Using Logon Agent for Transparent User Identification

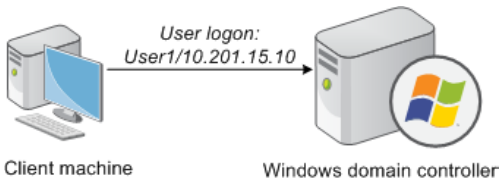
Websense Logon Agent (also called Authentication Server) identifies users in real time, as they log on to domains. Logon Agent works with the Websense logon application (**LogonApp.exe**), which runs on Windows client machines.

This collection includes the following articles to help you understand how Logon Agent works, configure Logon Agent, deploy the logon application, and troubleshoot user identification issues.

To navigate between articles, use the previous and next buttons at the top of the content pane, or click TOC for a list of articles in the collection.

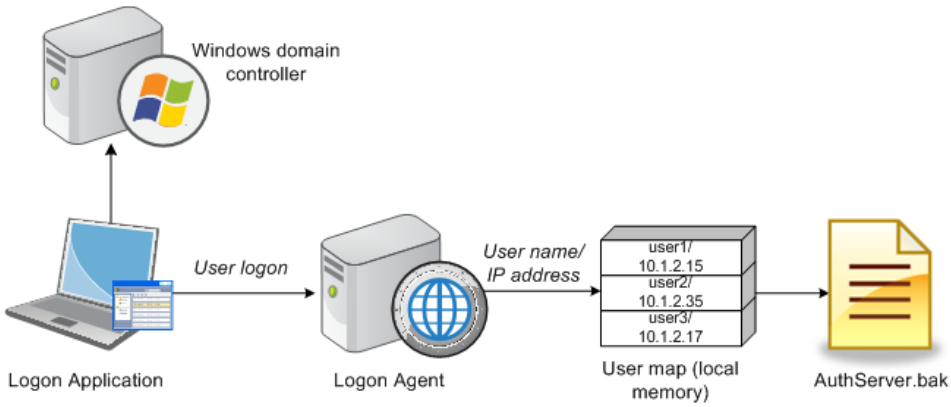
How Logon Agent identifies users

1. When users log on to the network, a network logon script invokes LogonApp.exe.



2. The logon application contacts Logon Agent via HTTP.

3. Logon Agent sends an NTLM authentication challenge, and the logon application provides a user name, hashed password, and IP address to Logon Agent.
4. Logon Agent verifies the user name/password combination from the logon application by establishing a session with the domain controller. (Logon Agent contacts User Service to determine which domain controller is the logon source.)
5. After verifying the user name/IP address pair, Logon Agent provides the information to Filtering Service and adds an entry to its user map in local memory. The user map is periodically saved to a backup file, **AuthServer.bak**.



6. Filtering Service records user name/IP address pairs to its own copy of the user map in local memory. Filtering Service is not sent confidential information (such as user passwords).

If you use both Logon Agent and DC Agent, Logon Agent takes precedence. DC Agent communicates a logon session to Filtering Service only in the unlikely event that Logon Agent has missed one.

Components used for transparent identification with Logon Agent

Using Logon Agent | Web Security Solutions | Version 7.7

Transparent identification with Websense Logon Agent uses the following components.

Logon Agent

The Websense Logon Agent can be installed on Windows or Linux, and works with the logon application installed on the Windows client.

Logon Agent can communicate with Windows Active Directory in native or mixed mode, and uses information sent by the logon application to authenticate user logon sessions from all Windows domains in your network. The agent stores authenticated user name/IP address pairs in a user map in local memory.

Multiple Logon Agent instances can be used if required; this may benefit larger networks (see *Logon Agent deployment*, page 4).

Filtering Service uses the information provided by Logon Agent to apply filtering policies to logged-on users.

