Java-Inhalte im Browser — Sicherheitsänderungen

Dieser Artikel gilt für:

- **Plattform(en):** Alle Plattformen
- **Java-Version(en):** 7.0, 7u21

Entwickler: Nach dem Stand von 7u51 (Januar 2014) müssen Ihre Rich Internet Applications (RIAs, auch als Applets und Web Start-Anwendungen bekannt) aktualisiert werden. Die erforderlichen Updates betreffen Packaging und Verteilung; API-Codeänderungen sollten nicht erforderlich sein. Der Auslöser für diese Änderungen bezieht sich auf die **mögliche Neuausrichtung von Sandbox-Anwendungen (http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/no_redeploy.html)** , durch die eine Änderung Ihrer angegebenen Berechtigungsstufe nach dem Platzieren von Berechtigungen innerhalb einer signierten Java-Archivdatei (JAR-Datei) nicht mehr möglich ist.
RIAs müssen zwei Dinge enthalten:

1. Code-Signaturen einer vertrauenswürdigen Quelle. Alle Codes für Applets und Web Start-Anwendungen müssen signiert sein, unabhängig von den Berechtigungsattributen des jeweiligen Codes.
2. Manifestattribute
   a. Berechtigungen – Eingeführt in 7u25, erforderlich ab 7u51. Gibt an, ob die RIA innerhalb der Sandbox ausgeführt werden oder volle Berechtigungen erfordern soll.
   b. Codebase – Eingeführt in 7u25 und optional/empfohlen ab 7u51. Zeigt auf den bekannten Speicherort des gehosteten Codes.

Weitere Informationen finden Sie im **Produktmanagement-Blog der Java-Plattform-Gruppe (https://blogs.oracle.com/java-platform-group/entry/new_security_requirements_for_rias)** .

Java 7 Update 45 (7u45), Oktober 2013: LiveConnect-Aufrufe erfordern vor der Interaktion mit Rich Internet-Anwendungen eine Bestätigung

- Benutzer werden aufgefordert, Berechtigungen für Webseiten (Domains) zu erteilen, die über JavaScript LiveConnect mit Java-Anwendungen interagieren.
- Entwickler müssen das Manifestattribut `Caller-Allowable-Codebase` hinzufügen, um die Verzeichnisse zu kennzeichnen, aus denen der JavaScript-Code Methoden in der Anwendung aufrufen darf

Java 7 Update 40 (7u40), September 2013: Systemadministratoren dürfen Anwendungen innerhalb ihrer verwalteten Desktops auf die weiße Liste setzen

- Systemadministratoren dürfen bestimmte Java-Anwendungen mithilfe von Deployment-Regelgruppen zur Ausführung auf Benutzerrechnern auf die weiße Liste setzen. Weitere Informationen finden Systemadministratoren in der **Dokumentation der Deployment-Regelgruppe (http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/deployment_rules.html)** oder über die Beispiele zu den Deployment-Regelgruppen.

Java 7 Update 21 (7u21), April 2013: Alle Java-Inhalte, auf die über den Browser zugegriffen wird (einschließlich Applets und Anwendungen), erfordern eine Bestätigung, bevor sie ausgeführt werden können.

- Die in dem Prompt enthaltene Meldung variiert je nach Risikofaktoren bei der Ausführung einer Anwendung. Lesen Sie die **FAQ zu Sicherheitsdialogfeldern (/de/download/help/appsecuritydialogs.xml)** für einen Überblick über die allgemeinen Sicherheitsmeldungen.
- Bei Szenarios mit geringerem Risiko werden nur wenige Meldungen angezeigt. Sie umfassen ein Kontrollkästchen, mit dem

die Anzeige dieser Meldungen beim nächsten Zugriff auf die Anwendung unterdrückt wird.
- Szenarios mit höherem Risiko, wie die Ausführung von Anwendungen ohne identifizierendes digitales Zertifikat, erfordern zusätzliche Maßnahmen.

Für Entwickler und Systemadministratoren sind **weitere technische Informationen über Änderungen bei signiertem Code (http://www.oracle.com/technetwork/java/javase/tech/java-code-signing-1915323.html)** verfügbar.

Welche Auswirkung haben diese Änderungen?

Zusammengenommen ermöglichen es diese Änderungen Benutzern, den Softwareanbieter zu verifizieren und die Interaktion mit der Anwendung zu bestätigen. Die Verwendung von Codesignaturzertifikaten ermöglicht es Java, präzise Informationen zum Anwendungshersteller bereitzustellen, die den Benutzern bei der Entscheidung helfen, ob die Anwendung ausgeführt werden soll.

Kann ich die Java-basierten Anwendungen, die ich normalerweise ausführe, trotz dieser Änderungen weiter verwenden?

Die beschriebenen Änderungen wirken sich nicht negativ auf Anwendungen aus, die Sie normalerweise ausführen. Möglicherweise werden Sie jedoch aufgefordert, eine explizite Genehmigung zur Ausführung der Anwendung zu erteilen, indem Sie auf eine Schaltfläche "Ausführen" klicken. Dadurch erhalten Sie die Möglichkeit, die automatische Ausführung von Anwendungen mit hohem Risiko auf Ihrem Computer zu verhindern.

