



Adobe

Securing Video Content and Playlists

Adobe® Flash® Media Rights Management Server

May 2008

Version 1.0

© 2008 Adobe Systems Incorporated. All rights reserved.

Adobe® Flash® Media Rights Management Server 1.0 Securing Video Content and Playlists for Microsoft® Windows®, Linux®, and UNIX® Edition 1.1, May 2008

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

Any references to company names, company logos and user names in sample material or sample forms included in this documentation and/or software are for demonstration purposes only and are not intended to refer to any actual organization or persons.

Adobe, the Adobe logo, AIR, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

All other trademarks are the property of their respective owners.

This product contains either BSAFE and/or TPEM software by RSA Security Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)

This product includes software developed by the IronSmith Project (<http://www.ironsmith.org/>).

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Notice to U.S. Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Contents

About this document.....	4
Who should read this document?	4
Conventions used in this	4
Additional information.....	4
.....	5
1 Workflow and configuration	6
Requirements.....	6
Installed files.....	7
Configuration file.....	7
Common properties.....	7
Rights Manager properties	8
Media Packager properties.....	8
AMOD Signer properties	9
2 Working with policies.....	10
Using Rights Manager.....	10
Viewing a list of policies.....	10
Creating and updating policies.....	11
Creating a policy.....	11
Updating a policy.....	12
Options for creating and updating policies	13
3 Packaging media files	16
Using Media Packager	16
Encrypting FLV files	16
Applying a policy.....	17
4 Signing playlists.....	18
Using AMOD Signer.....	18
Signing playlists.....	18

About this document

This document explains how to use the command-line tools that are provided with Adobe® Flash® Media Rights Management Server to help secure content by performing the following tasks:

- Creating and managing policies
- Encrypting video files
- Signing playlists

Who should read this document?

This document is intended for publishers of video files, who use Flash Media Rights Management Server to protect their content and manage policies.

Conventions used in this

This uses the following conventions:

Name	Description
Brackets []	Indicates an optional item.
<i>code italic</i>	Indicates that you should replace the text in code italic with an actual value.

Additional information

The resources in this table provide additional information about Flash Media Rights Management Server.

For information about	See
The Flash Media Rights Management Server solution, development environment, run-time environment, and each Flash Media Rights Management Server component	Overview
Installing, configuring, and deploying Flash Media Rights Management Server	Installing and Deploying Flash Media Rights Management Server for JBoss Using Turnkey Installing and Deploying Flash Media Rights Management Server for JBoss Installing and Deploying Flash Media Rights Management Server for WebLogic

For information about	See
Managing administrative users and user roles	<u>User Management Help</u>
Installing Flash Media Server	<u>Adobe Flash Media Server Installation Guide</u>
Customizing and configuring Flash Media Server	<u>Adobe Flash Media Server Administration and Configuration Guide</u>
Creating custom service providers for Adobe User Management and Adobe LiveCycle Rights Management	<u>Developing Service Providers</u>
The Java™ interfaces and classes used to create custom service providers	<u>Adobe Flash Media Rights Management Server API Reference (Javadoc)</u>
Securing video content and playlists by using the Flash Media Rights Management Server command line tools	<u>Securing Video Content and Playlists</u>
Delivering content in Adobe Media Player	<u>Adobe Media Player Content Developer Kit</u>
Using Adobe Media Player to find and view content	<u>Adobe Media Player Help</u>

1

Workflow and configuration

Using three command-line tools (Rights Manager, Media Packager, and AMOD Signer), you can create policies, apply policies to video files, encrypt the files, and sign playlists. The high-level steps for performing these tasks are as follows:

1. Set up the [Configuration file](#) on the computer where the Rights Management Server command-line tools are installed.
2. Create a policy by using Rights Manager; a policy identifier is generated. (See [Working with policies](#).) You might need to perform this step only once or a few times. Most users will create a small number of policies and apply the same few policies to many files.
3. Add to the configuration file the policy identifier of the policy you plan to use. (See [Media Packager properties](#).)
4. Package a file by using Media Packager. In this context, *packaging a file* means to encrypt it and apply a policy to it. (See [Packaging media files](#).)
5. Create a playlist that points to the packaged content. (See *Adobe Media Player Content Developer Kit*.)
6. Sign the playlist by using AMOD Signer. (See [Signing playlists](#).)

