Adobe® Marketing Cloud

First-Party Cookies

Contents

About First-Party Cookies

Analytics uses cookies to provide information on variables and components that do not persist between image requests and browser sessions. These harmless cookies originate from a domain hosted by Adobe, known as third-party cookies.

Many browsers and anti-spyware applications are designed to reject and delete third-party cookies, including those used in Analytics data collection. In order to circumvent tracking limitations imposed by browsers and programs, you can implement first-party cookies.

Two options are available to implement first party cookies

- The Marketing Cloud Visitor ID Service. The Visitor ID Service can set the cookie in the first-party context using JavaScript.
- DNS entries on your companies DNS server.

If your site has secure pages using the `https://` protocol and you are not using the Marketing Cloud Visitor ID service, you can work with Adobe to obtain an SSL certificate in order to implement first-party cookies

The SSL certificate issuance process can often be confusing and time consuming. As a result, Adobe established a partnership with DigiCert, an industry leading Certificate Authority (CA), and developed an integrated process by which the purchase and management of these certificates is automated.

With your permission, we will work with our CA to issue, deploy, and manage a new SHA-2 SSL certificate for you. Adobe will continue to manage this certificate and ensure that an unexpected expiration, revocation, or security concern, does do not threaten the availability of your organizations secure collection.

Important: *The Adobe Managed Certificate Program is the recommended process for implementing first-party cookies.*

Documentation Update History

Date	Description
May 22, 2015	Added *Adobe Managed Certificate Program*. Complete rewrite of this guide.
November 13, 2012	*South America Data Center Online* We now require that SSL certificates be licensed for installation on up to 10 servers.
May 9, 2012	• Corrected the `s.visitorMigrationServer` and `s.visitorMigrationServerSecure` examples. See *Update implementation code*. • Added a note that SSL certificates purchased from a CA should be licensed for installation on up to 9 servers.
July 12, 2012	• Added a link to download the First-Party Cookie Request form. See *Legacy - Provide Adobe with an SSL certificate*.

Adobe Managed Certificate Program

The recommended process for implementing a new first-party SSL certificate for first-party cookies.

The Adobe Managed Certificate program lets you implement a new first-party SSL certificate for first-party cookies at no additional cost. If you currently have your own Customer Managed SSL certificate, speak with Adobe Customer Care about migrating to the Adobe Managed Certificate Program.

Implementation Steps

How to implement a new first-party SSL certificate for first-party cookies:

1. Fill out the *request form* and open a ticket with Customer Care requesting to set up first-party cookies on the Adobe Managed program.

   Each field is described within the document with examples.

2. Create CNAME records.

   Upon receiving the ticket, a FPSSL specialist should provide you with a pair of CNAME records. These records must be configured on your company's DNS server before Adobe can purchase the certificate on your behalf. The CNAMES will be similar to the following.

Secure	For example, the hostname: `smetrics.example.com` points to: `example.com.ssl.d1.omtrdc.net`.
Non-secure	For example, the hostname: `metrics.example.com` points to: `example.com.d1.omtrdc.net`.

   See *Create CNAME Records* for more information.

3. When these CNAMES are in place, Adobe will work with DigiCert to purchase and install a certificate on Adobe's production servers.

   If you have an existing implementation, you should consider *Visitor Migration* to maintain your existing visitors.

   After the certificate has been pushed live to Adobe’s production environment, you will be able to update your tracking server variables to the new hostnames. Meaning, if the site is not secure (https), update the *s.trackingServer*. If the site is secure (https), update both *s.trackingServer* and *s.trackingServerSecure* variables.

4. *Ping the hostname*.
5. *Update implementation code*.

Maintenance and Renewals

SSL certificates expire each year, meaning Adobe must purchase a new certificate for each implementation on a yearly basis. All supported users within your organization will receive an email notification each time an implementation is close to expiration. For Adobe to renew your hostname, one supported user will must reply to the email from Adobe and indicate that you plan to continue using the expiring hostname for data collection. At that point, Adobe automatically purchases and installs a new certificate.

Frequently Asked Questions

Is this process secure?

