



**KERNEL AUTHENTICATION &
AUTHORIZATION FOR J2EE (KAAJEE)
SECURITY SERVICE PROVIDER
INTERFACE (SSPI)
VERSION XU*8*781
FOR WEBLOGIC (WL) VERSIONS 12.2
AND HIGHER**

INSTALLATION GUIDE

December 2022

Department of Veterans Affairs
Office of Information and Technology
Product Development

This page is left blank intentionally.


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	Kernel Patch XU*8*781	HDSO
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.	Health Product Support (HPS) Adriana Quintero – Technical Writer Arsen Mikhailutsa – Primary Developer
07/2020	Updated software and documentation with TRM and Fortify compliance items. Software Version: 1.2.0.005 Security Service Provider Interface (SSPI) Version: 1.2.0.005 Kernel Patches: XU*8.0*694 and XU*8.0*696	Health Product Support (HPS) Adriana Quintero – Technical Writer Arsen Mikhailutsa – Primary Developer
03/2011	Software and documentation for KAAJEE 1.1.0.007 and KAAJEE Security Service Provider Interface (SSPI) 1.1.0.002, referencing VistALink 1.6 and WebLogic 10.3.6 and higher. Software Version: 1.1.0.007 Security Service Provider Interface (SSPI) Version: 1.1.0.002 Kernel Patch: XU*8.0*504	Product Development Services Security Program HWSC development team. Bay Pines, FL Office of Information Field Office (OIFO): <ul style="list-style-type: none">• Development Manager—Charles Swartz Oakland, CA OIFO: <ul style="list-style-type: none">• Developer—Jose L. Garcia• Developer—Alan Chan• SQA—Gurbir Singh Technical Writer—Susan Strack

Date	Description	Author(s)
05/2006	<p>Initial software and documentation for KAAJEE 1.0.0.019 and KAAJEE Security Service Provider Interface (SSPI) 1.0.0.010, referencing VistALink 1.5 and WebLogic 8.1.</p> <p>Software Version: 1.0.0.019</p> <p>Security Service Provider Interface (SSPI) Version: 1.0.0.010</p> <p> NOTE: For a description of the current KAAJEE software version numbering scheme, please review the readme.txt file distributed with the KAAJEE software.</p> <p>In the future, the Development Technology Advisory Committee (DTAC) will be the authoritative source for determining future version numbering schemes for all HealthVet-VistA software file and folder names.</p>	<p>ISS KAAJEE Development Team</p> <ul style="list-style-type: none"> • Project Manager—Dan Soraoka • Lead Developer—Alan Chan • Developer—Jose Garcia • SQA—Matt Alderman • Technical Writer—Thom Blom

Patch Revisions

For a complete list of patches related to this software, please refer to the Patch Module on FORUM.

Contents

1	Pre-Installation Instructions.....	1-1
1.1	Purpose.....	1-1
1.2	Distribution Files.....	1-1
1.3	Installer/Developer Notes—KAAJEE Software First-Time Installations and Upgrades.....	1-1
1.4	Application Server Environment Requirements.....	1-2
2	Installation Overview.....	2-1
2.1	WebLogic v 12.2 and Higher Server Preparation	2-1
2.2	KAAJEE SSPI Installation.....	2-1
	UPGRADE and continuing the FIRST-TIME Installation	2-3
	Appendix A: Installation Back-Out or Roll-Back Procedure.....	1
	KAAJEE SSPI rollback.....	1

Figures

Figure 4-25. Database—Sample SSPI SQL script for KAAJEE table definitions 2-2

Tables

Table i. Documentation revision history iii

Table ii. Documentation symbol/term descriptions vii

Table 1-1. Application server minimum software/network tools/documentation required for KAAJEE. 1-2

Table 4-4. Caché Database—KAAJEE SSPI SQL table definitions 2-2

Orientation

How to Use this Manual

Throughout this manual, advice and instructions are offered regarding the installation and use of KAAJEE and the functionality it provides for Health_Vet-Veterans Health Information Systems and Technology Architecture (VistA) software products.

The installation instructions for KAAJEE are organized and described in this guide as follows:

1. Pre-Installation Instructions.
2. Installation Overview
3. **Error! Reference source not found.**
4. Java 2 Platforms, Enterprise Edition (J2EE) Application Server Installation Instructions



Where necessary, separate steps for the following two supported operating systems are provided:

- Linux (i.e., Red Hat Enterprise ES 8.0 or higher)
- Windows


There are no special legal requirements involved in the use of KAAJEE.

