The Java™ Tutorials

Trail: Deployment
Lesson: Packaging Programs in JAR Files
Section: Working with Manifest Files: The Basics

The Java Tutorials have been written for JDK 8. Examples and practices described in this page don't take advantage of improvements introduced in later releases.

Enhancing Security with Manifest Attributes

The following JAR file manifest attributes are available to help ensure the security of your applet or Java Web Start application. Only the `Permissions` attribute is required.

- The `Permissions` attribute is used to ensure that the application requests only the level of permissions that is specified in the applet tag or JNLP file used to invoke the application. Use this attribute to help prevent someone from re-deploying an application that is signed with your certificate and running it at a different privilege level.

  This attribute is required in the manifest for the main JAR file. See Permissions Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Codebase` attribute is used to ensure that the code base of the JAR file is restricted to specific domains. Use this attribute to prevent someone from re-deploying your application on another website for malicious purposes. See Codebase Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Application-Name` attribute is used to provide the title that is shown in the security prompts for signed applications. See Application-Name Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Application-Library-Allowable-Codebase` attribute is used to identify the locations where your application is expected to be found. Use this attribute to reduce the number of locations shown in the security prompt when the JAR file is in a different location than the JNLP file or the HTML page. See Application-Library-Allowable-Codebase Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Caller-Allowable-Codebase` attribute is used to identify the domains from which JavaScript code can make calls to your application. Use this attribute to prevent unknown JavaScript code from accessing your application. See Caller-Allowable-Codebase Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Entry-Point` attribute is used to identify the classes that are allowed to be used as entry points to your RIA. Use this attribute to prevent unauthorized code from being run from other available entry points in the JAR file. See Entry-Point Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Trusted-Only` attribute is used to prevent untrusted components from being loaded. See Trusted-Only Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

- The `Trusted-Library` attribute is used to allow calls between privileged Java code and sandbox Java code without prompting the user for permission. See Trusted-Library Attribute in the Java Platform, Standard Edition Deployment Guide for more information.

See Modifying a Manifest File for information on adding these attributes to the manifest file.

Previous page: Sealing Packages within a JAR File
Next page: Signing and Verifying JAR Files