Systemadministratoren, die um Kompatibilität besorgt sind, können mithilfe der Funktion **Deployment-Regelgruppe (/de/download/faq/deployment_rule.xml)** bestimmte Rich Internet-Anwendungen über verwaltete Desktops hinweg auf eine weiße Liste setzen.

Warum wird die Option *Diese Meldung nicht wieder für diese Anwendung anzeigen* nicht im Sicherheitsdialogfeld für eine nicht signierte Anwendung angezeigt?

Ab Java 7 Update 40 ist die Option **Diese Meldung nicht wieder für diese Anwendung anzeigen** nicht mehr verfügbar. Im Gegensatz zu vorherigen Versionen kann der Benutzer das Sicherheitsdialogfeld für eine nicht signierte Anwendung nicht mehr unterdrücken. Er muss jedes Mal die Option **Ich akzeptiere das Risiko und möchte diese Anwendung ausführen** wählen, um die nicht signierte Anwendung auszuführen.

Was ist eine Certificate Authority?

Eine Certificate Authority ist eine vertrauenswürdige Organisation, im Allgemeinen ein kommerzielles Unternehmen, das digitale Zertifikate ausstellt. Die Zertifikate werden an Unternehmen oder Einzelpersonen ausgegeben, nachdem deren Identität geprüft wurde. Das digitale Zertifikat wird Computeranwendungen hinzugefügt, um zu validieren, dass die Anwendung vom Eigentümer des Zertifikats stammt. Weitere Informationen finden Sie unter **http://wikipedia.org/wiki/Certificate_authority (http://wikipedia.org/wiki/Certificate_authority)** .

Warum sind diese Änderungen wichtig für mich?

Java im Browser ist ein beliebtes Angriffsziel. In 2012 hat Java 7u10 Sicherheitsfunktionen eingeführt, mit denen Sie die Ausführung von Java-Anwendungen ausdrücklich genehmigen müssen. Sie können Java auch so konfigurieren, dass die Ausführung von nicht vertrauenswürdigen Anwendungen blockiert wird. Vertrauenswürdige Anwendungen umfassen ein gültiges digitales Zertifikat, das von einer Certificate Authority ausgestellt wurde, und stellen somit Informationen über die Identität des Anwendungsproviders bereit. Mit diesen Zertifikaten kann Java die Sicherheit der Anwendungen verbessern, die von diesen Providern erstellt wurden.

Welche zusätzlichen Schritte kann ich ausführen, um die Sicherheit der Systeme sicherzustellen, die Java-Anwendungen im Browser ausführen?

Es wird unbedingt empfohlen, dass Java-Benutzer, Systemadministratoren und Entwickler ihre Systeme mit den neuesten Versionen auf dem neuesten Stand halten. Das automatische Java-Updateverfahren soll sicherstellen, dass Java-Benutzer immer mit den neuesten Sicherheitsfixes auf dem neuesten Stand sind.

Wenn Sie das automatische Updateverfahren deaktiviert haben, reaktivieren Sie es, um sicherzustellen, dass Sie die neueste und sicherste Java-Installation in Ihrem System haben. Weitere Informationen finden Sie in den **FAQ zum automatischen Update von Java 6 auf Java 7 (http://www.oracle.com/technetwork/java/javase/documentation/autoupdate-1667051.html)** .

Endbenutzer	**Java - Hilfe (/de/download/help)** (Java.com) **Einstellungen für die Sicherheitsebenen im Java Control Panel (/de/download/help/jcp_security.xml)**
Entwickler	**Java SE Security - Richtlinien zur sicheren Codierung (http://www.oracle.com/technetwork/java/seccodeguide-139067.html)** in der Java-Programmiersprache **Manifestattribute in JAR-Dateien für die Sicherheit (http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/manifest.html)** **Java SE 7-Sicherheitsdokumentation (http://docs.oracle.com/javase/7/docs/technotes/guides/security/)** **Technische Informationen zur Änderung des signierten Codes (http://www.oracle.com/technetwork/java/javase/tech/java-code-signing-1915323.html)**
Unternehmen	**Oracle Java SE Support (http://www.oracle.com/us/technologies/java/standard-edition/support/overview/index.html)** bietet rund um die Uhr an 7 Tagen die Woche E-Mail- und telefonischen Support für geschäftskritische Anwendungen **Oracle Java SE Advanced- und Oracle Java SE Suite- (http://www.oracle.com/us/technologies/java/standard-edition/advanced-suite/overview/index.html)** Produkte stellen Unternehmensfunktionen bereit, die die Kosten für Deployment, Überwachung und Wartung von Java-basierten IT-Umgebungen minimieren.
Systemadministrator	**Deployment-Regelgruppen, um Anwendungen auf die weiße Liste zu setzen (http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/deployment_rules.html)** **Best Practices beim Deployment (http://docs.oracle.com/javase/tutorial/deployment/deploymentInDepth/bestPractices.html)** **Java Plug-in Guide for System Administrators (http://docs.oracle.com/javase/7/docs/technotes/guides/plugin/developer_guide/faq/developer.html)** Tutorial: **Security Features in Java SE (http://docs.oracle.com/javase/tutorial/security/)**