This manual uses several methods to highlight different aspects of the material:

- Various symbols/terms are used throughout the documentation to alert the reader to special information. The following table gives a description of each of these symbols/terms:

Table ii. Documentation symbol/term descriptions

Symbol	Description
	NOTE/REF: Used to inform the reader of general information including references to additional reading material.
	CAUTION or DISCLAIMER: Used to inform the reader to take special notice of critical information.
	UPGRADES/FIRST-TIME INSTALLATION: Used to denote Upgrade or First-time installation instructions only.
	Skip forward to the referenced step or procedure that is indicated.
	Instructions that only apply to the Linux operating systems (i.e., Red Hat Enterprise ES 3.0 or higher) are set off and indicated with this Linux "Tux" penguin icon.

Symbol	Description
	Instructions that only apply to Microsoft Windows operating systems (i.e., Microsoft Windows 7 or 10) are set off and indicated with this stylized "Windows" icon.

- Descriptive text is presented in a proportional font (as represented by this font).
- "Snapshots" of computer online displays (i.e., roll-and-scroll screen captures/dialogues) and computer source code, if any, are shown in a *non*-proportional font and enclosed within a box.
 - User's responses to online prompts and some software code reserved/key words will be bold typeface.
 - Author's comments, if any, are displayed in italics or as "callout" boxes.



NOTE: Callout boxes refer to labels or descriptions usually enclosed within a box, which point to specific areas of a displayed image.

- Java software code, variables, and file/folder names can be written in lower or mixed case.
- All uppercase is reserved for the representation of M code, variable names, or the formal name of options, field and file names, and security keys (e.g., the XUPROGMODE key).

Assumptions About the Reader

This manual is written with the assumption that the reader is familiar with the following:

- VistALink—VistA M Server and Application Server software
- Linux (i.e., Red Hat Enterprise ES 8.0 or higher) or Microsoft Windows environment
- Java Programming language—Java 1.8 Standard Edition (J2SE) Java Development Kit (JDK, a.k.a. Java Software Development Kit [SDK])
- WebLogic 12.2 and higher—Application server
- Oracle Database 19g—Database (e.g., Security Service Provider Interface [SSPI] or Standard Data Services [SDS] 18.0 (or higher) database/tables)
- Oracle SQL*Plus Software 19 (or higher)

This manual provides an overall explanation of the installation procedures and functionality provided by the Kernel Authentication & Authorization for J2EE (KAAJEE) on Weblogic Application Server Versions 10.3.6 and higher software; however, no attempt is made to explain how the overall HealtheVet-VistA programming system is integrated and maintained. Such methods and procedures are documented elsewhere. We suggest you look at the various VA home pages on the VA Intranet for a general orientation to HealtheVet-VistA at the following address:

<http://vista.med.va.gov/>

Reference Materials

Readers who wish to learn more about KAAJEE should consult the following:

- *Kernel Authentication & Authorization for J2EE (KAAJEE) Deployment Guide*
- *VistALink Installation Guide*
- *VistALink System Management Guide*
- *VistALink Developer Guide*



REF: For more information on VistALink, please refer to the Application Modernization Foundations Web site located at the following Web address:

<http://vaww.vista.med.va.gov/vistalink/>

HealthVet-VistA documentation is made available online in Microsoft Word format and Adobe Acrobat Portable Document Format (PDF). The PDF documents *must* be read using the Adobe Acrobat Reader (i.e., ACROREAD.EXE), which is freely distributed by Adobe Systems Incorporated at the following Web address:

<http://www.adobe.com/>

HealthVet-VistA documentation can be downloaded from the VHA Software Document Library (VDL) Web site:

<http://www.va.gov/vdl/>

HealthVet-VistA documentation and software can also be downloaded from the Enterprise Product Support (EPS) anonymous directories:

- Preferred Method download.vista.med.va.gov



DISCLAIMER: The appearance of any external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs (VA) of this Web site or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of this VA Intranet Service.

1 Pre-Installation Instructions

1.1 Purpose

The purpose of this guide is to provide instructions for installing the HealthVet-Veterans Health Information Systems and Technology Architecture (VistA) Kernel Authentication and Authorization for Java (2) Enterprise Edition (KAAJEE) and related software.

KAAJEE is *not* an application but a framework. Users of the software need to understand how it integrates in their working environment. Thus, installing KAAJEE means to understand what jars and files need to be put where and what are the configuration files that you need to have and edit.

KAAJEE provides secure sign-on architecture for HealthVet-VistA Web-based applications.

