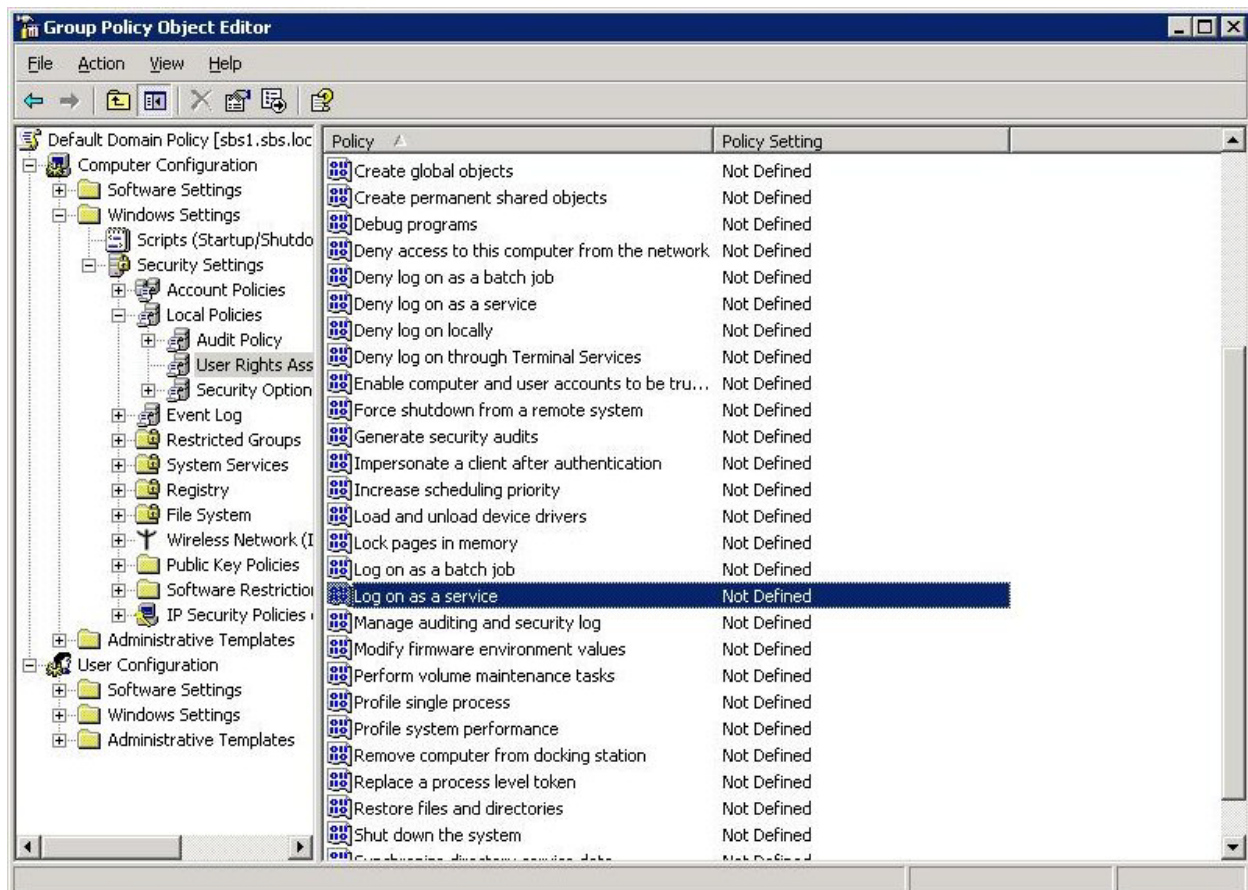




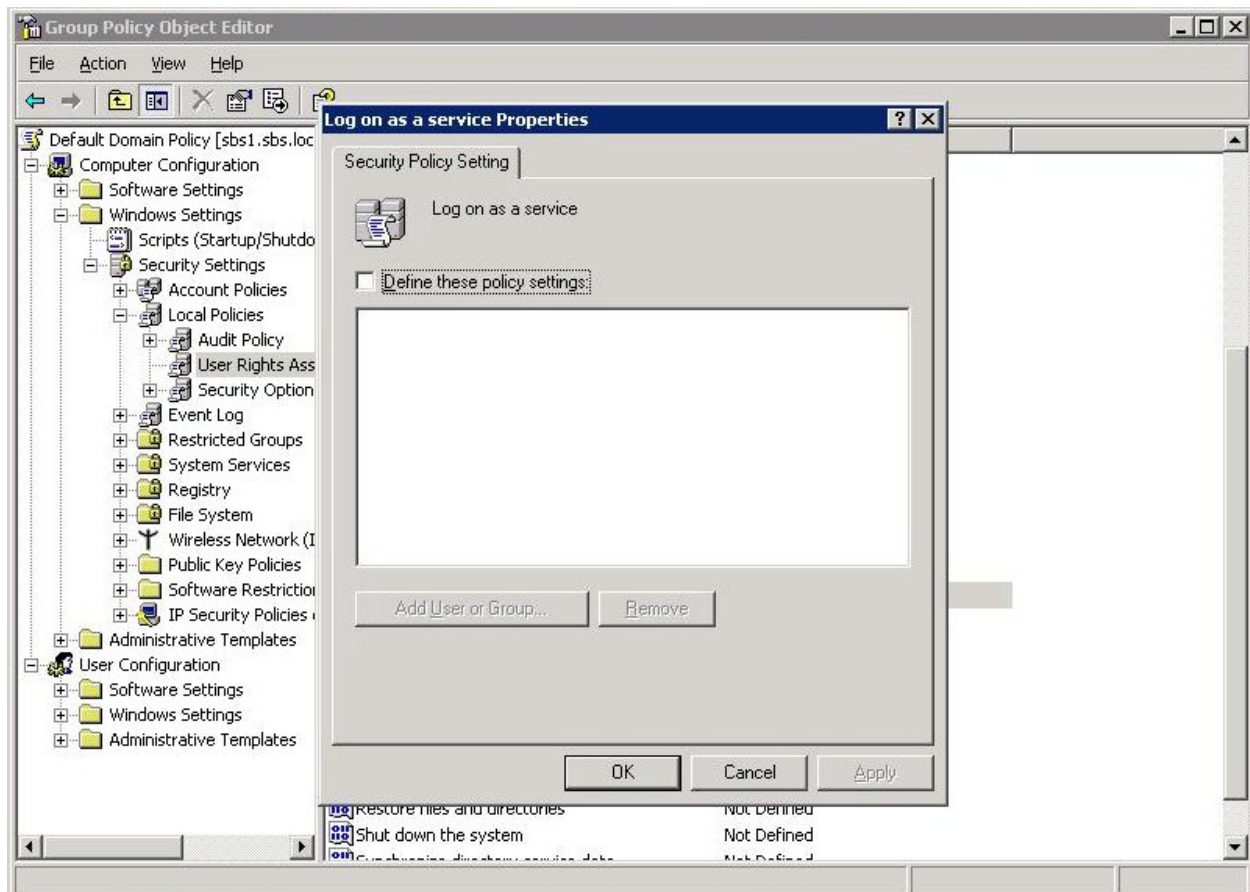
20. Click the User Rights Assignments node to select it.



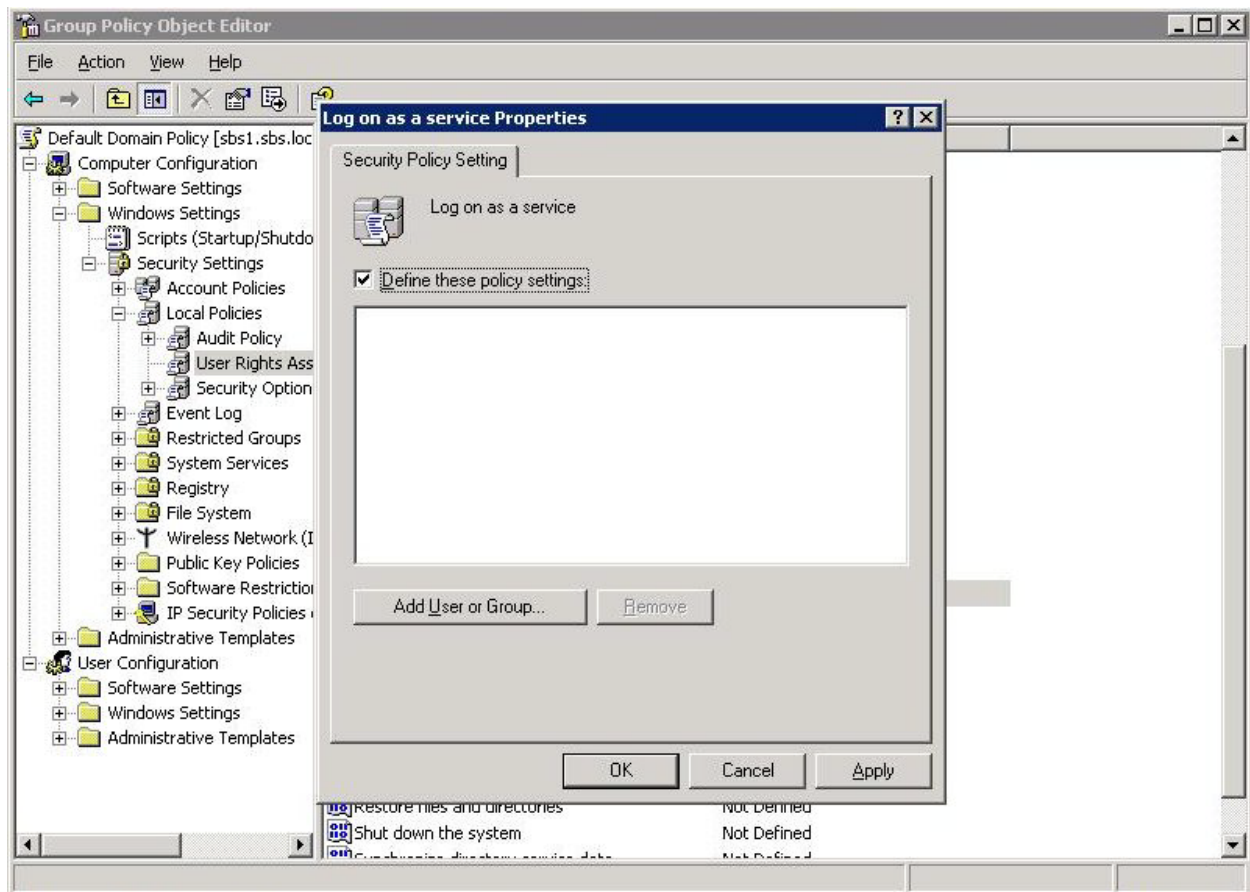
21. Locate the “Log on as a service” policy in the right pane by scrolling down the list.



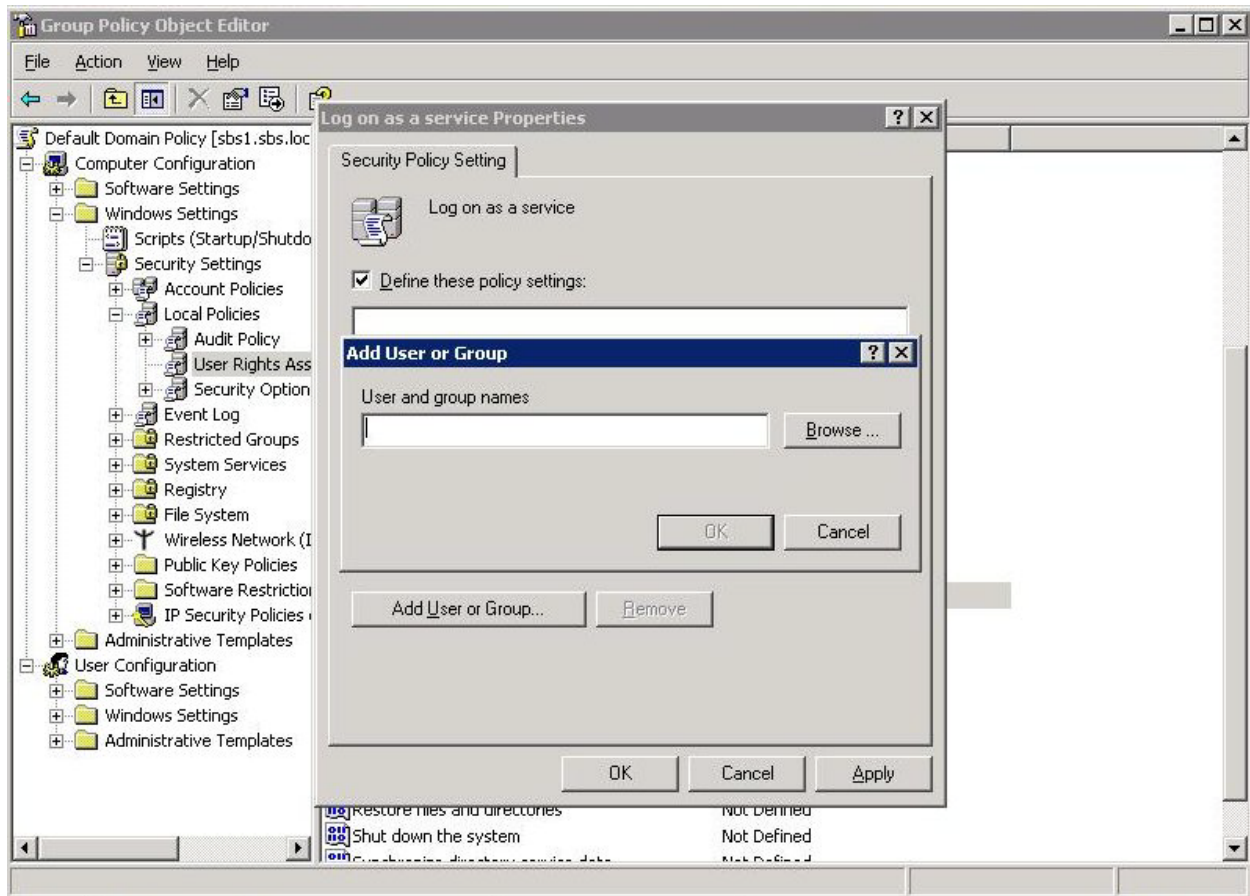
22. Double-click the “Log on as a service” entry to view its properties.



