

# v7.5: Using DC Agent

Paper 50200 / Updated: 26-May-2010

<b>Applies To:</b>	Websense Web Filter 7.5 Websense Web Security 7.5
--------------------	--

If your organization uses a Microsoft Windows-based directory service, you can use **Websense DC Agent** to enable transparent identification of users. The agent periodically queries domain controllers for user logon sessions and polls client machines to verify logon status. It runs on a Windows server and can be installed in any domain in the network.

For each logon session identified by a domain controller, DC Agent performs DNS lookup to resolve the machine name to an IP address. DC Agent stores the user name/IP address pair in a user map in local memory. It periodically writes a copy of the user map to the backup file **XidDcAgent.bak**.

DC Agent provides user names and IP addresses to Filtering Service each time its user map is updated. DC Agent sends only those new user name/IP address pairs recorded since the last query. Filtering Service records user name/IP address pairs to its own copy of the user map in local memory. There are no security risks in this data transfer, because no confidential information (such as user passwords) is transmitted.

DC Agent uses TCP (Transmission Control Protocol) to transmit data. The user data equals roughly 80 bytes per user name/IP address pair. On average, DC Agent uses 2.5 MB of RAM, but this varies by number of logon sessions per network domain controller. The following table shows average quantities of data transferred per day, by network size:

<b>Number of users</b>	<b>Data transmitted</b>
250	30 KB
2000	240 KB
10,000	1200 KB

After receiving information from DC Agent, Filtering Service queries User Service to get group information for user names in its copy of the user map. User Service queries the directory service for group information corresponding to those users, and sends the information to Filtering Service for use in applying filtering policies.

Although DC Agent requires local and domain administrator privileges to run, the agent only monitors information; it does not change any information on the domain controller or in the directory service.

See the *Transparent Identification of Users* technical paper for information comparing DC Agent and other transparent identification agents, deployment considerations, and configuration information.

The basic steps involved in using DC Agent to enable transparent user identification are simple:

1. Use the Websense Web Security installer to install Websense DC Agent on a Windows machine. See the *Installation Guide* for instructions.
2. In TRITON - Web Security, use the **Settings > General > User Identification** page to configure DC Agent to communicate with other Websense components and with domain controllers in your network. See "Configuring DC Agent" in the TRITON - Web Security Help for instructions.
3. Use TRITON - Web Security to add users and groups from your directory service as filtering clients, and assign policies to them.

## DC Agent troubleshooting (general)

Topic 50201 / Updated: 26-May-2010

<b>Applies To:</b>	Websense Web Filter 7.5 Websense Web Security 7.5
--------------------	--

### Overview

---

If you are using DC Agent for transparent identification, but it doesn't seem like user and group clients are being filtered properly, use the steps below to identify the source of the problem.

### Locate error messages

---

To start troubleshooting DC Agent user identification problems, start by assessing the status of the Websense DC Agent service:

1. On the DC Agent machine, open the Windows Services dialog box (Start > Administrative Tools > Services) and make sure that the **Websense DC Agent** service has started. If the service has stopped, right-click the service name and attempt to start it.

Regardless of whether the service starts, was already started, or refuses to start, continue with the next step.

2. Open the Windows Event Viewer (Start > Administrative Tools > Event Viewer) to look for error messages and warnings from the Websense DC Agent service.

The most common DC Agent errors are:

- ◆ **ERROR\_BAD\_NETPATH**, which indicates a network communication issue.
- ◆ **ERROR\_ACCESS\_DENIED**, which indicates a permissions issue. Although they do not make any changes to the domain, both Websense DC Agent and Websense User Service must run with domain administrator privileges. If you suspect a permissions issue, you can enable directory service auditing to find out what user and group information Websense software is trying to access.

See [DC Agent errors \(post-installation\)](#) for troubleshooting steps for both of these issues.