A Logon Agent installation includes the following files:

Filename	Location	Functionality
AuthServer.exe	Websense\Web Security\bin or /opt/Websense/bin/ Runs as the **Websense Logon Agent** service.	The Logon Agent executable sends new entries to Filtering Service and receives configuration information from TRITON - Web Security. Uses port 30602 by default.
LogonApp.exe	Stored in a shared network location (recommended), and activated on client machines by a logon script	Captures user logon sessions as they occur. Runs on Windows client machines.
logon.bat	Resides in the same shared network location as LogonApp.exe	Invokes LogonApp.exe.
AuthServer.bak	Websense\Web Security\bin\ or /opt/Websense/	Backup copy of the Logon Agent user name/IP address map. Read at startup.
AuthServer.ini	Websense\Web Security\bin\ or /opt/Websense/	Contains one initialization parameter for Logon Agent.

LogonApp.exe

The logon application runs on Windows clients and sends user logon information to Logon Agent for authentication. The application sends user data either when logon sessions first occur, or at a specified interval (default), depending on the application's operation mode.

- In **persistent mode** (default), the logon application sends logon information to Logon Agent at a specific interval (configured using the **Query interval (persistent mode)** setting in TRITON - Web Security).
- In **nonpersistent mode**, the logon application sends logon information to Logon Agent only once for each logon. The entry remains in the user map for a specific interval (configured using the **User entry expiration (nonpersistent mode)** setting in TRITON - Web Security).

User Service

User Service provides domain controller names and IP addresses to Logon Agent so that the agent can authenticate users logged on to domains. User Service also interacts with your directory service to get group information for logged-on users.

Filtering Service

Filtering Service translates logon session data provided by Logon Agent so that the appropriate filtering policies can be applied to users, groups, and domains (OUs).

Filtering Service receives user logon session information from Logon Agent as users log on to domain controllers or machines. Filtering Service gets user data as user name/IP address pairs. When Filtering Service receives the IP address of a machine making an Internet request, it consults its user map to match the address with a user name, allowing users to be identified transparently. Filtering Service then filters users according to policies assigned to those users or groups.

Websense software can be configured to prompt users to manually authenticate if it cannot obtain user information via Logon Agent. When manual authentication is enabled, users who cannot provide a valid user name and password are blocked from Internet access.

If a user cannot be identified transparently, and manual authentication is not enabled, Websense software filters requests using computer or network policies, or the **Default** policy.

Logon Agent deployment

Logon Agent is used with Windows Active Directory, and can run on Windows or Linux machines. The logon application runs only on Windows client machines.

Logon Agent needs to be installed on only one machine in the network. However, if your network is very large (10,000+ users or 30+ domain controllers), you may benefit from installing Logon Agent on multiple machines, particularly if you have different domains in separate subnets. This way, you have ample space for files that are continually populated with user information, and the user identification process is faster.

- Only one instance of Logon Agent can be installed on a machine.
- Logon Agent and DC Agent can be run on the same machine.
- Logon Agent does not run on Websense appliances.

In most cases, you need only one Filtering Service to communicate with every instance of Logon Agent in your network. If you have installed multiple Filtering

Services for load-balancing purposes, each Filtering Service must be able to communicate with every Logon Agent.

Configuring Logon Agent settings in TRITON - Web Security

Using Logon Agent | Web Security Solutions | Version 7.7

Use the **Settings > General > User Identification** page to review and edit Logon Agent configuration information.

1. Use the Transparent Identification Agents table to select the IP address or hostname of the Logon Agent instance that you want to configure.

   If you have installed a new Logon Agent instance that does not appear in the list, click **Add Agent**, then select **Logon Agent** from the drop-down list.
2. Under Basic Agent Configuration, enter or verify the **IPv4 address or hostname** of the Logon Agent machine.

Note

Hostnames must start with an alphabetical character (a-z), not a numeric or special character.

Hostnames containing certain extended ASCII characters may not resolve properly. To avoid this issue, enter an IP address instead of a hostname.