23. Check the “Define these local policy settings” checkbox.

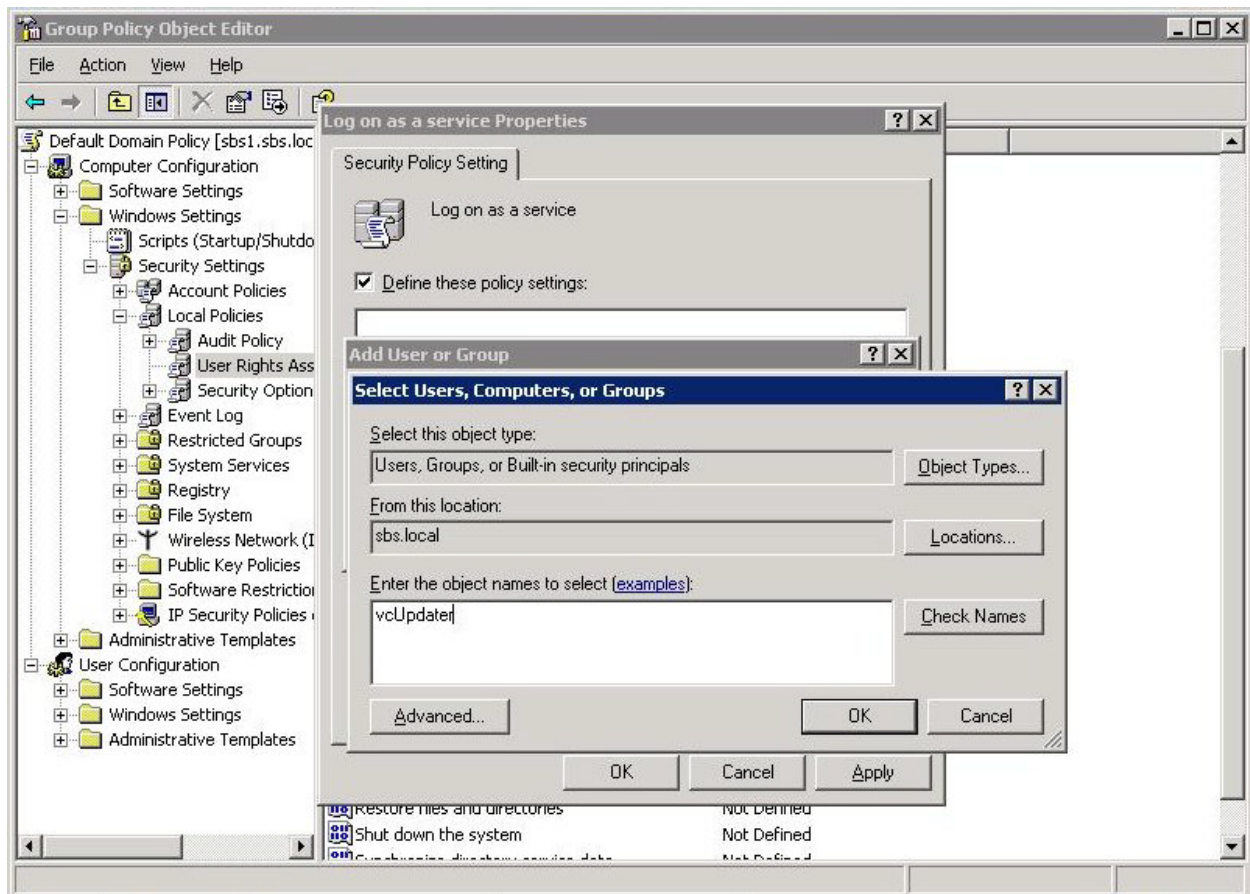


24. Click “Add User or Group”.

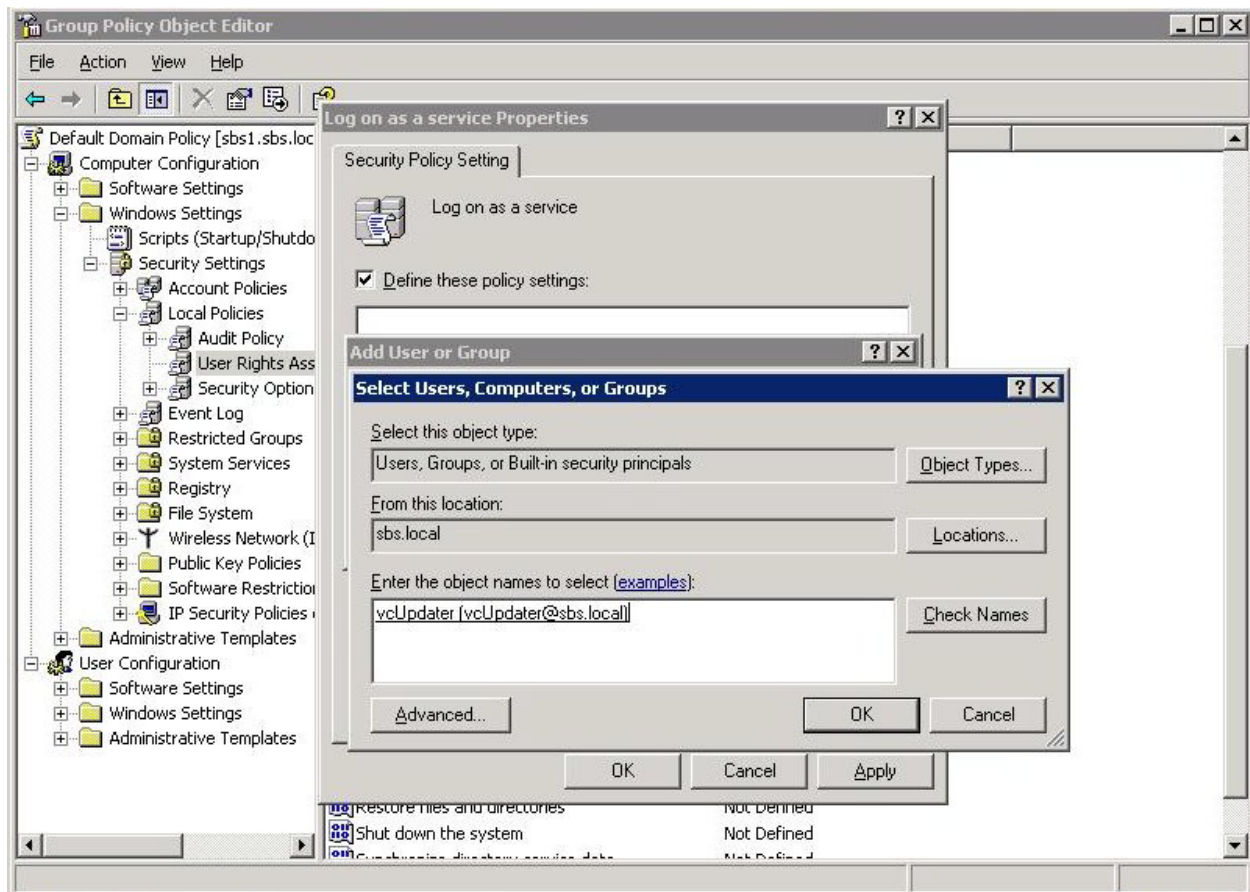


25. Click "Browse".



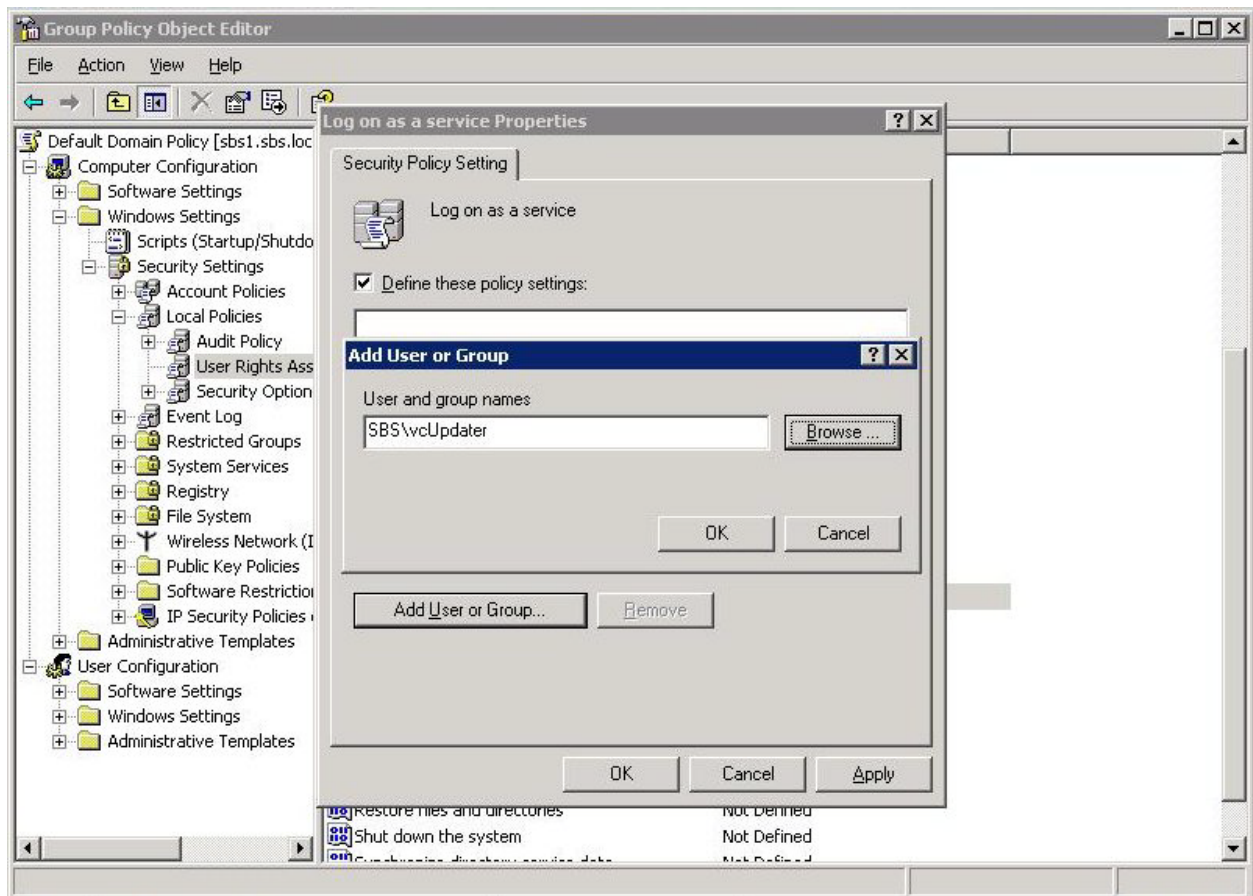


26. Enter the name of the newly created account in the edit box. Then click “Check Names”.

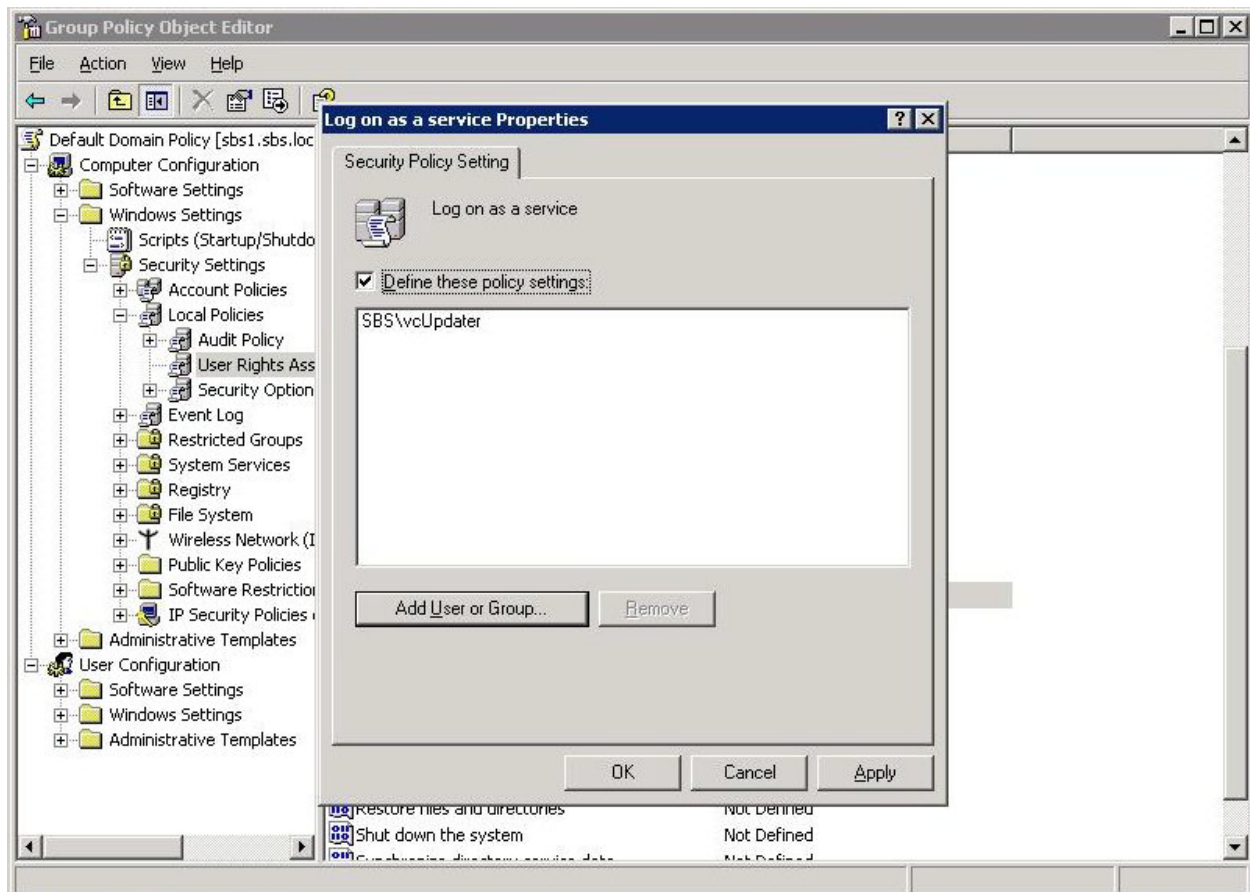


27. Click "OK".



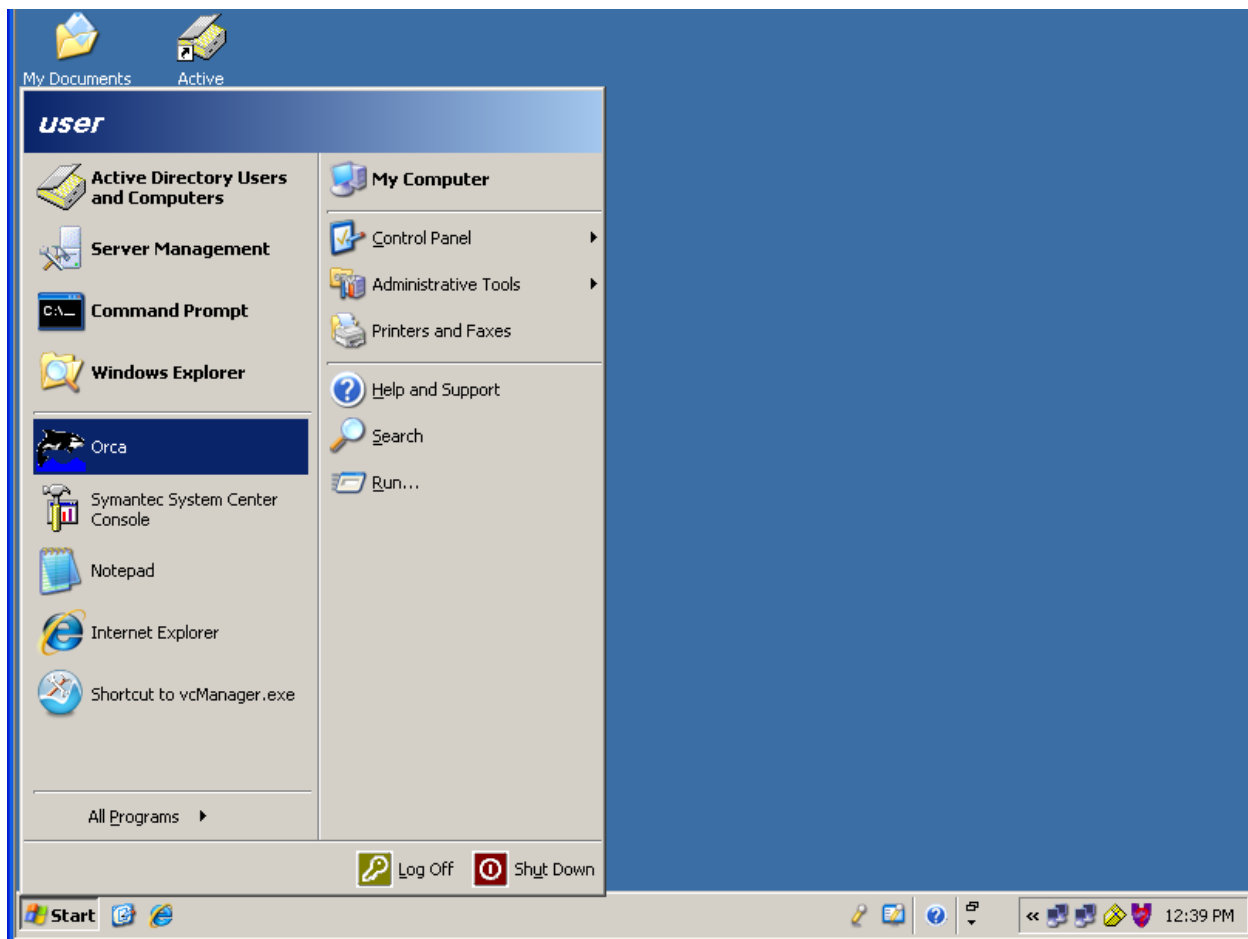


28. Click "OK".

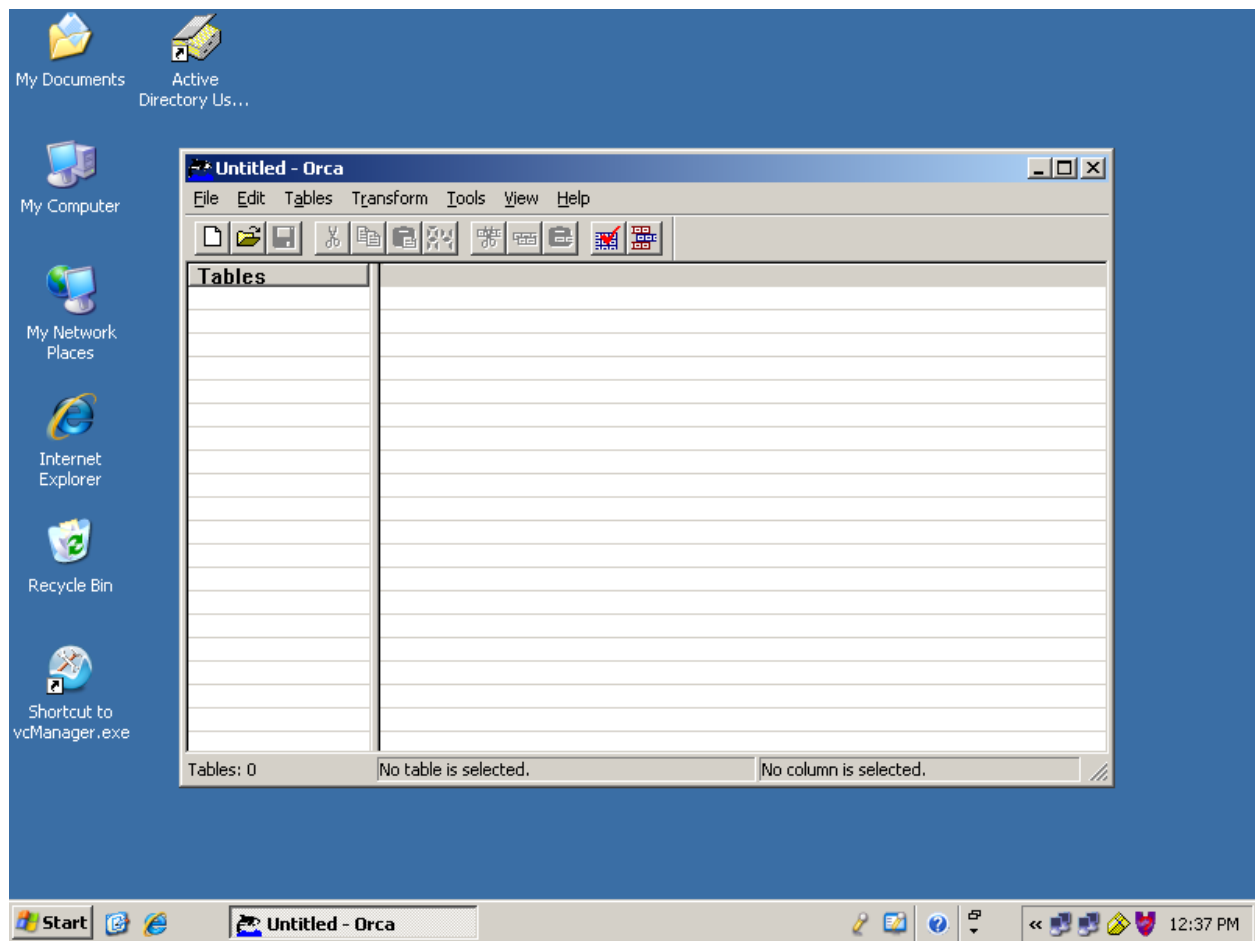


29. Click “OK”. For improved security, at this point you may also want to add the “Deny log on locally” policy. This will prevent this account from ever being used for interactive logons. To do this, return to step 22 and follow the same procedure but instead selecting the “Deny log on locally” policy from the list. This completes the creation of the service account. You may close all remaining open dialogs at this time.

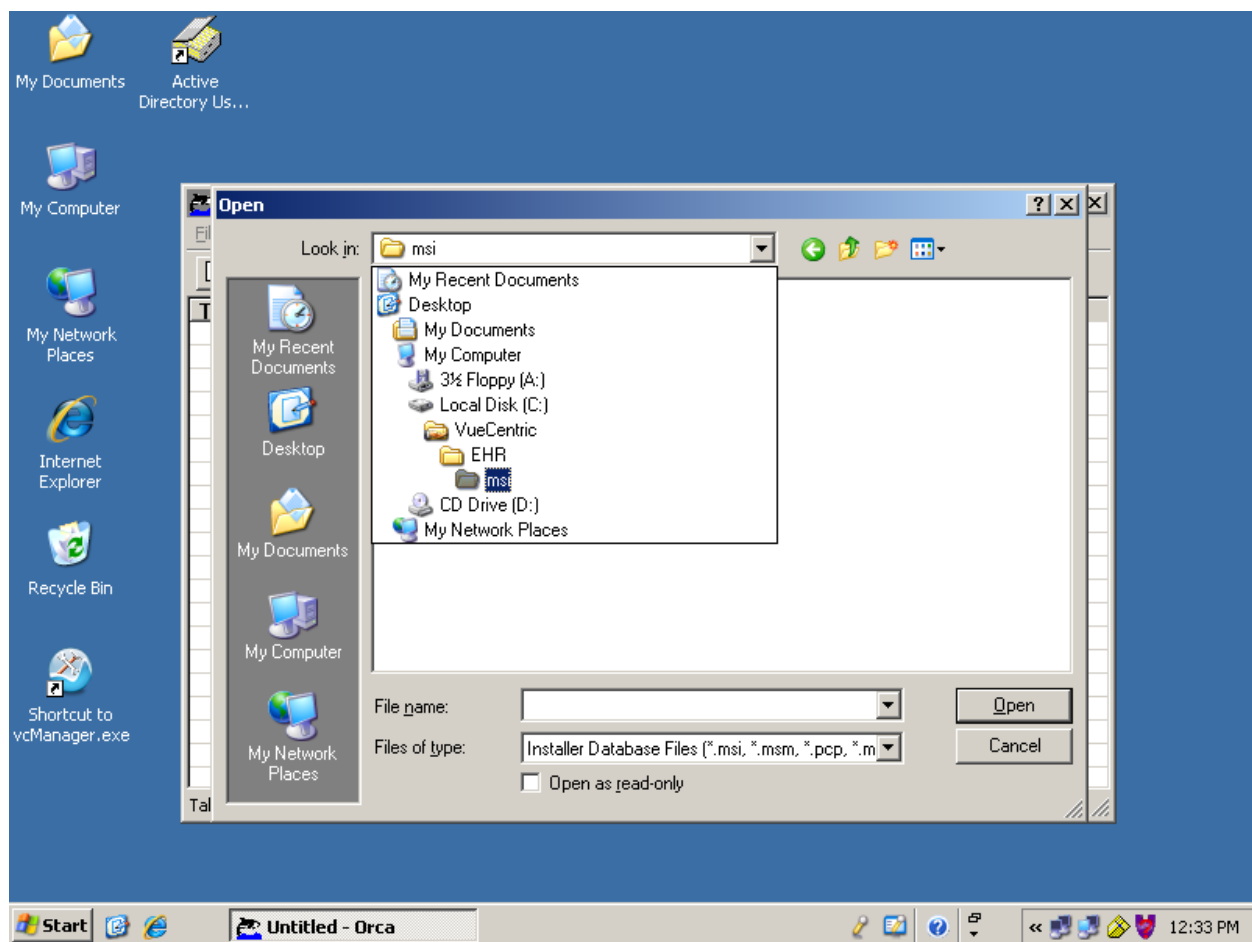
## B. Modify the vcUpdaterService\_Silent\_x.y.msi Properties Table using Orca



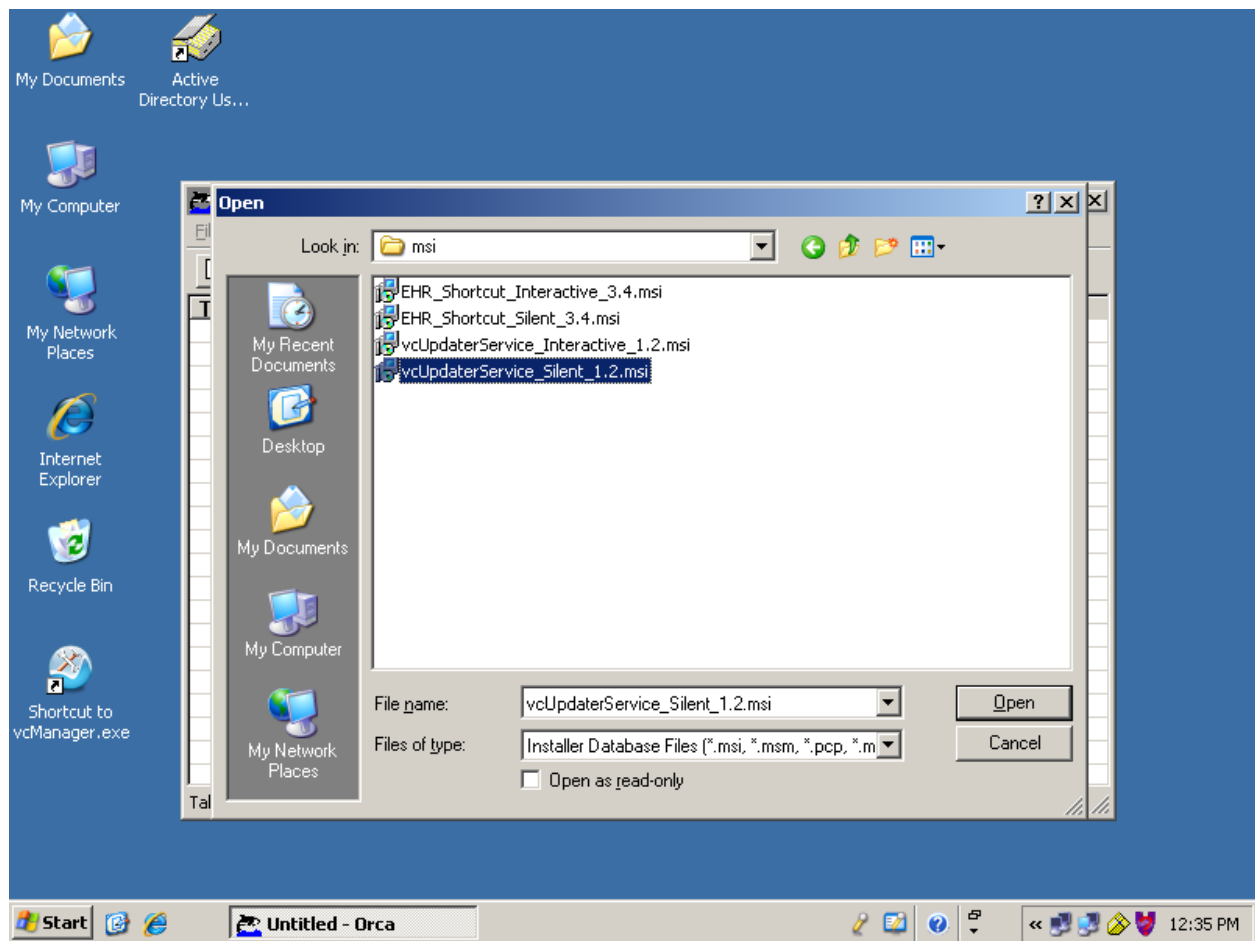
1. Open Orca from the Start menu.



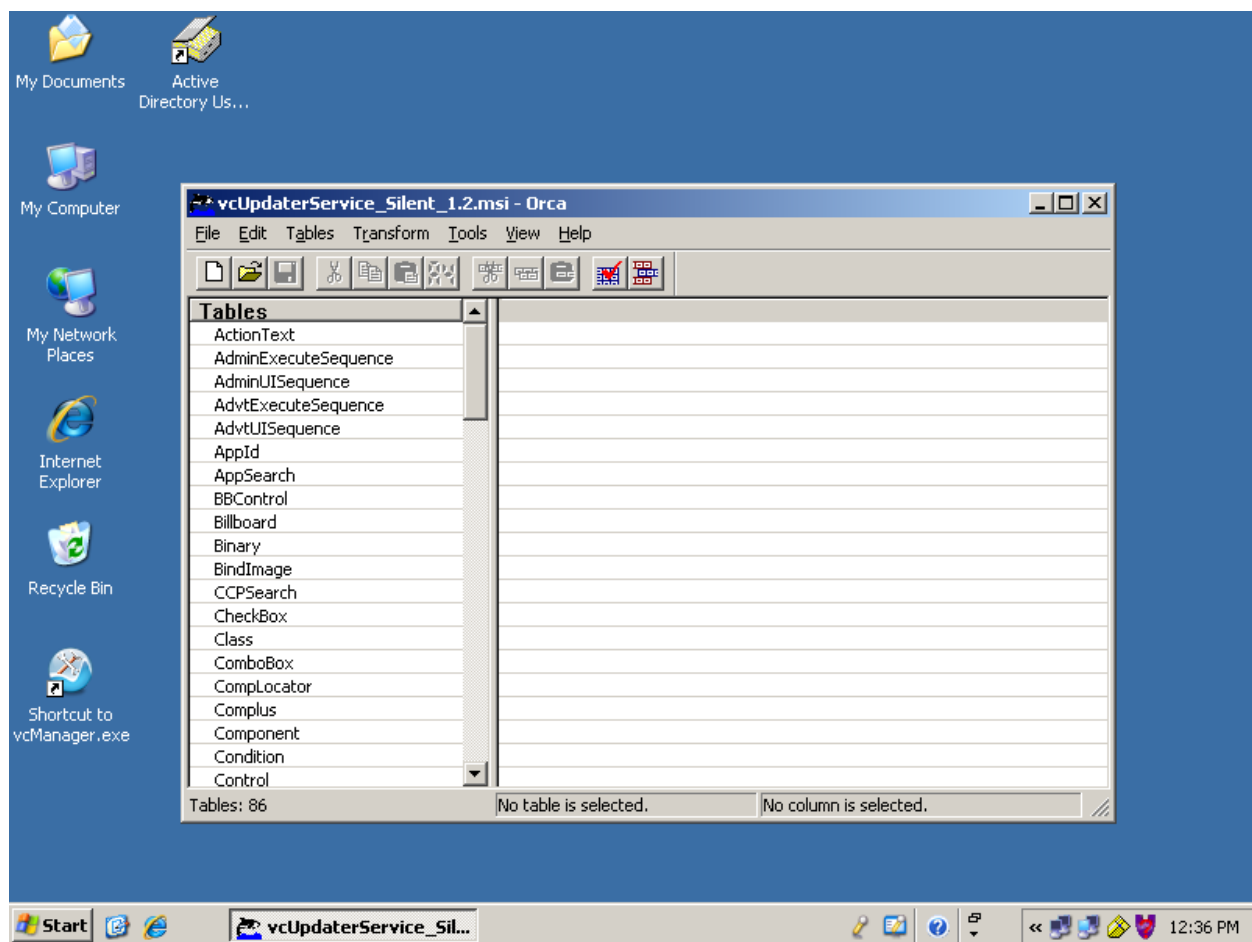
2. Click the folder icon.



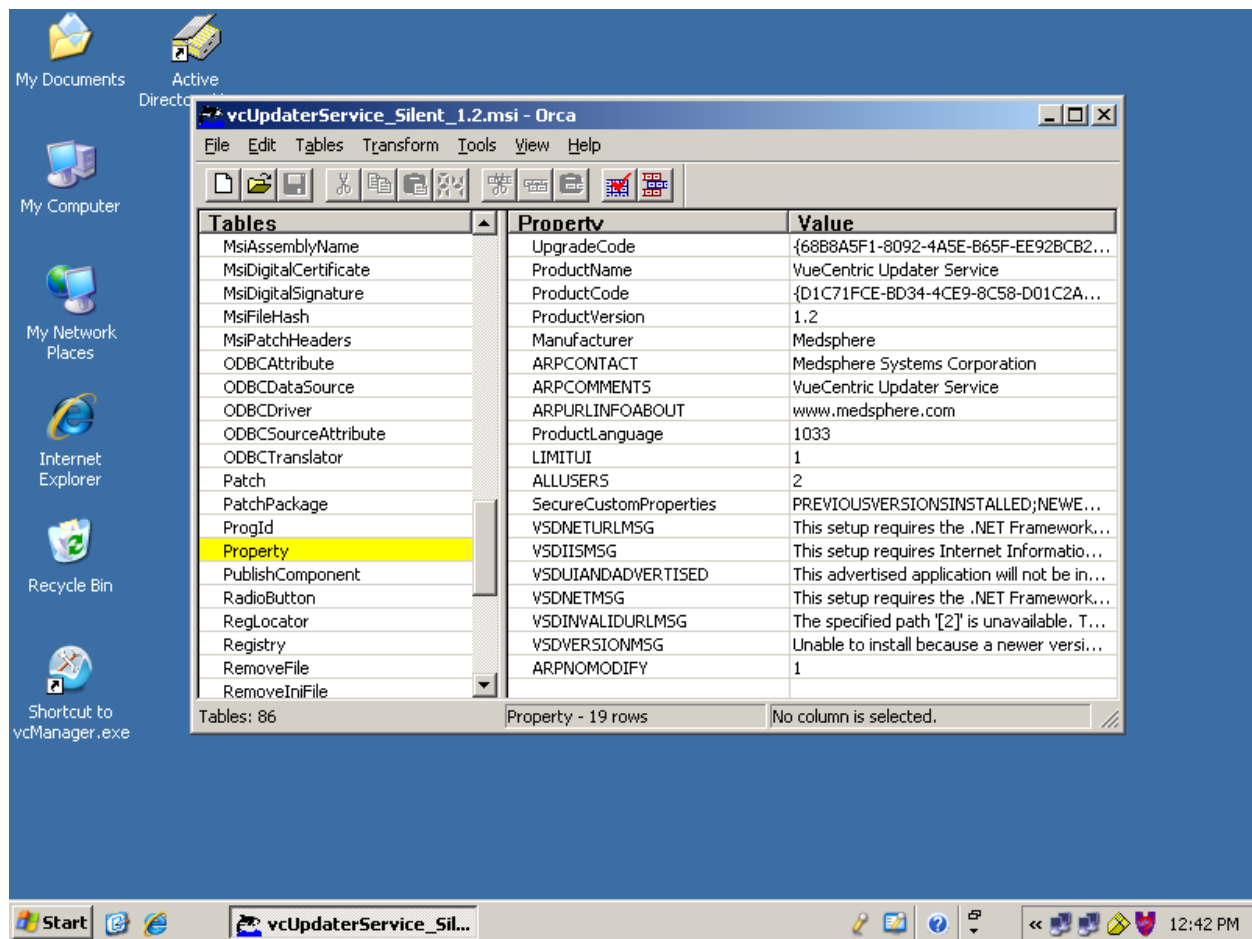
3. Select the location of the vcUpdaterService\_Silent\_x.y.msi file.



