

External data not accessible outside a Macromedia Flash movie's domain

For security reasons, a Macromedia Flash movie playing in a web browser is not allowed to access data that resides outside the exact web domain from which the SWF originated.

As an enhancement to Macromedia Flash Player 7, domains must be identical for data to be read. With this change a sub-domain can no longer read data from a parent domain and vice versa.

Cross-domain policy files

Another change to the Flash Player 7 framework is the use of cross-domain policy files. A policy file is a simple XML file that gives the Flash Player permission to access data from a given domain without displaying a security dialog. When placed on a server, it tells the Flash Player to allow direct access to data on that server, without prompting the user grant access.

The server can be in any location available to the Flash movie and does not have to be in the same domain. Cross-domain policy files, named `crossdomain.xml`, are placed at the root level of a server. When using a policy file you can use a wildcard character (*) in a domain name. For more information on policy files see [Why Use Policy Files](#) below.

Note: When serving a policy file, you must not use a cross-domain redirect, or the player will ignore the policy file.

Cross-domain file access

This applies to any ActionScript command or object that sends or receives data, including `loadVariables`, the `XMLSocket` object methods, and the XML object `send` and `sendAndLoad` commands.

Flash Player follows specific guidelines to determine domain compatibility. Refer to [Domain Comparison](#) below for details.

Descriptions and ways to address the following issues are outlined below.

[You cannot load variables or XML data into a Flash movie from another domain.](#)

[Data cannot be returned to Flash from an incompatible domain \(Flash Player 6,0,47,0 and above\)](#)

[Flash movies loaded from incompatible domains cannot access ActionScript objects and variables](#) (Flash 6 and above SWF files)

- **You cannot load variables or XML data into a Flash movie from another domain.**

For example, a Flash movie loaded from <http://www.yourserver.com/flashmovie.swf> can access data residing at <http://www.yourserver.com/data.txt>. The text file is located within the same domain as the SWF.

However, an attempt to load data from <http://www.NotMyServer.com/data.txt> will fail and no error messages are displayed. The load action will cause a warning dialog to appear.

For more information on this dialog please refer to [Macromedia Flash movie fails to load data in Flash Player 7](#) (TechNote [tn_18860](#)).

There are techniques available to work around this issue. Refer to [Loading data across domains](#) (TechNote [tn_16520](#)) for recommended workarounds.

Note: This security feature does not affect Flash movies playing in stand-alone projectors.

- **Data cannot be returned to Flash from an incompatible domain** (Flash Player 6,0,47,0 and above)
Data returned to a Flash movie from an incompatible domain will be ignored. Because of this, server-side redirects that return data from another domain will fail.
Note: This security feature does not affect Flash movies playing in stand-alone projectors.
- **Flash movies loaded from incompatible domains cannot access ActionScript objects and variables** (Flash 6 and above SWF files)
In order for two Flash MX movies to share objects and variables, both movies must reside in the same domain. Attempts to access cross-domain data will be ignored.

This security feature affects Flash 6 and later SWF files. Flash 4 and Flash 5 movies are able to access objects and variables from other Flash 4 or Flash 5 movies in different domains, and from Flash 6 movies in the same domain. However, Flash 4 or Flash 5 movies are not able to access objects and variables from Flash MX movies in a different domain.

You can override the security feature enabling access to Flash 6 movie objects and variables from a Flash 6 movie in a different domain. Use the `System.security.allowDomain` command to identify domains with access to the objects and variables.

Never call `System.security.allowDomain` unless you fully trust the operator(s) of the domain being specified. By using this code, you are granting access to any movie on that domain.

For more information, see [Flash Help](#) (Help > ActionScript Dictionary > `System.security.allowDomain`). You must have the updated ActionScript Dictionary to view this documentation. Refer to [Macromedia Flash MX Documentation Update](#) (TechNote [16470](#)) for information on obtaining this update.

Note: This security feature affects Flash movies playing in stand-alone projectors. A projector has access to movies loaded from another domain but

... This security feature ensures that movies playing in domain-wide projectors do not have access to movies loaded from another domain. For example, movies from another domain cannot access the projector without being granted access.

