



Secure Web Gateway Application Control User Brief

Legal Notice

Copyright © 2015 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:

Phone: +1.800.363.1621

Email: support@trustwave.com

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Revision History

Version	Date	Changes
1.0	November 2013	Initial Version 11.5 Release
2.0	October 2014	Update
2.1	December 2014	Update
2.2	January 2015	Update
2.3	February 2015	Update including Drive apps

Table of Contents

Legal Notice	ii
Trademarks	ii
Revision History	ii
1 Introduction to Application Control	4
2 Application Control Profiles	5
2.1 Working with Application Control	5
2.2 Application Control Reports.....	6
3 User Actions	6
3.1 Apple iCloud Drive.....	7
3.2 Box	7
3.3 Dropbox	8
3.4 Facebook.....	8
3.5 Google Apps	9
3.5.1 Google+	9
3.5.2 Google Drive.....	10
3.5.3 YouTube.....	10
3.6 LinkedIn.....	11
3.7 Microsoft OneDrive	11
3.8 Twitter	12

1 Introduction to Application Control

As business use of web 2.0 applications grows exponentially, it presents a number of security, compliance, and productivity issues.

In terms of security, social networking and Web 2.0 applications present new ways for malware and threats to enter an organization. For example, botmasters exploit social network websites (such as Twitter.com) as their command and control (C&C) infrastructures. This is quite stealthy because it is hard to distinguish C&C activities from legitimate social networking traffic. Such a botnet C&C has some advantages when compared to other botnet C&C infrastructures and methods, as it uses popular legitimate sites, where occasional light traffic is unlikely to be noticed. The botmaster uses application features such as RSS feeds to automatically update bots. Moreover, the commands are so lightweight that they cannot be easily discerned from normal social network traffic.

Another trend in social media is scams on Facebook, for example, tricking users into customizing their profile look or layout. This tricks the user into installing a rogue Facebook app, giving the scammer access to the user's personal data.

Another major concern related to social media usage is confidential information leaking from organizations through unauthorized channels, for example, file transfers or chat using instant messaging. In terms of productivity, employees can waste company time on social networking and online games. Trustwave SWG helps to mitigate these issues by providing granular control of common social media applications.

Application Control provides the following benefits:

- Visibility and control over applications
- Reduction in the risk of exposure of sensitive data
- Reduction in the vectors that can be utilized for attacks, and optimization of security scans by limiting allowed protocols and applications
- Optimization of bandwidth and improved productivity by limiting non-relevant application usage

This guide provides brief summaries of the user actions that can be controlled within each of the social media applications supported by SWG. See [User Actions](#).

You can also create Application Control profiles that suit your organization's specific policy requirements. See [Working with Application Control](#).

SWG provides a number of out-of-the-box reports that enable you to monitor and analyze social media usage. See [Application Control Reports](#).

2 Application Control Profiles

SWG provides a default set of Application Control profiles that enable administrators to define how users can interact with social media applications. Once a profile is defined, it can be used as a policy condition in rules with type "Application Control".

The default profiles are defined as:

- **Allow Read-only** - groups user activities that are not for viewing only
- **Allow Limited interactivity** - groups interactive activities
- **Block Chat** - Groups chat activities
- **Block Upload Pictures and Videos** - Groups uploading activities

Profiles contain Action Groups of relevant social media actions for each supported social media application. The actions included in these groups are continuously maintained in the background as part of the security update mechanism. Where deemed necessary, the action lists will be extended or adapted to support more activities or additional applications.

2.1 Working with Application Control

You cannot edit a pre-supplied profile or action list, but you can duplicate a profile and edit the duplicate, or create your own profile from scratch. This procedure comprises:

1. Create a profile:
 - a. Go to **Policies > Condition Elements > Application Control**, right-click the relevant profile in the tree and select **Duplicate Profile**.
 - b. Add or delete Action Groups as required.
 - c. Click the **Edit** button and for each Action Group, make the changes you require by selecting and clearing the check boxes according to the required controls.
2. Go to **Policies > User Policies > Security** and in the relevant policy, create and enable a new Block or Coach rule.
3. Add an Application Control Condition and then select the check box of the profile you created.

For more information, see the *SWG Reference Guide* or SWG Help.



Important Notes:

- Application control of social apps embedded in other social media must be applied to the app itself. For example, user access and use of YouTube from within Facebook is controlled by the Action Group selections of YouTube, not of Facebook.
- In some instances, blocked actions in applications may appear to succeed or may cause the browser window to not update until the user refreshes the page. In these cases, the action is blocked but the application does not display correctly.
- In the Drive apps (Apple iCloud Drive, Box, Dropbox, Google Drive, and Microsoft OneDrive), the Folder Upload operation comprises two steps; Create Folder and Upload Files to Folder. If Work in File System is blocked, the Folder Upload operation will fail even if the Upload operation is not blocked.

2.2 Application Control Reports

To view the predefined Application Control Reports, go to **Logs and Reports > Reporting Tool > Reports** and expand the **Productivity** node.

- **Social Media Usage Summary:** Displays the most commonly used Social Media sites and their respective share of total Social Media activity during the defined time period.
- **Top Users Of Social Media Applications:** Displays the top users of Social Media sites according to usage during the defined time period.
- **Transactions Blocked By Application Control:** Displays the transactions that were blocked by Application Control profiles during the defined time period.

