



WHITE PAPER



# FIRST-PARTY COOKIES

SiteCatalyst Implementation

June 30, 2008

Version 2.0





# 1 Implementing SiteCatalyst with First-Party Cookies

SiteCatalyst typically uses third-party cookies to enhance the collection of data on your web sites. Even though third-party cookies have been in use for over a decade and there is no inherent harm in using them, the practice has recently come under scrutiny. Some anti-spyware applications have been designed to delete third-party cookies, including the Omniture cookie set at the 2o7.net domain. In addition, some visitors to your web site may have their browsers configured to reject third-party cookies altogether because of privacy concerns. Despite these circumstances, Omniture is committed to your online success and to ensuring that your organization has the most accurate web analytics data possible, and has thereby developed an easy way to help implement SiteCatalyst with first-party cookies instead of third-party cookies.



**NOTE:** Implementing SiteCatalyst with first-party cookies should have no negative impact on your data collection. As a matter of fact, your data will even be more accurate.

Specifically, this document offers the following information to help you during your SiteCatalyst implementation with first-party cookies:

- Technical requirements necessary to implement SiteCatalyst with first-party cookies
- Identification of individuals within your organization who can assist with the implementation process
- Important technical terms that can help you communicate confidently with these individuals and/or other groups working on the implementation



**NOTE:** If your site does not use SSL (i.e. has no pages served via HTTPS), the steps to implement follow an abbreviated process. Please see Appendix A for the for non-SSL site implementations.

## 1.1 Process Checklist

The following checklist outlines the steps needed to implement first-party cookies.

**Table 1-A: Steps to Implement with First-Party Cookies**

Step #	Process Description	Process Owner
<input type="checkbox"/> Step 1	Completion of first-party cookie request form	Customer
<input type="checkbox"/> Step 2	Creation & delivery of Certificate Signing Request (CSR)	Omniture
<input type="checkbox"/> Step 3	Creation of new CNAME records in DNS zone file	Customer
<input type="checkbox"/> Step 4	Purchase of SSL certificate	Customer
<input type="checkbox"/> Step 5	Delivery of SSL certificate	Customer
<input type="checkbox"/> Step 6	Installation of SSL certificate on Omniture data collection servers	Omniture
<input type="checkbox"/> Step 7	Delivery of new data collection code (i.e. new JS file)	Omniture
<input type="checkbox"/> Step 8	Installation of new data collection code (i.e. new JS file)	Customer

### 1.1.1 Step 1: Completion of First Party Cookie Request Form

All SSL certificates must be tied to an organization. In other words, your SSL certificate will be associated with your company. The certificate confirms, in technical terms, that cookies are being set by a legitimate, trusted organization. Therefore, a critical dependency in obtaining an SSL certificate is to communicate key pieces of information about your organization, namely the following

- Organization Name
- Country
- State
- Locality (typically city)
- Organization Unit Name (optional)
- Email Address (optional)

This form is typically completed by a member of your Network Operations team so that the values entered match the values used for your existing SSL certificates. If improper values are entered, the process may be delayed when trying to purchase a certificate.

After completing the request form, send it to any one of the following Omniture representatives.

- A ClientCare representative at [clientcare@omniture.com](mailto:clientcare@omniture.com)
- Your Omniture Account Manager
- Your Omniture Implementation Consultant

The representative who receives the request form will then initiate the Certificate Signing Request (CSR) process.

### 1.1.2 Step 2: Creation & Delivery of Certificate Signing Request (CSR)

A CSR is a text file generated by the web server on which the SSL certificate will be installed. A Certificate Authority (e.g. VeriSign, Thawte, etc.) uses the text file to create a "signed" certificate that you can send to Omniture, as described in Step 3.

The CSR creation process is completely managed by Omniture. Although the process can take place in tighter time periods, it usually requires three business days beginning on the day Omniture receives the First-Party Cookie Request Form.

### 1.1.3 Step 3: Creation of New CNAME Records in DNS Zone File

When implementing first-party cookies, you need to create an "alias" (called a CNAME record) that points to the Internet location that sets the SiteCatalyst cookie. Although you may be required to engage your Network Operations team, the CNAME record is a common configuration setting on any web server. Think of a CNAME record as a mechanism that behaves much like call forwarding. The CNAME record points to Omniture's data collection servers even though it resides on your DNS servers. The net result is twofold. First, your domain hosts the Omniture cookie (a true first-party cookie), and second, Omniture continues to collect the data as usual.



