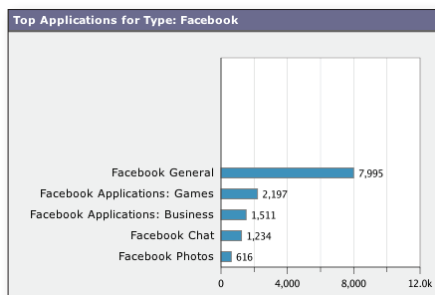


Controlling Facebook Activity

A Solution Guide

Facebook.com (Facebook) is a social networking website that allows users to interact with other users in a multimedia environment on the Web. Facebook users can install and use applications to enhance their experience. Many organizations want to allow Facebook access to maintain morale, increase retention, and boost hiring, but they also want to control access to it.



You can use the AVC engine to block part or all of Facebook to enable granular control of every element. You might want to configure Facebook controls to accomplish any of the following goals:

- **Enforce compliance.** You can make Facebook read-only to enable compliance with regulators and regulations, such as the Financial Industry Regulatory Authority (FINRA) and the Health Insurance Portability and Accountability Act (HIPAA).
- **Maintain productivity.** You can allow use of the main website while stopping access to third party applications which can consume significant time for users.
- **Enforce acceptable use policies.** You can allow complete access to Facebook after work hours or during the lunch hour, but make it read-only during work hours.

Facebook related applications are classified into one of the following groups:

- **Native Facebook applications.** These applications are developed by Facebook and are usually hosted on the facebook.com domain. Native Facebook applications use the “Facebook *Application_Name*” naming convention, such as Facebook Photos.
- **External Facebook applications.** These are created and managed by third party developers and are hosted outside of the facebook.com domain. External Facebook applications use the “Facebook Applications: *Category*” naming convention, such as Facebook Applications: Games.

Due to the nature of Facebook and how it hosts many of its own and third party applications, the AVC engine treats “Facebook” as its own application type, which includes both native and external Facebook applications. All Facebook applications, except for Facebook Videos, are grouped under the Facebook application type. Facebook Videos are grouped under the Media application type, enabling you to apply bandwidth controls.

Facebook is constantly updating and changing its native applications. Additionally, external Facebook applications are created and modified by third parties every day. Because these applications change constantly, the AVC engine updates its signatures to remain current with the available Facebook functionality and applications.

The controls that are applied to users are determined by where the user is located in the Facebook interface. For example, users can view photos from both Facebook Photos and from their Facebook walls. That means when the user is viewing another person’s photo in their photo album, the controls for Facebook Photos apply, but when the user is viewing the same photo on their own Wall, the controls for Facebook General apply.

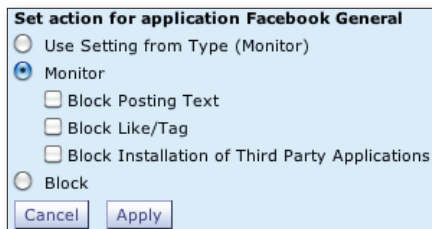
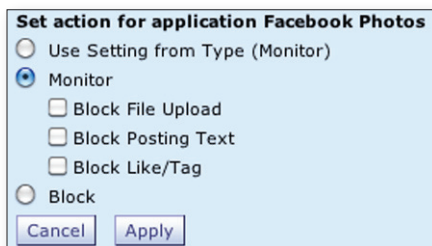
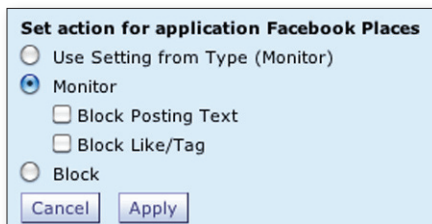
Configuring Facebook Controls

Like other application types, you can block or allow the Facebook application type or any of the particular applications included in that type. You can also apply more granular controls to most native Facebook applications by configuring different application behaviors, such as blocking the posting of text.

You can implement more granular controls to native Facebook applications using any of the following application behaviors:

- **Block File Upload.** This behavior blocks files uploaded to native Facebook applications, such as Facebook Photos and Facebook Videos. This application behavior does not affect links to external videos, such as YouTube. However, YouTube links in Facebook are controlled by the configured YouTube AVC controls in the Media application type.
- **Block Posting Text.** This behavior prevents users from entering text in fields, such as comments, status updates, or Notes. Blocking this behavior for an application is similar to making the application read-only.
- **Block Like/Tag.** This behavior blocks the ability to “like” a Facebook object, such as a status update or photo, by clicking the Like link. It also blocks the ability to tag people in Facebook objects, such as photos and videos.
- **Block Installation of Third Party Applications.** This behavior prevents users from installing external Facebook applications.

