bad_record_mac error when connecting to SSLv3-only server

This article applies to: **Deskzilla 1.x-2.x, JIRA Client 1.x-2.x**, and connecting to Bugzilla and JIRA servers via https://... connections.
For clarity, this article is written about JIRA Client and JIRA, but it applies to Deskzilla / Bugzilla as well.

Problem

When trying to establish a connection to a server with HTTPS-based URL, JIRA Client reports the following problem:

```
Received fatal alert: bad_record_mac
```

Check if the server allows only SSL v3 as the protocol for HTTPS connection.

The problem is caused by issues with Sun Java security package (#4815023), which makes the client (JIRA Client) try TLS even if it's not supported on the server. This results in aborted connection.

Solution

The workaround is to enable only SSLv3 on the client. This can be done by setting "https.protocols" system property to "SSLv3", and also turning on "force.http.jre.executor" system property.

On Windows

Find "JIRA Client" start menu item (or other shortcut that you use to launch JIRA Client), *Right-Click* on it and select *Properties*. The *Shortcut* tab will appear, with the *Target* field containing something like *"C:\Program Files\JIRA Client\bin\jiraclient.exe"*.

Click on the Target field and modify it so it says

```
"C:\Program Files\JIRA Client\bin\jiraclient.exe" -J-Dhttps.protocols=SSLv3 -J-Dforce.http.jre.executor=true
```

Use copy&paste from this article to avoid typos.

Note the quotes in this example. Don't put additional parameters inside the quotes around the .exe file path.

On Linux

Modify "jiraclient.sh" script. Find line that says *JAVA_OPTIONS="-Xmx600m -Duse.metal=true"*. Modify it so it says

```
JAVA_OPTIONS="-Xmx600m -Duse.metal=true -Dhttps.protocols=SSLv3 -Dforce.http.jre.executor=true"
```

Note the quotes are around all the line. Use full path to specify the location of jiraclient.jks.

On Mac

Right-click on JIRA Client application and select *Show Package Contents*. Open *Contents* folder. Double-click on the *Info.plist* file. Plist editor should start. Open *Java* section, then *Properties* subsection. Use "+" button to add the following properties:

Name	Value
force.http.jre.executor	true
https.protocols	SSLv3

For self-signed server certificates

If the server uses a self-signed certificate (or a certificate signed by an unknown CA), you will need to explicitly import server's certificate into the Java's trust keystore. (See instructions.) By default, the trust keystore is called *cacerts* and it resides in C:\Program Files\JIRA Client\jre\lib\security\cacerts. With the same method you used for setting the three properties described above, it's possible to specify a different location for cacerts: you need to set *javax.net.ssl.trustStore* property to *</path/to/your/cacerts>*, and, if the password is not default (*changeit*), set *javax.net.ssl.trustStorePassword* property.