



Clipstream

Playerless video and audio streaming

Clipstream™ Video 2.2 Technical Guide – Section 13 Security

Disclaimer: All content presented herein is subject to change without notice and is deemed as accurate as possible at time of publication. Please consult with Clipstream™ Video Support at <http://clipstream.com/help> for clarification if you encounter any erroneous or inconsistent material in this document.

© 2000, 2001, 2002 Destiny Media Technologies, Inc. All Rights Reserved. Clipstream, AudioClipstream, Clipstream Email, Bannerstream, Clipstream AudioMail and VideoClipstream are trademarks of Destiny Software Productions, Inc. All other trademarks are the property of their respective owners.

Section 13 - Security

About Clipstream Video Security	13-1
Security ID (SID)	13-1
Using the SID	13-1
Playback Sequence of Events	13-2
SID Summary	13-3
Preventing Codebasing / The Stealing of Bandwidth and Content	13-3
Prevent Codebasing Without Using an SID	13-3
Allowing Specific Sites to Codebase Using AuthorizedDomainURL Parameter	13-4
Modifying the Applet Code for AuthorizedDomainURL Parameter	13-4
Creating the AuthorizedDomains.txt Document	13-5
Emailing of SID Encoded and CODEBASE Protected Content	13-5

Clipstream Video Security

About Clipstream Video Security

Clipstream Video has 3 security features to prevent the pirating of streams:

1. A Security ID (SID) which ties the code key to the video preventing a third party from downloading a clip (.vcs) and streaming it from their server, whether or not they have a valid Clipstream code key.
2. Security ID encoded videos automatically prevent the usage of the CODEBASE statement to pirate your content and bandwidth.
3. A server folder structure that prevents CODEBASING of unsecured video content (i.e. content not encoded with an SID).

Security ID (SID)

Your Clipstream Account Representative will create an SID (a unique alphanumeric string) for you and secure code key that matches this SID. Once videos are encoded with an SID, each Clipstream encoded file will only play if the secure code key used by the server was created with the same SID.

SID encoded content effectively prevent piracy of Clipstream streams in this fashion:

Although the clip might be downloadable, it will not be playable, servable, or codebaseable even if a site or user has a valid Clipstream Video code key.

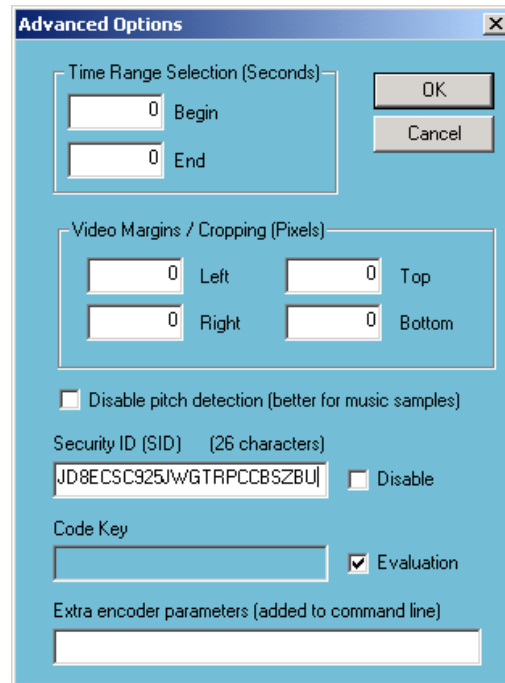
Note: Once streams have been encoded using an SID they cannot be unlocked to be made unprotected. To serve an SID encoded file from another site, the site will need to have a code key created using the same SID as the encoded clip. Ask your Clipstream account representative for more information.

Using the SID

To utilize IP Stream Locking, you will need to be given a Secure ID by your Clipstream Account Representative. Please note that the SID does not replace your Clipstream Code Key. In fact, it is from the SID that your code key is also created.

The SID is utilized during the encoding process. To encode secure content with your SID, follow these steps:

1. With the Clipstream Video Encoder open and ready to encode, open the settings window by clicking the “Settings” button.
2. The “Advanced Options” window should appear as follows:



Advanced Options Window

3. Beside the Security ID box, un-check Disable. You can re-check this for future encodings if you do not wish them to be secure.
4. Enter your Secure ID into the Secure ID Box.
5. Click OK.

NOTE: As long as Disable box is not checked, all clips in subsequent sessions will be encoded with the SID.

Playback Sequence of Events

When a server attempts to serve a SID encoded video:

1. The Applet notices that the video to be played has been encoded with a SID.
2. The Key or KeyFile parameters are checked for a Secure Code Key that satisfies all of these conditions:
 - The key has not time expired.
 - The key matches the server.
 - The SID that the key was created with matches the SID that created the video file.
3. If one or more of these conditions are not met, the stream will not play.

When a Server attempts to display a SID encoded video using the codebase statement:

1. The Applet notices that the video to be played has been encoded with a SID.
2. The AuthorizedDomainURL parameter is checked to see if the referring server is listed as an Authorized server.
3. If the server is not listed, the video will not play.

