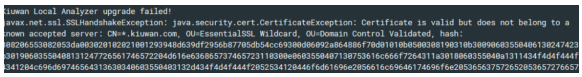
Certificate is Valid but does not Belong to a Known Accepted Server

Problem

Kiuwan Local Analyzer (KLA) does not start, raising an error message like below:



This error happens when **KLA detects that the SSL certificate is not the expected from kiuwan.com** and it might be a clue of a **Man-In-The-Middle (MITM) attack**.

Solution

Related articles

- SSO - Form-based authentication fails
- SSO - HTTP authentication fails
- SSO - WIA is not working
- SSO - Cannot authenticate with credentials
- Basic Authentication Error when Exporting Action Plan to Atlassian JIRA

The most common reasons for this problem are:

1. The **KLA being used is not the latest one** (and it is not considering a new SSL certificate from kiuwan.com)
2. The network department of your organization is using some kind of **SSL Inspection**
3. There's a **real MIME attack**

KLA Version Update

Check if you are using the latest KLA version. Kiuwan.com may have upgraded the SSL certificate and, for some reason, the automatic update mechanism is not working.

A clue of this situation is that the error message displays: *CN=Sectigo RSA Domain Validation Secure Server CA*

Force an update manually by deleting the following files (located at your KLA installation root directory):

- agent.version
- engine.version

In case this solution does not work, delete the current KLA installation, and download and install the latest version (Download Kiuwan Local Analyzer)

If you are using the **Kiuwan Plugin for Jenkins** (Jenkins plugin (old)), you should only delete the following directories (download and installation of the latest KLA will be automatically done):

- JENKINS_HOME/tools/kiuwan/KiuwanLocalAnalyzer, and
- JENKINS_HOME/cache/Kiuwan

SSL Inspection

Check with your Network Admins that SSL Inspection is being implemented.

Quite often, network departments implement **SSL Inspection** to avoid security threads through SSL encrypted channels.

These solutions lead to the KLA detecting that the SSL channel is not being established with the expected kiuwan.com server. If this happens, it might think that it's an MITM attack.

A usual clue of this situation is when the log message shows that Certificate CN is different from the above value.

If you are sure you are using the latest version of KLA, **get in contact with your Network Department**.

Some samples on how to configure SSL inspection in popular proxy/gateway products:

https://help.zscaler.com/zia/deploying-ssl-inspection

https://help.zscaler.com/zia/skipping-inspection-traffic-specific-urls-or-cloud-apps

https://wiki.squid-cache.org/ConfigExamples/Intercept/SslBumpExplicit

https://help.kaspersky.com/KWTS/6.0/en-US/166244.htm