

This article describes how to troubleshoot the HTTP AO.

Guide Contents
Main Article
Understanding the WAAS Architecture and Traffic Flow
Preliminary WAAS Troubleshooting
Troubleshooting Optimization
Troubleshooting Application Acceleration
Troubleshooting the CIFS AO
Troubleshooting the HTTP AO
Troubleshooting the EPM AO
Troubleshooting the MAPI AO
Troubleshooting the NFS AO
Troubleshooting the SSL AO
Troubleshooting the Video AO
Troubleshooting the Generic AO
Troubleshooting Overload Conditions
Troubleshooting WCCP
Troubleshooting AppNav
Troubleshooting Disk and Hardware Problems
Troubleshooting Serial Inline Clusters
Troubleshooting vWAAS
Troubleshooting WAAS Express
Troubleshooting NAM Integration

Contents

- [1 HTTP Accelerator Troubleshooting](#)
 - ◆ [1.1 Viewing HTTP Statistics](#)
 - ◆ [1.2 Viewing HTTPS Statistics](#)
 - ◆ [1.3 Viewing the HTTP Metadata Cache](#)
 - ◆ [1.4 Viewing the HTTPS Metadata Cache](#)
 - ◆ [1.5 Metadata Cache Cache-Control Behavior](#)
 - ◆ [1.6 Metadata Caching Exceptions](#)
- [2 HTTP AO Logging](#)

HTTP Accelerator Troubleshooting

The HTTP accelerator optimizes HTTP and HTTPS (in version 4.3.1 and later) traffic using the following techniques:

- **TCP connection reuse across the WAN.** Avoids a connection setup penalty for subsequent HTTP connections requested by the same client. (Does not apply to HTTPS traffic.)
- **HTTP metadata caching.** Certain HTTP responses are cached, along with their URLs and metadata information, so that the edge WAE can respond locally to subsequent requests for the same URL. (Available only in version 4.2.1 and later.) The three types of cached responses are as follows:
 - ◆ 301 Permanently-Redirected
 - ◆ 304 Not-Modified
 - ◆ 401 Authorization-Required
- **HTTPS metadata caching.** Certain HTTPS responses are cached, along with their URLs and metadata information, so that the edge WAE can respond locally to subsequent requests for the same URL. (Available only in version 4.3.1 and later.)
- **HTTP suppress server encoding.** Removes the Accept-Encoding header from the HTTP and HTTPS requests, preventing the server from sending compressed data towards the WAN. This allows the WAE to apply its own compression, typically resulting in a better compression ratio. (Available only in version 4.2.1 and later.)
- **DRE hints.** Provides specific hints to the DRE module to better compress the HTTP and HTTPS traffic based on the additional knowledge on the HTTP protocol provided by parsing the layer 7 payload:
 - ◆ Skip header: Instructs the DRE module to not compress HTTP/HTTPS headers resulting in a better compression of the object.
 - ◆ Flush: Instructs the DRE module to start compressing as soon as an HTTP/HTTPS transaction is fully processed.
 - ◆ Skip LZ: Instructs the DRE module to not apply LZ compression to all objects already compressed by the original server, thus reducing the CPU overhead.

The HTTP metadata caching, suppress server encoding, and DRE hinting features can be configured separately. The TCP connection reuse feature is always active when the HTTP AO is enabled and applies only to HTTP traffic.

You can verify the general AO configuration and status with the **show accelerator** and **show license** commands, as described in the [Troubleshooting Application Acceleration](#) article. The Enterprise license is required for HTTP accelerator operation.

Next, verify the status that is specific to the HTTP AO by using the **show accelerator http** command, as shown in Figure 1. You want to see that the HTTP AO is Enabled, Running, and Registered, and that the connection limit is displayed. If the Config State is Enabled but the Operational State is Shutdown, it indicates a licensing problem. For each of the HTTP features the current mode is shown (User/Default) along with the value (Enabled, Disabled or configured value). The Suppress Server Encoding and Metadacache items were added in version 4.2.1, and the DRE Hints and HTTPS Metadacache items were added in version 4.3.1.

For HTTPS traffic to be optimized by both the SSL and HTTP AOs, ensure that one of these optional features is enabled: HTTPS metadata caching, suppress-server-encoding or DRE hints.

