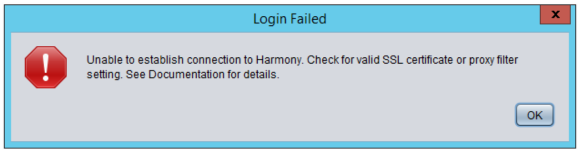
Check for Valid SSL Certificate or Proxy Filter Setting Error Message



Unable to establish connection to Harmony. Check for valid SSL certificate or proxy filter setting. See Documentation for details.

This error message occurs while trying to log in to Jitterbit Studio or Jitterbit Cloud Data Loader. Follow the steps below to troubleshoot what is causing the error to occur.

NOTE: Any of the Java Keytool commands presented in this document may be used for Jitterbit Studio, Jitterbit Cloud Data Loader, or Jitterbit Agent by substituting the home directory for the product you are working with. If the default is accepted during installation, the home directory will be one of:

- Windows (Cloud Data Loader): `C:\Program Files (x86)\Jitterbit Cloud Data Loader\`
- Windows (Harmony Design Studio): `C:\Program Files\Jitterbit Studio x.xx\`
- Windows (Harmony Agent): `C:\Program Files (x86)\Jitterbit Agent\`
- Linux (Harmony Agent): `/opt/jitterbit/`

Step 1: Verify You Can Log into the Management Console With the Same Desktop Machine

Verify that you can log into the Jitterbit Management Console from the same desktop machine that the Jitterbit Studio Is running on.

Step 2: Verify Jitterbit Studio Is Using the Java Version Installed With the Product

Jitterbit Studio and Jitterbit Cloud Data Loader should be running on the Java version that is installed with the product.

- Open `<Jitterbit Studio Home>\configuration\client.properties` in a text editor.
- Search for "JRE_HOME" in the file for instructions
- Verify the `client.properties` file has not been modified to point to a different Java version.

Step 3: Verify IP Whitelist

Verify if your browser is using a proxy server (such as Websense), a web filter (such as zScaler), a SSL inspection service on outgoing connections (such as Websense or zScaler) or a VPN (such as Pulse Secure) and make sure the correct Jitterbit sites are included in the IP whitelist.

- You may have to contact your Network Administrator or the third-party vendor that set up your Internet access to verify what browser services are being used.
- The following addresses will need to be included in the IP whitelist for these services: `*Jitterbit.com`, `*Jitterbit.eu` and `*Jitterbit.net`.
- If the proxy server, web filter, packet inspection service or VPN also use a trusted root CA certificate, please follow the steps below to add the certificate to the Jitterbit Java KeyStore.

Step 4: Verify SSL Certificate Is Not Located in the Jitterbit Java KeyStore

The error frequently occurs when a signed SSL or CA xxxxxxx.cer certificate is not located in the Jitterbit Java KeyStore. The error will also occur if a SSL inspection service, web filter, proxy server, or VPN changes which certificate is used and the certificate is not located in the Jitterbit Java KeyStore.

- You need to identify which certificates are being used and install each of them into the `\jre\lib\security` folder that Jitterbit included in the product installation.
- A process must be developed to install the certificate in the `\jre\lib\security` folder that Jitterbit ships with the product each time you upgrade or re-install Jitterbit.

On This Page

Related Articles

- Adding Certificates to Keystore for Private Agents
- Check for Valid SSL Certificate or Proxy Filter Setting Error Message
- Configuring Jitterbit with SSL
- Enabling Proxy for Design Studio
- SSL Server Certificates

Related Topics

- Agent
- Jitterbit Security
- Private Agents
- Troubleshooting and Debugging

Last updated: Jan 14, 2020

Copyright © 1998 - 2019 Jitterbit, Inc.

- Each time you change the certificate(s) that are used, it will be necessary to get the certificate(s) from your Network Administrator or the third-party vendor and install them in the `\jre\lib\security` folder that Jitterbit ships with the product..

How to Get the List of Security Certificates

- Run this command from within the `Java\jre\lib\security` folder: > `keytool -list -v -keystore cacerts`
- Verify the certificates are all located in `<Jitterbit Studio>\jre\lib\security\`.
- To add certificates that are not located in `<Jitterbit Studio>\jre\lib\security\`, follow the steps below.