3. Enter the **Port** that Logon Agent uses to communicate with other Websense components. The default is 30602.
4. To establish an authenticated connection between Filtering Service and Logon Agent, select **Enable authentication**, and then enter a **Password** for the connection.

Next, customize global Logon Agent communications settings. By default, changes that you make here affect all Logon Agent instances.

1. Under Logon Application Communication, specify the **Connection port** that the logon application uses to communicate with Logon Agent (15880, by default).
2. Enter the **Maximum number of connections** that each Logon Agent instance allows (200, by default).

   If your network is large, you may need to increase this number. Increasing the number does increase network traffic.

To configure the default settings that determine how user entry validity is determined, you must first determine whether Logon Agent and the client logon application operate in **persistent mode** or **nonpersistent mode** (default).

Nonpersistent mode is activated by including the /NOPERSIST parameter when launching **LogonApp.exe** (see *Prepare the logon scripts*, page 7).

- In persistent mode, the logon application contacts Logon Agent periodically to communicate user logon information.

  If you are using persistent mode, specify a **Query interval** to determine how frequently the logon application communicates logon information.

> **Note**
> If you change this value, the change does not take effect until the previous interval period has elapsed. For example, if you change the interval from 15 minutes to 5 minutes, the current 15-minute interval must end before the query starts occurring every 5 minutes.

- In nonpersistent mode, the logon application sends user logon information to Logon Agent only once for each logon.

  If you are using nonpersistent mode, specify a **User entry expiration** time period. When this timeout period is reached, the user entry is removed from the user map.

  The default interval is **24 hours**, randomized to prevent performance spikes. Individual user entries expire after 24 hours, give or take 0-20% of that time period.

When you are finished making configuration changes, click **OK** to return to the Settings > User Identification page, then click **OK** again to cache your changes. Changes are not saved until you click **Save and Deploy**.

Logon application deployment

Using Logon Agent | Web Security Solutions | Version 7.7

To use Logon Agent, you must modify the Group Policy on domain controllers so it launches the logon application (LogonApp.exe) as part of the logon script. The logon application provides a user name and IP address to Logon Agent each time a Windows client connects to Active Directory.

Client machines must use NTLM (v1 or v2) when authenticating users.

The logon application is activated via a logon script (a text file with a **.bat** or **.cmd** extension) that resides in the same directory as the logon application.

When any Websense component is installed on a Windows machine, the logon application and default script files are placed in the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin, by default).

- **LogonApp.exe**: The Websense executable that communicates user information to the Logon Agent.
- **logon.bat**: The batch file containing sample logon and logout scripts.

- **LogonApp_ReadMe.txt**: A summary of the procedures for creating and running the Websense logon script and optional logout script.

Customize the default script installed with your Websense software to meet your needs.

For preparatory steps and instructions for deploying the logon application, see:

- *Prerequisites for running the logon script*, page 7
- *Prepare the logon scripts*, page 7
- *Configure the scripts to run*, page 9

Prerequisites for running the logon script

Using Logon Agent | Web Security Solutions | Version 7.7

Logon Agent requires that the logon application run on Windows machines.

- If the logon script runs the logon application in persistent mode (sending logon information to Logon Agent at a specific interval), configure your Active Directory server **not** to run scripts synchronously.
- Be sure that all computers can connect to the shared drive on the domain controller containing **logon.bat** and **LogonApp.exe**. You must copy both of these files from the machine running Logon Agent to both the **logon** and **logout** directories on the domain controller.

  To determine if a Windows machine has access to the domain controller, run the following command from a command prompt:

  ```
  net view /domain:<domain_name>
  ```
- The TCP/IP NetBIOS Helper Service must be running on each Windows 2000, Windows XP, Windows Vista, Windows Server 2003, and Windows NT client machine that uses the logon application.
- The logon application on client machines must use NTLM (v1 or v2) authentication to communicate with Logon Agent.

