# CitiDirect BE℠ Java Security Configuration Guide

December 2013

Treasury and Trade Solutions

# Table of Contents

# Introduction

This document is intended for CitiDirect BE$^{SM}$ end users and IT security administrators of CitiDirect BE users. The information below outlines the configurations required on end users' computer to facilitate the seamless operation of CitiDirect Services after Oracle's Java 1.7 Update 51 release on January 14, 2014. The required steps, as detailed below, will be dependent on the version of Java presently installed on the end user computer.

We strongly recommend upgrading the Java on your workstation to the latest Java version 7 Update 51 as soon as it is released. This version has the latest security fixes and does not require configuration changes to continue to work on CitiDirect Services.

# Issues with new Java Version Release

Whenever Oracle releases a new version of Java for public use, they also change security baselines and configurations that potentially result in CitiDirect BE clients experiencing issues while launching CitiDirect Services or navigating within the CitiDirect Services application. The usual experience is the display of a blank screen while navigating to a specific screen, or JavaScript errors displayed in the CitiDirect Services window. Detailed screenshots are listed in **Appendix – C**.

**Immediately after the release of Java 1.7 Update 51, all users who use Java 1.7 Update 45, with a security setting of "High" in the Java Control Panel will be blocked and will experience problems while navigating to CitiDirect Services.**

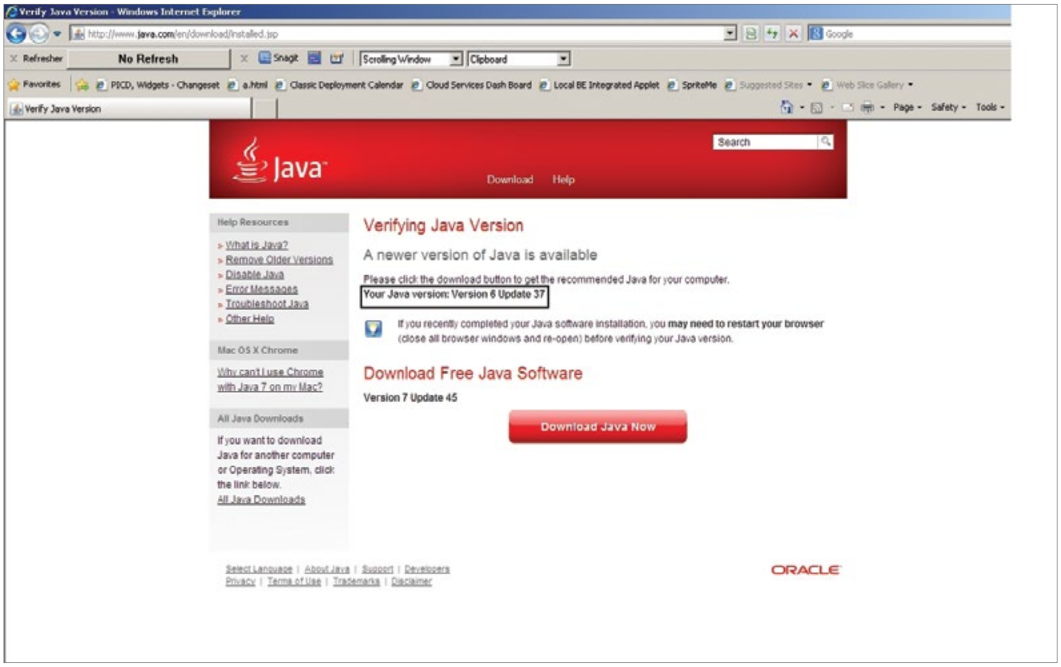
If you experience the above, follow the steps outlined below for specific JRE versions, to resolve the issue.

# What version of Java do I have?

To determine the version of Java currently installed on your computer see the steps below:

- Open Internet Explorer and go to the following website:
  http://www.java.com/en/download/installed.jsp?detect=jre

If Java is correctly installed, it will display the current Java version on your computer similar to the screenshot below.



Verifying Java Version

A newer version of Java is available

Please click the download button to get the recommended Java for your computer.

Your Java version: Version 6 Update 37

If you recently completed your Java software installation, you **may need to restart your browser** (close all browser windows and re-open) before verifying your Java version.

Why can't I use Chrome with Java 7 on my Mac?

If you want to download Java for another computer or Operating System, click the link below.
All Java Downloads

Download Free Java Software

Version 7 Update 45

Based on the Java version installed, select the relevant link from the list below to view the actions required to resolve your issue.