4. Select the vcUpdaterService\_Silent\_x.y.msi file and click open.

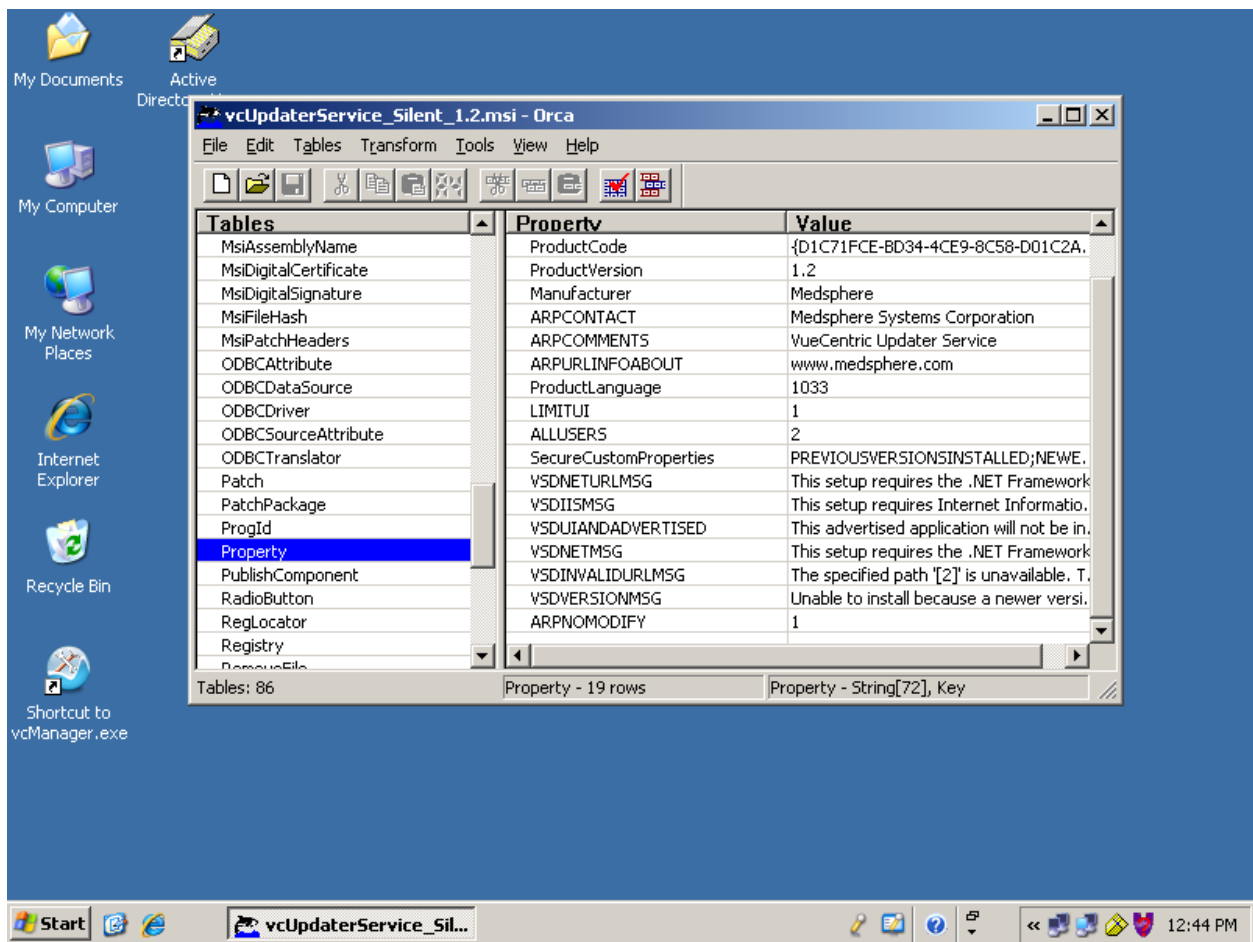


5. Scroll down to the Properties Table.

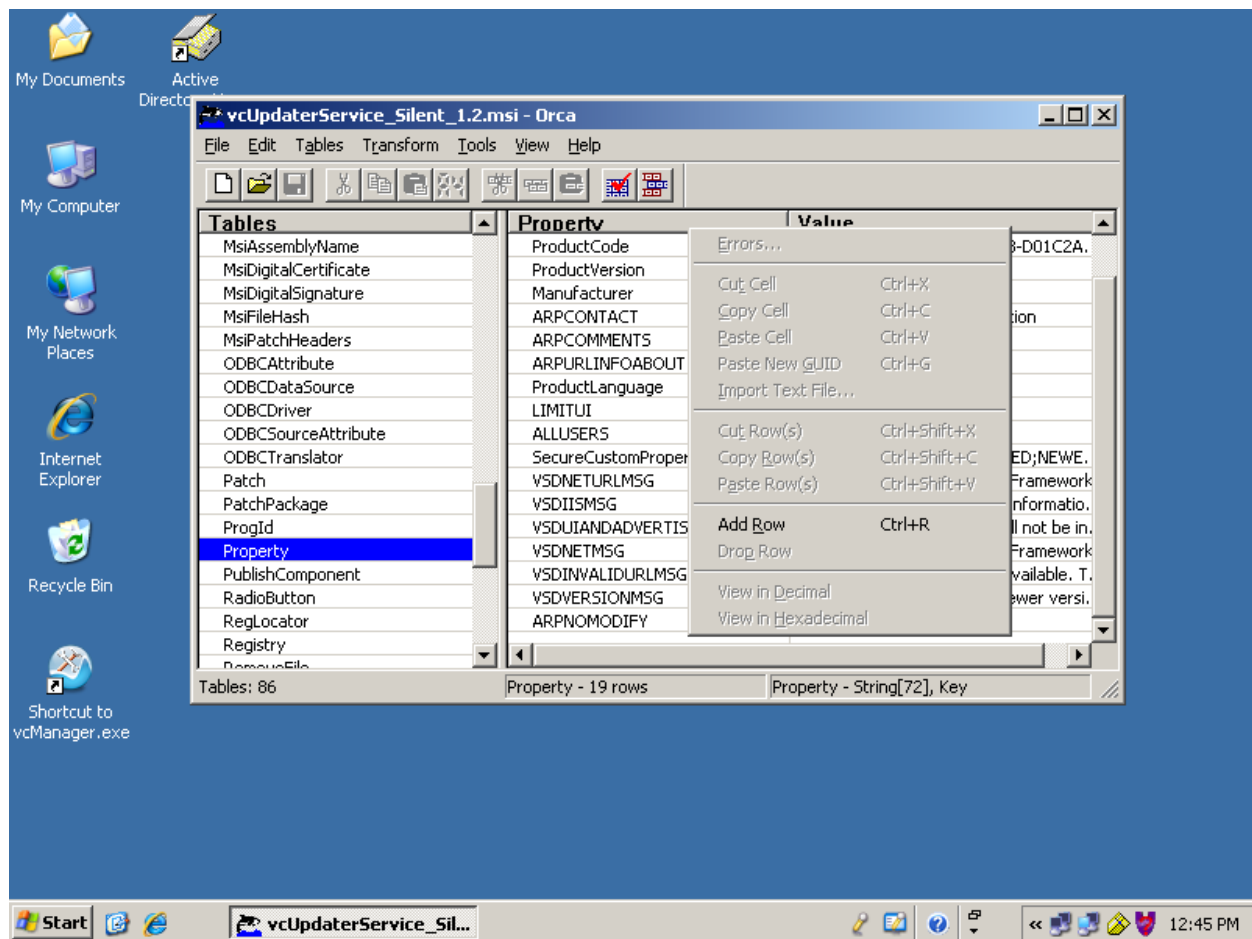


6. Select the Properties Table.

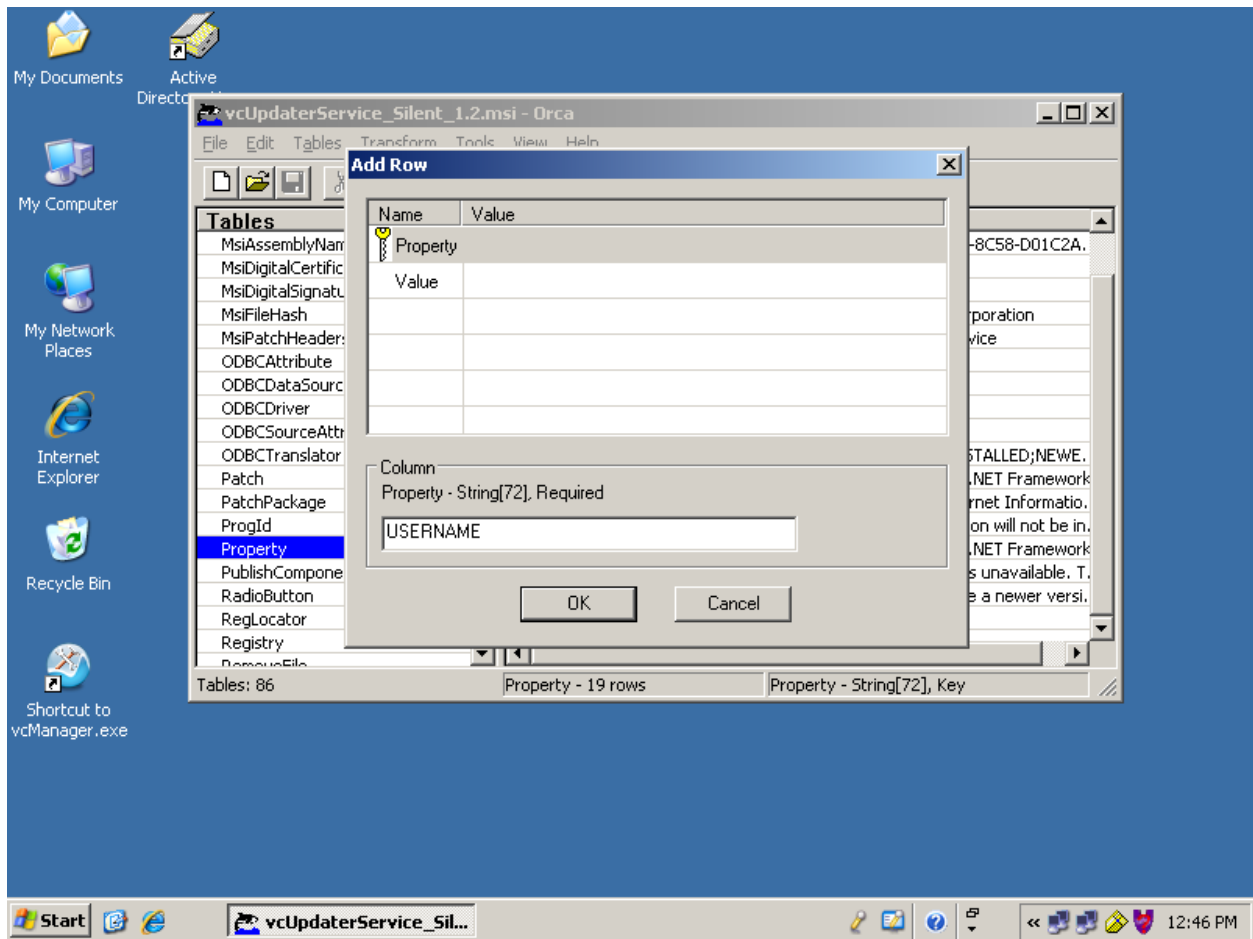




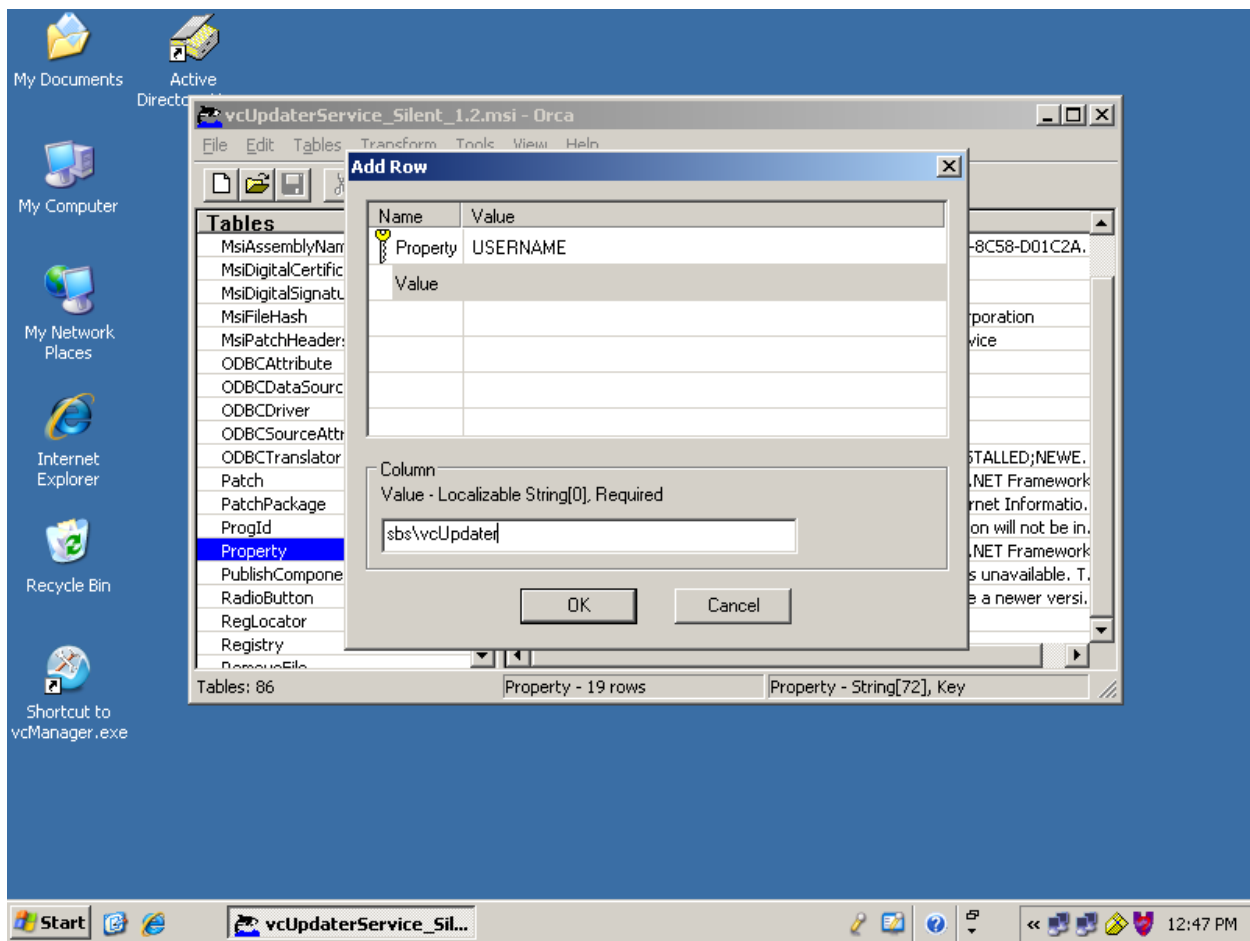
7. Scroll to the bottom of the Property Table.



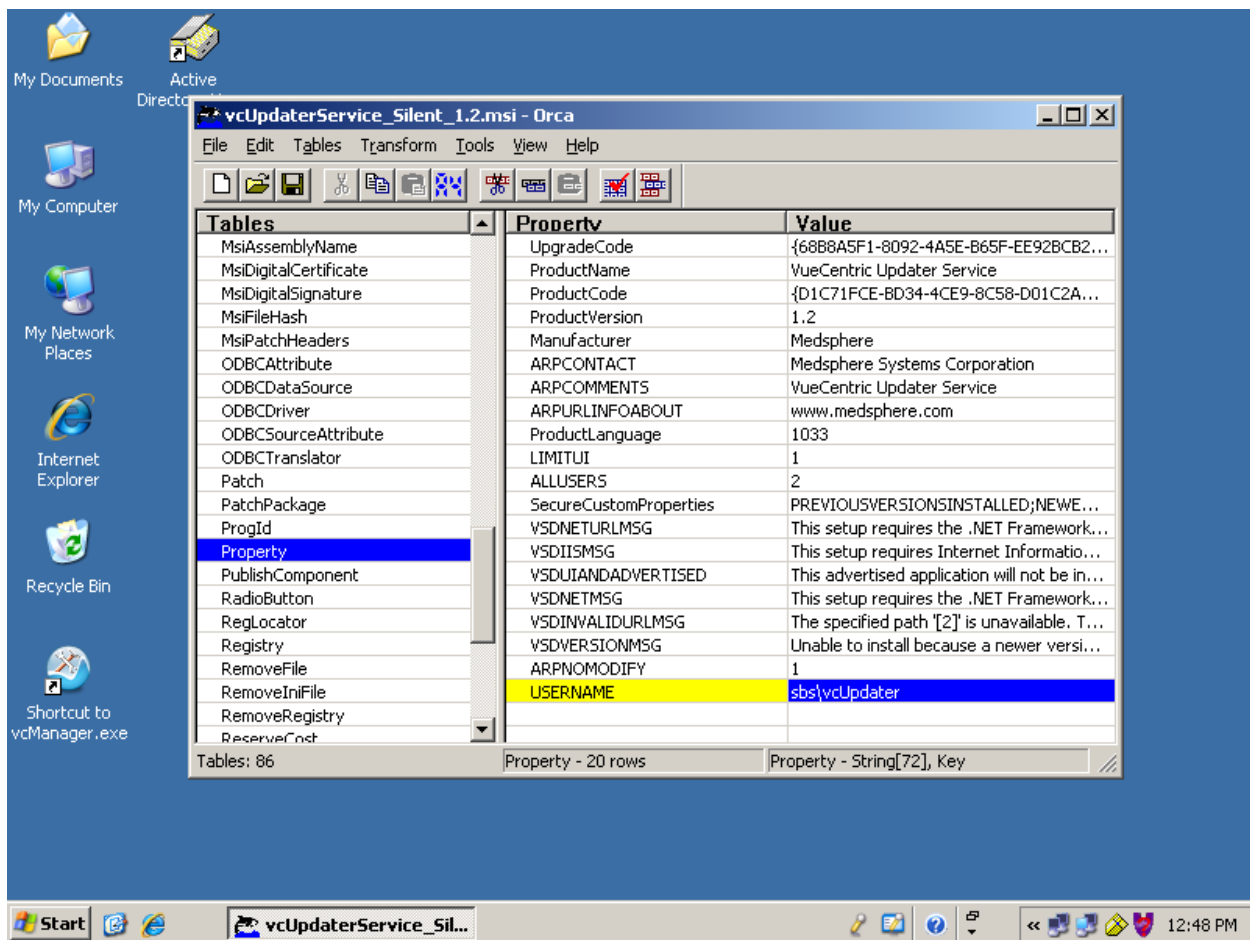
8. Right Click on the right pane and select "Add Row".



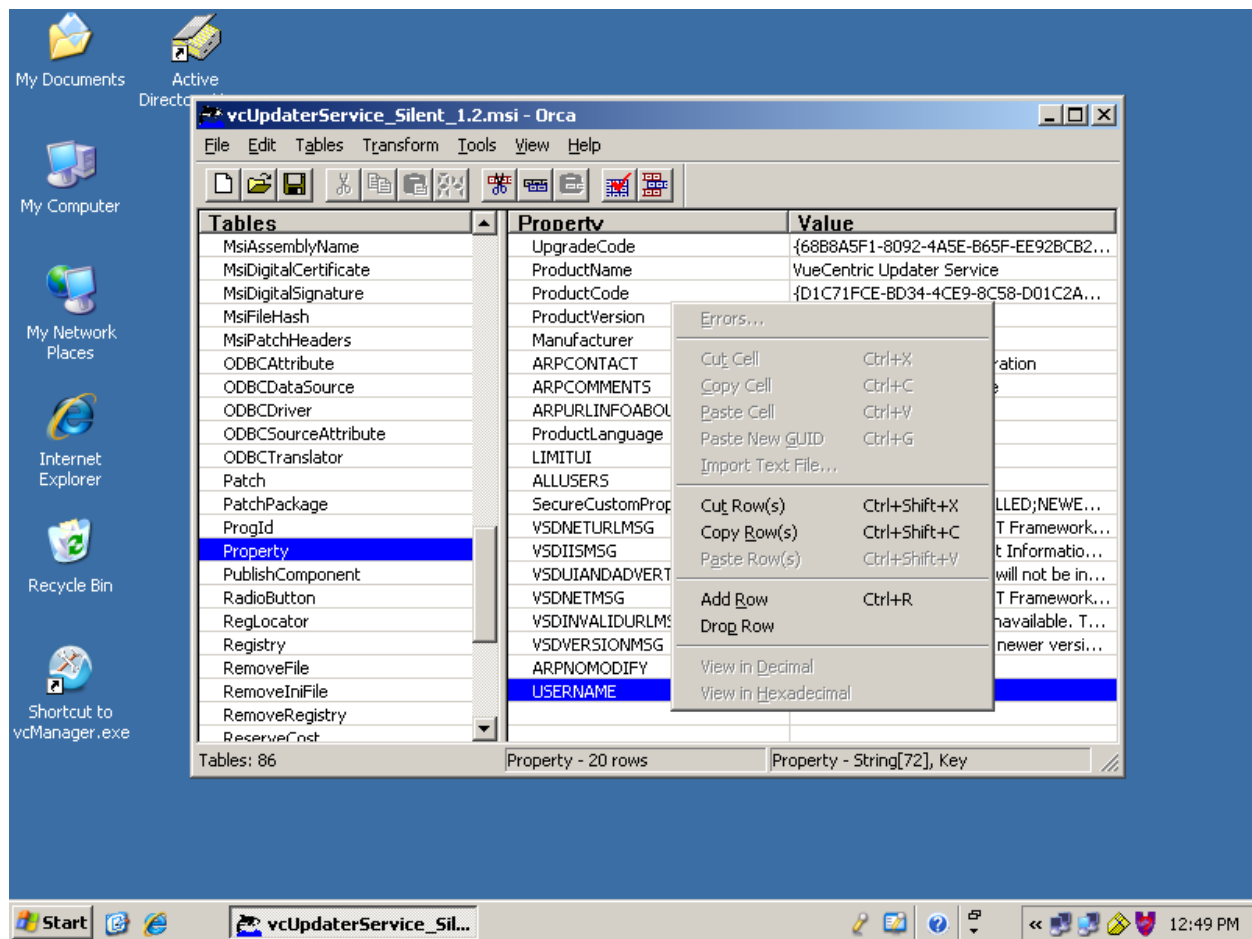
9. Type "USERNAME" and press Enter.



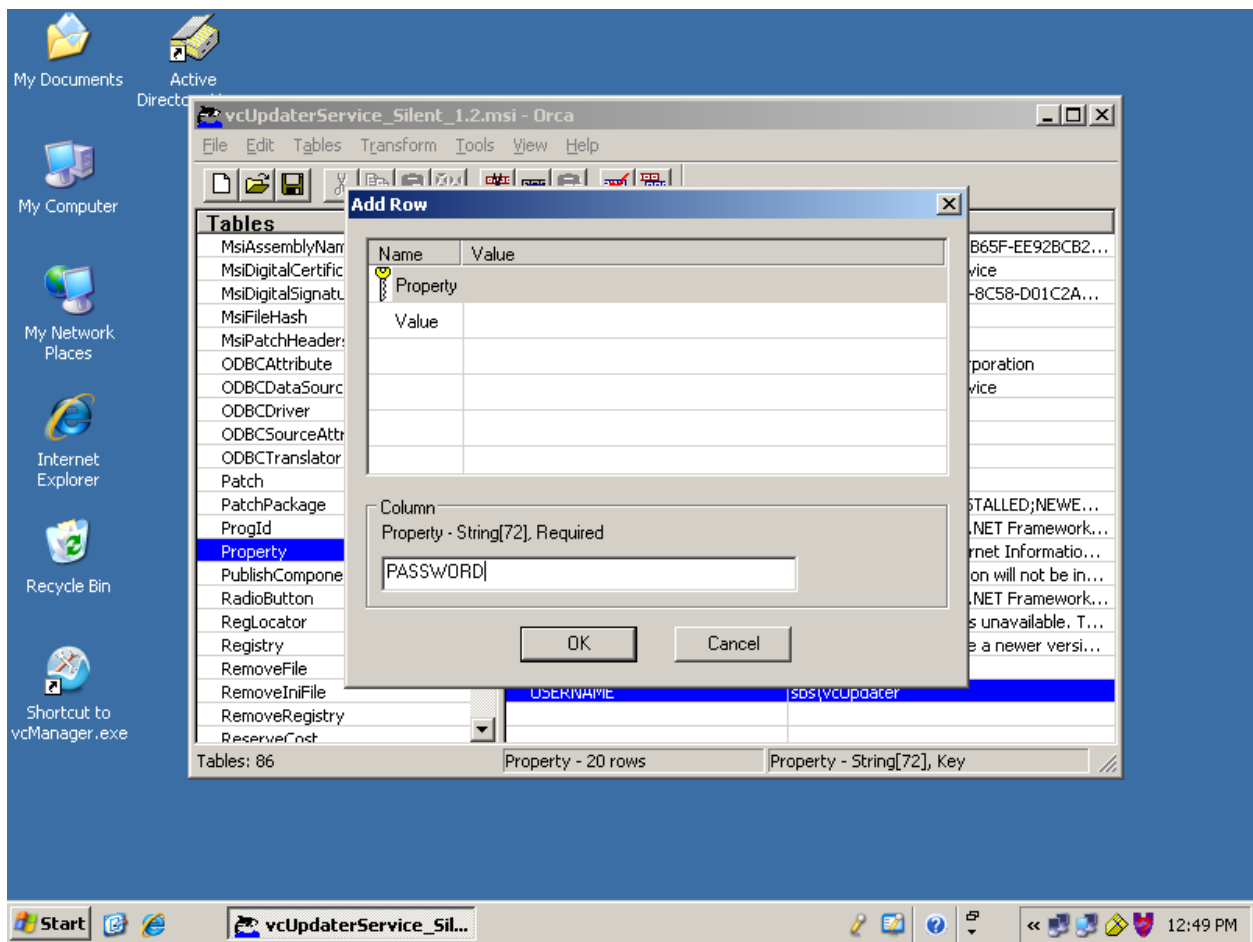
10. Type the name of the service account prefixed by the domain name and press Enter.



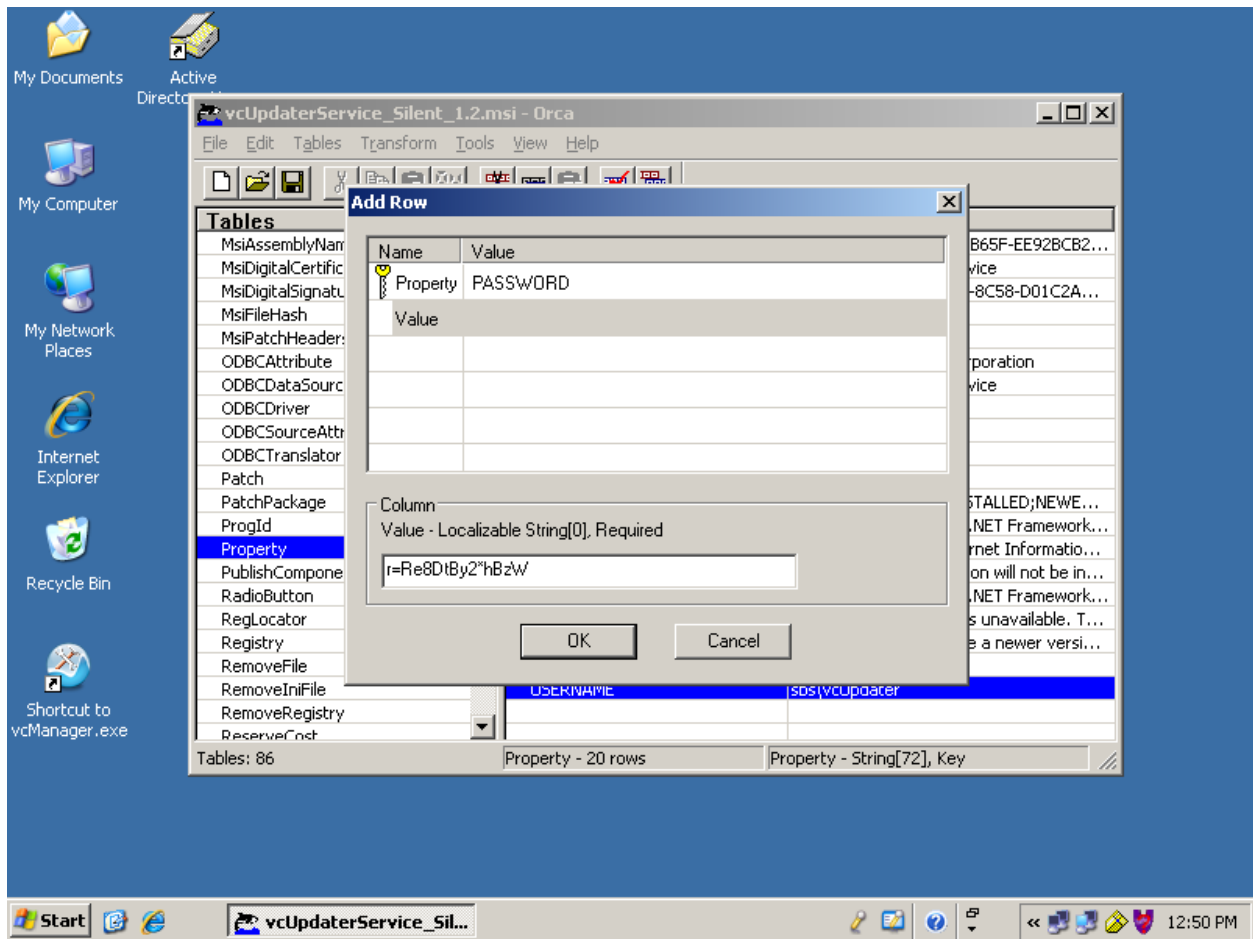
11. You have now added the username.



12. Right-click on the right pane and click "Add Row".



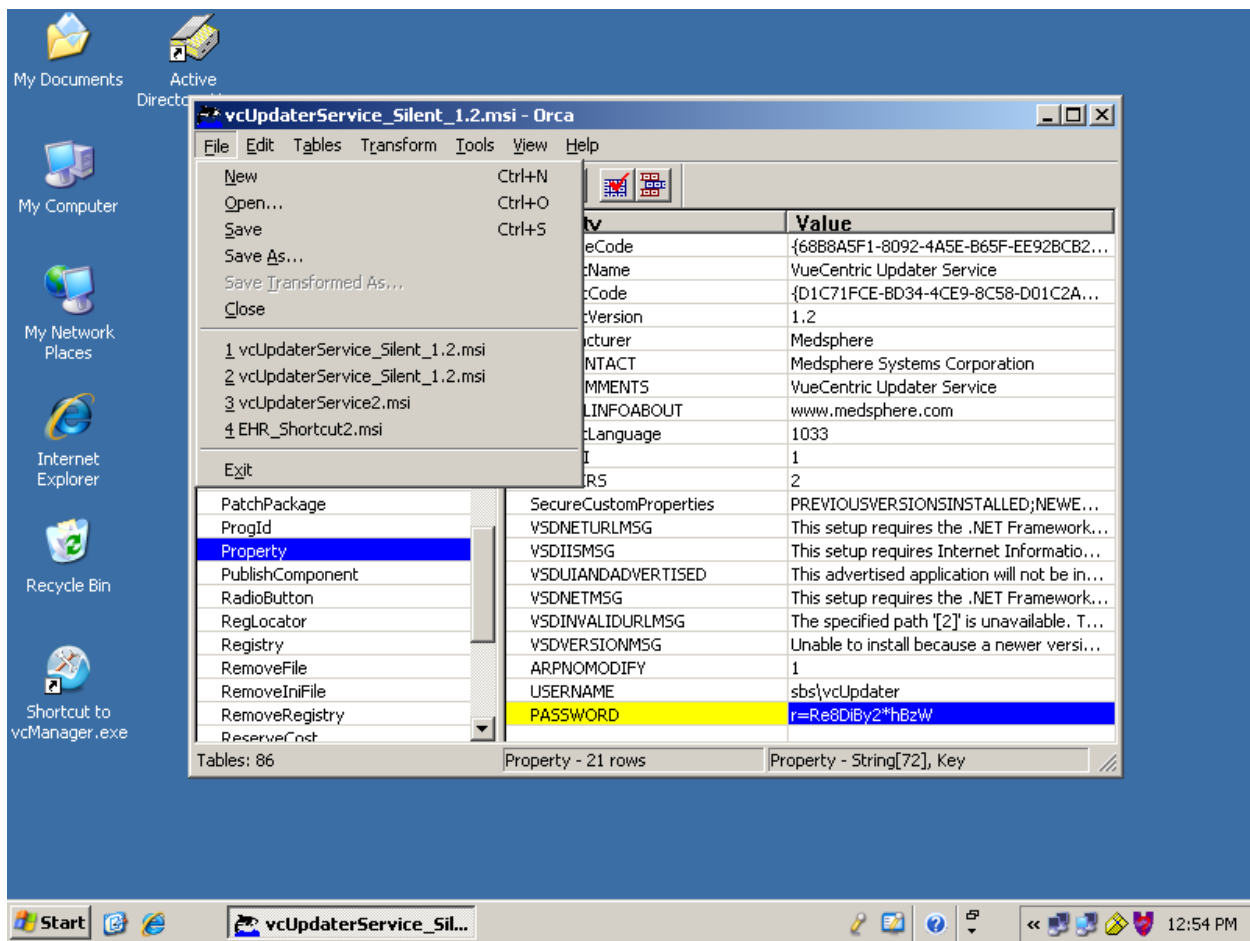
13. Enter PASSWORD and press Enter.



14. Enter the password that is assigned to the user account and press Enter.

Note: passwords are stored as clear text. Therefore, the modified msi file should be kept in a secure location. Do not leave the modified msi file in its original location as it may be overwritten by future updates.

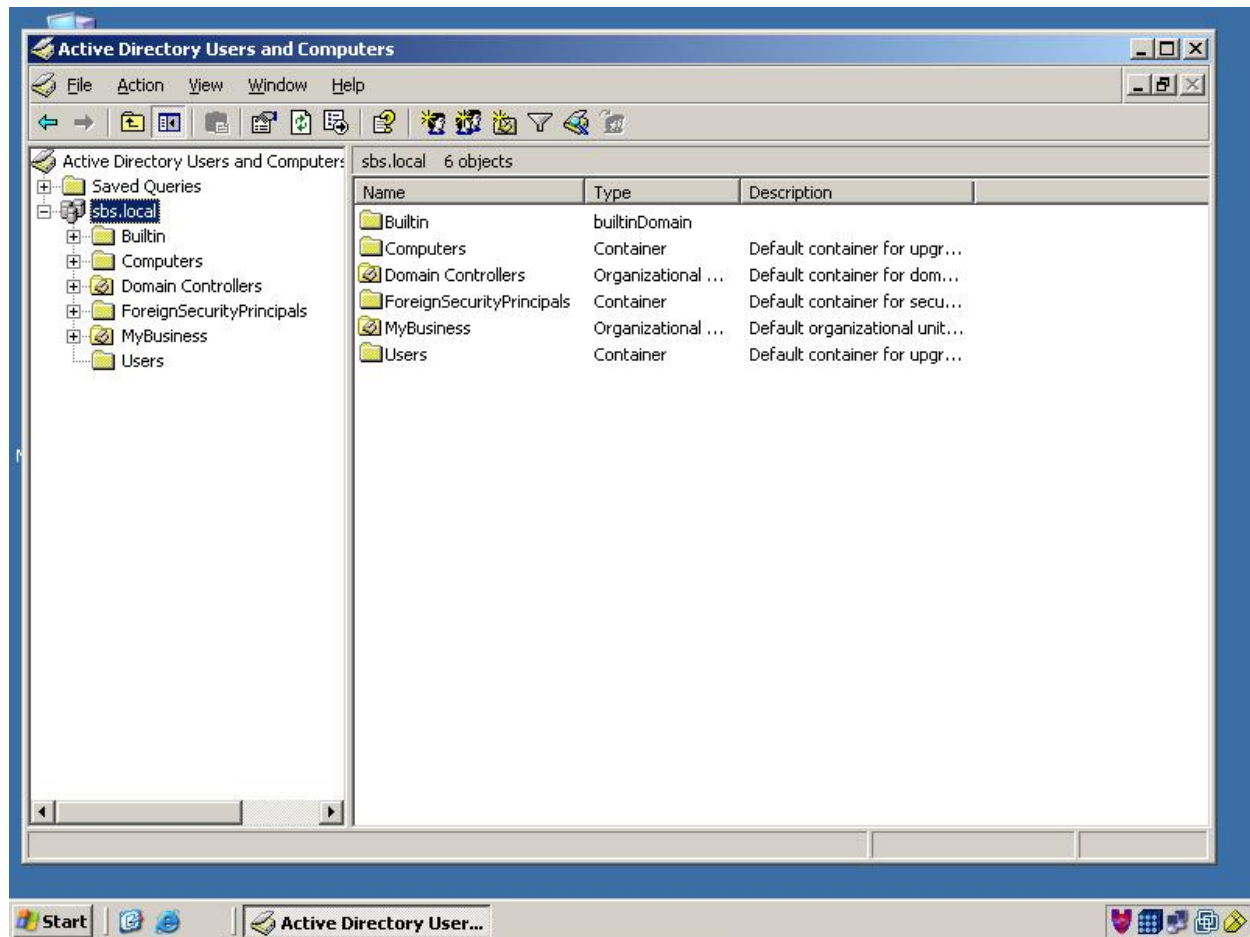




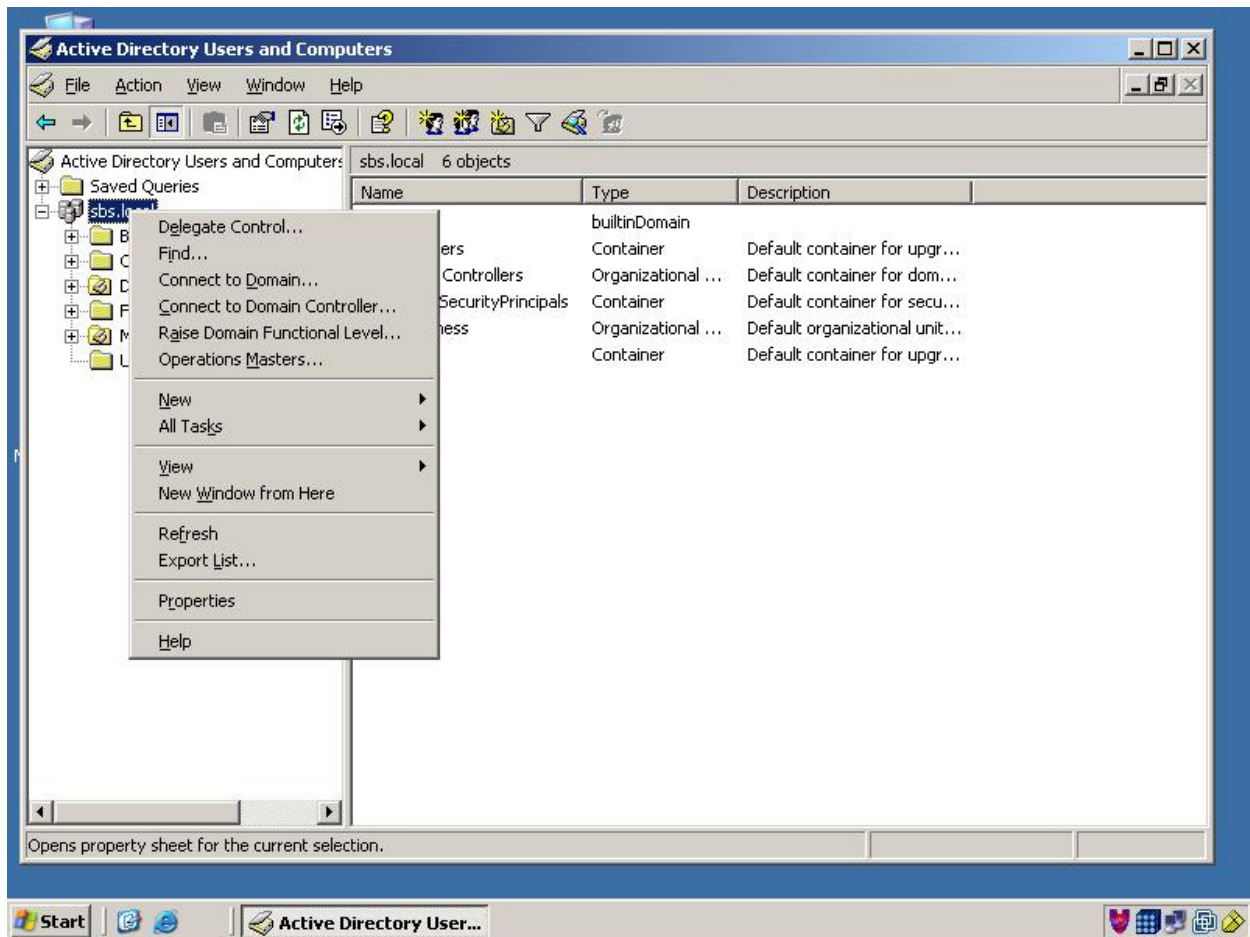
15. Click the file menu and select "Save". Then close Orca.