3 User Actions

User actions for the following social media are described in this section:

- Apple iCloud Drive
- Box
- Dropbox
- Facebook
- Google Apps
 - Google+
 - Google Drive
 - YouTube
- LinkedIn
- Microsoft OneDrive
- Twitter



Note: Application control support for the Drive apps Apple iCloud Drive, Box, Dropbox, Google Drive, and Microsoft OneDrive requires SWG version 11.6.

User actions provided by the various social media applications supported in SWG are continuously maintained. Where deemed necessary, these lists will be extended or adapted to reflect changes or extend the functionality.

3.1 Apple iCloud Drive

Action	Enables the user to ...
Delete Permanently	Permanently delete files or folders
Download	Download
Upload	Upload files or folders
Work in File System (Create folder, Move)	Work in File System (Create folder, Move)

3.2 Box

Action	Enables the user to ...
Assign Task	Create, Edit, and Delete tasks
Change User Settings	Change User Settings
Comment	Create, Edit, and Delete comments
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System (Create files and folders, Copy, Move, Rename, Delete)	Work in File System (Create files and folders, Copy, Move, Rename, Delete)

3.3 Dropbox

Action	Enables the user to ...
Change User Settings	Change User Settings
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or previous versions
Share	Share a new or existing folder, Invite people to collaborate, Import contacts, Allow members to invite others, Send invites, Reinvite, Uninvite, Unshare folder, Leave folder, Remove folder, Rejoin folder, Share link, Remove link, Get link
Upload	Upload files or folders
Work in File System (Create new folder, Copy, Move, Rename, Delete)	Work in File System (Create new folder, Copy, Move, Rename, Delete)

3.4 Facebook

Action	Enables the user to ...
Add Friend	Add someone to their friend list
Add People to Group	Add friends to a created group
App or Game Bookmarks	Open an app or game already installed by the user
Apps or Games Category	Display the apps or games within the App Center category
Chat Send	Send a chat or direct message
Comment	Post a comment or reply to a post
Create an Ad	Create an advertisement to be shown in facebook
Create a Page	Create a new facebook page
Create Event	Create an event and invite friends
Create Group	Create a group

Action	Enables the user to ...
Edit Picture	Edit a photo
Like	Mark posts/comments/pictures/video as liked
Message Delete	Delete a message, messages, or a full conversation
Poke	Send or respond to a poke
Post or Share	Post a new status or share a post from another user
Remove People from Group	Remove people from a previously created group
Upload Picture	Upload a photo
Upload Video	Upload a video
Video Chat	Chat with video
Write a Note	Create a note

3.5 Google Apps

3.5.1 Google+

Action	Enables the user to ...
+1	Mark a post/comment/picture/video as liked
Add a Person	Add a user to a circle, or group
Chat	Chat with other users
Create a Page	Create a page for any business, group, cause, or product
Create Community	Create ongoing conversations about particular topics
Create Event	See Share
Create New Circle	Create a group of people to follow and share with
Join Community	Join an ongoing conversation
Post Comment or Reply	Post a comment or reply to a post
Share (A Post, Event, Photo, Video, Link) and Create Event	Share something with other users
Video Chat	Chat with a friend or group of friends using video
Watch Video	Watch a video

3.5.2 Google Drive

Action	Enables the user to ...
Connect Apps To Drive	Connect apps to Google Drive
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System (Create folder, Create google docs, Copy, Move, Rename, Delete)	Work in File System (Create folder, Create google docs, Copy, Move, Rename, Delete)

3.5.3 YouTube

Action	Enables the user to ...
Add Video to Playlist	Add a video to the playlist
Create New Collection	Create a Group of subscriptions using collections
Delete Video	Delete an uploaded video
Edit Video	Edit a video
Like or Dislike a Video	Mark a video as liked or disliked
Play Video	Play a video
Playlist Settings	Save playlist settings, delete playlist, delete video from
Post	Post a new status
Post Comment	Comment on a video
Share	Share this video, Embed, Email
Report Video	Report a video as offensive
Subscribe or Unsubscribe	Include or exclude a channel from a collection
Upload Video	Upload a video
VideoManager.Videos	Manage properties of the videos uploaded
Vote Up/Down	Vote up/down on a comment

3.6 LinkedIn

Action	Enables the user to ...
Add Connections (Invite Contacts) or Connect	Add people to the user's connections
Comment	Make a comment to a post
Delete Message(s)	Delete a message or messages
Export Connections	Export information about connections to a file
Follow Company	Follow the posts that a specific company is posting
Join Group	Join a group
Like	Mark a post or comment as liked
Post a job	Post a job in order to recruit
Remove Connections	Remove a connection from the user's connections
Send Message	Send a message to the user's connection(s)
Share	Share something with other users

3.7 Microsoft OneDrive

Action	Enables the user to ...
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System (Create files and folders, Copy, Move, Rename, Delete)	Work in File System (Create files and folders, Copy, Move, Rename, Delete)

3.8 Twitter

Action	Enables the user to ...
Create List	Gather profiles into a list
Delete	Delete a tweet
Follow	Start following a user
Send Message	Send a direct message to another user
Tweet or Retweet	Tweet or retweet

About Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide.

For more information, visit <https://www.trustwave.com>.