Webinar Information

- **Title: Advanced Troubleshooting Techniques of Websense Web Security Products**

- Audio information:
  - **This presentation incorporates STREAMING AUDIO.**
  - Use of speakers or headsets is required. *If unable to hear streaming audio or it is choppy*, a limited number of dial-in numbers are available.
- Dial-in numbers:
  - **U.S. dial-in numbers:**

    Toll free: **1-888-373-5705**, pass-code: **922187**

    Toll: **1-719-457-3840**, pass-code: **922187**
  - **Find international dial-in numbers at:**
    - http://www.websense.com/dec2009_international
    - Pass-code: **922187**

websense
ESSENTIAL INFORMATION PROTECTION™

Advanced Troubleshooting Techniques of Websense Web Security Products

Support Webinars

web security | data security | email security

Webinar Presenter

Wiley DeMoll

- Title: Technical Support Specialist
  - Employee of Websense since 2005
  - Websense Certified Web Security Associate
  - CCNA (In progress)
  - Graduate of Coleman College

Goals and Objectives

- Identify the cause of common issues for troubleshooting
- Demonstrate comprehensive troubleshooting techniques used by Websense Technical Support
  - Filtering Service troubleshooting via ConsoleClient
  - User Service troubleshooting via DSTrace
  - WebsensePing
  - TestLogServer
  - Network Agent troubleshooting
  - Log Server troubleshooting

ConsoleClient

- What is ConsoleClient?
  - A command-line utility used to retrieve statistics and diagnostic information for Websense services.
- What do I get by running ConsoleClient?
  - View the user name/IP address map used by transparent identification agents and Filtering Service
  - Retrieve a list of manually authenticated users from Filtering Service
  - View status and http lookup requests received by Filtering Service (via a Filtering Service, or WISP, trace)

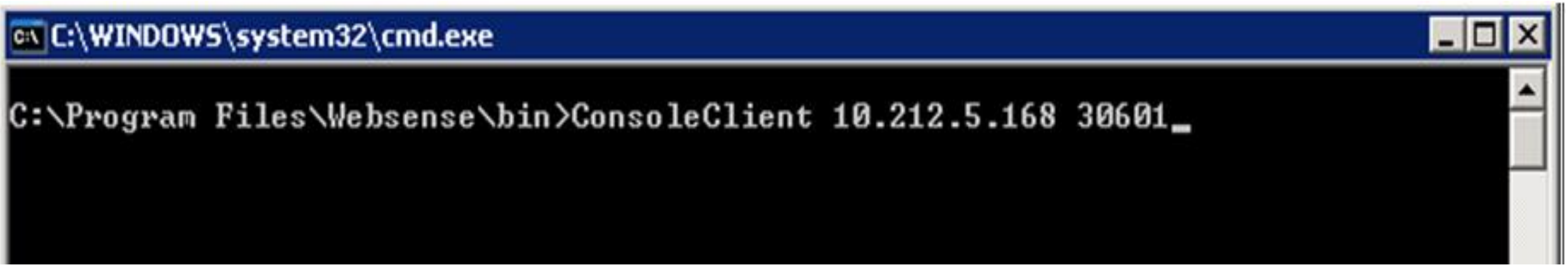
ConsoleClient

- To access ConsoleClient, open a command prompt and navigate to the appropriate directory:
  - Windows default:
    C:\Program Files\Websense\bin
  - Linux default:
    /opt/Websense/
- The command to run the utility is:
  - Windows:
    ConsoleClient <*IP address*> <*diagnostic port*>
  - Linux:
    ./WebsenseTools -d <*IP address*> <*diagnostic port*>

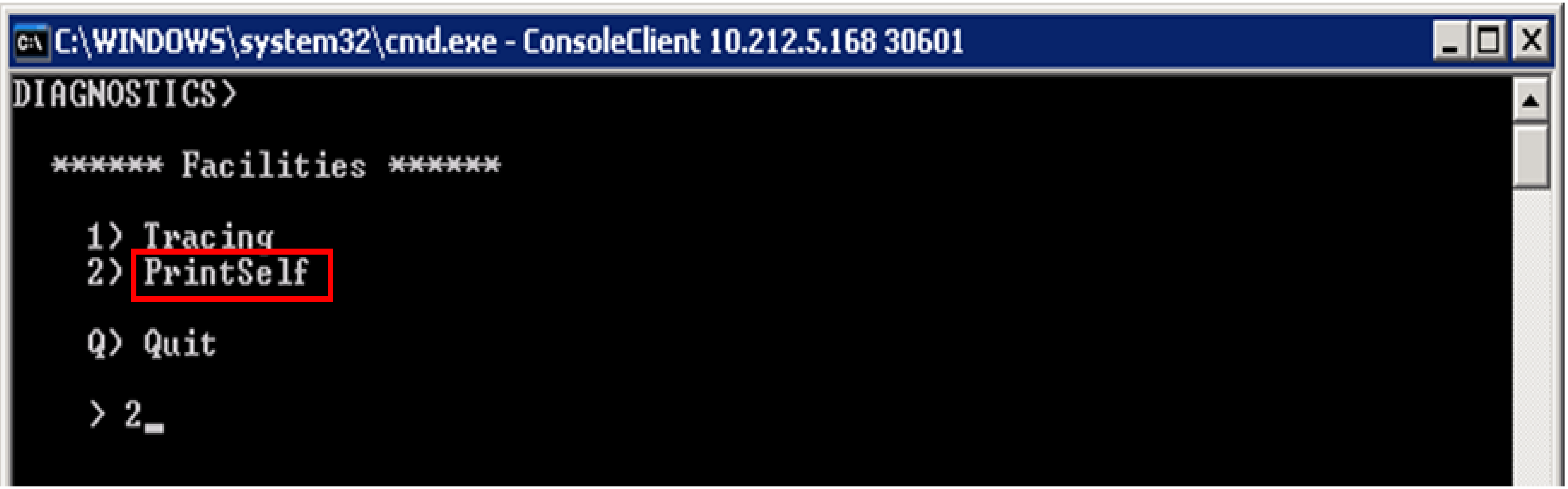
ConsoleClient

- Default diagnostic ports for transparent identification agents:
  - DC Agent: 30601 (Windows)
  - Logon Agent: 30603 (Windows)
  - eDirectory Agent: 30701 (Novell)
  - RADIUS Agent: 30801 (Windows)

ConsoleClient: DC Agent

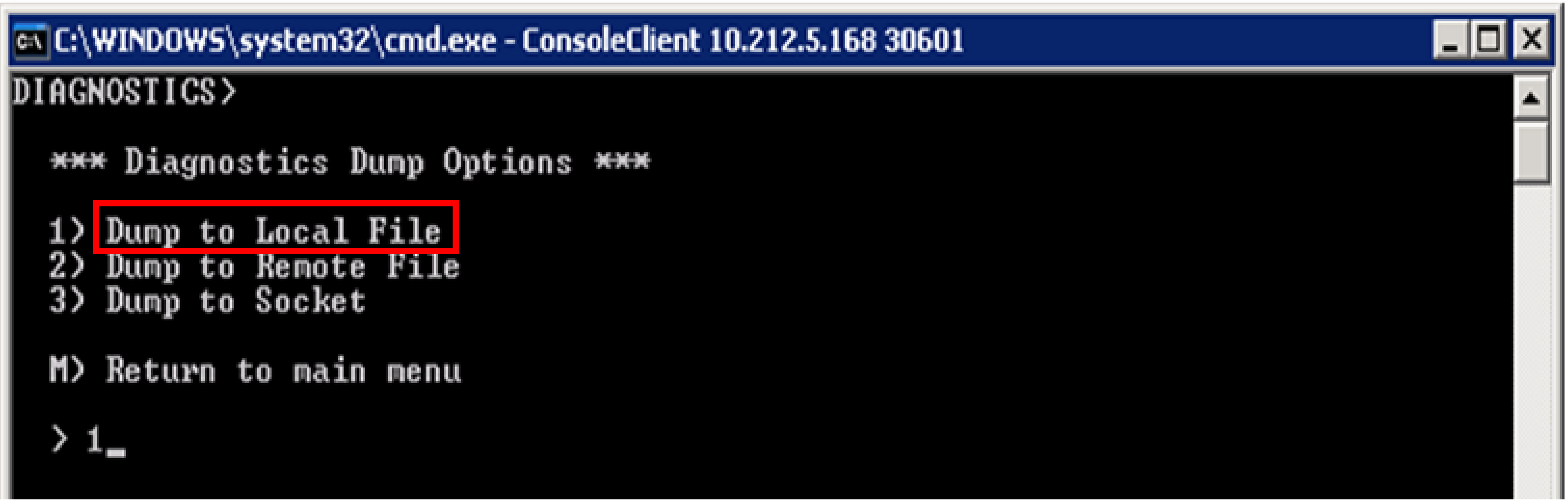


```
C:\Program Files\Websense\bin>ConsoleClient 10.212.5.168 30601_
```


C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 30601

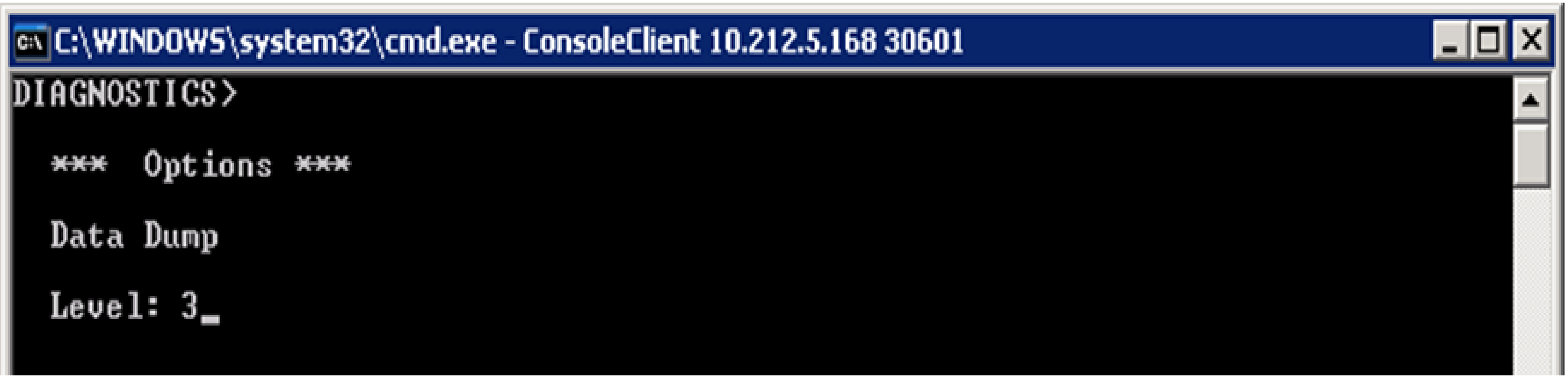
```
DIAGNOSTICS>

  ****** Facilities ******

    1) Tracing
    2) PrintSelf

    Q) Quit

    > 2_
```

ConsoleClient: DC Agent



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 30601

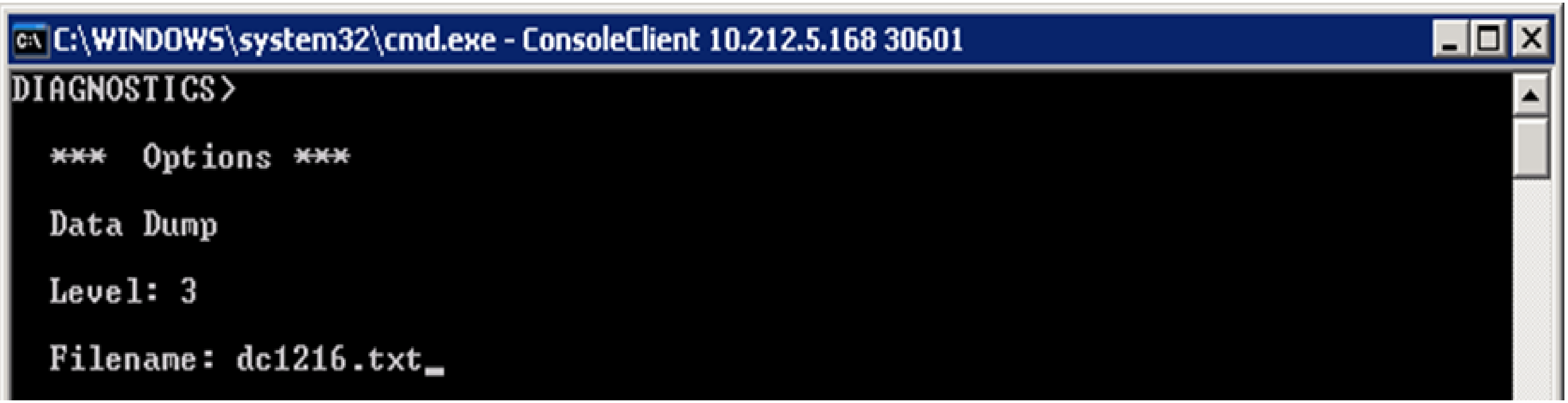
```
DIAGNOSTICS>

  *** Diagnostics Dump Options ***

  1) Dump to Local File
  2) Dump to Remote File
  3) Dump to Socket

  M) Return to main menu

  > 1_
```



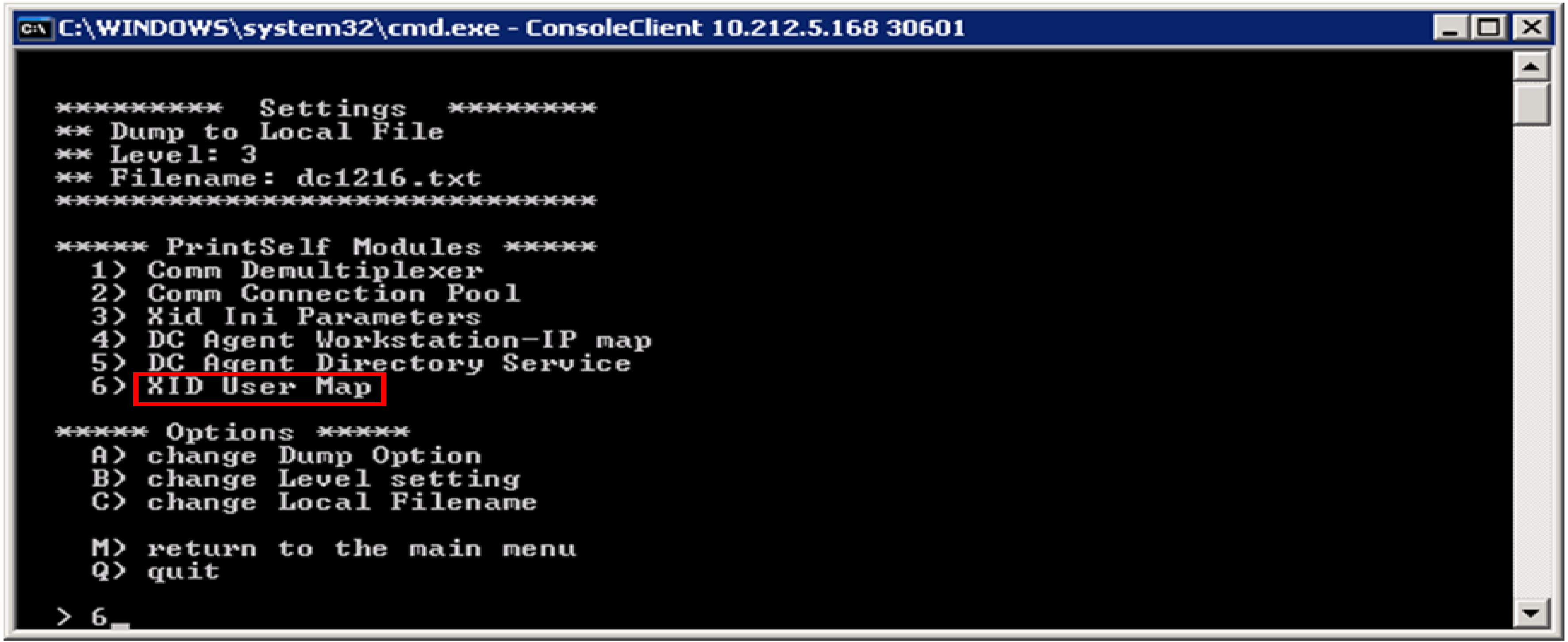
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 30601

```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Level: 3_
```

ConsoleClient: DC Agent

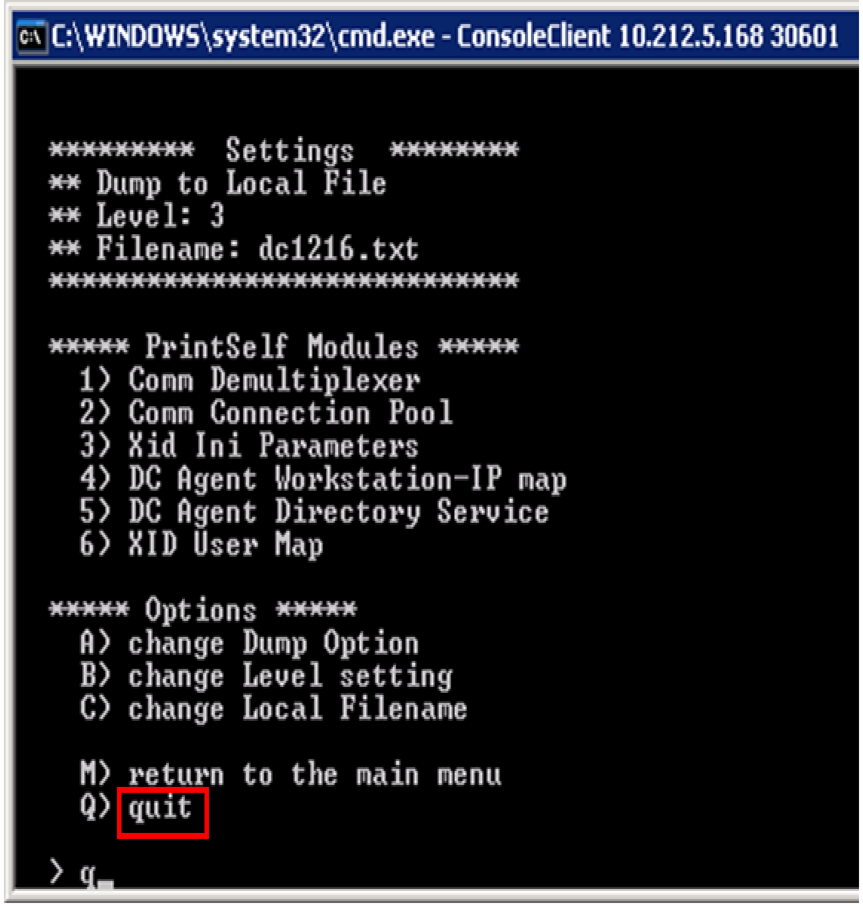

C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 30601

```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Level: 3

  Filename: dc1216.txt_
```


C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 30601

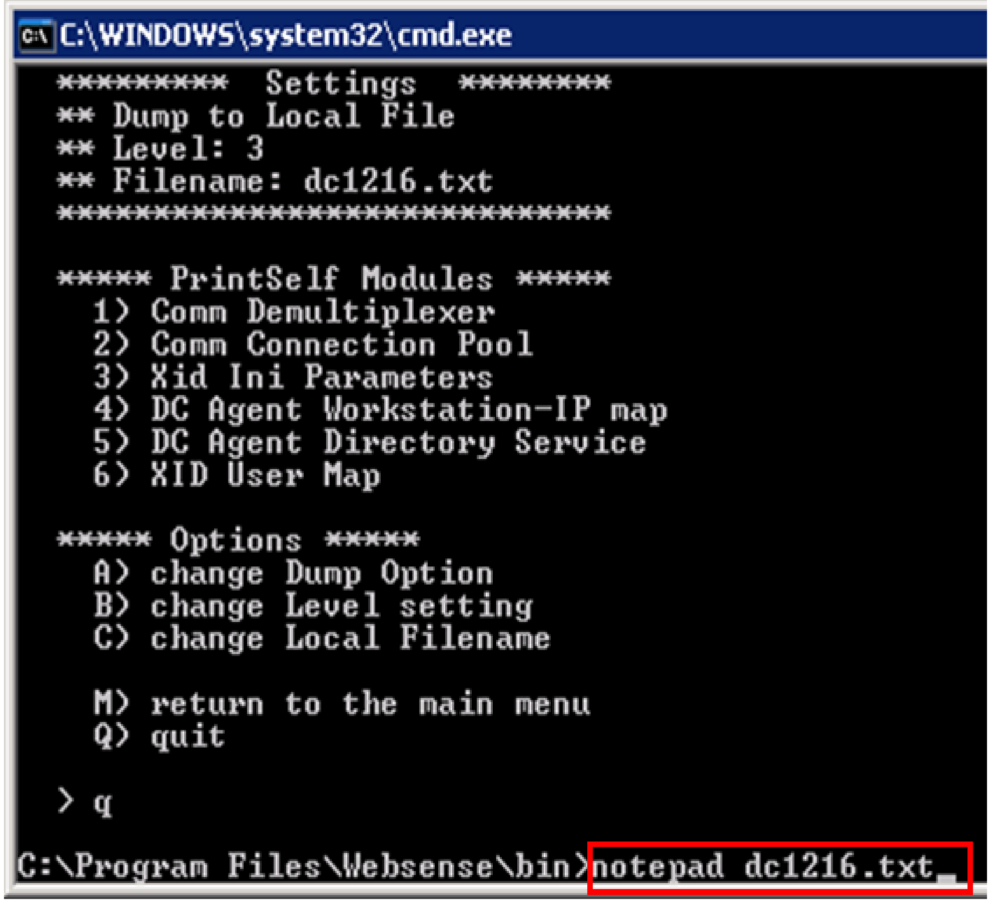
```

  *********  Settings  ********
  ** Dump to Local File
  ** Level: 3
  ** Filename: dc1216.txt
  *****************************

  ***** PrintSelf Modules *****
    1) Comm Demultiplexer
    2) Comm Connection Pool
    3) Xid Ini Parameters
    4) DC Agent Workstation-IP map
    5) DC Agent Directory Service
    6) XID User Map

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > 6_
```

