



sage

Enterprise Management

Sage Business Cloud Enterprise Management (formerly Sage X3)

PCI compliance using TLSv1.2 protocol
Version 6.5

June 18, 2018

Contents

INTRODUCTION	3
INSTALLATION	4
Installing the new Java Bridge Server Version 123.1	4
Configuring the Java Server	6

Introduction

To be PCI compliant, the Java Bridge server 123.1 and higher uses the TLSv1.2 protocol and is necessary to process credit card transactions through the PAYA portal.

Review the installation instructions below.

Installation

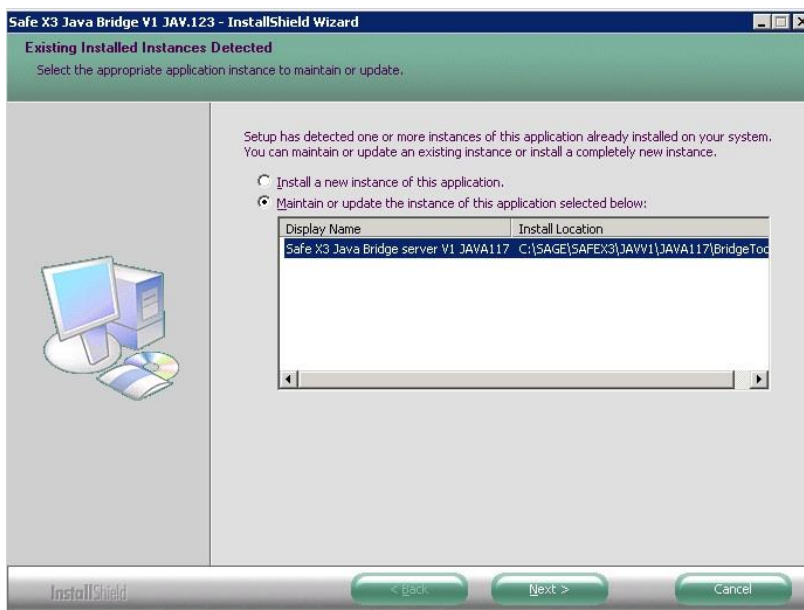
Installing the new Java Bridge Server Version 123.1

Download and run the **SafeX3V1JAV123.exe**.



Select **Maintain or update the instance of this application selected below:** and highlight the Java server you want to update.

Click **Next** to start the update.

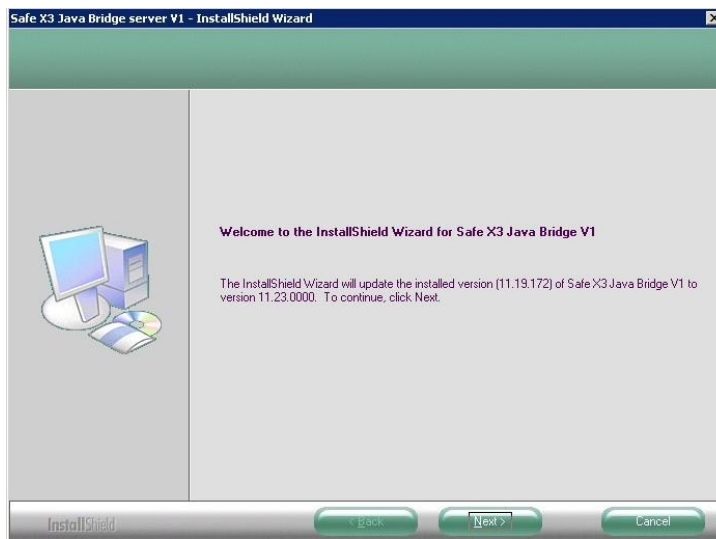


Let the command window close automatically.