- Java 1.6 (Version 6 Update XX – Any update level)
- Java 7 Update 01 to Update 09 ( 1.7 Update 01 to 1.7 Update 09)
- Java 7 Update 10 to Update 25 (1.7 Update 10 to 1.7 Update 25)
- Java 7 Update 40 (1.7 Update 40)
- Java 7 Update 45 (1.7 Update 45)
- Java 7 Update 51 (1.7 Update 51)

# Java 7 Versions

Based on the minor version installed (Update 01 to Update 51), the actions to be taken vary and are listed below:

## Java 7 Update 51 (1.7 Update 51)

This is the latest and most secure version of Java. There are no actions required to continue working with CitiDirect Services.

## Java 7 Update 45 (1.7 Update 45)

Users with Java 7 Update 45 have three options to continue working with CitiDirect Services:

a. Upgrade the Java version to Java 7 Update 51

b. Modify the security slider setting in the Control Panel ▶ Java to be at Medium level as shown in **Appendix A**

c. Contact your system administrator/network administrator team to install a deployment rule set as detailed in **Appendix B**

## Java 7 Update 40 (1.7 Update 40)

Users with Java 7 Update 40 have three options to continue working with CitiDirect Services:

a. Upgrade the Java version to Java 7 Update 51

b. Modify the security slider setting in Control Panel ▶ Java to be at Medium level as shown in **Appendix A**

c. Contact your system administrator/network administrator to install a deployment rule set as detailed in **Appendix B**

## Java 7 Update 10 to Update 25 (1.7 Update 10 to 1.7 Update 25)

Users with Java 7 Update 10 to Java 7 Update 25 have two options to continue working with CitiDirect Services.

a. Upgrade the Java version to Java 7 Update 51

b. Modify the security slider setting in Control Panel ▶ Java to be at Medium level as shown in **Appendix A**

## Java 7 Update 01 to Update 09 (1.7 Update 01 to 1.7 Update 09)

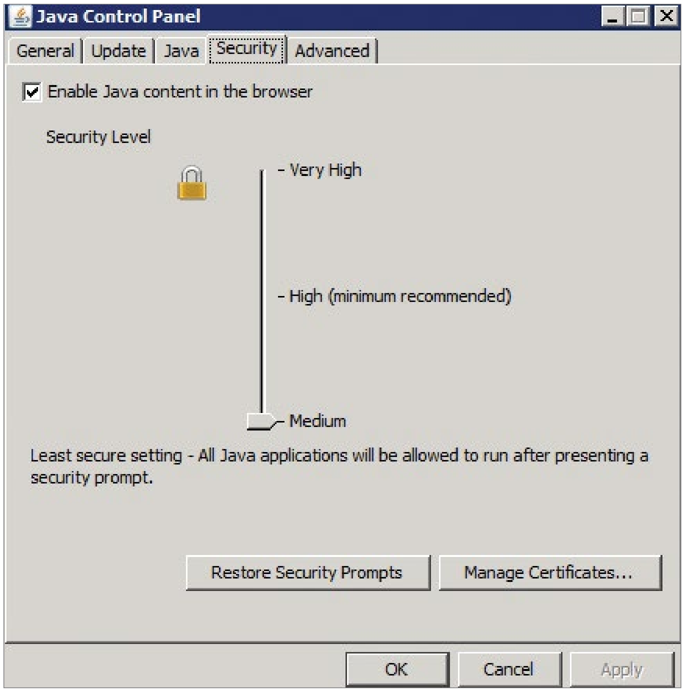
Users with Java 7 Update 01 to Update 09 versions are not required to perform any further actions to work with CitiDirect Services.

# Java 6 Versions (1.6 Update XX)

Users with Java 1.6 versions are not required to perform any further actions to work with CitiDirect Services.

# Appendix A – Modify Security Slider to Medium

In your computer, navigate to Control Panel ▶ Java. If you are using 32-bit Java in a 64-bit workstation such as Windows 7, navigate to Java settings using Control Panel ▶ View 32-bit Control Panel Items ▶ Java. Proceed to the "Security" tab and move the slider to **Medium**.



☑ Enable Java content in the browser

Security Level

- Very High

- High (minimum recommended)

- Medium

Least secure setting - All Java applications will be allowed to run after presenting a security prompt.

# Appendix B – Deployment Rule Set Installation

System Administrators: Follow the steps outlined below to create a deployment rule set for your workstation environment.

## Where is this applicable?

Users with Java 1.7 Update 40 and above can utilize the Java Deployment Rule set facility to minimize warnings shown when launching CitiDirect Services.