ConsoleClient: DC Agent



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 30601

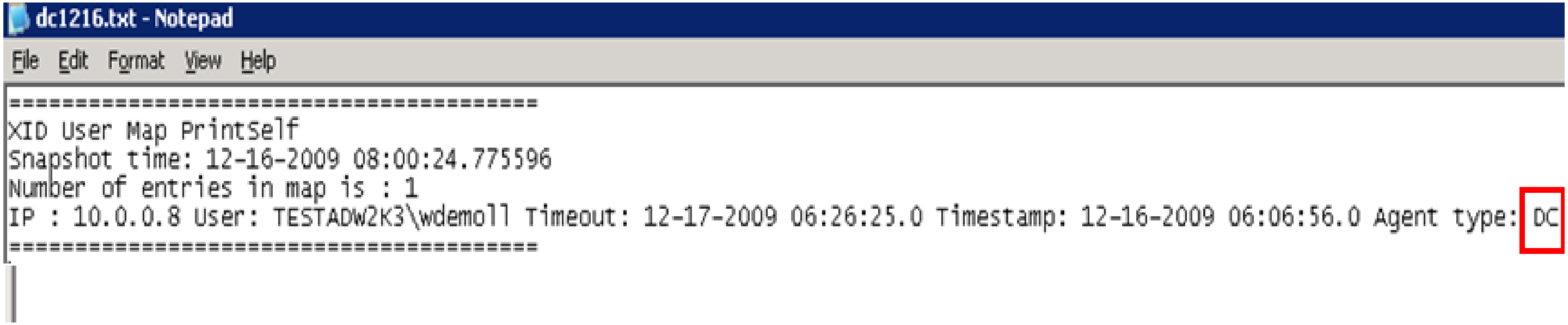
```
*********  Settings  ********
** Dump to Local File
** Level: 3
** Filename: dc1216.txt
*****************************

***** PrintSelf Modules *****
  1) Comm Demultiplexer
  2) Comm Connection Pool
  3) Xid Ini Parameters
  4) DC Agent Workstation-IP map
  5) DC Agent Directory Service
  6) XID User Map

***** Options *****
  A) change Dump Option
  B) change Level setting
  C) change Local Filename

  M) return to the main menu
  Q) quit

> q_
```



```
  *********  Settings  ********
  ** Dump to Local File
  ** Level: 3
  ** Filename: dc1216.txt
  *****************************

  ***** PrintSelf Modules *****
    1) Comm Demultiplexer
    2) Comm Connection Pool
    3) Xid Ini Parameters
    4) DC Agent Workstation-IP map
    5) DC Agent Directory Service
    6) XID User Map

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > q

C:\Program Files\Websense\bin>notepad dc1216.txt_
```

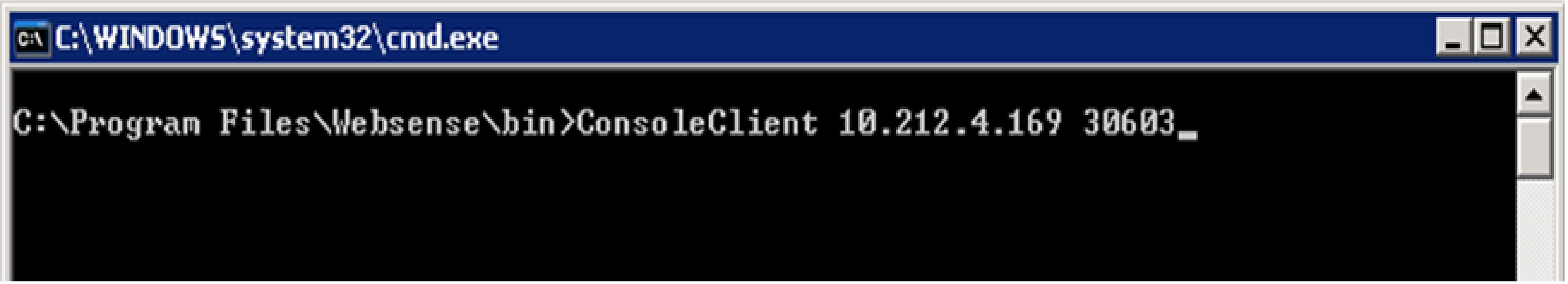
ConsoleClient: DC Agent

- The text file looks something like this:

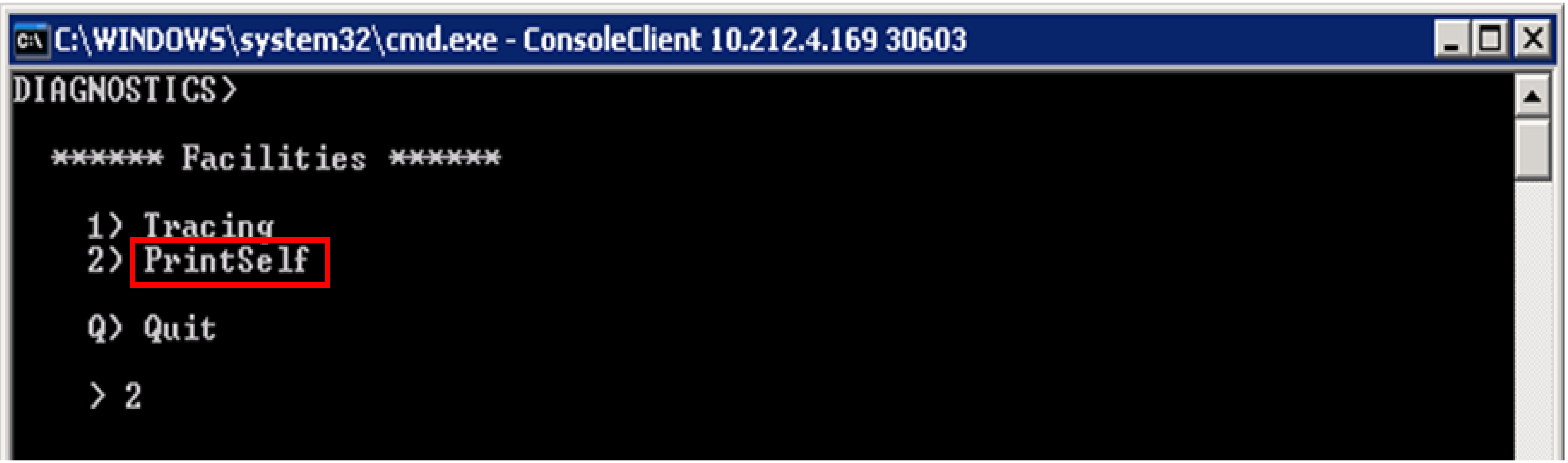


```
=========================================
XID User Map PrintSelf
Snapshot time: 12-16-2009 08:00:24.775596
Number of entries in map is : 1
IP : 10.0.0.8 User: TESTADW2K3\wdemoll Timeout: 12-17-2009 06:26:25.0 Timestamp: 12-16-2009 06:06:56.0 Agent type: DC
=========================================
```

ConsoleClient: Logon Agent



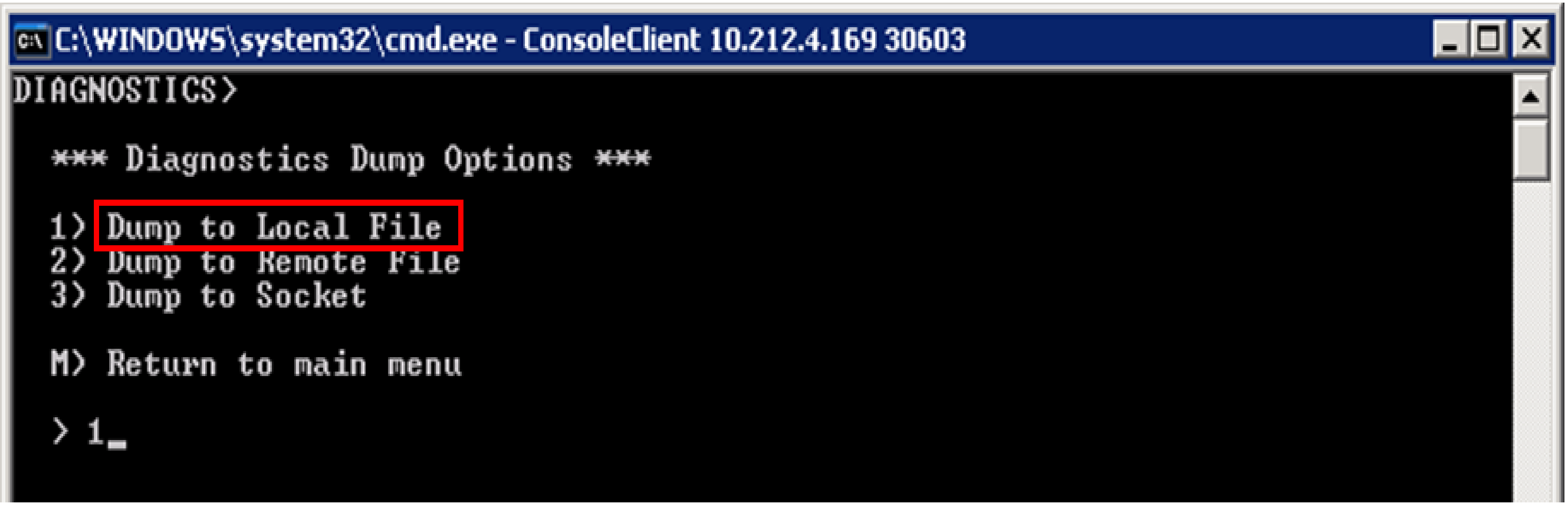
```
C:\Program Files\Websense\bin>ConsoleClient 10.212.4.169 30603_
```



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.4.169 30603

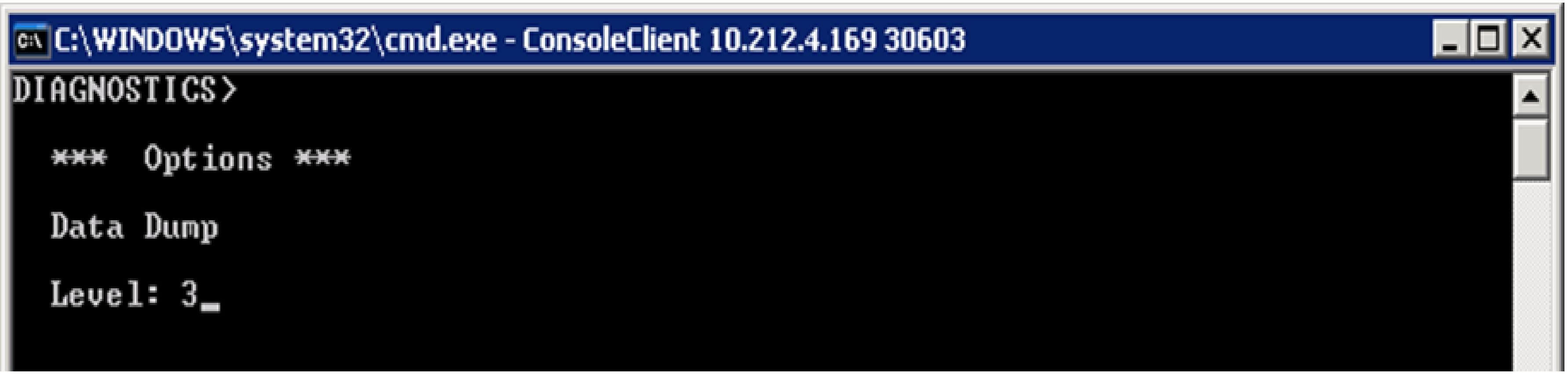
```
DIAGNOSTICS>

  ****** Facilities ******

    1) Tracing
    2) PrintSelf

    Q) Quit

    > 2
```

ConsoleClient: Logon Agent



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.4.169 30603

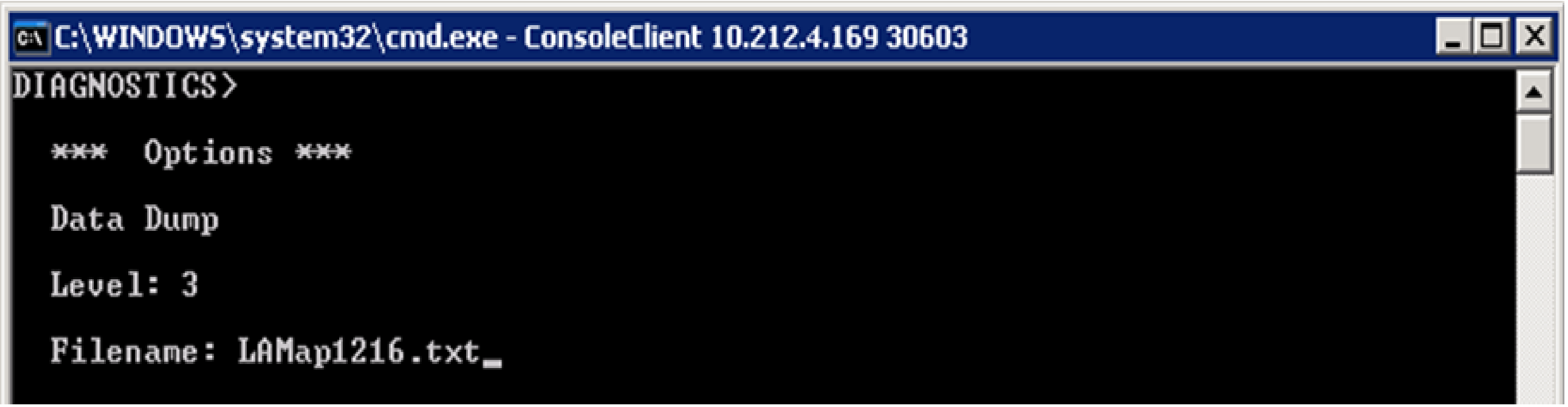
```
DIAGNOSTICS>

  *** Diagnostics Dump Options ***

  1) Dump to Local File
  2) Dump to Remote File
  3) Dump to Socket

  M) Return to main menu

  > 1_
```



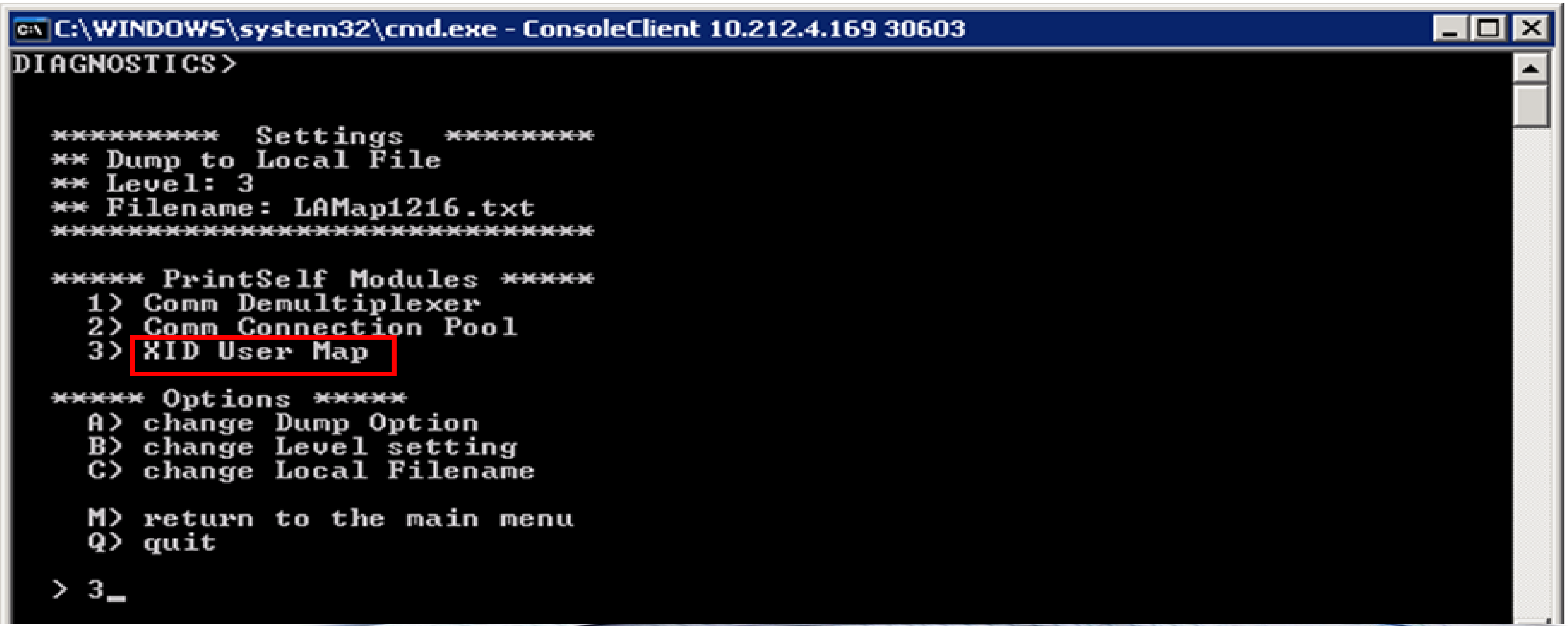
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.4.169 30603

```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Level: 3_
```

ConsoleClient: Logon Agent

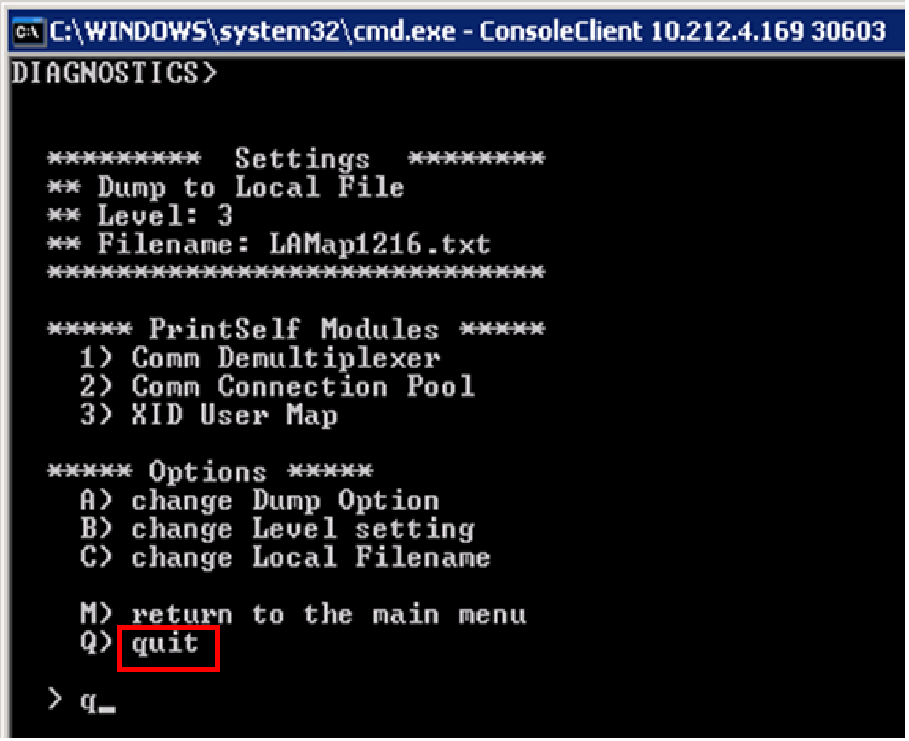

C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.4.169 30603

```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Level: 3

  Filename: LAMap1216.txt_
```

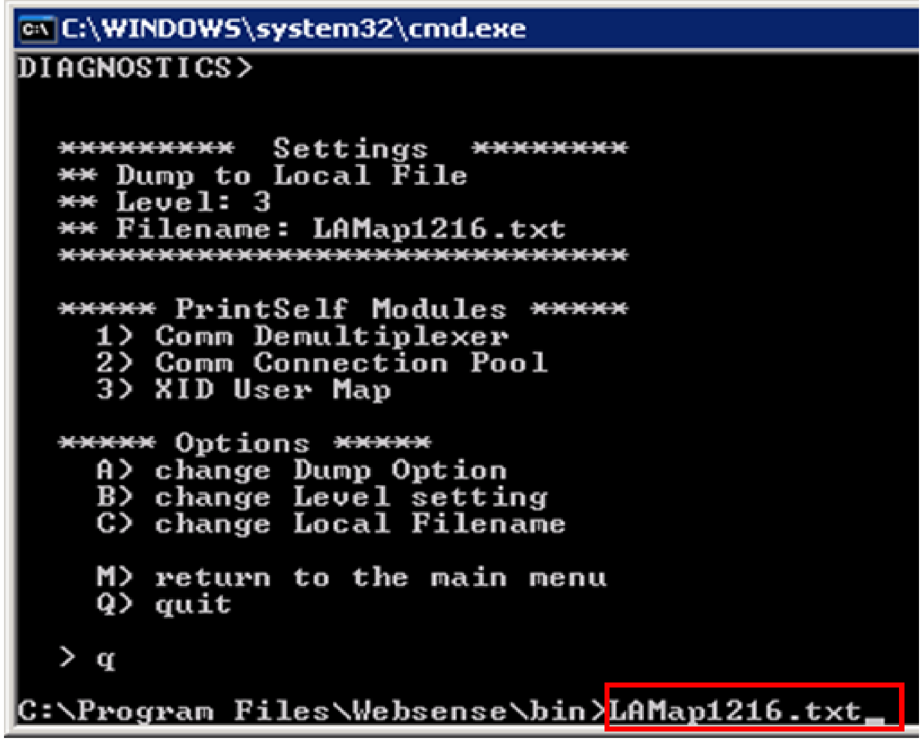

C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.4.169 30603

```
DIAGNOSTICS>


  *********  Settings  ********
  ** Dump to Local File
  ** Level: 3
  ** Filename: LAMap1216.txt
  *****************************

  ***** PrintSelf Modules *****
    1> Comm Demultiplexer
    2> Comm Connection Pool
    3> XID User Map

  ***** Options *****
    A> change Dump Option
    B> change Level setting
    C> change Local Filename

    M> return to the main menu
    Q> quit

  > 3_
```