The playlist and encrypted content are then ready for deployment.

Requirements

The requirements for using the command-line tools are as follows:

- A user with the Services User role on Rights Management Server

Note: Only the user who creates a policy can view it, modify it, and apply it to files by using Media Packager.

- Signing credentials (certificate and password), issued by Adobe. You need one certificate to encrypt and sign video files and one to sign playlists. For more information about credentials, see *Installing and Configuring Guide*.
- Java Runtime Environment (JRE) version 1.6
- A 32-bit operating system. The tools are not officially supported on 64-bit operating systems (though they may work).

Note: Because of a Java bug, arguments used on the command line, such as filenames or policy names or descriptions, must use only characters from the ISO 8859-1 (Latin-1) character set. For more information and a workaround, see the product ReadMe.

Installed files

The Rights Management Server root installation directory is *[Root directory]/Adobe/FMRMS1.0*. This directory contains a directory called *fmrms_tools*, which contains the default configuration file, *fmrmsstools.properties*, and a *libs* directory, which contains the JAR files for the tools.

Configuration file

The tools require a configuration file that contains information for the tools to use to apply policies, encrypt files, or sign playlists. The default configuration file is *fmrmsstools.properties*, located in the working directory, that is, the directory from which you run the tools (*Root install directory/Adobe/FMRMS1.0/fmrms_tools*). Each tool also contains an option (-c) that lets you point to the configuration file you want to use, if you don't want to use the default. If you don't use the -c option, the tools look for the configuration file in the working directory.

The configuration file uses the Java property file format. If values for any of the properties contain special characters, keep in mind the following restrictions:

- Escape backslashes with an additional backslash. For example, to specify the file *C:\credentials.pfx*, specify it as *C:\\credentials.pfx* or *C:/credentials.pfx*. To specify a file on a network server, specify *\\server\folder\filename.pfx*.
- The configuration file can only contain Latin-1 characters. If you must use non-Latin-1 characters, use the appropriate Unicode escape sequence (using, if you like, the *native2ascii* tool that comes with Java).

For more information, see the Java documentation.

Set values for some properties in the configuration file before you run the tools. For policies, you can set the values for some properties through either Rights Manager or the configuration file. In those cases, values set through Rights Manager take precedence over any values in the configuration file (but they do not overwrite the values).

Note: The tools do not modify values in the configuration file.

The configuration file contains four sections, one for common properties and one for each tool.

Common properties

Common properties relate to the Rights Management Server where policies are administered and stored.

Property	Description
<code>policyServer.server</code>	The URL to your Rights Management Server (for example, <code>http://localhost:8080</code>). This location may or may not be on the same computer where the command-line tools are installed. In either case, the URL must be fully qualified and specify the correct protocol, domain name, and port number of the server.
<code>policyServer.username</code>	The user name of the Rights Management Server administrator user that is used to start web services; the user must have the Services User role.
<code>policyServer.password</code>	The password for this user.

Rights Manager properties

Using Rights Manager, you can create and manage policies. Before you run Rights Manager, set values for Rights Manager properties in the configuration file. The configuration file specifies information that will be applied to all policies.

The configuration file specifies the following properties:

Property	Description
policy.defaultExternalAuthorizer	The name of the external authorization handler. You can specify the name of the handler you created and specified in component.xml, or you can specify <code>AllowAllAuthorizer</code> , the handler provided with Flash Media Rights Management Server (in the root install directory).
policy.defaultUserDomain	Default domain name for user authentication. This value is the domain name specified by the external authentication provider (used for identity-based licenses). Users in the specified domain can access content protected by this policy.
policy.maxResults	An integer indicating how many policies to return when using the <code>list</code> command. The default is 100. If you change the default value, Adobe recommends that you set a value higher than the actual number of policies you have.

Media Packager properties

Using Media Packager, you can specify what data in the file to encrypt and the policy to apply to the content file. For example, you can specify that the video data is encrypted but the audio data is unencrypted.