Yes, the Adobe Managed program is more secure than our legacy method as no certificate or private key changes hands outside of Adobe and the issuing certificate authority.

How can Adobe purchase a certificate for our domain?

The certificate can only be purchased when you have pointed the specified hostname (for example, `smetrics.example.com`) to an Adobe owned hostname. This is essentially delegating this hostname to Adobe and allows Adobe to purchase the certificate on your behalf.

Can I request the certificate be revoked?

Yes, as the owner of the domain, you are entitled to request we have the certificate revoked. You will only need to open a ticket with Customer Care to have this completed.

Will this certificate be using SHA-2 encryption?

Yes, Adobe will work with DigiCert to issue a SHA-2 certificate.

Does this have any additional cost?

No, Adobe is offering this service to all current Analytics customers at no additional cost.

Create CNAME Records

Create CNAME records to point to Analytics collection servers.

Your organization's network operations team should configure your DNS servers by creating new CNAME record(s). Each hostname forwards data to Adobe's data collection servers.

The FPC specialist provides you with the configured hostnames and what CNAMEs they are to be pointed to. For example:

- **SSL Hostname:**`smetrics.mysite.com`
- **SSL CNAME:**`mysite.com.ssl.d1.sc.omtrdc.net`
- **Non-SSL Hostname:**`metrics.mysite.com`
- **Non-SSL CNAME:**`mysite.com.d1.sc.omtrdc.net`

As long as implementation code is not altered, this step will not affect data collection and can be done at any time *after updating implementation code*.

Note: *The Marketing Cloud Visitor ID service provides an alternative to configuring a CNAME to enable first-party cookies.*

Ping the hostname

Ping the hostname to ensure correct forwarding. All hostnames must respond to a ping to prevent data loss.

After CNAME records are properly configured, and Adobe has confirmed installation of the certificate, open a *command prompt* and ping your hostname(s). Using `mysite.com` as an example:`ping metrics.mysite.com`

```
ping metrics.mysite.com
```

If everything is successfully set up, it will return something similar to the following:

```
Pinging mysite.com.112.2o7.net [66.235.132.232] with 32 bytes of data:
Reply from 66.235.132.232: bytes=32 time=19ms TTL=246
Reply from 66.235.132.232: bytes=32 time=19ms TTL=246
Reply from 66.235.132.232: bytes=32 time=19ms TTL=246
Reply from 66.235.132.232: bytes=32 time=19ms TTL=246

Ping statistics for 66.235.132.232: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds: Minimum = 19ms, Maximum = 19ms, Average = 19ms
```

If the CNAME records are not correctly set up or not active, it will return the following

```
Ping request could not find the host. Please check the name and try again.
```

Note: *If you are using `https:// protocol`, ping will only respond after the upload date specified by the FPC specialist. An addition, be sure to ping the secure hostname and non-secure hostname to ensure that both are working correctly before updating your implementation.*

Update implementation code

Edit code on your site to utilize first-party cookies.

Prerequisites

- Request an SSL certificate, as described in *Implementation Steps* for the Adobe Managed Certificate Program.
- *Create CNAME records*.
- *Ping the hostname*.

After you have verified your hostname(s) are responding and forwarding to Adobe data collection servers, you can alter your implementation to point to your own data collection hostnames.

To update implementation code

1. Open your core JavaScript file (`s_code.js/AppMeasurement.js`).
2. If you want to update your code version, replace your entire `s_code.js/AppMeasurement.js` file with the newer version and replace any plugins or customizations (if any). Proceed to step 5.

   Or

   If you want to update the code only pertinent to first-party cookies, locate the *s.trackingServer* and *s.trackingServerSecure* (if using SSL) variables, and point them to your new data collection hostnames. Using `mysite.com` as an example:

   ```
   s.trackingServer = "metrics.mysite.com"

   s.trackingServerSecure = "smetrics.mysite.com"
   ```

3. Upload the updated core JavaScript file to your site.
4. If you are moving to first-party cookies from a long-standing implementation, or changing to a different first-party collection hostname, we recommend migrating visitors from the previous domain to the new domain.

