sage

Enterprise Management

Sage Business Cloud Enterprise Management (formerly Sage X3)

PCI compliance using TLSv1.2 protocol
Version 6.5

June 18, 2018

Contents

Enterprise Management PCI compliance using TLSv1.2 protocol

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.

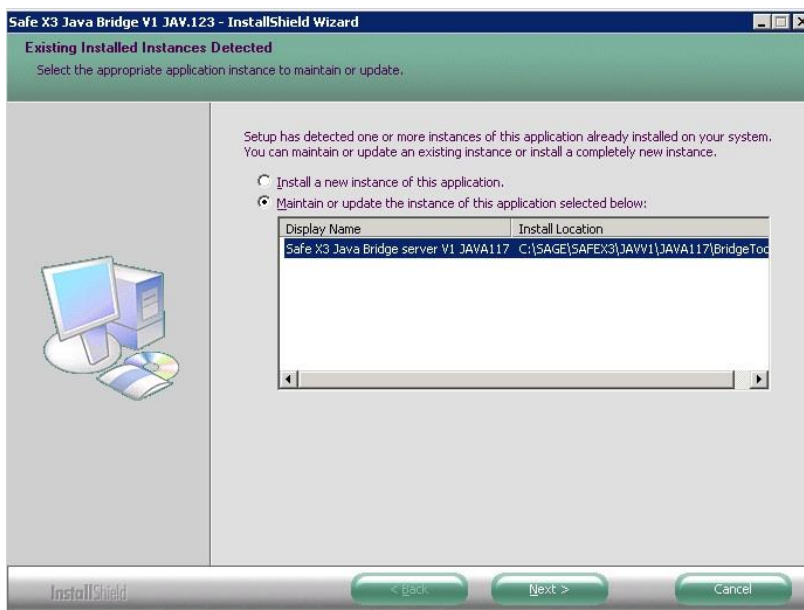Enterprise Management PCI compliance using TLSv1.2 protocol

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.

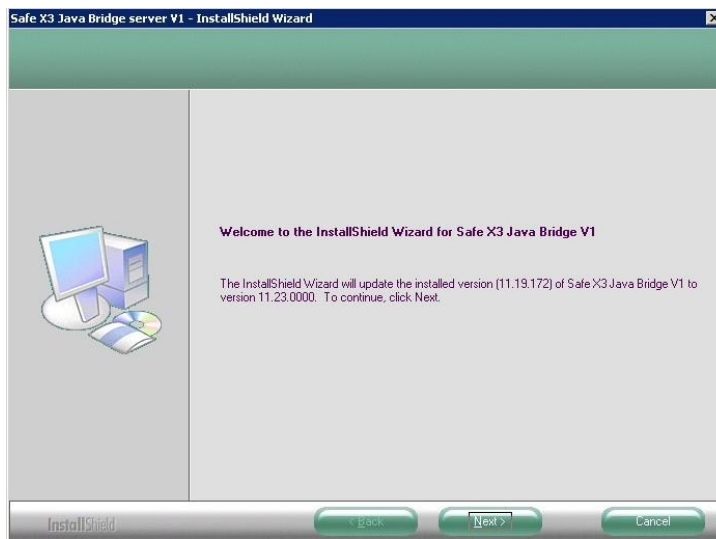Click **Next** to start the update.
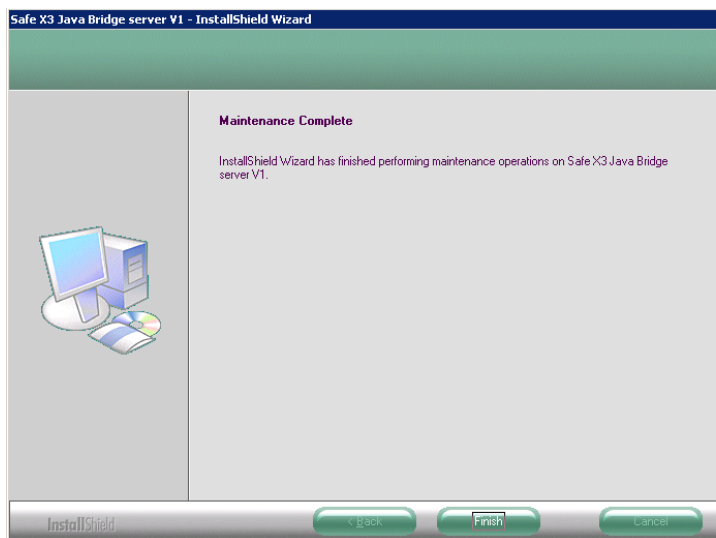
Let the command window close automatically.