Figure 1. Verifying the HTTP Accelerator Status

The screenshot shows the output of the command `WAE# sh accelerator http`. The output is structured as follows:

Accelerator	Licensed	Config State	Operational State
http	Yes	Enabled	Running

Below this, the HTTP configuration is shown:

Accelerator Config Item	Mode	Value
Suppress Server Encoding	User	Enabled
DRE Hints	Default	Disabled
Metadatatocache	User	Enabled
HTTPS Metadatatocache	Default	Disabled
MaxAge	Default	86400
MinAge	Default	60
Filter-extension	User	All
Redirect	Default	Enabled
Unauthorized	Default	Enabled
Conditional	Default	Enabled

Finally, the Policy Engine Config Item is shown:

Policy Engine Config Item	Value
State	Registered
Default Action	Use Policy
Connection Limit	6000
Effective Limit	5990
Keepalive timeout	5.0 seconds

Callouts in the image highlight the **Enabled** and **Running** states, and the **Registered** state with its associated values (6000, 5990, 5.0 seconds).

Use the **show running-config** command to verify that the HTTP/HTTPS traffic policy is properly configured and which of the features is enabled. You want to see **accelerate http** for the Web application action and you want to see appropriate match conditions listed for the HTTP classifier, as follows:

WAE674# **sh run | include HTTP**

```

accelerator http suppress-server-encoding enable
accelerator http metadatatocache https enable
accelerator http dre-hints enable

classifier HTTP
classifier HTTPS
  name Web classifier HTTP action optimize full accelerate http
  name Web classifier HTTPS action optimize DRE no compression none
    
```

Annotations on the right side of the output:

- <----- in 4.2.1 and lat
- <----- in 4.3.1 and lat
- <----- in 4.3.1 and la
- at least one of
- <----- HTTP acceleration
- <----- HTTPS static pol
- matching any SSL

WAE674# **sh run | begin HTTP**

```

...skipping
classifier HTTP
  match dst port eq 80
  match dst port eq 8080
  match dst port eq 8000
  match dst port eq 8001
  match dst port eq 3128
    
```

WAE674# **sh run | begin HTTPS**

```

...skipping
classifier HTTPS
  match dst port eq 443
    
```

<----- add here any non

Viewing HTTP Statistics

Use the **show statistics accelerator http** command to see the following statistics:

- How much time is being saved by the HTTP AO. You can see the overall Time Saved by the entire HTTP AO or the Time Saved by each of the features:
 - ◆ Time Saved by fast connection reuse
 - ◆ Time Saved by the three metadata caches
- Number of cache hits/misses for the metadata caches
- Number of times suppress server encoding is applied to HTTP requests
- Number of times DRE hints are provided based on the content of the HTTP headers
- Number of HTTP transactions (request+response) processed
- Number of errors in the HTTP header processing
- Number of cache revalidations

```
WAE674# sh stat accel http
```

```
HTTP:
```

```
Global Statistics
```

```
-----
```

```
Time Accelerator was started: Tue Apr 6 06:04:06 2010
Time Statistics were Last Reset/Cleared: Tue Apr 6 06:04:06 2010
Total Handled Connections: 3743984
Total Optimized Connections: 3743984
Total Connections Handed-off with Compression Policies Unchanged: 0
Total Dropped Connections: 0
Current Active Connections: 48
Current Pending Connections: 0
Maximum Active Connections: 176
Total Time Saved (ms): 35584437 <-----Should be in
Current Active Connections Free For Fast Connection Use: 2
Total Connections Handed-off: 0
Total Connections Handed-off with Compression Policies Disabled: 0
Total Connections Handed-off to SSL: 0
Total Connection Hand-off Failures: 0
Total Fast Connection Successes: 3617244 <-----Should be in
Total Fast Connection Failures: 0
Maximum Fast Connections on a Single Connection: 100
Total CONNECT Requests with Incomplete Message: 0
Percentage of Connection Time Saved: 37
Total Round Trip Time For All Connections (ms): 4922767377
Total Fast Connections Initiated by Peer: 0
Total SYN Timeouts: 0
Total Time for Metadata Cache Miss (ms): 2 <-----Output from
RTT saved by Redirect Metadata Cache (ms): 5988 <-----Should be in
RTT saved by Authorization Redirect Metadata Cache (ms): 345 <-----Should be in
RTT saved by Content Refresh Check Metadata Cache (ms): 44987 <-----Should be in
Total Time Saved by Fast Connection Use (ms): 456
Total Locally Served Redirect Responses: 453 <-----Should be in
Total Locally Served Unauthorized Responses: 56 <-----Should be in
Total Locally Served Conditional Responses: 4932 <-----Should be in
Total Remotely Served Redirect Responses: 0
Total Remotely Served Unauthorized Responses: 0
Total Remotely Served Conditional Responses: 1
Total Requests with URL Longer than 255 Characters: 0
Total Requests with HTTP Pipelining: 0
Total Transactions Handled: 2 <-----Total number
Total Server Compression Suppression: 1 <-----Total number
Total Requests Requiring Server Content-Revalidation: 0
Total Responses not to be Cached: 0
Total Connections Expecting Authentication: 0
```

```

Total Connections with Unsupported HTTP Requests:      0
Total Connections with Unsupported HTTP Responses:    0
Total Hints Sent to DRE Layer to Flush Data:         2
Total Hints Sent to DRE Layer to Skip LZ:           0
Total Hints Sent to DRE Layer to Skip Header Information: 1