## Make sure that users are being identified correctly

To ensure that users are being identified correctly, start with the following procedure:

1. Log on to a machine whose users do not appear to be getting identified properly.
2. Open a browser and navigate to 4 or 5 distinctive Web sites.
3. Go to the DC Agent machine and check the Windows Event Viewer for error messages. If error message appear, see [DC Agent errors \(post-installation\)](#) for troubleshooting suggestions.
4. If there are no errors, open TRITON - Web Security and use investigative reports to see if your Internet activity (in step 2) is being logged to the correct user.
  - If the correct user name appears associated with the requests, there may be a policy configuration issue, rather than a user identification issue. Use the Check Policy tool in TRITON - Web Security to troubleshoot the issue.
  - If the user name is incorrect, see [DC Agent doesn't see some or all users](#).
  - If no user name information appears, verify that the Websense DC Agent and Websense User Service components are able to communicate with your directory service.

You can also use the TestLogServer utility, installed on the Log Server machine, to verify that user names are being recorded correctly. Note that using TestLogServer requires that Log Server be stopped. Perform this test during a low-traffic period.

1. On the Log Server machine, stop the **Websense Log Server** service.
2. Open a command prompt and navigate to the Websense **bin** directory (C:\Program Files\Websense\bin, by default).
3. Run **TestLogServer.exe**. This tool runs on port 55805, listening for data sent by Filtering Service and displaying the data to the terminal.
4. Go to another (filtered) machine, log on, open a browser, and navigate to 2 or 3 sites.

5. Return to the Log Server machine and check the information displayed by TestLogServer.
  - If the correct user name appears associated with the requests, there may be a policy configuration issue, rather than a user identification issue. Use the **Check Policy** tool in TRITON - Web Security to troubleshoot the issue.
  - If the user name is incorrect, see DC Agent does not see some or all users.
  - If no user name information appears, verify that the Websense DC Agent and Websense User Service components are able to communicate with your directory service.
6. Enter **Ctrl + C** to stop TestLogServer.
7. Restart the Websense Log Server service.

## DC Agent installation errors

Topic 50202 / Updated: 26-May-2010

<b>Applies To:</b>	Websense Web Filter 7.5 Websense Web Security 7.5
--------------------	--

### Overview

---

If you have attempted to install Websense DC Agent for transparent identification, but received installation errors, follow the steps below to troubleshoot the issue. Possible errors include:

```
Error Code 997
Could not configure DC Agent (Code 3)
```

### Details

---

Error messages can appear when you attempt to install DC Agent using an account that does not have domain and local administrator privileges. As a result, some of the required DC Agent files are not installed properly, and the Websense DC Agent service cannot run.

To correct this issue, manually remove the failed installation and reinstall the service:

1. Log on to the DC Agent machine with **domain** and **local administrator** privileges.
2. Open a command prompt (Start > Run > cmd).
3. Navigate to the Websense **bin** directory (C:\Program Files\Websense\bin, by default).

4. Use the following command to manually uninstall the DC Agent service:  

```
XidDcAgent.exe -u
```

A status message verifies that the service was successfully removed.
5. Use the following command to manually reinstall and register the DC Agent service:  

```
XidDcAgent.exe -i
```

A status message verifies that the service was successfully installed.
6. To start the service, open the Windows Services dialog box (Start > Control Panel > Administrative Tools > Services).
7. Scroll down to find the **Websense DC Agent** service, then right-click the service name and select Start.
8. Close the Services dialog box.

If the service is running correctly, after a few minutes, a **dc\_config.txt** file is created in the Websense **bin** directory.

## DC Agent errors (post-installation)

Topic 50203 / Updated: 26-May-2010

<b>Applies To:</b>	Websense Web Filter 7.5 Websense Web Security 7.5
--------------------	--

### Overview

---

If you are seeing DC Agent errors in the Windows Event Viewer or the websense.log file, or pop-up errors appear on the DC Agent machine, the sections below explain what the errors mean, which can be ignored, and which are important. The error messages addressed include:

```
System error while enumerating the domain controllers
Error Code 1058 (seen starting DC Agent)
ERROR_ACCESS_DENIED - 5
ERROR_BAD_NETPATH - 53
Kerberos Errors generated on domain controller
```

### System error while enumerating domain controllers

---

```
System error while enumerating the domain controllers.
domain: (****)ecode: 71 : message: No more connections can
```

be made to this remote computer at this time because there are already as many connections as the computer can accept."