Before you run Media Packager, specify values for the Media Packager properties. The configuration file specifies the following properties:

Property	Description
encrypt.contents.video.keyframe	Indicates whether to encrypt video keyframes.
encrypt.contents.video.interframe	Indicates whether to encrypt video interframes.
encrypt.contents.video.disposable	Indicates whether to encrypt video disposable frames.
encrypt.contents.audio	Indicates whether to encrypt audio.
encrypt.contents.script	Indicates whether to encrypt script data. <code>onMetaData</code> script data tags at timestamp 0 are never encrypted, even if this option is enabled.
encrypt.keys.policyServer.policy ID	ID of the policy to apply to the FLV file when Media Packager is run. You can get the policy ID or create policies by using Rights Manager.
encrypt.keys.policyServer.domainName	(Optional) The Rights Management Server domain name for user authentication (required only if you are using an external authentication provider to enable identity-based licenses).

Property	Description
encrypt.URL	Optional URL to which players that do not support Adobe digital rights management direct the user. Applies only to F4V content.
encrypt.sign.certfile	The certificate file used to digitally sign this content. For information on correctly specifying file paths, see Configuration file .
encrypt.sign.certpass	The password used for the digital certificate to sign this content.

AMOD Signer properties

AMOD Signer properties are used by AMOD Signer. (AMOD stands for Adobe Media Orchestration Document.) They contain the name of the certificate file and password used to sign the playlist. Set these properties before you run AMOD Signer.

Property	Description
sign.certfile	The name of the certificate file. For information on correctly specifying file paths, see Configuration file .
sign.certpass	The password for this certificate

2

Working with policies

Using Rights Management Server, content providers can apply policies to FLV files and F4V files. Using Rights Manager, administrators can create, list, view details of, and update policies.

A *policy* defines how users can view content; it is a collection of information that includes security settings, authorized users, and usage rights. When policies are applied, encryption and signing allow content providers to maintain control of their content no matter how widely it is distributed. Encrypted files can be delivered using Flash Media Server or over an HTTP server. They can be downloaded and played in Adobe Media Player or custom players built with Adobe AIR™.

You can accomplish the following tasks using Rights Manager:

- [Viewing a list of policies](#)
- [Viewing policy details](#)
- [Creating and updating policies](#)

Using Rights Manager

Before using Rights Manager, ensure that you fulfill the requirements listed in [Requirements](#) and that the configuration file contains the required information (see [Configuration file](#)).

Rights Manager is installed in `[install directory]/Adobe/FMRMS1.0/fmrms_tools/libs`. To run the tool, use the following syntax:

```
java -jar libs/AdobeRightsManager.jar command options
```

where *command* is the command you want to perform and *options* are flags you can set on the command.

Viewing a list of policies

You can view a list of active policies using the `list` command. When you have a list of policies, you can use the `detail` command to view the details of a particular policy.

- To view a list of policies, on the command line, type the following string:

```
java -jar libs/AdobeRightsManager.jar list
```

- To configure how many policies are returned when you use the `list` command, set `policy.maxResult` in the configuration file for [Rights Manager properties](#). (Adobe recommends that you set `maxResult` to a value that is higher than your actual number of policies.)
- (Optional) To specify the configuration file that is used, use the `-c` option. (See [-c configfile](#).)

Viewing policy details

You can get the details of a particular policy using the `detail` command and either the ID or the name of the policy. You can also get the details of all available policies using the `detail all` command.

- To get the details of a particular policy, on the command line, type the following string:

```
java -jar libs/AdobeRightsManager.jar detail policy_ID|policy_name
```

For example, to get the details on the policy with ID 123456ABC and name AdobePolicy1, type either

```
java -jar libs/AdobeRightsManager.jar detail 123456ABC
```

or

```
java -jar libs/AdobeRightsManager.jar detail AdobePolicy1
```

- To get the details of all available policies (useful if you have only a small number of policies), on the command line, type the following string:

```
java -jar libs/AdobeRightsManager.jar detail all
```

- (Optional) To specify the configuration file that is used, use the `-c` option. (See [-c configfile.](#))

Creating and updating policies

[Creating a policy](#)

[Updating a policy](#)

[Options for creating and updating policies](#)

Creating a policy

[Creating an anonymous policy](#)

[Creating a policy with an external authorization handler](#)

[Creating a policy with a publisher ID and application ID](#)

To create a policy, use the `new` command. On the command line, type the following string:

```
java -jar libs/AdobeRightsManager.jar new -n options
```

When the policy is created, the ID of the new policy is displayed. You can specify this policy ID when you use Media Packager to apply this policy to a piece of content.