Not all application behaviors apply to all native Facebook applications.

Understanding Facebook General

Any area of Facebook.com that is not explicitly covered under one of the native Facebook applications is covered under the “Facebook General” native application. This includes users’ Wall and Profile pages, for example.

Some Facebook objects that are included in a native Facebook application, such as photographs in Facebook Photos, might also appear on a user’s Wall. When users view their Walls, access to objects on the Wall is determined by the settings configured for the Facebook General application. For example, if you configure the Block Like/Tag behavior control for Facebook Photos, but not for Facebook General, users can click the Like link for photos from their Wall, but not from a photo album.

Note

If you block Facebook General, it is the same as blocking the entire Facebook application type.

However, bandwidth controls always apply to videos, even if they appear on a user’s Wall.

User Experience when Accessing Facebook

When you block a Facebook application or application behavior, users are prevented from performing the intended action, but it is not always clear to users that their actions are explicitly being blocked by the Web Security appliance. When the AVC engine blocks Facebook content, it sends an end-user notification page by default. However, due to how Facebook displays content in the web browser, it quite often does not show the end-user notification page.

Additionally, there are multiple ways to accomplish most tasks in Facebook. For example, users can reach a page to upload photos using different paths. Users trying to access blocked Facebook content may observe different responses depending on the application they are accessing, the path used to reach the application, and how the applicable Access Policy is configured to handle the application and application behaviors.

The following list summarizes the types of responses users might observe based on which applications and application behaviors are blocked:

- **Block external Facebook application.** Users are prevented from navigating to the external Facebook application webpage. Facebook displays a generic error message.
- **Block native Facebook application.** Users cannot navigate to any page dedicated to that application. For example, if you block Facebook Photos, users cannot navigate to the page where they click a link to upload photos to an album. Facebook displays a generic error message.
- **Block native Facebook application behavior.** Users might observe any of the following behaviors:
 - **The user’s request is silently ignored.** This typically occurs when the user clicks a link or button and expects something to happen, but nothing happens. For example, this might occur when the user tries to cancel an event, delete a comment, or tag a person in a photo.

- **A dialog box appears and then disappears.** This typically occurs when the user clicks a link or button that would normally bring up a dialog box. Facebook appears at first to comply with the request by showing a dialog box, but then the dialog box disappears. For example, this might occur when the user tries to add guests to an event.
- **Facebook displays a generic error message.** This typically occurs when the user clicks a link that would normally cause part of the page to display new data from the server, but the AVC engine blocks that process. Facebook determines that something is preventing it from accomplishing the requested task, but does not distinguish the cause. The error message can appear inline in the webpage, or as a Facebook dialog box. For example, this might occur when the user tries to attach a link or photo to an event or message.
- **The web browser is redirected to an appliance end-user notification page.** This typically occurs when the user clicks a link that would normally navigate to a page in Facebook that is blocked by the AVC engine. For example, this might occur when the user tries to publish a note or delete a photo in an album.
- **The user waits indefinitely for a response from Facebook.** This typically occurs when the user clicks a link or button that would normally bring up a list of objects that Facebook loads, but the list is never populated. For example, this might occur when the user tries to tag a friend at a particular place.

Note

When you block the Posting Text application behavior for Facebook Events, some actions are only blocked after users have started the action (instead of immediately) due to how Facebook Events works. For example, users can create and edit an event, but cannot save them.

Rules and Guidelines

Consider the following rules and guidelines when configuring Facebook controls:

- Blocking Facebook General is the same as blocking the entire Facebook application type.
- You can prevent users from uploading photos and videos to Facebook from the web interface, but users can still upload photos and videos by sending emails with attachments to their Facebook email account. To prevent users from uploading photos and videos by email, configure your outgoing mail server, such as the Cisco IronPort Email Security appliance, to block email sent to the m.facebook.com domain.
- Some third party websites, such as cnn.com and espn.com, interact with Facebook to display or modify content in a user's Facebook account. The AVC engine blocks some of these sites from posting content to Facebook, but it cannot block all sites or all updates.
- When you block Facebook Chat, users may receive chat messages, but cannot send chat messages. Additionally, users do not see anyone else online, but others can see them online. When your users try to reply to received chat messages, the intended recipient never receives the message, which essentially blocks communication.