ConsoleClient: Logon Agent


C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.4.169 30603

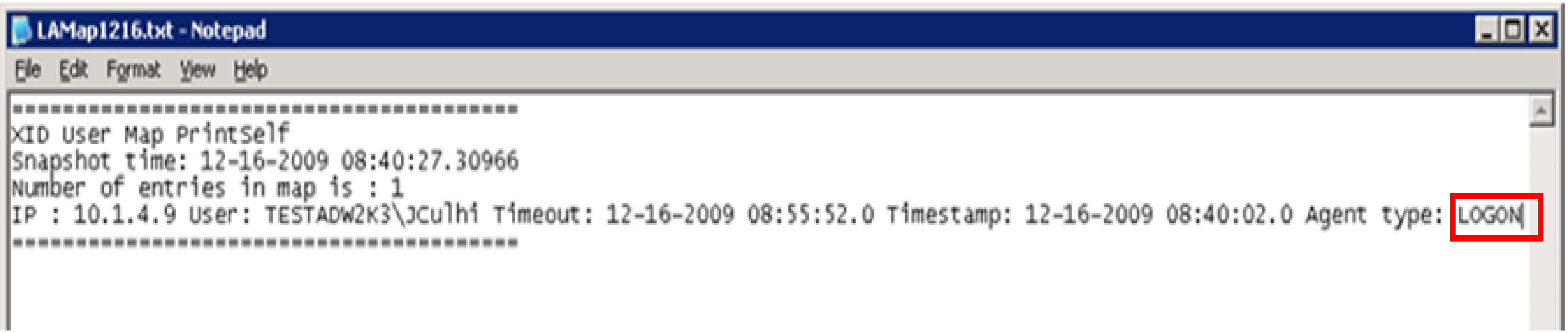
```
DIAGNOSTICS>


  *********  Settings  ********
  ** Dump to Local File
  ** Level: 3
  ** Filename: LAMap1216.txt
  *****************************

  ***** PrintSelf Modules *****
    1) Comm Demultiplexer
    2) Comm Connection Pool
    3) XID User Map

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > q_
```



```
DIAGNOSTICS>


  *********  Settings  ********
  ** Dump to Local File
  ** Level: 3
  ** Filename: LAMap1216.txt
  *****************************

  ***** PrintSelf Modules *****
    1) Comm Demultiplexer
    2) Comm Connection Pool
    3) XID User Map

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > q

C:\Program Files\Websense\bin>LAMap1216.txt_
```

ConsoleClient: Logon Agent

- The text file looks something like this:



```
========================================
XID User Map PrintSelf
Snapshot time: 12-16-2009 08:40:27.30966
Number of entries in map is : 1
IP : 10.1.4.9 User: TESTADW2K3\JCulhi Timeout: 12-16-2009 08:55:52.0 Timestamp: 12-16-2009 08:40:02.0 Agent type: LOGON
========================================
```

Transparent Identification Agent Options

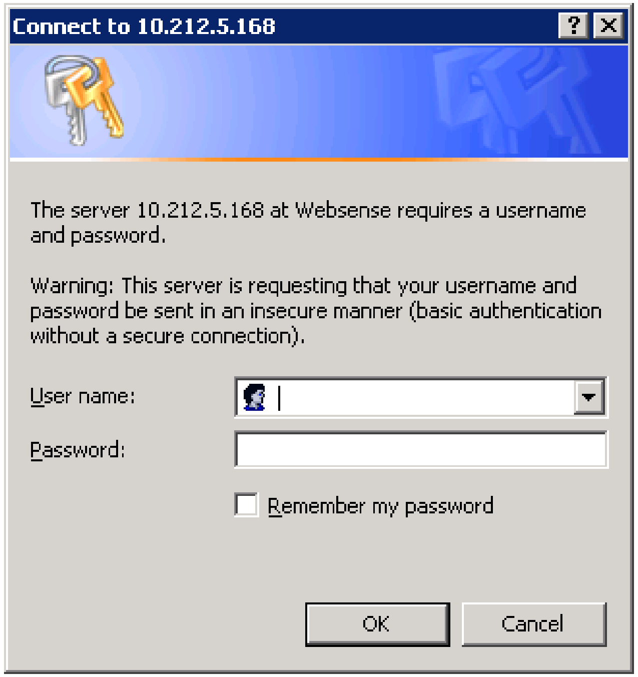
- When using ConsoleClient to view DC Agent information, the user map option is either #5 or #6 (depending on version).
- When using ConsoleClient to view Logon Agent, eDirectory Agent, and RADIUS Agent data, the user map option is #3.
- The following Knowledge Base article (3349), discusses additional options you can use with the ConsoleClient utility:
  - http://kb.websense.com/article.aspx?article=3349&p=12

ConsoleClient: Manual Authentication

- When you use manual authentication:
  - By default, the user map timeout for manually authenticated users is 10 minutes.
  - If a user provides credentials within a browser session, the browser re-caches the credentials for another 10 minute session.
  - Users who close the browser and open a new browser after the 10 minute session has passed are prompted to re-authenticate.
  - Users who open a new browser within the 10 minute manual authentication window are NOT prompted to re-authenticate.

ConsoleClient: Manual Authentication

- When unidentified users browse to a URL, they receive this prompt:



Connect to 10.212.5.168

The server 10.212.5.168 at Websense requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

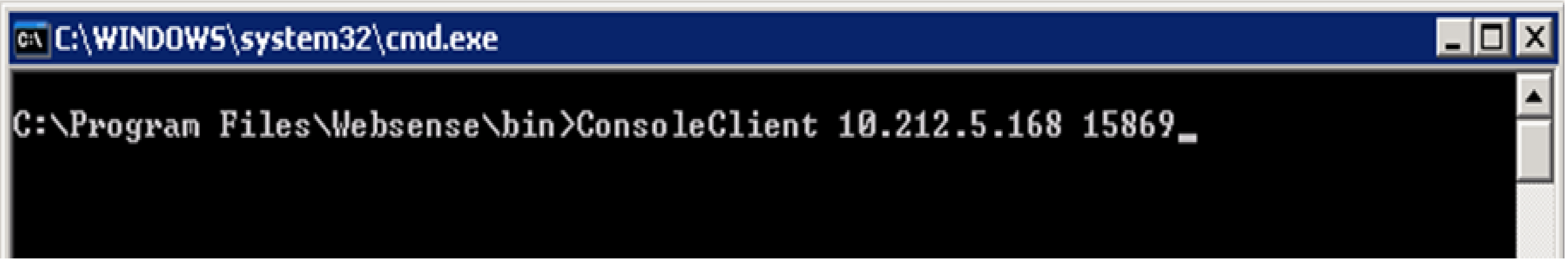
User name:

Password:

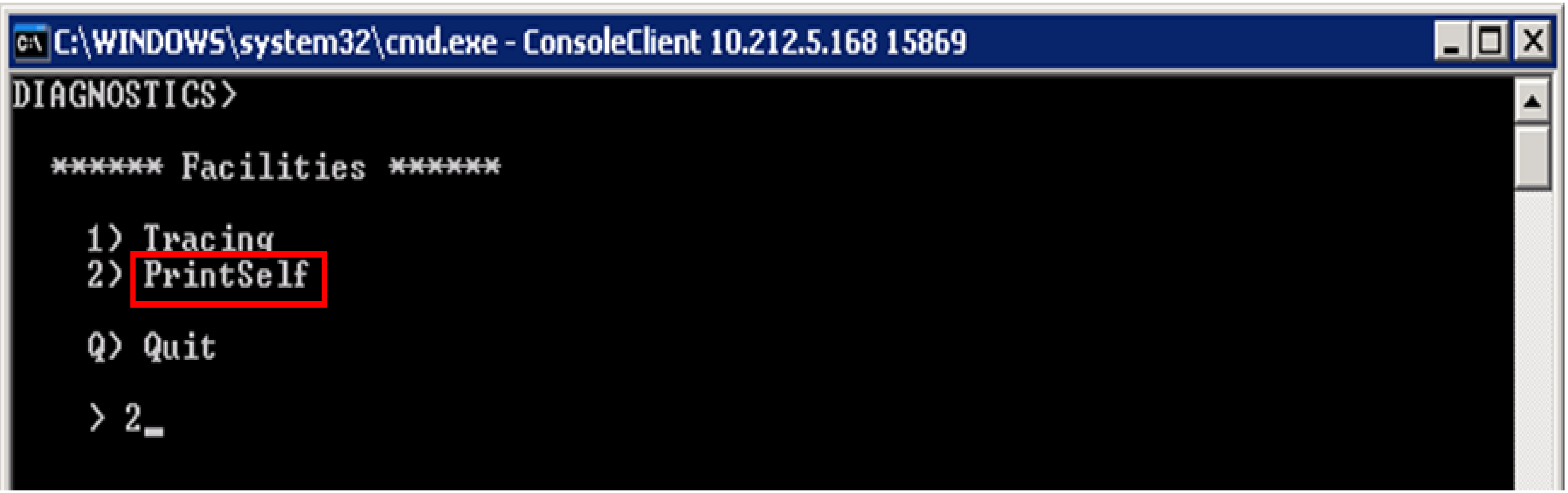
□ Remember my password

- Log on with network credentials, using one of the following formats:
  - User name and password
  - Domain\User name and password

ConsoleClient: Manual Authentication



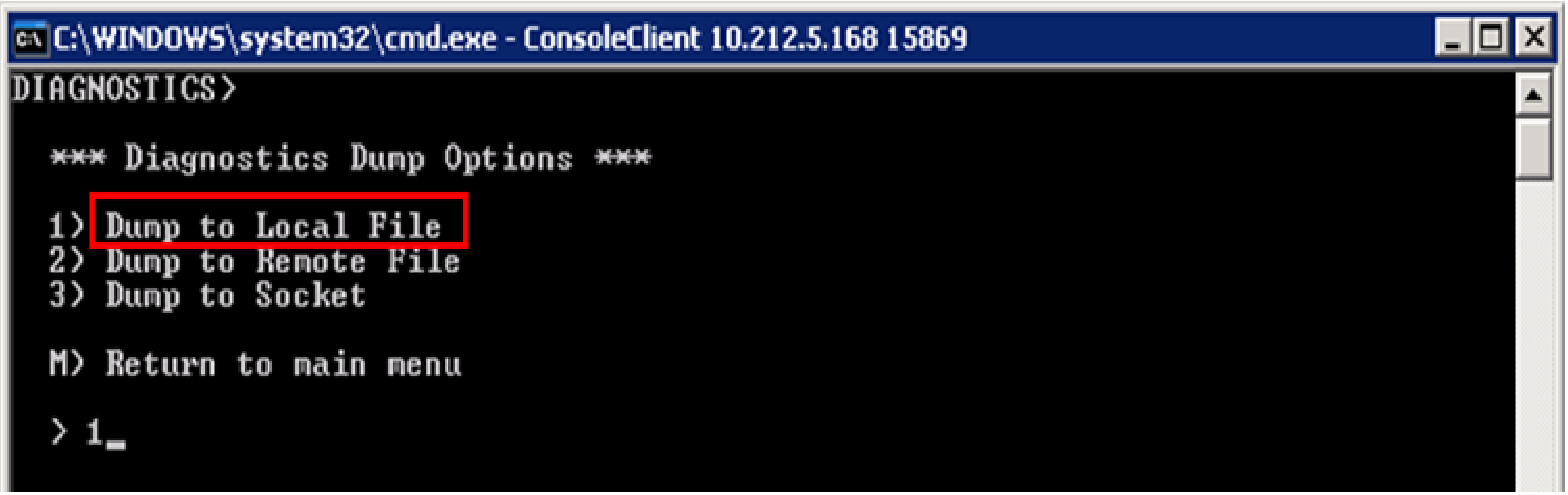
```
C:\Program Files\Websense\bin>ConsoleClient 10.212.5.168 15869_
```



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

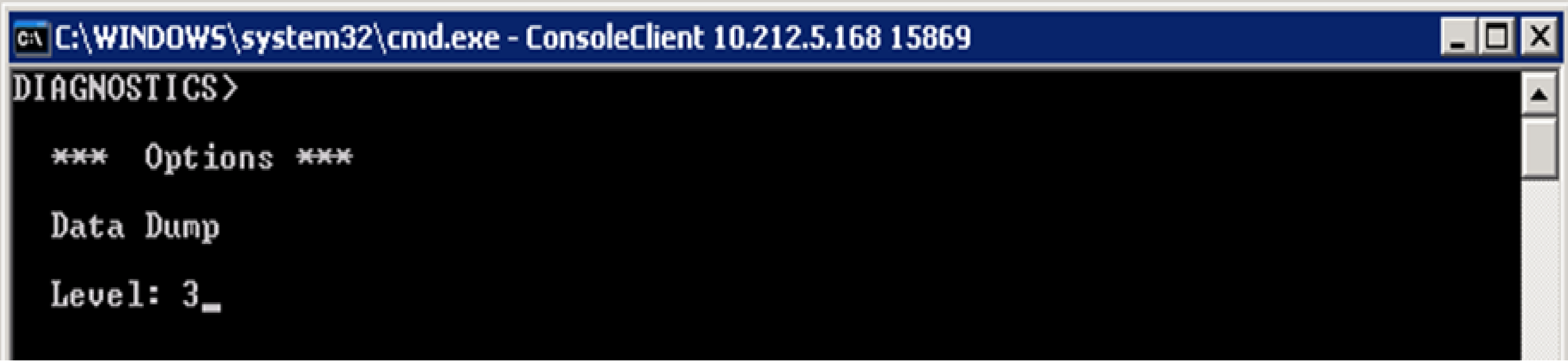
```
DIAGNOSTICS>

  ****** Facilities ******

    1) Tracing
    2) PrintSelf

    Q) Quit

    > 2_
```

ConsoleClient: Manual Authentication



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

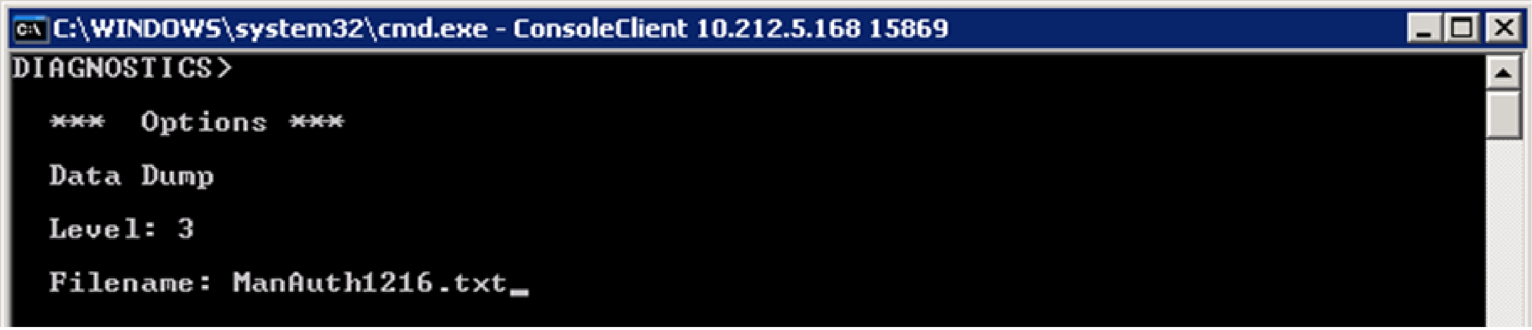
```
DIAGNOSTICS>

  *** Diagnostics Dump Options ***

  1) Dump to Local File
  2) Dump to Remote File
  3) Dump to Socket

  M) Return to main menu

  > 1_
```



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

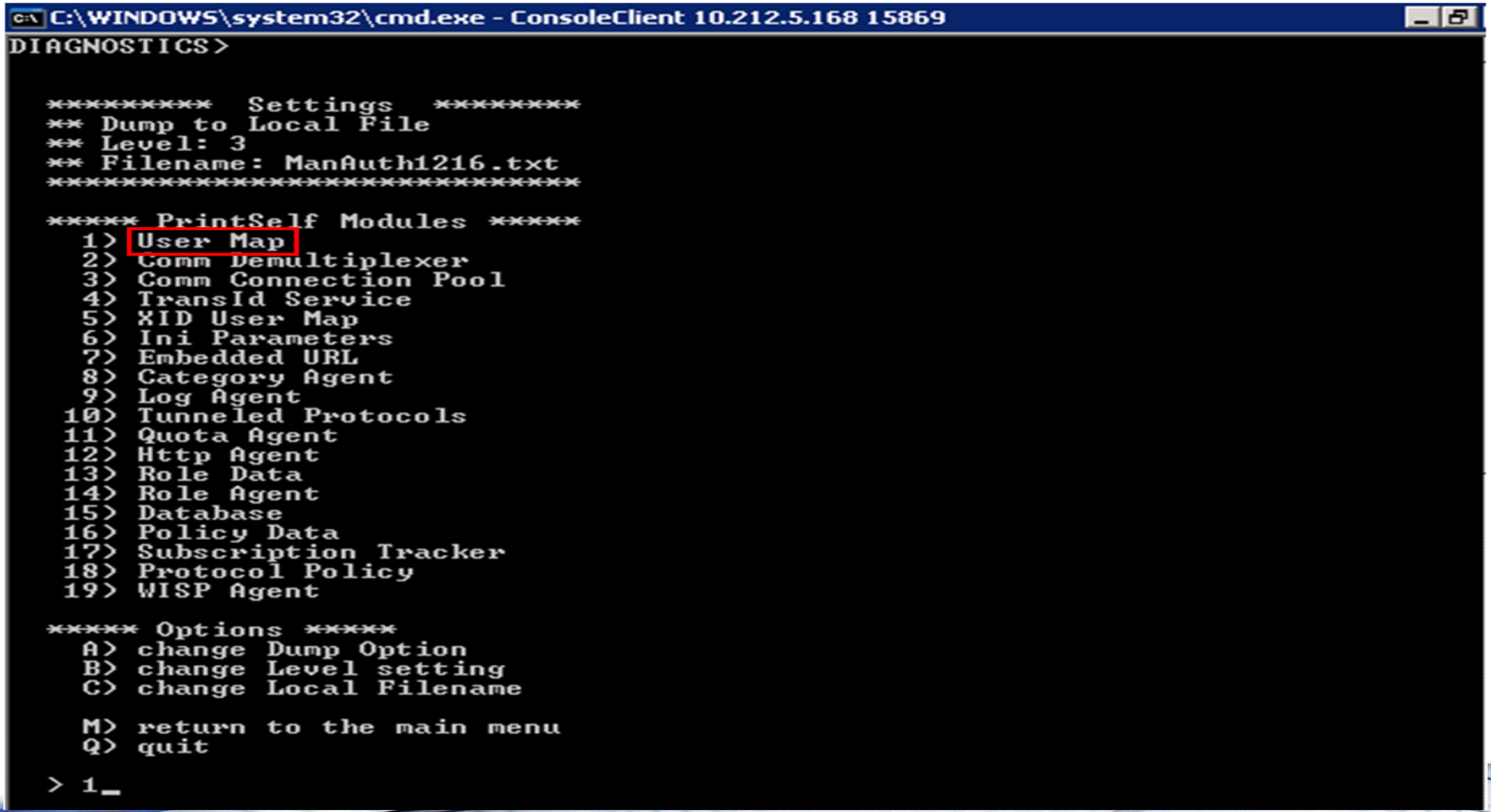
```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Level: 3_
```

ConsoleClient: Manual Authentication



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

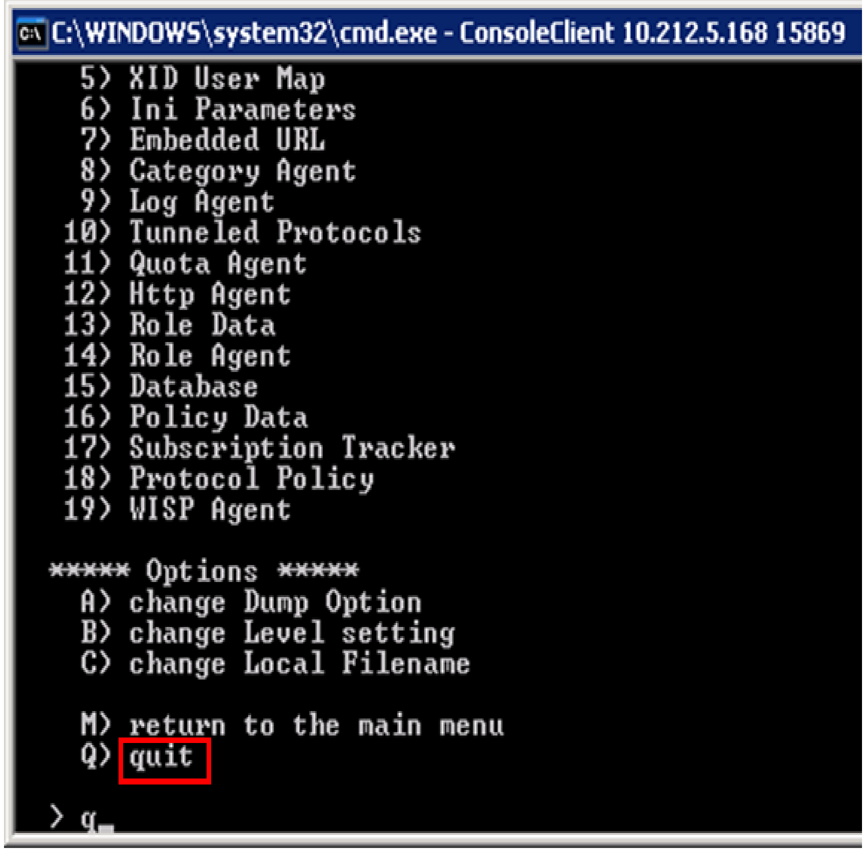
```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Level: 3

  Filename: ManAuth1216.txt_
```



