

KERNEL AUTHENTICATION & AUTHORIZATION FOR J2EE (KAAJEE)

SECURITY SERVICE PROVIDER INTERFACE (SSPI) VERSION 8.0.748

FOR WEBLOGIC (WL) VERSIONS 12.2 AND HIGHER

**ROLLBACK GUIDE**

December 2021

Department of Veterans Affairs

Office of Information and Technology

Product Development

Revision History

**Documentation Revisions**

The following table displays the revision history for this document. Revisions to the documentation are based on patches and new versions released to the field.

Table i. Documentation revision history

| **Date** | **Description** | **Author(s)** |
| --- | --- | --- |
| 12/2021 | Updated software and the installation guide with relation to the KAAJEE SSPI. **Kernel Patch: XU\*8.0\*748**, makes changes the Technical Reference Model (TRM) compliance changes and upgrades/certifications of a KAAJEE SSPI component for the WebLogic 12.2/Java 1.8 and Oracle Relational Database Management System (RDMS), version 19c platform. | REDACTED |
| 11/2021 | Second version of this document. | REDACTED |

Table of Contents

[KAAJEE SSPI rollback 4](#_Toc86829052)

List of Figures

**No table of figures entries found.**

List of Tables

[Table i. Documentation revision history 3](#_Toc50638487)

## KAAJEE SSPI rollback

1. Locate and Run the setWLSEnv.sh script on the application server



The file is located under the **server/bin** directory by default (Ex: /u01/app/oracle/weblogic-server-12.2.1.4/wlserver/server/bin/setWLSEnv.sh)

#### Run the java weblogic.WLST and pass the required properties file to the deleteDSSSPI.py

**java weblogic.WLST deleteDSSSPI.py -p createDSSSPI.properties**

#### The script will attempt to remove a datasource as well as the SQLAuthenticationProvider. It will use the same properties file. Upon successful script completion, you will be offered to shutdown an admin server.

1. Start the server; Log onto admin console.
2. Navigate to the Authentication Directory:
	1. Select Security Realms under Domain Structure.
	2. Navigate to the Providers tab, as shown below:

 - Home > Summary of Security Realms > myrealm > Providers > Authentication tab

1. Confirm absence of the KaajeeManageableAuthenticator.
	1. When returned to the Authentication page, select and edit the DefaultAuthenticator Authentication Provider. Ensure that Control Flag is '**REQUIRED**'.
2. Restart the admin server, if any changes to the Authentication Providers has been made.
3. Verify all Changes Have Taken Place:
	1. Use the WebLogic console software (i.e., WebLogic Server 10.3.6 Console Login) to navigate to the following locations:
		* Home > Summary of Security Realms > myrealm > Users and Groups
		 (Users tab)
		* Home > Summary of Security Realms > myrealm > Users and Groups
		 (Groups tab)
	* Confirm absense of application-level users retrieved by the KaajeeManageableAuthenticator