You have now readied the msi file with the necessary settings for unattended installation.

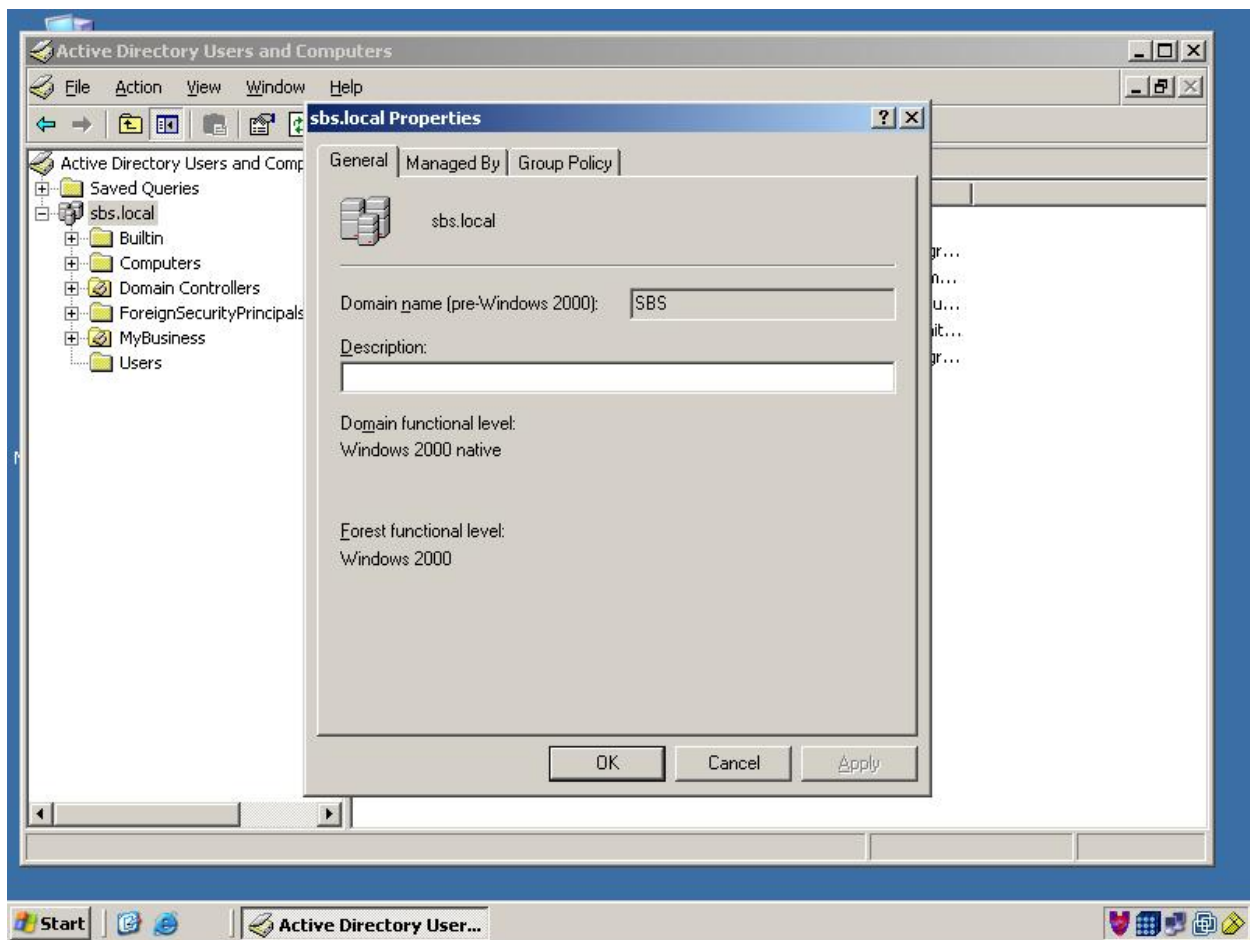
### C. Deploy the vcUpdaterService\_Silent\_x.y.msi via Group Policy



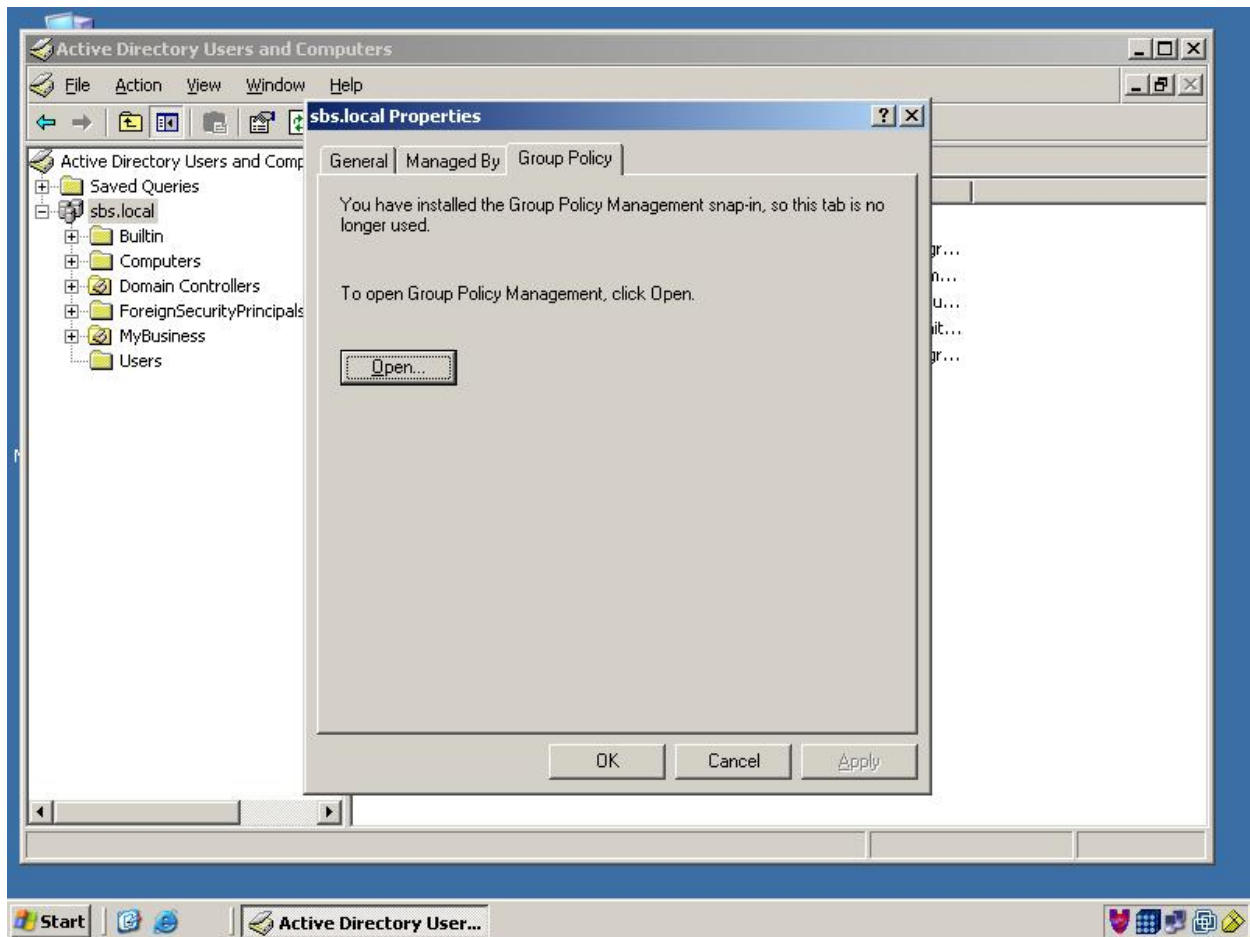
1. Open Active Directory Users and Computers.



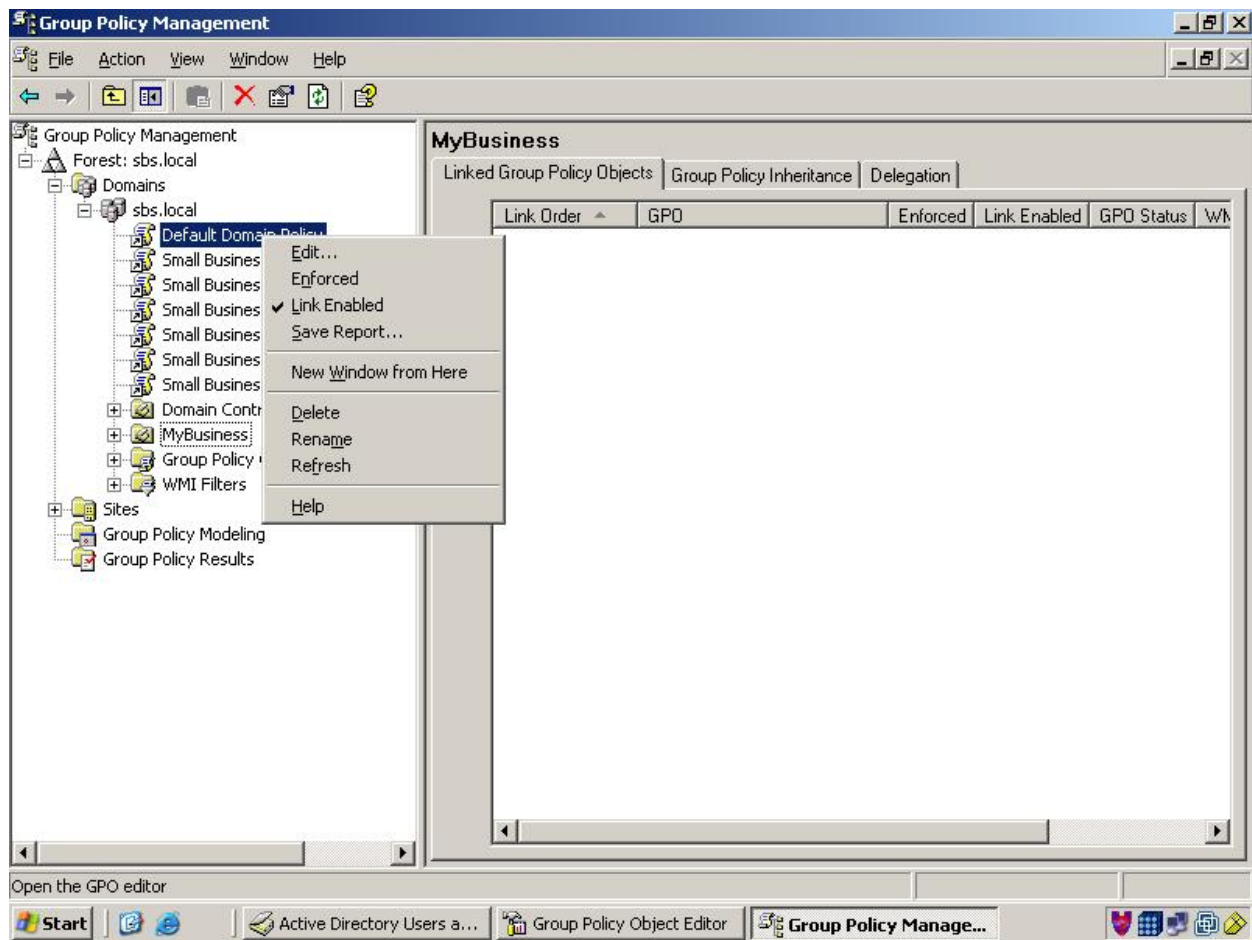
2. Right-click on the domain or OU that should have the service deployed and select properties.



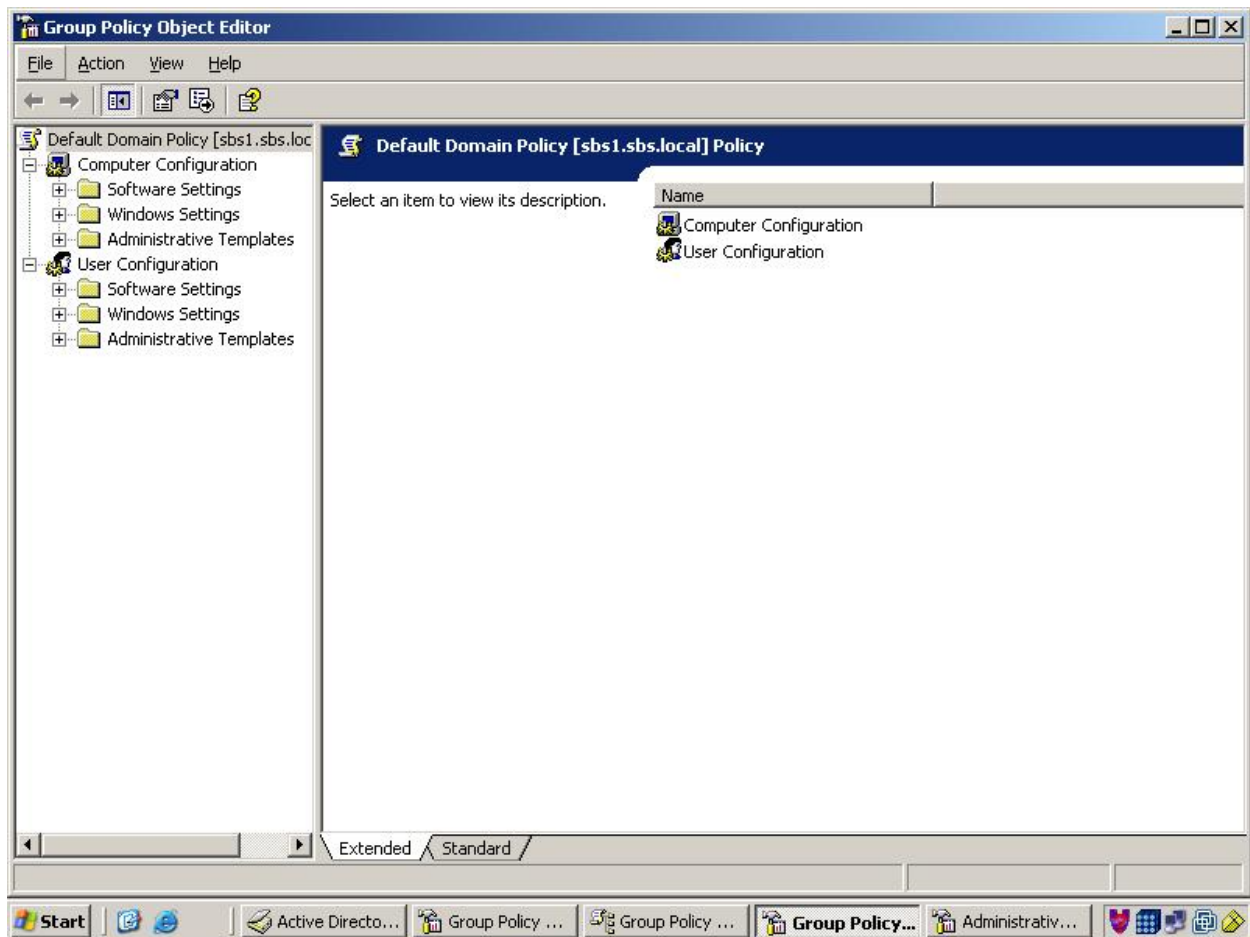
3. Click on the "Group Policy" tab.



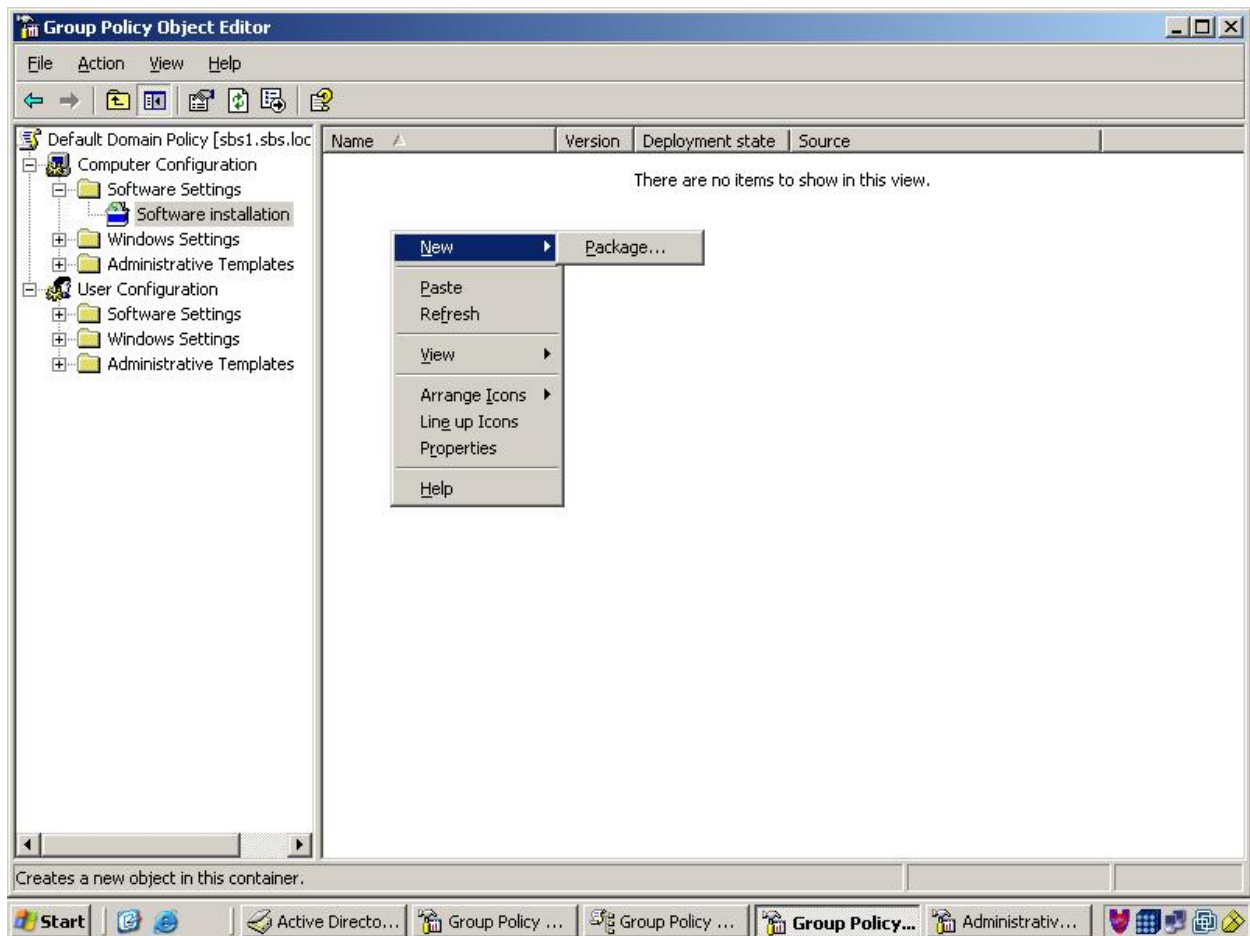
4. Click "Open".



5. Right-click an existing policy and click edit or create a new policy. Dismiss any informational dialogs that may appear.

