



Akamai Edge Staging Network

User Guide

August 24, 2009

Akamai Technologies, Inc.

Akamai Customer Care: **1-877-425-2832** or, for routine requests, email **ccare@akamai.com**

Akamai EdgeControl, for customers and resellers: **<http://control.akamai.com>**

US Headquarters
8 Cambridge Center
Cambridge, MA 02142

Tel: 617.444.3000
Fax: 617.444.3001

US Toll free 877.4AKAMAI (877.425.2624)

For a list of offices around the world, see:
<http://www.akamai.com/html/about/locations.html>

Edge Staging Network User Guide

Copyright © 2007—2009 Akamai Technologies, Inc. All Rights Reserved.

Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai, the Akamai wave logo, and the names of Akamai services referenced herein are trademarks of Akamai Technologies, Inc. While every precaution has been taken in the preparation of this document, Akamai Technologies, Inc. assumes no responsibility for errors, omissions, or for damages resulting from the use of the information herein. The information in these documents is believed to be accurate as of the date of this publication but is subject to change without notice. The information in this document is subject to the confidentiality provisions of the Terms & Conditions governing your use of Akamai services.

Other trademarks contained herein are the property of their respective owners and are not used to imply endorsement of Akamai or its services.

Contents

WHAT YOU CAN AND CANNOT TEST ON ESN	6
USING ESN, STEP BY STEP	8
Maintaining a Permanent Test Environment on ESN	8
Optional: Limit Access to Your Permanent Staging Applications	8
Add Akamai Firewall Rules	8
Limit Access to Specific End User IPs	8
1. MODIFY THE CONFIGURATION FILE, DEPLOY THE CHANGES TO ESN	9
2. PURGE THE TEST CONTENT ON STAGING	9
Warning!	9
3. IDENTIFY STAGING IP ADDRESS AND CONFIGURE YOUR BROWSER	10
Automatic Identify-and-Edit with the Akamai Hosts Toggle Tool	10
Manually Identifying a Staging IP Address and Editing the Hosts File	12
Using nslookup at the Windows Command Prompt	12
Edit the Hosts File to Add the Staging Address	13
4. CREATE TEST REQUESTS AND VERIFY THE FUNCTIONALITY	14
Contacting Akamai for Help with Unresolved Problems	15
5. ACTIVATE THE SAME VERSION ON PRODUCTION	15
VALIDATING FUNCTIONALITY	16
Viewing HTTP Response Headers Using Akamai-Provided Utilities	16
Using EdgeSuite Booster—for Microsoft Internet Explorer (MSIE)	17
Using Live HTTP Headers—for Firefox	18
HTTP Response Headers to View	19
The X-Cache HTTP Response Header	21
Validating Site Functionality	21



Edge Staging Network User Guide

The Edge Staging Network (ESN) provides an environment to test your Akamai configurations without impact to production configurations. After testing the functionality on ESN, you can use the same configuration file in production.

ESN is a small network of Akamai edge servers built to simulate Akamai's production network to test most of your site or application functionality with current production-version configuration options and functions.

About this Document

This guide briefly describes the capabilities and limits of ESN, its setup and usage, and is intended for use by those responsible for testing and validating configurations for applications that will be using the Akamai production network.

Before you use this document, you should have read your product Implementation guides and the Edge Server Configuration Guide. You can contact the same Akamai representatives as you do today with questions or issues with your service on the ESN.

How it Works, In Brief

If you use services other than Object Caching with Secure Delivery, you use an object called a Host Header form of digital property in your configuration. This digital property, an Akamai identifier, is most often a full, customer facing host name for your site or application. When you set up to serve content through Akamai, the digital property is CNamed to an Akamai edge hostname, in effect redirecting traffic that would go to an origin to edge servers in the Akamai network.

For example, for a host, **example.com**, the digital property might be **www.example.com**, which might be CNamed to an edge hostname of **www.example.com.edgesuite.net**.

When you test on ESN, the testing host name, or “staging” hostname, is most often created by adding a “-staging” before the suffix of the edge hostname. For example, the production edge host, **www.example.com.edgesuite.net**, would correlate to a staging hostname, **www.example.com.edgesuite-staging.net**.

You modify your local testing computer to temporarily re-direct to the staging server in order to test configuration and functionality. In order to do this testing, you must have modified your edge server configuration and purged existing content.

Object Caching with Secure Delivery Works in a Different Way



Note: If you use Object Caching with Secure Delivery, you use a different form of digital property, called an ARL token, than the form described here. The ARL token and Secure Origin are described in the Object Caching with Secure Delivery Implementation Guide, and you use special procedures in ESN as described on page 6.

ESN Reporting and Billing

All reporting, monitoring, alerting and billing functions will treat Production and ESN traffic the same. Your reports and monthly invoice will reflect the combined traffic from both the production and Edge Staging Networks.

What You Can and Cannot Test on ESN

Most standard current-version production features can be tested on ESN.