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

Click **Finish** when maintenance is complete.

Enterprise Management PCI compliance using TLSv1.2 protocol
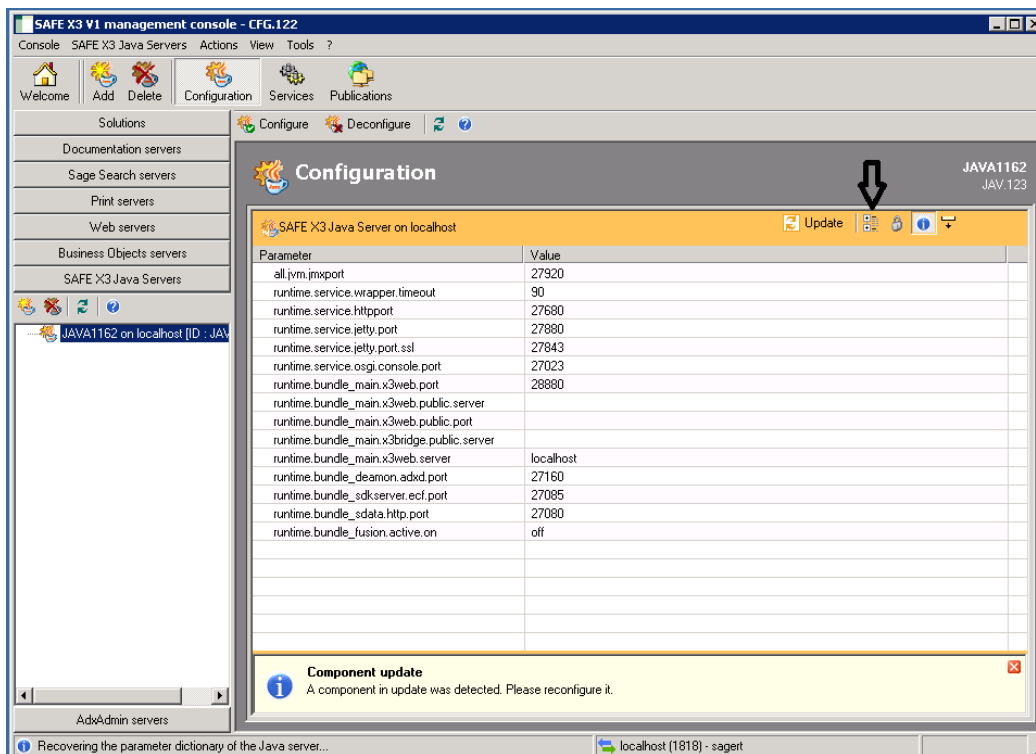
Configuring the Java Server

Launch the SAFE X3 V1 management console.

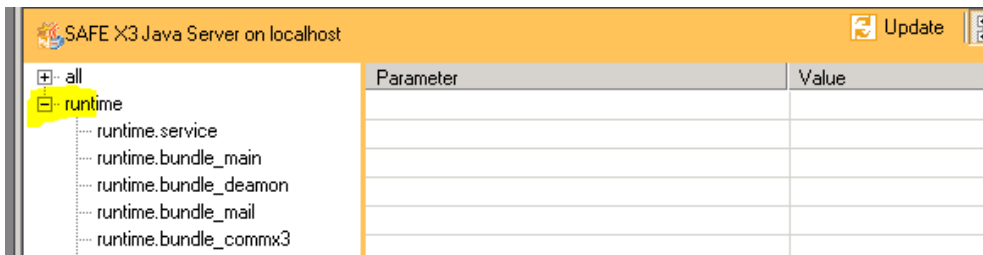In the SAFE X3 V1 management console, expand the **SAFE X3 Java Servers** menu.
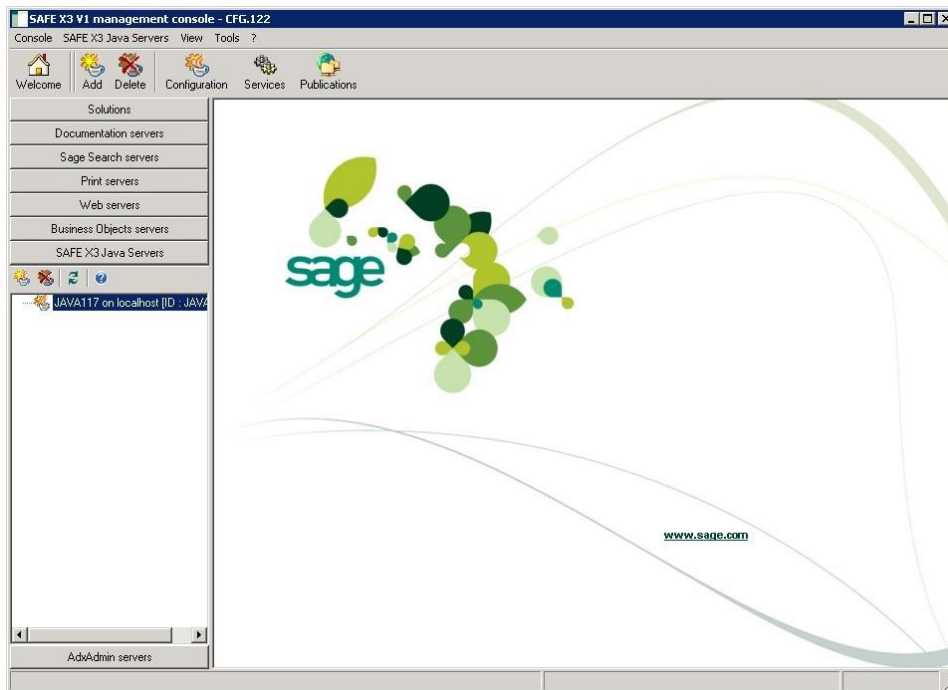
Open the Java bridge configuration by double-clicking.