How to Add a New Certificate to the Jitterbit Studio KeyStore

Command Using Java Keytool

NOTE:

- The following Java command may be used for Jitterbit Studio, Jitterbit Cloud Data Loader, and Jitterbit Agent by substituting the home directory for the product you are working with.
- You must be in *administrator* mode.
- The default password for all of the Jitterbit keystores is '`changeit`'.

The Java Keytool Command is:

```
> <Jitterbit Studio Home>\jre\bin\keytool -importcert -trustcacerts -alias
<alias> -file <certfile> -keystore "<Jitterbit Agent
Home>\jre\lib\security\cacerts"
```

EXAMPLE:

This example is a Websense certificate in Cloud Data Loader. In this example, the Websense certificate file was first copied into `C:\temp\cacerts`. The certificate can be installed directly from the original directory using this command as well.

```
> cd C:\Program Files (x86)\Jitterbit Cloud Data Loader\jre\bin
> C:\Program Files (x86)\Jitterbit Cloud Data
Loader\jre\bin\keytool -importcert -trustcacerts -alias Websense -
file C:\temp\cacerts\xxxxx.cer -keystore "C:\Program Files (x86)
\Jitterbit Cloud Data Loader\jre\lib\security\cacerts"
```

Additional KeyTool command resources:

- Adding Certificates to Keystore for Private Agents
- https://www.sslshopper.com/article-most-common-java-keytool-keystore-commands.html
- https://azure.microsoft.com/en-us/documentation/articles/java-add-certificate-ca-store/

NOTE:

- A process must be developed to install the certificate(s) in the `\jre\lib\security` folder that Jitterbit ships with the product each time you upgrade or re-install Harmony Studio, Harmony Agent or Cloud Data Loader.
- Each time you change the certificate(s) that are used, it will be necessary to get the new certificate(s) from your Network Administrator or the third-party vendor and install them in the `\jre\lib\security` folder that Jitterbit ships with the product.

Instructions for using Portecle:

1. Download and install Portecle.

2. First, be certain which JRE or JDK is being used to run your program. On a 64-bit Windows 7, there can be quite a few JREs. Process Explorer can help you with this, or you can use this Jitterbit script command:

   ```
   System.out.println(System.getProperty("java.home"));
   ```

3. Copy the file `JAVA_HOME\lib\security\cacerts` to another folder.
4. In Portecle, click **File > Open Keystore File**
5. Select the cacerts file.
6. Enter this password: `changeit`
7. Click **Tools > Import Trusted Certificate**
8. Browse for the file `mycertificate.pem`
9. Click **Import**
10. Click **OK** when the trust path warning displays.
11. Click **OK** when the details about the certificate display.
12. Click **Yes** to accept the certificate as trusted.
13. When it asks for an alias, click **OK**.
14. Click **OK** when message indicating it has imported the certificate displays.
15. Click **Save**. Don't forget to do this or the change will be discarded.
16. Copy the file `cacerts` back to its original location (`JAVA_HOME\lib\security\cacerts`).

NOTE:

- A process must be developed to install the certificate(s) in the `\jre\lib\security` folder that Jitterbit ships with the product each time you upgrade or re-install Jitterbit Harmony Studio, Harmony Agent, or Cloud Data Loader.
- Each time you change the certificate(s) that are used, it will be necessary to get the new certificate(s) from your Network Administrator or the third-party vendor and install them in the `\jre\lib\security` folder that Jitterbit ships with the product.

Turn on SSL Debug Logging to Determine Which Certificate Is Not Being Accepted

1. Turning on logging will show what is causing the error. It will show which certificate is not being accepted. The certificate will need to be added to the Jitterbit Java KeyStore by following the steps above.
2. Open `<Jitterbit Studio Home>\configuration\client.properties` in a text editor
3. Make a note of the current value of the `STARTUP_ARGUMENTS` property
4. Change the `STARTUP_ARGUMENTS` property to:

   ```
   STARTUP_ARGUMENTS='-Djavax.net.debug=ssl:handshake -Xms512m -
   Xmx1024m -Djava.util.Arrays.useLegacyMergeSort=true'
   ```

5. Save the file
6. Launch Jitterbit Studio and attempt to log in
7. Once the error displays, dismiss the error dialog
8. Go to the folder `C:\Users\[windows username]\JitterbitStudio\`
9. Zip up the `logs` sub-folder
10. Create a support case and attach the zip file to the case, or (if not larger than 10MB) email the zip file to support@jitterbit.com
11. Reset the startup argument property back to its original value to turn off logging