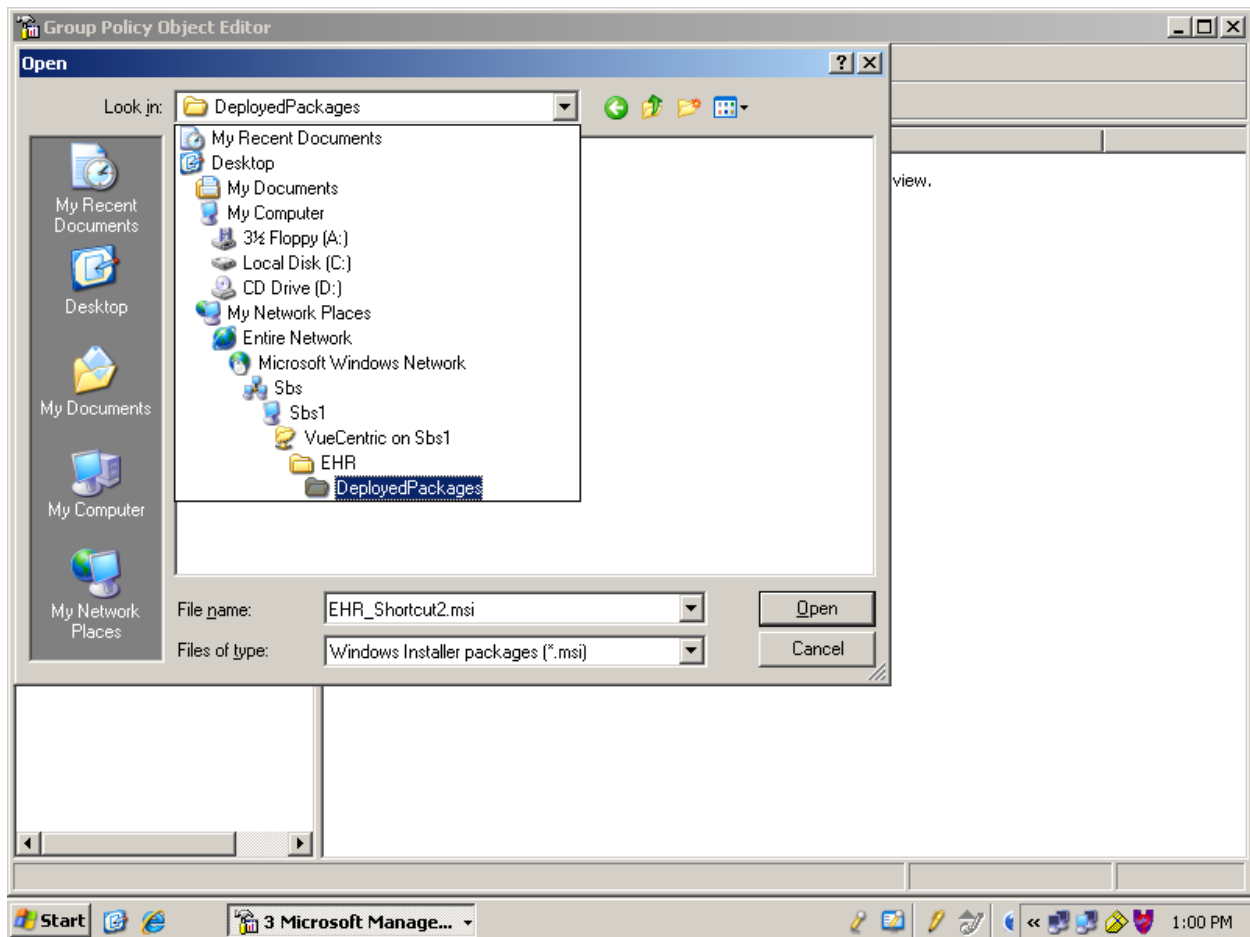


6. Expand the "Software Settings" folder under "Computer Configuration". Select "Software Installation".

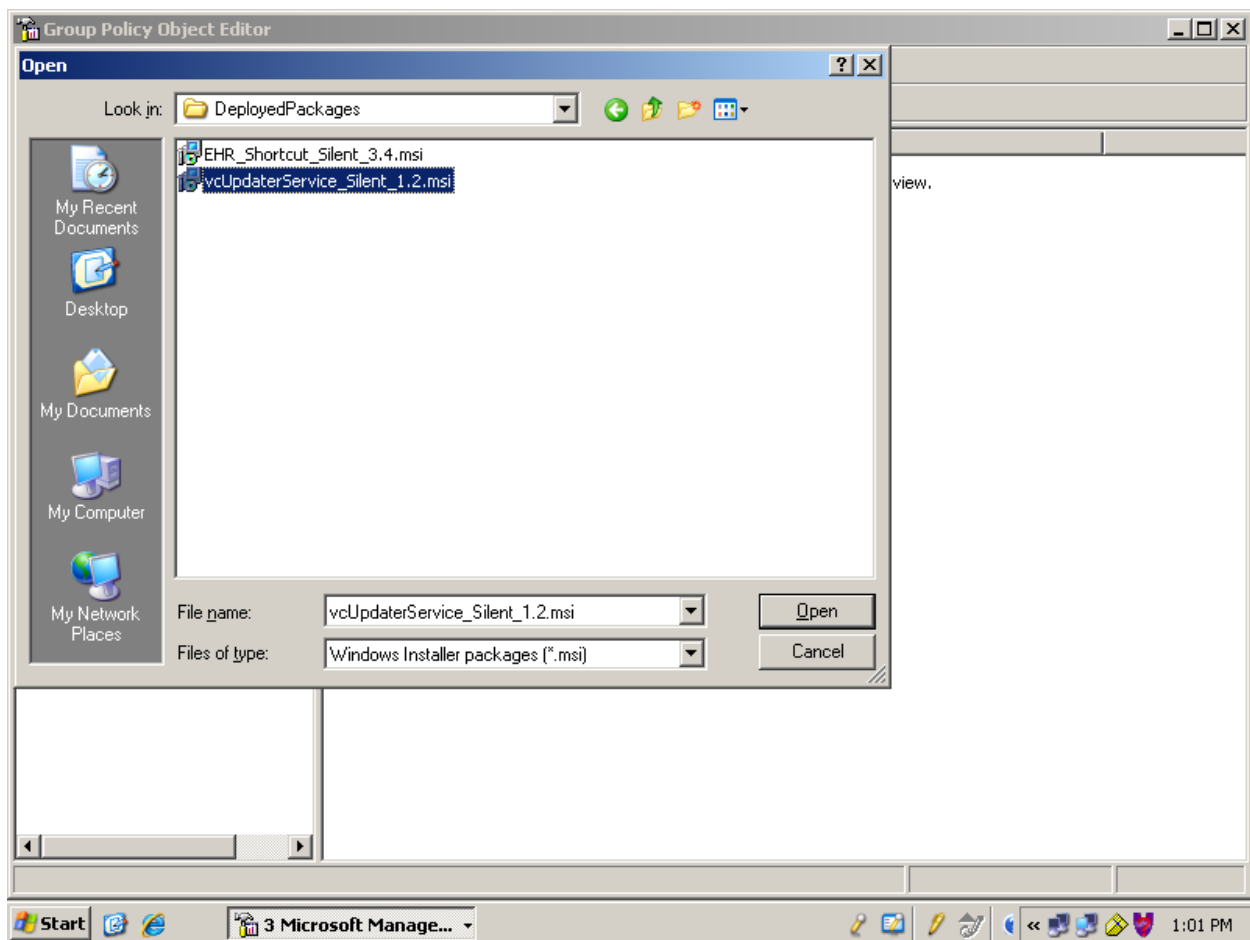


7. Right-click in the right pane and click "New", then click "Package".

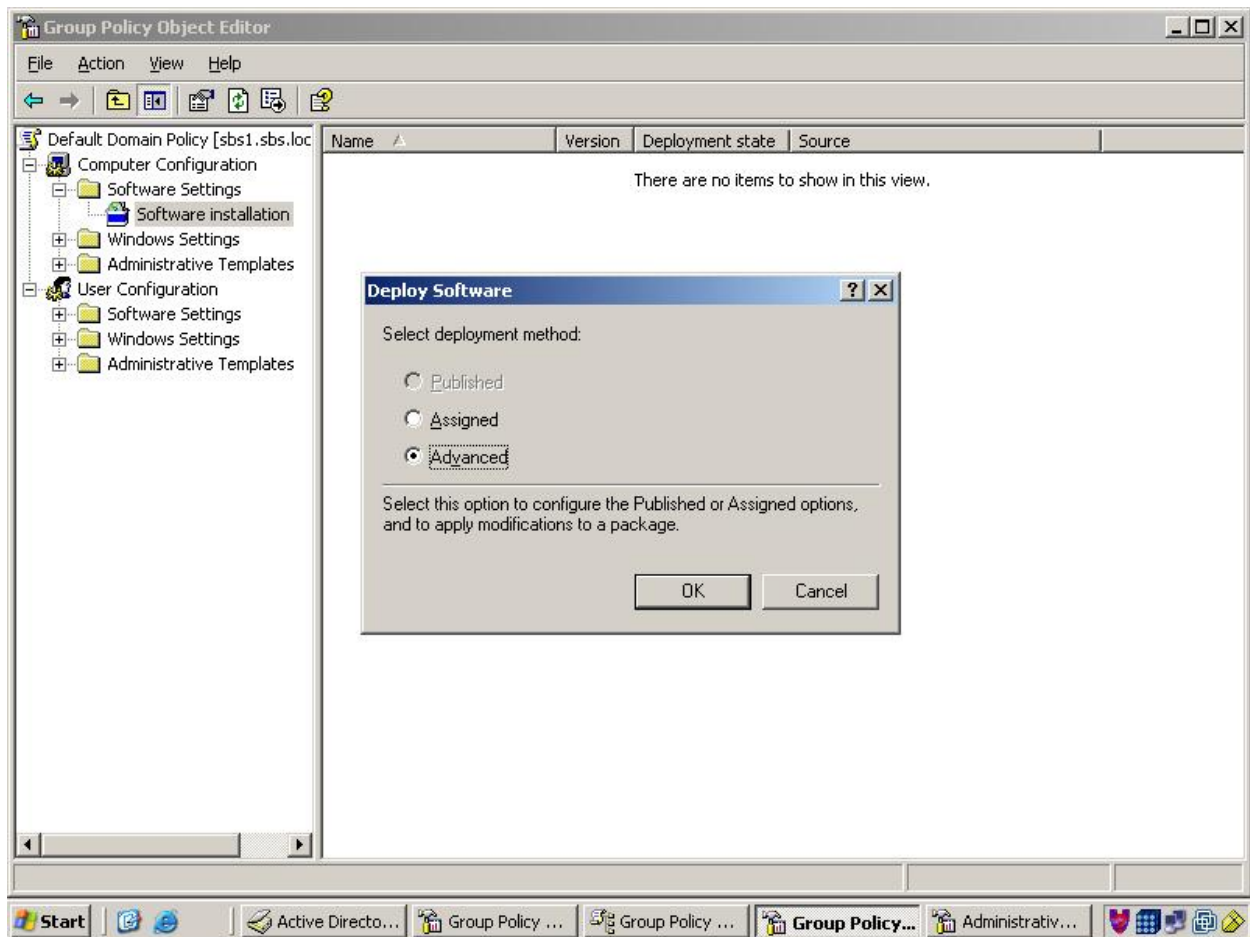




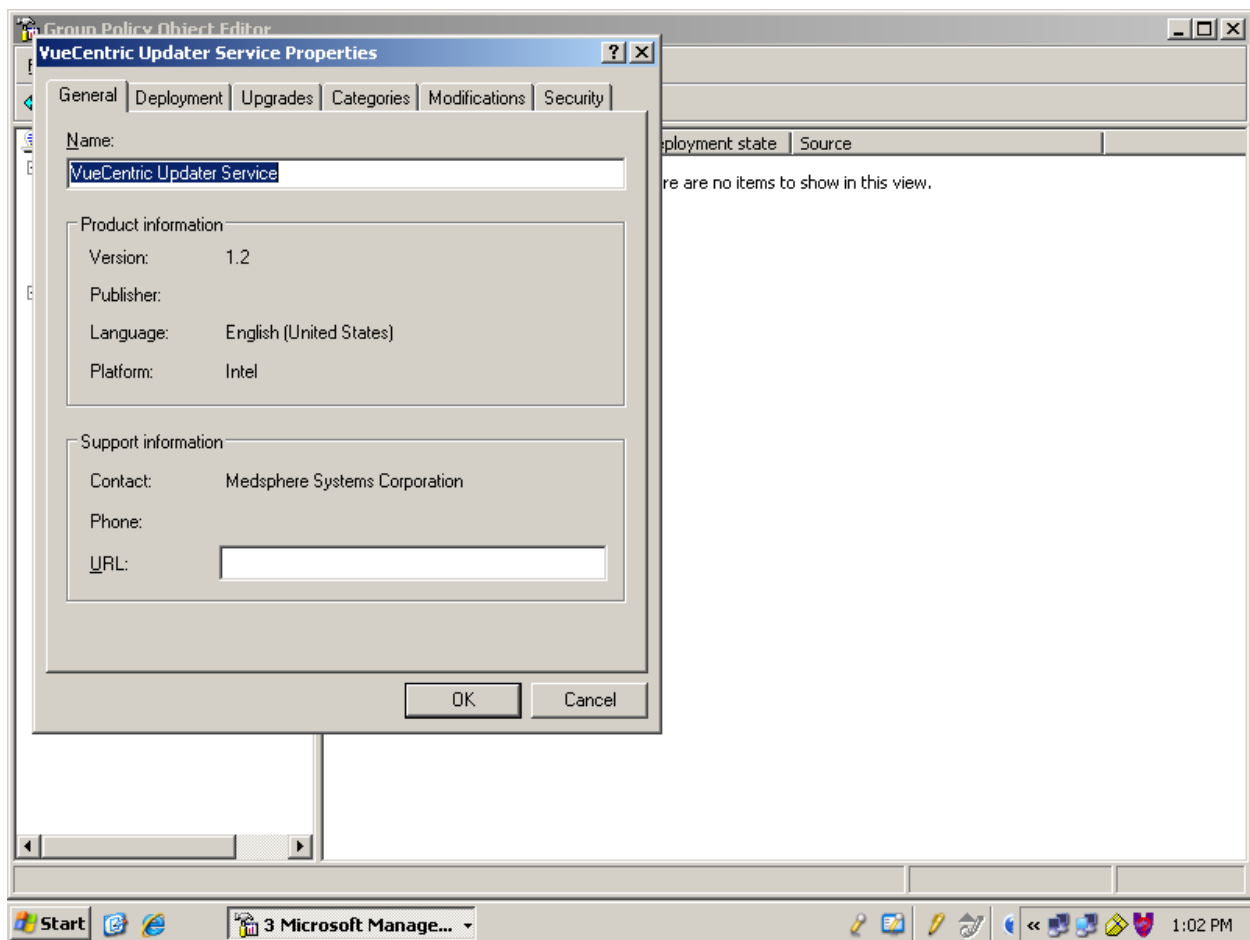
8. Browse to the UNC path of where the modified `vcUpdaterService_Silent_x.y.msi` was copied. Be sure to use a UNC path name. Do not use local drive designations. Do not deploy the modified msi file from its original location as future updates may overwrite it.



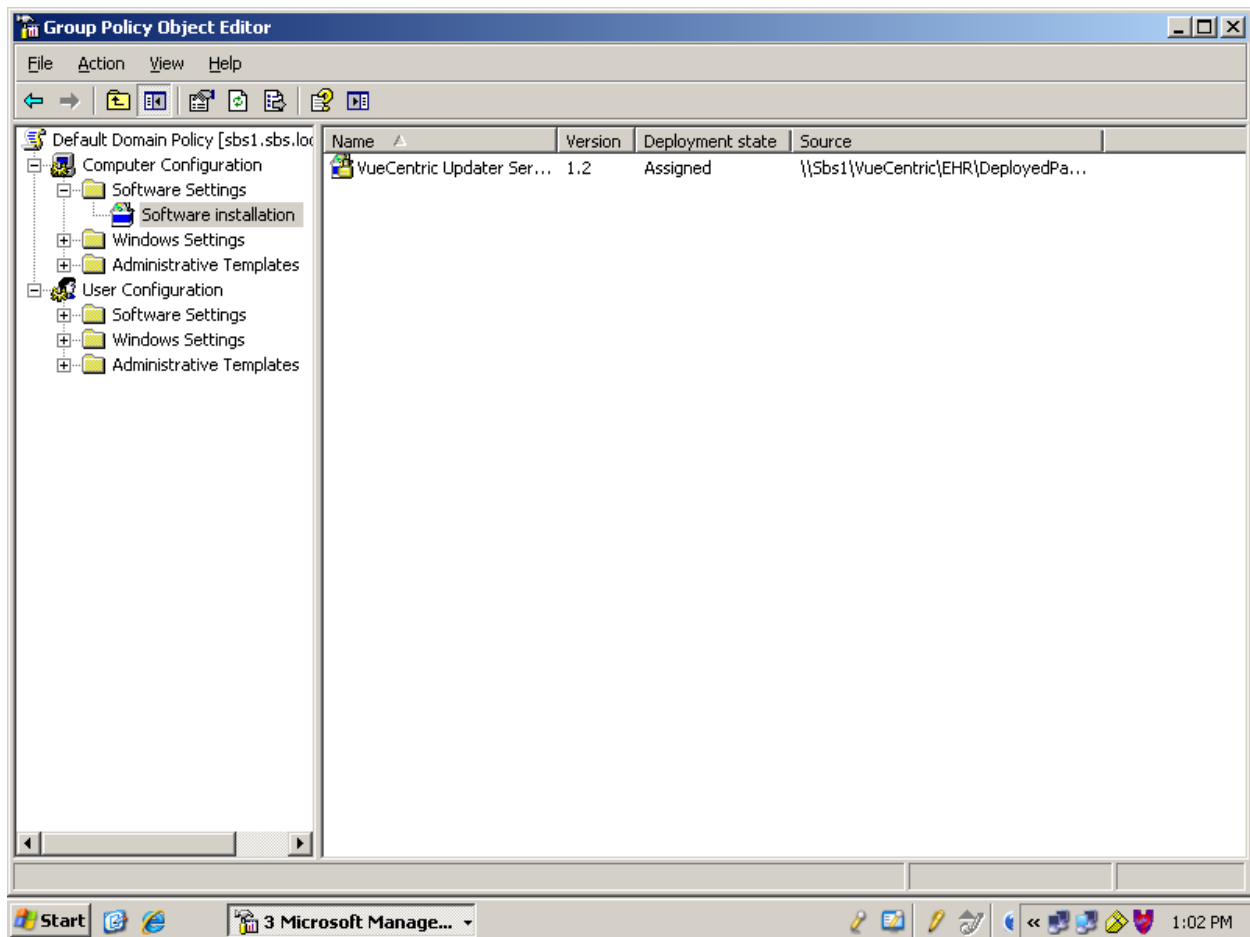
9. Select the modified vcUpdaterService\_Silent\_x.y.msi. Click "Open".



10. Select "Advanced" and click "OK".



11. Click "OK".

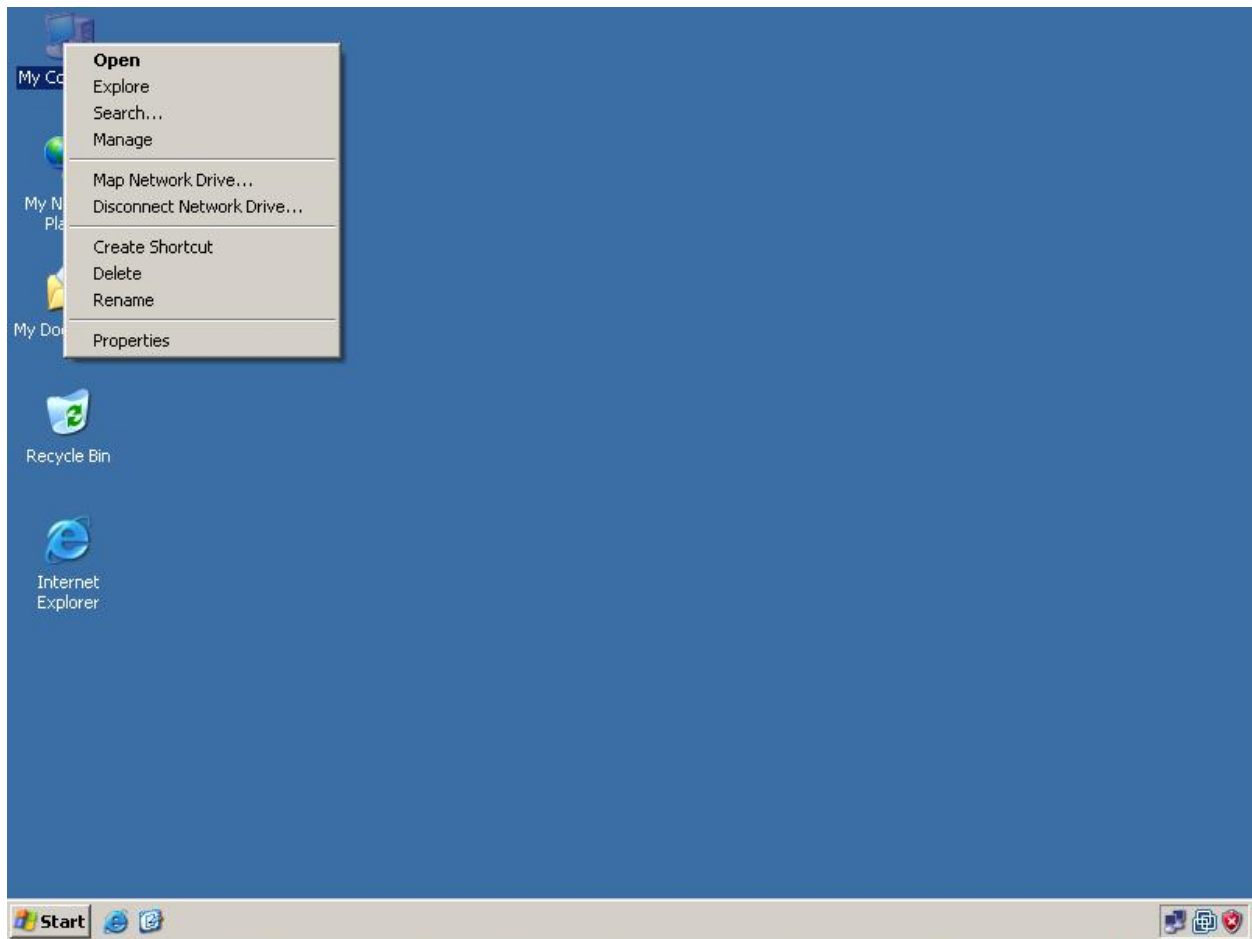


12. The package is now queued for deployment.

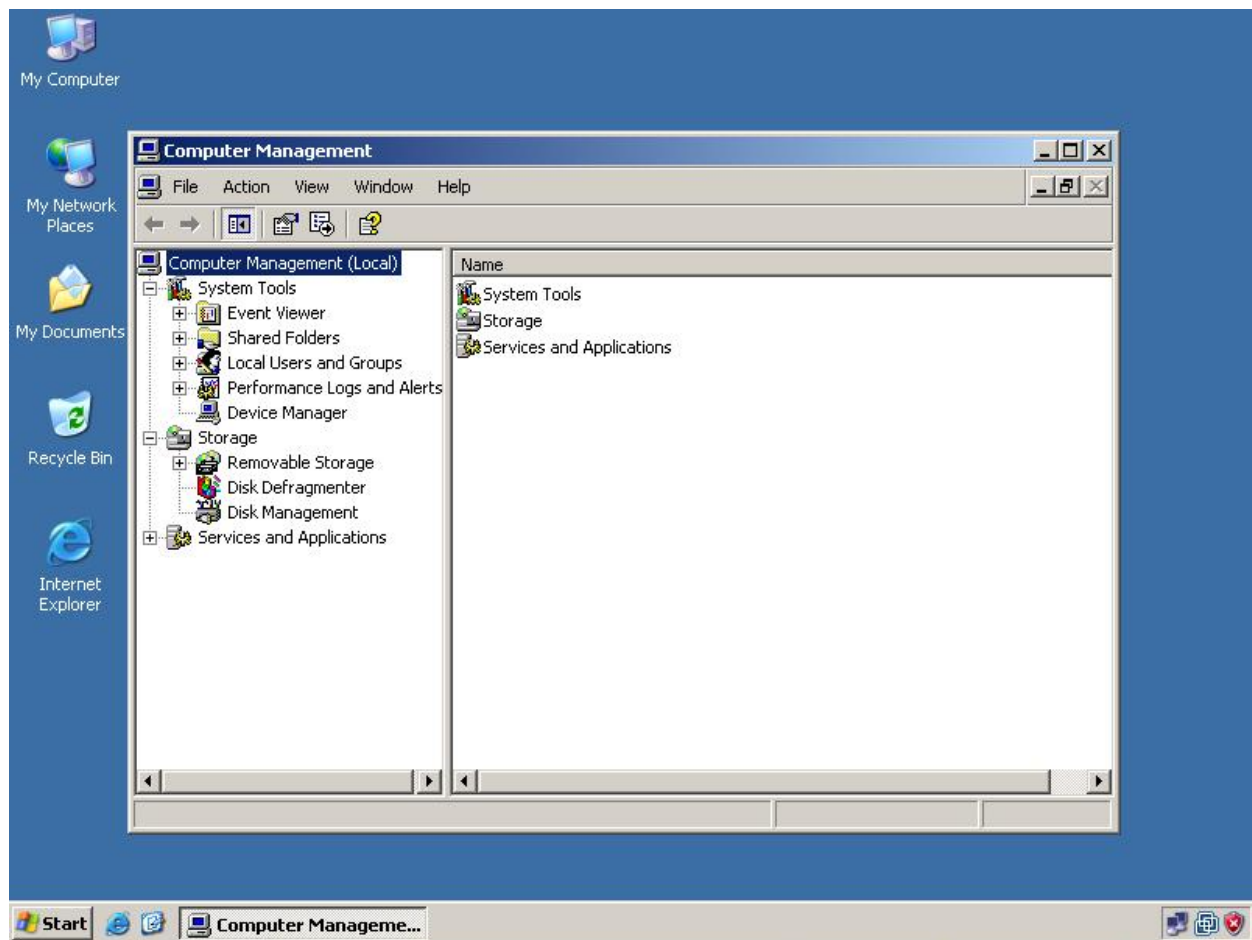
#### D. Verify vcUpdaterService\_Silent\_x.y.msi deployment on Client



1. Deployment via group policy may take several hours to complete. To force an immediate installation, simply reboot a selected workstation that is a member of the designated domain or OU. Then follow the procedure below.

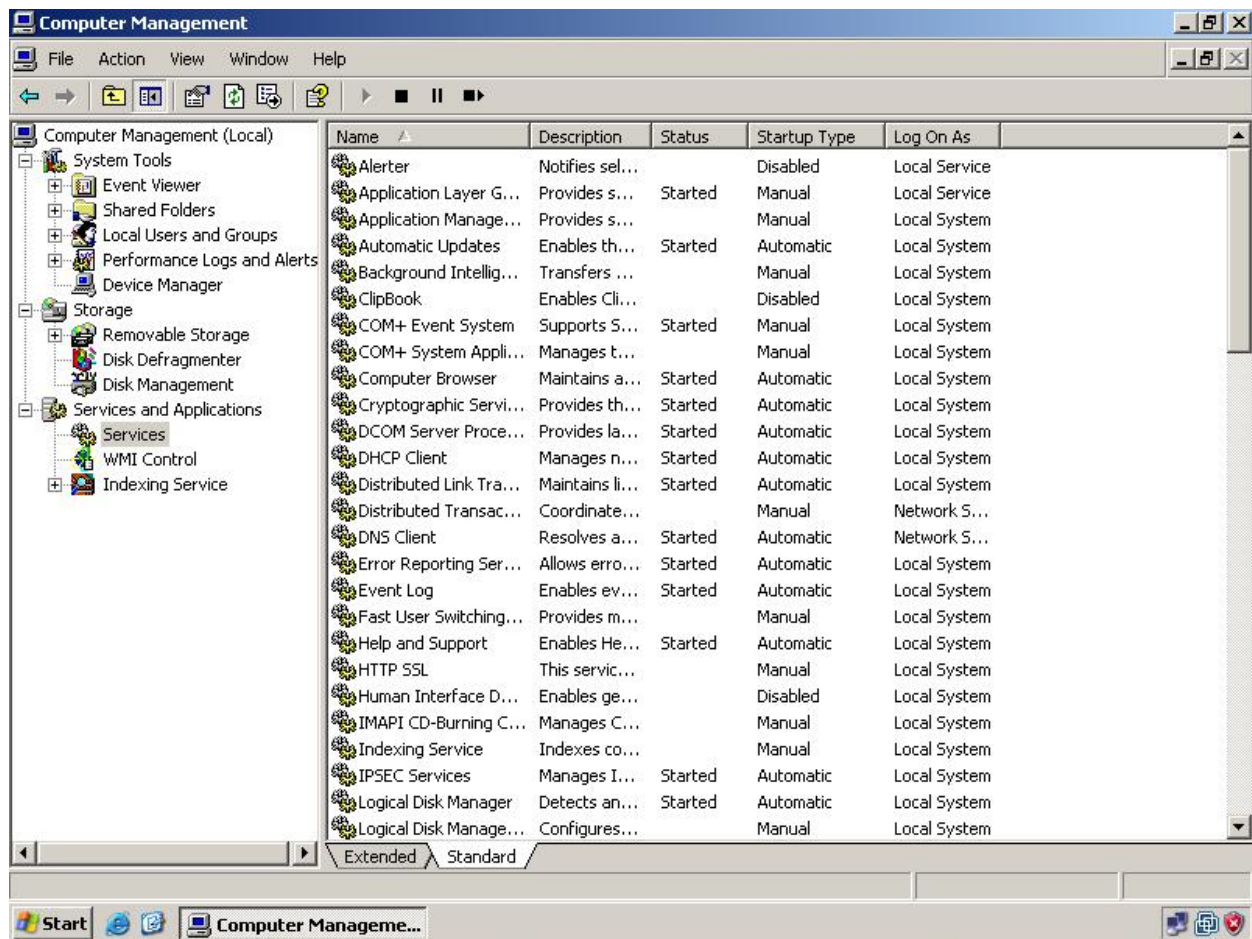


2. On a client workstation, right-click on "My Computer" and click "Manage".

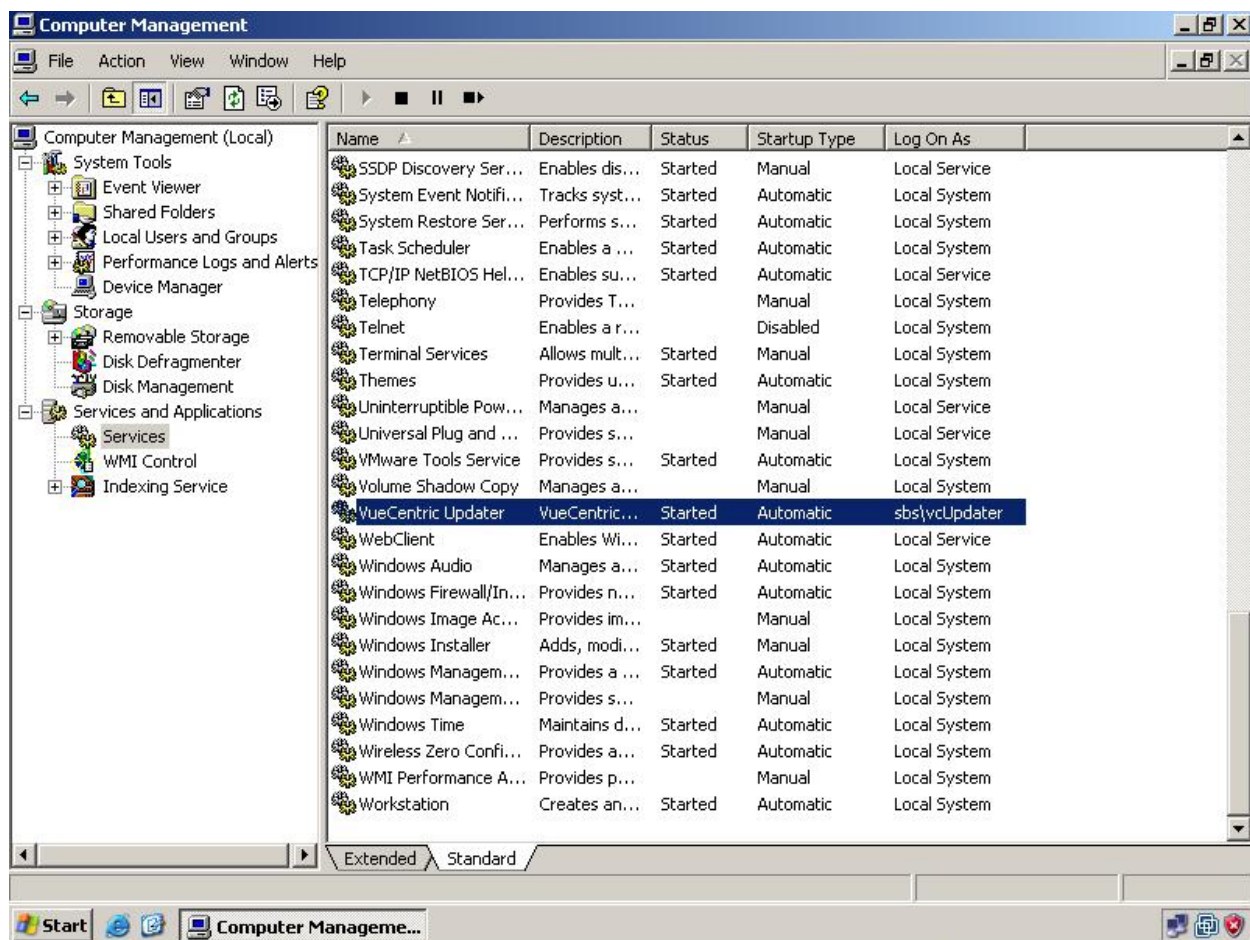


3. Expand "Services and Applications" and then expand "Services".





4. Scroll down in the services list to the entry labeled VueCentric Updater.

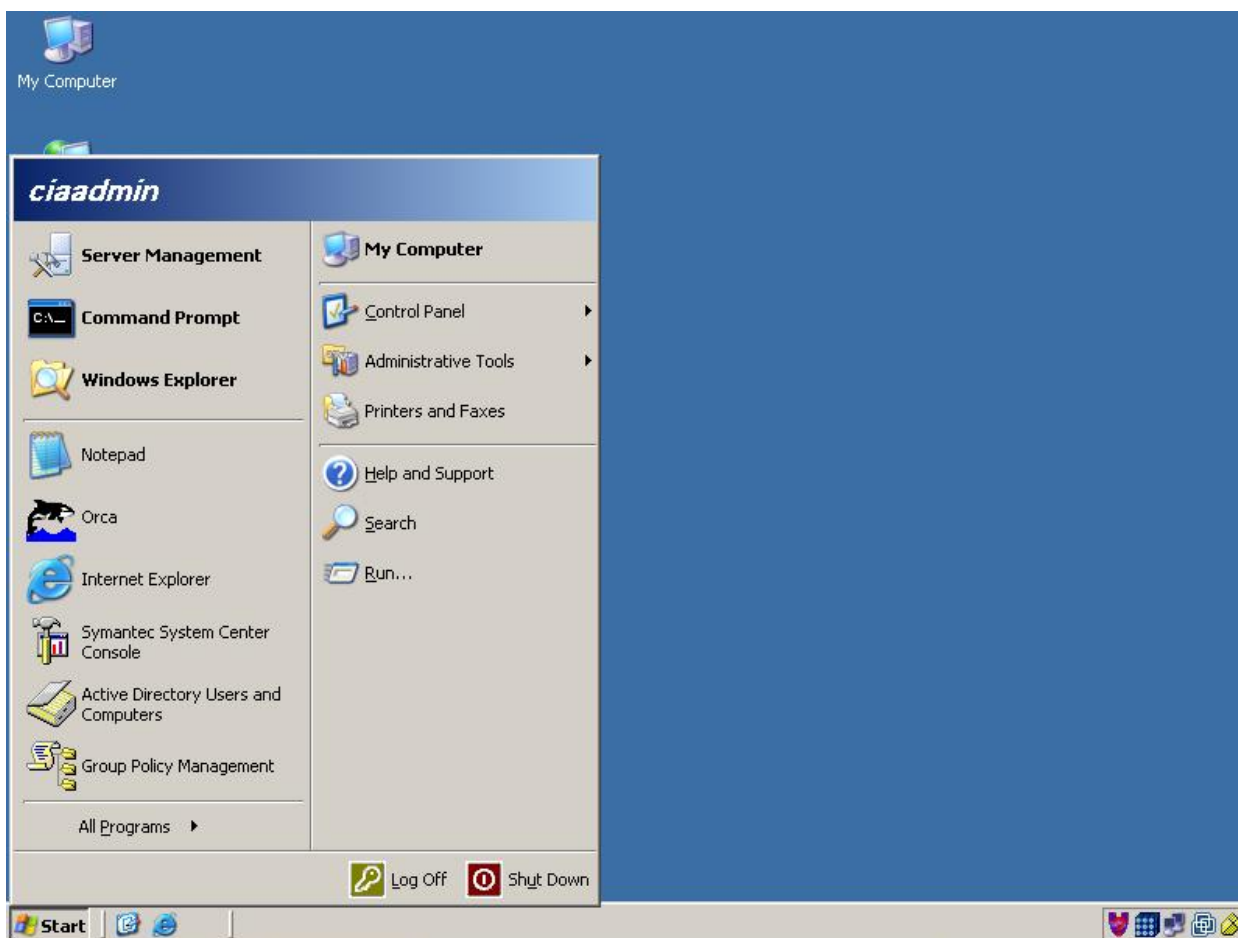


5. Verify that the VueCentric Updater Service is set to Automatic, it is started, and that it is running under the correct account.