These HealthVet-VistA Web-based applications are able to authenticating against Kernel on the VistA M Server via an Internet Browser on the client workstation and a middle tier application server (e.g., WebLogic).

1.2 Distribution Files



NOTE: Please refer to "Table 1-1. Application server minimum software/network tools/documentation required for KAAJEE" for confirmation of all KAAJEE and related software and documentation files.



REF: For the KAAJEE software preview/test release, all distribution files are available at the following Web address:

http://vista.med.va.gov/kernel/kaajee/download_9-10.asp

1.3 Installer/Developer Notes—KAAJEE Software First-Time Installations and Upgrades

First-time KAAJEE installers *must* perform *all* installation steps/procedures, except where noted. Those installation steps/procedures that can be skipped during a first-time installation will be displayed as follows:



FIRST-Time INSTALLATION: *First-time installation-specific instructions or information that can be skipped will be found here.*

If you were a test site prior to the final release of KAAJEE, we have notated those installation steps/procedures that have special information based on the final software upgrades that may affect how you install the released version of KAAJEE or provide other pertinent information. The upgrade information will be displayed as follows:



UPGRADES: *Upgrade-specific instructions or information will be found here.*

In addition, we will use this section to also highlight any KAAJEE code changes from previous test/preview versions of the software to the released version of the software that may affect development teams coding KAAJEE-enabled applications.

1.4 Application Server Environment Requirements



NOTE: The information in this topic is directed at the systems management personnel responsible for maintaining the application servers.

The following minimum software tools and files are required to install the KAAJEE software and documentation for application servers running KAAJEE-based Web applications:

Table 1-1. Application server minimum software/network tools/documentation required for KAAJEE

Minimum Software/Configuration/Documentation	Version and Description
Operating System Software	One of the following operating systems: <ul style="list-style-type: none"> Linux (i.e., Red Hat Enterprise ES 7.0 or higher)
Application Server Software	WebLogic Versions 12.2 and higher application servers.
VistALink Software	Version 1.6
Vista Kernel Software	Patch XU*8*504
KAAJEE_SSPI_8_781_RN.PDF	Release Notes describes the changes to KAAJEE 1.1 to include new features and enhancements.
KAAJEE_SSPI_8_781_IG.PDF	Installation Guide.
XU_8_781.zip	Security Provider Interface (SSPI) Software. The KAAJEE SSPI software download Zip file for installation on the application server.
XU_8_781.zip.MD5	Security Service Provider Interface (SSPI) Software Checksum. The MD5 checksum value for the KAAJEE SSPI software download Zip file.

This page is left blank intentionally.

2 Installation Overview

This section provides an overview of the installation procedures for the Kernel Authentication and Authorization for Java (2) Enterprise Edition (KAAJEE). The chapters that follow address the specific installations that comprise KAAJEE:

- **Error! Reference source not found.**



NOTE: Instructions for the VistA M Server installation can also be found in the description for Kernel Patch XU*8*504, located in the Patch Module on FORUM.

- **Error! Reference source not found.**

2.1 WebLogic v 12.2 and Higher Server Preparation

Follow the VistALink 1.6 instructions to deploy your VistALink connector(s).

2.2 KAAJEE SSPI Installation

1. Unzip the Kaajee Security Provider zip distribution into a staging folder.



FIRST-TIME INSTALLATIONS: Execute [this section](#) if you have *never* deployed KAAJEE SSPIs on a WebLogic Application Server.



UPGRADES: Go to the [Upgrade section](#) if you have deployed KAAJEE SSPIs on the WebLogic Application Server and will be installing (upgrading to) a newer version of the KAAJEE SSPIs.

FIRST-TIME INSTALLATIONS – Start here - Create KAAJEE Schema & SSPI Tables –

- a. Contact the **DBA to create the KAAJEE user ID, schema, and SSPI tables on the Oracle database.
- b. Create KAAJEE User ID & Schema.
- c. To create the SSPI tables, run the OracleTables.sql script, which can be found in the KAAJEE SSPI distribution zip file.
- d. Validate/Verify the Creation of the KAAJEE Database Schema & Tables. In summary, the DBA will need to perform the following procedures:
 - Identify and create an Oracle Tablespace to hold the KAAJEE schema.
 - Create a user account KAAJEE.
 - Give "connect" and "resource" and "unlimited tablespace" privileges to the user account.
 - The user account should have a "default" profile.

- Set the default tablespace for the KAAJEE user to the one created earlier.
- Set the default "TEMP" tablespace for the KAAJEE user.