This is a nuisance error can be ignored. It occurs when DC Agent is unable to find a specific domain controller in a perceived domain. The issue may lie with NetBIOS connectivity to the domain controller, but it is more likely that the "domain" is actually a workgroup with no domain controllers. Verify that the domain that appears in the error is a legitimate domain. If the "domain" that appears in the error message is actually a workgroup, or doesn't exist, you can ignore the error, or edit the DC Agent dc\_config.txt file to change the value of the false domain controller entry from on to off. See "Configure which domain controllers DC Agent polls" in *DC Agent doesn't see some or all users* for instructions.

When this error appears, it results from the DC Agent automatic domain discovery process, used to identify new domains and domain controllers. It can also occur when DC Agent tries to connect to a Windows XP machine that is broadcasting itself as the master browser for a non-company domain or workgroup.

## Error Code 1058 (seen starting DC Agent)

---

This issue may be caused by a Local Security Policy on the DC Agent machine that has disabled the service. To troubleshoot this issue:

1. Open the Windows Services dialog box (Start > Control Panel > Administrative Tools > Services) on the DC Agent machine.
2. Scroll down to locate the **Websense DC Agent** service. If the service is running, no further troubleshooting is necessary.
3. If the service has not started, right-click on the service name, and then select **Properties**.
4. Click the **Log On** tab of the Properties dialog box. The Hardware Profile list shows whether the service is enabled or disabled. Typically, you receive the Windows error message "Error Code 1058 - The service cannot be started" when the profile is Disabled.
5. Click **Enable** to attempt to enable the service.



### Note

For further details about the causes of this error message, refer to Microsoft KB article [241584](#).

---

6. Once the service is enabled, click OK to return to the Services dialog box.
7. Right-click on the Websense DC Agent entry, and then select Start.
8. Close the Services dialog box.

## ERROR\_ACCESS\_DENIED - 5

---

This error appears when the Websense DC Agent service does not have sufficient permissions to perform its required tasks. To address this issue, create an account with domain administrator privileges for DC Agent to use when requesting user logon information from the directory service:

1. On the DC Agent machine, create a user account with a descriptive name, like **WsDcAgent**. This account exists only to provide a security context for DC Agent when it requests information from the directory service.
  - Assign the new account domain administrator privileges in all domains.
  - Assign the same password to this account in all domains.
  - Set the password to never expire.

Make a note of the user name and password, as you will need them again shortly.

2. Open the Windows Services dialog box (Start > Administrative Tools > Services).
3. Scroll to the **Websense DC Agent** service, right-click the service name, and then select **Stop**.
4. Double-click the service name, and then select the **Log On** tab.
5. Select **This account**, and then enter the DC Agent account name and password that you just created. Some domains require that the account name be entered in the format **domain\username**.
6. Click **OK** to return to the Services dialog box.
7. Right-click the service name again, and then select **Start**.
8. Close the Services dialog box.

You may also need to assign User Service the same administrative privileges as DC Agent.

## ERROR\_BAD\_NETPATH - 53

---

If you encounter this remote access issue:

1. On the DC Agent machine, use the Windows Services dialog box (Start > Administrative Tools > Services) to verify that the **Remote Registry Service** is running.
2. Make sure that NetBIOS is bound to the network adapter on the DC Agent machine:
  - a. Right-click **My Network Places**, and then select **Properties**.
  - b. Right-click the entry for the network adapter, and then select **Properties**.
  - c. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
  - d. Click **Advanced**, and then select the **WINS** tab.
  - e. Make sure that the NetBIOS setting is **Default** or **Enable**.

- f. If you made a change, click **OK** three times to save your changes and close Properties dialog boxes.
3. Verify that the DC Agent machine and the domain controller machine are using the same network protocol for communication (for example, TCP/IP).
4. Use the **net view** command to verify that the DC Agent machine can communicate with client machines in the network:

```
net view \\<machineIPAddress>
```
5. Use the **net view** command to verify that the DC Agent machine can communicate with the domain controller machine:

```
net view \\<domaincontrollerIPAddress>
```

If the net view command fails, check the DC Agent machine's network connection and placement within the network.