Production-equivalent functionality *cannot* be assured for the following features:

- **akadns.net domains from Global Traffic Manager (GTM)**
GTM (sometimes called First Point) does not have a staging equivalent. Currently it is not possible to test configurations using GTM by default.
- **Edge Hostnames with hard coded targets**
Some *.edgesuite.net and *.edgekey.net domains have special mappings which prevents them from resolving to ESN IPs automatically. If you believe your configuration uses hard-coded targets, you can check by using **nslookup** as described on page 12. The staging IP will be the same as the production IP.
- **Two Tree configurations**
Some “advanced” configurations use this technique to add functionality.
- **SiteShield**
Customers using SiteShield must add the ESN CIDR blocks to their firewall configuration.

ESN is for Functional Testing—not for Load, Stress, or Performance Testing



The ESN is designed for functional testing only—it is never to be used for load, stress testing, or performance testing.

Corporate Network Restrictions

It is not possible to test configuration changes on the ESN in some corporate networks with proxy servers. In these situations, the corporate proxy server overrides the tester's browser configuration and prevents the request from going to the staging network. You should contact your network administrator and ask to bypass the proxy server or test from outside the corporate network.

Special Procedures for Object Caching with Secure Delivery

You can skip this section if you are not using Object Caching with Secure Delivery.

When using Object Caching with Secure Delivery, you use a different URL structure to deliver your content through Akamai. The structure looks like this:

```
https://a248.e.akamai.net/images.example.com/images/example.jpg
```

In this example, “a248.e.akamai.net” is the Akamai secure host name that directs the browser request to an Akamai server, and the rest of the URL (images.example.com/images/example.jpg), is the URI for the object the Akamai server will fetch. To test a configuration on ESN, follow these steps:

1. Run **dig** (UNIX) or **nslookup** (Windows) on **a248.e.akamai-staging.net**. (Note the “-staging” between **a.248.e.akamai**, and **.net**)

Here's an example running dig:

```
dig a248.e.akamai-staging.net.  
;; QUESTION SECTION:  
;a248.e.akamai-staging.net.    IN      A
```

```
;; ANSWER SECTION:
a248.e.akamai-staging.net. 20      IN      A      96.17.77.194
a248.e.akamai-staging.net. 20      IN      A      96.17.77.187
```

- Using the IP in the results of the **dig** or **nslookup**, you now follow the procedures under “Edit the Hosts File to Add the Staging Address” on page 13 to modify your Hosts file using the IP you obtained in this workaround.

Important: **a248.e.akamai.net** is the host name you enter into your Hosts file to associate with the IP you obtained with **dig** or **nslookup**.

China CDN—A Known Issue Requires Special Steps

You can skip reading section this if you are not using China CDN.

As explained in Step 3 in this document, configuring for ESN involves identifying an IP address for the DNS CName for the digital property you want to test. For China CDN applications, however, there is a known issue that requires using the workaround described here.



When you identify the DNS CName in order to locate the Staging IP as described in in this document, do not use the automated Hosts Toggle Tool and do not use the normal manual method described in Step 3 starting on page 10.

Instead of the manual method described on page 10, follow these steps:

- Run **dig** (UNIX) or **nslookup** (Windows) on your digital property as described under “Manually Identifying a Staging IP Address and Editing the Hosts File” on page 12. Here’s an example running **dig**:

```
dig www.example.com.edgekey.net
;; QUESTION SECTION:
;www.example.com.edgekey.net. IN      A

;; ANSWER SECTION:
www.example.com.edgekey.net. 21600 IN CNAME
www.example.com.edgekey.net.globalredir.akadns.net.
www.example.com.edgekey.net.globalredir.akadns.net. 3600 IN CNAME
e1848.b.akamaiedge.net.
e1848.b.akamaiedge.net. 20      IN      A      72.247.19.172
```

- If you used **dig**, take the last name in the list. If you used **nslookup**, take the name listed after “Name”. Using the above **dig** example, the name you want to use is **e1848.b.akamaiedge.net**.
- Add “-staging” before the prefix to get the staging edge hostname. For example, **e1848.b.akamaiedge-staging.net**.
- To obtain the staging IP, run **dig** or **nslookup** a second time on the staging host name. For example:

```
dig www.example.com.edgekey-staging.net
```

- Using the IP in the results of the **dig** or **nslookup**, you now follow the procedures under “Edit the Hosts File to Add the Staging Address” on page 13 to modify your Hosts file using the IP you obtained in this workaround.

Using ESN, Step by Step

A high-level overview of ESN setup and use includes the following steps, each of which is described in greater detail the remainder of the document.

- Step 1** Modify the configuration file and deploy the changes to ESN
- Step 2** Purge the test content on the staging networks.
- Step 3** Identify the staging IP address and configure Your Browser
- Step 4** Make a test request or requests against the staging network and verify the functionality.
- Step 5** Activate changes on production

Maintaining a Permanent Test Environment on ESN

The procedures in this document refer to your production configuration and digital property. Note that to more easily facilitate the testing process on an ongoing basis, some Akamai customers create a staging Digital Property and leave it CNAMED to the Staging Network.

To do this, simply add the staging digital property (e.g. akamaistaging-www.example.com) using the Configuration Manager and point the digital property to the staging edge hostname (e.g. www.example.com.edgsuite-staging.net). If necessary, contact your Akamai Representative for help.

Optional: Limit Access to Your Permanent Staging Applications

Consider the following ways to limit access to your Staging sites and applications.

