Contents

Running ConsoleClient

To launch the ConsoleClient utility:

1. Open a command prompt (Windows) or shell (Linux/Solaris) on a machine running Websense software.
2. Navigate to the appropriate directory for your operating system. By default:
   Windows: **C:\Program Files\Websense\bin**
   Linux/Solaris: **/opt/Websense/**
1. Enter the following command:
   Windows: **ConsoleClient <*IP address*> <*port*>**
   Linux/Solaris: **./WebsenseTools -d <*IP address*> <*port*>**
   Here, <*IP address*> is the IP address of the machine running the service for which you want to gather data, and <*port*> is the service's diagnostic port.
2. If the service is active and the diagnostic port is open, then the following menu displays:
   <DIAGNOSTICS>
   ****** Facilities ******
   1) Tracing
   2) PrintSelf
   Q) Quit

Use the **Tracing** option to log current activity by the selected service. Use the **PrintSelf** option to capture a service's current state or status. Other ConsoleClient menu selections vary from service to service.

Viewing the user name/IP address map for a transparent identification agent or Filtering Service

1. Navigate to the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default).
2. Enter the following command:
    - *Windows*: ConsoleClient <*IP address*> <*port*>
    - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> <*port*>

    Here, <*IP address*> is the IP address of the machine running the Websense component for which you want to gather data, and <*port*> is the component's diagnostic port. Filtering Service and the Websense transparent identification agents use the following default diagnostic ports:
    - Filtering Service: **15869**
    - DC Agent: **30601**
    - Logon Agent: **30603**
    - eDirectory Agent: **30701**
    - Radius Agent: **30801**
1. Select the following menu options:
    - PrintSelf
    - Dump to Local File
    - Level: **3**
    - Filename: **UserMap.txt**
    - XID User Map
    - Quit
2. Open the output file (**UserMap.txt**) in a text editor and examine the entries to ensure the user map contains correct user name, workstation, and IP address information.

Gathering DC Agent troubleshooting data

If incorrect user name information appears in the DC Agent user name/IP address map, you can use the following 2 procedures to gather diagnostic data:

1. Navigate to the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default).
2. Enter the following command:
    - *Windows*: ConsoleClient <*agent ip address*> 30601
    - *Linux/Solaris*: ./WebsenseTools -d <*agent IP address*> 30601

    Here, <*agent ip address*> is the IP address of the machine on which DC Agent is running. If you have changed the DC Agent diagnostic port for any reason, substitute the new diagnostic port for 30601.
1. Select the following options:
    - Tracing
    - XID DC Tracing
    - Enable Tracing
2. Have a user who was previously not properly authenticated log on to the domain again.
3. Return to ConsoleClient and select the following options:
    - Disable Tracing
    - Dump Decoded Buffer
    - Dump to Local File
    - Filename: **dctrace.txt**
    - Format Option: **0**
    - Return to Previous Menu

- Quit

4. Open the output file (**dctrace.txt**) in a text editor and examine its contents. Search for the user who logged onto the network for testing. If the user is not found, look for NetBIOS errors, which may explain the problem.

To gather further DC Agent logging data:

1. Enter the ConsoleClient command again:
   - *Windows*: ConsoleClient <*agent ip address*> 30601
   - *Linux/Solaris*: ./WebsenseTools -d <*agent IP address*> 30601

   Here, <*agent ip address*> is the IP address of the machine on which DC Agent is running. If you have changed the DC Agent diagnostic port for any reason, substitute the new diagnostic port for 30601.
1. Select the following options:
   - Tracing
   - XID DC Streaming Tracing
   - Enable Tracing
2. Let the utility gather data for 10 minutes.
3. After 10 minutes, return to ConsoleClient and select the following options:
   - Disable Tracing
   - Dump Decoded Buffer
   - Dump to Local File
   - Filename: **dclog.txt**
   - Format Option: **4**
   - Return to Previous Menu
   - Quit
4. Open **dclog.txt** file in a text editor and examine its contents.

Collecting Network Agent diagnostic data

You can use ConsoleClient to review the data (packets) being monitored by Network Agent.