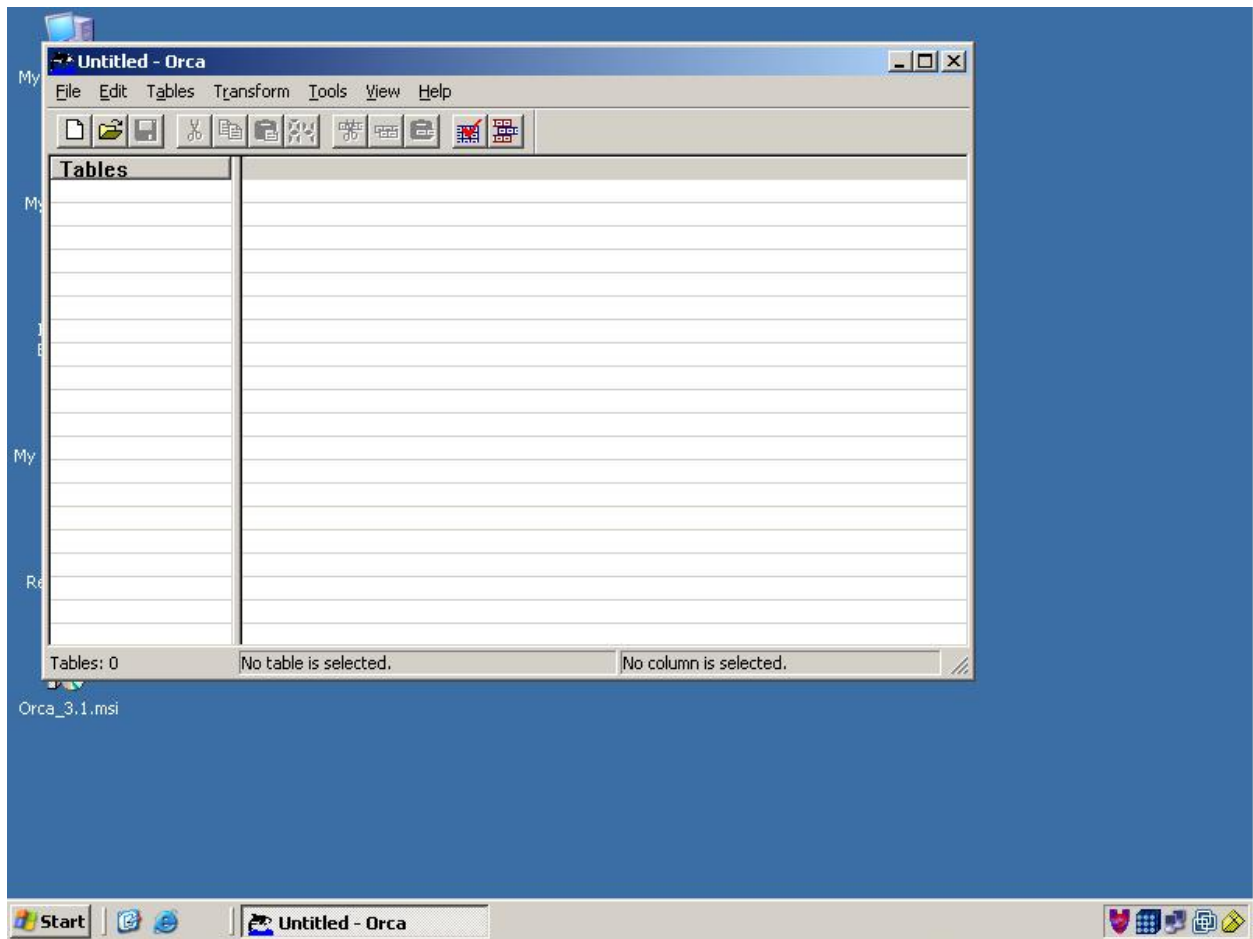
### III. Deploy the EHR Shortcut

For sites that have already deployed the EHR shortcut, this step is optional.

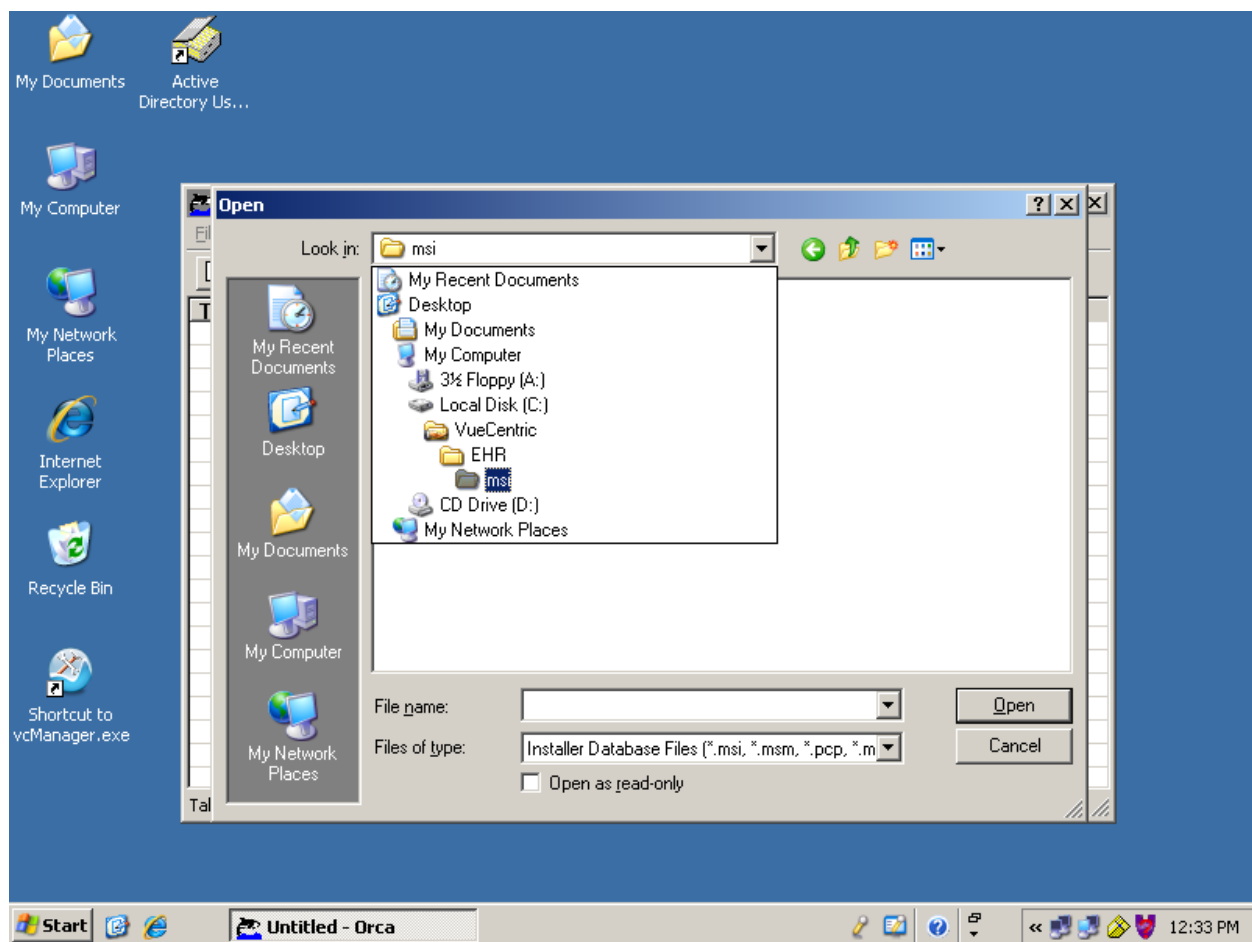
#### A. Modify the EHR\_Shortcut\_Silent\_x.y.msi Properties Table using Orca



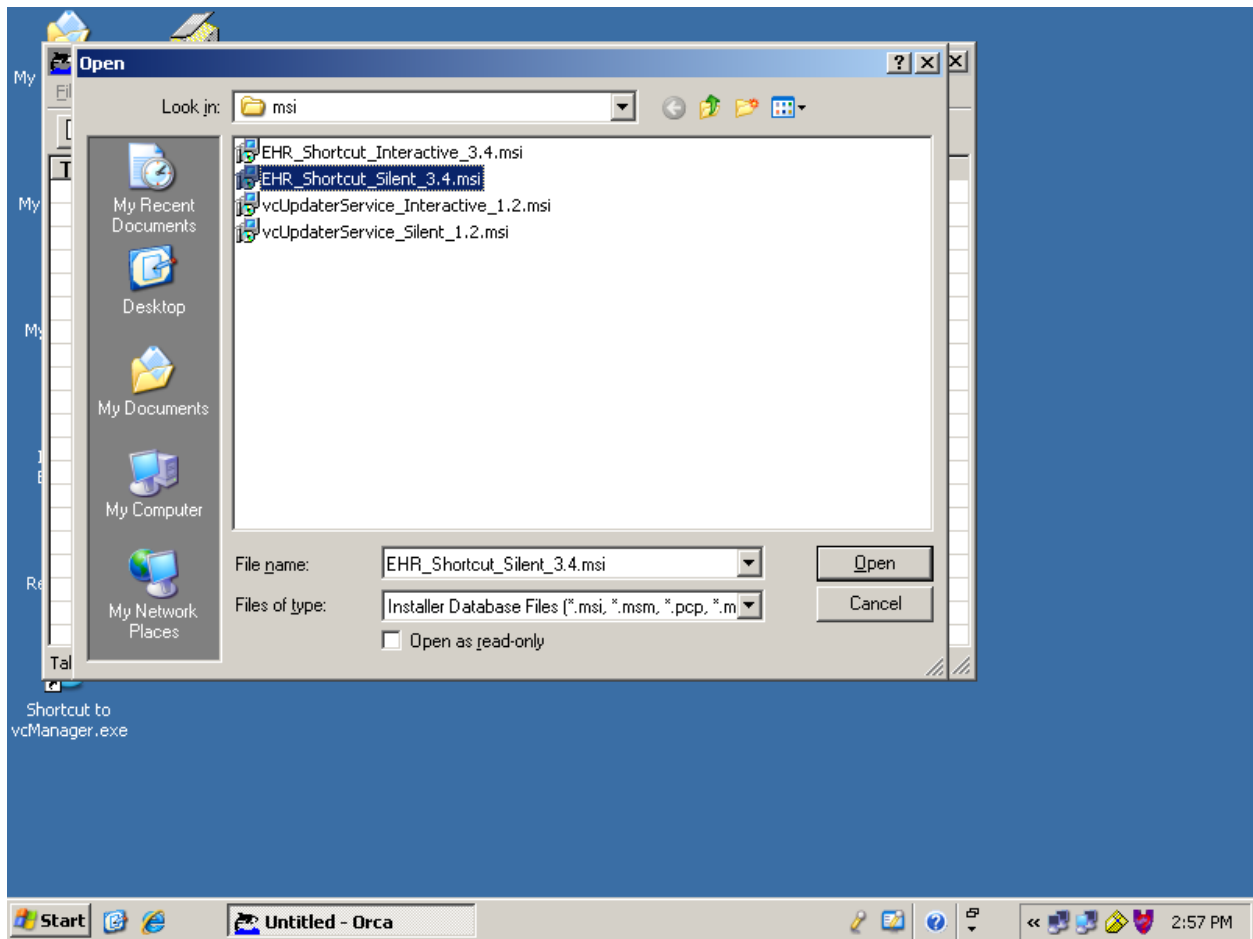
1. Open Orca.



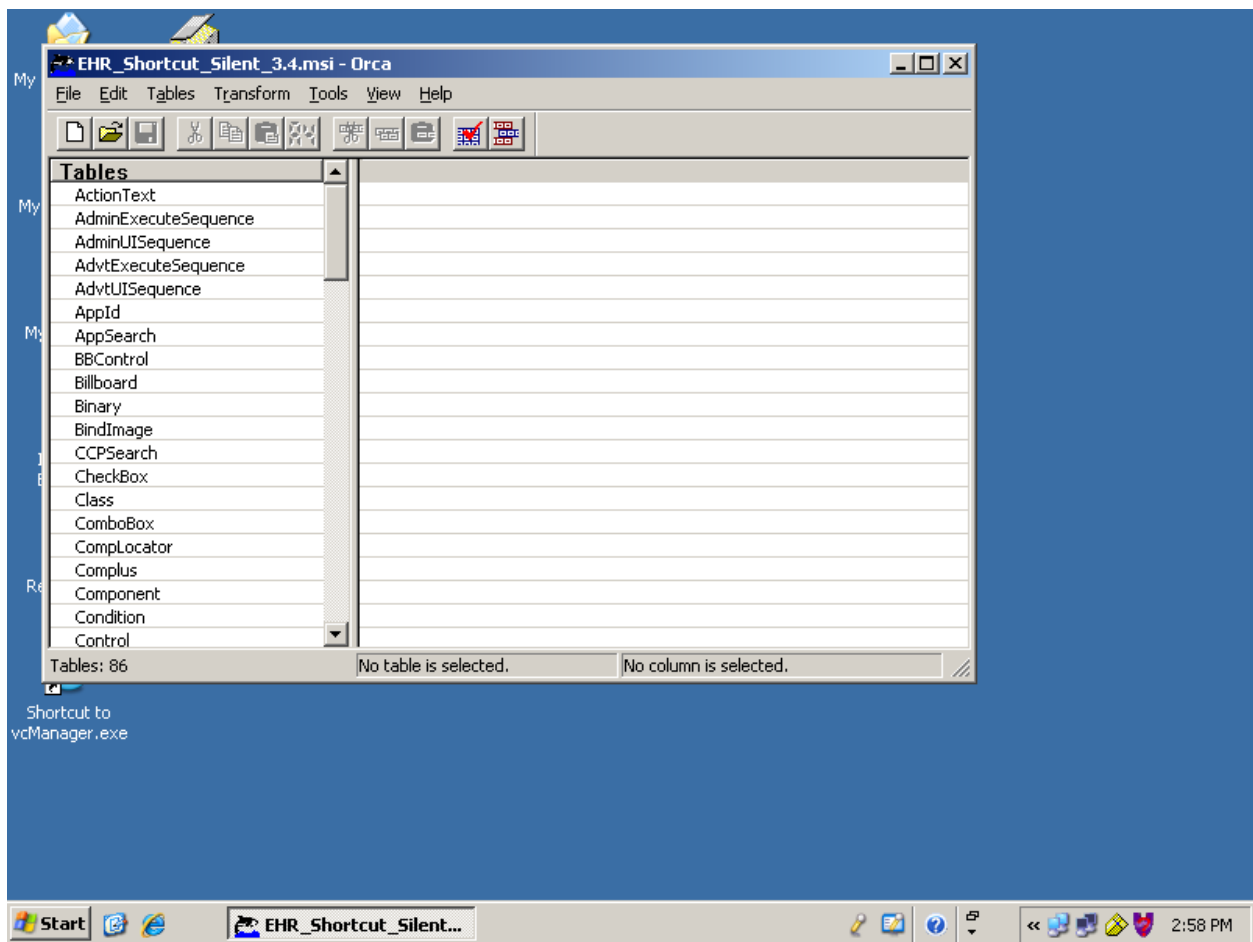
2. Click the open folder.



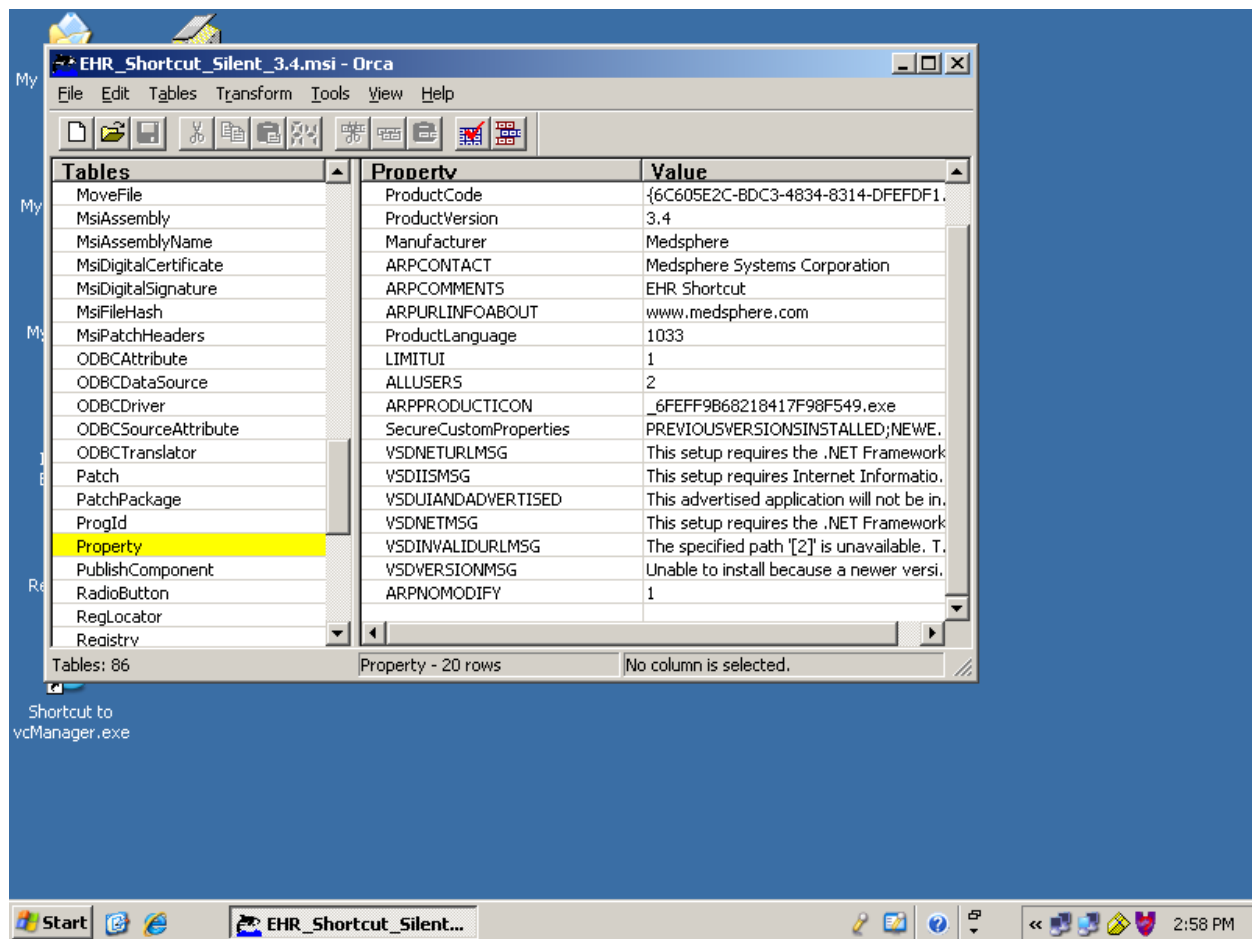
3. Browse to the EHR\_Shortcut\_Silent\_x.y.msi file.



4. Click on the EHR\_Shortcut\_Silent\_x.y.msi file to be modified and click "Open".

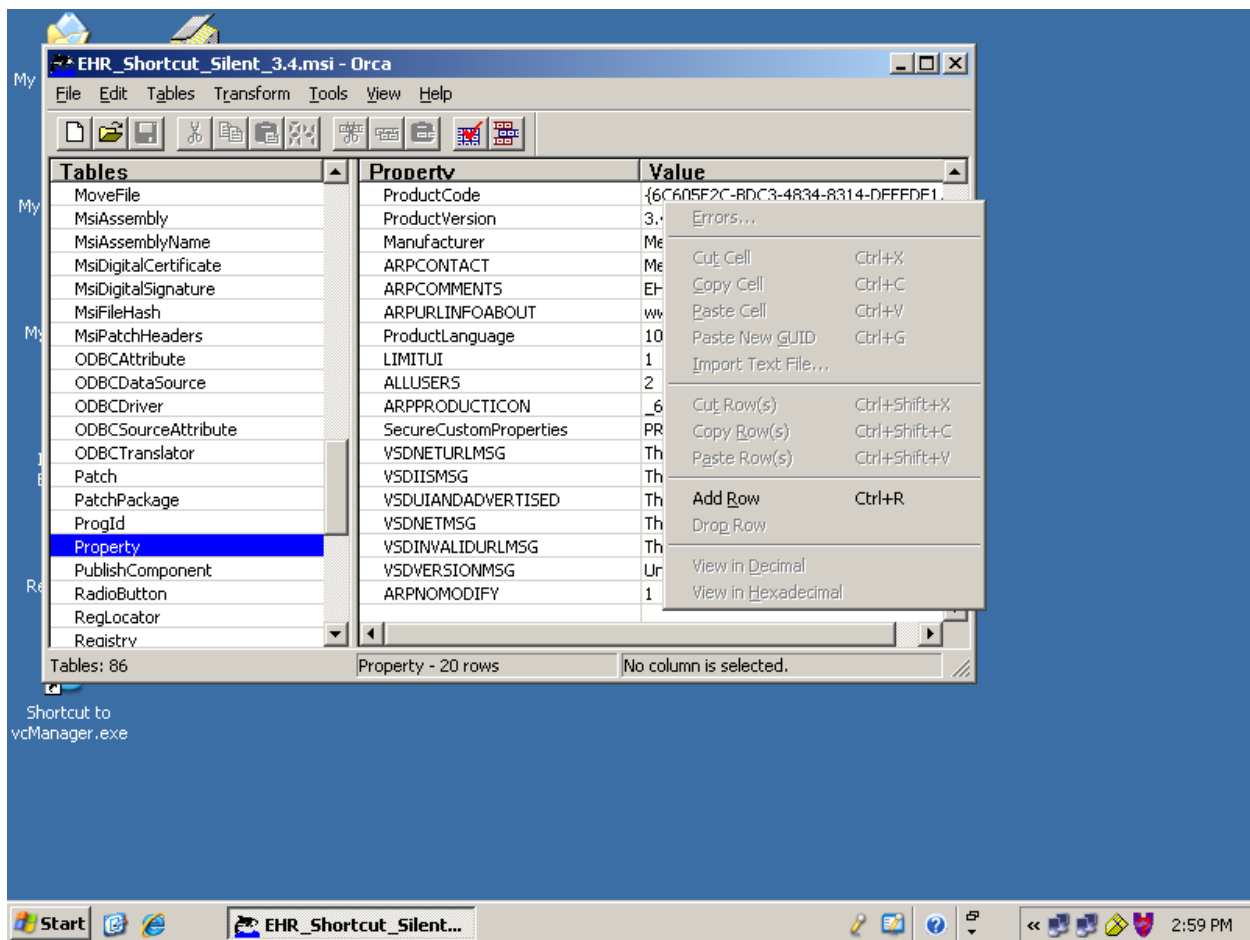


5. Browse down to the property table.

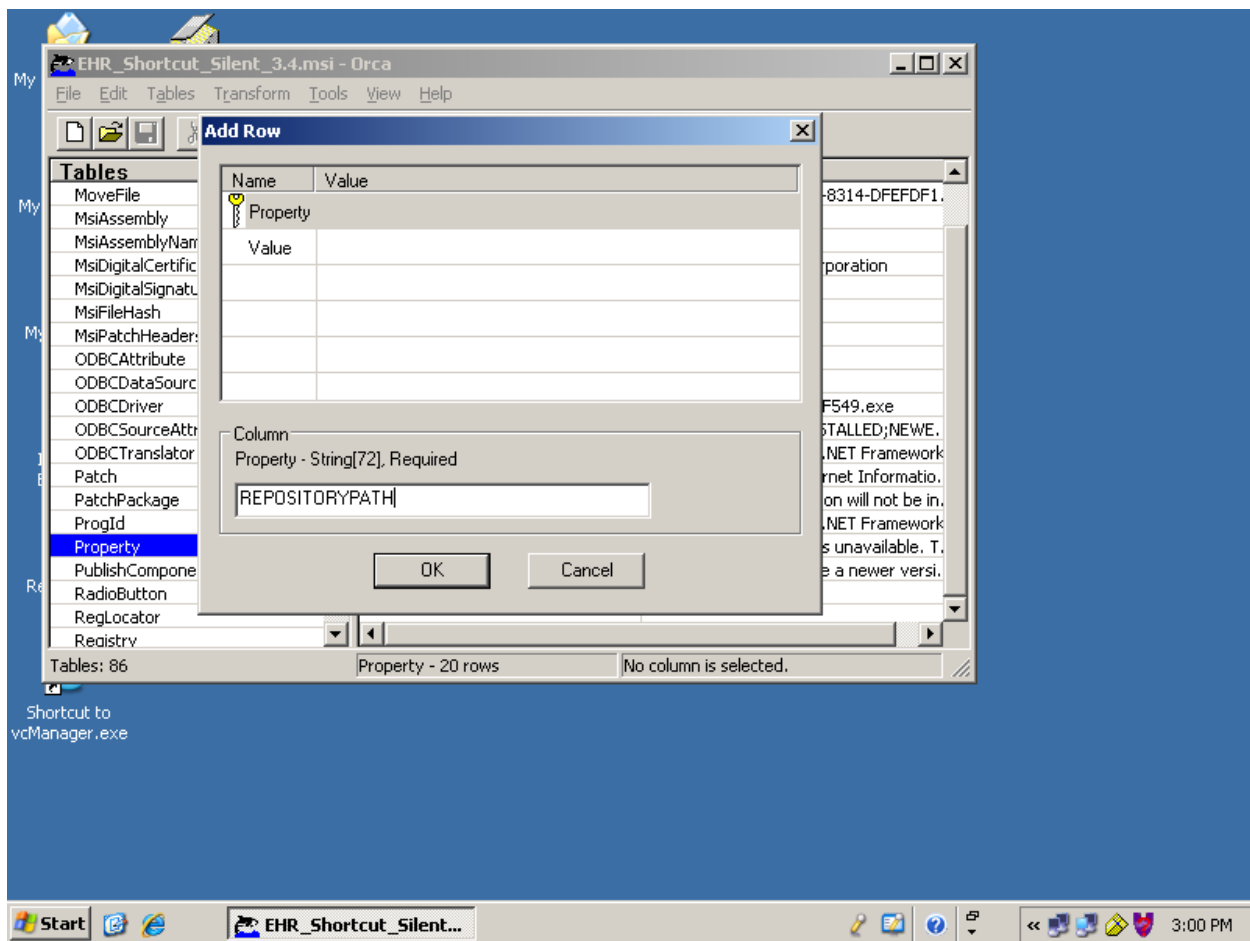


6. Select Property, scroll down to the end of the table.

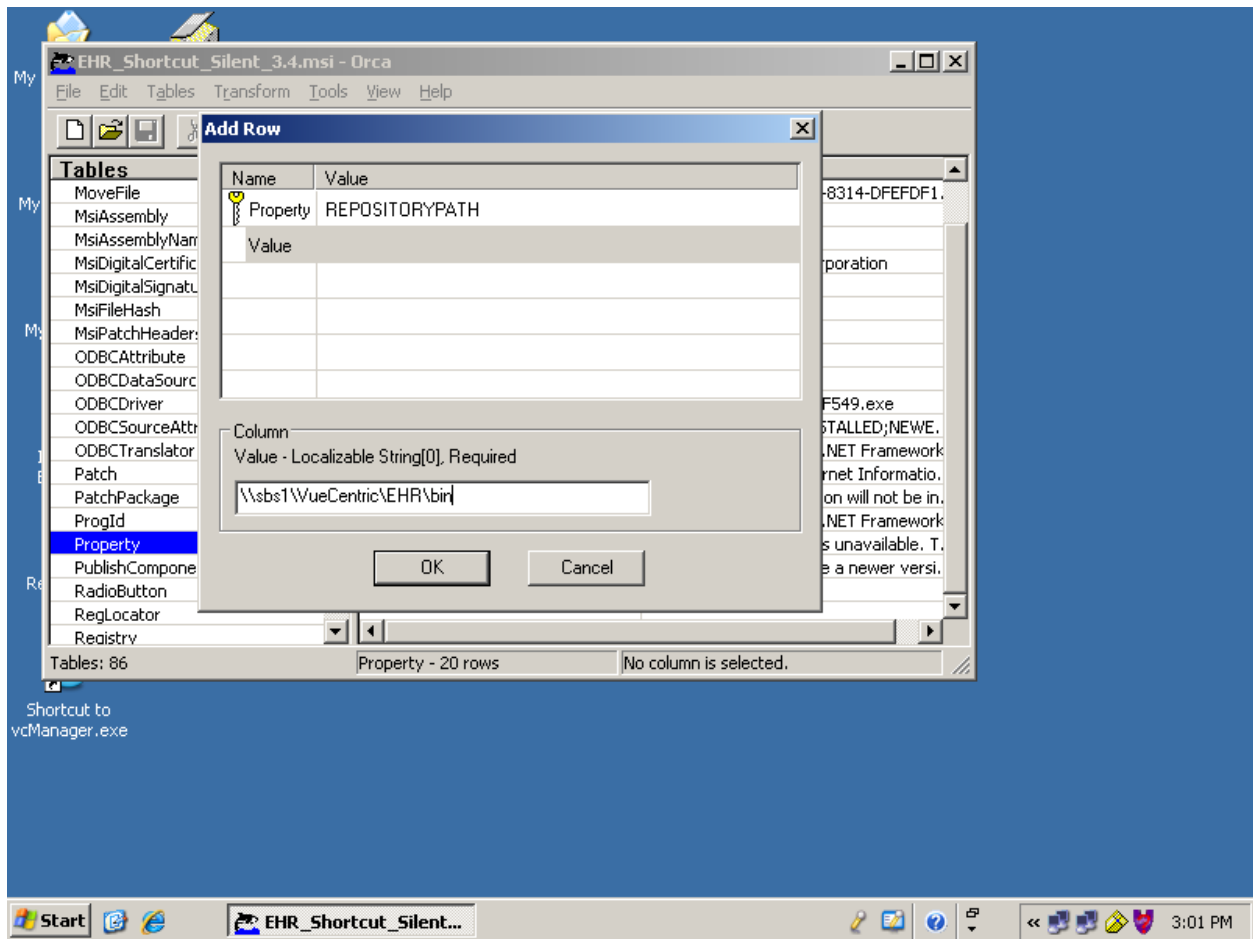




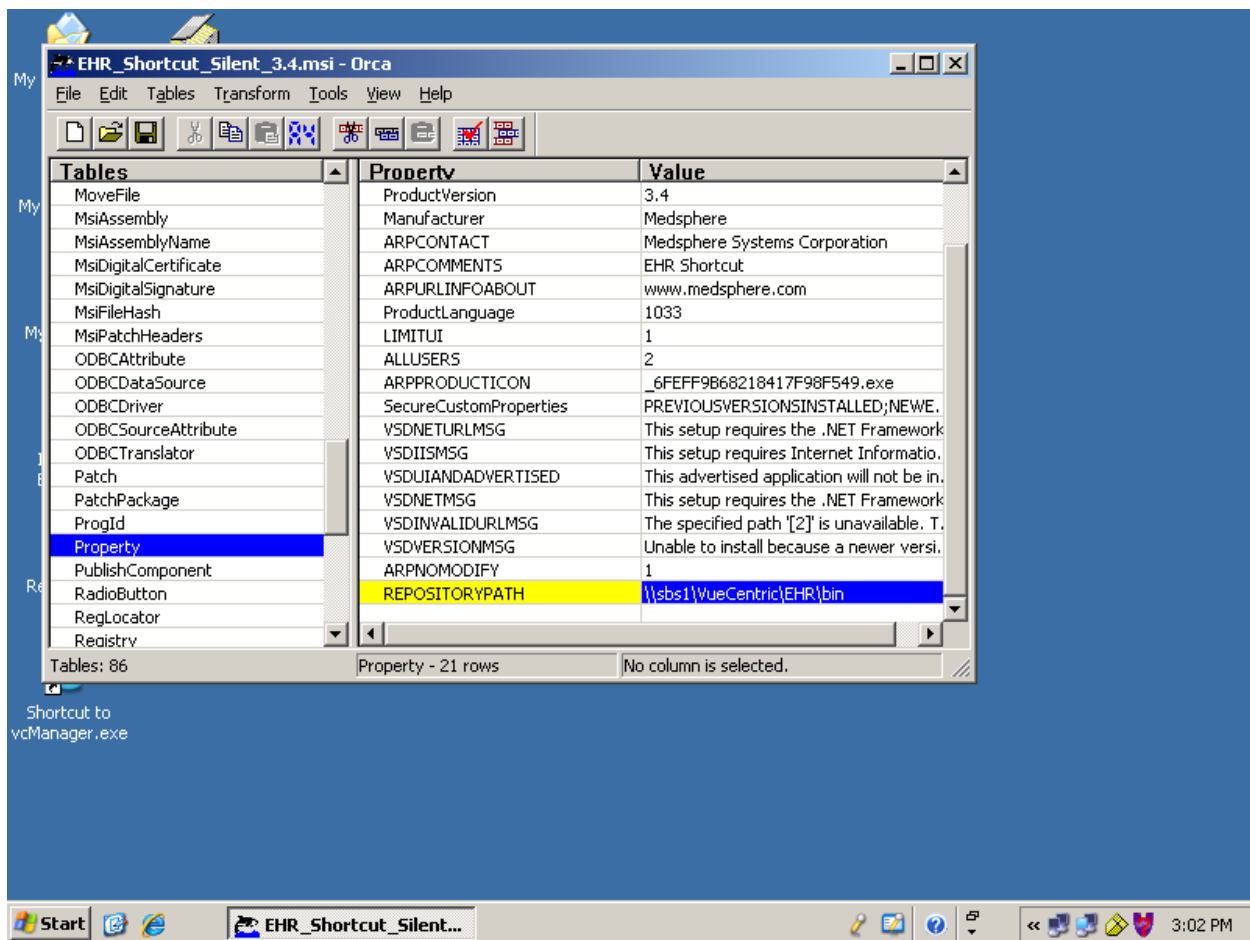
7. Right-click in the right pane and select "Add Row".