Add Akamai Firewall Rules

If you have a more permanent staging setup, you'll probably have a dedicated origin staging-environment server and you may want to restrict access to Akamai ESN or Secure ESN servers. Go to **All Services --> Firewall Rules** to set IP restrictions.

You may also wish to subscribe firewall notifications to let you know of changes to Akamai edge server CIDR IP addresses so that you can modify your firewall rules. Click the **Firewall Rules Notification** link from the navigation menu or the **Subscribe** link from the Firewall Rules page.

Limit Access to Specific End User IPs

You can limit access to your Staging application to specific end user IPs with an option in the Configuration Manager when you set up your staging configuration. In the Configuration Manager **Optional Features** page, select the **Control Access by URL or IP** option, then specify the end-user IPs that will be allowed to access the site or application.

1. Modify the Configuration File, Deploy the Changes to ESN

There are several ways to have a configuration modified. If your Akamai representative makes the changes, they will activate the changes to the staging network and prepare it for testing.

If you are making the changes, you use the Configuration Manager to make whatever changes you need to make, and then you activate the new version of your configuration file *on the staging network*.

Note that Akamai also has a set of staging servers that are outside of both ESN and production. You might be asked to test on one of these additional staging servers.

2. Purge the Test Content on Staging

Removing the files you'll be testing if there are existing versions currently stored in staging network server caches is a best practice that will ensure that every step in the request process defined in the newly activated configuration file will be exercised during the test. You do remove the files using Akamai's Content Control Utility.

If you do not purge the objects, it's possible to test against a cached file and potentially miss a mistake in the configuration file.

Use the CCU (and not the ECCU)

Warning!



To purge files from staging only, use the original Content Control Utility (CCU) or CCUAPI (SOAP Web service), and not the Enhanced Content Control Utility (ECCU), because the latter does not allow for selectively removing files from staging. Specify which network to remove files from: since the default is Production, you need to specify Staging to purge staging caches only. Contact your Akamai representative with any questions on this step in the process.

3. Identify Staging IP Address and Configure Your Browser

If your application uses China CDN, see the issue and workaround on page 7. If you use Object Caching with Secure Delivery, see page 6.

This step involves “hard coding” an IP address in your “Hosts” file to point to the staging network—a practice commonly referred to as “spoofing”.

There are two ways to do this: using an Akamai utility, or manually.

Automatic Identify-and-Edit with the Akamai Hosts Toggle Tool

The first option involves using Akamai’s Hosts Toggle Tool, which is currently available for Windows only. This automatically identifies the best staging IP address of the Edge Server Network and configures your browser to use it for testing.

NOTE that this procedure amounts to overriding your computer’s DNS and it may not work in some corporate networks with proxy servers. Contact your network administrators to bypass the proxy server. Or you may want to test from a location outside of your company’s network.

(Windows only) To spoof the DNS from your computer using Akamai’s Hosts Toggle tool:

1. Download and install the EdgeSuite Booster from the EdgeControl Management Center.

The link is in on your product’s Tools page.

2. From your **Start -> Programs** menu, open the **EdgeSuite Booster** application group and run the **Hosts Toggle** application.

The application should look like this when you first start it.

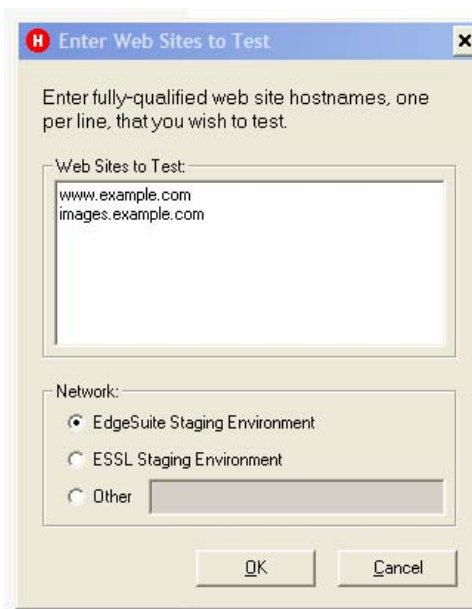


Figure 1. Akamai Hosts Toggle Tool Default View

3. Replace the **Web Sites to Test** examples with the digital property or properties you're going to test on ESN, and select the **Network**.

Do *not* leave the “Web Sites to Test” text block blank. There is a bug that may be triggered when that text box is left blank.

If you were given the IP of a specific test edge server:

Click the **Other** radio button and type the IP into the **Web Sites to Test** text box. For example:

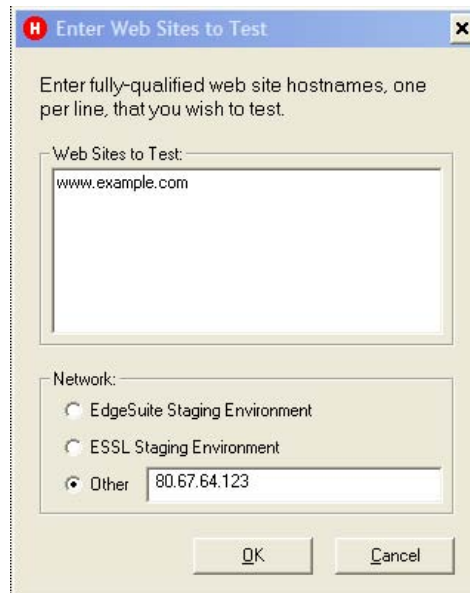


Figure 2. If You Already Have a Specific Test Server IP

4. Click **OK**.

If you see this message your browser is configured and you're ready to go.

