KERNEL AUTHENTICATION & AUTHORIZATION FOR J2EE (KAAJEE)

SECURITY SERVICE PROVIDER INTERFACE (SSPI) VERSION XU*8*781

FOR WEBLOGIC (WL) VERSIONS 12.2 AND HIGHER

ROLLBACK GUIDE

December 2022

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)
12/2022	Updated the document for the XU*8*781	Arsen Mikhailoutsa - HDSO
11/2021	Second version of this document.	Health Services Portfolio (HSP) Adriana Quintero – Technical Writer Arsen Mikhailutsa – Primary Developer

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

KAAJEE SSPI rollback

1. Locate and Run the setWLSEnv.sh script on the application server. This script will initialize the WLST environment:

```
[weblogic@vaausappsds801 scripts]$ locate setWLSEnv.sh
/u01/app/oracle/weblogic-server-12.2.1.4/inventory/Templates/wlserver/server/bin
/setWLSEnv.sh
/u01/app/oracle/weblogic-server-12.2.1.4/wlserver/server/bin/setWLSEnv.sh
/u01/wlsdomains/inventory/Templates/wlserver/server/bin/setWLSEnv.sh
/u01/wlsdomains/wlserver/server/bin/setWLSEnv.sh
```

   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)

2. Run the *java weblogic.WLST* and pass the required properties file to the **delete**DSSSPI.py

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

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

3. Start the server; Log onto admin console.

4. Navigate to the Authentication Directory:
   a. Select Security Realms under Domain Structure.
   b. Navigate to the Providers tab, as shown below:

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

5. Confirm absence of the KaajeeManageableAuthenticator.

   a. When returned to the Authentication page, select and edit the DefaultAuthenticator Authentication Provider. Ensure that Control Flag is '**REQUIRED**'.

6. Restart the admin server, if any changes to the Authentication Providers has been made.

7. Verify all Changes Have Taken Place:

   a. Use the WebLogic console software (i.e., WebLogic Server 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 absence of application-level users retrieved by the KaajeeManageableAuthenticator