SID Summary

- Request a SID from your Account Representative
- Your applet Code Key is created from your SID
- Content Encoded with a SID will not play on a site without a code key created with the same SID, even a local drive
- The SID is entered when encoding
- Previously encoded content will not run with a SID code key
- Previously encoded content must be re-encoded with a SID to be secure
- Codebase protection is automatically on when SID encoded content is streamed.

Preventing Codebasing / The Stealing of Bandwidth and Content

Using the codebase statement in the applet code, it is possible for other sites to copy your applet code and paste it into their web pages and thus stream your content from their site, without having downloaded any of your content. In essence, the perpetrator will not only be stealing your content, but also your bandwidth. In these situations, it is possible to protect your content using the built in codebase protection of AudioClipstream.

A new parameter has been added to Version 2.0, AuthorizedDomainURL, that allows you to specify a text file that lists sites allowed to codebase your material. If a site is not on the list, the content will not be able to be codebased. This permission to codebase can also be time based, if desired. When content is encoded using a SID, codebase protection automatically activates and you will be required to use the AuthorizedDomainURL parameter to allow people to codebase your content. Not that content can be codebase protected without using a SID.

There are two ways to prevent Codebasing:

1. Encode your content with a SID
2. Store and stream your content in a sub folder behind the path /scs/

Prevent Codebasing Without Using an SID

It is possible to prevent the Codebasing of video content even if it has not been encoded with an SID. In this case, content will not be streamed from unauthorized sites, but sites with a valid code key might be able to download your content and stream it themselves. This is useful when you would like people to be able to stream your content, but may not want them to use your bandwidth to do so and you do not wish to encode your content using an SID.

To prevent other sites from Codebasing his material without using a SID, the videoclipstream.zip file should be located in a folder beneath the sub directory /_scs_/ . All the other content for the applet (vcs and image files) can be located elsewhere on the same server, or in this sub-directory. When the .zip file is here and someone uses the codebase statement, if their domain does not appear in the AuthorizedDomainURL parameter file, then the site will not be allowed to codebase the content.

Allowing Specific Sites to Codebase Using AuthorizedDomainURL Parameter

Under certain arrangements, you may wish to allow some sites or servers to codebase your video files. This becomes attractive with Clipstream video as it allows you to control who access or codebases your content, and for how long. This is accomplished using the AuthorizedDomainURL parameter in the Clipstream Video Applet Code (see applet code section). The AuthorizedDomainURL parameter points the Clipstream Video Applet to a text file on your server that specifies which sites are allowed to codebase your video content, and for how long. If a site does not appear on the list, or is operating outside the specified dates, the content will not stream.

Syntax for the AuthorizedDomainURL parameter is as follows:

AuthorizedDomainURL

Type
String

Values
URL

Default
None

Description
URL points to a text file on the server outlining sites allowed to codebase applets using content encoded with a secure ID. If this parameter is not used, content encoded with the secure ID will only be servable by the host server.

Example
<param name="AuthorizedDomainURL" value="authorizedsites.txt">

Modifying the Applet Code for AuthorizedDomainURL Parameter

In your AudioClipstream applet, now, create a new parameter called AuthorizedDomainURL. See the examples below:

```
<param name="AuthorizedDomainURL"  
value="AuthorizedDomains.txt">
```

As you can see, the value of the AuthorizedDomainURL parameter identifies the location of the AuthorizedDomains.txt.

Note: As with all other elements within the applet, the AuthorizedDomains.txt file must exist on the same server as the

audioclipstream.zip file. This is due to Java security.

Now you can add or subtract authorized site at will, simply by modifying the AuthorizedDomains.txt file on your server.

Creating the AuthorizedDomains.txt Document

Create a txt document named something like AuthorizedDomains.txt (you can name the txt file anything you want but it must be reflected in the parameter value) and place it in a permanent folder on your remote site. In that txt document, type in all of the URLs that you want to give permission to codebase your content. Construct the format of the .txt file as follows:

```
URL #Comment1 ##Comment2 #EXP:YYMMDD
```

- URL is the URL of the site allowed to CodeBase. Sub directories can be specified. Note that when the URL is specified, all directories below are permitted.
- #Comment1 is any user definable comment
- ##Comment2 is any user definable comment
- #EXP:YYMMDD is the date that the CodeBase permissions expire for that URL (Time based permission)

A sample AuthorizedDomains.txt file might look as follows:

```
#This is the list of web sites using codebase to remote streaming
http://www.clipstream.com## Clipstream
http://clipstream.com
http://www.dsnyc.com          ## DSNY
http://dsnyc.com
http://www.videoclipstream.com/demo
http://www.videoclipstream.com/akamai/testclips      #EXP:011201
```

Note that you can comment your authorized domains by typing # and commenting after each authorized domain. Whatever text comes after the # on that line will be ignored.

Upload the AuthorizedDomains.txt file and make note of the URL.

Emailing of SID Encoded and CODEBASE Protected Content

SID and Codebase protected content can be delivered via email. Certain changes must be made to the AuthorizedDomainURL text file to enable emailing of protected content.

The following entries must be added to your AuthorizedDomainURL text file:

```
file:
mailbox
http://mail.
localhost
```

Once these entries are present in your AuthorizedDomainURL text file, people should be able to view your videos sent via email.