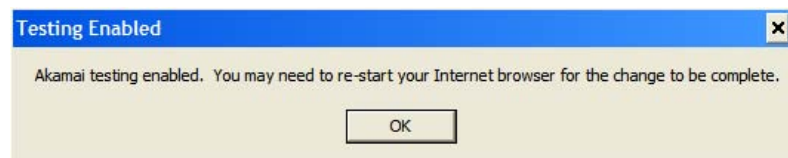


Figure 3. Successful completion of Spoofing

If You Get An Error Message...

If you get an error message instead of the Testing Enabled message shown in Figure 3, you should not proceed. Turn off Akamai testing and contact your Akamai Representative.

The error may mean that you cannot use the Hosts Toggle tool and you'll need to use the manual steps below.

Turning Akamai Testing Off and On

Windows System Tray Icon Displays Enabled State

- **Testing Enabled icon.** You will see a bright red icon in your system tray if any site is **enabled** for Akamai testing. This bright red icon tells you your browser is pointing to at least one Akamai test configuration.
Right click on the red icon to enable or disable testing.
- **Testing Disabled icon.**
A dark red icon shows in your Windows system tray when Akamai testing is **disabled**.

Manually Identifying a Staging IP Address and Editing the Hosts File

Before you begin:

- This procedure amounts to overriding your computer's DNS and it may not work in some corporate networks with proxy servers. Contact your network administrators to bypass the proxy server. Or you may want to test from a location outside of your company's network.
- A best practice is to *find the staging IP address before each round of testing, for the simple reason that Akamai IP addresses can and do change.*

If you don't or can't use the Hosts Toggle Tool, you can get the IP address by performing a DNS lookup, a task best illustrated by example.

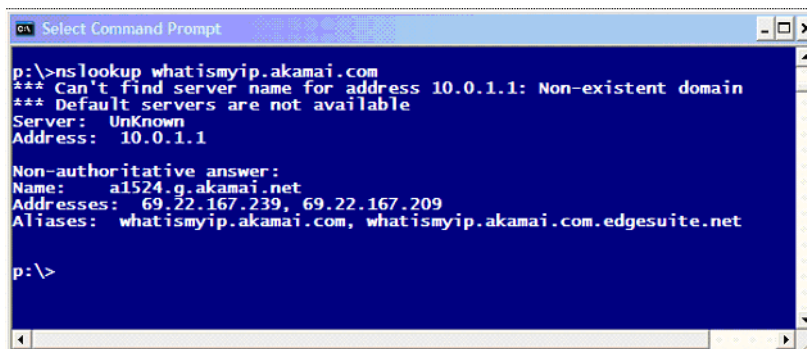
Assume your digital property is **whatismyip.akamai.com**.

This digital property is directed to the Akamai network via an *edge hostname* also known as a **DNS CNAME**. You can identify the DNS CNAME chain by running **nslookup** in the command window on Windows, or by running **dig** for a unix type system.

Using nslookup at the Windows Command Prompt

1. To go to the Windows command prompt, use **Start -> Command Prompt** on XP or **Start -> Accessories -> Command Prompt** on Windows 2000.
2. At the command prompt, type **nslookup** and the **name of the digital property**.

For example:



```

C:\>nslookup whatismyip.akamai.com
*** Can't find server name for address 10.0.1.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 10.0.1.1

Non-authoritative answer:
Name: a1524.g.akamai.net
Addresses: 69.22.167.239, 69.22.167.209
Aliases: whatismyip.akamai.com, whatismyip.akamai.com.edgesuite.net

C:\>
```

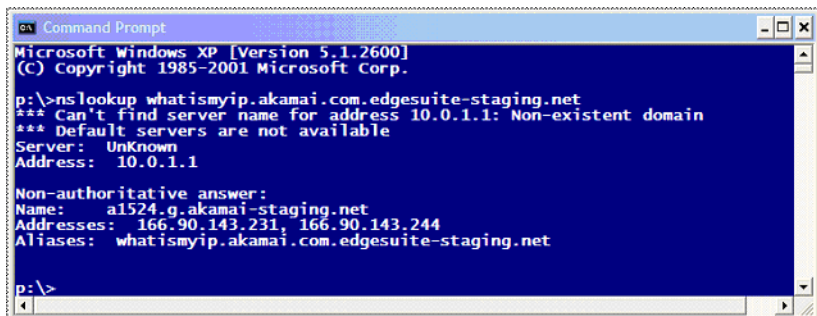
Figure 4. Using nslookup on the digital property.

Note that the Aliases: field shows **whatismyip.akamai.com.edgesuite.net**, which is the Akamai edge hostname.

3. To determine the staging IP address to use for your site replace the “edgesuite.net” with “.edgesuite-staging.net” in the edge hostname, and use nslookup a second time on the longer name.

Note: if you’re using an “edgekey.net” edge hostname—that is, an Akamai secure content name—replace “edgekey.net” with “edgekey-staging.net” in the edge hostname.