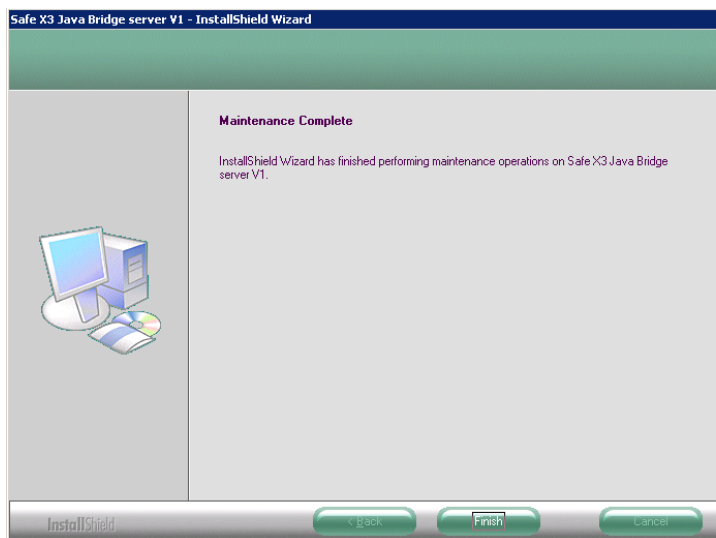
```
Windows\system32\cmd.exe
C:\> yajsv-stable-11.11
: Windows Server 2008 R2/6.1/amd64
: Oracle Corporation/1.7.0_45/C:\SAGE\SAFEX3\JAVU1\JAVU117\BridgeTools\SOFT
M\jre/64
13, 2018 10:33:22 AM org.apache.commons.ufs2.UfsLog info
0: Using "C:\Users\ADMINI~1\AppData\Local\Temp\2\ufs_cache" as temporary file
ore.
13, 2018 10:33:24 AM org.rzo.yajsw.wrapper.WrappedService JVMOptions
0: Windows & JVM7: Setting -Djava.net.preferIPv4Stack=true (see java bug 7179
)
***** STOPPING SageX3_JAU_coreserver_JAVU117 *****

Service SageX3_JAU_coreserver_JAVU117 stopped
Wait for the end of stopping
Look at the deletion of the file : [C:/SAGE/SAFEX3/JAVU1/JAVU117/BridgeData\te
osgi\bridge.stopping]
Wait start
hArgs={3}
totalDelay=[90000]
Wait deleting the file<1> [C:/SAGE/SAFEX3/JAVU1/JAVU117/BridgeData\temp\osgi\
ge.killing]
maxDelay=[89996]
```

Click **Next** to continue with the update.



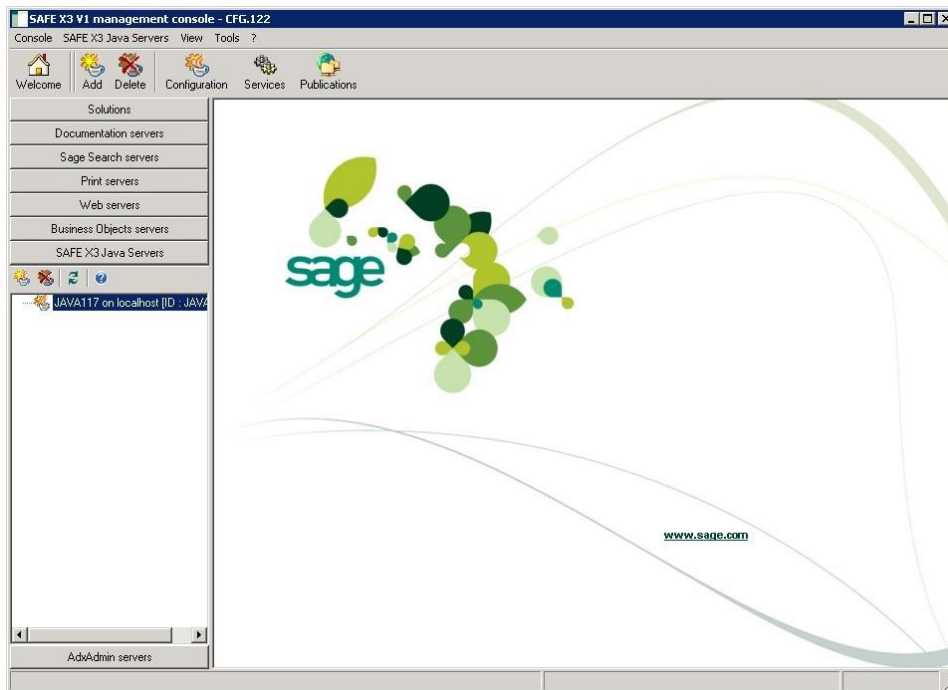
Click **Finish** when maintenance is complete.