**TIP:** Although Step 3 is not a dependency for Step 4, it helps to engage your technical teams as early in the process as possible to ensure a timely implementation.

Two hostnames will be used in a first-party cookie implementation that supports SSL. For example, if visitors to your site point their browsers to [mywebsite.com](http://mywebsite.com), your new CNAME records might be [shop.mywebsite.com](http://shop.mywebsite.com) (to support non-secure pages) and [sshop.mywebsite.com](http://sshop.mywebsite.com) (to support secure pages). The mapping that defines the relationship between the cookie hostname and Omniture's data collection hostname will be provided in connection with your CSR (Step 2).

⊗ **WARNING!** Test the CNAME mappings before rolling the first-party cookie implementation live (i.e. before Step 8). For instructions on how to validate that the CNAME records are working properly, please refer to Appendix B.

### 1.1.4 Step 4: Purchase of SSL Certificate

Any reputable Certificate Authority can issue your SSL certificate. Prices and service levels can vary widely among vendors. Many of Omniture's customers use VeriSign or Thawte, but simply conducting a web search on "Certificate Authority" will yield many other options that might be suitable for your needs.



**NOTE:** Your organization may already have an SSL certificate in place. Regardless of whether you have an SSL certificate or not, you will need to purchase a separate certificate for the management of cookies over SSL.

### 1.1.5 Step 5: Delivery of SSL Certificate

After you have received the SSL certificate from the certifying authority, send it to one of the following Omniture representatives.

- A ClientCare representative at [clientcare@omniture.com](mailto:clientcare@omniture.com)
- Your Omniture Account Manager
- Your Omniture Implementation Consultant

### 1.1.6 Step 6: Installation of SSL Certificate on Omniture Data Collection Servers

Omniture manages the process for installing the SSL certificate. Omniture SSL certificates are installed during scheduled maintenance windows that occur on the second and fourth Thursday of every month. To have your certificate installed on a scheduled date, make sure it is submitted by the preceding Tuesday.

### 1.1.7 Step 7: Delivery of the Data Collection Code

Omniture will generate a new JavaScript file that you will need to place on your web server.

⊗ **WARNING!** Do not use the new JavaScript file until you have verified the following.

- Your SSL Certificate is in place on Omniture's data collection servers
- Your CNAME record is functioning properly (refer to Appendix B)

### 1.1.8 Step 8: Deploy the Data Collection Code

After you have verified that the CNAME mapping is functioning properly and the SSL certificate is in place on Omniture's Data Collection servers, you can place a JavaScript file that supports first-party cookies on your server.

### Important Considerations for Sites that Use Multiple JS Files for a Single Report Suite

⊗ **WARNING!** Any time you have more than one JavaScript file that is sending data to a single report suite, you must update all JavaScript files simultaneously.

## 1.2 Ongoing Maintenance

Since SSL certificates carry an expiration date, please provide Omniture with an SSL certificate 30 days in advance of the expiration in order to ensure that no interruption in service occurs. If the SSL certificate expires, your visitors will receive a warning in their browsers.

## 2 Appendices

### 2.1 Appendix A: Implementing Sites that Do Not Require SSL Support

The process for implementing SiteCatalyst with first-party cookies is much simpler for sites that do not contain secure pages.


Table 2-A: Steps for Implementing with First-Party Cookies

Step #	Process Description	Process Owner
<input type="checkbox"/> Step 1	Creation of new CNAME records in DNS zone file	Customer
<input type="checkbox"/> Step 2	Delivery of new data collection code (i.e. new JS file)	Omniture
<input type="checkbox"/> Step 3	Installation of new data collection code (i.e. new JS file)	Customer

#### 2.1.1 Step 1: Creation of New CNAME Records in DNS Zone File

When implementing SiteCatalyst with first-party cookies, you need to create an "alias" (called a CNAME record) that points to the Internet location that sets the SiteCatalyst cookie. Although you may be required to engage your Network Operations team, the CNAME record is a common configuration setting on any web server. Think of a CNAME record as a mechanism that behaves much like call forwarding. The CNAME record points to Omniture's data collection servers even though it resides on your DNS servers. The net result is twofold. First, your domain hosts the Omniture cookie (a true first-party cookie), and second, Omniture continues to collect the data as usual.

