
# Getting Set Up

# Contents

# Getting Set Up

To get up and running with Jive Video, you need to install the plugin, configure your firewall, configure video in the application's Admin Console, and then configure Jive to use HTTPS if you'd like.

You may want to configure a few options to get video up and running the way you want it.

## Setting up Your Firewall for Video

When you set up your environment for using Jive Video, you need to make sure your firewall is equipped to pass the video stream and other related assets through it. The following IP address ranges and inbound ports are required to allow the Video service to communicate through your firewall for publishing notifications and playback authentication. You should enable inbound traffic from these addresses on ports 80 and 443.

- 208.122.47.224/27
- 74.63.51.48/28
- 72.251.201.144/28
- 107.6.89.96/28
- 54.241.10.197/28

Videos are streamed using Real Time Messaging Protocol (RTMP), which runs on port 1935. If port 1935 is unavailable, video uses Real Time Messaging Protocol Tunnel (RTMPT), which runs on port 80. Make sure these ports are available for the application to use. For more about this, see Setting up Your Firewall for Twistage CDNs.

If your firewall also limits outbound traffic, please see the table in the Jive Community Video FAQ here, which provides a detailed list of regional IP ranges.

## Configuring Video

If you have the enhanced video feature, you can set up your community to support videos recorded and uploaded by community members. This feature is different from the ability to embed video from other sites such as YouTube or Vimeo.

With this feature, members of the community can upload their own video (even record if they have a webcam). Videos uploaded in this way are visible only within the community, making this a more secure way to share video that's specific to the community.

**Fastpath: Admin Console: Video** > **Preferences**

To configure this feature:

- Enter the license number you received, then click **validate**.

- Select the **Allow webcam** check box if you want people to be able to use their computer's webcam to record video for uploading.
- Choose an image to use as a watermark. Some version of your community's logo is a good choice.
- Select **Autoplay** to automatically play video when a user navigates to the content it's embedded in.

**Supported Formats**

- Supported video container type -- AVI, MOV, WMV, MP4, MPEG, FLV, 3GP, and 3G2.
- Supported video codecs -- All of the popular MPEG-4 variants like DivX, XviD, H.264, 3IVX, and MSMPEG4, plus Windows Media 9.
- Supported audio codecs -- MP2, MP3, WAV, AAC (typically seen in QuickTime files), Windows Media audio, and for mobile devices AMR in both narrow-band and wide-band varieties.

## Allowing or Preventing Embedding from Video Sites

Users can link to or embed videos into the community from video sites such as Vimeo, Veoh, Dailymotion, Google, or YouTube. You can restrict the video web sites where users get their videos by turning off the macro for that site. You can also edit the macro settings to say how to display videos from each site.

**Fastpath:** Admin Console: Spaces > Settings > Filters and Macros

1. In the admin console, on the **Filters and Macros** page, scroll down to the **Macros** section.
2. Locate the video macros, then click **On** next to the video sites you want user to be able to link to from content.
3. To edit the macros for the video sites, click **Settings** next to each video site macro, such as VimeoMacro.
4. Edit the macro settings for how the video displays when content is posted.
5. Click **Save Properties**.

## Configuring to Allow Flash Video Embedding

You can allow Flash video (as SWF files) to be embedded by editing settings for the HTML post-processing filter. This can be useful, for example, when you want to embed Flash video published on a trusted web site. Keep in mind, however, that by allowing content from another domain, you could be creating a security vulnerability. Flash videos are inherently insecure because they allow the execution of JavaScript code, which opens the security vulnerability of cross-site scripting. Be sure to add only domains that you trust.

You can set up the community to enable Flash embedding by configuring the HTML filter on the admin console Filters and Macros page. There, you can allow access to the domain from which people will be embedding Flash video.

**Fastpath:** Admin Console: Spaces > Settings > Filters and Macros

1. In the admin console, on the **Filters and Macros** page, scroll down to the **Post Processing Filters** section.
2. Locate the **HTML** filter, then click **Settings** to display the filter's settings page.
3. In the **allowedDomains** box, add your domain. Do not include any sub-domain in the list; if your video is hosted at http://flash.example.com/, enter only example.com. For example, after your edits the box might include: youtube.com, dailymotion.com, veoh.com, vimeo.com, google.com, example.com.
4. Click **Save Properties**.

#### Embedding Flash Video

People embed Flash SWF files by adding the HTML markup to content.

1. While editing content, click the special formatting button (it looks like **>>**), then click **Insert Raw HTML**.
2. Into the content box this command adds, paste HTML markup for embedding the SWF file. Be sure to include your src URL as well as the width and height of your video.