```

If the Total Time Saved counter in the output above is not incrementing or is quite small, it indicates that the HTTP AO is not providing much benefit. If the Total Time Saved by one of the three metadata caches is not incrementing or is quite small, it indicates that the corresponding metadata cache is not providing much benefit.

The Total Server Compression Suppression counter indicates how many times the Accept-Encoding header has been removed, in an attempt to provide a better compression by the WAE device. The Total Hints Sent to DRE Layer counters indicate how many times each of the DRE hints (Flush Data, Skip LZ, Skip Header) has been issued to the DRE module, in an attempt to better compress the data.

To view similar information from the Central Manager in version 4.2.1 and later, choose the WAE device, then choose **Monitor > Acceleration > HTTP Acceleration Report** and choose the Details tab to see the following charts:

- HTTP Response Time Savings (fast connection reuse, redirect, conditional, and unauthorized cached)
- HTTP Optimization Count (number of times each of the above optimizations has been applied)
- HTTP Optimization Techniques (for all HTTP optimizations, including metadata caches, connection reuse, DRE hints and suppress-server-encoding)

To see debugging information on the HTTP header parsing and error conditions, use the **show statistics accelerator http debug** command (in 4.3.1 and later) to determine the following:

- Number of 301, 304 and 401 responses cached
- Number of HTTP headers, version and methods
- Reasons for HTTP responses not being cached
- Total number of HTTP responses being cached
- Reasons for HTTP requests not being served from the local cache

Use the **show statistics connection optimized http** command to check that the WAAS device is establishing optimized HTTP connections. Verify that an "H" appears in the Accel column for HTTP connections, which indicates that the HTTP AO was used, as follows:

```

WAE674# sh stat conn opt http
Current Active Optimized Flows:                2
  Current Active Optimized TCP Plus Flows:     2
  Current Active Optimized TCP Only Flows:    0
  Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows:          0
Current Active Pass-Through Flows:            0
Historical Flows:                             100
D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO
ConnID  Source IP:Port      Dest IP:Port      PeerID              Accel
5929    10.10.10.10:3446    10.10.100.100:80  00:14:5e:84:24:5f  THDL      <-----Look for

```

You can check connection statistics for closed connections by using the **show statistics connection closed http** command.

To view similar information from the Central Manager, choose the WAE device, then choose **Monitor > Optimization > Connections Statistics**.

Figure 2. Connection Statistics Report with HTTP

The screenshot shows the Cisco Wide Area Application Services (WAAS) Central Manager interface. The main content area displays the 'Connections Summary Table For Device: dc-wae-03'. The table has the following columns: Source IP:Port, Dest IP:Port, Peer Id, Applied Policy, Open Duration, Org Bytes, Opt Bytes, % Comp, and Classifier Name. A red circle highlights the 'Applied Policy' column, and a yellow box with the text 'HTTP AO applied' points to the globe icon in the 'Applied Policy' column for the first row.

Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open Duration	Org Bytes	Opt Bytes	% Comp	Classifier Name
2.43.85.131:3536	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:54	194 Bytes	62 Bytes	68%	HTTP
2.43.85.131:3728	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:49	194 Bytes	62 Bytes	68%	HTTP
2.43.85.131:4311	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:40	194 Bytes	62 Bytes	68%	HTTP
2.43.85.131:4180	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:39	194 Bytes	62 Bytes	68%	HTTP
2.43.85.131:4540	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:34	0 Bytes	62 Bytes	-	HTTP
2.43.85.131:1031	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:29	0 Bytes	62 Bytes	-	HTTP
2.43.85.131:1124	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:1:25	0 Bytes	62 Bytes	-	HTTP
2.43.85.131:3492	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:0:54	0 Bytes	62 Bytes	-	HTTP
2.43.85.131:4312	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:0:43	0 Bytes	62 Bytes	-	HTTP
2.43.85.131:4422	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:0:42	0 Bytes	62 Bytes	-	HTTP
2.43.85.131:4624	2.43.85.3:80	wae84-08-psirt2-br-wae2	[Globe Icon]	0:0:41	194 Bytes	62 Bytes	68%	HTTP

In the Connection Statistics report, the globe icon in the Applied Policy column shows that the HTTP AO was used for a connection. (Place your cursor over an icon to see its meaning.)

You can view the HTTP connection statistics by using the **show statistics connection optimized http detail** command. Look for the "Fast connections" counter in the output. A positive value for this counter means that the HTTP AO benefits clients by reusing persistent connections, which reduces latency.

```
WAE674# show stat conn opt http detail
```

```

Connection Id:          1496
  Peer Id:              00:14:5e:84:24:5f
  Connection Type:     EXTERNAL CLIENT
  Start Time:         Wed Jul 15 05:09:52 2009
  Source IP Address:   10.10.10.10
  Source Port Number:  1760
  Destination IP Address: 10.10.100.100
  Destination Port Number: 80
  Application Name:    Web
  Classifier Name:     HTTP
  Map Name:           basic
  Directed Mode:      FALSE
  Preposition Flow:   FALSE
  Policy Details:
    Configured:        TCP_OPTIMIZE + DRE + LZ
    Derived:          TCP_OPTIMIZE + DRE + LZ
    Peer:             TCP_OPTIMIZE + DRE + LZ
    Negotiated:       TCP_OPTIMIZE + DRE + LZ
    Applied:          TCP_OPTIMIZE + DRE + LZ
  Accelerator Details:
    Configured:       HTTP
    Derived:         HTTP
    Applied:         HTTP
    Hist:           None

```

<-----Should see Web
 <-----Should see HTTP

<-----Should see HTTP configured
 <-----Should see HTTP applied

```

                                Original                Optimized
                                -----                -----
Bytes Read:                        266                139160
Bytes Written:                     82686               128
. . .
HTTP : 1496

Time Statistics were Last Reset/Cleared:                Wed Jul 15
05:09:52 2009
Total Bytes Read:                        3269
56367
Total Bytes Written:                     3269
56367
Total Bytes Buffered:                    0
0
Total Internal Bytes Read:                92
Total Internal Bytes Written:             92
Bit Flags for I/O state:                 1040
Internal object pointer:                 2046823200

Fast connections:                            11      <-----Reused connec
. . .

```

Viewing HTTPS Statistics

(This section applies only to version 4.3.1 and later.)

Use the **show statistics accelerator http https** command to see the following statistics:

- How much time is being saved by the HTTP AO for HTTPS traffic. You can see the overall Time Saved by the entire HTTPS metadata cache or the Time Saved by each of the three metadata caches
- Number of cache hits/misses for the metadata caches
- Number of times suppress server encoding is applied to HTTPS requests
- Number of times DRE hints are provided based on the content of the HTTPS headers
- Number of HTTPS transactions (request+response) processed
- Number of errors in the HTTPS header processing
- Number of cache revalidations