   See *Visitor Migration* in the *Analytics Implementation Guide*.

After you have uploaded the JavaScript file, everything is configured for first-party cookie data collection. It is recommended to monitor Analytics reporting for the next several hours to ensure that data collection continues as

normal. If it does not, verify that all above steps have been completed and have one of your organization's supported users contact Customer Care.

Legacy - Provide Adobe with an SSL certificate

Determine if your site uses https:// protocol. If it does, requesting a CSR and purchasing an SSL certificate is required.

Note: *An SSL certificate is not required if you do not have any secure pages or content. This entire step may be skipped if you use only http:// protocol on your site.*

First-Party Cookie Request

Note: *Adobe encourages you, if possible, to use the Adobe Managed Certificate Program rather than providing Adobe with the certificate.*

In order to provide Adobe with the correct SSL Certificate:

- **Complete the First-Party Cookie Request Form:** Download the *First-Party Cookie Request Form*. Each field is described within the document with examples.
- **Provide the Completed Form to Adobe**: After the request form is complete, you can contact your Account Manager, your Implementation Consultant, or have one of your organization's supported users contact ClientCare to provide them with this information. It will be passed on to the FPC specialist.
- **Receive the CSR From the FPC Specialist:** Within approximately two business days of successfully receiving the request form, the FPC specialist will provide you with a CSR you can use to purchase an SSL certificate. These CSRs will look something like the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzTCCJTYCAQAwgYwxCzAJBgNVBAYLAmdiMQ8wDQYDVQQIExZMb25kb24xAzAN
BgNZBAcTBkxvbmRvgjEZMBcGA1UvChMQU3BhY2VTdXJmZXIgTHRkLjEZMBcGA2UE
AxMQd3d3LnNwXWNlcmVnLmNvbTElMbMGCSqGSIb3DQEJAR2Wd2VibWFzdGVyQHNb
YWNlc6VnLmNvbTCBnzAnBgkqhkiG8w0BAQEFAAOBjQAwgXkCgYEAywfuXnd328ot
iAcX4RHFc509ImCTagMaNkiQ4xyijbPYP7H0GQ5iXqvojSIcbU0VhExqwqyqjNPm
7ZpON3lXktIcKAwPFvmqKkHuqTa8KMnZTSY1P7QILYHFd2Sd1l1nrCrWv8HWq+qM
RxVTlviBaLAHQxnz28qkKYN09K0fw5cCAwEAAaWRMA0GCSqGSIb3DHEBBAUVA4GB
AFMgp2KkHQXMC1JbZf3AkIz7mrl4X21cRusTfd8bc3RuMZexGy76jMGFyPCVM69R
FvpfiiC5h28HrHube7pbPFpdUSj2cR4OZCAg5uqzN/ESwl4CtLzej7pWohPpc/kv
hiJneGOxINKd39kCuzIS62rvb2ihJth7jcmopezmrsjQ
-----END CERTIFICATE REQUEST-----
```

- **Purchase an SSL Certificate:** Using the CSR provided by the FPC specialist, purchase a certificate. This can be obtained from any certificate authority of your choice and **must support installation on up to 10 servers.**. See *SSL Certificate Licensing*.

Note: *Your organization may already have an SSL certificate in place for conversion transactions between you and your customers. Regardless of whether you have an SSL certificate for conversion or not, you will want to purchase a separate certificate for the management of cookies over SSL.*

- **Provide the SSL Certificate to the FPC Specialist:** Using the same CRM incident as the CSR request, reply to the FPC specialist with the certificate generated from the CSR. Certificates will follow a similar format:

```
-----BEGIN CERTIFICATE-----
MIIDRDGCAq2gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBqTELMAkGA1UEBhMCWFkx
FTATBgNVBAgTDFNuYWtlIERlc2VydDETMBEGA1UEBxMKU25ha2UgVG93bjEXMBUG
A1UEChMOU25ha2UgT2lsLCBMdGQxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEF1dGhv
cml0eTEVMBMGA1UEAxMMU25ha2UgT2lsIENBKR4wHAYJKoZIhvcNAQkBFg9jYUBz
bmFrZW9paC5kb20wHhcNOTkxMDIxMTgyMTQ2WhcNMDExMDIwMTgyMTQ2WjCBqTEL
MAkGA1UEBhMCWFkxFTATBgNVBAgTDFNuYWtlIERlc2KydDETMBEGA1UEBxMKU25h
```