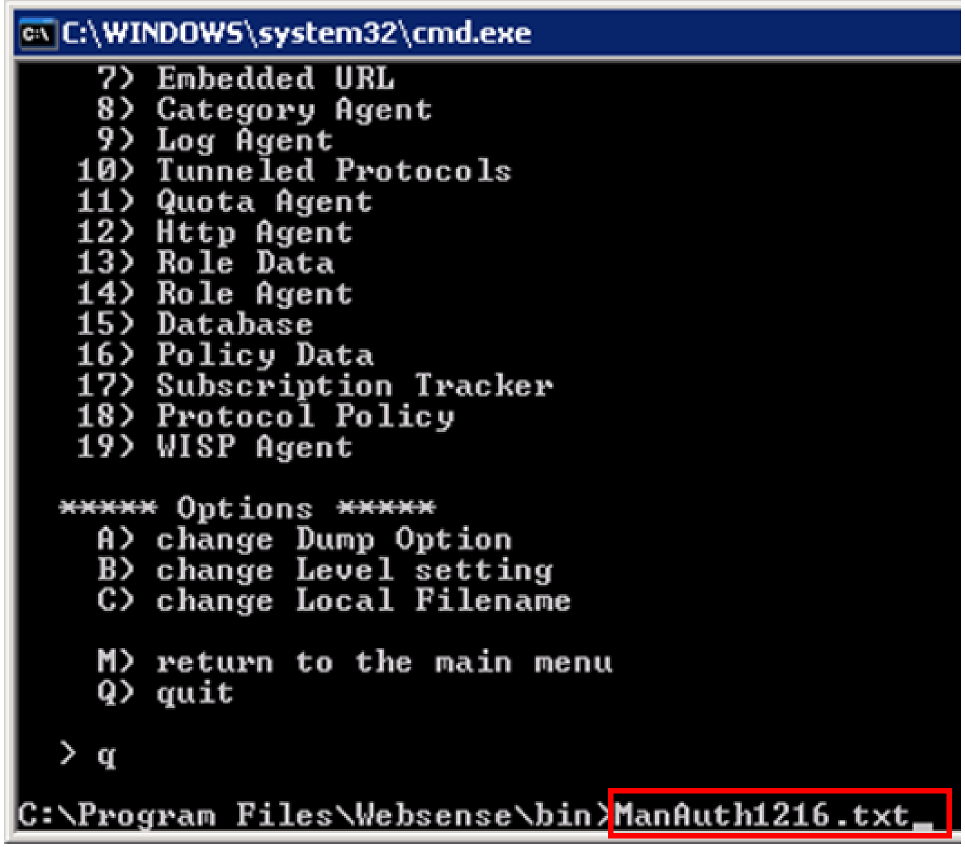
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

```
DIAGNOSTICS>

  *********  Settings  ********
  ** Dump to Local File
  ** Level: 3
  ** Filename: ManAuth1216.txt
  *****************************

  ***** PrintSelf Modules *****
    1) User Map
    2) Comm Demultiplexer
    3) Comm Connection Pool
    4) TransId Service
    5) XID User Map
    6) Ini Parameters
    7) Embedded URL
    8) Category Agent
    9) Log Agent
   10) Tunneled Protocols
   11) Quota Agent
   12) Http Agent
   13) Role Data
   14) Role Agent
   15) Database
   16) Policy Data
   17) Subscription Tracker
   18) Protocol Policy
   19) WISP Agent

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > 1_
```

ConsoleClient: Manual Authentication

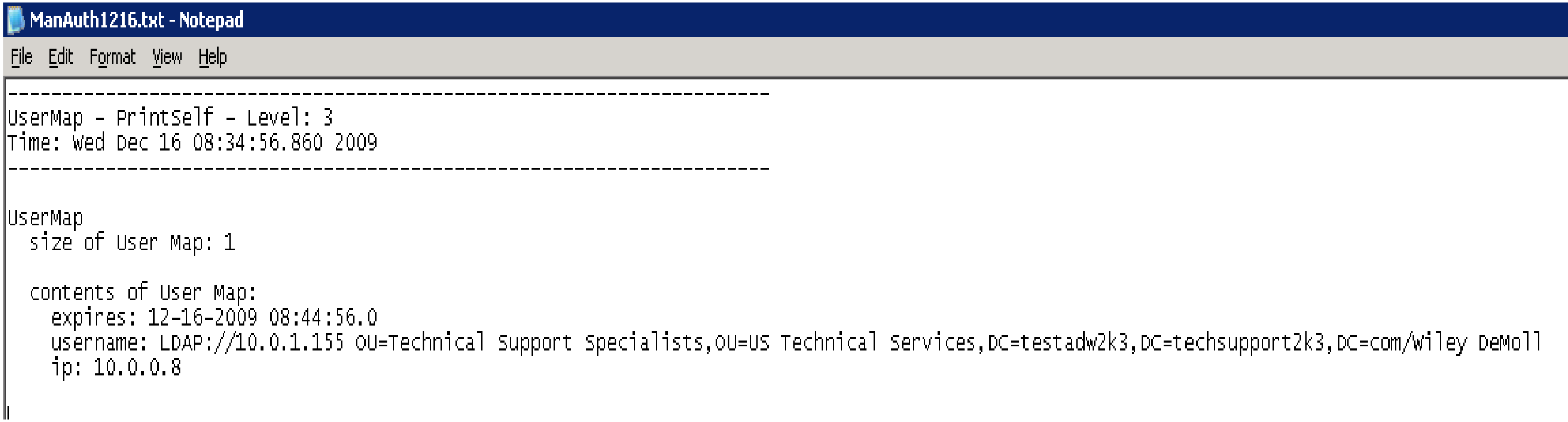


```
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869
    5) XID User Map
    6) Ini Parameters
    7) Embedded URL
    8) Category Agent
    9) Log Agent
   10) Tunneled Protocols
   11) Quota Agent
   12) Http Agent
   13) Role Data
   14) Role Agent
   15) Database
   16) Policy Data
   17) Subscription Tracker
   18) Protocol Policy
   19) WISP Agent

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > q_
```



```
C:\WINDOWS\system32\cmd.exe
    7) Embedded URL
    8) Category Agent
    9) Log Agent
   10) Tunneled Protocols
   11) Quota Agent
   12) Http Agent
   13) Role Data
   14) Role Agent
   15) Database
   16) Policy Data
   17) Subscription Tracker
   18) Protocol Policy
   19) WISP Agent

  ***** Options *****
    A) change Dump Option
    B) change Level setting
    C) change Local Filename

    M) return to the main menu
    Q) quit

  > q

C:\Program Files\Websense\bin>ManAuth1216.txt_
```

ConsoleClient: Manual Authentication



```
----------------------------------------------------------------------
UserMap - PrintSelf - Level: 3
Time: Wed Dec 16 08:34:56.860 2009
----------------------------------------------------------------------

UserMap
  size of User Map: 1

  contents of User Map:
    expires: 12-16-2009 08:44:56.0
    username: LDAP://10.0.1.155 OU=Technical Support Specialists,OU=US Technical Services,DC=testadw2k3,DC=techsupport2k3,DC=com/Wiley DeMoll
    ip: 10.0.0.8
```

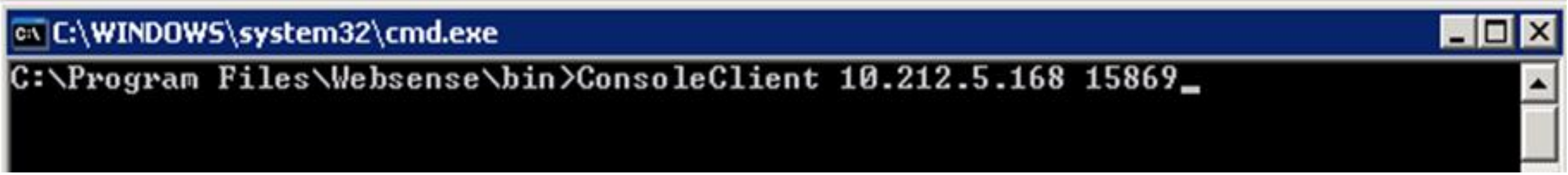
Filtering Service (WISP) Trace

- A Filtering Service (WISP) trace shows whether Filtering Service is responding to server status requests from Network Agent or an integration product.
  - Should the integration not receive a response from Filtering Service within its time limit, it will fail open or closed (permitting or blocking all requests), as configured.
  - Filtering Service normally responds to server status requests within 1 minute.

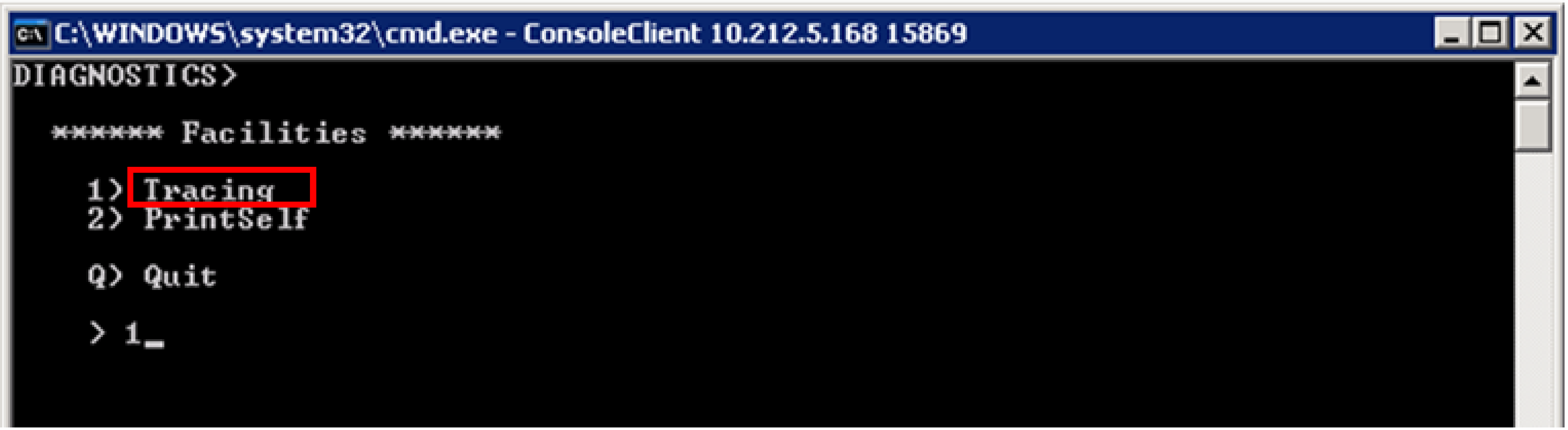
Filtering Service (WISP) Trace

- Symptoms of Filtering Service is not responding in a timely manner include:
  - Latency of Web pages loading
  - Web pages may load partial or no data
- Verify that Filtering Service responds correctly to URL requests

Running a WISP Trace



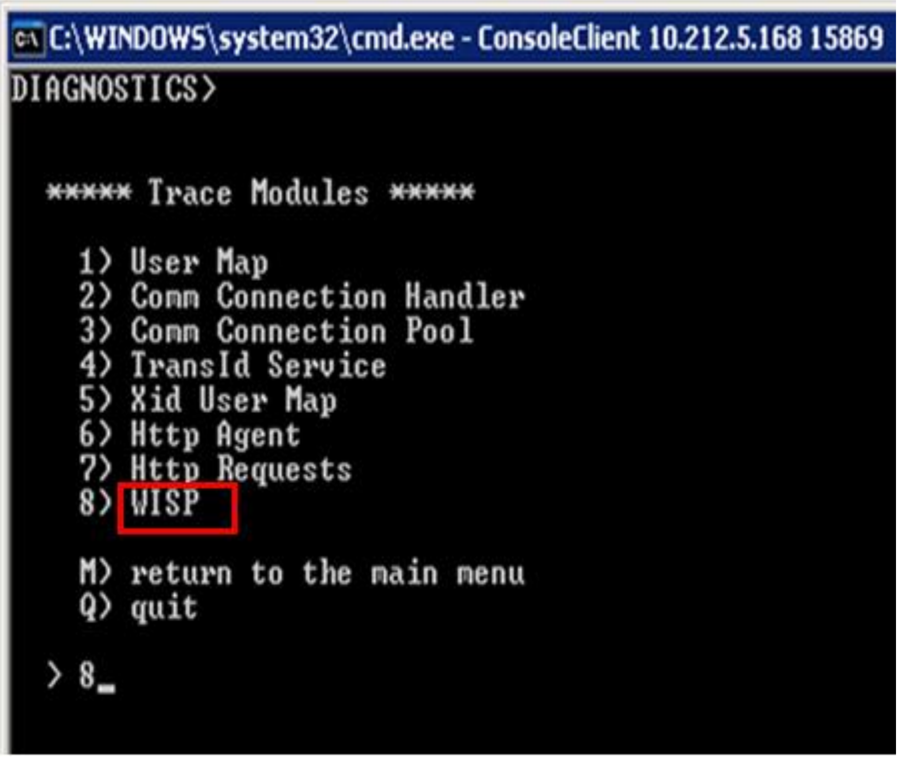
```
C:\Program Files\Websense\bin>ConsoleClient 10.212.5.168 15869_
```



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

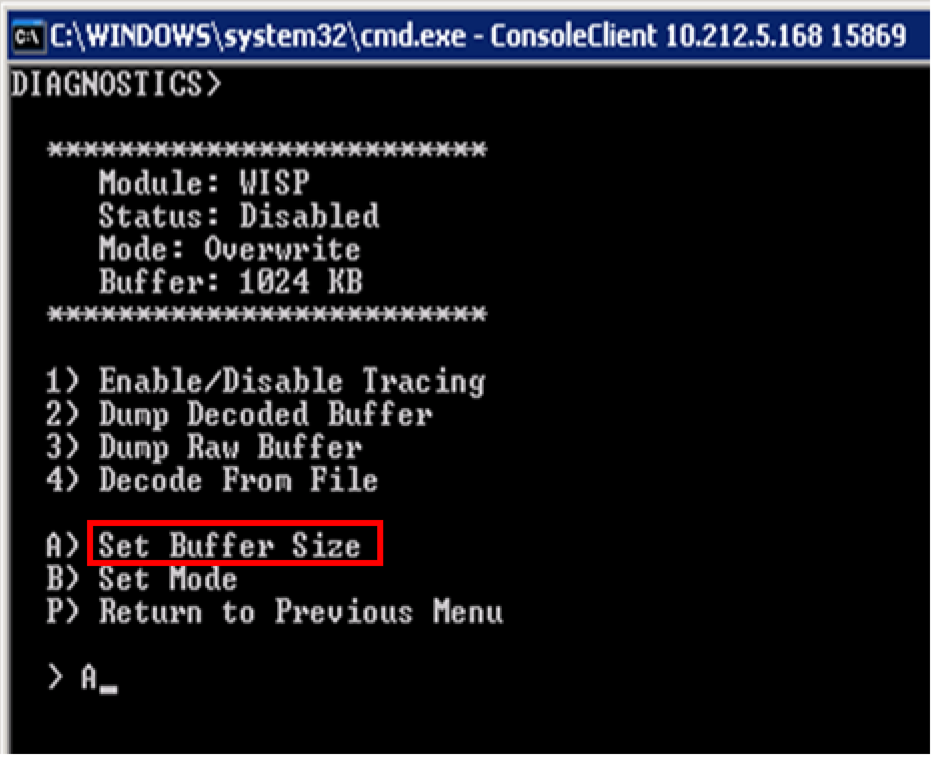
```
DIAGNOSTICS>

  ******* Facilities *******

    1) Tracing
    2) PrintSelf

    Q) Quit

    > 1_
```

Running a WISP Trace



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

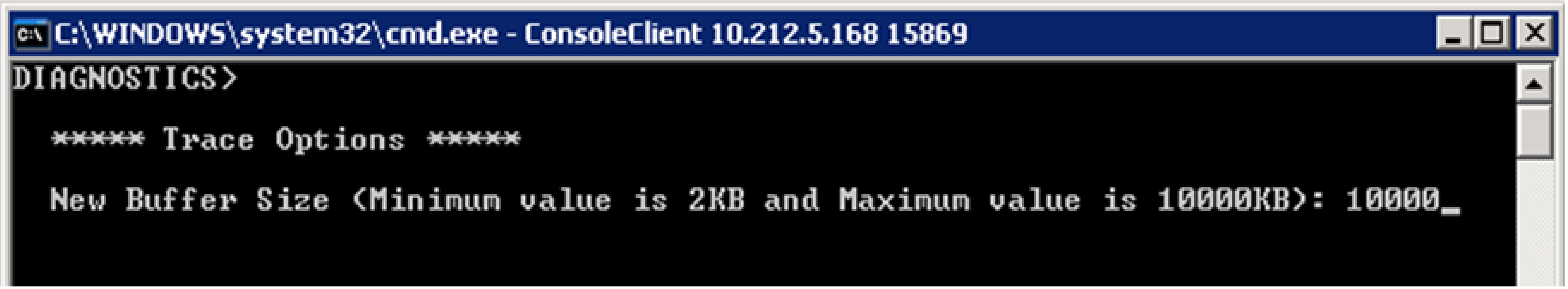
```
DIAGNOSTICS>


 ***** Trace Modules *****

   1) User Map
   2) Comm Connection Handler
   3) Comm Connection Pool
   4) TransId Service
   5) Xid User Map
   6) Http Agent
   7) Http Requests
   8) WISP

   M) return to the main menu
   Q) quit

 > 8_
```



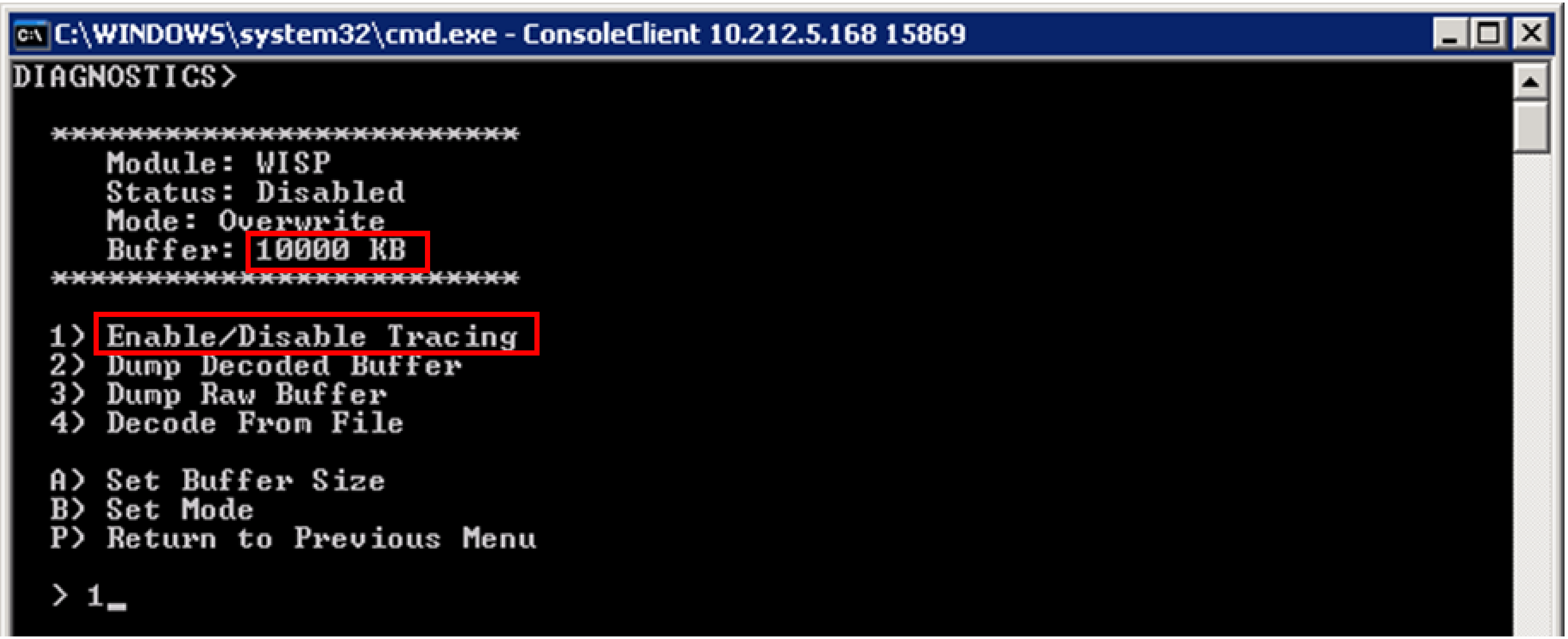
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

```
DIAGNOSTICS>

   **************************
      Module: WISP
      Status: Disabled
      Mode: Overwrite
      Buffer: 1024 KB
   **************************

   1) Enable/Disable Tracing
   2) Dump Decoded Buffer
   3) Dump Raw Buffer
   4) Decode From File

   A) Set Buffer Size
   B) Set Mode
   P) Return to Previous Menu

   > A_
```