1. Navigate to the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default).
   - *Windows*: ConsoleClient <*IP address*> 55870
   - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 55870

   Here, <*IP address*> is the IP address of the machine on which Network Agent is running.
1. Select the following options:
   - Tracing
   - NetworkAgent Tracing
   - Set Buffer Size: **10000** KB
   - Enable Tracing
2. Reproduce the issue that you are trying to troubleshoot. For example, browse the Internet from a specific machine, or as a specific test user. Typically, perform the test for at least 1 minute.
3. Return to ConsoleClient and select the following options:
   - Disable Tracing
   - Dump Decoded Buffer
   - Dump to Local File
   - File name: **nadiag.txt**
   - Format Option: **0**
   - Return to the Previous Menu

- Quit

4. Open the **nadiag.txt** file in a text editor, and then search the file for the traffic generated during the test.

You can also use the **PrintSelf** option to troubleshoot performance issues. A high number of active connections may indicate problems.

1. Navigate to the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default).
   - *Windows*: ConsoleClient <*IP address*> 55870
   - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 55870

   Here, <*IP address*> is the IP address of the machine on which Network Agent is running.
1. Select the following options:
   - PrintSelf
   - Dump to Local File
   - Level: **3**
   - File name: **nainfo.txt**
   - Network Agent PrintSelf
   - Quit
2. Open the **nainfo.txt** file in a text editor.

Retrieving a list of manually authenticated users from Filtering Service

You can use the ConsoleClient PrintSelf option to capture a list of users prompted for manual authentication. To do this, follow the steps in Viewing the user name/IP address map for a transparent identification agent or Filtering Service, but after entering a name for the output file, select **User Map** instead of **XID User Map**.

The resulting output file shows only users who were prompted for their logon information. Users who fail manual authentication are denied Internet access. Denied users do not generate Internet traffic, so no data is logged to the Websense reporting database. Thus, SQL queries against the database will not show denied users. However, since Websense received the Internet request, one seat is added to the current subscription count.

Viewing status and HTTP lookup requests received by Filtering Service

ConsoleClient can be used to log HTTP lookup requests sent to Filtering Service by Network Agent or a third-party integration product. Review HTTP lookup requests to see whether Network Agent or your integration is communicating successfully with Filtering Service. This procedure can also be used to detail the latency involved in processing a lookup request.

The same ConsoleClient procedure can be used to determine whether Filtering Service is responding to server status requests from a third-party integration product. If the integration does not receive a reply from Filtering Service within its time limit, than an integrated firewall product will fail open or closed, as configured. Filtering Service normally responds within 1 minute to server status requests.

To create a log file showing Filtering Service responses to status and lookup requests:

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default), enter the enter the following command:
   - *Windows*: ConsoleClient <*IP address*> 15869
   - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 15869

   Here, <*IP address*> is the IP address of the Filtering Service machine, and 15869 is the Filtering Service diagnostic port.

1. Select the following options:
    - Tracing
    - WISP
    - Set Buffer Size: **10000** KB
    - Enable Tracing
2. At this point, ConsoleClient begins to log all traffic between Network Agent or the integration product and Filtering Service. Begin generating HTTP lookup requests by browsing the Internet for at least 1 minute. Note the specific sites (URLs) that you visit so that you can verify that the associated lookup requests are being passed to Filtering Service correctly.
3. When you are finished performing the test, return to ConsoleClient and select the following options:
    - Disable Tracing
    - Dump Decoded Buffer
    - Dump to Local File
    - Filename: **fstrace.txt**
    - Format Option: **0**
    - Return to Previous Menu
    - Quit
4. Open the output file (**fstrace.txt**) in a text editor and search for the URLs that you visited during the test. Check the received and response times. Requests taking longer than 200 ms (milliseconds) may be indicative of a problem. If the sites that you visited are not in the logs, Filtering Service is not receiving the lookup requests. If no traffic at all appears in the logs, make sure that Network Agent or the integration product is configured properly. Also check to see if any network device is intercepting traffic between Filtering Service and Network Agent or the integration product.

NOTE	Not all third-party integration products use the same method to communicate with Filtering Service, and some send lookup requests that do not include full URLs. This can result in tracing output that does not include all of the URL information described in this article, even though the integration product and Filtering Service are communicating correctly.