Configuring the Java Server

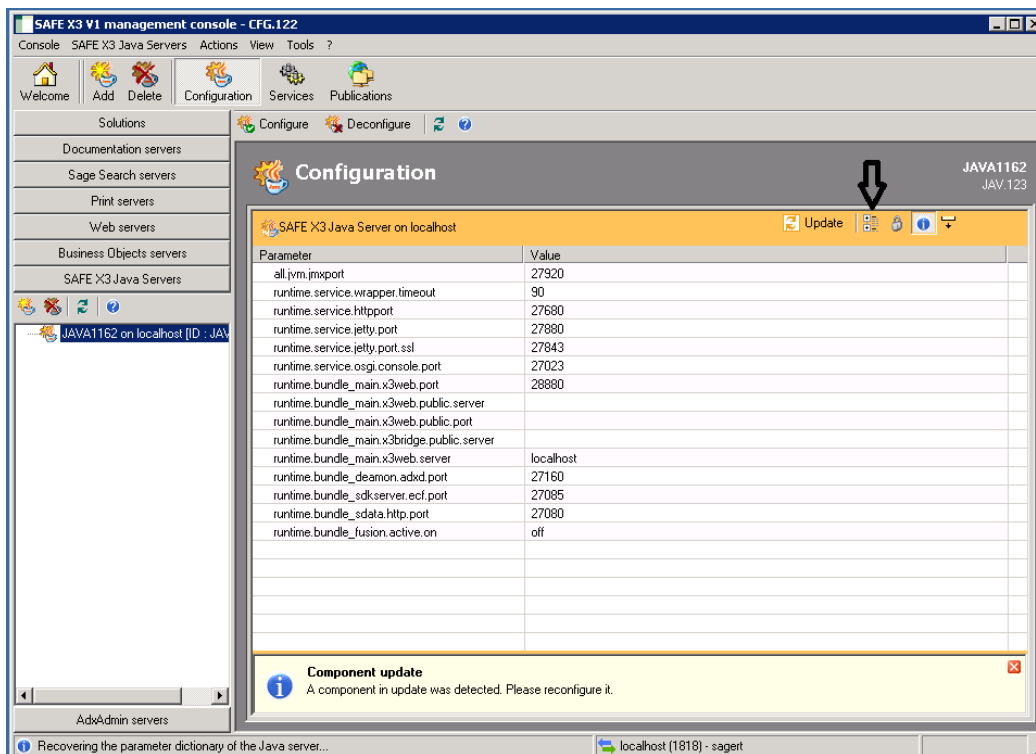
Launch the SAFE X3 V1 management console.

In the SAFE X3 V1 management console, expand the **SAFE X3 Java Servers** menu.



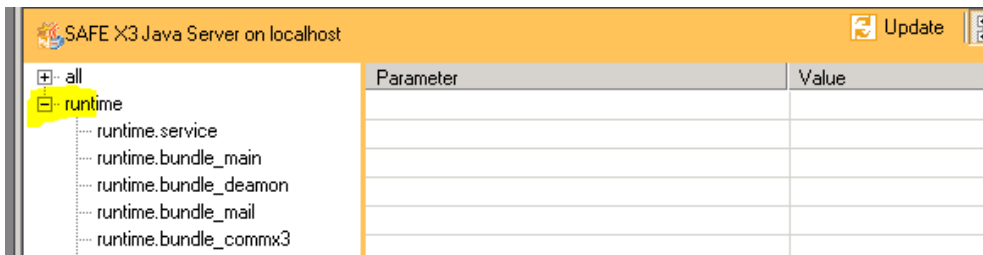
Open the Java bridge configuration by double-clicking.