For new policies, set the following options:

- The policy name (-n). If the name contains spaces, it must be enclosed in quotes.
- The authorization handler (-z). Can be specified on the command line or in the configuration file. If you are not using a custom external authorization handler, you can specify `AllowAllAuthorizer`. See [Creating a policy with an external authorization handler.](#)
- The access method (-x, anonymous; or -m, all users in domain). If -m is specified, be sure to also specify a domain, which can also be specified in the configuration file.

For additional options that you can specify with this command, see [Options for creating and updating policies.](#)

Creating an anonymous policy

An anonymous policy does not require users to log in to access content. Use the `-x` option, and also specify an authorization handler (in the following example, `AllowAllAuthorizer` is used).

```
java -jar libs/AdobeRightsManager.jar new -n MyNewPolicy -x -z
AllowAllAuthorizer
```

Creating a policy with an external authorization handler

An external authorization handler provides centralized access control for video files. You can create an external authorization handler by using the service provider interface (SPI), or you can use the `AllowAllAuthorizer` SPI that is provided with Rights Management Server. Whatever authorization handler you use, install it first; for more information, see *Developing Service Providers*.

You can either set the authorization handler name in the configuration file, or on the command line, use the `-z` option and specify the name, as in the following example:

```
java -jar libs/AdobeRightsManager.jar new -n MyNewPolicy -z MyAuthorizer -x
```

You must also specify the access method; in the example, anonymous access is specified.

If you specify the authorization handler name on the command line, the value specified takes precedence over the value in the configuration file.

Creating a policy with a publisher ID and application ID

You can restrict which applications can access content that is protected with this policy. Use the `-a` option and specify a publisher ID and, optionally, an application ID and minimum and maximum versions. The following example restricts access to applications with the following specifications:

- Publisher ID = `4875E02D9FB21EE389F73B8D1702B320485DF8CE.1`
- Application ID = `com.adobe.amp`
- Minimum version of 1.0 and maximum of 2.0

```
java -jar libs/AdobeRightsManager.jar new -n MyNewPolicy -a
4875E02D9FB21EE389F73B8D1702B320485DF8CE.1:com.adobe.amp:1.0:2.0
```

For more information and additional examples, see [-a publd \[:appld\[:\[min\]:\[max\]\]\]](#).

Updating a policy

To update an existing policy, use the `update` command and specify either the policy name or the policy ID. On the command line, type the following:

```
java -jar libs/AdobeRightsManager.jar update policy_name|policy_ID options
```

After a policy is updated, the policy allows only access by users in a single domain or anonymous access (any other users in the policy are removed). Default values specified in the configuration file are not used for updates.

For options that you can specify with this command, see [Options for creating and updating policies](#).

Options for creating and updating policies

When creating policies or updating policies, you can specify the following options:

[-a *publd* \[:*appld*\[:*\[min\]*:*\[max\]*\]\]](#)

[-c *configfile*](#)

[-d *description*](#)

[-e \[*date*\]](#)

[-l *days*](#)

[-m *domainName*](#)

[-n *policyName*](#)

[-p *name=value*](#)

[-r \[*days*\]](#)

[-s \[*date*\]](#)

[-v](#)

[-x](#)

[-z *authorizer*](#)

[-zname *value*](#)

-a *publd* [:*appld*[:*[min]*:*[max]*]]

Specifies a publisher ID (*publd*) and application ID (*appld*). Use this option to restrict which applications and versions can access content that is protected with this policy.

Both the publisher ID and application ID are used to identify and certify (digitally sign) an AIR application (such as Adobe Media Player). The publisher ID is derived from the certificate that is used to sign the AIR application. It can be found in the generated publisher ID file (*application_installation_directory*/META-INF/AIR/publisherID). The application ID is in the application.xml file created by the AIR application developer (in the case of Adobe Media Player, the application developer is Adobe).

If no options are specified, all applications can access this content. *min* and *max* version numbers are optional. If used, version numbers must be in *major.minor* format (for example, 1.0 or 2.5). Multiple -a options can be specified to allow multiple applications. See also [Creating a policy with a publisher ID and application ID](#).

When you use this option with the `update` command without any arguments, -a removes all previously specified publishers and application IDs from the list.