Click the icon below the arrow shown below.

Enterprise Management PCI compliance using TLSv1.2 protocol
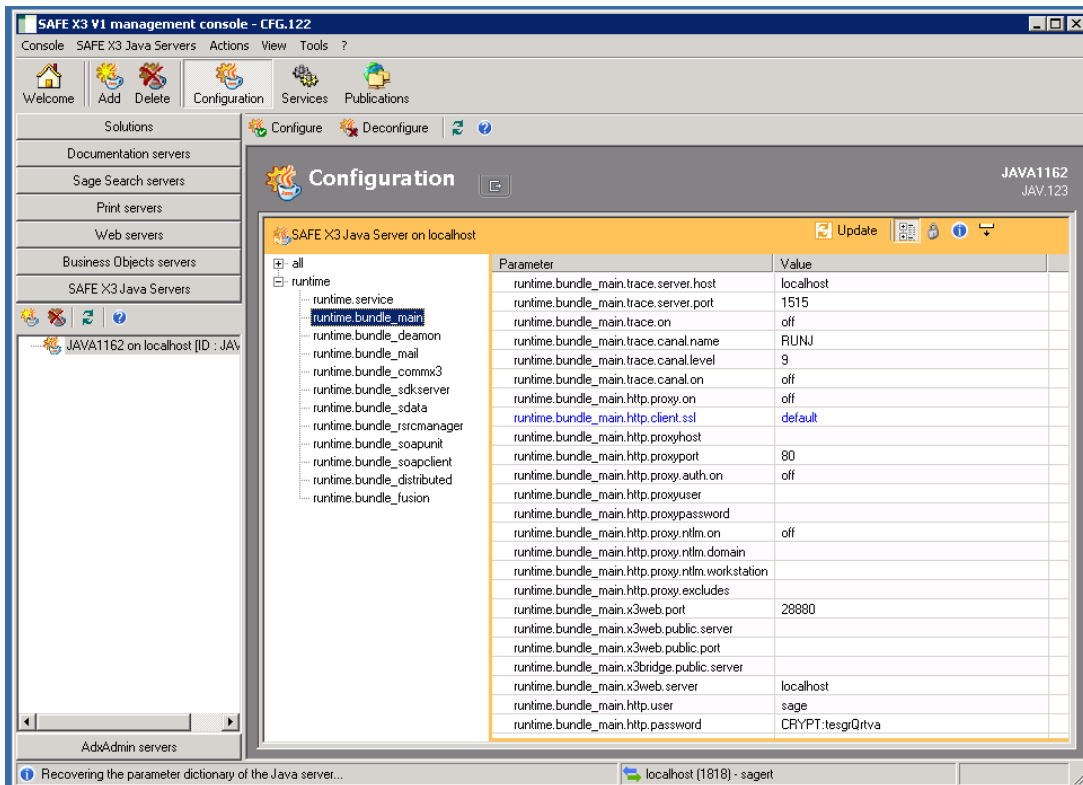
You are now in Advance mode to display all of the parameters.