Click the icon below the arrow shown below.



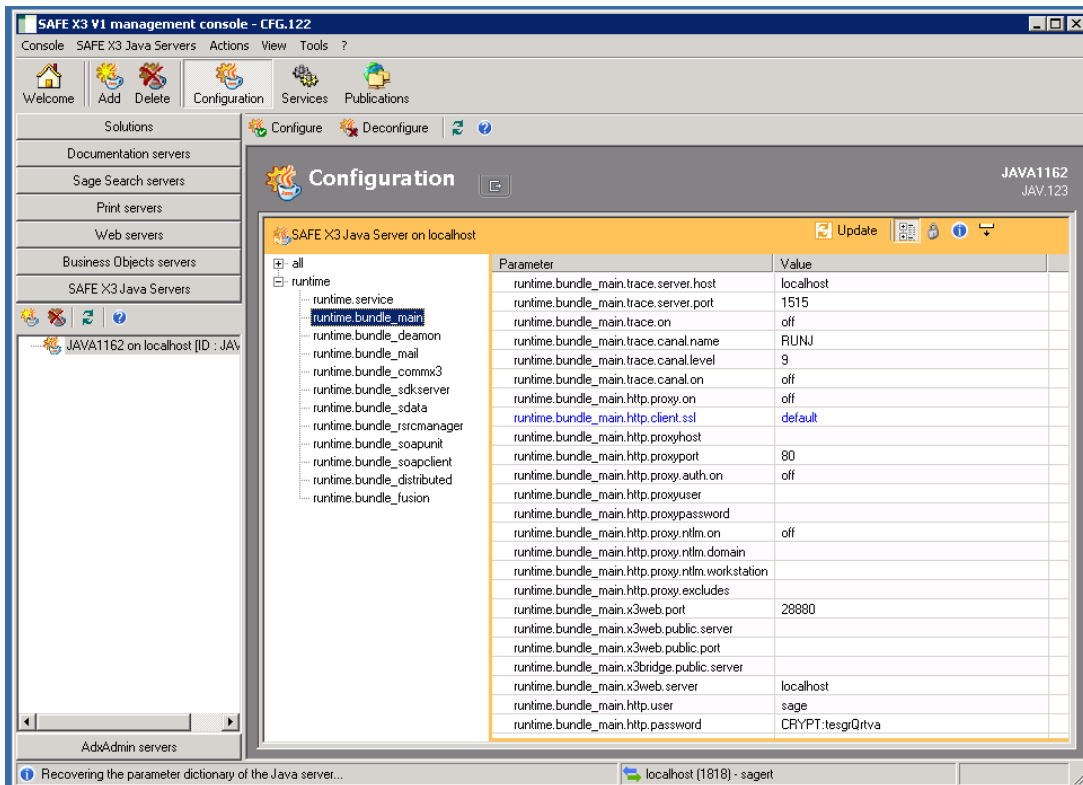
You are now in Advance mode to display all of the parameters.

Expand the runtime menu from the left list.



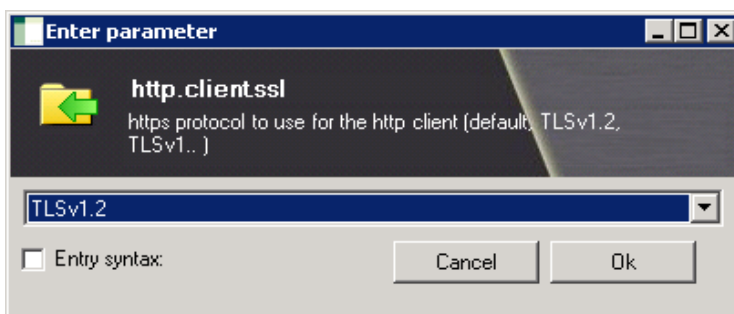
Select **runtime.bundle_main** then highlight **runtime.bundle_main.http.client.ssl**.

The current **Value** setting is **default** and must be changed to **TLSv1.2**.