Requesting a subscription count from Filtering Service

A valid subscription is required to download the Master Database and begin filtering with Websense software. The number of users filtered depends on the subscription level.

ConsoleClient includes a Subscription Tracker that can be used to list each unique IP address encountered by Filtering Service for today, the current week, and the previous week. The Subscription Tracker shows:

Subscription Map Contents
: The list of IP addresses seen by Filtering Service

Number of subscribed users (EIM DTF CPM net)
: Number of subscriptions purchased for Filtering (EIM), Remote Filtering (DTF), and Client Policy Manager (CPM)

Subscription map size
: Current IP address count

Exceeded subscription map size

Number of unique IP addresses in excess of the subscription level

Previous day user count

Total count of unique IP addresses seen the previous day

Current week user count (max)

Total unique IP addresses counted for any single day since Sunday

Previous week user count (max)

Total unique IP addresses counted for any single day since Sunday of the previous week.

Last date map cleared

Indicates the day of the week when the Subscription map was last cleared.
(0= Sunday, 1=Monday, 2=Tuesday, 3=Wednesday, 4=Thursday, 5=Friday, 6=Saturday)

Last day subscription exceeded email

A value of **-1** indicates this has never happened.
A value of **0** indicates a subscription-exceeded email was sent.

Last day subscription 90% email

A value of **-1** indicates this has never happened.
A value of **0** indicates an email was sent.

To find out how many unique connections Websense software has added to its user count:

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default), enter the following command:
   - *Windows*: ConsoleClient <*IP address*> 15869
   - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 15869

   Here, <*IP address*> is the IP address of the Filtering Service machine, and 15869 is the Filtering Service diagnostic port.
1. Select the following options:
   - PrintSelf
   - Dump to Local File
   - Level: **3**
   - Filename: **subscrip.txt**
   - Subscription Tracker
   - Quit
2. Open the output file (**subscrip.txt**) in a text editor.

Troubleshooting a blank block page

If users are receiving blank block pages, use ConsoleClient to capture the HTTP traffic associated with the request.

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default), enter the following command:
   - *Windows*: ConsoleClient <*IP address*> 15869
   - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 15869

   Here, <*IP address*> is the IP address of the Filtering Service machine, and 15869 is the Filtering Service diagnostic port.
1. Select the following options:
   - Tracing
   - HTTP Agent
   - Set Buffer Size: **10000** KB
   - Enable Tracing

2. Spent 1 minute browsing the Internet on a machine that has received a blank block page. After 1 minute, go to a site that results in a blank block page.
3. Return to the ConsoleClient and select the following:
    - Disable Tracing
    - Dump Decoded Buffer
    - Dump to Local File
    - Filename: **tsblockpage.txt**
    - Format Option: **4**
    - Return to Previous Menu
    - Quit
4. Repeat the previous process, but this time select **HTTP Requests** instead of HTTP Agent. Also, give the output file a different name (like "httpreq.txt").
5. Open each output file and search for both the IP address of the machine on which the test was performed, and the site (URL) that resulted in a blank block page.

Reviewing quota time usage

Use ConsoleClient to retrieve quota time statistics from Filtering Service.

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default), enter the following command:
    - *Windows*: ConsoleClient <*IP address*> 15869
    - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 15869

Here, <*IP address*> is the IP address of the Filtering Service machine, and 15869 is the Filtering Service diagnostic port.

1. Select the following options:
    - PrintSelf
    - Dump to Local File
    - Level: **3**
    - Filename: **quotatime.txt**
    - Quota Agent
    - Quit
2. Open the output file (**quotatime.txt**) in a text editor.
   Here's a sample quota log:

   ```
   ---------------------------------------------------------------------
   Quota Agent1 - PrintSelf - Level: 3
   Time: Thu Dec 20 07:38:06.888 2007
   ---------------------------------------------------------------------
   User/Group cache size: 0
   WkSta/Network cache size: 0

   QuotaNames
   Nbr of users configured by name: 0
   Current configuration key: 1

   QuotaNetWorks
   Nbr of wksta/networks configured: 0
   Current configuration key: 2
   ```

QuotaGroups
Nbr of users configured by group: 0
Current configuration key: 2

QuotaDomains
Nbr of users configured by domain: 0
Current configuration key: 2

QuotaOtherTime
Current quota interval in minutes: 10
Current quota default time in minutes: 60

Requesting protocol and policy status from Filtering Service

If there appears to be an unexplained conflict between policies, use the following procedure to diagnose the issue.