This example shows a regular, not a secure, name. That is, it shows **edgesuite-staging.net** and not **edgekey-staging.net**.



```

C:\>nslookup whatismyip.akamai.com.edgesuite-staging.net
*** Can't find server name for address 10.0.1.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 10.0.1.1

Non-authoritative answer:
Name:      a1524.g.akamai-staging.net
Addresses: 166.90.143.231 166.90.143.244
Aliases:   whatismyip.akamai.com.edgesuite-staging.net

C:\>
  
```

Figure 5. Using nslookup to find the ESN edge server IP address.

In this example, the IP address 166.90.143.231 is the Akamai ESN edge server address you’re looking for.

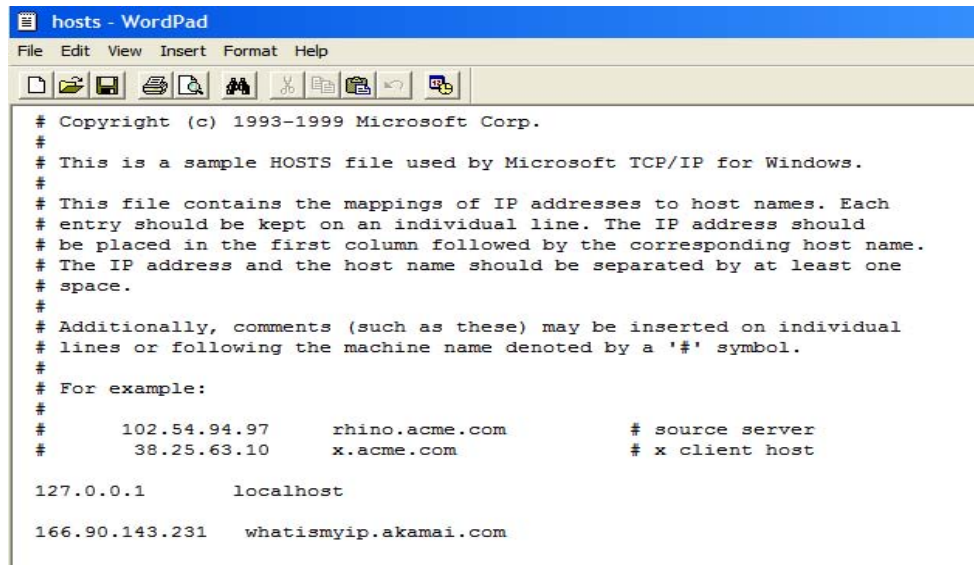
Edit the Hosts File to Add the Staging Address

1. Using Windows Explorer, locate the **hosts** file
The file, **hosts** (without any extension) is actually a simple text file, and is located in the /etc/ directory or C:\WINDOWS\system32\drivers\etc\ or other system-specific directory.
2. Add an entry, following the syntax documentation in comments in the hosts file or in your operating system documentation.

If you are using Windows Vista and you see an error at this step, it may be related to a known issue and a workaround.

See <http://support.microsoft.com/kb/923947>.

Here's an example of adding a last line to a hosts file using WordPad:

A screenshot of the WordPad application window titled "hosts - WordPad". The window shows the standard Windows menu bar (File, Edit, View, Insert, Format, Help) and a toolbar. The text content of the hosts file is displayed in a monospaced font. It includes copyright information for Microsoft Corp., instructions on how to use the file, and a list of IP-to-hostname mappings. The last line added is "166.90.143.231 whatismyip.akamai.com".