Running a WISP Trace

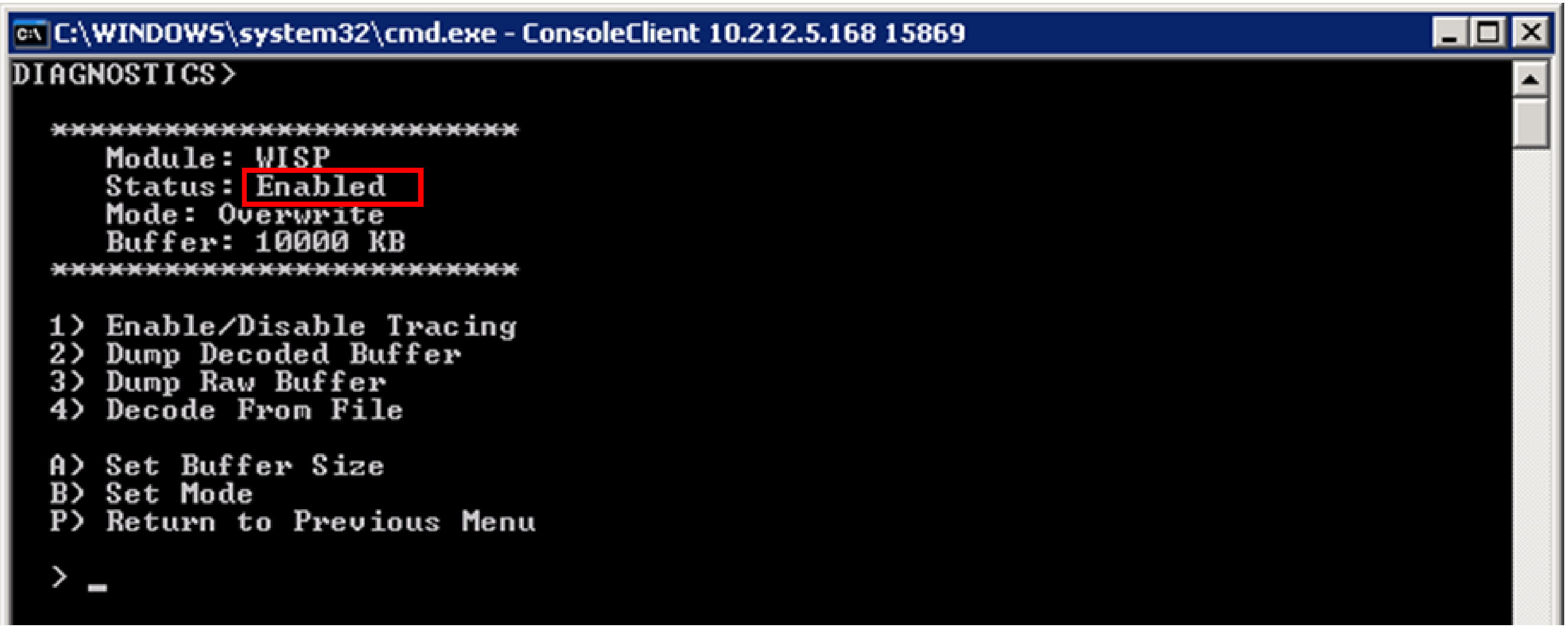


```
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869
DIAGNOSTICS>

  ***** Trace Options *****

  New Buffer Size (Minimum value is 2KB and Maximum value is 10000KB): 10000_
```



```
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869
DIAGNOSTICS>

  *************************
     Module: WISP
     Status: Disabled
     Mode: Overwrite
     Buffer: 10000 KB
  *************************

  1) Enable/Disable Tracing
  2) Dump Decoded Buffer
  3) Dump Raw Buffer
  4) Decode From File

  A) Set Buffer Size
  B) Set Mode
  P) Return to Previous Menu

  > 1_
```

Running a WISP Trace

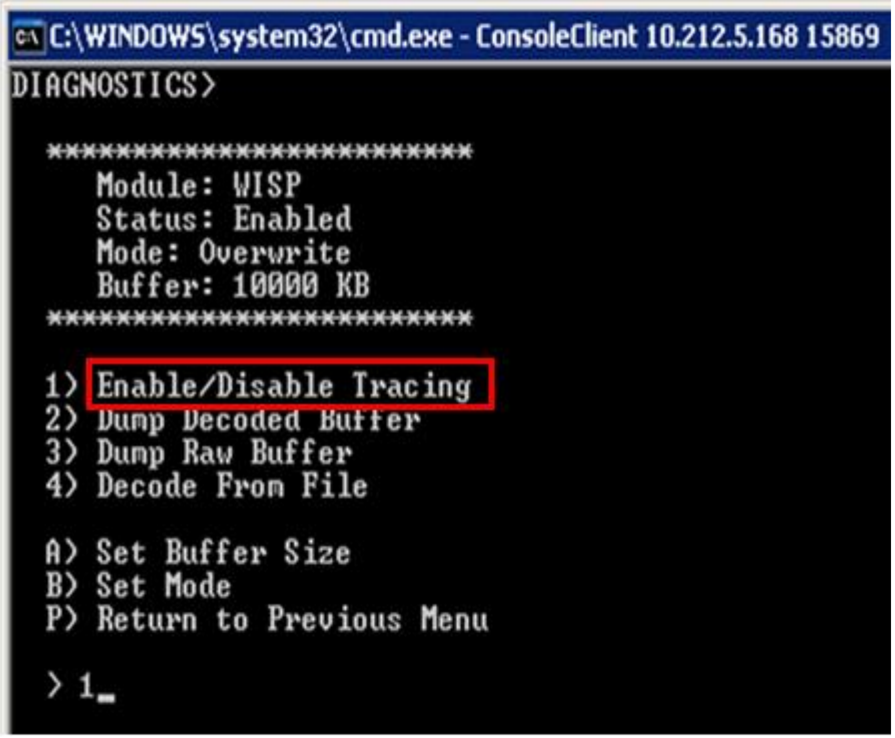


C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

```
DIAGNOSTICS>

  **************************
     Module: WISP
     Status: Enabled
     Mode: Overwrite
     Buffer: 10000 KB
  **************************

  1> Enable/Disable Tracing
  2> Dump Decoded Buffer
  3> Dump Raw Buffer
  4> Decode From File

  A> Set Buffer Size
  B> Set Mode
  P> Return to Previous Menu

  > _
```

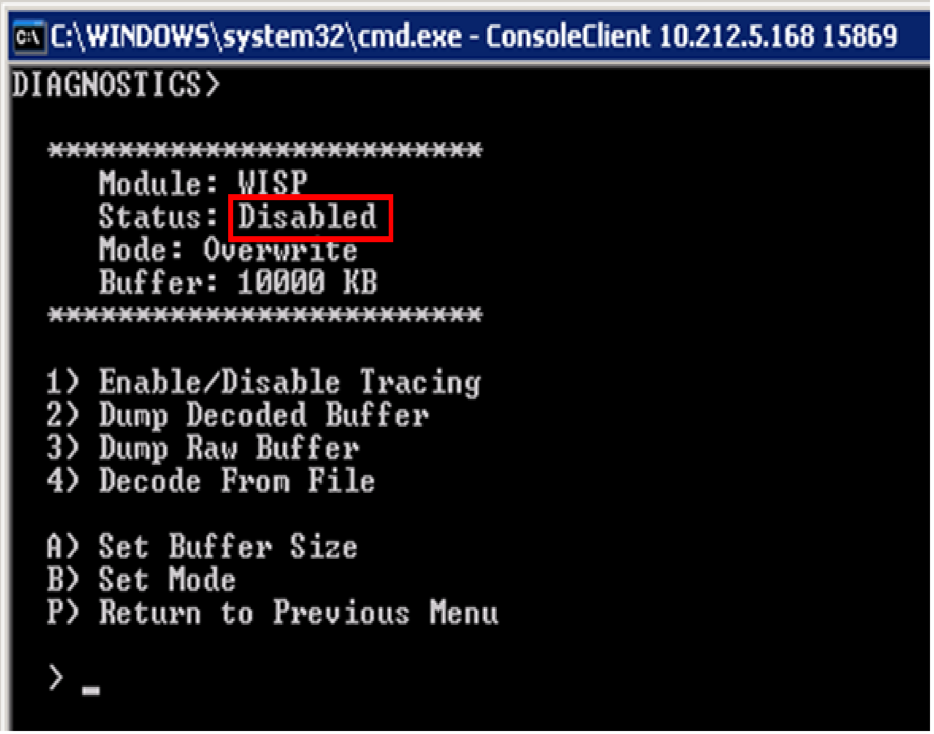
- Open a Web browser (Internet Explorer or Firefox) and browse to a URL:
  - http://www.mexico.com
  - http://jellybelly.com

Running a WISP (Filtering Service) Trace



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

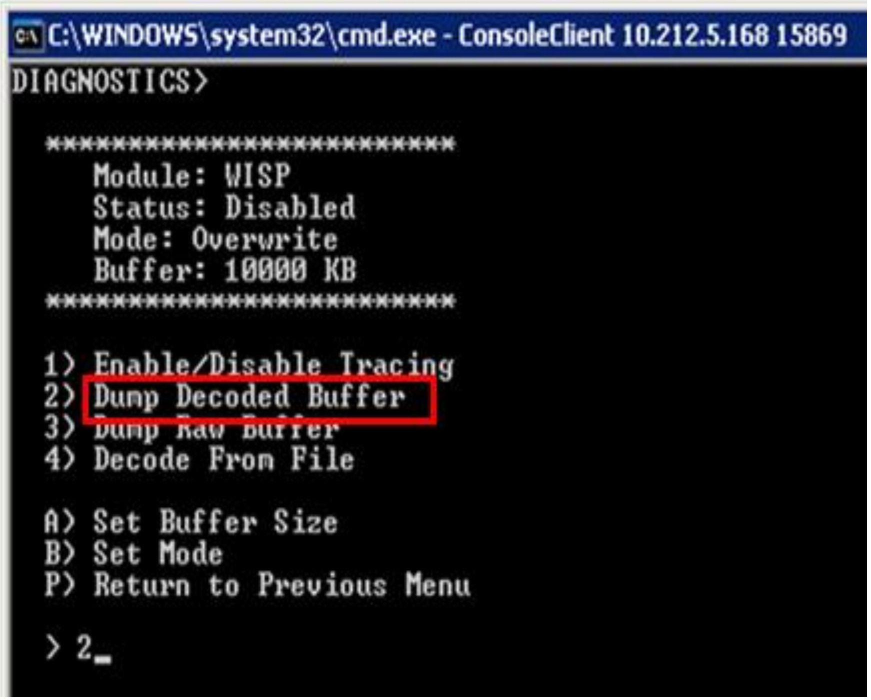
```
DIAGNOSTICS>

  *************************
     Module: WISP
     Status: Enabled
     Mode: Overwrite
     Buffer: 10000 KB
  *************************

  1) Enable/Disable Tracing
  2) Dump Decoded Buffer
  3) Dump Raw Buffer
  4) Decode From File

  A) Set Buffer Size
  B) Set Mode
  P) Return to Previous Menu

  > 1_
```



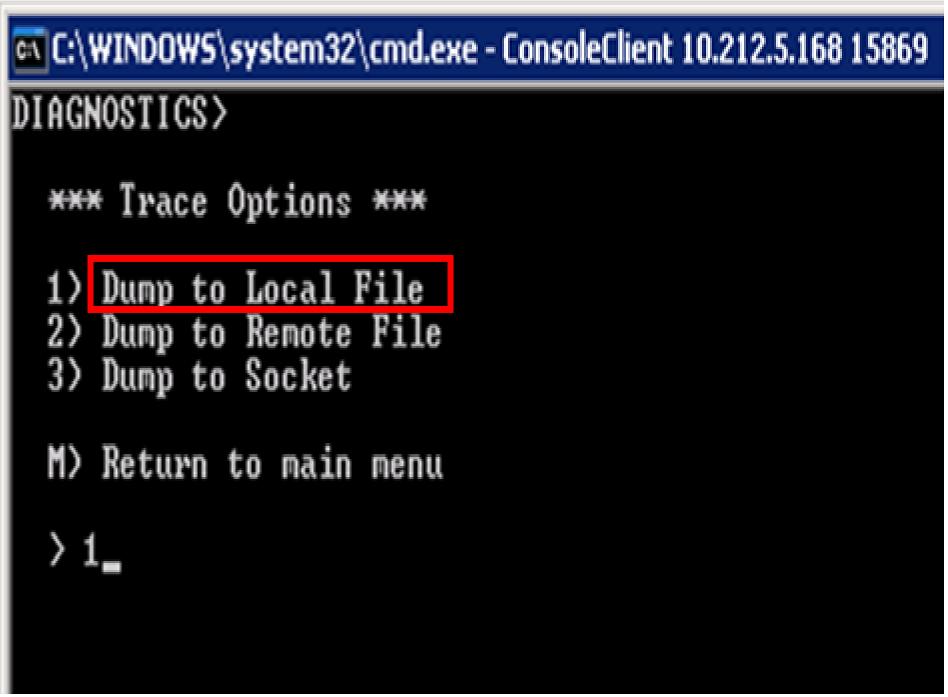
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

```
DIAGNOSTICS>

  *************************
     Module: WISP
     Status: Disabled
     Mode: Overwrite
     Buffer: 10000 KB
  *************************

  1) Enable/Disable Tracing
  2) Dump Decoded Buffer
  3) Dump Raw Buffer
  4) Decode From File

  A) Set Buffer Size
  B) Set Mode
  P) Return to Previous Menu

  > _
```

Running a WISP (Filtering Service) Trace

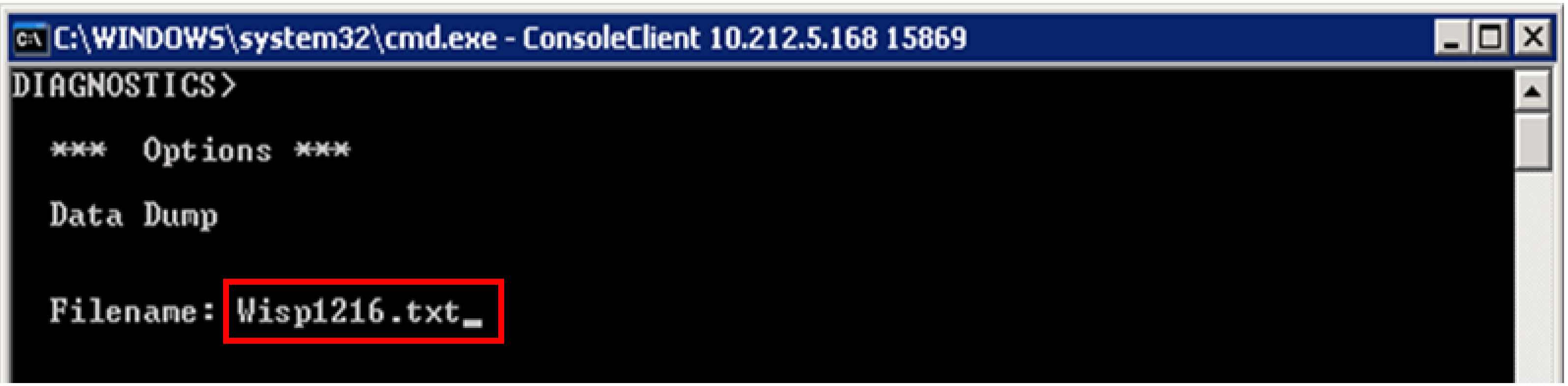


```
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869
DIAGNOSTICS>

  **************************
     Module: WISP
     Status: Disabled
     Mode: Overwrite
     Buffer: 10000 KB
  **************************

  1) Enable/Disable Tracing
  2) Dump Decoded Buffer
  3) Dump Raw Buffer
  4) Decode From File

  A) Set Buffer Size
  B) Set Mode
  P) Return to Previous Menu

  > 2_
```

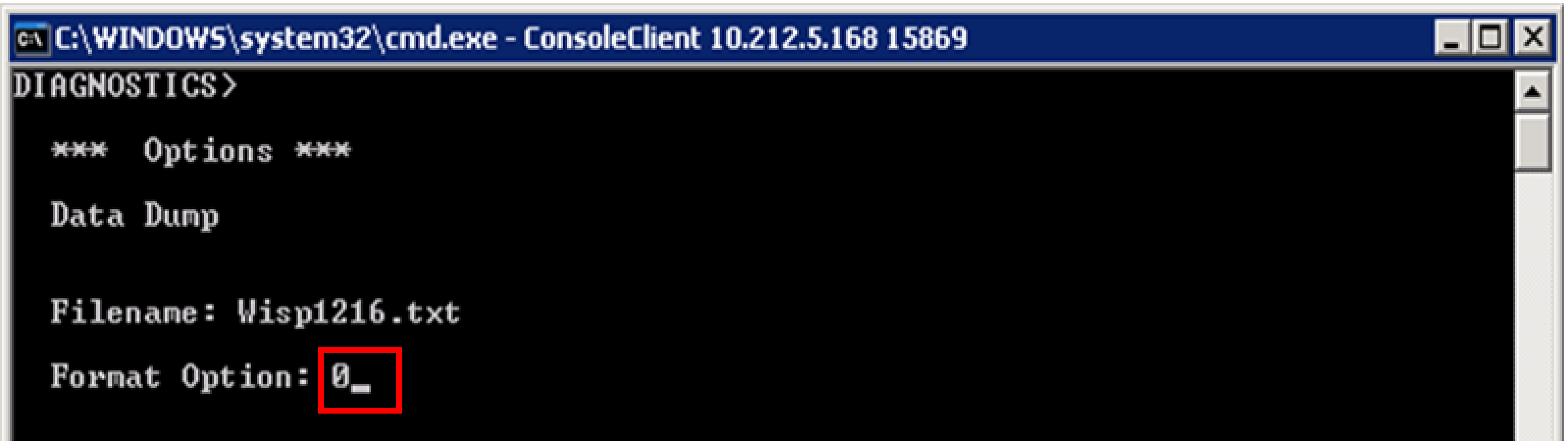


```
C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869
DIAGNOSTICS>

  *** Trace Options ***

  1) Dump to Local File
  2) Dump to Remote File
  3) Dump to Socket

  M) Return to main menu

  > 1_
```

Running a WISP (Filtering Service) Trace

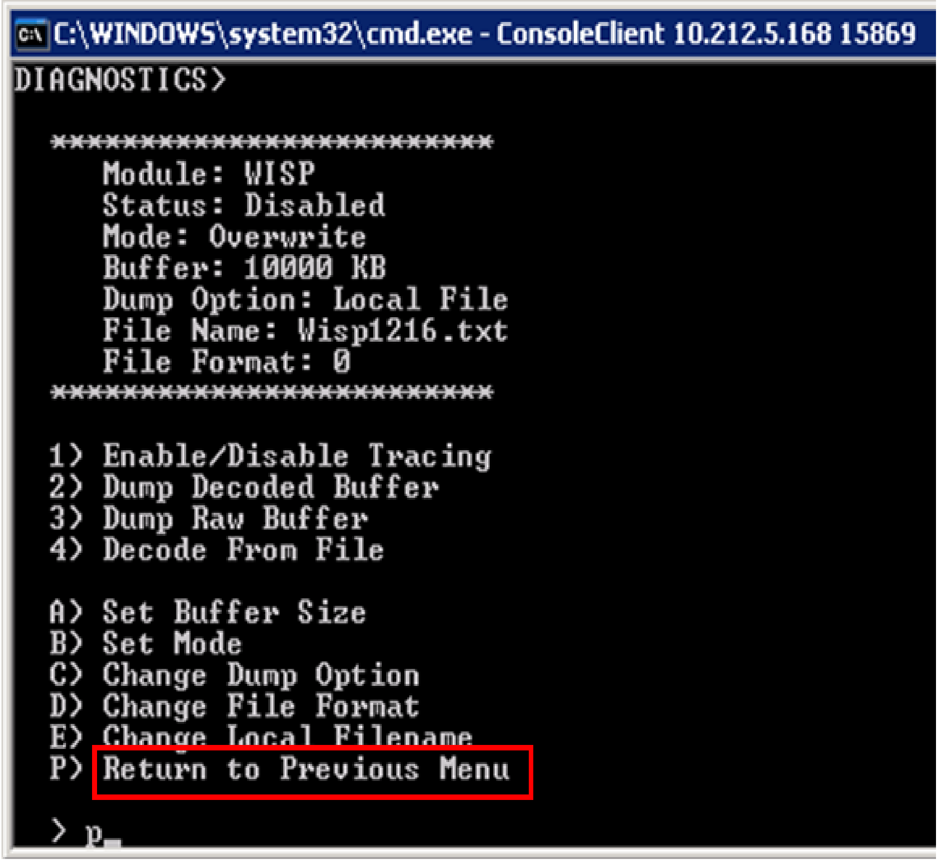

C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Filename: Wisp1216.txt_
```


C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

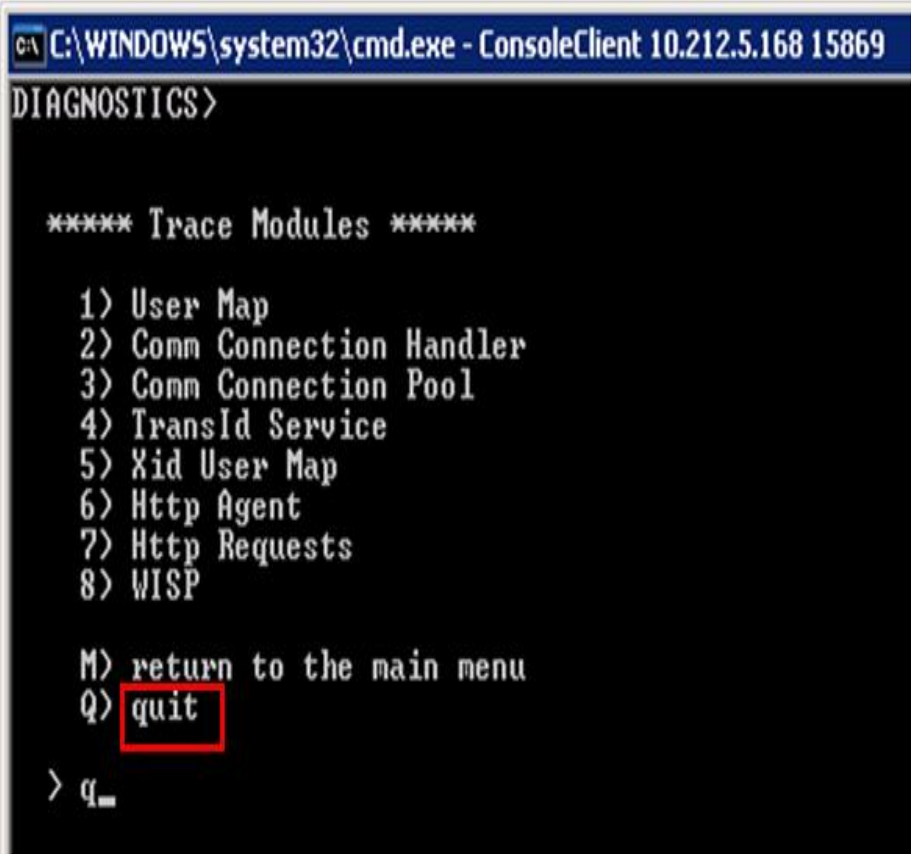
```
DIAGNOSTICS>