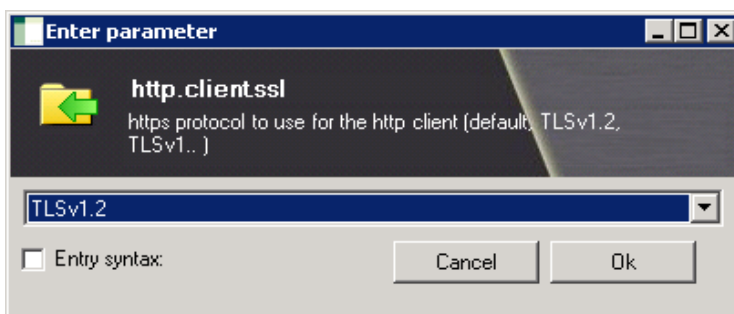Expand the runtime menu from the left list.

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

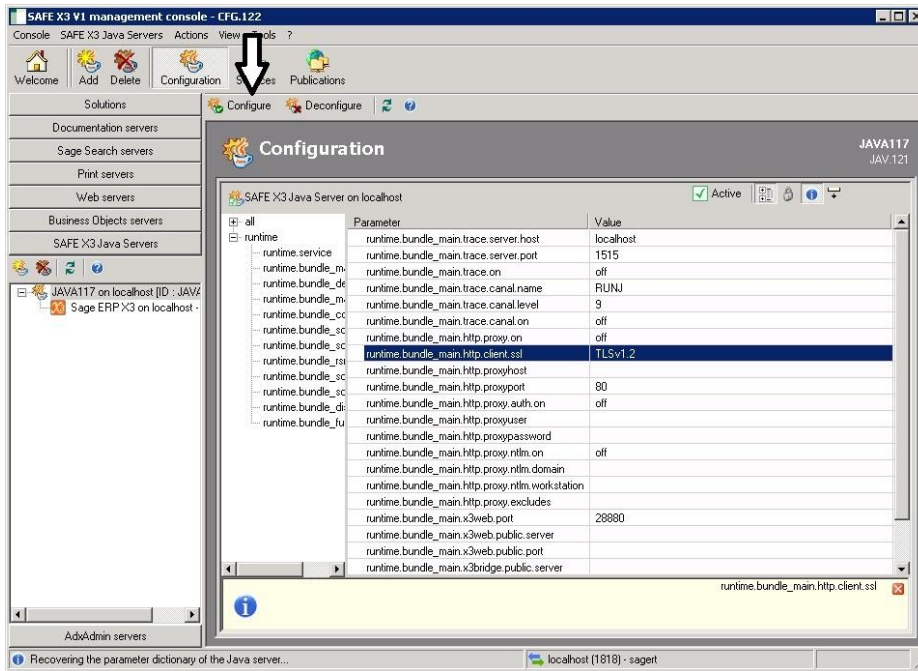The current **Value** setting is **default** and must be changed to **TLSv1.2**.

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

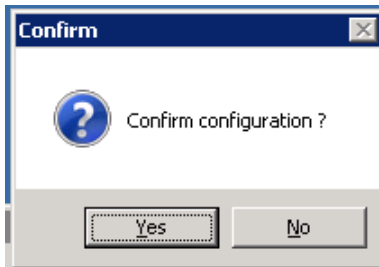In the window that opens, select **TLSv1.2** from the drop-down list.

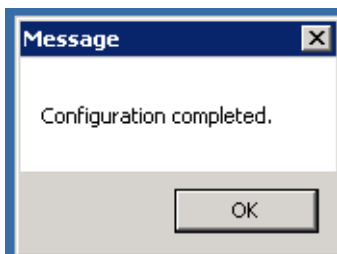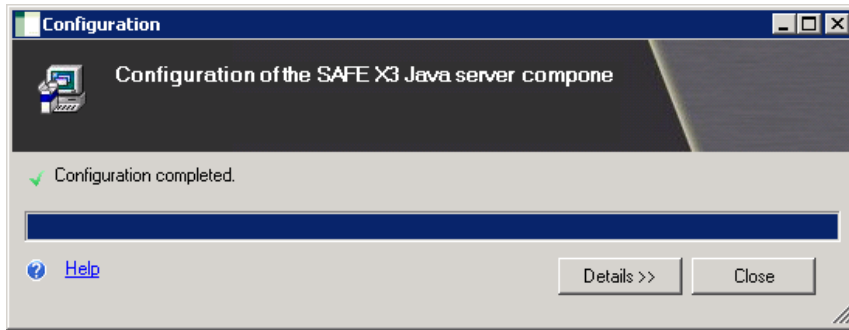Enterprise Management PCI compliance using TLSv1.2 protocol

Click **Ok**.

Click **Configure**.

Click **Yes**.

Click **OK**.

Click **Close**.

Enterprise Management PCI compliance using TLSv1.2 protocol

You can now close the SAFE X3 console.

sage