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host
#
127.0.0.1                localhost
#
166.90.143.231           whatismyip.akamai.com
```

Figure 6. A hosts file, with the last line added to point the digital property (whatismyip.akamai.com) to the staging IP (166.90.143.231).

4. Create Test Requests and Verify the Functionality

Now that your browser is configured to make requests directly from the staging network, the next step is to make test requests against the new configuration on the staging edge server and verify the functionality.

1. Close all browser windows and re-open the browser.
2. Create test requests. For example, for a URL you want to test, type a URL name into the browser address window and hit Enter.
3. View the HTTP response headers to verify your request is going to a staging server.

See “Validating Functionality” on page 16 for a description of how to do this. The presence of either of these response headers means your request made it to the staging network:

“X-Akamai-Staging: EdgeSuite” OR “X-Akamai-Staging: ESSL”

4. Verify the functionality.
See “HTTP Response Headers to View” on page 19 for additional information and instructions.
5. When you're done testing, remove the DNS override from your hosts file by undoing or commenting out the line you added, OR if you used the Hosts Toggle tool, disable it in the Windows system tray.

Contacting Akamai for Help with Unresolved Problems

If you have problems you cannot resolve in testing your Akamai configuration, you can contact Akamai Customer Care most expediently by opening a support request. On Akamai's EdgeControl Management Center, go to **Support --> Open/View Support Cases**.

Please include the following information in the ticket:

- If you were connected, the ESN IP.
- The URL involved if there was one.
- The request and response headers.
- The functionality tested with expected and actual behavior.

5. Activate the Same Version on Production

Once the new version of your configuration has been tested and validated on ESN, you can activate that same version on production network.

To do this, go to the **Configuration Manager -> Configuration History** page, select "Activate this version" and then select "Production."

It may be that you'll need to refresh the cached content on production—for example, if the old content is set in configuration to be served from cache for a longer time than you'd want. You can use either the Content Control Utility or the Enhanced Content Control Utility to manually refresh content. Under normal conditions, the best practice is to let content expire in caches so that new objects are fetched from the origins as needed, because that can provide the least spikes in traffic to the origin. Refreshing many objects at one time can result in heavy loads on the origin.

Validating Functionality

There are two types of validation you can perform using ESN:

- Validating Akamai configuration through viewing HTTP response headers
- Validating your site or application functionality

Viewing HTTP Response Headers Using Akamai-Provided Utilities

Akamai provides two HTTP response header viewers to help you when using commonly-used browsers. They are built for different browsers and they behave in slightly different ways.

- **EdgeSuite Booster for Microsoft Internet Explorer (MSIE)**

This provides for viewing response headers for the currently viewed page.

- **Live HTTP Headers for Firefox**

This provides for viewing response headers for pages that you view after you open the tool window.