To prepare and run the logon scripts, see:

- *Prepare the logon scripts*, page 7
- *Configure the scripts to run*, page 9

Prepare the logon scripts

Using Logon Agent | Web Security Solutions | Version 7.7

The default **logon.bat** file contains instructions for using the scripting parameters, and two sample scripts: a logon script that runs the logon application and a logout script. The logout script removes user information from the Websense user map when the user logs out. Only Windows Active Directory can use both types of scripts.

Construct a logon or logout script using the samples provided and the parameters in the table below. When you have finished customizing the script, continue with *Configure the scripts to run*, page 9.

The required portion of the logon script is:

```
LogonApp.exe http://<server>:<port>
```

This command runs LogonApp.exe in persistent mode (the default).

> **Note**
> You can edit the sample, or create a new batch file containing a single command.

Parameter	Description
<server>	IP address or name of the Websense Logon Agent machine. This entry must match the machine address or name entered in TRITON - Web Security.
<port>	The Logon Agent communication port (default **15880**).
/NOPERSIST	Causes the logon application to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the user map until the user's data is automatically cleared at a predefined time interval. The default user entry expiration is 24 hours, and can be changed in TRITON - Web Security. If the NOPERSIST parameter is omitted, LogonApp.exe operates in persistent mode, residing in memory on the domain server and updating the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes, and can be changed in TRITON - Web Security.
/COPY	Copies the logon application to the **%USERPROFILE%\Local Settings\Temp** directory on users' machines, where it is run by the logon script from local memory. This optional parameter helps to prevent your logon script from hanging. COPY can be used only in persistent mode.
/D	Debugging parameter that causes messages to be sent to a debugging file (Ws_LogonAppLog.txt). Use at the direction of Websense Technical Support. The file is placed in the default **temp** directory for the current user (C:\Documents and Settings\<user_account>\Local Settings\Temp).
/DHCP	Designed to accommodate mobile users. Forces LogonApp.exe to send updates to the Logon Agent when an IP address change is detected. By default, LogonApp.exe does not detect IP address changes.
/filename	Overrides the default name of the debugging file. Use the format: `/filename <debug_filename>`
/IPV6	Causes LogonApp.exe to record IPv6 addresses in its user map. By default, only IPv4 addresses are recorded.

Parameter	Description
/LEGACY	Causes LogonApp.exe to use the communication format used in versions 7.5 and earlier. This allows version 7.7 LogonApp.exe instances to communicate with earlier versions of Logon Agent.
/T	Causes trace information to be added to the HTTP records sent to Logon Agent. Use at the direction of Websense Technical Support. By default, the trace file is created in C:\.
/VERBOSE	Debugging parameter that must be used only at the direction of Technical Support.
/LOGOUT	Used only in an optional logout script, this parameter removes the user's logon information from the Websense user map when the user logs off. If you use Active Directory, this parameter can clear the logon information from the user map before the interval defined for Logon Agent has elapsed. Use this optional parameter in a logout script in a different batch file than the one containing the logon script.

Examples

The sample logon script sends user information to the Logon Agent at logon only. The information is not updated during the user's session (NOPERSIST). The information is sent to port 15880 on the server identified by IP address 10.2.2.95.

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST
```

With Active Directory you have the option to clear the logon information for each user as soon as the user logs out. (This option is not available with Windows NTLM.) Create a companion logout script in a different batch file, and place it into a different directory than the logon script.

Copy the logon batch file and rename it **Logout.bat**. Edit the script to read:

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT
```

Configure the scripts to run

Using Logon Agent | Web Security Solutions | Version 7.7

You can configure your logon script to run with a group policy on Active Directory 2003 or 2008.

Note

The following procedures are specific to Microsoft operating systems and are provided here as a courtesy. Websense, Inc., cannot be responsible for changes to these procedures or to the operating systems that employ them. For more information, see the links provided.

Active Directory 2008

Before beginning, make sure your environment meets the conditions described in *Prerequisites for running the logon script*, page 7.