Here are some examples that show usage of the -a option.

- With publisher and application ID and minimum/maximum versions specified:

```
-a 4875E02D9FB21EE389F73B8D1702B320485DF8CE.1:com.adobe.amp:1.0:2.0
```

- With publisher and application ID specified, without version information:
`-a 02D88EEED35F84C264A183921344EEA353A629FD.1:com.example.air.test_app`
- With only publisher ID specified:
`-a 02D88EEED35F84C264A183921344EEA353A629FD.1`

For more information on publisher IDs and application IDs, see the following topics in the Adobe AIR documentation:

- [Setting AIR application properties](#)
- [Getting the application and publisher identifiers](#)

-c configfile

Specifies the location of the configuration file. If this option is not used, the tool looks for the configuration file in the working directory. For more information, see [Configuration file](#).

If the file path contains backslashes, escape them with an additional backslash. For example, to specify the file `C:\folder\myconfig.properties`, specify it as `C:\\folder\\myconfig.properties` or `C:/folder/myconfig.properties`. To specify a file on a network server, specify `\\server\folder\myconfig.properties`.

This option can also be used for the `list` and `detail` commands.

-d description

A description for this policy. If a description includes spaces, it must be enclosed in quotes. For example, any of the following descriptions are valid:

- `PolicyForVideoAuthoredByAdobe`
- `Policy_For_Video_Authored_By_Adobe`
- `"Policy for video authored by Adobe"`

-e [date]

Year, month, day, and (optionally) time of the policy end date (date on which all content that is protected with this policy expires). Specify as `yyyy-mm-dd` or `yyyy-mm-dd-hr:min:sec`, where `hr` is the hour in 24-hour format. For example, specify `2008-12-1` or `2008-12-1-00:00:00` for midnight on December 1, 2008. This option cannot be used with `-r`. The maximum value for `date` is `2029-12-31`.

When you use this option with the `update` command, you can remove the end date from the policy by not specifying a date.

-l days

Offline lease period (number of days a license is valid after initial user download). The value can be set to 0 if you do not want the client to access the content offline. If a value is not specified, the default value, 365, is used. The maximum value is 32767.

-m domainName

Specifies that users in this domain can access content. This value is the domain name specified by the external authentication provider (used for identity-based licenses). For more information on specifying the domain name, see *Installing and Configuring Adobe Flash Media Rights Management Server*. For new policies, the default domain can be specified in the configuration file, but the value given on the command line takes precedence. This option cannot be used with `-x`.

-n *policyName*

A unique name for this policy. Required for new policies. If a name includes spaces, it must be enclosed in quotes. For example, any of the following names are valid:

- MyPolicy
- My_Policy
- "My Policy"

-p *name=value*

Adds a custom property to the policy. You can specify multiple custom properties. When you use this option with the update command, use -p without any arguments to remove all properties.

-r [*days*]

Relative policy duration (number of days content that is protected with this policy is valid). The duration begins when you run Media Packager on the content. This option cannot be used with -e or -s. The maximum value is 9999.

When you use this option with the `update` command, you can remove the duration by not specifying the number of days.

-s [*date*]

Year, month, day, and (optionally) time that the policy takes effect (date on which all content that is protected with this policy can start being used). Specify as *yyyy-mm-dd* or *yyyy-mm-dd-hr:min:sec*, where *hr* is the hour in 24-hour format. For example, specify 2008-12-1 or 2008-12-1-00:00:00 for midnight on December 1, 2008. This option cannot be used with -r. When you use this option with the update command, you can remove the start date by not specifying a date.

-v

Prints the version information of the tool; can be used independently of any command.

-x

Allows anonymous access. Anonymous access allows users to access content without providing a user name and password (the opposite of identity-based licensing). This option cannot be used with -m and cannot be used with the `update` command. See also [Creating an anonymous policy](#).

-z *authorizer*

Name of the external authorization handler in Rights Management Server. For new policies, you can specify a default value in the configuration file, but the value given on the command line takes precedence. See also [Creating a policy with an external authorization handler](#).

-zname *value*

Name-value pairs, if the authorization handler requires additional properties. You can specify default values in the configuration file, but the values given on the command line take precedence. You can specify multiple -zname options if multiple authorizer properties exist.