New installation only - Create KAAJEE SSPI Tables

KAAJEE requires the following two SSPI SQL database tables:

Table 2-1. Caché Database—KAAJEE SSPI SQL table definitions

KAAJEE SSPI Table Name	Description
PRINCIPALS	This table has users and group data and is stored in a database.
GROUPMEMBERS	This table has users and group mappings and is stored in a database.



NOTE: We recommend that you create the KAAJEE SSPI database tables in the same schema created in the previous step.

Run the createSchema.sql script, which can be found in the KAAJEE SSPI distribution zip file (i.e., XU_8_708.zip) in the following directory:

<STAGING_FOLDER> /sql/createSchema.sql

This SQL script creates the required KAAJEE SSPI SQL table definitions.

Use the terminal, or other similar software of your choice, to import the SQL script and run it to create/edit the SSPI SQL table definitions (Table 2-1):

Figure 2-1. Database—Sample SSPI SQL script for KAAJEE table definitions

```
drop table Principals;
drop table GroupMembers;

create table Principals ( name varchar(32) not null, isuser varchar(10) not null, password varchar(40),
CONSTRAINT Principals_pk PRIMARY KEY (name,isuser));

create table GroupMembers ( principal varchar(40) not null, mygroup varchar(32) not null, CONSTRAINT
GroupMembers_pk PRIMARY KEY (principal, mygroup));
```


UPGRADE and continuing the FIRST-TIME Installation

1. Edit the createDSSSPI.properties file with information pertaining to your environment:

There are several property values to edit. Pay special attention to the case and whitespace. The ds.name and the ds.jndi.name should be left unchanged. The rest of the datasource information gets copied from the existing KaajeeDatabase.properties file (for upgrades).

```
# AdminServer connection details.
admin.username=arsen
admin.password=xxx
admin.url=t3://vaauseamappdev5.aac.va.gov:7001

ds.url=jdbc:oracle:thin:@//vaausdsadr668-scan.aac.va.gov:1521/ADRSBX02.AAC.VA.GOV
ds.driver=oracle.jdbc.xa.client.OracleXADataSource
ds.username=KAAJEE
ds.password=xxx

ds.target.type=Server
ds.target.name=appdev5domladminsvr
domain.name=appdev5doml

# don't change
provider.name=KaajeeManageableAuthenticator
ds.name=SSPIDS
ds.jndi.name=jdbc/SSPIDS
```

2. Locate and Run the setWLSEnv.sh script on the application server Ex(12.2):

```
[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 for the 12.2 version of application server)





3. Run the java weblogic.WLST and pass the required properties file to the createDSSSPI.py

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

4. The script will attempt to create a new datasource, wire it up to a database and instantiate an instance of SQLAuthenticationProvider. Upon successful script completion, you will be asked to shutdown an admin server. Type “Y” to agree.
5. Start the server; Log onto admin console.
 - a. 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

- c. Click on New in the Authentication tab
6. Find the KaajeeManageableAuthenticator, ensure Control Flag is set to '**OPTIONAL**'.
- d. When returned to the Authentication page, select the DefaultAuthenticator Authentication Provider.
- e. Ensure that Control Flag is '**SUFFICIENT**'.

This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequence.

 Name:	DefaultAuthenticator	The name of this WebLogic Authentication provider. More Info...
 Description:	WebLogic Authentication Provider	A short description of the Authentication provider. More Info...
 Version:	1.0	The version number of the Authentication provider. More Info...
 Control Flag:	<input type="text" value="SUFFICIENT"/>	Returns how the login sequence uses the Authentication provider. More Info...

- f. 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 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)



NOTE: If this is a first-time install, you will not see users populated in the Oracle tables or in the WebLogic console.

- b. Confirm presence of application-level users retrieved by the KaajeeManageableAuthenticator –

<input type="checkbox"/>	PATS_DUZ_10000000081~CMPSYS_110	KaajeeManageableAuthenticator
<input type="checkbox"/>	pats_DUZ_10000000081~CMPSYS_110	KaajeeManageableAuthenticator
<input type="checkbox"/>	PATS_DUZ_10000000082~CMPSYS_110	KaajeeManageableAuthenticator
<input type="checkbox"/>	pats_DUZ_10000000082~CMPSYS_110	KaajeeManageableAuthenticator

This page is left blank intentionally.

Appendix A: Installation Back-Out or Roll-Back Procedure

KAAJEE SSPI rollback

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

```
[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 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.

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 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 absence of application-level users retrieved by the KaajeeManageableAuthenticator

This page is left blank intentionally.