  ***  Options ***

  Data Dump

  Filename: Wisp1216.txt

  Format Option: 0_
```

Running a WISP (Filtering Service) Trace



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

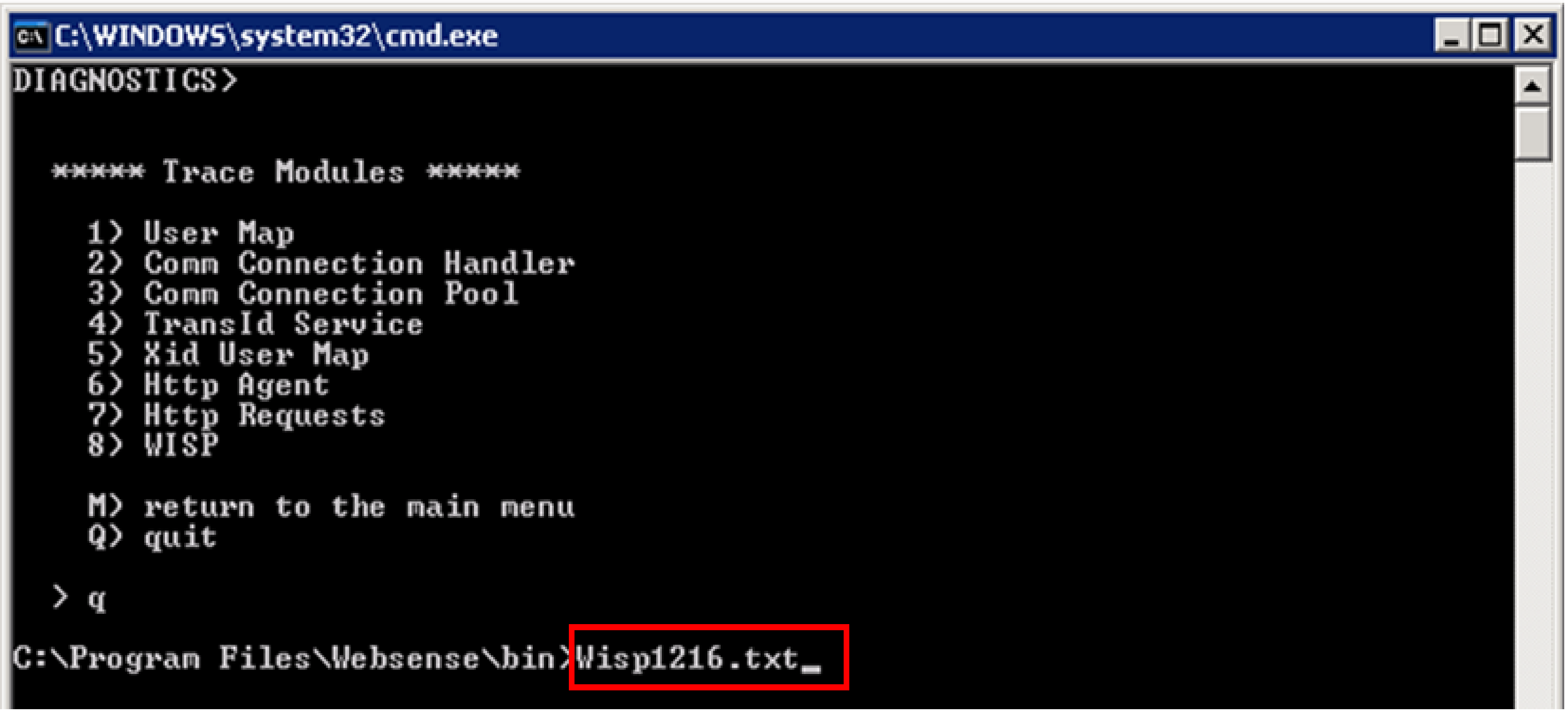
```
DIAGNOSTICS>

  **************************
     Module: WISP
     Status: Disabled
     Mode: Overwrite
     Buffer: 10000 KB
     Dump Option: Local File
     File Name: Wisp1216.txt
     File Format: 0
  **************************

  1) Enable/Disable Tracing
  2) Dump Decoded Buffer
  3) Dump Raw Buffer
  4) Decode From File

  A) Set Buffer Size
  B) Set Mode
  C) Change Dump Option
  D) Change File Format
  E) Change Local Filename
  P) Return to Previous Menu

  > p_
```



C:\WINDOWS\system32\cmd.exe - ConsoleClient 10.212.5.168 15869

```
DIAGNOSTICS>


  ***** Trace Modules *****

    1) User Map
    2) Comm Connection Handler
    3) Comm Connection Pool
    4) TransId Service
    5) Xid User Map
    6) Http Agent
    7) Http Requests
    8) WISP

    M) return to the main menu
    Q) quit

  > q_
```

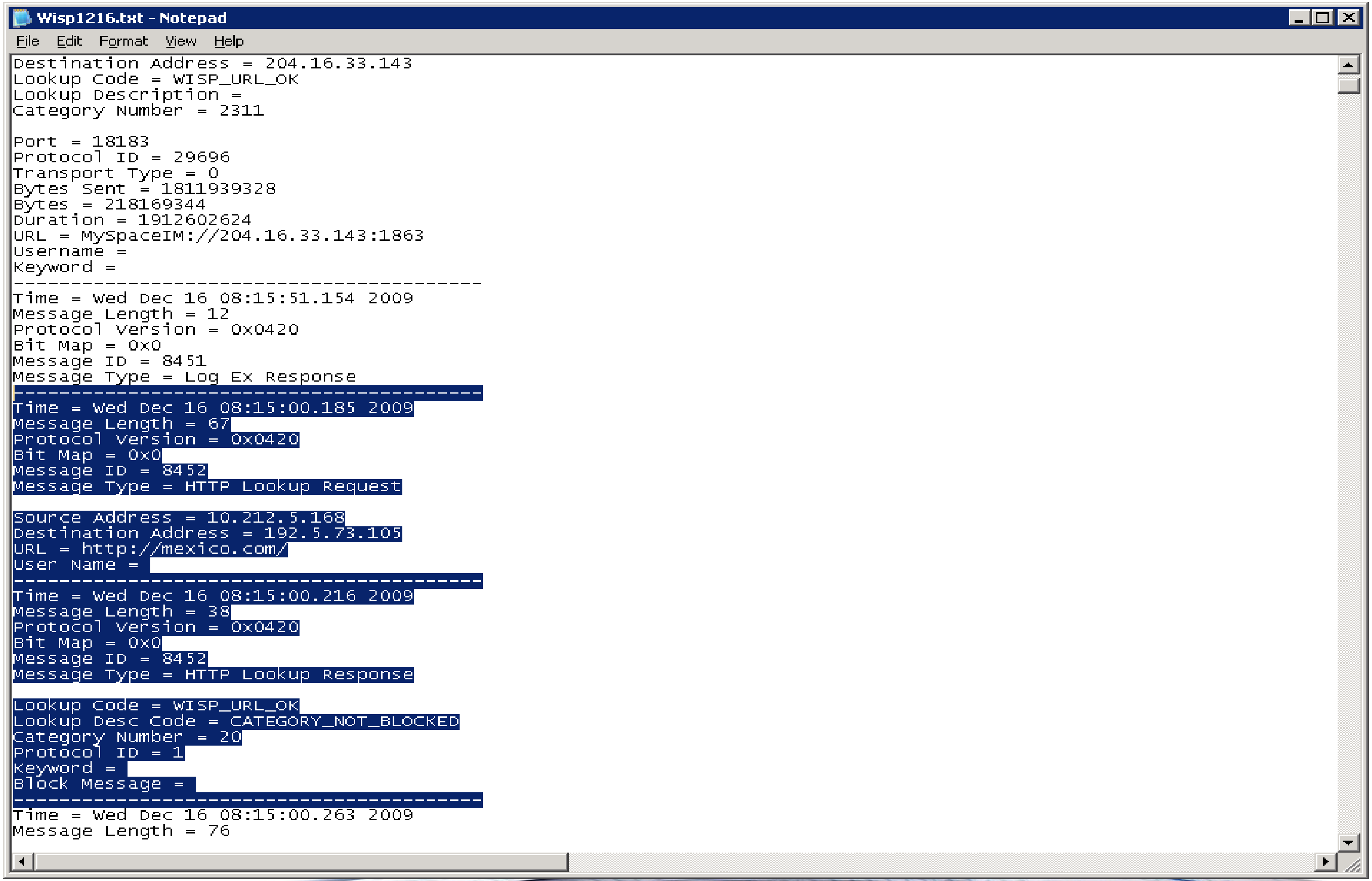
Running a WISP (Filtering Service) Trace



```
DIAGNOSTICS>


  ***** Trace Modules *****

    1) User Map
    2) Comm Connection Handler
    3) Comm Connection Pool
    4) TransId Service
    5) Xid User Map
    6) Http Agent
    7) Http Requests
    8) WISP

    M) return to the main menu
    Q) quit

  > q

C:\Program Files\Websense\bin>Wisp1216.txt_
```

- Open the file with a text editor, such as Notepad, to see the results.

Running a WISP (Filtering Service) Trace



```
Destination Address = 204.16.33.143
Lookup Code = WISP_URL_OK
Lookup Description =
Category Number = 2311

Port = 18183
Protocol ID = 29696
Transport Type = 0
Bytes Sent = 1811939328
Bytes = 218169344
Duration = 1912602624
URL = MySpaceIM://204.16.33.143:1863
Username =
Keyword =
-----------------------------------------
Time = Wed Dec 16 08:15:51.154 2009
Message Length = 12
Protocol Version = 0x0420
Bit Map = 0x0
Message ID = 8451
Message Type = Log Ex Response
-----------------------------------------
Time = Wed Dec 16 08:15:00.185 2009
Message Length = 67
Protocol Version = 0x0420
Bit Map = 0x0
Message ID = 8452
Message Type = HTTP Lookup Request

Source Address = 10.212.5.168
Destination Address = 192.5.73.105
URL = http://mexico.com/
User Name =
-----------------------------------------
Time = Wed Dec 16 08:15:00.216 2009
Message Length = 38
Protocol Version = 0x0420
Bit Map = 0x0
Message ID = 8452
Message Type = HTTP Lookup Response

Lookup Code = WISP_URL_OK
Lookup Desc Code = CATEGORY_NOT_BLOCKED
Category Number = 20
Protocol ID = 1
Keyword =
Block Message =
-----------------------------------------
Time = Wed Dec 16 08:15:00.263 2009
Message Length = 76
```

User Service Troubleshooting (DSTrace)

- Directory service tracing (DSTrace) is a way to identify user information collected by Websense software components.
  - Used to identify why user and group filtering policies are not applied
  - Shows whether User Service can collect user information from domain controllers
- By default, User Service updates user and group information every 3 hours (not constantly).

User Service Troubleshooting (DSTrace)

- To configure directory service tracing:

1. Navigate to the Websense bin directory (C:\Program Files\Websense\bin or /opt/Websense/bin/, by default.
2. Open the websense.ini file in a text editor.
3. Append the following parameters to the end of the file:

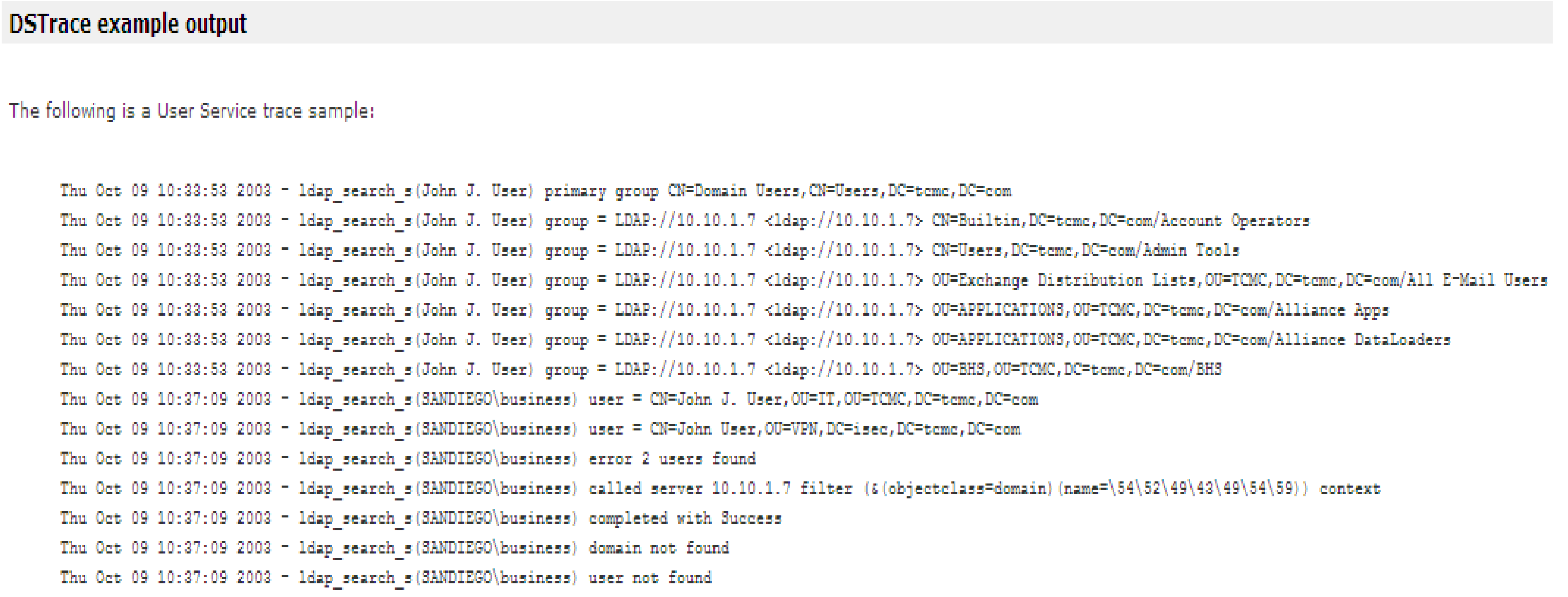
```
[DirectoryService]
BindLog=true
GroupLog=true
CacheLog=true
```

4. Save and close the file.
5. Restart Websense User Service.

User Service Troubleshooting (DSTrace)

- With the trace enabled, any time User Service queries the directory service user or group information, the request is logged.
  - The log file is called dstrace.txt, and located in the Websense bin directory.
- To create data to analyze:
  - Have a known user browse to a specific Web site.
  - Add a new directory (user or group) client in Websense Manager.
  - Use the Save All button to save changes in Websense Manager.

User Service Troubleshooting (DSTrace)



DSTrace example output

The following is a User Service trace sample:

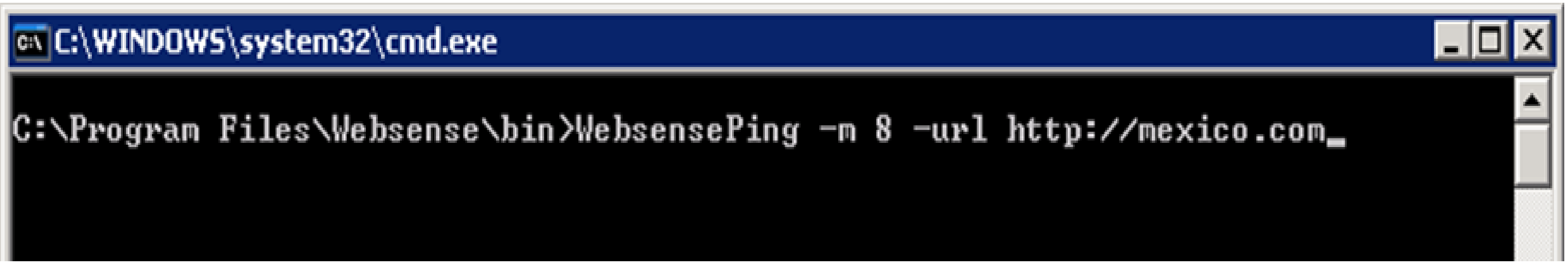
```
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) primary group CN=Domain Users,CN=Users,DC=tcmc,DC=com
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) group = LDAP://10.10.1.7 <ldap://10.10.1.7> CN=Builtin,DC=tcmc,DC=com/Account Operators
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) group = LDAP://10.10.1.7 <ldap://10.10.1.7> CN=Users,DC=tcmc,DC=com/Admin Tools
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) group = LDAP://10.10.1.7 <ldap://10.10.1.7> OU=Exchange Distribution Lists,OU=TCMC,DC=tcmc,DC=com/All E-Mail Users
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) group = LDAP://10.10.1.7 <ldap://10.10.1.7> OU=APPLICATIONS,OU=TCMC,DC=tcmc,DC=com/Alliance Apps
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) group = LDAP://10.10.1.7 <ldap://10.10.1.7> OU=APPLICATIONS,OU=TCMC,DC=tcmc,DC=com/Alliance DataLoaders
Thu Oct 09 10:33:53 2003 - ldap_search_s(John J. User) group = LDAP://10.10.1.7 <ldap://10.10.1.7> OU=BHS,OU=TCMC,DC=tcmc,DC=com/BHS
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) user = CN=John J. User,OU=IT,OU=TCMC,DC=tcmc,DC=com
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) user = CN=John User,OU=VPN,DC=isec,DC=tcmc,DC=com
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) error 2 users found
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) called server 10.10.1.7 filter (&(objectclass=domain)(name=\54\52\49\43\49\54\59)) context
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) completed with Success
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) domain not found
Thu Oct 09 10:37:09 2003 - ldap_search_s(SANDIEGO\business) user not found
```

- You cannot select different LDAP paths to a user object when more than one object for that user exists in Active Directory.

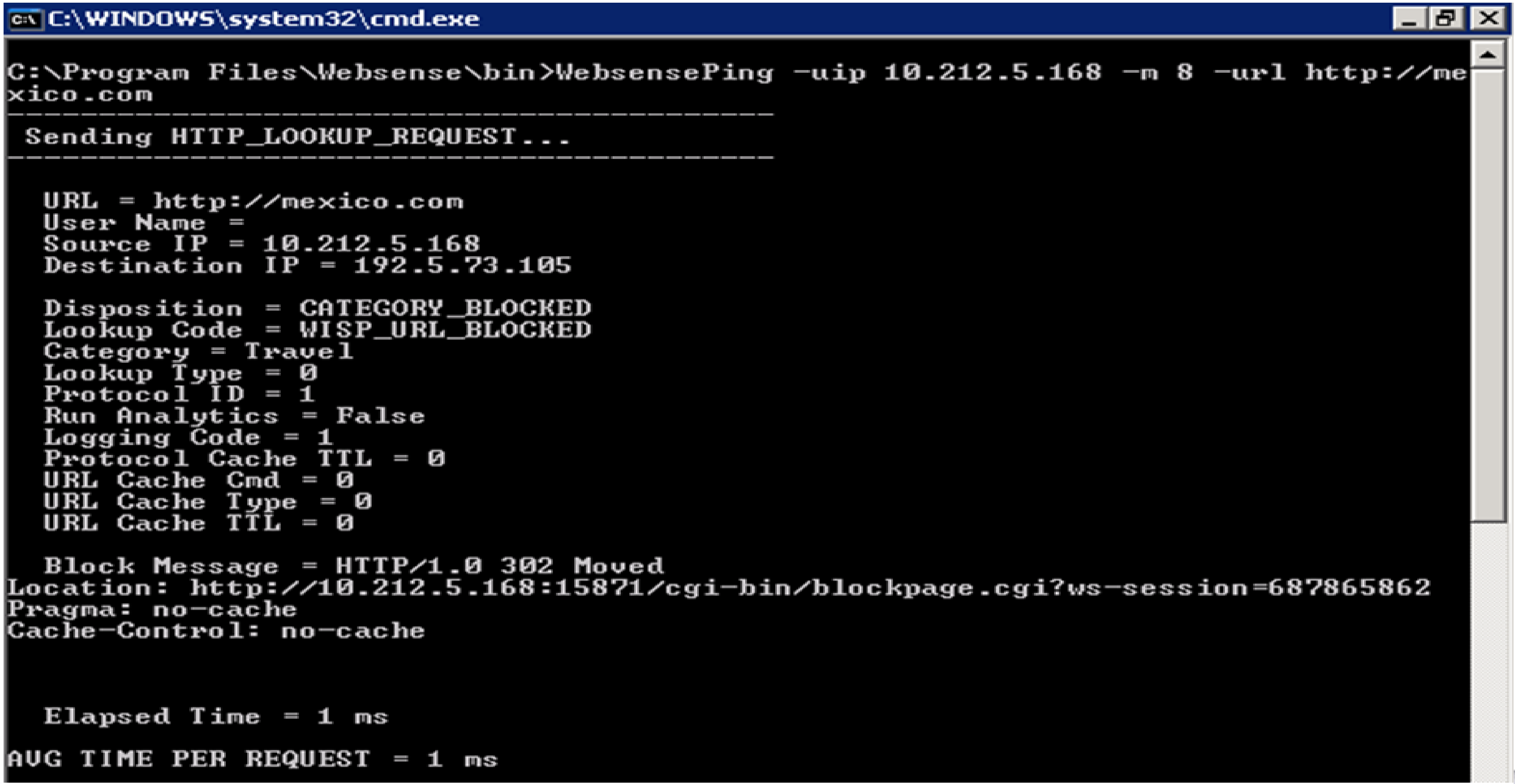
WebsensePing

- WebsensePing allows you to determine which category a certain URL belongs to.
  - Since a WebsensePing does NOT rely on data passed from other network applications or services, it can test internal Websense processes
- For a list of WebsensePing parameters:
  - Windows:
    Navigate to the Websense bin directory and enter WebsensePing.exe ?
  - Linux:
    Navigate to the /opt/Websense/ directory and enter: ./WebsenseTools -p ?

WebsensePing