These applications are included in the install package with the Hosts Toggle Tool discussed on page 10—where you'll find instructions on how and where to get, download, and install the utilities. Documentation accompanies these utilities, and those instructions are not duplicated here.

Using EdgeSuite Booster—for Microsoft Internet Explorer (MSIE)

See the included documentation accompanying EdgeSuite Booster for system requirements and installation instructions.



At this time, EdgeSuite Booster does not support secure HTTPS (e.g. <https://www.example.com>) requests.

When you are viewing a URL page, right click anywhere on a page and select the option to view the HTTP response headers called “Show Images”.

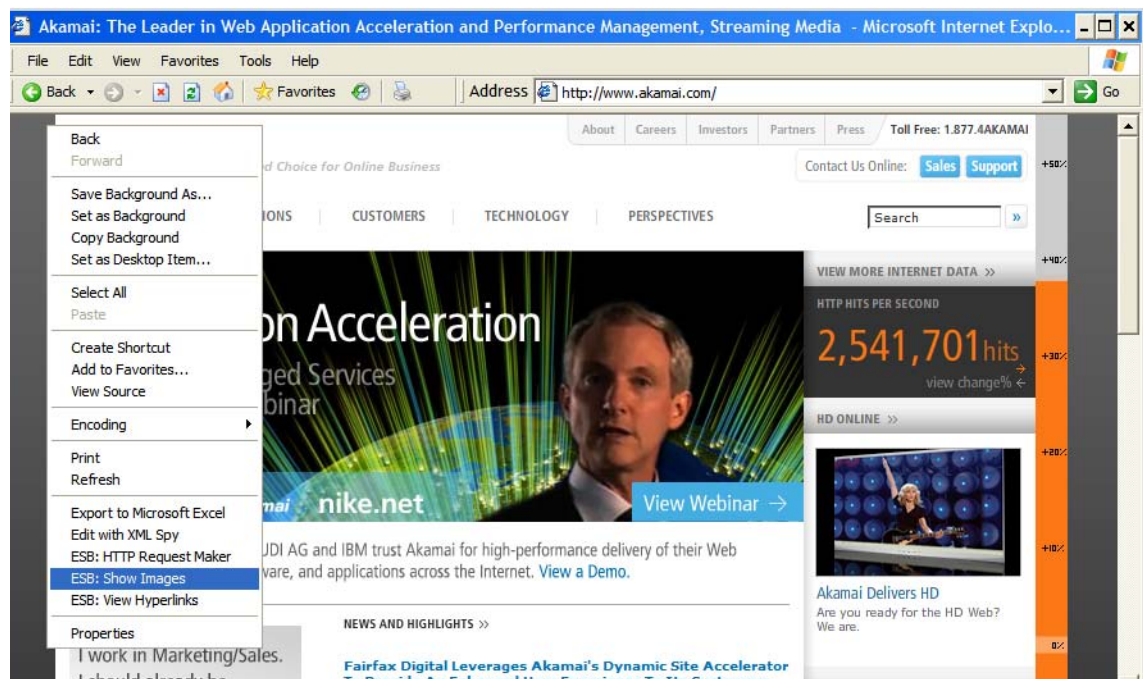


Figure 7. Using EdgeSuite Booster to view HTTP Response Headers

And an example of part the results (there was more information on the page than is useful to show in an image of the screen.):

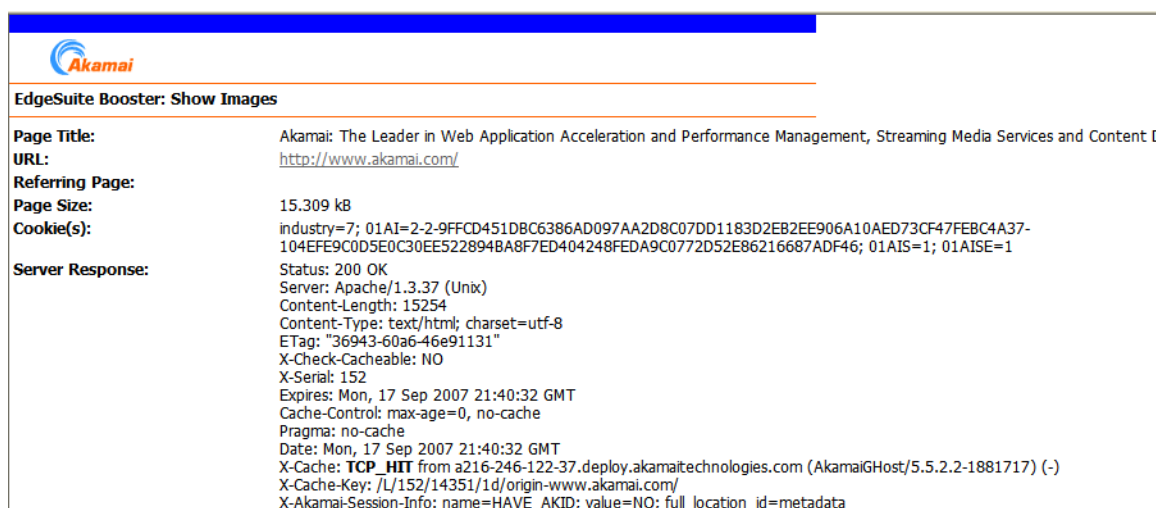


Figure 8. Example Results of “Show Images” in EdgeSuite Booster

Using Live HTTP Headers—for Firefox

See the included documentation accompanying Live HTTP Headers for system requirements and installation instructions.

1. Select Live HTTP Headers from the Firefox Tools menu to open the Live HTTP Headers window.

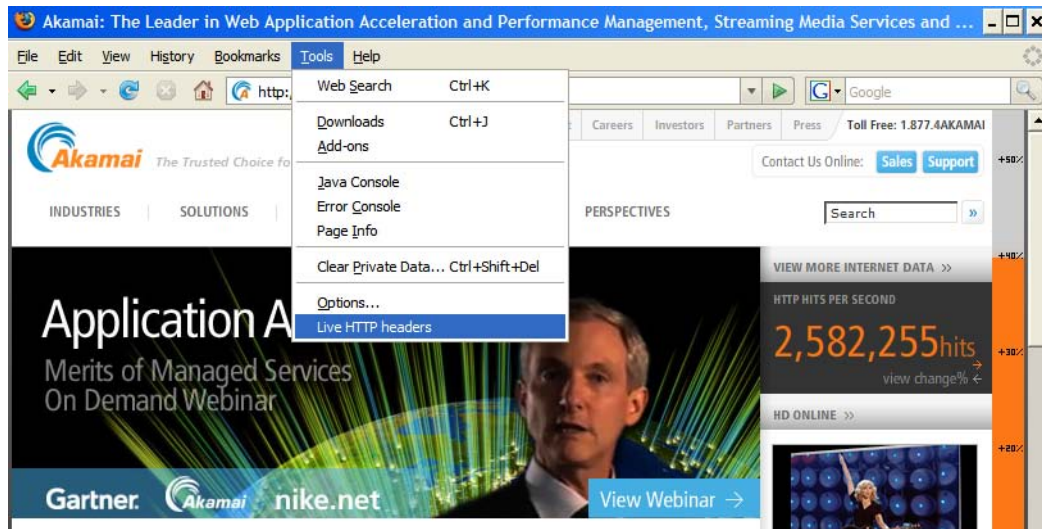


Figure 9. Using Live HTTP Headers in Firefox

2. With the Live HTTP Headers windows open, go to a URL you want to test. Response headers will be displayed in the Live Headers window. For example:

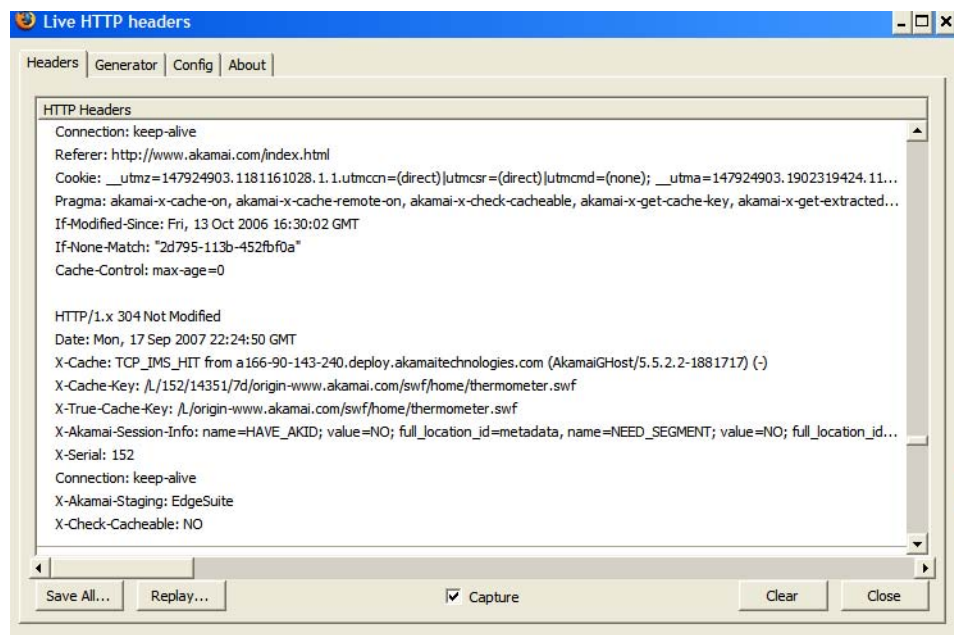


Figure 10. Results from using Live HTTP Headers in Firefox

HTTP Response Headers to View

After installing and running one of the utilities described in the previous section, you can review and examine the response headers. In the examples, the relevant or significant data or is **highlighted in bold red**.

This table shows examples of Akamai's X-Cache HTTP response header, which is described in more detail following the table.

DESCRIPTION	VERIFICATION
Verify cpcode	<p>The cpcode is the third component in the X-Cache-Key response header.</p> <p>Example: X-Cache-Key: /L/9/12345/1d/www.example.com/index.html</p>
Verify time-to-live (TTL)	<p>The TTL is the fourth component in the X-Cache-Key response header. Note that this only reflects TTL values set in the configuration file. If you are overriding the TTLs in your configuration using HTTP response headers, this will not reflect the overriding value.</p> <p>Example: X-Cache-Key: /L/9/12345/1d/www.example.com/index.html</p>
Verify cacheability of content	<p>Purge test content first, then make a first request for the test object. With no content in cache, a TCP_MISS is always returned on the first request, even if the content is cacheable. Verify a TCP_MISS in the X-Cache header. (Note that the X-Check-Cacheable: header is not authoritative for cacheability status.)</p> <p>Issue a second test request. If the content is non-cacheable, look for another TCP_MISS. If the content is cacheable, expect the second test request to return a TCP_HIT or TCP_MEM_HIT.</p> <p>Example: X-Cache: TCP_MISS from a80-67-64-110.deploy.akamai-technologies.com (AkamaiGHost/5.5.2.2-1881717) (S)</p>

DESCRIPTION	VERIFICATION