Unlike a first-party cookie implementation that supports SSL, non-SSL implementations only require one DNS entry. Also, you can pick the CNAME definition that creates the relationship between the new cookie hostname and Omniture's cookie hostname.

 **WARNING!: Test the CNAME mappings before rolling the first-party cookie implementation live (i.e. before Step 8). For instructions on how to validate that the CNAME records are working properly, please refer to Appendix B.**

#### 2.1.2 Step 2: Delivery of New Data Collection Code

After you have consulted Omniture about what your data collection domain will be, Omniture will generate a JavaScript file that you will need to place on your web server.

#### 2.1.3 Step 3: Deploy the new Data Collection Code

After you have verified that the CNAME mapping is functioning properly you can replace your former SiteCatalyst JavaScript file with the new file that supports first-party cookies.

#### Important Considerations for Sites that Use Multiple JS Files for a Single Report Suite

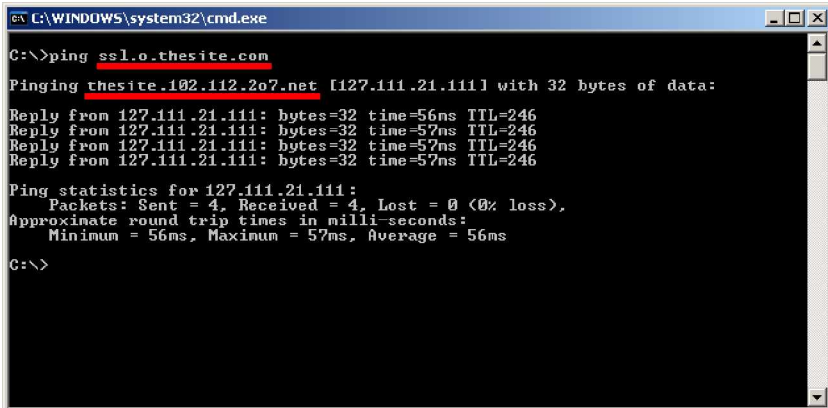
 **WARNING!: Any time you have more than one JavaScript file that is sending data to a single report suite, you must update all files simultaneously.**

## 2.2 Appendix B: Verifying that the CNAME Record is Functioning Properly

Table 2-B: Steps to Verify that the CNAME Record is Functioning Correctly

Follow these steps:

1. Open the Windows command prompt by clicking the Windows Start button, and then click **Run**.
2. Type "cmd" and click **OK**.
3. Type "ping " and the hostname of the new cookie domain. So, if your new cookie hostname were "ssl.o.thesite.com" you would type "ping ssl.o.thesite.com" in the command line.
4. The screen shot shows an example of a properly functioning CNAME record. The key indicator that it is functioning properly is the "Pinging thesite.102.112.2o7.net" (Omniture' s data collection domain).



```
C:\WINDOWS\system32\cmd.exe
C:\>ping ssl.o.thesite.com
Pinging thesite.102.112.2o7.net [127.111.21.111] with 32 bytes of data:
Reply from 127.111.21.111: bytes=32 time=56ms TTL=246
Reply from 127.111.21.111: bytes=32 time=57ms TTL=246
Reply from 127.111.21.111: bytes=32 time=57ms TTL=246
Reply from 127.111.21.111: bytes=32 time=57ms TTL=246

Ping statistics for 127.111.21.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 57ms, Average = 56ms

C:\>
```

If the CNAME has not been configured correctly, the response will show a message similar to the one shown here.