1. From the Start menu on the Active Directory machine, navigate to **Administrative Tools > Group Policy Management**.
2. Expand the Domains tree, right-click a domain or OU name, and select **Create a GPO in this domain and Link it here**.
3. In the New GPO dialog box, give the GPO a descriptive name, then click **OK**.
4. Locate the new GPO in the Domains tree (under the domain or OU that you selected above), right-click it, and select **Edit**.

   If a pop-up message appears when you click on the GPO name, click **OK**.
5. In the Group Policy Object Editor, navigate to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**, then double-click **Logon** in the right pane.
6. In the Logon Properties window, click **Show Files**.

   A folder whose name ends in User\Scripts\Logon\ is displayed.
7. Copy two files into this folder: your logon script (for example, **Logon.bat**) and the application **LogonApp.exe**.
8. In the Logon Properties window, click **Add**.
9. Click **Browse** to open the logon script directory, then select your logon script file and click **OK**.
10. Verify that the logon script now appears in the list on the Logon Properties window, then click **OK**.
11. (Optional) If you are also using a logoff script, repeat steps 5 through 9. This time, double-click Logoff at Step 5 and copy your logoff batch file into the folder that opens.
12. Close the Group Policy Management Editor window for your GPO, then close the Group Policy Management window.

Repeat this procedure on each domain controller in your network, as needed.

Active Directory 2003

Before beginning, make sure your environment meets the conditions described in *Prerequisites for running the logon script*, page 7.

If your network uses Windows 98 client machines, go to the Microsoft website for assistance.

1. On the Active Directory machine, go to **Start > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the domain, and then select **Properties**.
3. On the Group Policy tab, click **New** and create a policy called **Websense Logon Script**.

4. Double-click the new policy or click **Edit**.
5. In the tree structure displayed, expand **User Configuration**, then go to **Windows Settings > Scripts (Logon/Logoff)**.
6. In the right pane, double-click **Logon**, then click **Show Files** to open this policy's logon script folder in Windows Explorer.
7. Copy two files into this folder:
   - **Logon.bat**, your edited logon batch file
   - **LogonApp.exe**, the logon application

   When you are finished, close the Explorer window.
8. In this Logon Properties dialog box, click **Add**, then enter **Logon.bat** in the Script Name field. (You can also browse to the file.)

   Leave the **Script Parameters** field empty.
9. Click **OK** twice to accept the changes.
10. (Optional) If you have prepared a logout script, repeat the preceding steps.
    - Select **Logoff** in step 6.
    - Use your logout batch file when you are prompted to copy or name the batch file.
11. Close the Group Policy Object Editor dialog box, then click **OK** in the domain Properties dialog box to apply the script.

Repeat this procedure on each domain controller in your network, as needed.

For additional information about deploying logon scripts to users and groups in Active Directory, go to the Microsoft TechNet site (technet2.microsoft.com/), and search for "Logon Scripts How To."

Windows Active Directory (mixed mode)

1. Make sure your environment meets the conditions described in *Prerequisites for running the logon script*, page 7.
2. Copy the **Logon.bat** and **LogonApp.exe** files to the **netlogon** share directory on the domain controller machine.

   ```
   C:\WINNT\system32\Repl\Import\Scripts
   ```

   Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.
3. In the Control Panel of the domain controller, select **Administrative Tools > User Manager for Domains**.
4. Select the users for whom the script must be run, and double-click to edit the user properties.
5. Click **Profile**.
6. Enter the path to the logon batch file in the **User Profile Path** field (see step 2).
7. Enter **Logon.bat** in the Logon Script Name field, then click **OK**.

Repeat this procedure on each domain controller in your network, as needed.

Configuring Logon Agent to ignore certain user names

The method that some Windows services use to contact domain controllers from user machines can cause the users logged on to those machines to be misidentified. For example, problems can be caused by:

- The internal user names (Local Service and Network Service) that Windows XP assigns for processes to use for communication with domain controllers
- Running Systems Management Server (SMS) on a client machine.