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense, by default), enter the following command:
    - *Windows*: ConsoleClient <*IP address*> 15869
    - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 15869

    Here, <*IP address*> is the IP address of the Filtering Service machine, and 15869 is the Filtering Service diagnostic port.
1. Select the following options:
    - PrintSelf
    - Dump to Local File
    - Level: **3**
    - Filename: **PolicyData.txt**
    - Policy Data
    - Quit
2. Repeat the preceding steps, but this time give the output file a different name (like "protocoldata.txt") and select **Protocol Policy** instead of Policy Data.
3. Open the output files in a text editor and examine the data.

Requesting current status from CPM Server

You can use the PrintSelf option to capture the current state of CPM Server.

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense), enter the following command:
    - *Windows*: ConsoleClient <*IP address*> 55830
    - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 55830

    Here, <*IP address*> is the IP address of the CPM Server machine, and 55830 is the CPM Server diagnostic port.
1. Select the following options:
    - PrintSelf
    - Dump to Local File
    - Level: **3**
    - Filename: **cpmstatus.txt**
    - Select additional information as appropriate:

        ******** Settings ********

** Dump to Local File
** Level: 3
** Filename: cmpstatus.txt
****
***** PrintSelf Modules *****
1) Ini File Parameters
2) Comm Demultiplexer
3) Comm Connection Pool
4) WsDTMClientIDCache
5) Inventory Queue
6) WsDTMStatusAgent
7) DTM User Stats
8) WsDTMAppServer
9) Response Map
10) WsDTMPolicyAgent
11) RTUConfigCallback
12) Category Diff Manager
13) Log Agent Statistics
14) WsDTMNacServer
***** Options *****
A) change Dump Option
B) change Level setting
C) change Local Filename
M) return to the main menu
Q) Quit

- Quit

2. Open the output file (**cpmstatus.txt**) in a text editor to review the data.

If CPM Server seems to be "hung," so that CPM clients are unable to connect, or if clients appear unresponsive, select the **WsDTMAppServer** option.
If clients appear unresponsive and all connections are in use, note their state. They may be handling a log file.

Retrieving email and SNMP alert data and status from Usage Monitor

1. From the appropriate directory (C:\Program Files\Websense\bin or /opt/Websense), enter the following command:
   - *Windows*: ConsoleClient <*IP address*> 55816
   - *Linux/Solaris*: ./WebsenseTools -d <*IP address*> 55816

   Here, <*IP address*> is the IP address of the Usage Monitor machine, and 55816 is the Usage Monitor diagnostic port.
1. Select the following displayed options:
   - PrintSelf
   - Dump to Local File
   - Level: **3**
   - Filename: **usage.txt**
   - WsAlertFilterEngine
   - Quit

2. Open the output file (**usage.txt**) in a text editor and examine the contents.

ConsoleClient "Server Timeout Occurred" error

If you attempt to use ConsoleClient to connect to a Websense service that runs on a Windows machine, and receive the error **Server Timeout Occurred**, try the following:

1. On the Websense service machine, go to **Start > Run** and enter **services.msc**.
2. Select, and then double-click, the name of the Websense service for which the issue occurs.
3. On the **Log On** tab, select the **Local System account** radio button.
4. Mark the **Allow services to interact with desktop** check box.
5. Click **Apply**.
6. Select the **This account** radio button. The **Allow services to interact with desktop** check box is disabled, but the check mark is not removed.
7. Re-enter the service account name and password.
8. Click **OK**.
9. Restart the Websense service.

If you encounter this error when attempting to connect to Filtering Service (port 15869):

- Make sure that the IP address is correct and that the service is running.
- Open the **eimserver.ini** file and verify that the **DiagServerPort** entry shows the correct port (by default, **15869**. If this data is missing, add it, save and close the file, and restart Filtering Service.
- Use ConsoleClient to connect to another Websense service to verify that the tool is working (for example, connect to DC Agent on port 30601 or Network Agent on port 55870.)
- Restart the queried service.
- The error may be encountered if no data is available.