Controlling Access to Adobe Creative Cloud Services

INTRODUCTION

This document is written for Adobe® customers who for reasons of security or network access cost may wish to restrict access to Creative Cloud™ services by their employees or other personnel. It explains the different types of Adobe Creative Cloud services, the various methods that customers can use to restrict access to those services, and the pros and cons of the different methods.

SYNOPSIS

Four types of Adobe Creative Cloud services are defined: deployment, licensing, core, and auxiliary. All of these service types can be accessed from various types of clients: Adobe applications, non-Adobe applications and plug-ins, and web browsers. Three methods of blocking access to these services are discussed: configuring Adobe user accounts to disallow access to a service, preventing access to a service at the customer's firewall, and configuring applications or plug-ins so that they do not attempt to access a service. Also discussed are methods of restricting access to Creative Cloud desktop applications in online situations and of allowing access to the same applications in offline situations.

Adobe Systems Incorporated
345 Park Avenue
San Jose CA 95110-2704
USA
www.adobe.com

Adobe, the Adobe logo, Photoshop, and Creative Cloud are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2013 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

May 2013

TYPES OF CREATIVE CLOUD SERVICES

Deployment services download Adobe applications and updates to a user's system and then install them. In order to make changes to a user's system, some of these services must run locally rather than on Adobe servers. For example, Adobe Application Manager, which most users think of as a desktop application, is considered by Adobe a deployment service that runs locally. Local deployment services depend on Adobe-hosted deployment services for catalogs of available applications and updates, downloads, and validation of local machine configurations.

The deployment services are visible to users in activities such as browsing lists of available applications and services, downloading and installing applications, and updating installed applications.

NOTE: In the past, the local deployment services accepted physical media rather than requiring contact with Adobe-hosted deployment services. This is no longer true. Customers cannot deploy without some contact with Adobe-hosted deployment services. Customers who have low-bandwidth connections can make special arrangements with Adobe to receive downloads on media rather than online. However, network connectivity to the deployment services is still required in order to prepare this media-based download for use in deployment.

Licensing services authenticate users and authorize them to access Creative Cloud services and desktop applications. Authentication means verifying the user's identity and connecting that identity with the user's Creative Cloud membership. Authorization includes checking a user's membership to determine its overall status, determining which applications and services the user's membership allows the user to access, and discovering any restrictions or special permissions granted to the user.

Most of the licensing services run on Adobe servers. A few of them, however, run locally. For example, Adobe Application Manager, which most users think of as a desktop application, is considered by Adobe a licensing service that runs locally. (It is also a deployment service, as explained above.) The local licensing services depend on Adobe-hosted licensing services for all of their functions.

The licensing services are visible to users in activities such as logging in, accepting terms of use, and accepting end-user license agreements.

NOTE: For backward compatibility and offline use, the licensing services also handle authorization of applications licensed with serial numbers rather than by membership.

Core services provide the value of the Creative Cloud. They provide document editing, web site hosting, color and font management, etc. From the Creative Cloud perspective, the desktop applications are also core services; they are differentiated from other core services by the fact that they run on the user's local system rather than on an Adobe server.

All Creative Cloud core services (including the desktop applications) require a user to have a membership that authorizes the use of the service and specifies the level of functionality the service can provide, for example, free versus paid levels. Since a user's identity and membership status are determined by the licensing services, all core services (including the desktop applications) require access to the licensing services in order to work.

Some core services make use of other core services. For example, the Photoshop® application, while mostly self contained, may require access to other core services to provide some of its functionality, such as posting a document to Creative Cloud storage or performing a special image processing operation that cannot be done locally.

NOTE: All core services require authentication and authorization, whether they are paid or free.

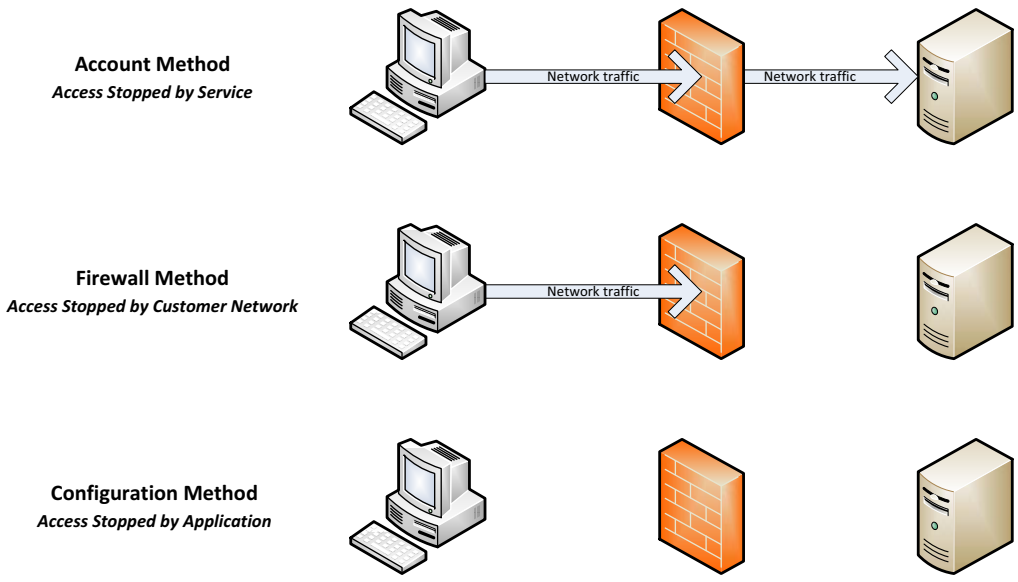
Auxiliary services provide non-essential, optional information or guidance that is not part of the core functionality of the Creative Cloud. These services provide things such as marketing information, educational or supplementary material, tutorials, templates, and online help.