WAE674# **sh stat accel http https**

```

HTTPS Statistics
-----
Total Optimized HTTPS Connections:                10      <-----Should be incre
Total Handled HTTPS Connections:                 10      <-----Should be incre
Total Active HTTPS Connections:                   2
Total Proxy-Connect HTTPS Connections:           0
Total Proxy-Connect HTTPS Insert Failures:        0
RTT saved by HTTPS Content Refresh Check Metadata Cache - (ms): 44      <-----Should be increm
RTT saved by HTTPS Redirect Metadata Cache - (ms): 10      <-----Should be increm
RTT saved by HTTPS Authorization Required Metadata Cache - (ms): 5      <-----Should be increm
Total Locally Served HTTPS Conditional Responses: 44      <-----Should be increm
Total Locally Served HTTPS Redirect Responses:    10      <-----Should be increm
Total Locally Served HTTPS Unauthorized Responses: 5      <-----Should be increm
Total Remotely Served HTTPS Conditional Responses: 32
Total Remotely Served HTTPS Redirect Responses:  2
Total Remotely Served HTTPS Unauthorized Responses: 1
Total Hints Sent to DRE Layer to Skip Header Information - HTTPS: 121
Total Hints Sent to DRE Layer to Flush Data - HTTPS: 121
Total Hints Sent to DRE Layer to Skip LZ - HTTPS: 0

```

```

Total Server Compression Suppression - HTTPS:                110
Total Time Saved from all HTTPS metadata cache hits:         59      <-----Should be increm
Total Time HTTPS Cache Miss:                                  4
Total HTTPS Requests Requiring Server Content-Revalidation: 32
Total HTTPS Responses not to be Cached:                     0
Total HTTPS Connections Bypassed due to URL Based Bypass List: 0
Total HTTPS Connections Bypassed due to IP Based Bypass List: 0

```

If the Total Time Saved counter in the output above is not incrementing or is quite small, it indicates that the HTTP AO is not providing much benefit to the HTTPS traffic. If the Total Time Saved by one of the three metadata caches is not incrementing or is quite small, it indicates that the corresponding metadata cache is not providing much benefit.

The Total Server Compression Suppression counter indicates how many times the Accept-Encoding header has been removed from HTTPS requests, in an attempt to provide a better compression by the WAE device. The Total Hints Sent to DRE Layer counters indicate how many times each of the DRE hints (Flush Data, Skip LZ, Skip Header) has been issued to the DRE module, in an attempt to better compress the data.

To view similar information from the Central Manager in version 4.3.1 and later, choose the WAE device, then choose **Monitor > Acceleration > HTTPS Acceleration Report** and choose the Details tab to see the following charts:

- HTTPS Response Time Savings (redirect, conditional, and unauthorized cached)
- HTTPS Optimization Count (number of times each of the above optimizations has been applied)
- HTTPS Optimization Techniques (for all HTTPS optimizations, including metadata caches, DRE hints and suppress-server-encoding)

To see debugging information on the HTTPS header parsing and error conditions, use the **show statistics accelerator http debug** command to determine the following:

- Number of 301, 304 and 401 responses cached
- Number of HTTP headers, version and methods
- Reasons for HTTP responses not being cached
- Total number of HTTP responses being cached
- Reasons for HTTP requests not being served from the local cache