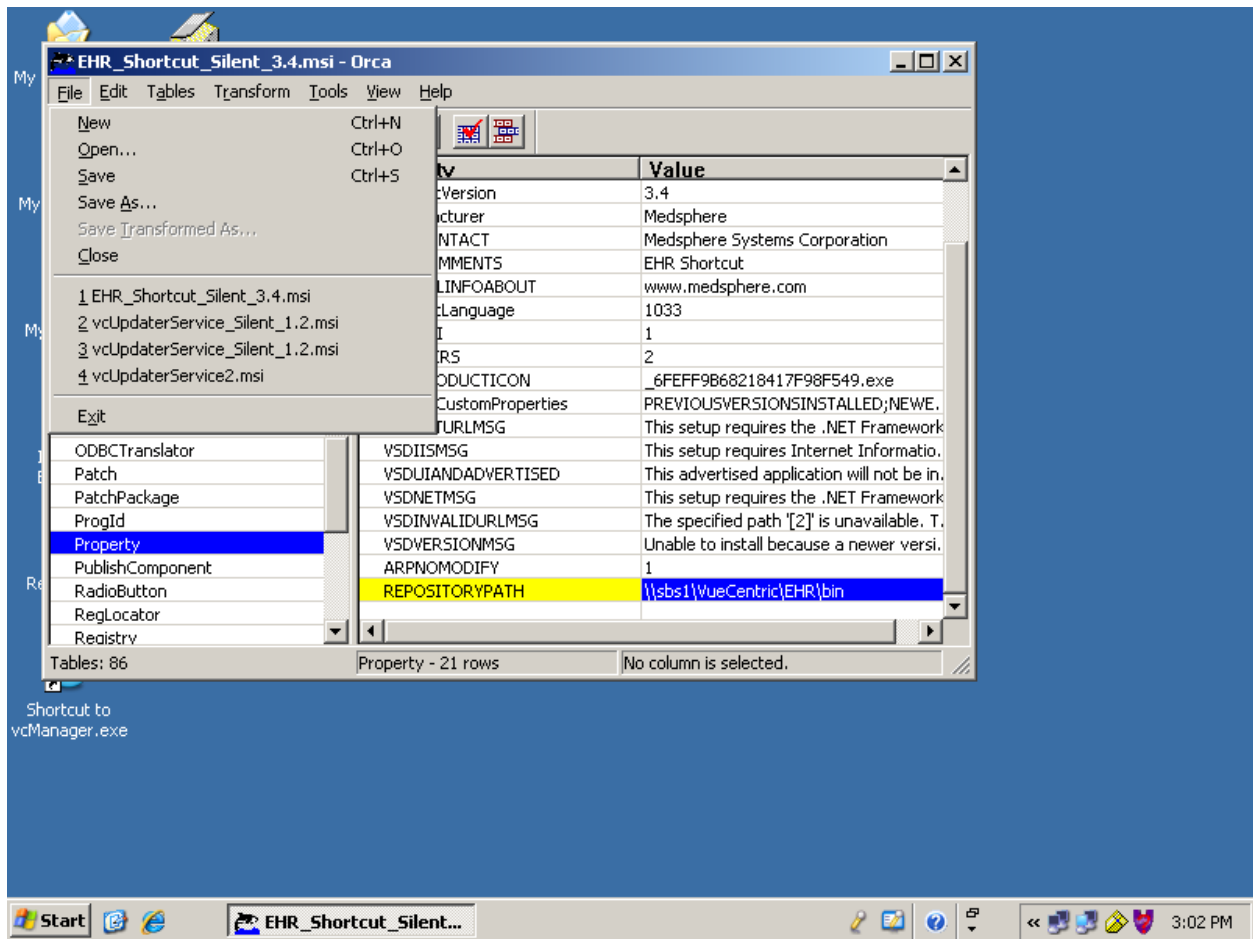
8. Type "REPOSITORYPATH" and press Enter.



9. Type in the UNC path to the bin directory containing the vuecentric.ini file and press Enter.



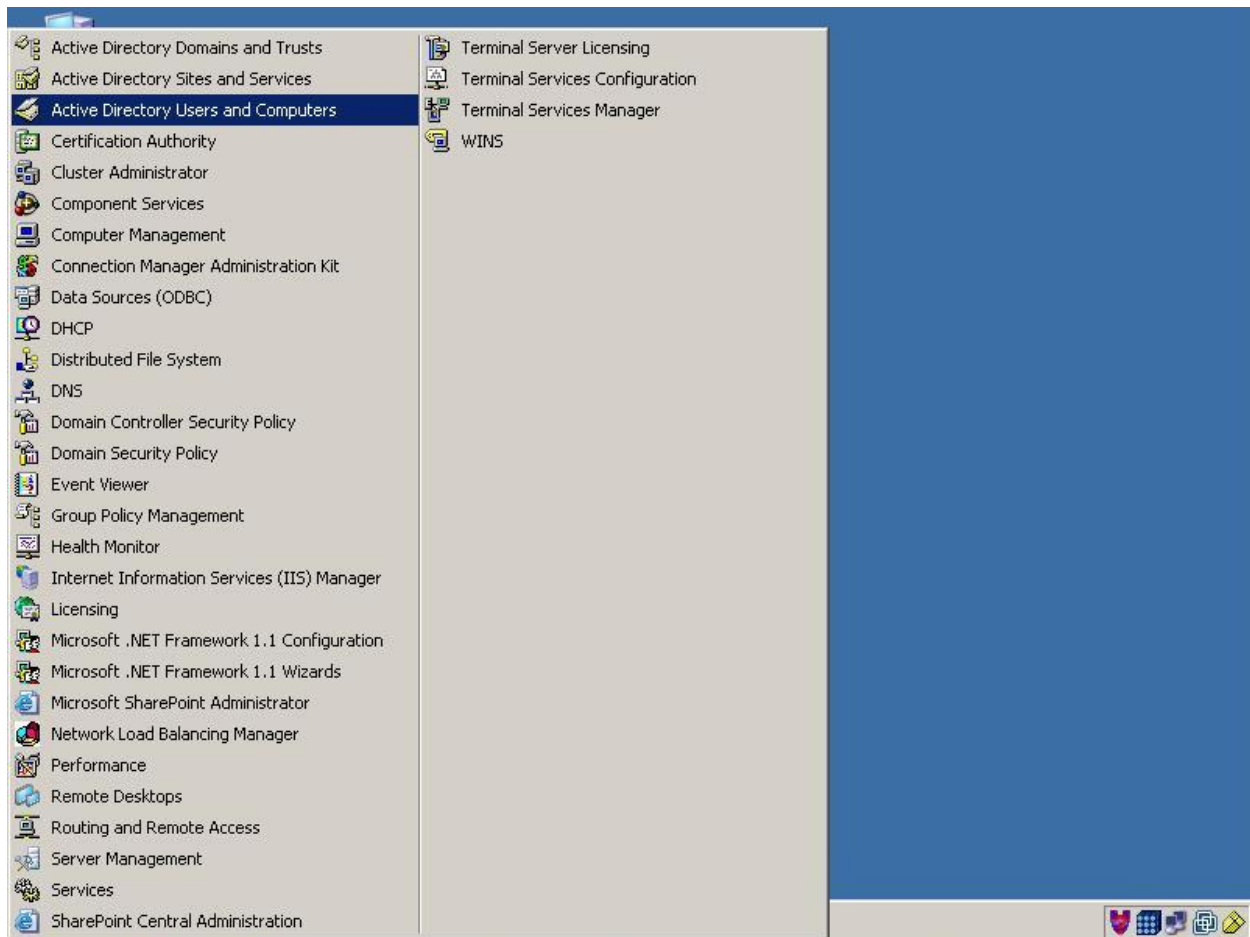
10. You have now modified the EHR shortcut.



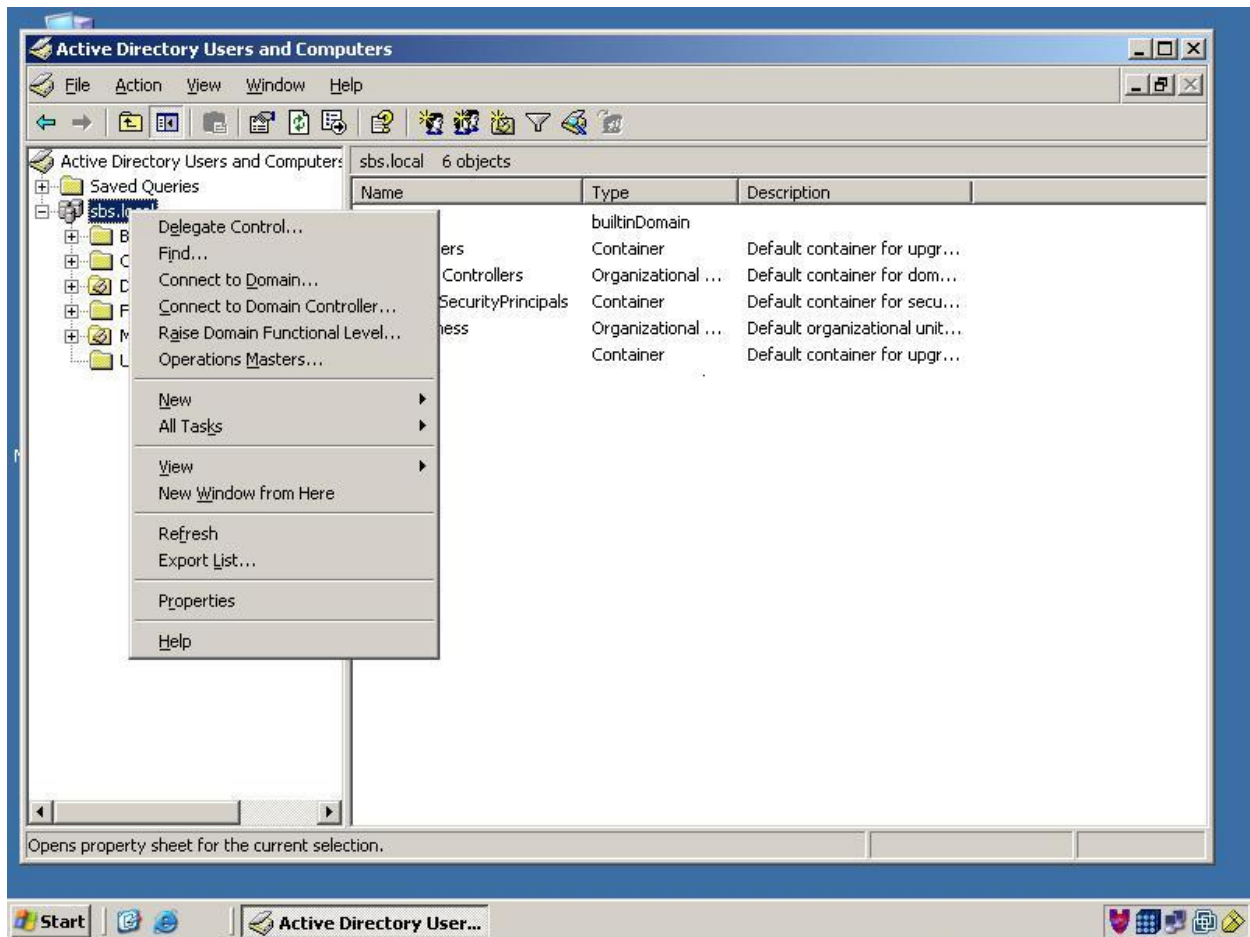
11. Open the file menu and click on "Save".

Note: Do not deploy the modified msi file from its original location as future updates may overwrite it. Move it to another folder and deploy it from that location.

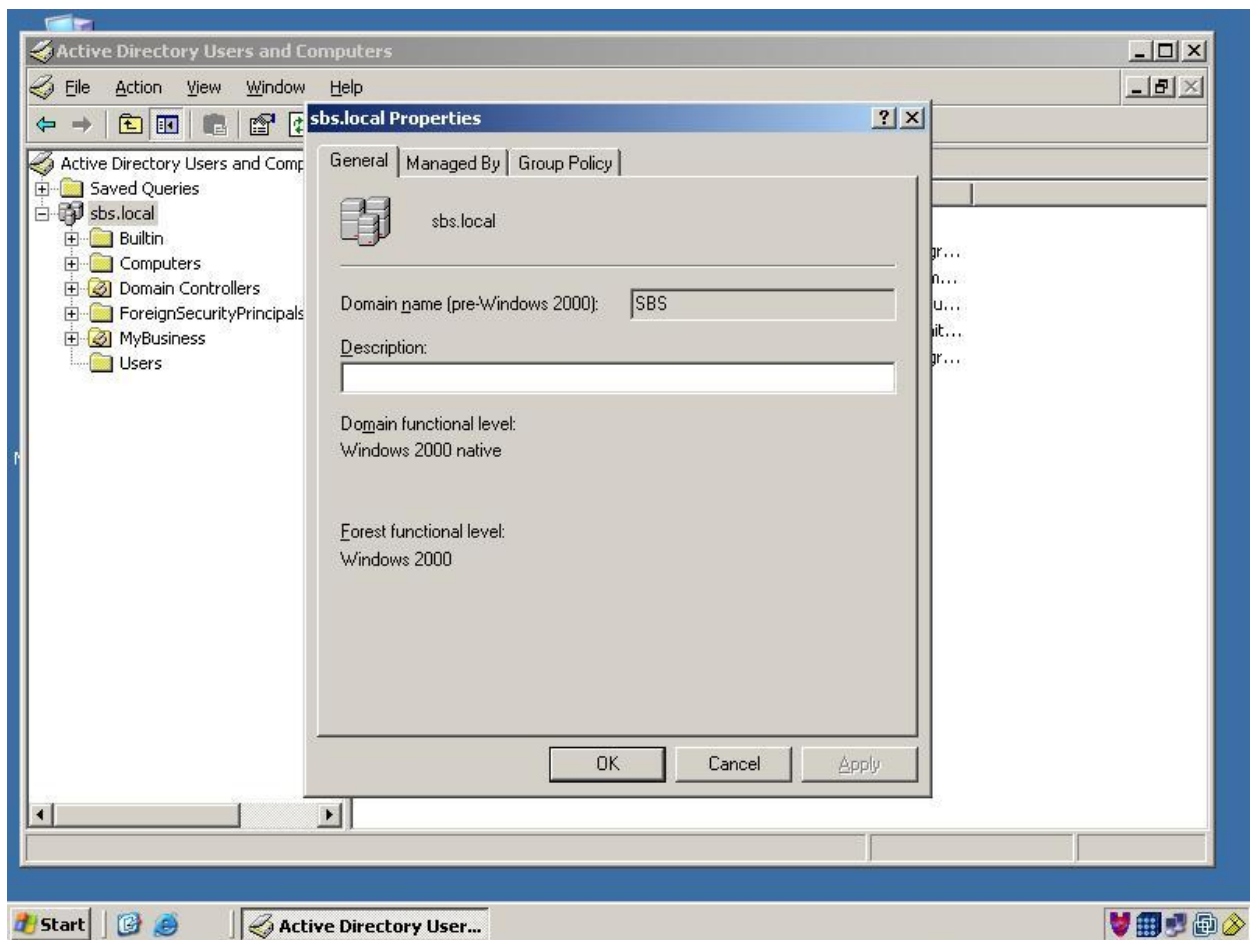
## B) Deploy the EHR\_Shortcut\_Silent\_x.y.msi via Group Policy



1. Open Active Directory Users and Computers.

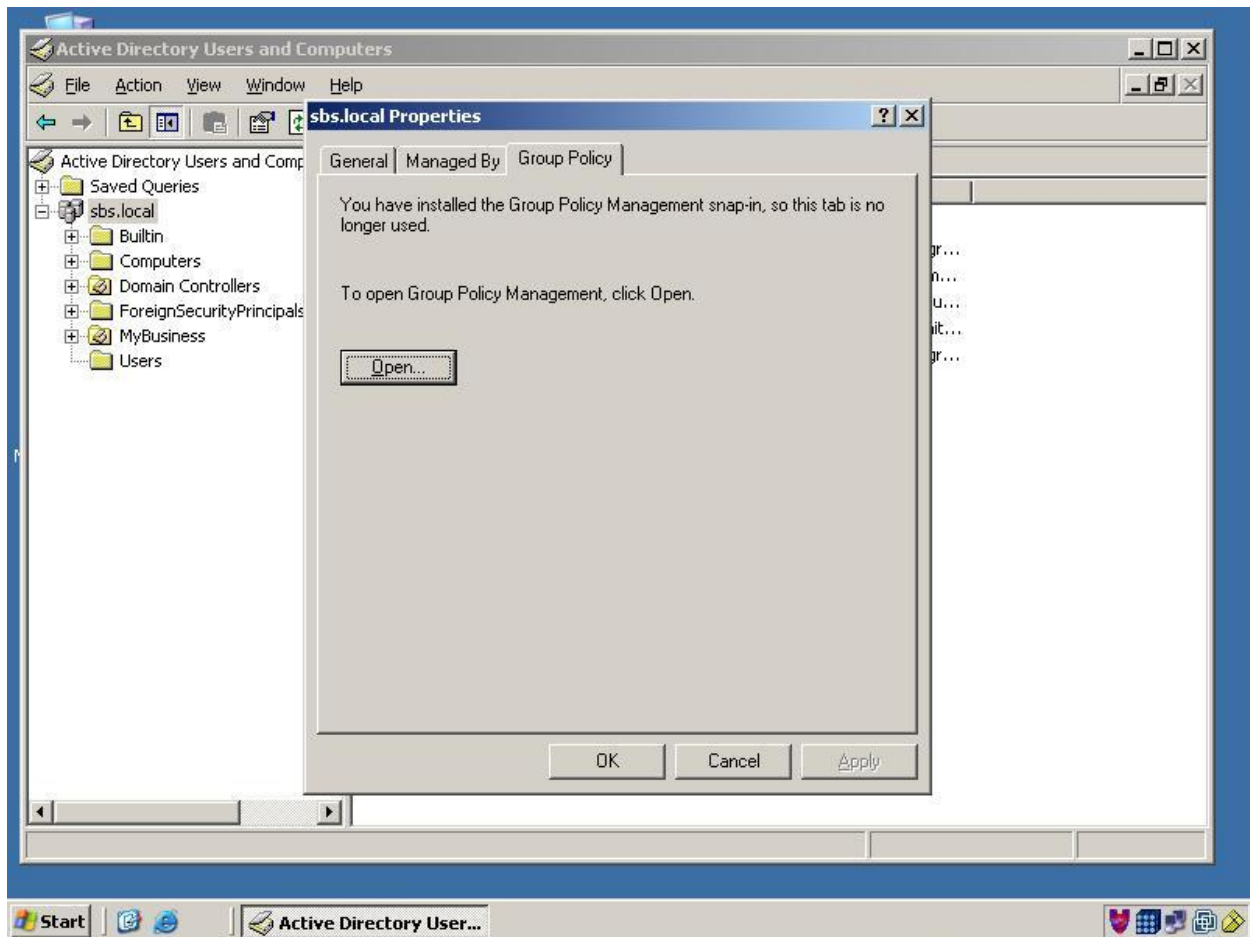


2. Right-click on the domain or OU that should have the shortcut deployed and select properties.

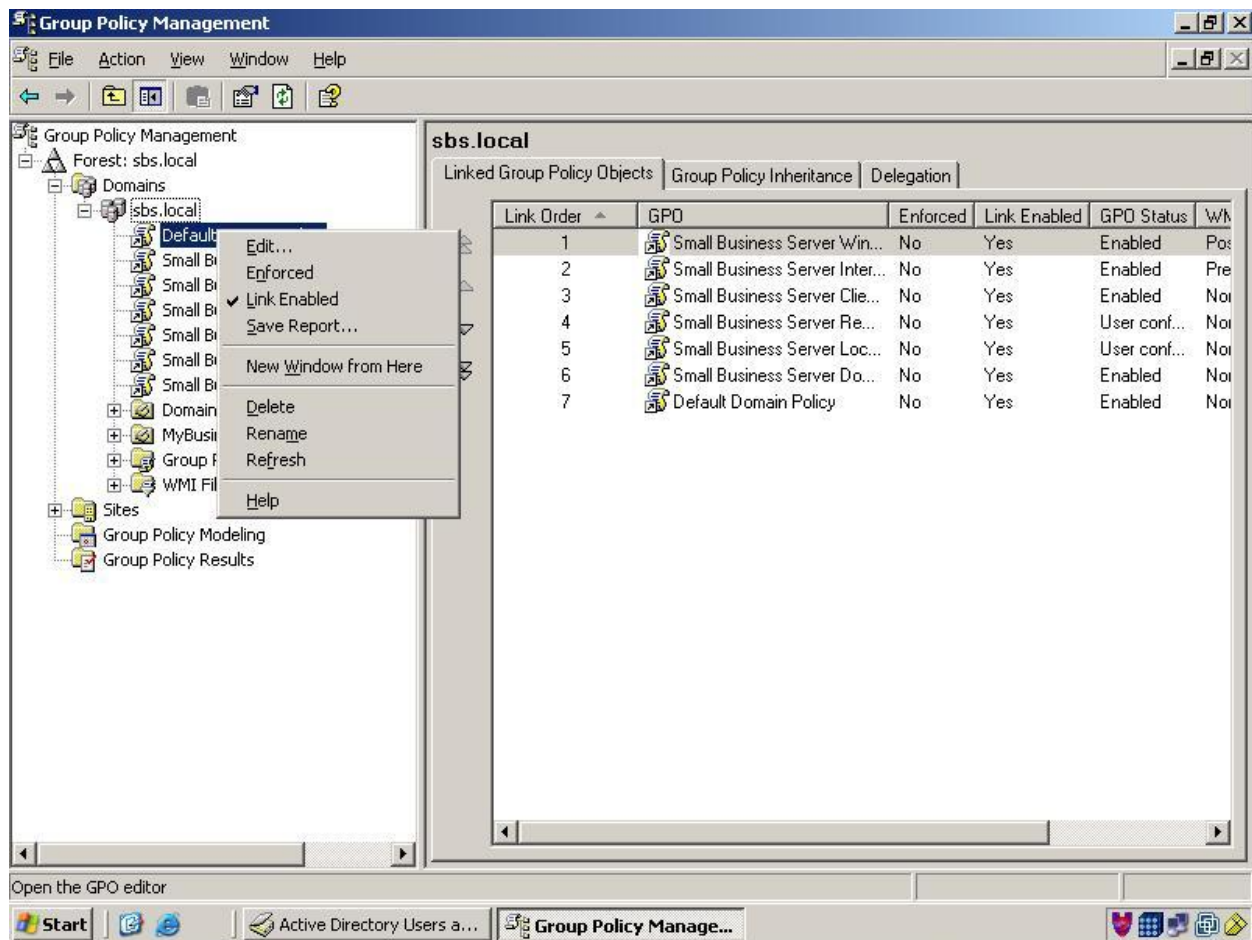


3. Click on the "Group Policy" tab.

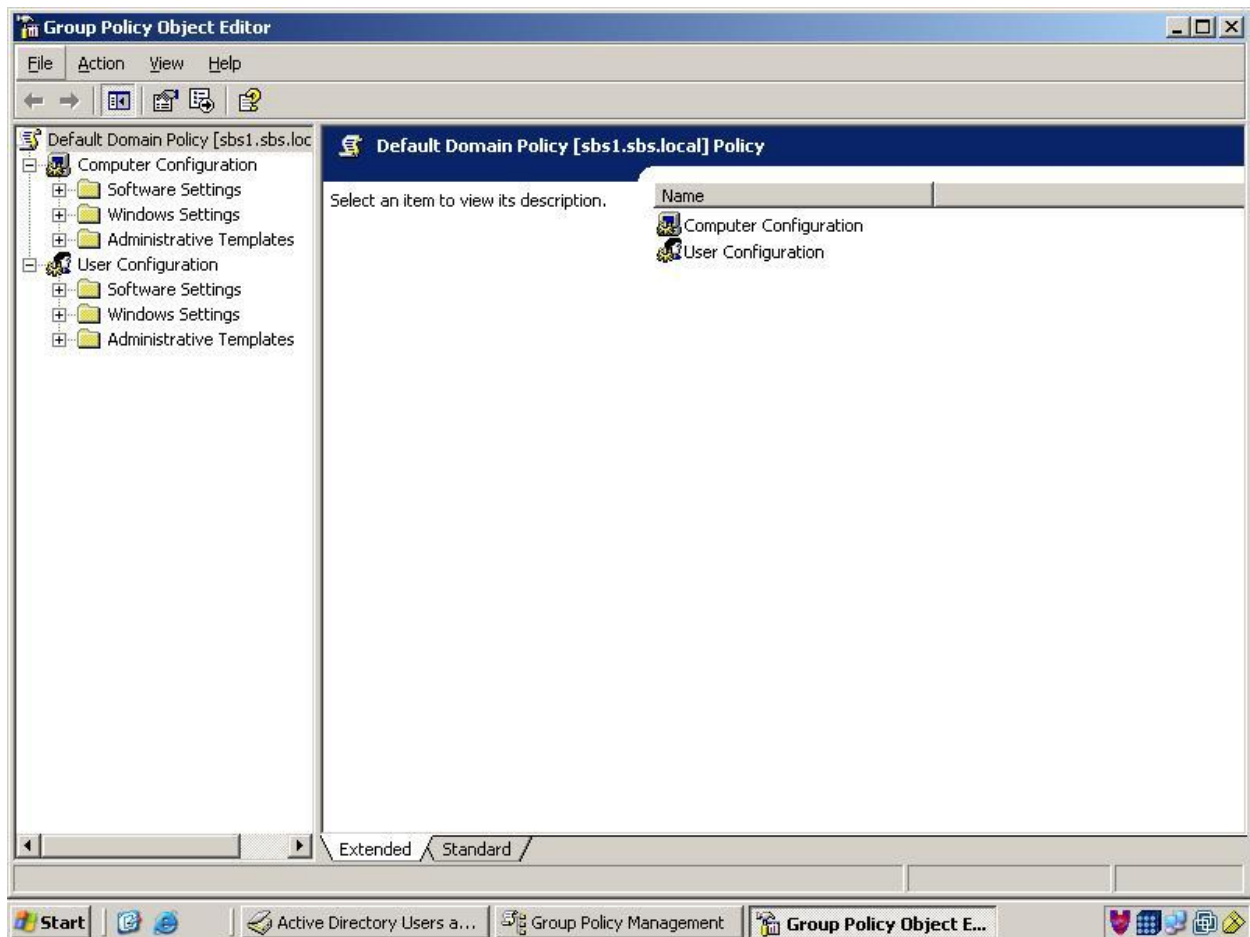




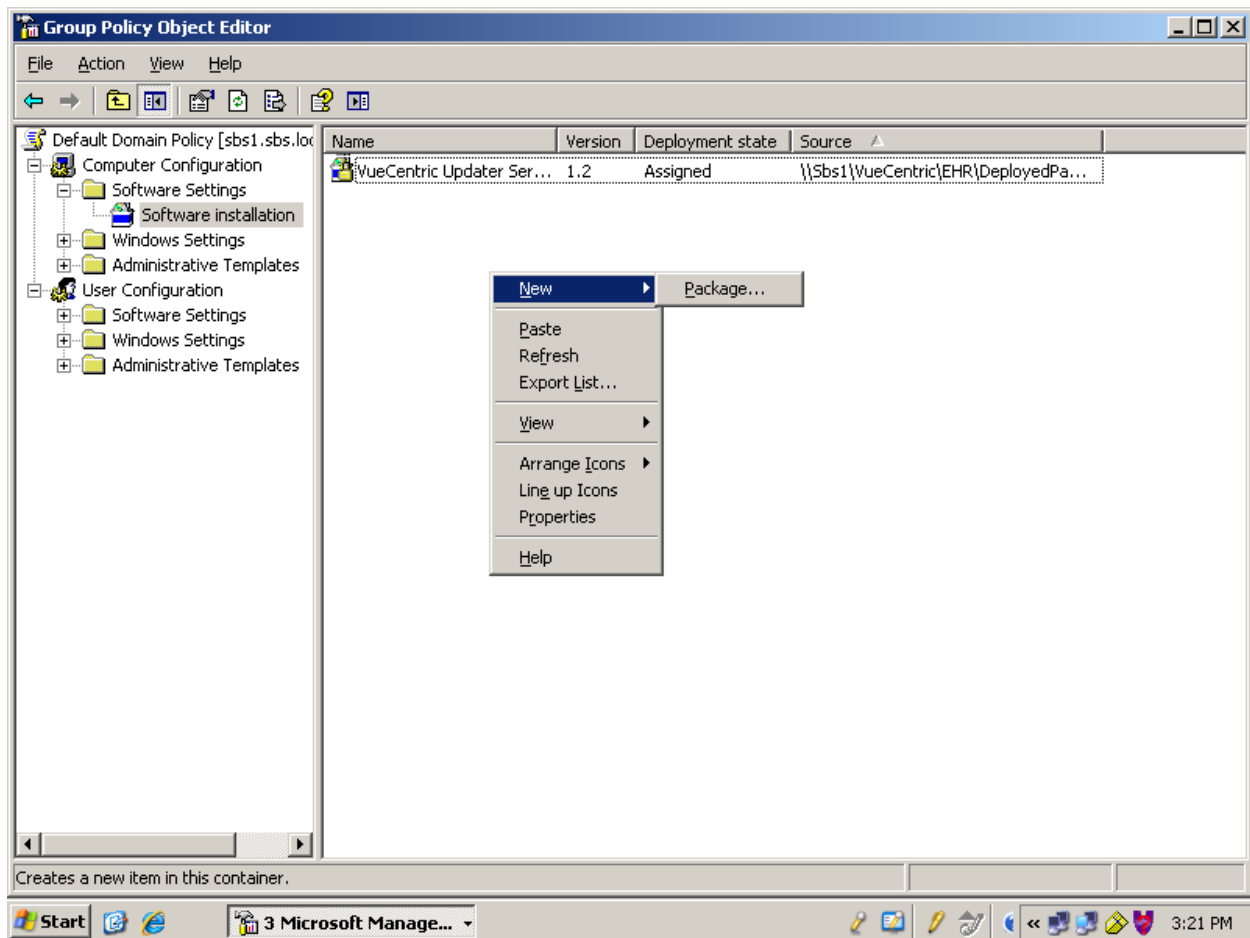
4. Click “Open”.