To prevent or work around possible misidentification, configure your transparent identification agent to ignore logon names that are not associated with actual users.

1. Stop **Websense Logon Agent**.
   - Windows: Use the Services dialog box.
   - Linux: Use the /opt/Websense/WebsenseDaemonControl command.
2. Navigate to the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default).
3. Use a text editor to either create or open **ignore.txt**.
4. Populate the file as follows. Place each entry on a separate line.
   - Add each **user name** that should be ignored on its own line. Websense software ignores these users, regardless of which machine they use.
   - To add a **user name/machine pair**, enter the user name, followed by a comma, and then the machine host name or IP address (ypark,YPARK-WS1). In this case, Websense software ignores the specified user only on the specified machine.
   - To add a **machine**, enter an asterisk (*), followed by a comma, followed by the machine host name, IP address, or IP address range.

   The following example shows correctly formatted entries:

   ```
   anonymous logon
   admin,WKSTA-NAME
   *, WKSTB-NAME
   *, 10.209.34.56
   *, 10.203.34.1-10.203.34.255
   ```

   In this example, the Windows 7 service account **anonymous logon** is ignored on all machines, the user name **admin** is ignored only when associated with machine **WKSTA-NAME**, and logons for **WKSTB-NAME**, **10.209.34.56**, and the network range **10.203.34.1** to **10.203.34.255** are ignored.
5. When you are finished making changes, save and close the file.
6. Start Logon Agent.

Custom configuration for a Logon Agent instance

Using Logon Agent | Web Security Solutions | Version 7.7

There is only one Logon Agent setting that can be configured locally in the configuration file for an agent instance: **UserServerWaitTime**.

This parameter ensures that Websense User Service is running before Logon Agent starts.

Default	1 [second]
Options	0 or greater
Required	No
Synopsis	Logon Agent cannot communicate data to Filtering Service if User Service is not running. When this parameter is set to 0, Logon Agent starts even if User Service is down.

To adjust the settings for this parameter:

1. Stop **Websense Logon Agent**.
   - Windows: Use the Services dialog box.
   - Linux: Use the /opt/Websense/WebsenseDaemonControl command.
2. Navigate to the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default) and open the **authserver.ini** file in a text editor.
3. Modify the value of **UserServerWaitTime** as needed.
4. Save and close the INI file.
5. Start Logon Agent.

Logon Agent troubleshooting

Using Logon Agent | Web Security Solutions | Version 7.7

If some users in your network are filtered by the **Default** policy because Logon Agent is not able to identify them:

- Make sure that Windows Group Policy Objects (GPO) are being applied correctly to these users' machines (see *Group Policy Objects*, page 14).
- If User Service is installed on a Linux machine and you are using Windows Active Directory (Native Mode), check your directory service configuration (see *User Service on Linux*, page 16).
- Verify that the client machine can communicate with the domain controller from which the logon script is being run (see *Domain controller visibility*, page 14).
- Ensure that NetBIOS is enabled on the client machine (see *NetBIOS*, page 14).

- Make sure that the user profile on the client machine has not become corrupt (see *User profile issues*, page 15).

Group Policy Objects

Using Logon Agent | Web Security Solutions | Version 7.7

After verifying that your environment meets the prerequisites described in the Deployment and Installation Center for your Websense software, make sure that Group Policy Objects are being applied correctly:

1. On the Active Directory machine, go to **Start > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the domain entry, and then select **Properties**.
3. Click the **Group Policy** tab, and then select the domain policy from the Group Domain Policy Objects Links list.
4. Click **Edit**, and then expand the User Configuration node in the directory tree.
5. Expand the Windows Settings node, and then select **Scripts**.
6. In the right pane, double-click **Logon**, and then verify that **logon.bat** is listed in the Logon Properties dialog box.

   This script is required by the client Logon Application.

