# GPO Installation of Barracuda WSA from the Windows Interface

https://campus.barracuda.com/doc/6160386/

This article covers installation using a Windows GPO from the Windows interface on Win2K8 server and Win2k3 server.

Note that behavior in the Microsoft Small Business Server (SBS) 2008 breaks the server-client trust relationship when using GPO deployment. The client has to be rejoined to the server, manually. See GPO Installation of the Barracuda WSA With Microsoft SBS 2008 Server for instructions.

## Install the Barracuda WSA application on Win2K8 Server

### Step 1: Download the MSI Windows Installer Package and create an MST file

1. Log on to the server computer as an administrator.
2. Create a shared folder on the network where you will put the installer package (.msi file) that you want to distribute. Clients to which you want to push the Barracuda WSA must have access to this shared folder.
3. Log in to the Barracuda Web Security Gateway Web interface with the administrator credentials. Navigate to the **ADVANCED > Remote Filtering** page.
4. Click on the **Download/Install** link to download the Barracuda WSA **MSI** installer from the **Download Web Security Agent** section of the page.
5. Save the MSI installer file in the shared folder on the network.
6. Download the open source ORCA tool, a Windows installer package editor which you can use to create a Windows transform file (.mst file). You can download the ORCA tool from: http://www.softpedia.com/progDownload/Orca-Download-79861.html
7. Launch the ORCA tool after download. Click on File -> Open in the dialog window. Select the installer package *BarracudaWSASetupshared folder* from the shared folder. Click on Open. Once all the database tables are loaded, select New Transform from the Transform menu item. You will see the Property table listing the following properties with corresponding values to specify the use of Barracuda Web Security Gateway as a service.
   Property:SERVICE_MODEValue:1
   Property:USER_MODEValue:0
   Property:SERVICE_URLValue:<Barracuda Web Security Gateway IP Address>
   Property:SERVICE_PORTValue:8280
8. Select “Generate Transform” from the Transform menu item. Save this .mst file in the same shared folder which contains the .msi file. Close the ORCA tool window.

## Step 2: Deploy the Barracuda WSA through the Active Directory by creating a GPO

1. Create a Container or Organizational Unit. Open the Active Directory **Users and Computers** window. In the console tree, right-click your domain, and then select New -> Organizational Unit. Provide a name for the container and uncheck the checkbox “Protect container from accidental deletion” so as to be able to delete this container later. If checkbox is marked, it is not possible to delete this container.
   In the same Active Directory Users and Computers window, to the Container, add the users and machines for which the policy needs to be applied. OR you can move the users from the USERS account to the container and machine accounts from COMPUTERS account to the container. Moving the users or machines prompts a warning. New domain users and computers can be created in this container.
2. Create a GPO. Click Start, point to Administrative Tools, and then click Group Policy Management. Expand the tree for your domain, select the newly created Container or OU, right-click and select the item “Create a GPO in this domain, and Link it here...”. Provide a name for the GPO and click the OK button to close the window. This GPO will be added to your container and also to the Group Policy Objects list.
3. Now, select this GPO which is present in your container and right-click. Click on Edit to open the Group Policy Management Editor. If you assign this application to a user, it is installed when the user logs on to the computer. If you assign this application to a computer, it is installed when the computer starts.

**To assign an application to a computer**:

1. In the Group Policy Management Editor, expand “Computer Configuration”, then expand “Policies” and “Software Settings”. Select “Software Installation”, right-click and select New -> Package...
2. In the open dialog box, make sure to type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example:
   \\QAWIN2K8DC\msi files\BarracudaWSASetup.msi
3. Click Open. Select the Deployment Method as *Advanced* and click OK. In the Barracuda Web Security Agent Properties window, Click on the Modifications tab and click the Add button. In the Open dialog box, type the full Universal Naming Convention (UNC) path of the .mst Transform file. For example, \\QAWIN2K8DC\msi files\mysetup.mst and click Open.
4. Click the OK button in the Barracuda Web Security Agent Properties window, and close all open windows.
5. From the command-line window, run the command to force an update of group policy:
   C:\Users\Administrator>gpupdate /Force
   You should see the following output:

```
Updating Policy...

User Policy update has completed successfully.

Computer Policy update has completed successfully.
```

**To assign an application to a user**:

1. Expand “User Configuration”, and then expand “Policies” and “Software Settings”.
2. Select “Software installation”, right-click and select New -> Package. The rest of the setup for User Configuration is similar to the Computer Configuration as described above, concluding with a forced group policy update.

### Step 3: Application Install (both Win2K3 and Win2K8 servers)

1. Start a computer that is joined to the domain for applying the computer-based policy.
2. Log in as the domain user to apply the user-based policy.
3. You should see the Barracuda WSA Monitor icon in the system tray. This indicates that the Barracuda WSA application has been installed. You can also verify this in Add/Remove Programs from the Windows Control Panel.