Domain Comparison

The basis of domain comparison is the domain name, not IP address. This means that two domains resolving to the same IP address are not necessarily compatible; the names themselves must be compared.

Here are some examples of compatible domains for Macromedia Flash Player 7. In each row, the domain on the left is compatible with the domain on the right:

http://www.macromedia.com	http://www.macromedia.com
http://macromedia.com	http://macromedia.com
http://127.0.0.1	http://127.0.0.1
https://www.macromedia.com	https://www.macromedia.com

In Flash Player 6 the following examples are compatible, however these are no longer compatible in Flash Player 7 because of exact domain matching rules. An additional rule, also added under Flash Player 7, is content accessed via HTTP may not access data from a HTTPS location.

http://www.macromedia.com	http://hello.macromedia.com
http://www.macromedia.com	http://macromedia.com
http://hello.macromedia.com	http://hello
http://www.macromedia.com	https://www.macromedia.com

Here are some examples of incompatible domains for both Flash Player 6 and 7. In each row, the domain on the left is incompatible with the domain on the right:

http://www.macromedia.com	http://www.not-macromedia.com
http://127.0.0.1	http://127.0.0.2
http://www.macromedia.com	http://127.0.0.1

Why use a policy file?

There are some circumstances where it may be desirable to deploy a policy file. Policy files can handle all of the following issues, and movies themselves do not need modification. Also, the file can be created in a simple text editor such as Notepad or SimpleText.

- A version 6 movie (or earlier) on one domain, hosted via HTTP, wishes to access data on a sub-domain, HTTPS location, or with an incomplete URL. These situations prompt Flash Player 7 to display a warning dialog, which may be undesirable.
- A version 7 or above SWF wishes to perform the same transaction, but is prohibited by the Flash Player 7s security model.
- A movie wishes to make a request to content hosted on a public server, such as web services, but is prohibited by the Flash Player cross-domain data access restrictions.

Scenarios that require policy files

A web site relies on sub-domain data access

A company has a large web site that includes several sub-domains. Each sub-domain is used to run specialized activities, such as hosting an application, database, or department data. With Flash Player 6 and earlier, a movie hosted on one sub-domain could freely access any other sub-domain without restriction.

Example domains:

http://www.company.com - sub-domain that hosts the Flash movie
http://remoting.company.com - sub-domain that hosts Flash Remoting services
http://info.company.com - sub-domain that houses scripts used to access the company databases
http://finance.company.com - sub-domain used by the company's finance department
http://ads.company.com - sub-domain used by the company's advertising department

With Flash Player 7, movies published as version 6 or earlier performing this sub-domain data access will display a warning dialog box asking the end user for permission to perform the transaction. In this scenario, the site owner designed the movies to work this way, so it is expected that end users allow it. However, the prompt may cause a misunderstanding with users and they may accidentally disallow the operations.

Since the Flash movie was previously allowed to access all servers, the company wants to enable this behavior for Flash Player 7 and above. Policy files are set on all servers from which the movie needs data access. Using a text editor, a simple policy file is created telling servers to allow access to Flash movies hosted on http://www.company.com.

Example of this policy file:

```
<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="www.company.com" />
</cross-domain-policy>
```

The file is saved as crossdomain.xml, and placed on the site root of all servers that the movie needs to access: http://remoting.company.com, http://info.company.com, http://finance.company, and http://ads.company.com.

From this point forward, all Flash content on http://www.company.com functions as it did with Flash Player 6.

Note: A common mistake is to place the policy file on the server on which the Flash movie resides. It must be placed *on the server that the Flash movie wishes to access*.

A movie that makes a data request with an incomplete URL

A company has a web site loads Flash data from its own domain. However, they discover a movie on their site is no longer able to access a file, even though the file is located in the same domain.

It's determined that the URL the Flash movie attempts to access is located on http://company.com, which fails when accessed from http://www.company.com. While the creator of the Flash movie did not think much of this oversight, the Flash Player 7 determines that - since the "www" prefix is omitted - this must be treated as a unique and therefore prohibited domain.

