Using Logon Agent for Transparent User Identification

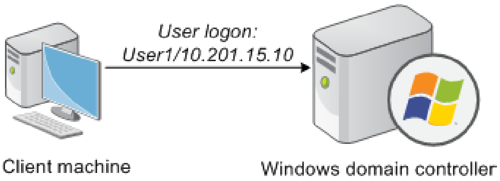
Websense Logon Agent (also called Authentication Server) identifies users in real time, as they log on to domains. Logon Agent works with the Websense logon application which runs on Windows or Mac client machines.

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

- *How Logon Agent identifies users*, page 1
- *Components used for transparent identification with Logon Agent*, page 2
- *Logon Agent deployment*, page 4
- *Configuring Logon Agent*, page 5
- *Deploying the logon application for Windows clients*, page 7
- *Deploying the logon application for Mac clients*, page 11
- *Configuring Logon Agent to ignore certain user names*, page 13
- *Logon Agent troubleshooting*, page 14

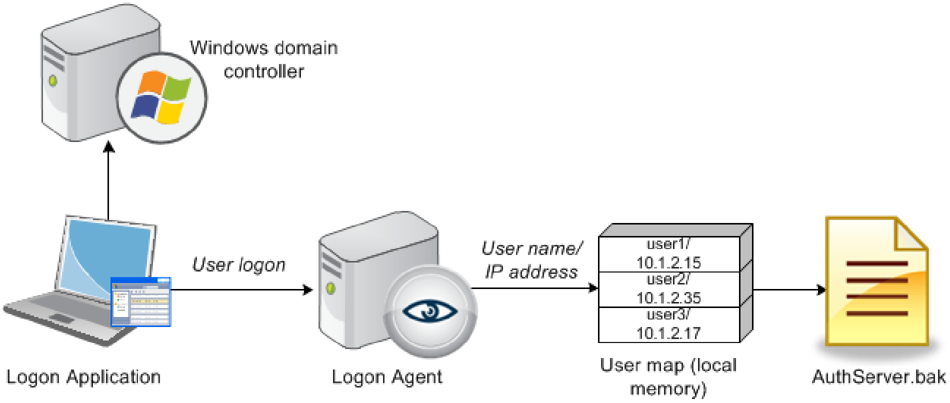
How Logon Agent identifies users

1. When users on supported Mac or Windows clients log on to a Windows domain, the logon application is invoked.



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

Transparent identification with Websense Logon Agent uses the following components.

Logon Agent

Websense Logon Agent works with the logon application installed on Windows or Mac clients.

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 policies to logged-on users.

A Logon Agent installation includes the following files:

Filename	Location	Functionality
AuthServer.exe	Websense\Web Security\bin Runs as the **Websense Logon Agent** service.	The Logon Agent executable sends new entries to Filtering Service and receives configuration information from the TRITON RiskVision manager. Uses port 30602 by default.
LogonApp.exe	Websense\Web Security\bin\LogonApp\Windows\x64 *or* \x86	Activated on Windows client machines by a logon script (logon.bat). Captures user logon sessions as they occur.
logon.bat	Websense\Web Security\bin\LogonApp\Windows	Invokes LogonApp.exe (the Windows logon application).
LogonApp.tar.gz	Websense\Web Security\bin\LogonApp\Mac	Contains an install script that, when run on Mac client machines, installs the logon application.
AuthServer.bak	Websense\Web Security\bin\	Backup copy of the Logon Agent user name/IP address map. Read at startup.
AuthServer.ini	Websense\Web Security\bin\	Contains one initialization parameter for Logon Agent.

The logon application

The logon application runs on Windows and Mac clients and sends user logon information to Logon Agent for authentication.

- In **persistent mode** (default), the Windows or Mac logon application sends logon information to Logon Agent at a specific interval (configured using the **Query interval (persistent mode)** setting in the TRITON RiskVision manager).
- In **nonpersistent mode**, the Windows 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 the TRITON RiskVision manager).

User Service

Logon Agent must be able to communicate with 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 the directory service to get group information for logged-on users.