```
C:\Program Files\Websense\bin>WebsensePing -m 8 -url http://mexico.com_
```

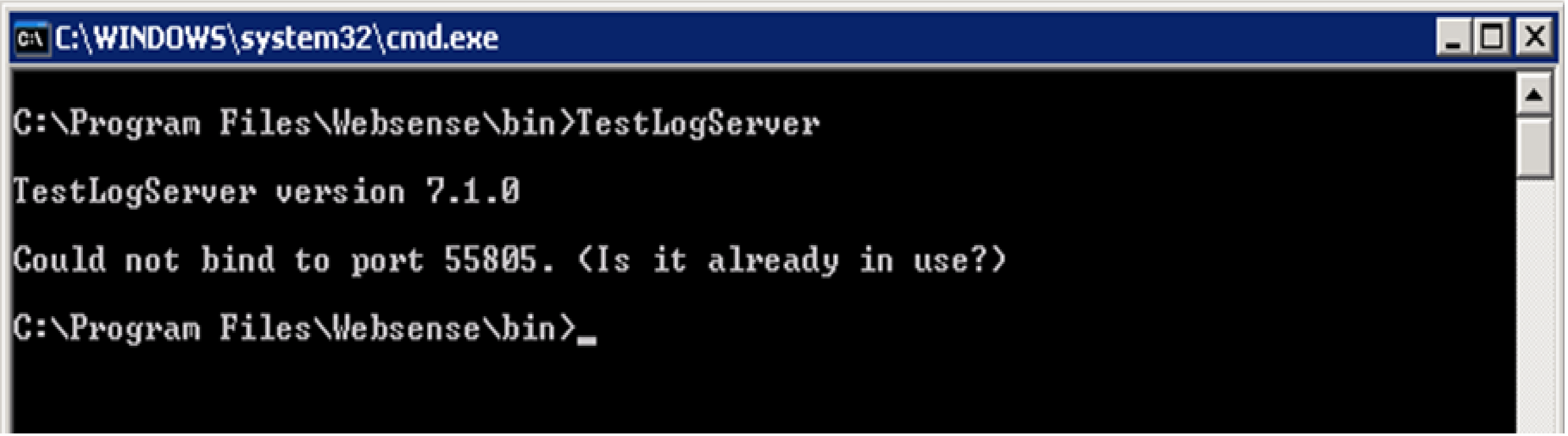


```
C:\Program Files\Websense\bin>WebsensePing -uip 10.212.5.168 -m 8 -url http://me
xico.com
------------------------------------------
 Sending HTTP_LOOKUP_REQUEST...
------------------------------------------

  URL = http://mexico.com
  User Name =
  Source IP = 10.212.5.168
  Destination IP = 192.5.73.105

  Disposition = CATEGORY_BLOCKED
  Lookup Code = WISP_URL_BLOCKED
  Category = Travel
  Lookup Type = 0
  Protocol ID = 1
  Run Analytics = False
  Logging Code = 1
  Protocol Cache TTL = 0
  URL Cache Cmd = 0
  URL Cache Type = 0
  URL Cache TTL = 0

  Block Message = HTTP/1.0 302 Moved
Location: http://10.212.5.168:15871/cgi-bin/blockpage.cgi?ws-session=687865862
Pragma: no-cache
Cache-Control: no-cache



  Elapsed Time = 1 ms

AVG TIME PER REQUEST = 1 ms
```

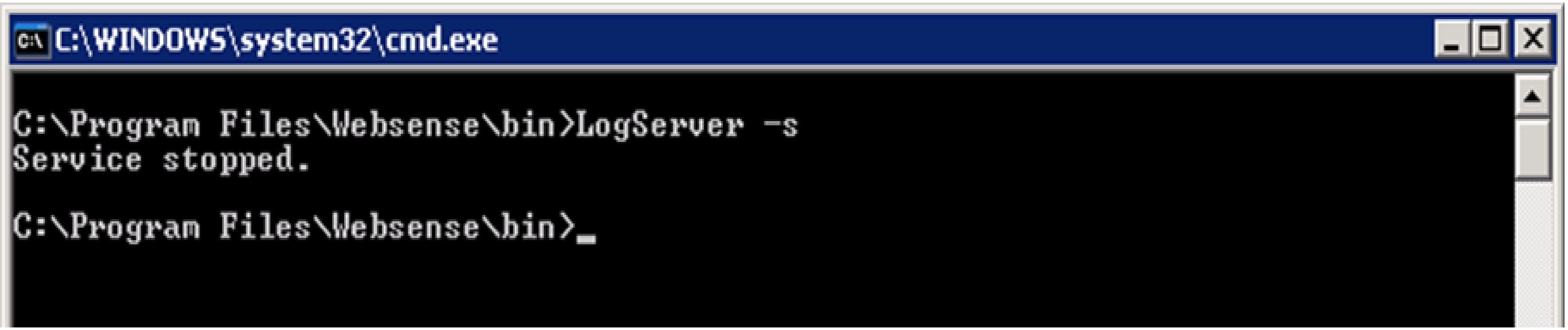
TestLogServer

- TestLogServer is a command-line utility that shows how URL Web traffic is seen by an integration or port span.
  - Useful for identifying URLs that need to be recategorized without permitting an entire category
  - Shows whether or not Websense software is seeing user names within URL Web traffic requests
- Why is this utility helpful?
  - Allows you to identify whether or not user names are being identified within URL requests
  - Allows you to identify whether the URLs you are trying to re-categorize are blocked or permitted

TestLogServer

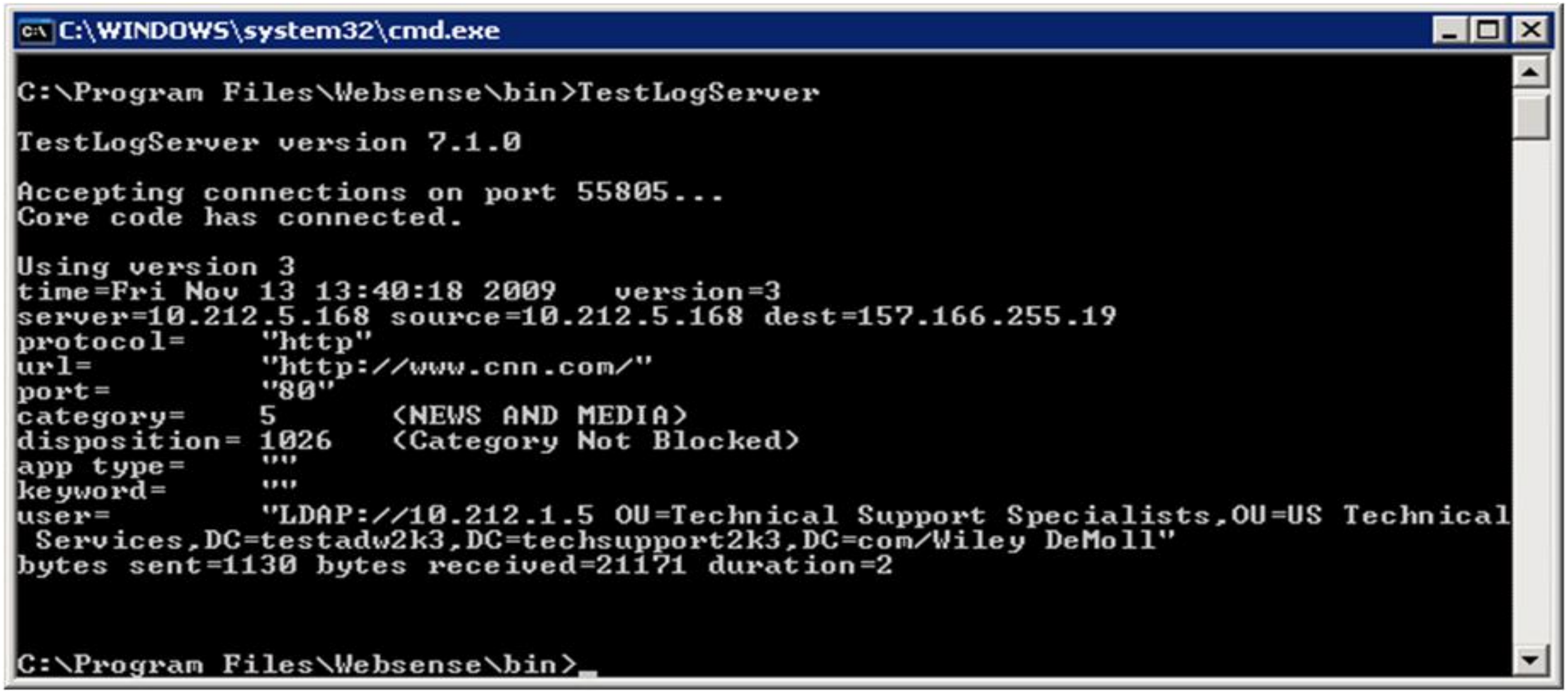


```
C:\Program Files\Websense\bin>TestLogServer

TestLogServer version 7.1.0

Could not bind to port 55805. (Is it already in use?)

C:\Program Files\Websense\bin>_
```



```
C:\Program Files\Websense\bin>LogServer -s
Service stopped.

C:\Program Files\Websense\bin>_
```

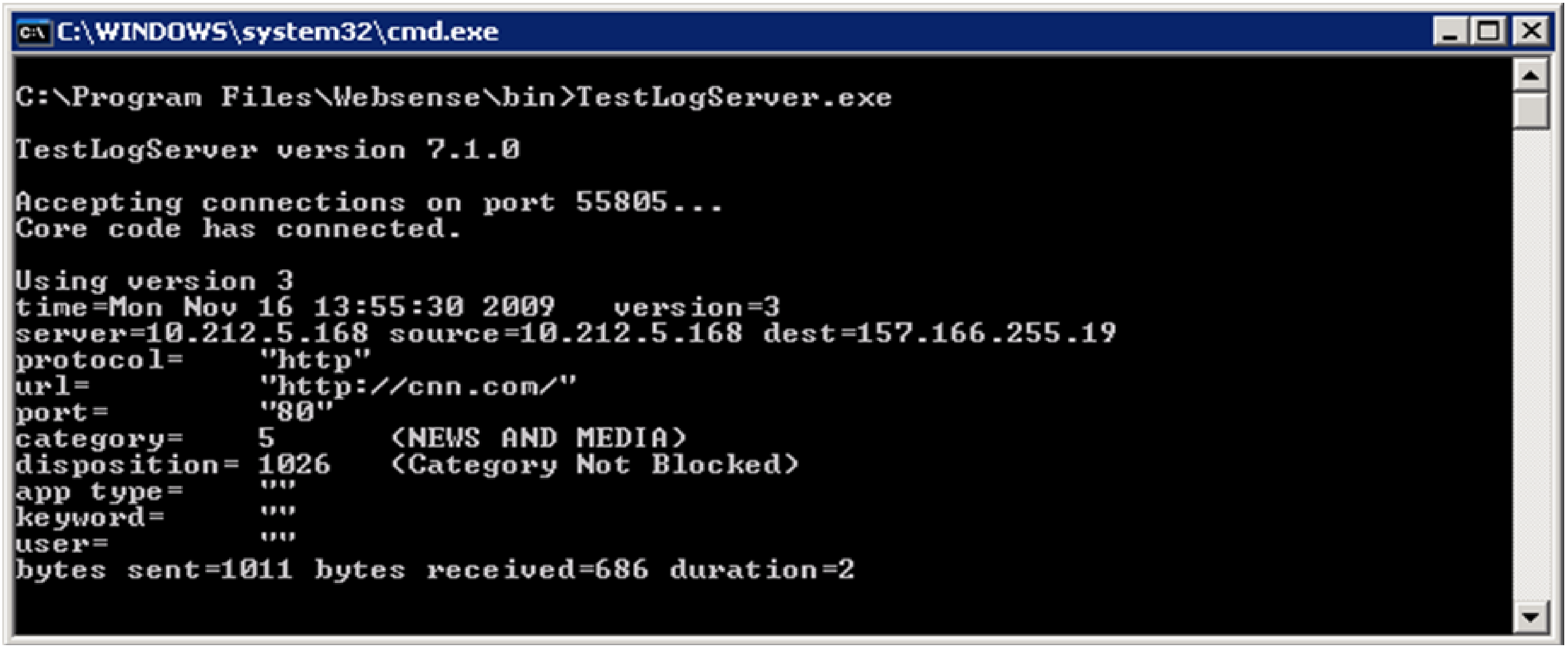
TestLogServer



```
C:\Program Files\Websense\bin>TestLogServer

TestLogServer version 7.1.0

Accepting connections on port 55805...
Core code has connected.

Using version 3
time=Fri Nov 13 13:40:18 2009   version=3
server=10.212.5.168 source=10.212.5.168 dest=157.166.255.19
protocol=    "http"
url=         "http://www.cnn.com/"
port=        "80"
category=    5      (NEWS AND MEDIA)
disposition= 1026   (Category Not Blocked)
app type=    ""
keyword=     ""
user=        "LDAP://10.212.1.5 OU=Technical Support Specialists,OU=US Technical
 Services,DC=testadw2k3,DC=techsupport2k3,DC=com/Wiley DeMoll"
bytes sent=1130 bytes received=21171 duration=2


C:\Program Files\Websense\bin>_
```

- TestLogServer output shows the URL, Category, Disposition (action applied), and Username.
- Also shows the IP address of the integration or Network Agent (server IP), as well as source and destination IP address.

TestLogServer



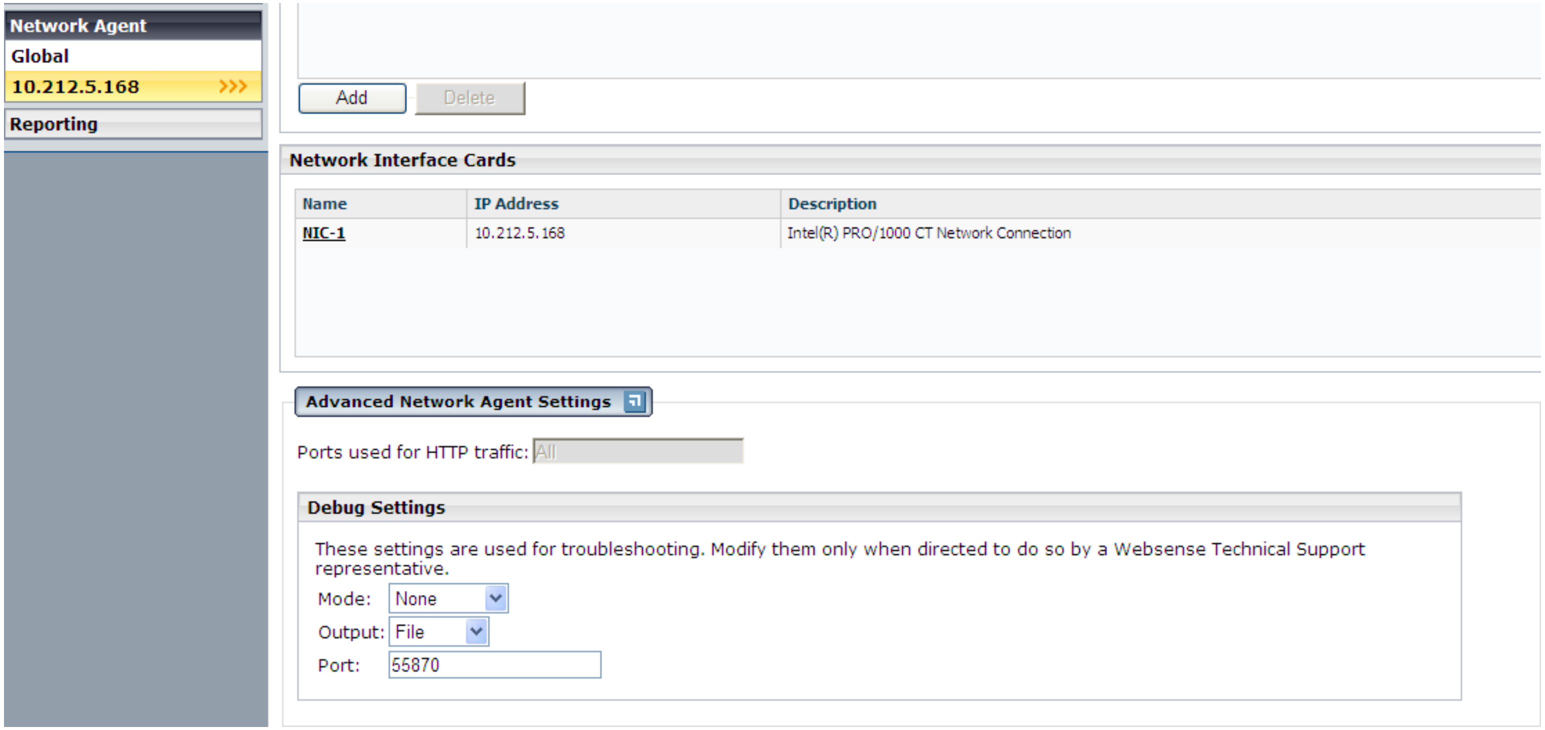
```
C:\Program Files\Websense\bin>TestLogServer.exe

TestLogServer version 7.1.0

Accepting connections on port 55805...
Core code has connected.

Using version 3
time=Mon Nov 16 13:55:30 2009   version=3
server=10.212.5.168 source=10.212.5.168 dest=157.166.255.19
protocol=     "http"
url=          "http://cnn.com/"
port=         "80"
category=     5       (NEWS AND MEDIA)
disposition= 1026    (Category Not Blocked)
app type=     ""
keyword=      ""
user=         ""
bytes sent=1011 bytes received=686 duration=2
```

- In this output, the user name is NOT identified.
  - This prevents user and group policies from being applied.
  - ONLY an IP address-based policy or the Default (*Global) policy can be applied.

Network Agent Troubleshooting

- Why am I NOT seeing traffic in TestLogServer?
  - What is your integration?
    - Proxy
    - Firewall
    - Stand-alone (Network Agent)
  - Have you configured a span/mirror along with your integration for protocol filtering?
- Network Agent troubleshooting reveals whether Network Agent can see the protocol signatures to filter and block of URLs and protocols.

Network Agent Troubleshooting



Network Interface Cards

Name	IP Address	Description
NIC-1	10.212.5.168	Intel(R) PRO/1000 CT Network Connection

Advanced Network Agent Settings

Ports used for HTTP traffic: All

Debug Settings

These settings are used for troubleshooting. Modify them only when directed to do so by a Websense Technical Support representative.

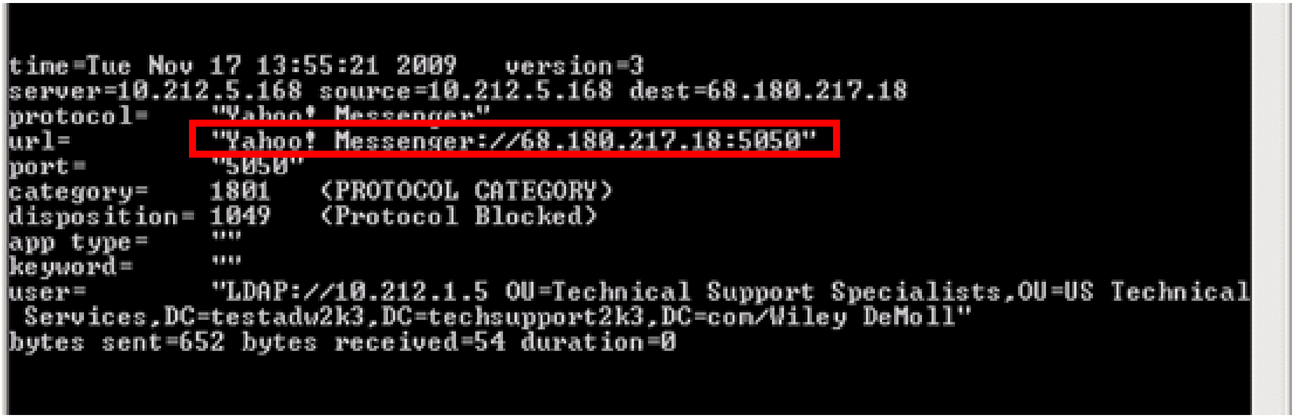
Mode: None

Output: File

Port: 55870

1. From the Mode drop-down list, select Detail.
2. Click OK, and then click Save All.

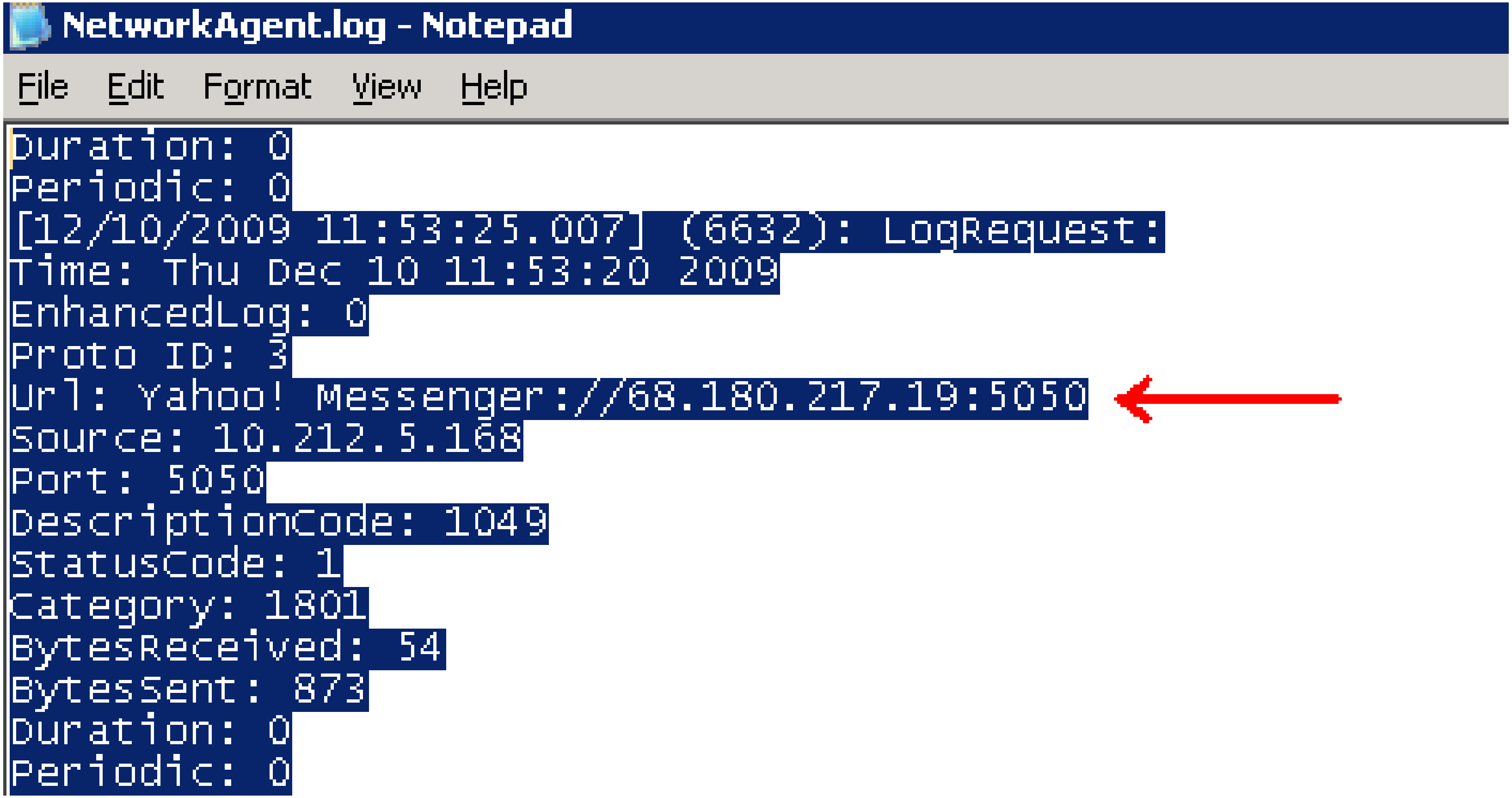
Network Agent Troubleshooting



