

Security for Flash Player compatible content in Acrobat 9

CONTENTS

Introduction	1
Overview	1
Flash Player in Acrobat 9.0	2
External Access Security Features	3
Flash Player Sandbox Security Model	6
Update model	7
Flash Player compatible content in Acrobat 8.0	7
References	8

Introduction

The latest releases of Adobe® Acrobat® and Adobe Reader® 9 introduce new native support for the playback of Flash® Player compatible content. This new feature uses an embedded Flash Player runtime and hence is independent of other instances of Adobe Flash Player installed on the system. This white paper provides an overview of the security model for Flash Player compatible content playing inside Acrobat and Adobe Reader® software. It is important to note that not all capabilities allowed for SWF content playing in a network or web environment are allowed when playing inside Acrobat or Reader. Also note that where this paper refers to Flash Player compatible content playing in Acrobat 9, the behavior described also applies to Adobe Reader 9.

Intended Audience

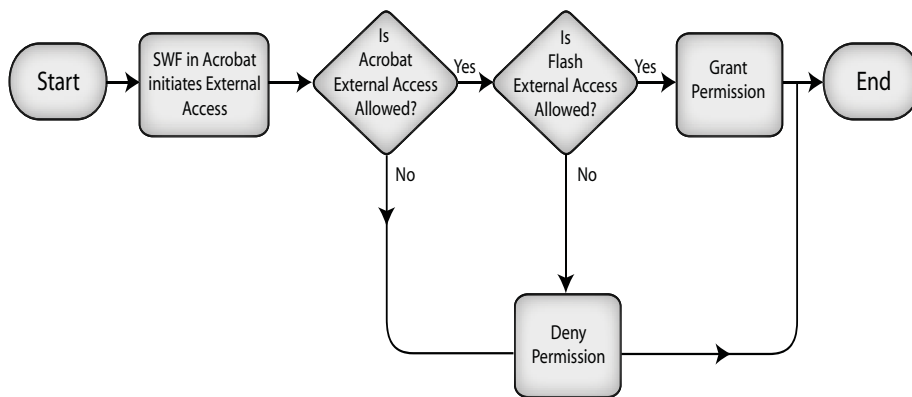
This document is intended for:

- IT managers and system administrators who are interested in the security of Acrobat and PDF in their network environment
- Developers (including programmers and document authors) who create PDF documents containing Flash Player compatible content

Overview

In general, Flash Player compatible content is allowed to invoke resources embedded during the authoring of the PDF file, but is restricted from accessing resources external to the document except to support streaming FLV files or to access trusted URLs. In all cases, SWF and FLV content running in Acrobat is subject to both Acrobat and Flash Player security rules. Acrobat provides the first layer of security features. The operation fails if Acrobat disallows the access. If it is allowed by Acrobat then it is checked against the security rules of

Flash Player. The operation fails if Flash Player disallows the access. External Access is permitted only if both Acrobat and the Flash Player allow it.



Flash Player in Acrobat 9.0

Acrobat 9 introduces new authoring and playback capabilities leveraging the Flash Player including the following:

PDF Portfolios

PDF Portfolios allow customers to package multiple file types into a single, compressed PDF file. PDF Portfolios provide presentation and organization capabilities, called navigators, which are Flash based UI components or skins that can be customized or branded for any given PDF Portfolio. The following features of a PDF Portfolio navigator rely on Flash Player for playback.

- PDF Portfolio navigators are Flex® or Flash templates that present unique navigational styles and animations
- Navigators can include optional welcome pages that support playback of embedded SWF content
- FLV, MP3, and SWF can be previewed directly inside the PDF Portfolio UI

Multimedia

Multimedia features allow authors to embed video, audio, and SWF content for playback in a PDF document. Almost any multimedia format supported by the Flash Player runtime can be embedded and played back natively in a PDF document or Portfolio.

- Video – FLV and H.264 files can be embedded for direct playback. Acrobat Pro Extended also provides capabilities for transcoding other video formats to FLV format. Additionally, streaming FLV content can be inserted through a URL reference
- Audio – MP3 and AAC files can be embedded for direct playback
- Animations and Applications – SWF content can be embedded including all required resources and FlashVars

Ads for Adobe PDF

Ads for Adobe PDF, also referred to in this document as Sponsored Content, is a service provided in a partnership between Adobe and Yahoo! that allows content creators to monetize their content by embedding relevant ads inside of their PDF documents.

External Access Security Features

As stated in the overview, there are quite a few additional security restrictions for SWFs hosted in Acrobat. The following section lists the different types of external access and their behavior in Acrobat.

Local File-System Access

This will be blocked for all SWFs in Acrobat. The rule would apply for all SWFs including SWFs that belong to the local-with-file-system sandbox.