3

Packaging media files

Packaging refers to the process of encrypting and applying a policy to FLV files or F4V files. Use Media Packager to package files.

When a file is encrypted, its contents cannot be parsed without the appropriate user license or token, or outside the Adobe Media Player or other AIR application. Flash Media Rights Management Server allows you to select which parts of the file to encrypt (see [Configuration file](#)). Because Flash Media Rights Management Server can parse the file format of the video, it can intelligently encrypt selective parts of the video file, rather than the entire file as a whole. Data such as metadata and cue points can remain unencrypted, so search engines can still search the file.

If identity-based licensing is used, passwords ensure that only authorized users can open and view media. The user must specify the password before the media can be viewed using Adobe Media Player or other AIR applications.

Using Media Packager

Before using Media Packager, ensure that you fulfill the requirements listed in [Requirements](#) and that the configuration file contains the required information (see [Configuration file](#)).

Media Packager is installed in `[install directory]/Adobe/FMRMS1.0/fmrms_tools/libs`. Media Packager uses the following syntax:

```
java -jar libs/AdobePackager.jar sourcefile destfile [options]
```

where *sourcefile* is the file to encrypt and *destfile* is the destination where the encrypted contents are written. If *destfile* is a directory, the encrypted file is saved in this folder, using the same filename as the source file. Otherwise, ensure that *sourcefile* and *destfile* have different filenames. Adobe recommends that you store your source files and destination (encrypted) files in different directories. To specify a network location, specify it as follows: `\\server\folder\filename.extension`

Note: Packaging a file in a network location might take longer than packaging a file locally.

Encrypting FLV files

To encrypt an FLV file or F4V file, on the command line, type the following:

```
java -jar libs/AdobePackager.jar sourcefile destfile [options]
```

You can use the following options with this command:

-c *configfile*

Specifies the location of the configuration file. If you do not use this option, the tool looks for the default configuration file in the working directory. For more information, see [Configuration file](#).

-i contentID

Specifies an ID for this content. This ID is used by the external authorization handler to determine whether a user is authorized to view this content. If you do not specify an ID, the tool uses the filename specified in the *destfile* path as the content ID. For example, if *destfile* is C:/flvs/video.flv, the default content ID is video.flv.

-o

If the destination file exists, overwrites that file without prompting.

-s

Turns off prompts for commands, such as the prompt to confirm whether the destination file is overwritten.

-v

Prints version info; can be used independently of a command.

Applying a policy

Before you run Media Packager, specify the ID of a policy in the configuration file (see [Media Packager properties](#)). When you run Media Packager, the tool automatically applies that policy to the file. You do not need to run a special command.

4

Signing playlists

Using AMOD Signer, you can sign playlists. Signatures protect playlists within Adobe Media Player from being tampered with, ensuring that the integrity of the playlist is protected. For more information about playlists, see the *Adobe Media Player Content Developer's Kit*.

Note: Currently, signing is only supported for content that is viewed within Adobe Media Player.

Using AMOD Signer

Before using AMOD Signer, ensure that you fulfill the requirements listed in [Requirements](#) and that the configuration file contains the required information (see [Configuration file](#)).

AMOD Signer is installed in `[install directory]/Adobe/FMRMS1.0/fmrms_tools/libs`. AMOD Signer uses the following syntax:

```
java -jar libs/AdobeMODSigner.jar sourcefile destfile [options]
```

where *sourcefile* is the AMOD file to sign and *destfile* is where the signed AMOD file is written to. If *destfile* is in a directory that is different from the source file directory, the signed playlist is saved in this directory, using the same filename as the source file. Otherwise, ensure that *sourcefile* and *destfile* have different filenames. Adobe recommends that you store your source files in one directory and your destination (signed) files in another directory. To specify a network location, specify it as follows:
\\server\folder\filename.extension

Signing playlists

To sign a playlist, on the command line, type the following:

```
java -jar libs/AdobeMODSigner.jar sourcefile destfile [options]
```

You can specify the following options:

-c

Specifies the location of the configuration file. If this option is not specified, the tool looks for the default configuration file in the working directory. For more information, see [Configuration file](#).

-o

If the destination file exists, overwrite that file without prompting.

-s

Turns off prompts for commands, such as the prompt to confirm whether the destination file is overwritten.

-v

Prints the version information for the tool.