Important

Because User Server resides on a Websense appliance, if you are using Logon Agent with Windows Active Directory in native mode, WINS is required to enable transparent user identification. See *WINS setup*, page 5.

Filtering Service

Filtering Service translates logon session data provided by Logon Agent so that the appropriate 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 uses the policies assigned to those users or groups.

If a user cannot be identified transparently, Filtering Services applies computer or network (IP address-based) policies, or the **Default** policy, to user requests.

Logon Agent deployment

Logon Agent is used with Windows Active Directory in native mode or mixed mode.

If you are using Logon Agent with Active Directory in native mode, WINS is required to enable transparent user identification (see *WINS setup*, page 5).

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.
- Transparent identification agents do not run on the appliance.

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

WINS setup

Because Websense User Service runs on a Websense appliance, Logon Agent must be configured to communicate with a Windows Internet Name Server (WINS). Without this step, Logon Agent cannot resolve domain names to domain controller IP addresses.

Use the **Settings > General > Directory Services** page in the TRITON RiskVision manager 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.

Click **OK** to cache your changes, then click **Save and Deploy**.

Logon Agent settings

Use the **Settings > General > User Identification** page in the TRITON RiskVision manager 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 logon application for Windows clients operate in **persistent mode** or **nonpersistent mode** (default).

Nonpersistent mode is activated by including the /NOPERSIST parameter when launching **LogonApp.exe** (see *Prepare the Windows logon scripts*, page 8).

◆ 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**.

Deploying the logon application for Windows clients

To use Logon Agent with Windows clients, modify the Group Policy on domain controllers so it launches the logon application (LogonApp.exe) as part of the logon script.

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 TRITON RiskVision component is installed on a Windows machine, the logon application and its support files are placed in a subdirectory of the Websense **bin** folder:

```
C:\Program Files (x86)\Websense\Web Security\bin\LogonApp\
Windows\x86
```

```
C:\Program Files (x86)\Websense\Web Security\bin\LogonApp\
Windows\x64
```

- **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 logon.bat script to meet your needs.

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

- *Prerequisites for running the Windows logon script*, page 7
- *Prepare the Windows logon scripts*, page 8
- *Configure the Windows logon scripts to run*, page 10

Prerequisites for running the Windows logon script

- 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 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 Windows logon scripts*, page 8
- *Configure the Windows logon scripts to run*, page 10

Prepare the Windows logon scripts

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 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 Windows logon scripts to run*, page 10.

The required portion of the logon script is:

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

Be sure to enter a hard return at the end of the line.

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 RiskVision.
<port>	The Logon Agent communication port (default **15880**).

Parameter	Description
/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 the TRITON RiskVision manager. 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 the TRITON RiskVision manager.
/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.
/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 Windows logon scripts to run

You can configure your logon script to run with a group policy on Active Directory 2012 or 2008. Note that earlier versions of Active Directory have not been certified with this Websense TRITON RiskVision version.

✓ **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.

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

1. Open the Group Policy Management console:
   - Active Directory 2012: From the Server Manager, navigate to **Tools** > **Group Policy Management**.
   - Active Directory 2008: 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 Management 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 version of the **LogonApp.exe** file that you want to run (32-bit or 64-bit).
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.

Deploying the logon application for Mac clients

To use Logon Agent with Mac clients, deploy a copy of the logon application to each client machine.

The logon application runs as a launch agent. It is started by the operating system for every logged-on user. At startup, the logon application queries Active Directory for logged user credentials, and if the user is authenticated, sends the user name and all client IP addresses (IPv4 and IPv6) to Logon Agent.

- After logon, the logon application sends a periodic user logon update (every 15 minutes, by default).
- When the user logs out, the logon applications sends a logout request to Logon Agent so that the user name can be removed from the user map.

When any TRITON RiskVision component is installed on a Windows machine, the logon application and its support files are placed in a subdirectory of the Websense **bin** folder:

```
C:\Program Files (x86)\Websense\Web Security\bin\LogonApp\
Mac
```

- **LogonApp.tar.gz**: A compressed archive that contains the logon application and installation scripts:
  - **LogonApp**: The logon application executable file for Mac OS X 10.8.2 and later.
  - **LogonApp.install**: The primary installation script for LogonApp.
  - **Helper files** (LogonApp.install.local, LogonApp.isntall.common, scp.expect, and ssh.expect): Additional scripts used by the main installation script. Should not be run by themselves.