SharedObjects

[SharedObjects](#) are not allowed for SWFs hosted inside Acrobat. Trying to create a shared object from a SWF in Acrobat would result in runtime error 2134.

LocalConnection

[LocalConnection](#) is not allowed for SWFs hosted inside Acrobat. Trying to write to a LocalConnection from a SWF in Acrobat would result in runtime error 2146.

File Upload and Download

Using the [FileReference](#) to upload a file from the user's file system to the server is blocked. Using the same class to download a file from the server to the user's file system is blocked for SWFs in Acrobat.

Socket

Acrobat uses the Acrobat URL Trust Manager to control RTMP socket access. Acrobat generates a URL of the form 'flashSocketAccess:\\<ip address>:<port>' and uses the URL Trust Manager to get permission from the user for the given RTMP socket. The socket access is allowed or denied based on the input from the user. In the URL, 'flashSocketAccess' is a hardcoded scheme used by Acrobat to represent RTMP sockets. RTMP sockets are used for streaming FLVs from the Flash Media Server. Acrobat URL Trust Manager is explained in the [Absolute URL Access](#) section.

All other types of socket access are blocked for SWF in Acrobat.

Absolute URL Access

Acrobat enforces URL checks at the scheme level and the domain. Flash Player would return an error for access made using ActionScript® 3.0 classes when the URL access is rejected by Acrobat.

Scheme Whitelist

Acrobat uses a configurable scheme whitelist for controlling external URL access from content in Acrobat. The default set of schemes in this whitelist are http, https, ftp, rtmp, rtmpe, rtmpte, rtmpts, and mailto. Acrobat would not allow content to access any URL whose scheme is not present in that whitelist. IT managers can add or remove schemes to this list based on their needs.

On Windows®, the Flash Player whitelist is stored at the following location in the registry.

Acrobat

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Adobe Acrobat\9.0\FeatureLockDown\cDefaultLaunchURLPerms

String Value Name: 'tFlashContentSchemeWhiteList'

Adobe Reader

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockDown\cDefaultLaunchURLPerms

String Value Name: 'tFlashContentSchemeWhiteList'

The default value in that list is

"http|https|ftp|rtmp|rtmpe|rtmpte|rtmpts|mailto". Changing that to an empty list would mean that no external URL Access is allowed from Flash Player in Acrobat.

On the Macintosh, this is stored in the FeatureLockDown file inside Acrobat or Adobe Reader Package. This file is normally located in 'Contents/MacOS/Preferences' folder inside the package. The setting is stored under the 'FlashContentSchemeWhiteList' section in the FeatureLockDown file.

Sponsored Content Scheme Whitelist

Acrobat uses a configurable scheme whitelist for controlling external URL access from Sponsored Content SWFs in Acrobat. The default set of schemes in this whitelist are http, and https. IT managers can add or remove schemes to this list based on their needs.

On Windows, the sponsored content whitelist is stored at the following location in the registry:

Acrobat

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Adobe Acrobat\9.0\FeatureLockDown\cDefaultLaunchURLPerms

String Value Name: 'tSponsoredContentSchemeWhiteList'

Adobe Reader

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockDown\cDefaultLaunchURLPerms

String Value Name: 'tSponsoredContentSchemeWhiteList'

The default value in that list is "http|https ". Changing that to an empty list would mean that no external URL Access is allowed from Sponsored Content SWFs in Acrobat.

On the Macintosh, this is stored in the FeatureLockDown file inside Acrobat or Adobe Reader Package. This file is normally located in Contents/MacOS/Preferences folder inside the package. The setting is stored under the 'SponsoredContentSchemeWhiteList' section in the FeatureLockDown file.

Acrobat URL Trust Manager

Acrobat's URL Trust Manager ensures that a local document cannot connect to the web without the permission of the user. The dialog asking for permission has an "always" checkbox to avoid multiple prompts for a given domain. Web documents are allowed to connect to the web without asking the user for permission. This is explained in detail in the Adobe® Acrobat Trust Manager Internet Resource Access Control document.

The user is asked for permission for external URL Access from the following SWFs:

- Rich media annotation SWFs embedded inside a local PDF file
- Remote Rich media annotation SWFs linked from inside a local PDF file
- SWF Attachments previewed inside local Portfolios
- SWF Welcome Screen in local Portfolios
- Navigators in local portfolios
- Sponsored Content SWFs are exempted when they access <https://sc.adobe.com> but are subject to URL Trust Manager for all other external URL access.

The user is not asked for permission for external URL Access from the following SWFs:

- Rich media annotation SWFs embedded/linked inside a remote PDF
- SWF Attachments previewed inside remote Portfolios
- SWF Welcome Screen in remote Portfolios
- Navigators in remote portfolios

Invalid URLs

Acrobat will do one level of percent decoding of URLs if the URL is percent encoded. If the URL contains '%' characters even after the decoding then it is rejected.