Use the **show statistics connection optimized http** command to check that the WAAS device is establishing optimized HTTPS connections. Verify that both an "H" and an "S" appear in the Accel column for HTTPS connections, which indicates that both the HTTP and SSL AOs were used, as follows:

```

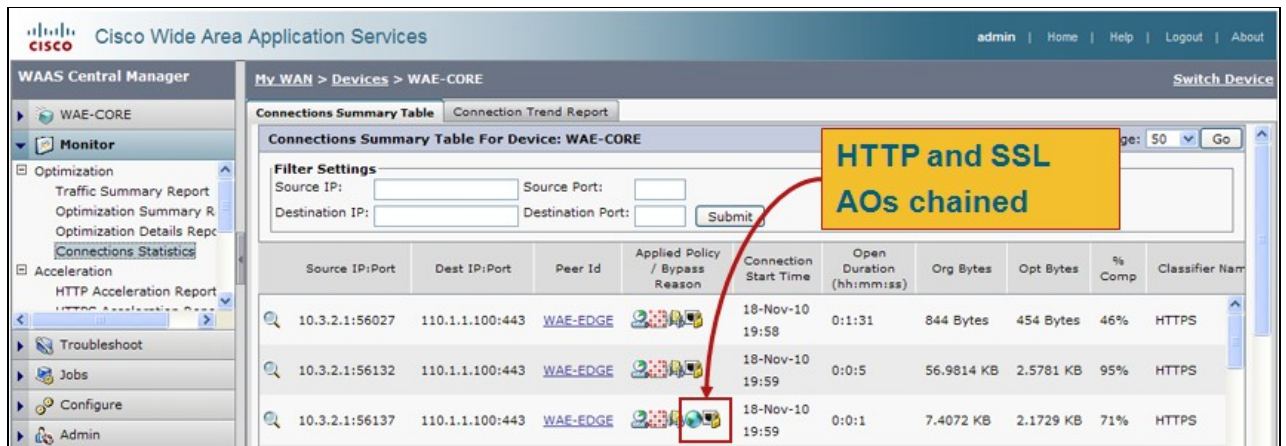
WAE674# sh stat conn opt http
Current Active Optimized Flows:                2
  Current Active Optimized TCP Plus Flows:     2
  Current Active Optimized TCP Only Flows:     0
  Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows:           0
Current Active Pass-Through Flows:             0
Historical Flows:                              100
D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO
ConnID  Source IP:Port  Dest IP:Port  PeerID  Accel
5929    10.10.10.10:3446  10.10.100.100:80  00:14:5e:84:24:5f  THSDL      <-----Look fo

```

You can check connection statistics for closed connections by using the **show statistics connection closed http** or **show statistics connection closed ssl** commands.

To view similar information from the Central Manager, choose the WAE device, then choose **Monitor > Optimization > Connections Statistics**.

Figure 3. Connection Statistics Report with HTTP and SSL



In the Connection Statistics report, the globe icon in the Applied Policy column shows that the HTTP AO was used for a connection and the lock icon indicates that the SSL AO was applied. (Place your cursor over an icon to see its meaning.)

You can view the HTTPS connection statistics by using the **show statistics connection optimized http detail** and **show statistics connection optimized ssl detail** commands.

```

WAE674# show stat conn opt http detail
Connection Id:          34
Peer Id:                00:14:5e:cd:9c:c9
Connection Type:       EXTERNAL CLIENT
Start Time:            Thu Oct 28 14:47:56 2010
Source IP Address:     10.3.2.1
Source Port Number:    40829
Destination IP Address: 110.1.1.100
Destination Port Number: 443
Application Name:      SSL
Classifier Name:       HTTPS
Map Name:              basic
Directed Mode:         FALSE
Preposition Flow:      FALSE
Policy Details:
    Configured:         TCP_OPTIMIZE
    Derived:            TCP_OPTIMIZE
    Peer:               TCP_OPTIMIZE
    Negotiated:         TCP_OPTIMIZE + DRE + LZ
    Applied:            TCP_OPTIMIZE + DRE + LZ
Accelerator Details:
    Configured:         None
    Derived:            None
    Applied:            HTTP, SSL
    Hist:               None
    
```

<-----Should see SSL

<-----Should see HTTPS

<-----Should see HTTP and SSL applied

	Original	Optimized
Bytes Read:	5162	21874
Bytes Written:	1977819	5108
Total Reduction Ratio: 98.639%		

HTTP : 34

```

Time Statistics were Last Reset/Cleared: Thu Oct 28
14:47:56 2010
Total Bytes Read: 4620
1972570
Total Bytes Written: 4620
1972570
. . .

```

SSL : 34

```

Time Statistics were Last Reset/Cleared: Thu Oct 28
14:47:56 2010
Total Bytes Read: 0
0
Total Bytes Written: 0
0
. . .