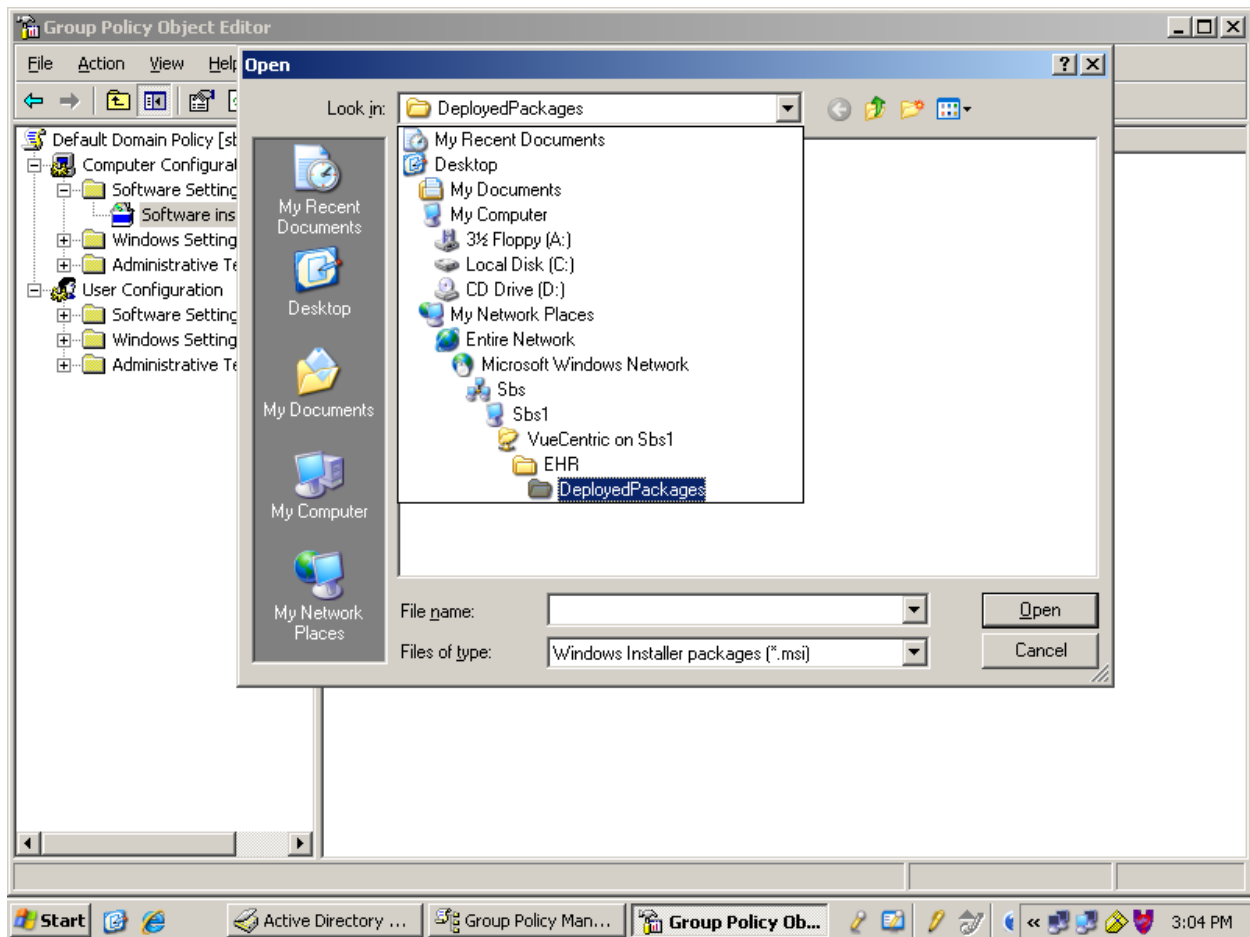
5. Edit the policy that you created or modified earlier when deploying the vcUpdaterService\_Silent\_x.y.msi.



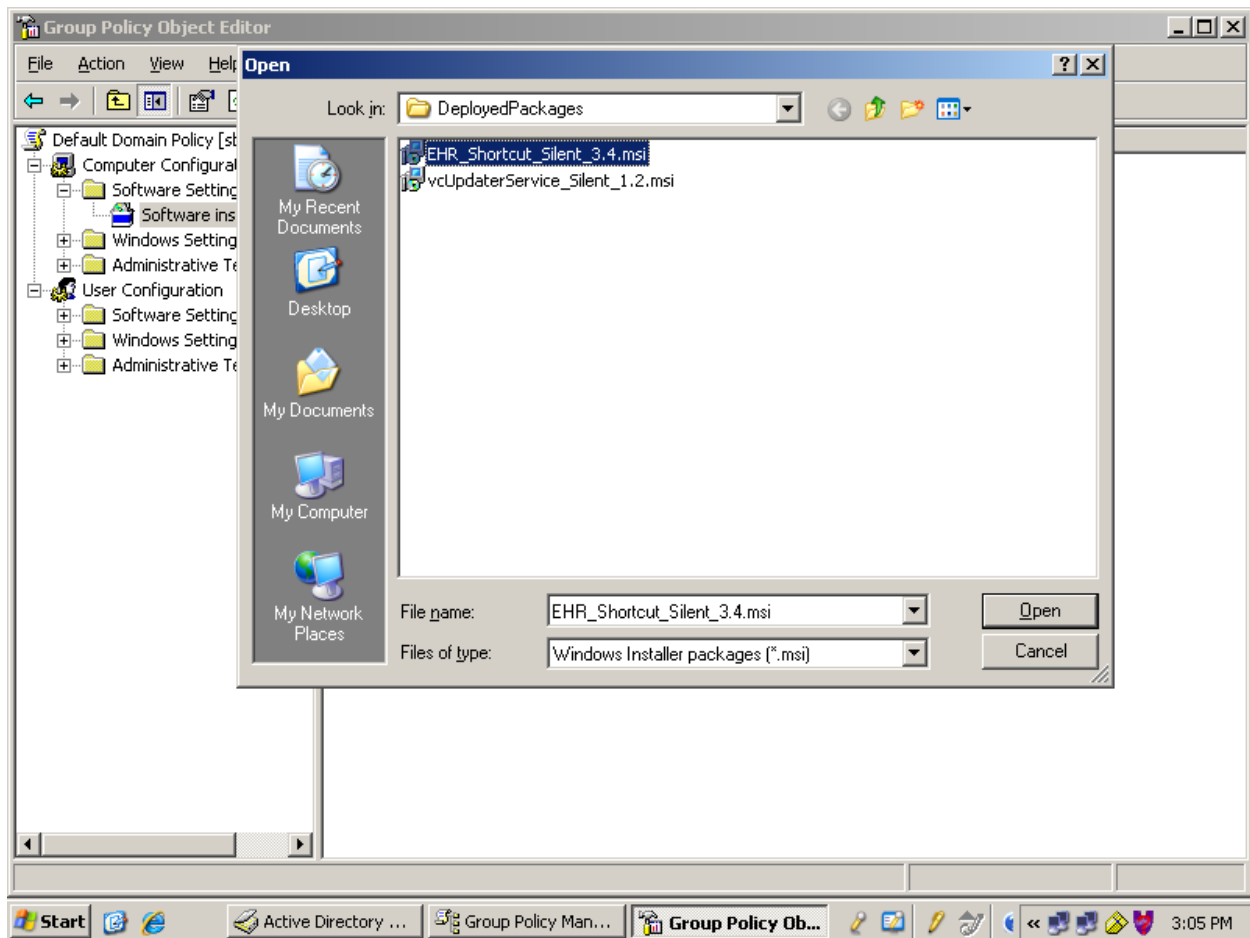
6. Expand Software Settings under Computer Configuration. Click on "Software Installation".



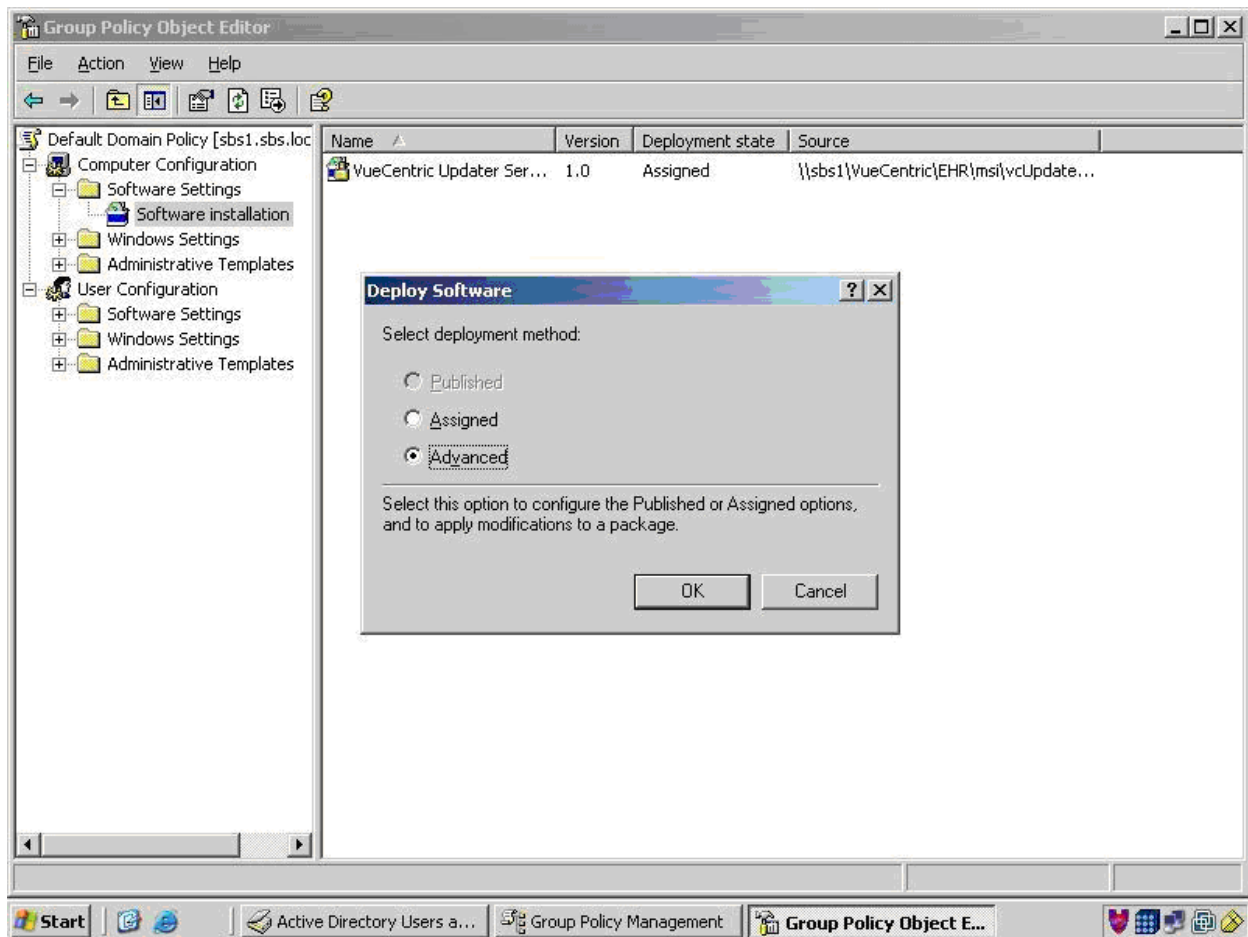
7. Right-click in the right pane and select "Package".



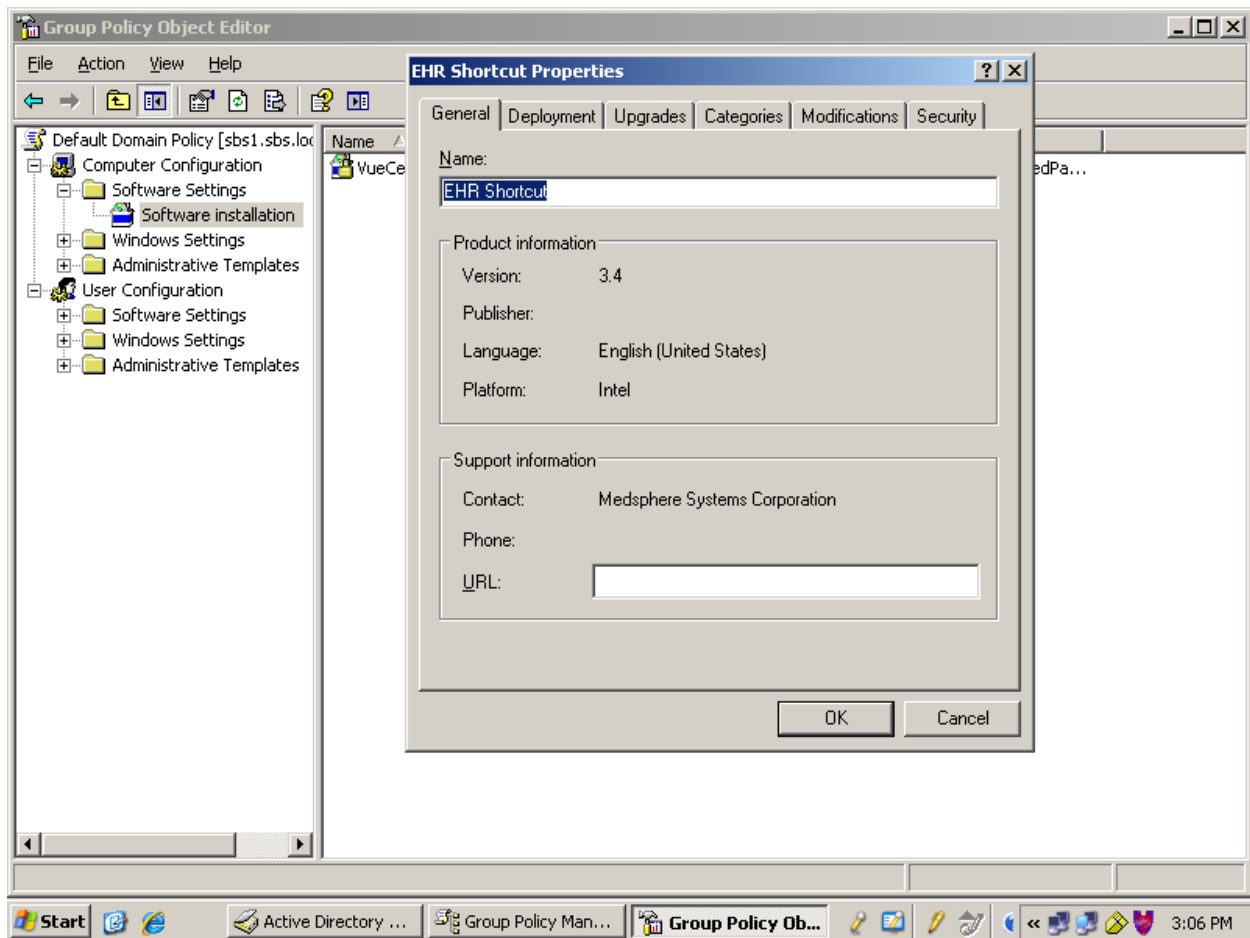
8. Browse to the UNC path where the modified EHR shortcut was copied. Be sure to follow the network path to this file. Do not use the local drive path. Do not deploy the modified file from its original location as future updates may overwrite it.



9. Select EHR\_Shortcut\_Silent\_x.y.msi and click "Open".

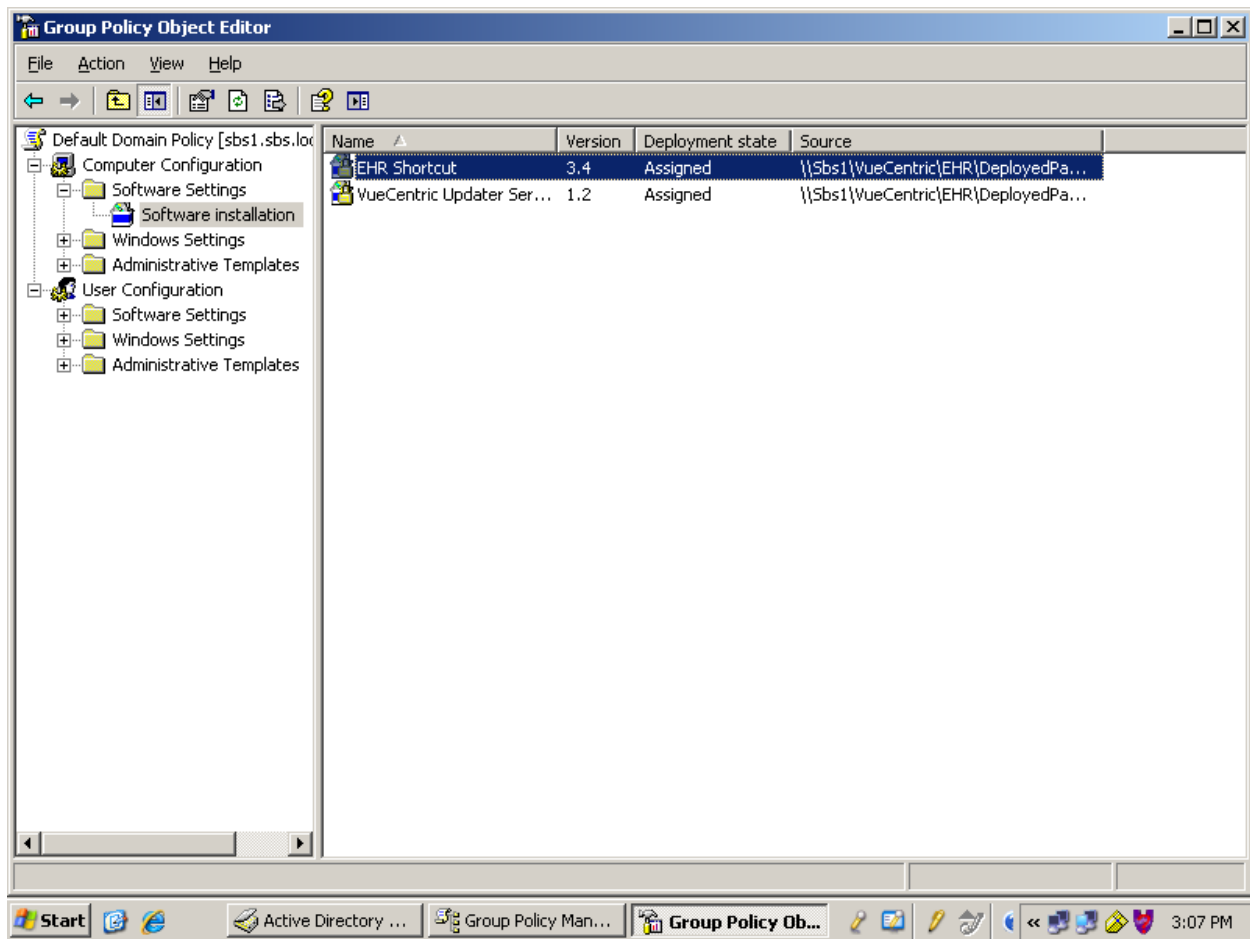


10. Choose Advanced and then click OK.



11. Click "OK".





12. The EHR Shortcut is now queued for deployment.

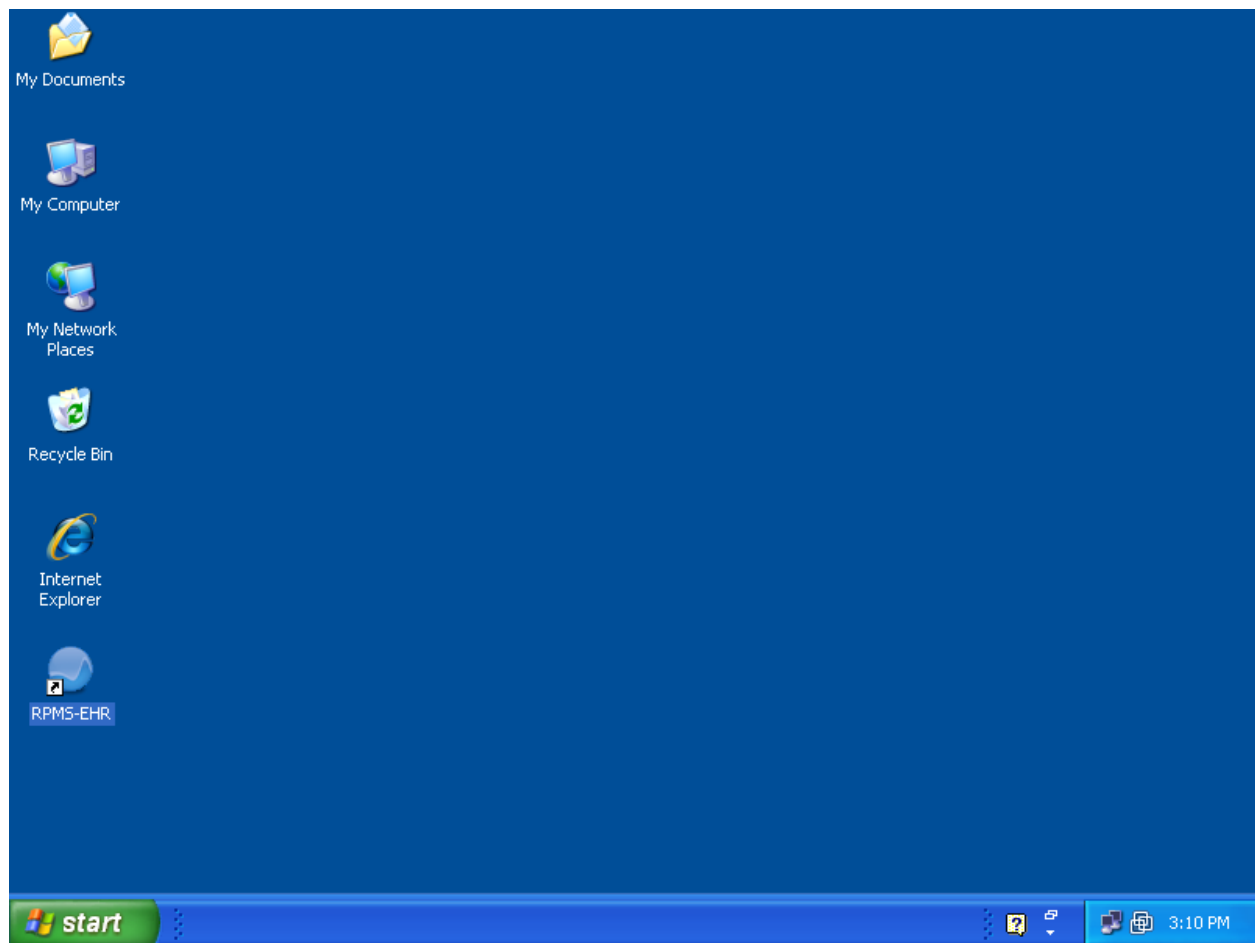
### C) Verify EHR\_Shortcut\_Silent\_x.y.msi deployment on Client



1. Upon boot up of the client workstation, you should see this.



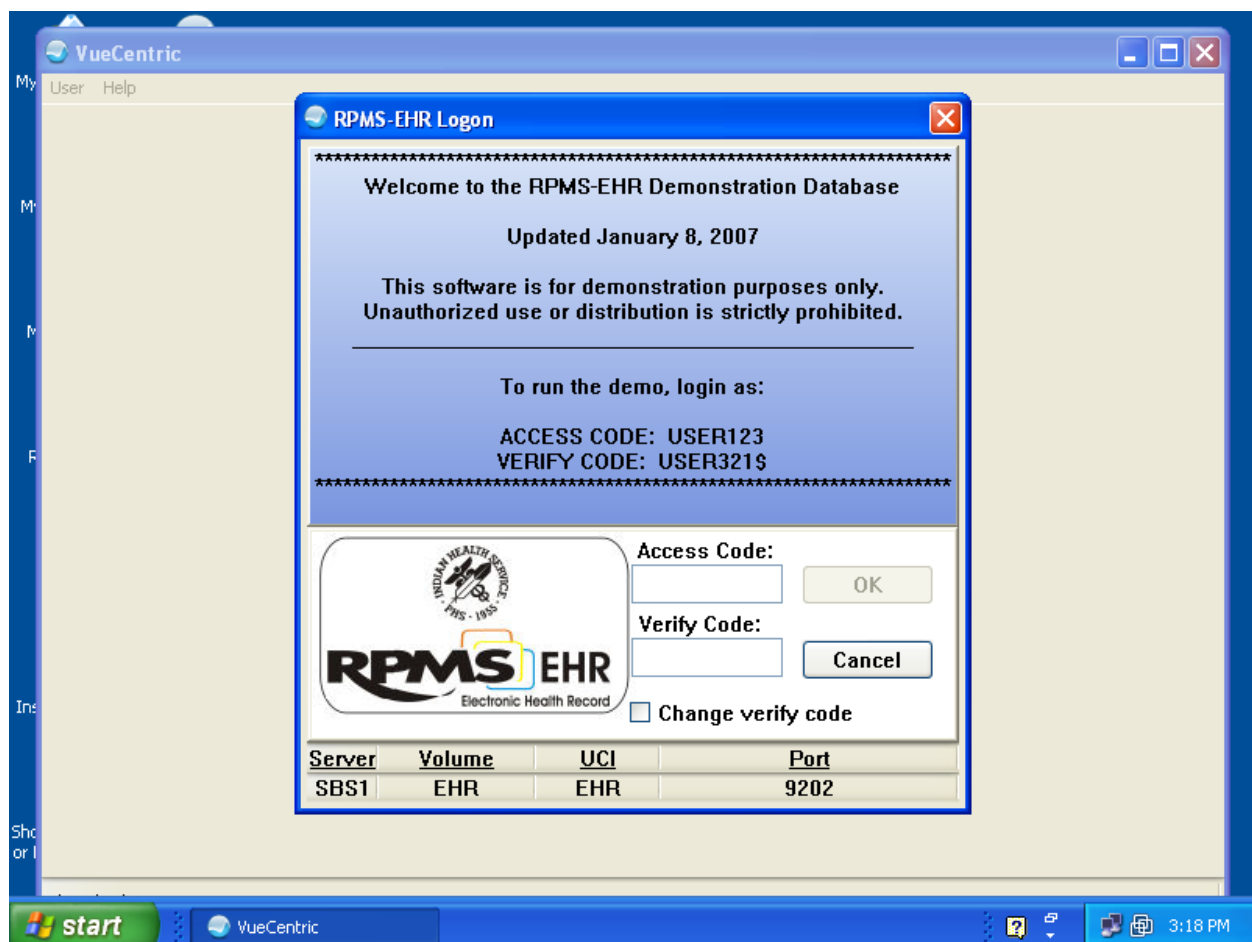
2. Login as a domain user without administrative privileges.



3. Click on the RPMS-EHR Shortcut on the desktop.



4. If there are any pending EHR updates, you should see the files being updated.



5. Deployment is complete.