## Prerequisites

System administrators should digitally sign JAR file and push them (copy) to individual workstations that have Java 1.7 Update 40 and above. More technical information about the steps listed below is available at **https://blogs.oracle.com/java-platform-group/entry/introducing_deployment_rule_sets**

## Sample Steps

a. Create Deployment Rule Set JAR. The JAR file includes the ruleset.xml file which contains the CitiDirect BE URLs which are to be trusted by the Java runtime on the user workstation. The contents required in the ruleset.xml file for trusting all URLs of CitiDirect BE is shown below. **This data is a sample and system administrators are encouraged to create a similar XML file containing all the trusted URLs used by trusted Java Applets running in the client environment.**

```
<ruleset version="1.0+">
        <rule>
                <id location="https://citidirectportal.citidirect.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://europe.citidirectportal.citidirect.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://citidirectportalasia.citidirect.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://citidirectbeportalnam.citidirect.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://citidirectbeportalemea.citidirect.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://citidirectbeportalasia.citidirect.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://citidirect-eb.citcorp.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://asia.citidirect-eb.citcorp.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://europe.citidirect-eb.citcorp.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id location="https://us.citidirect.citcorp.com" />
                <action permission="run" />
        </rule>
        <rule>
                <id /><!-- Because this is both blank and shown last, it will be
the default policy. -->
                <action permission="default">
                        <message>Access for Applet is blocked. Please contact
system administrator.</message>
                </action>
        </rule>
</ruleset>
```

b. Create the xml file in C: drive – called ruleset.xml.

c. Create a JAR file with this xml file using the commands similar to the following from the command prompt after navigating to C:\

   ```
   jar -cvf DeploymentRuleSet.jar ruleset.xml
   ```

d. This creates the following file C:\DeploymentRuleset.jar

e. This JAR file should now be digitally signed with a valid certificate procured from a certificate authority. An example command that can be run from the command prompt to sign this JAR with a certificate named testcertstore.jks is shown below:

   ```
   jarsigner -verbose -keystore “c:\testcertstore.jks” -signedjar DeploymentRuleSet.jar
   DeploymentRuleSet.jar
   ```

   More details about jarsigner is available at
   http://docs.oracle.com/javase/6/docs/technotes/tools/windows/jarsigner.html

   The output of Jar signer is similar to

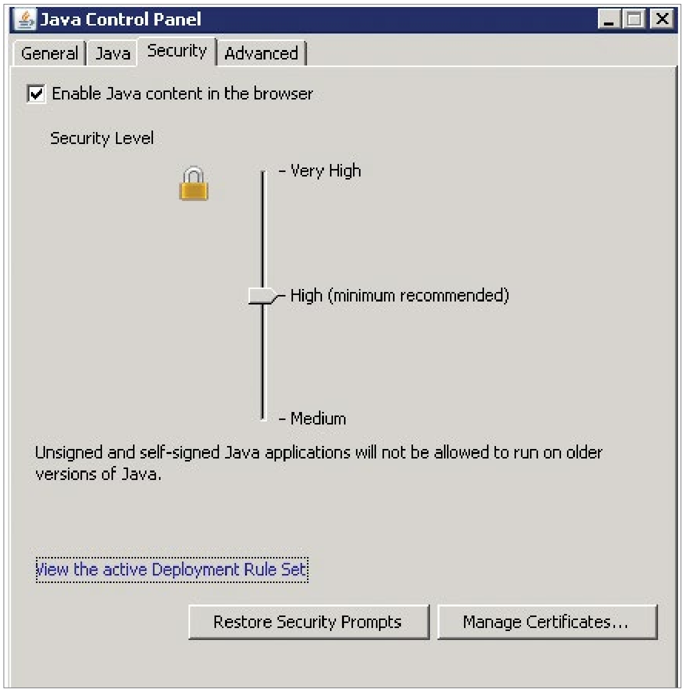
   ```
   Enter Passphrase for keystore:
   updating: META-INF/MANIFEST.MF
   adding: META-INF/mycompanycert.SF
   adding: META-INF/mycompanycert.RSA
   signing: ruleset.xml
   ```

   **How does my company procure a digital certificate?** Digital certificates can be procured from authorities such as Verisign, Thawte – www.verisign.com, http://www.entrust.net/ssl-cert-comparisons.htm

f. After creating the signed JAR, desktop administrators should copy the DeploymentRuleSet.jar to the common area so that rules are enforced for all users, across Java updates.