   Here's an example:

```
<embed src="http://flash.example.com/myflashvideo.swf"
    quality="high" width="300" height="500" allowScriptAccess="always"
    wmode="transparent" type="application/x-shockwave-flash" flashvars=""
    pluginspage="http://www.macromedia.com/go/getflashplayer">
</embed>
```

### Exporting videos

**Fastpath:** Admin Console: System > Settings > Video > Preferences

As an administrator or community manager, you can export a copy of all the videos you have uploaded to your community and save them elsewhere. To do this, Select **Click here to export all videos** to export a file containing your videos. Copies of the videos you uploaded will remain on the Twistage site.

## Using HTTPS for Video

For Jive versions earlier than 4.5, the video player was delivered via a legacy Hypertext Transfer Protocol (HTTP). Although there is no security danger in delivering the player via HTTP, it did create confusing messaging. To solve this problem, Twistage added the ability to deliver the player over Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure (HTTPS). This topic helps you configure the Video plugin for secure delivery of the video player. For more about how Jive achieves secure delivery of the video content itself, refer to Security for Jive Video Communication.

Complete the following steps for video uploads and video player downloads to happen over https:

1. Upgrade to 5.0.1 or later version of the Video plugin.
2. Set the Jive property `video.player.url` to `https://video-svc.jivesoftware.com`.
3. Change outbound firewall rules as necessary to allow the player and videos to navigate through the firewall. For more on this, see Setting up Your Firewall. If your Jive instance is hosted by Jive, you can create a support request to make these changes.

## Security for Jive Video Communication

Jive provides the ability to view videos without sacrificing the security of your instance. Jive also enables you to configure your video instance with additional security features.

The Jive Video plugin enables users to upload videos into Jive. To accomplish this, Jive has partnered with a company called Twistage for video upload, encoding, storage, and playback. In order to play video assets that have been uploaded, Jive uses a flash video player that is provided by Twistage.

### How Jive Makes Video Secure

- Users who view videos must be using a valid Jive instance. Jive uses an encrypted security token to retrieve videos from the Content Delivery Network (CDN) and Twistage. This token is verified with an authentication callback script before the video is played for the user.
- Users who request videos must be authorized to view them. The security token passed from Jive to the CDN/Twistage and back to Jive contains the information regarding whether the user who is viewing the video has permission.
- Videos cannot easily be copied and stored locally.
    - The video plugin uses Real Time Messaging Protocol (RTMP) to stream the video to the flash player. This prevents the video from being cached on the user machine and therefore makes it more difficult to record the video.
    - Even though you can strip the embed code from a Jive video to view the video in a third party page, the token associated with the video is only valid for the configured amount of time and plays. Once one of these values are exceeded, the video no longer plays.
- As a security precaution, most modern web browsers will block from playback any embedded videos that do not support https endpoints. However, most sites that users are likely to embed videos from support https endpoints. Your Jive instance does not have any control over this browser behavior.

### Overview of Security Architecture

The following outlines the request lifecycle for an authenticated RTMP video stream:

1. The user attempts to view a video within Jive.
2. While generating the video page, Jive generates an encrypted security token.
3. When the user clicks play, the player requests the video from the CDN, passing along the security token.
4. The CDN calls Twistage using the video ID and authentication token to verify that it can deliver the requested video content.
5. Twistage calls a script on the Jive instance, called the "authentication callback script", passing it the video ID and the authentication token.
6. The authentication callback script determines whether the provided authentication token is valid for viewing the provided video ID, and accepts or rejects the request with its response code.

7. Twistage responds to the CDN's verification request accordingly, and the CDN delivers the video content to the browser or rejects the request.
8. If your script returned an OK response code, the video plays on the page. If not, it doesn't.

#### How Security Tokens Work

When you open a page that contains the Twistage video player plugin, Jive generates an encrypted single-use security token that it passes to Twistage through the plugin. The token contains the following information:

- The ID of the user requesting the video.
- The object type of the content. This should always be 1100.
- The ID of the video that is requested.
- The current time.

Jive encrypts the security token using Advanced Encryption Standard (AES) encryption and intends for it only to be used once. When you play the video, Jive receives the token back from the CDN via Twistage and validates the following token information:

- Is the user represented by the user ID authorized to view this video?
- Has the token expired? By default tokens will expire after 5 minutes. This timeout can be configured using the 'video.max.token.time' property.
- Have the number of plays allowed by the token been exceeded? By default a token can be used to play the video up to 5 times. This value can be configured using the `video.max.token.plays` property.

## Troubleshooting Tips

You can use the following tips to diagnose issues with Jive Video.

### Videos are no longer available

Changing the jiveURL system property causes your site to lose connection to your Video library. You need to create a Support case to update your Video library with the new URL.