Verify proper refreshing of cached content	<p>Purge test content first, then make a first request for the test object. Verify a TCP_MISS in the X-Cache header.</p> <p>Issue a second request for the test object before the TTL passes. Verify a TCP_MEM_HIT.</p> <p>Issue another request for the test object after the length of time specified as the TTL passes from the time of the first request. Verify a TCP_REFRESH_HIT if the file hasn't changed and origin responded to the edge server's If-Modified-Since GET with a 304. Verify a TCP_REFRESH_MISS if the file has changed and origin responded to the edge server's If-Modified-Since GET with a 200.</p> <p>Note: if the origin does not serve content with a Last-Modified header, the edge server will always issue a full, non-conditional GET request to refresh cached content.</p> <p>Example: X-Cache: TCP_REFRESH_MISS from a80-67-64-110.deploy.akamai.com (AkamaiGHost/5.5.2.2-1881717) (S)</p>
Verify cache key	<p>The value of the X-True-Cache-Key header is the unique identifier that the edge servers use to identify an object in cache. Use this to check for caching the same content as separate cache entries because of inclusion of query strings in the cache key, or case-sensitivity.</p> <p>Example: X-True-Cache-Key: /L/www.example.com/index.html</p>
Confirm how a parent edge server served content	<p>This test is essentially the same as akamai-x-cache-on only that it applies to how the object was served from a parent edge server to a child edge server. It is only applicable for requests using Tiered Distribution and SureRoute.</p> <p>Example: X-Cache-Remote: TCP_REFRESH_MISS from a63-215-124-86 (AkamaiGHost/5.5.2.2-1881717) (S)</p> <p>Example: X-Cache-Remote: TCP_REFRESH_MISS from a63-215-124-86 (AkamaiGHost/5.5.2.2-1881717) (S)</p>
Confirm the version of the Akamai server software running on the edge server serving your content	<p>Example: X-Cache: TCP_REFRESH_MISS from a63-215-124-86 (AkamaiGHost/5.5.2.2-1881717) (S)</p>

The X-Cache HTTP Response Header

The X-Cache HTTP response header, shown in the examples in the preceding table, is returned from requests using **Pragma: akamai-x-cache-on:**. The possible responses and their meanings are as follows

Response	Meaning
TCP_HIT:	The object was fresh in cache and object from disk cache.
TCP_MISS:	The object was not in cache, server fetched object from origin.
TCP_REFRESH_HIT:	The object was stale in cache and we successfully refreshed with the origin on an If-Modified-Since request.
TCP_REFRESH_MISS:	Object was stale in cache and refresh obtained a new object from origin in response to our IF-Modified-Since request.
TCP_REFRESH_FAIL_HIT:	Object was stale in cache and we failed on refresh (couldn't reach origin) so we served the stale object.
TCP_IMS_HIT:	IF-Modified-Since request from client and object was fresh in cache and served.
TCP_NEGATIVE_HIT:	Object previously returned a "not found" (or any other negatively cacheable response) and that cached response was a hit for this new request.
TCP_MEM_HIT:	Object was on disk and in the memory cache. Server served it without hitting the disk.
TCP_DENIED:	Denied access to the client for whatever reason
TCP_COOKIE_DENY:	Denied access on cookie authentication (if centralized or decentralized authorization feature is being used in configuration)

Validating Site Functionality

In addition to testing Akamai configuration settings on ESN, it is strongly recommended that you perform regression testing on your site's functionality using your normal tests, noting that load, stress and performance testing are not done on ESN. For example, you might:

- Verify session management.
- Verify that personalized content for one logged in user is not improperly displayed to another.
- Verify shopping cart and checkout functions.