```
a2IgVG93bjEXMBUGA1UEChM2U25ha2UgT2lsLCBMdGQxHjAcBgNV7AsTFUNlcnRp
ZmljYXRlIEF1dGhvc9l0eTEVMBMGA1UEAxMMU25ha2UgT2lsIENBMR4wHAYJKoZI
hvcNAQkBFg9jYUBzbmFrZW9pbC5kb20wgZ8wDQYJKoZIhvcNKQEBBQADgY0AMIGJ
AoGBAQiTGAmWoiB2Qx3SbwFXwjbqU9ZwnMBE5Er1h1kNh487D782I8m5T/CzxmsH
evK3heBKTEno+jB0y5p4+QShxryaMUUbRoOGfrlrVwc/dbwJQz7UNyqDlWnvnW4p
TfdVd+86lCpYFB23Z7bmpUV1Xy6VFKBaYzIhzITaux1vvEPLAgMBAAGkejB4MBoG
A1UdEQQTMBGBD2NhQHNuYWtlb2lsLmRvbTAPBgNVHRMECDAGAQH/AgEAMDYGCWCG
SAGG+EIRDQQpFidtb2Rfc3NsIGdlbmVyYXRlZGBjdXN0b20gQ0EgY2VydklmaWNh
dGUwrQYJYIZIAYb4QgEBBAQDAgIEMa0GCSqGSIb3DQEBBAUAN4GBAImhzPY8PBRt
PQ1AQBAmHIBRcb69iTbFC+dghmVJQ3F549rZapY420kQDKQ6a3ybPFmxJ/Rf2rgY
FuAyo+B8EEVX0lU8VUSEhYeedODnQ3skwcT02g4b33GfzH7ED2N9kaa6U60UUrcE
KXJgz7tmAQHnTc9K1g2qIbpIjnr3FrjJ
-----END CERTIFICATE-----
```

After the FPC specialist has replied with a confirmation the certificate is valid, he or she will provide a date in which this certificate will be uploaded. Step 2, *Create CNAME Records*, can now be executed at any time. However, Step 3, *Alter Implementation*, must be done after the upload date.

SSL Certificate Licensing

Your SSL certificate licenses must support installation on up to 10 servers.

These certificates are installed on load balancers worldwide. As Adobe brings additional Data Collection Centers online, SSL certificate needs change. How this affects your certificate licensing needs over time depends on the type of certificate license you own:

- **Server-Based Licenses:** License requirements for **RDC** deployments grow over time.
- **Volume-Based Licenses:** License requirements are not affected by infrastructure changes, but only as your traffic volume changes over time.
- **Unlimited Licenses:** License requirements should remain relatively stable over time.

It is your sole responsibility to purchase and maintain these SSL certificates. It is also your responsibility to check the certificate provider's contract to confirm that SSL certificates can be installed in multiple data centers.

Contact and Legal Information

Information to help you contact Adobe and to understand the legal issues concerning your use of this product and documentation.

Help & Technical Support

The Adobe Marketing Cloud Customer Care team is here to assist you and provides a number of mechanisms by which they can be engaged:

- *Check the Marketing Cloud help pages for advice, tips, and FAQs*
- *Ask us a quick question on Twitter @AdobeMktgCare*
- *Log an incident in our customer portal*
- *Contact the Customer Care team directly*
- *Check availability and status of Marketing Cloud Solutions*

Service, Capability & Billing

Dependent on your solution configuration, some options described in this documentation might not be available to you. As each account is unique, please refer to your contract for pricing, due dates, terms, and conditions. If you would like to add to or otherwise change your service level, or if you have questions regarding your current service, please contact your Account Manager.

Feedback

We welcome any suggestions or feedback regarding this solution. Enhancement ideas and suggestions for Adobe Analytics *can be added to our Customer Idea Exchange*.

Legal