URLs that try to access the parent folder using the '..' notation are rejected.

Relative URL Access

Relative URL Access is resolved based on the SWF making the request.

If the SWF making the request is a SWF embedded inside a document then the relative URL is assumed to be relative to the embedded root SWF. If the relative URL is not contained in the document then the call results in an error.

If the SWF making the request is a remote SWF and the root SWF is embedded inside a document then the relative URL is assumed to be relative to the remote SWF making the request. If the relative URL is not contained in the resolved remote location then the call results in an error.

If the SWF making the request is a remote SWF and the root SWF is a remote SWF then the relative URL is assumed to be relative to the root SWF. If the relative URL is not contained in the resolved remote location then the call results in an error.

Flash Player Sandbox Security Model

If external access is allowed by Acrobat then Flash Player enforces its checks based on its sandbox rules. Flash Player uses sandboxes which are logical groupings to control resource access. It consists of a Remote sandbox, Local-with-filesystem sandbox, Local-with-networking sandbox and the Local-trusted sandbox as described in the [Security Sandboxes](#) article. [Flash Player Security White Paper](#) describes how Flash Player applies security based on these different sandboxes.

Flash Player in Acrobat uses the Local-with-networking and the Remote sandbox. The Local-with-filesystem setting in the SWF is ignored for SWFs inside Acrobat. The following section shows how SWF in Acrobat map to the different Flash Player sandboxes.

Local-with-networking sandbox SWFs

SWFs embedded inside a document on the local file system are placed in this sandbox. SWFs belonging to this type would be loaded using URLs of type 'file://pdfmediaNNNN/pdfmediaNNNN.swf' where 'NNNN' is a random number that would differ from instance to instance.

Here are some examples of these SWFs:

- Rich media annotation SWFs embedded inside a local PDF
- SWF Attachments previewed inside local Portfolios
- SWF Welcome Screen in local Portfolios
- Navigators in local portfolios

Remote sandbox SWFs

SWFs inside a remote document or remote SWFs linked from a local document are placed in this sandbox. SWFs embedded inside a remote document are loaded using URLs of type

'http://<domainOfRemotePdf>/<dirnameOfRemotePdf>/pdfmediaNNNN/pdfmediaNNNN.swf' where 'NNNN' is a random number that would differ from instance to instance. Documents that do not embed the SWF but contain a URL for a remote SWF would use their real URL when activating the SWF instead of a custom generated URL.

Here are some examples of these SWFs.

- Remote Rich media annotation SWFs linked from inside a local PDF
- Rich media annotation SWFs embedded/linked inside a remote PDF
- SWF Attachments previewed inside remote Portfolios
- SWF Welcome Screen in remote Portfolios
- Navigators in remote portfolios
- Sponsored Content SWFs

The random number used in the custom URLs is to avoid collisions when accessing resources contained in the document and not as a security issue.

Update model

Future security feature updates to the Flash Player runtime will be made through updates to both Acrobat and Reader. Those security feature updates will be separate from any updates to Adobe Flash Player. Because the Flash Player runtime in Acrobat is independent from the Flash Player running in a browser, and because Flash Player running in Acrobat is governed by two security models, a security vulnerability discovered in the browser environment does not necessarily affect Flash Player in Acrobat. Newly discovered Flash Player security issues will be evaluated in terms of their impact, if any, on Acrobat and distributed through the standard Acrobat update mechanisms as necessary.

Flash Player compatible content in Acrobat 8.0

Acrobat 6.0 to Acrobat 8.0 supported Flash Player compatible content in a very limited way as part of the legacy Multimedia annotation. This support was based on the browser plug-in and that has not changed in 9.0. Features introduced in 9.0 use an embedded Flash Player that helps enable a much higher level of security. Hence the security rules described in this document do not apply to the legacy Multimedia annotation.

As soon as a legacy Multimedia annotation is activated, the user is asked for permission to run the multimedia content. They are not asked later when the external URL access is done. All local file system access is blocked.

References

[Flash Player Security White Paper](#)

[Adobe® Acrobat Trust Manager Internet Resource Access Control](#)

[Flash Runtime Errors](#)

[Enhanced Security in Adobe Acrobat 9 and Adobe Reader 9](#)

Copyright 2008 Adobe Systems, Incorporated. All rights reserved.

Adobe Systems Incorporated

345 Park Avenue, San Jose, CA 95110-2704 USA

<http://www.adobe.com>

Adobe, the Adobe logo, Acrobat, Reader, Flash, Flex and ActionScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Macintosh is a trademark of Apple Computer, Inc., registered in the United States and other countries. Microsoft, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.