## DC Agent doesn't see some or all users

Topic 50204 / Updated: 02-Dec-2010

<b>Applies To:</b>	Websense Web Filter 7.5 Websense Web Security 7.5
--------------------	--

### Overview

---

If DC Agent is installed, but user and group policies aren't being applied, DC Agent might: not be able to contact the domain controller, be retrieving information from the wrong domain controller, or have a corrupted or missing configuration file.

The following error may accompany the problem:

```
WSDCAgent : Error reading Config File: dc_config.txt  
Erroneous Entry: <string>
```

To troubleshoot issues of this type:

- ◆ [Understand how DC Agent locates domain controllers](#)
- ◆ [Configure which domain controllers DC Agent polls](#)
- ◆ [Uncover DC Agent communication issues](#)
- ◆ [Create a missing dc\\_config.txt file](#)
- ◆ [Enable the Computer Browser service \(Windows 2008\)](#)

## Understand how DC Agent locates domain controllers

---

DC Agent works by identifying domain controllers in the network, and then querying those domain controllers for user logon sessions. By default, the agent automatically verifies existing domain controllers and detects new domains or domain controllers added to the network. It stores this information in a file called **dc\_config.txt** (located in the Websense **bin** directory [C:\Program Files\Websense\bin, by default] on the DC Agent machine).

If you want DC Agent to use this automatic domain detection, make sure that NetBIOS is enabled on firewalls and routers connecting virtually or physically separate subnets or domains. In particular, TCP port 139 (used by NetBIOS) must be enabled. If NetBIOS port 139 is not enabled, then you must deploy additional DC Agents in the virtually or physically remote domains.

To identify newly added domains and domain controllers, DC Agent performs a "domain discovery" action at startup, and then once daily thereafter. If a domain controller is added just after DC Agent completes its discovery action, that controller may not be used to authenticate users for up to 24 hours. As a result, users may not be identified properly. To avoid this possibility, you can:

- ◆ Restart DC Agent after adding a new domain controller.
- ◆ Manually add the new domain controller to the **dc\_config.txt** file. (See [Configure which domain controllers DC Agent polls.](#))

DC Agent contacts each domain controller listed in the file, round-robin fashion, every ten seconds.

If you want to change how often DC Agent looks for new domain controllers, or if you do not want DC Agent to perform automatic domain detection:

1. Go to the Websense **bin** directory (by default, C:\Program Files\Websense\bin) on the DC Agent machine.
2. Make a backup copy of the **transid.ini** file in another location.
3. Open the original copy of the **transid.ini** in a text editor (like Notepad).
4. Add the line **DiscoverInterval=nn** to the file, where *nn* indicates the interval between discovery attempts. This entry is case sensitive.
  - To disable automatic domain detection, set **DiscoverInterval=0**.
  - To change how often DC Agent looks for new domain controllers, specify a new interval value (in seconds). The minimum value is 3600 seconds (1 hour). The default is 86400 seconds (24 hours).
5. Save your changes and close the file.
6. Restart the **Websense DC Agent** service.

## Configure which domain controllers DC Agent polls

---

If DC Agent is attempting to poll domain controllers that don't exist, or if you have turned off automatic domain discovery and want to have DC Agent poll a new domain controller, edit the `dc_config.txt` file to configure DC Agent behavior.