Prerequisites for running the Mac logon application

Websense User Service and Websense Logon Agent may be installed on different machines, but Logon Agent must be able to communicate with User Service to both send and receive information. If Logon Agent cannot communicate with User Service, users may not be identified correctly.

Before installing the logon application on any client machine, make sure:

- You either have the administrator password for local installation or you have a user name and password with administrator privileges for remote installation.
- The (local or remote) client machine is using Microsoft Active Directory for user authentication.

Installing the Mac logon application

To install the logon application on Mac OS X 10.8.2 and later clients, you can either run the installer on the local machine, or use a remote deployment tool.

Local installation

To install the logon application locally on a client machine:

1. Use the following command to extract the contents of the **LogonApp.tar.gz** file:

   ```
   tar -zxf LogonApp.tar.gz
   ```

2. Run the **LogonApp.install** script with appropriate parameters:

   ```
   ./LogonApp.install -ah <LogonAgent> -sp <SudoPassword> [-pd]
   ```

The installation script takes the following parameters:

Parameter	Value Format	Description
-ah	10.2.20.17,10.10.50.1	The -ah parameter takes as input a comma-separated list of Logon Agent host IPv4 addresses.
-sp	password	Specifies the administrator password of the client machine.
-pd	(none)	(*optional*) Enables debugging output, recorded in the LogonApp.log file in the installation directory.
-r	(none)	(*optional*) Prompts the installer to restart the client machine after successful installation.

Remote installation

To install the logon application to one or more remote clients from a Mac server:

1. Use the following command to extract the contents of the **LogonApp.tar.gz** file:

   ```
   tar -zxf LogonApp.tar.gz
   ```

2. Run the **LogonApp.install** script with appropriate parameters:

   ```
   ./LogonApp.install -ah <LogonAgent> -sp <SudoPassword> [-pd]
   -cl <Clients> -u <Username> -p <Password>
   ```

The installation script takes the following parameters:

Parameter	Value Format	Description
-ah	10.2.20.17,10.10.50.1	The -ah parameter takes as input a comma-separated list of Logon Agent host IPv4 addresses.
-sp	password	Specifies the administrator password of the machine on which the installation script is being run (the local machine).
-pd	(none)	(*Optional*) Enables debugging output, recorded in the LogonApp.log file in the installation directory.
-cl	10.5.1.1,10.5.1.2 *or* @filename.txt	The -cl parameter can take as input either: ◆ A comma-separated list of client IPv4 addresses ◆ The name of a text file containing a list of client IPv4 addresses with each address on a separate line
-u	username	The user name for the account that the installation script should use to connect to remote client machines via SSH.
-p	password	The password for the account that the installation script should use to connect to remote client machines via SSH.
-r	(none)	(*optional*) Prompts the installer to restart client machines after successful installation.

Configuring Logon Agent to ignore certain user names

The method that some 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. Use the Windows Services tool to stop **Websense Logon Agent**.
2. Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\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.

Logon Agent troubleshooting

If some user requests are being monitored by the Default policy because Logon Agent is not able to identify the user:

- Make sure that Group Policy Objects (GPO) are being applied correctly to Windows clients, as described in *Configure the Windows logon scripts to run*, page 10.
- Because User Service is installed on a Websense appliance, if you are using Windows Active Directory (Native Mode), make sure you have configured WINS communication (see *WINS setup*, page 5).
- 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 15).
- Make sure that the user profile on the client machine has not become corrupt (see *Windows user profile issues*, page 15).

Domain controller visibility

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 Windows logon script normally runs, and where **LogonApp.exe** resides.
2. On the Windows client machine, open a 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

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 Windows client machines.

To make sure that NetBIOS for TCP/IP is enabled:

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 tool to verify that the **TCP/IP NetBIOS Helper** service is running on the client machine.

Windows user profile issues

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 affected user. A new user profile is created automatically.
5. Check to make sure the user receives the expected policy.

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.