```
time=Tue Nov 17 13:55:21 2009   version=3
server=10.212.5.168 source=10.212.5.168 dest=68.180.217.18
protocol=      "Yahoo! Messenger"
url=           "Yahoo! Messenger://68.180.217.18:5050"
port=          "5050"
category=      1801    <PROTOCOL CATEGORY>
disposition=   1049    <Protocol Blocked>
app type=      ""
keyword=       ""
user=          "LDAP://10.212.1.5 OU=Technical Support Specialists,OU=US Technical
 Services,DC=testadw2k3,DC=techsupport2k3,DC=com/Wiley DeMoll"
bytes sent=652 bytes received=54 duration=0
```

- This TestLogServer output shows that the protocol is blocked.
- To also review the Network Agent Debug output:
  - Make a note of the URL and port.
  - The NetworkAgent.log is the file generated when debugging is enabled.
  - Be careful as this logs ALL data and will grow quite large in size.

Network Agent Troubleshooting



```
Duration: 0
Periodic: 0
[12/10/2009 11:53:25.007] (6632): LogRequest:
Time: Thu Dec 10 11:53:20 2009
EnhancedLog: 0
Proto ID: 3
Url: Yahoo! Messenger://68.180.217.19:5050
Source: 10.212.5.168
Port: 5050
DescriptionCode: 1049
StatusCode: 1
Category: 1801
BytesReceived: 54
BytesSent: 873
Duration: 0
Periodic: 0
```

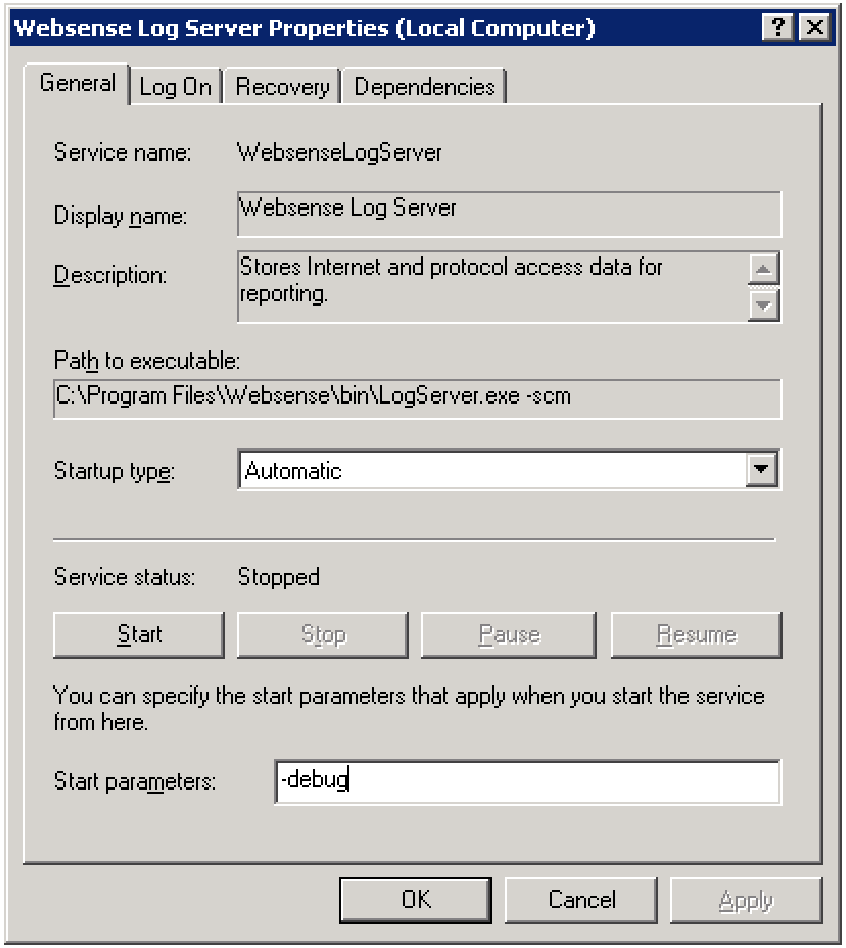
Network Agent Troubleshooting

- If you do not see the URL or protocol listed in the log, Network Agent is probably not seeing it.
- Some things to check when this occurs:
  - Is the Network Agent service running?
  - Have you properly configured your span/mirror port on your managed switch?
  - If you have multiple NICs on the Network Agent machine, is the correct NIC configured to see the traffic from your span/mirror?

Log Server Troubleshooting

- Log Server debug can be used to troubleshoot problems with logging and reporting.
  – Verify whether Log Server can connect to Policy Server and the Log Database
- To run LogServer in debug mode:
  1. Open the Windows Services dialog box.
  2. Right-click Websense Log Server.
  3. Select Properties.

Log Server Troubleshooting



Websense Log Server Properties (Local Computer)

Service name: WebsenseLogServer

Display name: Websense Log Server

Description: Stores Internet and protocol access data for reporting.

Path to executable:
C:\Program Files\Websense\bin\LogServer.exe -scm

Startup type: Automatic

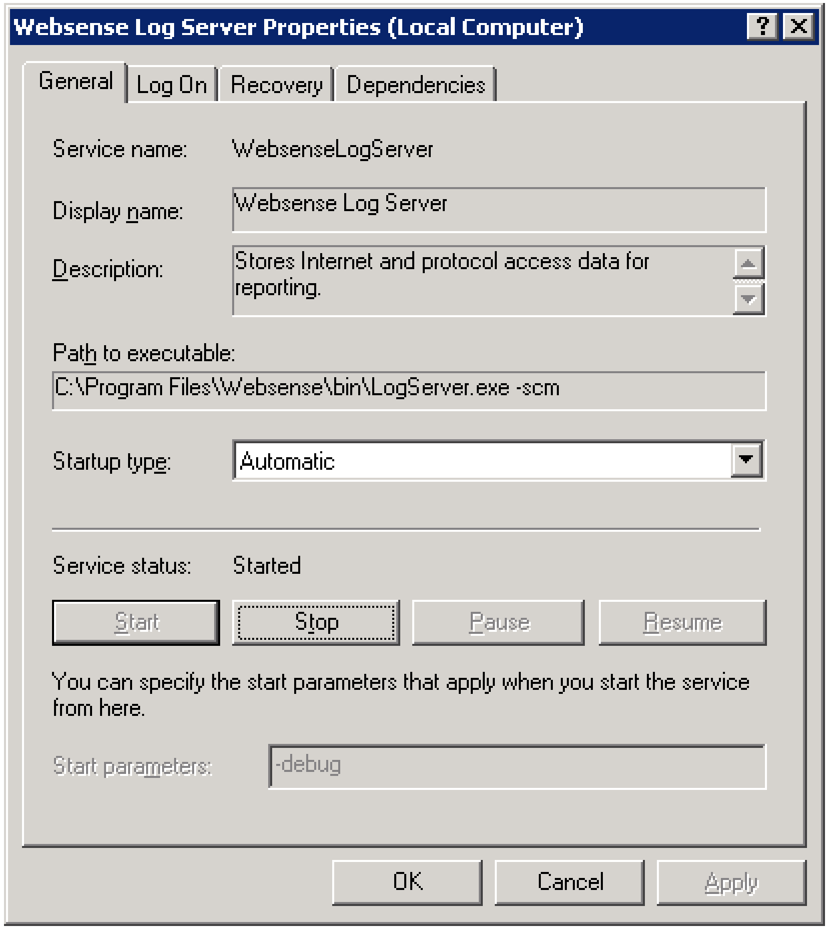
Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters: -debug

4. Enter -debug in the Start parameters field (near the bottom of the dialog box).

Log Server Troubleshooting



Websense Log Server Properties (Local Computer)

Service name: WebsenseLogServer

Display name: Websense Log Server

Description: Stores Internet and protocol access data for reporting.

Path to executable:
C:\Program Files\Websense\bin\LogServer.exe -scm

Startup type: Automatic

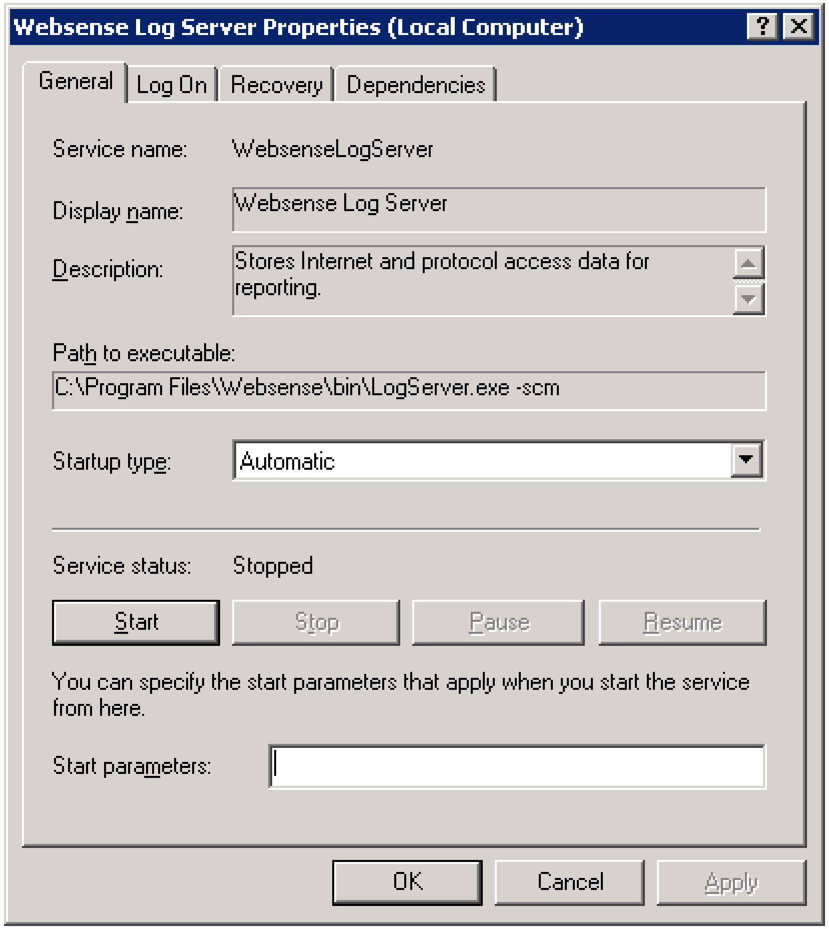
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters: -debug

5. Restart the Log Server service.

Log Server Troubleshooting



Websense Log Server Properties (Local Computer)

Service name: WebsenseLogServer

Display name: Websense Log Server

Description: Stores Internet and protocol access data for reporting.

Path to executable:
C:\Program Files\Websense\bin\LogServer.exe -scm

Startup type: Automatic

Service status: Stopped

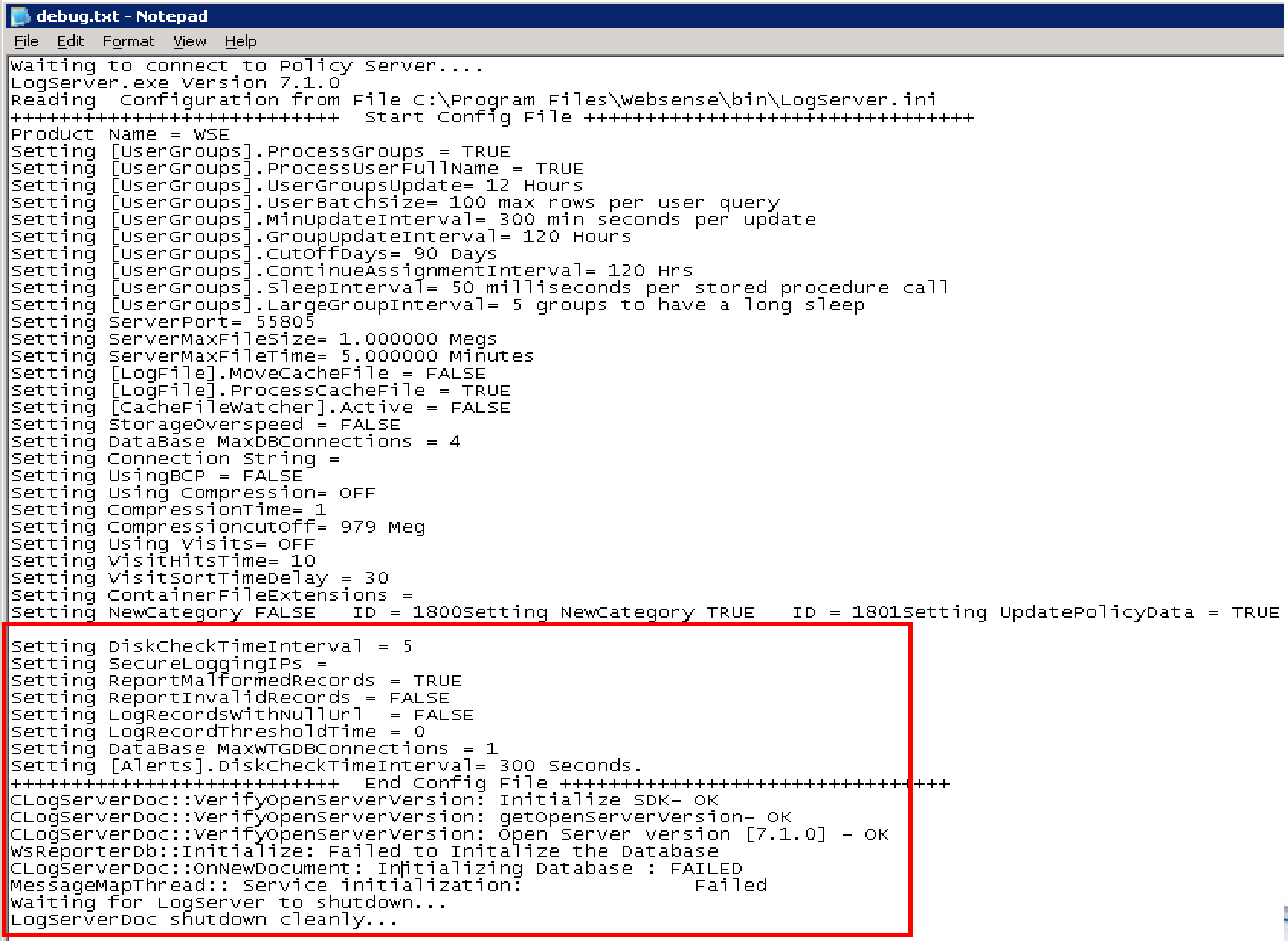
You can specify the start parameters that apply when you start the service from here.

Start parameters:

6. When the service stops on its own, remove the -debug parameter.

Log Server Troubleshooting

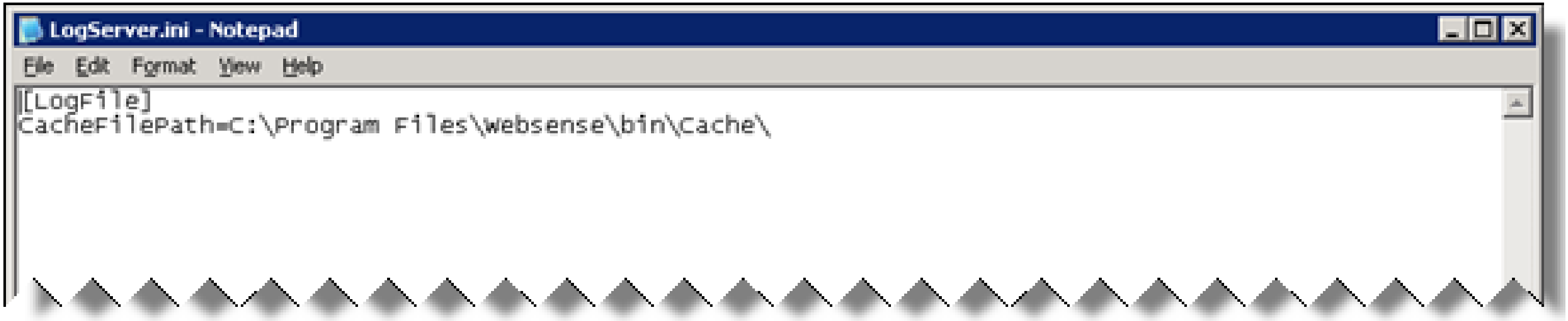
- A file called debug.txt is created in the Websense bin directory.



```
Waiting to connect to Policy Server....
LogServer.exe Version 7.1.0
Reading  Configuration from File C:\Program Files\Websense\bin\LogServer.ini
+++++++++++++++++++++++++++  Start Config File ++++++++++++++++++++++++++++++++
Product Name = WSE
Setting [UserGroups].ProcessGroups = TRUE
Setting [UserGroups].ProcessUserFullName = TRUE
Setting [UserGroups].UserGroupsUpdate= 12 Hours
Setting [UserGroups].UserBatchSize= 100 max rows per user query
Setting [UserGroups].MinUpdateInterval= 300 min seconds per update
Setting [UserGroups].GroupUpdateInterval= 120 Hours
Setting [UserGroups].CutoffDays= 90 Days
Setting [UserGroups].ContinueAssignmentInterval= 120 Hrs
Setting [UserGroups].SleepInterval= 50 milliseconds per stored procedure call
Setting [UserGroups].LargeGroupInterval= 5 groups to have a long sleep
Setting ServerPort= 55805
Setting ServerMaxFileSize= 1.000000 Megs
Setting ServerMaxFileTime= 5.000000 Minutes
Setting [LogFile].MoveCacheFile = FALSE
Setting [LogFile].ProcessCacheFile = TRUE
Setting [CacheFileWatcher].Active = FALSE
Setting StorageOverspeed = FALSE
Setting DataBase MaxDBConnections = 4
Setting Connection String =
Setting UsingBCP = FALSE
Setting Using Compression= OFF
Setting CompressionTime= 1
Setting Compressioncutoff= 979 Meg
Setting Using Visits= OFF
Setting VisitHitsTime= 10
Setting VisitSortTimeDelay = 30
Setting ContainerFileExtensions =
Setting NewCategory FALSE   ID = 1800Setting NewCategory TRUE   ID = 1801Setting UpdatePolicyData = TRUE

Setting DiskCheckTimeInterval = 5
Setting SecureLoggingIPs =
Setting ReportMalformedRecords = TRUE
Setting ReportInvalidRecords = FALSE
Setting LogRecordsWithNullUrl  = FALSE
Setting LogRecordThresholdTime = 0
Setting DataBase MaxWTGDBConnections = 1
Setting [Alerts].DiskCheckTimeInterval= 300 Seconds.
+++++++++++++++++++++++++++  End Config File ++++++++++++++++++++++++++++++++
CLogServerDoc::VerifyOpenServerVersion: Initialize SDK- OK
CLogServerDoc::VerifyOpenServerVersion: getOpenServerVersion- OK
CLogServerDoc::VerifyOpenServerVersion: Open Server version [7.1.0] - OK
WsReporterDb::Initialize: Failed to Initalize the Database
CLogServerDoc::OnNewDocument: Initializing Database : FAILED
MessageMapThread:: Service initialization:              Failed
Waiting for LogServer to shutdown...
LogServerDoc shutdown cleanly...
```

Log Server Troubleshooting

- Also check the LogServer.ini file in the Websense bin directory.



```
[LogFile]
CacheFilePath=C:\Program Files\Websense\bin\Cache\
```

Log Server Troubleshooting

- If Log Server does not start:
  - Check the ODBC connection, and either reconfigure the existing data source, or delete and recreate the ODBC source. (Be sure to reconnect Log Server to the ODBC source after recreating it.)
  - If you are using a trusted connection to the database, try a SQL connection.
  - Is your SQL Server allowing both Windows trusted and SQL connections (Mixed Security) or just one or the other?
  - Open the websense.ini file, located in the Websense bin directory, and make sure that the Log Server UID matches the one that appears in the config.xml file.
  - If all else fails, contact Websense Technical Support: create a case online at http://ask.websense.com.

Support Online Resources

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

- Create and manage support service requests using our online portal.

Customer Training Options

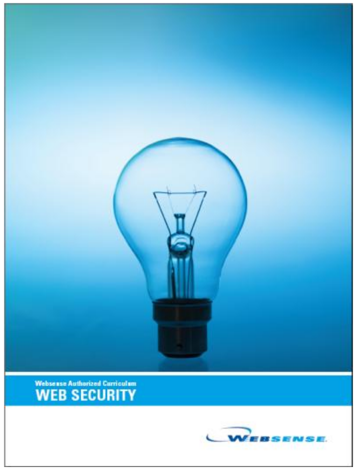
- To find Websense classes offered by Authorized Training Partners in your area, visit:

  http://www.websense.com/findaclass
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:

  readiness@websense.com

WEBSENSE®
Authorized Training
Partner

WEBSENSE®
Certified Instructor



Webinar Announcement

websense
ESSENTIAL INFORMATION PROTECTION™

Webinar Update

Title: Controlling Risk, Conserving Bandwidth, and Monitoring Productivity with Websense Web Security and Websense Content Gateway

Date: January 20, 2010

Time: 8:30 AM PST (GMT -8)

How to register:

http://www.websense.com/content/SupportWebinars.aspx

Questions?