   - If **logon.bat** is not in the script, refer to the Deployment and Installation Center.
   - If **logon.bat** does appear in the script, but Logon Agent is not working, use the additional troubleshooting steps in this section to verify that there is not a network connectivity problem, or refer to the Websense Knowledge Base.

Domain controller visibility

Using Logon Agent | Web Security Solutions | Version 7.7

To verify that the client machine can communicate with the domain controller:

1. Attempt to map a drive on the client machine to the domain controller's root shared drive. This is where the logon script normally runs, and where **LogonApp.exe** resides.
2. On the client machine, open a Windows command prompt and execute the following command:

   ```
   net view /domain:<domain_name>
   ```

If either of these tests fails, see your Windows operating system documentation for possible solutions. There is a network connectivity problem not related to Websense software.

NetBIOS

Using Logon Agent | Web Security Solutions | Version 7.7

NetBIOS for TCP/IP must be enabled and the TCP/IP NetBIOS Helper service must be running for the Websense logon script to execute on the user's machine.

To make sure that NetBIOS for TCP/IP is enabled on the client machine.

1. Right-click **My Network Places**, and then select **Properties**.
2. Right-click **Local Area Connection**, and then select **Properties**.
3. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. Click **Advanced**.
5. Select the **WINS** tab, and then verify that the correct NetBIOS option is set.
6. If you make a change, click **OK**, then click **OK** twice more to close the different Properties dialog boxes and save your changes.

   If no change was needed, click **Cancel** to close each dialog box without making changes.

Use the Windows Services dialog box to verify that the **TCP/IP NetBIOS Helper** service is running on the client machine. The TCP/IP NetBIOS Helper service runs on Windows 2000, Windows XP, Windows Server 2003, and Windows NT.

User profile issues

Using Logon Agent | Web Security Solutions | Version 7.7

If the user profile on the client machine is corrupt, the Websense logon script (and Windows GPO settings) cannot run. This problem can be resolved by recreating the user profile.

When you recreate a user profile, the user's existing My Documents folder, Favorites, and other custom data and settings are not automatically transferred to the new profile. Do not delete the existing, corrupted profile until you have verified that the new profile has solved the problem and copied the user's existing data to the new profile.

To recreate the user profile:

1. Log on to the client machine as a local administrator.
2. Rename the directory that contains the user profile:

   ```
   C:\Documents and Settings\<user_name>
   ```

3. Restart the machine.
4. Log on to the machine as the filtered user. A new user profile is created automatically.
5. Check to make sure the user is filtered as expected.

Copy the custom data (such as the contents of the My Documents folder) from the old profile to the new one. Do not use the File and Settings Transfer Wizard, which may transfer the corruption to the new profile.

User Service on Linux

When Websense User Service runs on Linux and Logon Agent is used for transparent user identification, Websense software must be configured to communicate with a Windows Internet Name Server (WINS). Without this step, Websense software cannot resolve domain names to domain controller IP addresses.

Use the **Settings** > **General** > **Directory Services** page in TRITON - Web Security to configure WINS communication:

1. Select **Windows Active Directory (Mixed Mode)**.

   This step is required even if you are not actually using mixed mode.
2. Enter the **Administrative user** name and **Password** for an account with administrator permissions.
3. Enter the **Domain** name.

   If your organization uses multiple domains, enter the name of a domain that is trusted by all domains that authenticate your users.
4. Enter the IP address of a Windows Internet Name Server (WINS) that can resolve the domain name entered above to a domain controller IP address.
5. Click **OK** to cache your changes, then click **Save and Deploy**.

If your network uses Active Directory in native mode, also perform the following steps:

1. On the Directory Services page, select **Active Directory (Native Mode)**.
2. Configure the global catalog servers and other settings for your directory service, if needed. Previously configured settings are typically saved when you switch from native mode to mixed mode and back again.
3. Click **OK** to cache your changes, then click **Save and Deploy**.