## Install the Barracuda WSA application on Win2K3 Server

### Step 1: Download the MSI Windows Installer Package and create an MST

1. Log on to the server computer as an administrator.
2. Create a shared folder on the network where you will put the installer package (.msi file) that you want to distribute.
3. Log in to the Barracuda Web Security Gateway interface using the administrator credentials. Navigate to the **ADVANCED > Remote Filtering** page.
4. Click on the **Download/Install** link to download the Barracuda WSA **MSI** installer from the **Download Web Security Agent** section of the page.
5. Save the MSI Installer file in the shared folder.
6. Download the open source ORCA tool, a Windows installer package editor which you can use to create a Windows transform file (.mst file). You can download the ORCA tool from: http://www.softpedia.com/progDownload/Orca-Download-79861.html.
7. Launch the ORCA tool after download. Click on File -> Open in the dialog window. Select the installer package *BarracudaWSASetupshared folder* from the shared folder. Click on Open. Once all the database tables are loaded, select New Transform from the Transform menu item. Select the Property table from the left list. Scroll to the bottom of the table, right click and select “Add Row”. Add the following Properties with corresponding values to specify the use of Barracuda Web Security Gateway as a service.
   Property:SERVICE_MODE Value:1
   Property:USER_MODE Value:0
   Property:SERVICE_URL Value:<*Barracuda Web Security Gateway IP Address*>
   Property:SERVICE_PORT Value:8280
8. After adding all the properties, select “Generate Transform” from the Transform menu item. Save this .mst file in the same shared folder which contains the .msi file. Close the ORCA tool window.

## Step 2: Deploy the Barracuda WSA application through the Active Directory by creating a GPO

1. Create a Container or Organizational Unit. Open the Active Directory **Users and Computers** window. In the console tree, right-click your domain, and then select New -> Organizational Unit. Provide a name for the container and Click OK. In the same Active Directory Users and Computers window, to the Container, add the users and machines for which the policy needs to be applied. OR you can move the users from the USERS account to the container and machine accounts from COMPUTERS to the container. Moving the users or machines prompts a warning. New domain users and computers can be created in this container.
2. Create a GPO. Open the Active Directory Users and Computers window, select your domain, right-click and select Properties. In the Properties window, click on the Group Policy tab. Click on New button. Provide a name for this new Policy object. Close the Properties window by clicking on Close button.
3. Link this GPO to the new Container. In the same Active Directory Users and Computers window, select the new container, right-click and choose Properties. In the Properties window, click on the Group Policy tab. Click the Add button. In the window “Add a Group Policy Object Link”, click the All tab. Select the new GPO and Click OK to close the window. Click on Apply and OK to close the Container Properties window. If you assign this application to a user, it is installed when the user logs on to the computer. If you assign this application to a computer, it is installed when the computer starts.
4. Deploy the application.

### To assign the application to a computer:

1. Right-click your domain in Active Directory Users and Computers window and select Properties. In the domain Properties window, click on the Group Policy tab. Select the new GPO and click on the Edit button. This opens the Group Policy Object Editor.
2. Expand “Computer Configuration”, and then “Software Settings”. Select “Software installation”, right-click and select New -> Package…
3. In the Open dialog box, make sure you type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\WFDEVDC01\msi files\BarracudaWSASetup.msi Click Open. Select the Deployment Method as Advanced and click OK.
4. In the Barracuda Web Security Agent Properties window, Click on the Modifications tab and click the Add button. In the Open dialog box, type the full Universal Naming Convention (UNC) path of the .mst Transform file. For example, \\WFDEVDC01\msi files\mysetup.mst and click Open. Click the OK button in the Barracuda Web Security Agent Properties window. Close all the open windows.
5. From the command-line window, run the command to force update of group policy.
   ```
   C:\Documents and Settings\Administrator.WFDEVDC01>gpupdate/Force
   Refreshing Policy..
   User Policy Refresh has completed.
   Computer Policy Refresh has completed.
   ```

To check for errors in policy processing, review the event log. Certain user policies are enabled that can only run during login. Certain computer policies are enabled that can only run during startup.

OK to Reboot? (Y/N)

If the server computer is rebooted, it installs the Barracuda WSA on the server machine also.

### To assign the application to a user:

Expand “User Configuration”, then expand “Policies” and “Software Settings”. Select “Software installation”, right-click and select New -> Package… The rest of the setup for User Configuration is similar to Computer Configuration as described above, concluding with a forced group policy update.

### Step 3: Application Install (both Win2K3 and Win2K8 servers)

1. Start a computer that is joined to the domain for applying the computer-based policy.
2. Log in as the domain user to apply the user-based policy.
3. You should see the Barracuda WSA Monitor icon in the system tray. This indicates that the Barracuda WSA application has been installed. You can also verify this in Add/Remove Programs from the Windows Control Panel.

### Troubleshooting

- A common cause of failure is that the user and/or the user’s computer does not have adequate access to the share location. Verify that all access and network privileges have been configured appropriately.
- Additional error messages may be found in the Event Log on the domain computer.
- If the Event Log has no useful information, consider enabling verbose logging and restarting the computer.
- Additional information on fixing Group Policy issues can be found on the Microsoft technet: http://technet.microsoft.com/en-us/library/cc775423.aspx