```

```

Hostname in HTTP CONNECT:
IP Address in HTTP CONNECT:
TCP Port in HTTP CONNECT:

```

<----- the last three counters are
Proxy Connect type of HTTP

Viewing the HTTP Metadata Cache

To display the content of the three HTTP metadata caches (redirect, conditional, and unauthorized), use the **show cache http-metadatacache all** command. Only the full URL and the expiration (in seconds) are displayed. You can also display the content of each of the three caches separately by using the following commands:

- **show cache http-metadatacache redirect-response**
- **show cache http-metadatacache conditional-response**
- **show cache http-metadatacache unauthorized-response**

The typical output of the above commands is as follows:

```

Redirect Cache
Active entries: 1, Max Entries: 1500
URL: www.abcnews.com/, Expiration (sec): 3206
Conditional Cache
Active entries: 6, Max Entries: 10500
URL: www.cisco.com/web/fw/i/quicklinks-rnd-corners.gif, Expiration (sec): 3594
URL: www.cisco.com/web/fw/i/hp-sprites.gif, Expiration (sec): 3594
URL: www.cisco.com/en/US/home/images/ba-actsGreen-logo.jpg, Expiration (sec): 3594
URL: www.cisco.com/en/US/home/images/fp-eos3.jpg, Expiration (sec): 3594
URL: www.cisco.com/en/US/home/images/fp-AP541n.jpg, Expiration (sec): 3594
URL: www.cisco.com/web/fw/c/home.min.css, Expiration (sec): 3592
Unauthorized Cache
Active entries: 1, Max Entries: 3000
URL: 1.yimg.com/index.html, Expiration (sec): 86393

```

You can clear the content of the three caches with the **clear cache http-metadatacache all** command.

If you want to clear the content of each cache separately, you can use the following commands:

- **clear cache http-metadatacache redirect-response**

- **clear cache http-metadatabcache conditional-response**
- **clear cache http-metadatabcache unauthorized-response**

If you want to specify a URL to be deleted you can use the following command:

```
clear cache http-metadatabcache {allredirect|conditional|unauthorized} URL
```

Viewing the HTTPS Metadata Cache

To display the number of entries in the three HTTPS metadata caches (redirect, conditional, and unauthorized), use the **show cache http-metadatabcache https** command. Unlike the corresponding command for the HTTP metadata cache, the URL and the expiration time are not displayed. You can also display the number of entries for each of the three caches separately by using the following commands:

- **show cache http-metadatabcache https redirect-response**
- **show cache http-metadatabcache https conditional-response**
- **show cache http-metadatabcache https unauthorized-response**

The typical output of the above commands is as follows:

```
HTTPS Redirect Cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 3250
HTTPS Conditional Cache
Active HTTP entries: 0, Active HTTPS entries: 11 Max Entries: 22750
HTTPS Unauthorized Cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 6500
```

You can clear the content of the three caches with the **clear cache http-metadatabcache https** command.

If you want to clear the content of each cache separately, you can use the following commands:

- **clear cache http-metadatabcache https redirect-response**
- **clear cache http-metadatabcache https conditional-response**
- **clear cache http-metadatabcache https unauthorized-response**

Metadata Cache Cache-Control Behavior

For HTTP and HTTPS (in version 4.3.1) 304 responses, the metadata cache honors all Cache-Control directives (Cache-Control: no-cache, no-store, private, must-revalidate, proxy-revalidate, max-age=0, Pragma: no-cache). There is an option to disable such Cache-Control checks, which means that all 304 responses with Cache-Control headers specifying no-cacheability are cached and all requests with Cache-Control headers specifying no-cacheability can be served from the local cache.

Understand that disabling the cache control checks might increase the benefits of the metadata-cache, because some browsers or web servers might have a default option to include one cache control header in all responses in order to force revalidation of the object through the original server. This would make the metadata cache ineffective for 304 responses.

The option can be independently controlled for HTTP/S requests (cache lookups) and responses (cache insertions).

To disable cache control checks on HTTP/S 304 requests, use the following command:

```
WAE#accelerator http metadatabcache request-ignore-no-cache enable
```

This command forces the metadatatcache to disregard all Cache-Control directives in HTTP/S 304 requests. (The default [no] form of this command forces the metadatatcache to honor all Cache-Control directives in HTTP/S 304 requests.)

To disable cache control checks on HTTP/S 304 responses, use the following command:

```
WAE#accelerator http metadatatcache response-ignore-no-cache enable
```

This command forces the metadatatcache to disregard all Cache-Control directives in HTTP/S 304 responses. (The default [no] form of this command forces the metadatatcache to honor all Cache-Control directives in HTTP/S 304 responses.)

The metadata cache honors Cache-Control headers for 301 and 401 responses. If the response has any of the Cache-Control headers (no-cache, no-store, private, must-revalidate, proxy-revalidate, max-age=0, Pragma: no-cache), it is not cached.