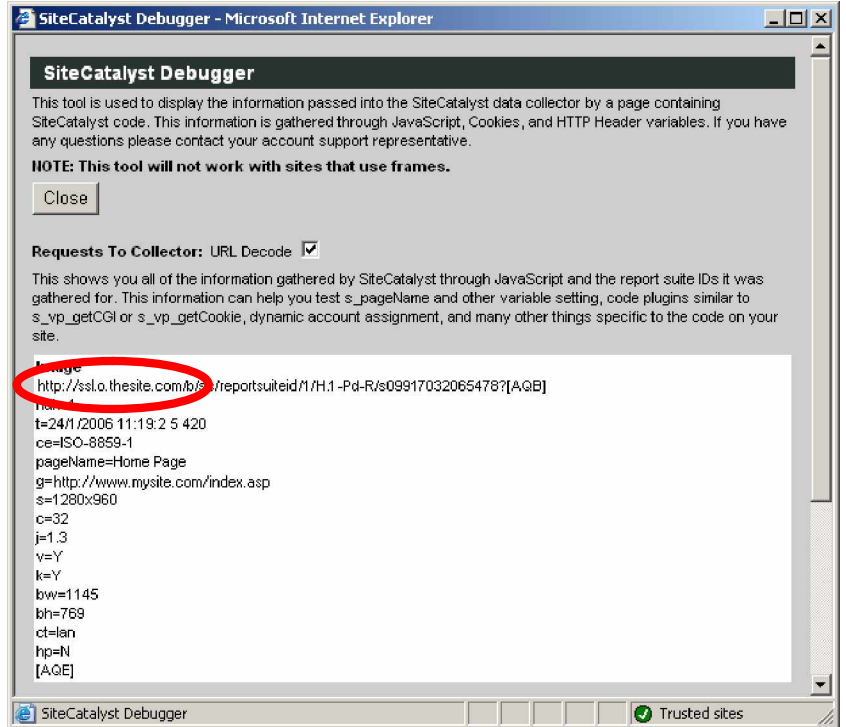


```
C:\WINDOWS\system32\cmd.exe
C:\>ping ssl.o.thesite.com
Ping request could not find host ssl.o.thesite.com. Please check the name and
try again.

C:\>_
```

**Follow these steps:**

- Once you have implemented the code, check the image request to ensure that data is being sent to the new cookie domain. Omniture's recommended best practice is to always check the code in your development and QA environments first.



Once the CNAME record is correctly implemented and the code sets cookies at the first-party cookie domain, check your cookies folder. For example, the “o.thesite.com” domain will save a cookie in the format of [username]@thesite[1].txt.



**NOTE:** If you are using Internet Explorer (with Windows 2000 or above), you can find this cookie at C:\Documents and Settings\[username]\Cookies on your local hard drive.

### 2.3 Appendix C: Friendly Third-Party Cookies for Multi-Suite Tagging Implementations

In certain situations, you may have a report suite that spans several of your domains. In this situation, Omniture recommends using a friendly third-party approach. The friendly third-party approach calls for a cookie that is set on a single "metrics collection subdomain" that has a friendly name.

Consider the scenario in which a hypothetical media conglomerate named NewsNow, Inc. owns ten different domains. To ensure accurate data collection, NewsNow would set its friendly third-party cookie to omn.newsnow.com. The benefit to this approach is that NewsNow could continue to have insight into the global view of all of their domains (e.g. de-duplicated visits, de-duplicated visitors, cross-domain campaign tracking, et cetera) by utilizing the cross-domain functionality that third-party cookies satisfy.

### 3 Important Glossary Terms

**Table 3-A: Glossary Terms**

SSL	<p>An agreed-upon format for exchanging encrypted data using two separate encryption keys – a public key (known to everyone) and a private key (known only to the recipient of the data). By convention, URLs that require an SSL connection start with <i>https</i> instead of <i>http</i>.</p>
SSL Certificate	<p>An attachment to an electronic message used for security purposes. The most common use of a digital certificate is listed below.</p> <ul style="list-style-type: none"><li>▪ To verify that a user sending a message is who he or she claims to be</li><li>▪ To provide the receiver with the means to encode a reply</li></ul> <p>An individual wishing to send an encrypted message applies for a digital certificate from a <i>Certificate Authority (CA)</i>. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.</p> <p>The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA, and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.</p>
DNS Entry	<p>A web server configuration setting that maps IP addresses to a domain names. A CNAME is an example of a DNS Entry.</p>
CNAME	<p>A computer hosting a web site must have an IP address in order to be connected to the World Wide Web. The DNS resolves the computer's domain name to its IP address, but sometimes more than one domain name resolves to the same IP address - this is where the CNAME is useful. A machine can have an unlimited number of CNAME aliases, but a separate CNAME record must be in the database for each alias.</p>
Certificate Signing Request (CSR)	<p>A CSR is a text file generated by the web server on which the SSL certificate will be installed. A Certificate Authority uses this text file to create a "signed" SSL certificate.</p>



**CALL 1.877.722.7088**  
**1.801.722.0139**

[www.omniture.com](http://www.omniture.com)  
[info@omniture.com](mailto:info@omniture.com)

550 East Timpanogos Circle  
Orem, Utah 84097