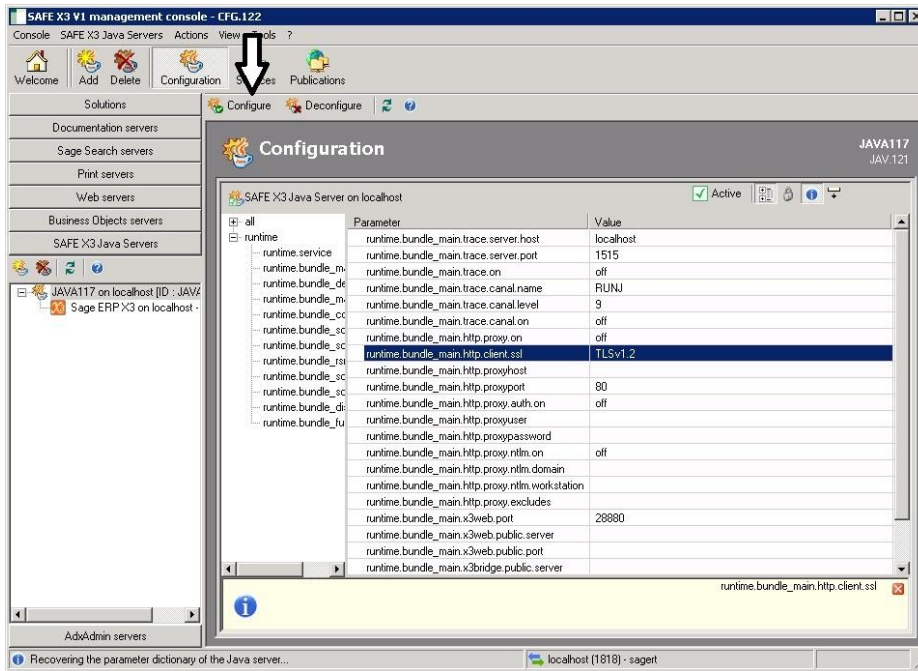
To change the **Value**, double-click **default**.

In the window that opens, select **TLSv1.2** from the drop-down list.

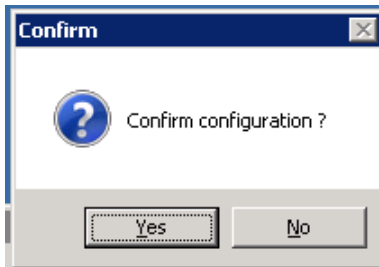


Click **Ok**.

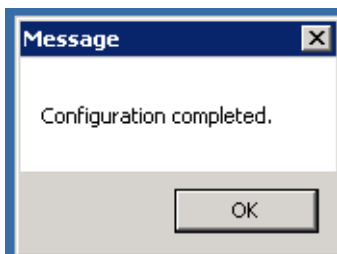
Click **Configure**.



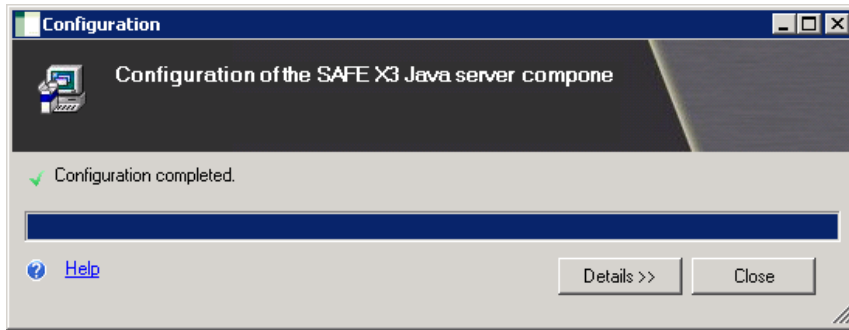
Click **Yes**.



Click **OK**.



Click **Close**.



You can now close the SAFE X3 console.

sage

www.sage.com

© 2018 The Sage Group plc or its licensors. All rights reserved. Sage, Sage logos, and Sage product and service names mentioned herein are the trademarks of The Sage Group plc or its licensors. All other trademarks are the property of their respective owners.