Metadata Caching Exceptions

There are certain exceptions to what is cached. The cache insertion or lookup does not occur when the HTTP AO encounters one of the following conditions on the HTTP/S request/response being processed:

- Non-RFC complaint requests and responses: malformed/invalid headers, repeated headers, missing headers, unexpected body, unexpected chunked encoding
- URL size is more than 255 characters
- HTTP pipelined transactions
- WebDav methods
- HEAD method
- 301/401 responses with cookie headers
- 301 responses with a total header length of more than 768 bytes
- 401 responses with a total header length of more than 384 bytes
- 401 responses with a chunked body
- 401 responses with unsupported authentication method (supported methods include: Basic, NTLM, Negotiate, Kerberos, Digest, Oauth)
- Partial HTTP header (header split) available for processing

HTTP AO Logging

The following log files are available for troubleshooting HTTP AO issues:

- Transaction log files: /local1/logs/tfo/working.log (and /local1/logs/tfo/tfo_log_*.txt)
- Debug log files: /local1/errorlog/httpao-errorlog.current (and httpao-errorlog.*)

For easier debugging, you should first set up an ACL to restrict packets to one host.

```
WAE674(config)# ip access-list extended 150 permit tcp host 10.10.10.10 any  
WAE674(config)# ip access-list extended 150 permit tcp any host 10.10.10.10
```

To enable transaction logging, use the **transaction-logs** configuration command as follows:

```
wae(config)# transaction-logs flow enable  
wae(config)# transaction-logs flow access-list 150
```

You can view the end of a transaction log file by using the **type-tail** command as follows:

Cisco_WAAS_Troubleshooting_Guide_for_Release_4.1.3_and_Later_--_Troubleshooting_the_HTTP_AO

```
wae# type-tail tfo_log_10.10.11.230_20090715_130000.txt
Wed Jul 15 13:37:00 2009 :1529 :10.10.10.10 :2004 :10.10.100.100 :80 :OT :END :EXTERNAL CLIENT : (H
Wed Jul 15 13:37:00 2009 :1529 :10.10.10.10 :1880 :10.10.100.100 :80 :SODRE :END :14357 :8406 :21
Wed Jul 15 13:38:19 2009 :1533 :10.10.10.10 :2008 :10.10.100.101 :135 :OT :START :EXTERNAL CLIENT
:Other :MS-EndPointMapper :F : (TFO) (TFO) (TFO) (TFO) (TFO) :<None> : (EPM) (EPM) (EPM) :<None> :<
Wed Jul 15 13:38:19 2009 :1534 :10.10.10.10 :2009 :10.10.100.101 :1025 :OT :START :EXTERNAL CLIENT
:uuide3514235-4b06-11d1-ab04-00c04fc2dcd2
```

To set up and enable debug logging of the HTTP AO, use the following commands.

NOTE: Debug logging is CPU intensive and can generate a large amount of output. Use it judiciously and sparingly in a production environment.

You can enable detailed logging to the disk:

```
WAE674 (config)# logging disk enable
WAE674 (config)# logging disk priority detail
```

You can enable debug logging for connections in the ACL:

```
WAE674# debug connection access-list 150
```

The options for HTTP AO debugging (on 4.2.1 and later) are as follows:

```
WAE674# debug accelerator http ?
all enable all HTTP accelerator debugs
bypass-list enable HTTP bypass-list debugs
cli enable HTTP CLI debugs
conditional-response enable HTTP metadatatcache conditional (304) response
debugs
connection enable HTTP connection debugs
dre-hints enable HTTP dre-hints debugs
metadatatcache enable HTTP metadatatcache debugs
prefetch enable HTTP prefetch debugs
redirect-response enable HTTP metadatatcache redirect (301) response
debugs
shell enable HTTP shell debugs
suppress-server-encoding enable HTTP suppress-server-encoding debugs
transaction enable HTTP transaction debugs
unauthorized-response enable HTTP auth-optimization debugs bugs
```

You can enable debug logging for HTTP connections and then display the end of the debug error log as follows:

```
WAE674# debug accelerator http connection
WAE674# type-tail errorlog/httpao-errorlog.current follow
```