Auxiliary services may ask users about their membership in order to provide more personalized information targeted for each user. However, unlike the core services, auxiliary services do not require authentication and authorization to function.

CONTROLLING ACCESS TO ADOBE-HOSTED SERVICES

CAUTION: Restricting access to deployment and licensing services may make it impossible for customers to install or use Creative Cloud desktop applications. Restricting access to core hosted services may make it impossible for users to accomplish tasks in desktop applications. Thus, customers are advised to proceed with caution when restricting access to services.

There are three methods which customers can use to control access to services; each method stops access at a different point, as shown in the picture below. The *account method* stops access at the service itself; the *firewall method* stops access at the customer's firewall; the *configuration method* stops access from within desktop applications on a user's system. These control methods are discussed in more detail in the next three sections.



There are a number of characteristics that are used to describe these methods. A given method may or may not have a particular characteristic. These characteristics are described in the following table.

Characteristic	Description
Service-specific	A control method is service-specific if it enables customers to selectively block certain individual services or groups of services while not blocking others.
User-specific	A control method is user-specific if it enables customers to block access to a service for some users while allowing access for others.
Machine-specific	A control method is machine-specific if it blocks access to a service on some machines and not others.
Client-specific	The three main types of clients that generate service access requests are Adobe desktop applications, web browsers, and non-Adobe plug-ins or applications. A control method is client-specific if it enables customers to selectively block service access requests from a particular type of client while not blocking access from other types of client.
Location-specific	A control method is location-specific if it blocks service access for a given user from some network locations but not from other network locations, even if that access is attempted from the same machine. For example, a control method that blocks access from a person's laptop at work but does not block access from the same laptop when it is used in the person's home is a location-specific blocking method.
Specialized	A control method is specialized if it is expected to be implemented only by technical personnel with skills and technical access beyond what a normal user or admin has.

These characteristics are discussed for each of the three control methods in the next three sections. A summary table on page 7 shows the three methods and which characteristics each method has.

THE ACCOUNT METHOD

The account method is not yet supported by Adobe. This section describes how it will operate when it becomes available.

The account method enables admins to control service access to particular services for users on an individual basis. This control is accomplished by setting parameters in a user's account so as to specify which level of access (for example, paid, free, or none) is allowed to which services for that user.

Only services that rely on the licensing services to verify a user's identity and account status can be restricted using this method. This includes all of the core services, most of the deployment services, and a few of the auxiliary services.

The account method is service-specific and user-specific.

The account method is not machine-specific, client-specific, or location-specific and is not specialized, although it does require an admin to configure the users' accounts.

THE FIREWALL METHOD

The firewall method controls service access by blocking service-specific URLs at the customer's firewall.

Each service receives requests at a specific *endpoint* (URL). Related services may have similar endpoints with related URLs (for example, the same first part and a different last part). When using a firewall to block access, the granularity of the blocking is determined by how much of the endpoint path is blocked.

For example, assume the following three service endpoints:
https://utilities.com/color/define, a service that allows you to define colors;
https://utilities.com/color/mix, a service that allows you to mix defined colors;
https://utilities.com/font/list, a service that allows you to choose from a list of fonts.
Each of these services can be individually blocked by blocking the entire endpoint path.
Blocking just https://utilities.com/color/ blocks both the define and mix services, as well as any other services whose endpoints begin with "https://utilities.com/color".
Blocking https://utilities.com/ blocks not only all the color services but also the font services and any other groups of services whose endpoints begin with "http://utilities.com".

A related document, *Adobe Creative Cloud Network Endpoints*, lists endpoints for Creative Cloud services, some of which are used by one or more of the Creative Cloud desktop applications.

The firewall method can be service-specific for a single service or a group of services, as described above. It is location-specific because it relies on the configuration of a specific physical network. It is also specialized, as it requires IT expertise and access to configure.

The firewall method is not user-specific, machine-specific, or client-specific.

BLOCKING WEB SITES WITH THE FIREWALL METHOD

Customers who wish to block users from accessing services from web browsers as well as Adobe applications may decide to firewall Adobe websites which host the services (e.g. creative.adobe.com) instead of the service endpoints themselves. However, doing so may have undesirable effects of which customers should be aware: the services blocked on the web site may be accessible via other endpoints not related to the site and the site may be the only access point for services that should not be blocked.