Another complication to this problem is not all users are experiencing this behavior because some are accessing the site using http://company.com, while others type out the full URL in their web browser.

To address this problem, the company creates a policy file that accounts for both URLs.

```
<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="www.company.com" />
  <allow-access-from domain="company.com" />
</cross-domain-policy>
```

The file is saved as crossdomain.xml, and placed on the site root of the same server that hosts the Flash movie. The movie now functions as it did with Flash Player 6.

A web site that allows access to and from all sub-domains

A company decides to deploy Flash content on several sub-domains within the company's web site. These movies are allowed access to any other sub-domain within the company, similar to the movie in the example above. However, the process of adding multiple sub-domains to each policy file can be laborious, and there can be issues with policy files not getting updated regularly with new sub-domains added to the site.

To address this problem, the company creates a policy file that grants access to the Flash Player, regardless of which sub-domain makes the request, by using a wild card ("*") in the sub-domain token field.

```
<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="*.company.com" />
</cross-domain-policy>
```

The file is saved as crossdomain.xml, and placed on the site root of all servers used to host sub-domains on the company site.

An internal web site allows access to selected sub-domains and local servers

A company has an internal server application hosted on http://finance.company.com. This server is behind a firewall and not accessible to the outside world.

The company has two Flash business applications hosted on two internal sub-domains: http://hr.company.com and http://it.company.com. These two sub-domains should be allowed to access http://finance.company.com, and all other sub-domains are not permitted access.

A policy file can be created for http://finance.company.com to allow access to the two sub-domains only. By not specifying other sub-domains in the policy they will be denied.

One additional issue to take into account are internal server "friendly names." Web users sometimes type only the server's shortened name. An example typing http://hr, or even hr. Because of DNS resolution, the URL is routed to the correct location. However, when the Flash Player sees a friendly name, and not a fully qualified URL, it's treated as a unique, and therefore, separate domain.

To address this problem, the company creates a policy file that accounts for both scenarios. It grants access to both desired sub-domains, using their fully qualified domain names, and it grants access if accessed via an internal friendly server name.

```
<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="hr.company.com" />
  <allow-access-from domain="it.company.com" />
  <allow-access-from domain="hr" />
  <allow-access-from domain="it" />
</cross-domain-policy>
```

Again, the file is saved as crossdomain.xml and placed on the site root of http://finance.company.com.

Note: Because this scenario involves servers behind a firewall, the policy file should not be placed on a public server.

A public server that allows data access from any domain

Some sites are intended to be accessed by anyone. They contain publicly available data, such as news feeds and web services.

The Flash Player, and web browsers, generally disallow access to data outside the current domain. Because of this, a common practice is to deploy a proxy script on the server that hosts the Flash movie, which then requests data server-side before returning it to the movie.

This is a standard practice, but it requires the creator of the Flash movie create server-side logic just to access public data. If the public server has a policy file, all Flash movies can access its data without any additional server scripts.

A policy file that permits all domains to access it uses a wild card instead of specifying individual domains.

```
<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="*" />
</cross-domain-policy>
```

It is saved as crossdomain.xml and placed on the site root of the public server.

Note: This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies.

A secure server that allows access to movies hosted via a non-secure protocol

It is not advisable to permit HTTP content to access HTTPS content. This practice can compromise the security offered by HTTPS.

However, there may be cases where legacy Flash content is allowed access to data of a HTTPS site. With Flash Player 7, this is no longer allowed by default. To permit access to HTTPS data by Flash movies served via HTTP, use the secure attribute in a "allow-access-from" tag and set it to false.

```
<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="www.company.com" secure="false" />
</cross-domain-policy>
```

It is saved as crossdomain.xml and placed on the site root of the HTTPS server.

Additional Information

The security features documented in this TechNote were added to the Flash Player at the request of developers.

These enhanced security features were added to address potential issues with data transfer to and from Flash movies. For a more comprehensive review of the security features added in Flash Player 7, please refer to [Security Changes in Macromedia Flash Player 7](#)

Last updated: August 8, 2002

Easy Link this TechNote http://www.macromedia.com/go/tn_14213