1. Go to the Websense **bin** directory (by default, `C:\Program Files\Websense\bin`) on the DC Agent machine.
2. Make a backup copy of the **dc\_config.txt** file in another location.
3. Open the original **dc\_config.txt** file in a text editor (like Notepad).
4. Confirm that all of your domains and domain controllers are listed. For example:

```
[ WEST_DOMAIN ]
dcWEST1=on
dcWEST2=on
[ EAST_DOMAIN ]
dcEAST1=on
dcEAST2=on
```

5. If there are entries in the list that DC Agent should not poll, change the entry value from on to off. For example:

```
dcEAST2=off
```

- If you configure DC Agent to avoid polling an active domain controller, the agent cannot transparently identify users logging on to that domain controller.
  - If DC Agent's automatic domain discovery has detected a domain controller that should not be used to authenticate users, set the entry to off, rather than removing it. Otherwise, the next discovery process will re-add the controller.
6. If there are domain or domain controller entries missing from the list, you can add them manually. Before adding entries, run the **net view /domain** command on the DC Agent machine to make sure that the agent can see the new domain.
  7. Save your changes and close the file.
  8. Restart the **Websense DC Agent** service.

## Uncover DC Agent communication issues

---

In order to authenticate users, DC Agent sends a NetBIOS broadcast to identify domains and their associated domain controllers. If NetBIOS is not configured properly, or if there are network communication problems, DC Agent may be unable to identify domain controllers. To identify these issues:

1. Open a command prompt (Start > Run > cmd) on the DC Agent machine.
2. Attempt to telnet to a domain controller on port **139**. If the telnet command is successful, you will see a blank screen. If unsuccessful:
  - A router, firewall, or other device may be blocking NetBIOS traffic.

- NetBIOS may not be enabled, and the domain controller may not be listening on port 139. To check the status of the port, use the **netstat** command:

Windows:

```
netstat -na | find "139"
```

Linux:

```
netstat -na | grep 139
```

3. To verify that the DC Agent machine can see all required domains, use the **net view** command:

```
net view /network
```

## Create a missing dc\_config.txt file

---

If DC Agent does not create a dc\_config.txt file, there are 2 ways to address the situation:

- ◆ Prompt DC Agent to create the file.
- ◆ Create the file manually.

To prompt DC Agent to create the file:

1. Go to the Websense **bin** directory (C:\Program Files\Websense\bin or /opt/Websense/bin/, by default) on the User Service machine.
2. Create a backup copy of the **transid.ini** file in another location.
3. Open the original **transid.ini** file in a text editor and add the following line:

```
UseUserService=False
```

This entry is case sensitive.

4. Save and close the file.
5. Restart the Websense DC Agent service. After about 2 minutes, the **dc\_config.txt** file should be created automatically.

To create the file manually:

1. Open a text editor on the DC Agent machine.
2. Use the following format to list each domain that DC Agent should poll, followed by its domain controllers, as shown below. The square brackets ([]) around the domain name are required.

```
[WEST_DOMAIN]
```

```
dcWEST1=on
```

```
dcWEST2=on
```

```
[EAST_DOMAIN]
```

```
dcEAST1=on
```

```
dcEAST2=on
```

3. Enter a carriage return after the last line in the new file. If this hard return is not included (in essence, creating a blank line at the end of the file), the last entry in the file gets improperly truncated, and an error message like "WSDCagent : Error reading Config File: dc\_config.txt Erroneous Entry: dcEAST2=o" appears in the **websense.log** file.
4. Save the file in the Websense **bin** directory (C:\Program Files\Websense\bin, by default) with the name **dc\_config.txt**.
5. Restart the Websense DC Agent service.

## Enable the Computer Browser service (Windows 2008)

When User Service or DC Agent run on a Windows Server 2008 machine, a Microsoft Service, the **Computer Browser** service, must be running to enable user identification.

Websense Setup offers the option to turn on the Computer Browser service during installation.

If you chose not to have the service started, or the installer was not successful, you must turn on the service manually:

1. Make sure that Windows Network File Sharing is enabled.
  - a. Go to **Start > Network > Network and Sharing Center**.
  - b. In the Sharing and Discovery section, set **File Sharing** to **On**.
2. Go to **Administrative Tools > Services** to open the Windows Services dialog box.
3. Double-click **Computer Browser** to open the Properties dialog box.
4. Set the Startup type to **Automatic**.
5. Click **Start**.
6. Click **OK** to save your changes and close the Services dialog box.
7. Repeat these steps on each machine running Windows Server 2008 and an affected component.