An example of the first effect is a service available from a web site that has another non-site endpoint, such as an API endpoint used by a desktop application. Many services have such endpoints. For example, blocking https://typekit.com will block users from using the font services from their browser, but they will still have access to those services from their desktop applications, because the desktop applications use endpoints hosted at https://api.typekit.com.

An example of the second effect is the administrative UI pages available on the creative.adobe.com web site. These are necessary for a subset of users, the admins. Blocking https://creative.adobe.com in order to block user access to the sync/store/share services has the additional effect of blocking admins from reaching the admin UI. In this case, you may need to allow admins through the firewall.

THE CONFIGURATION METHOD

The configuration method is only partially supported by Adobe at this time.

The configuration method controls service access by preventing Adobe desktop applications on a single machine from issuing service requests for Adobe-hosted services.

The Creative Cloud desktop applications can be configured to prevent them from attempting to contact specific services. The actual blocking mechanisms may include: setting various operating system preferences and/or product preferences; configuring desktop applications with Adobe installation & configuration software (e.g. AAMEE or the Creative Cloud Packager); and running scripts prepared by Adobe or other technical personnel.

When available, related documents that explain how to use the configuration method will be posted in the same location as this document. The list of Creative Cloud services referenced in the firewall method section on page 5 will also be a helpful reference when using the configuration method.

The configuration method is service-specific and machine-specific. It is also client-specific, as it blocks only access attempts from Adobe desktop applications; it does not block requests from web browsers or third party applications. The method has the effect of decreasing local network traffic because the Adobe products do not even attempt to access the blocked services. This is the only control method that actually stops network activity.

The configuration method is not user-specific; the specified service attempts will be blocked no matter who is using the desktop applications on the machine. The method is not location-specific; the machine could be taken from the work environment to the home

environment without affecting the configured blocking behavior. The method is a collection of techniques, some of which are specialized and some of which are not.

PROS AND CONS OF THE VARIOUS CONTROL METHODS

If you have a need or desire to block access to Creative Cloud services, which method you choose to employ depends on the problem you are trying to solve. The table below lists the defined characteristics of the control methods and indicates which characteristics each method has or does not have. You can use this information to determine which method is the best choice for your situation.

Keep in mind that successful access to a service that does authentication and authorization is controlled ultimately by the user's account settings. Even if an application can issue a service request and that request is allowed to pass through the firewall, the user's account is the ultimate arbiter on whether or not the request is granted.

Characteristic	Configuration Method	Firewall Method	Account Method
Service-specific	Yes	Yes	Yes
User-specific	No	No	Yes
Machine-specific	Yes	No	No
Client-specific	Yes	No	No
Location-specific	No	Yes	No
Specialized	Yes & No	Yes	No
Other	Decreases customer network activity		Works only for services that use the licensing services to do authentication and/or authorization

CONTROLLING ACCESS TO APPLICATIONS

There are two basic approaches customers can take to control access to the Creative Cloud desktop applications: they can control who can deploy an application onto a machine, or they can control which users can use a given application once it has been deployed.

CONTROLLING DEPLOYMENT

Customers may wish to partially or completely control who can deploy Creative Cloud desktop applications on their machines. One customer may want to prevent all normal users from installing any software on their machines. Another customer may want to allow a given user to install only certain applications and prevent them from installing others.

Complete Blocking — To achieve complete blocking, a customer can configure their operating systems to prevent their users from altering machine configurations. This prevents users from using the Adobe deployment services on the local machine to download and install any Creative Cloud software. Alternatively, a customer can simply not install the local deployment services at all. In that case, the normal user has no way of even attempting to download or deploy anything.

Selective Blocking — To achieve selective blocking, a customer can use the account method to configure each user's account with information that specifies which desktop applications that user is allowed to install and not allowed to install. When the user attempts to download a particular desktop application, the deployment services will refuse to perform the download if the user's account has blocked this application.

CONTROLLING USE

The easiest way to control access to deployed desktop applications is with the account method. Customers can configure a user's account to allow that user to run certain applications and not others.

However, customers in high-security or offline environments face a different problem. In these environments, network access is severely limited or nonexistent and so the desktop applications' attempts to authenticate and authorize the user by using the licensing services will fail. The problem for these customers, then, is how to grant access in the absence of the necessary network connection.

For these customers, Adobe provides an alternate way to grant access to the applications. A single admin for the customer can contact Adobe once (via the network) to get a special license token which is deployed onto users' machines along with the desktop applications. When the desktop applications are launched, the local licensing service finds the special license token and allows the application to run. This method of licensing is called *anonymous licensing* because the user is not required to log in to the application in order to use it.

NOTE: Use of anonymous licensing is only permitted to customers under a special licensing agreement with Adobe, which restricts the use of anonymous licensing to installations at customer sites with secure or no network access.