   That area is:
   **Windows:** C:\Windows\Sun\Java\Deployment
   **Mac, Linux, Unix:** /etc/.java/deployment

g. Successful installation of the deployment rule set can be validated by navigating to Control Panel ▶ Java ▶ Security. A link named – "**View the active Deployment Rule Set**" will be available. On clicking, the XML file will be displayed which details the security settings for Java runtime. If the DeploymentRuleset.jar is not correctly copied, this link will not be displayed in the Control panel's security tab.



☑ Enable Java content in the browser

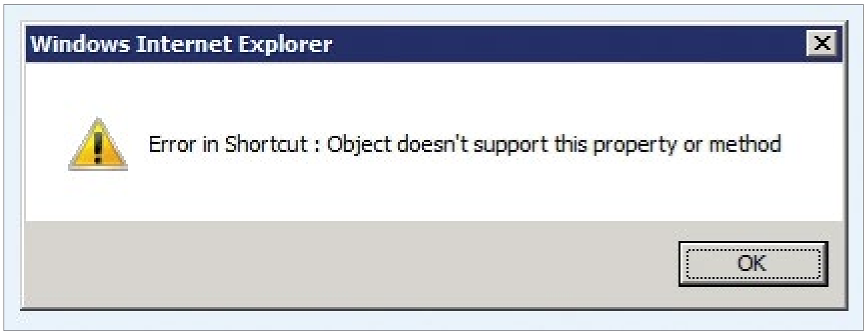
Security Level: High (minimum recommended)

Unsigned and self-signed Java applications will not be allowed to run on older versions of Java.

# Appendix C – Issue Screenshots after Oracle's release of new version of Java

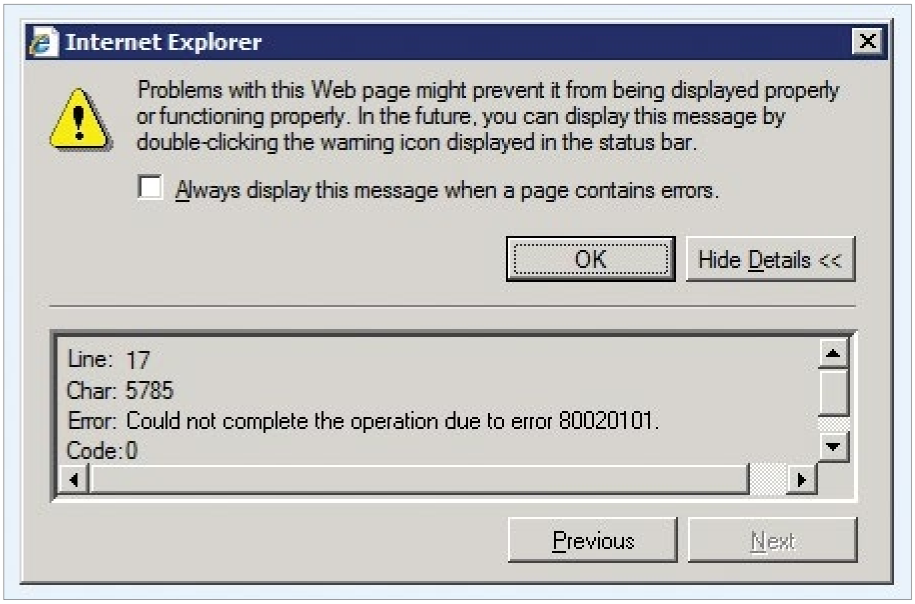
CitiDirect BE users will get Javascript errors/alerts while accessing CitiDirect Shortcuts from BE Portal or CitiDirect Services with Java 1.7 versions lower than Java 1.7 Update 51

Error from Shortcut:



Error in Shortcut : Object doesn't support this property or method

Error accessing services from CitiDirect Services Menu: Empty screen and Javascript errors similar to below screenshot



Problems with this Web page might prevent it from being displayed properly or functioning properly. In the future, you can display this message by double-clicking the warning icon displayed in the status bar.

□ Always display this message when a page contains errors.

```
Line: 17
Char: 5785
Error: Could not complete the operation due to error 80020101.
Code: 0
```

## Root Cause

When the 1.7 Update 51 version of Java is released, Oracle updates the security baseline version for 1.7 series JRE to 1.7 Update 51. Due to this change in baseline version, if a user has a 1.7 version of JRE which is below the new security baseline version and has "High" as security level setting, the Javascript communication with CitiDirect Services is blocked without prompting the user. Additionally, the user is not provided with any option to override this block and prevents the user interface interaction with Java, which prevents the navigation in the screen.

For additional information regarding configuration changes to facilitate the Java 1.7 Update 51 release on January 14, 2014, contact your Citi Representative.

**transactionservices.citi.com**