KERNEL AUTHENTICATION & AUTHORIZATION FOR J2EE Single Sign-On Web Application Plugin (KAAJEE SSOWAP) VERSION 8.0.791

FOR WEBLOGIC (WL) VERSIONS 12.2 AND HIGHER

INSTALLATION GUIDE

May 2024

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)
05/2024	Updated version of KAAJEE SSOWAP **KAAJEE SSOWAP patch, XU*8.0*791**	REDACTED
12/2021	New version of KAAJEE SSOWAP for WL 12/2/Java 8 **KAAJEE SSOWAP patch, XU*8.0*747,** makes Technical Reference Model (TRM) compliance changes and upgrades/certification of a KAAJEE Single Sign-On Web Application Plugin (SSOWAP) component for the WebLogic 12.2/Java 1.8 platform and above.	REDACTED
09/2021	WebLogic 12.2/Java 8 release.	REDACTED
09/2020	Splitting information into new SSOWAP-focused documentation.	REDACTED
07/2018	Updated software and documentation with TRM and Fortify compliance items. **Software Version: 1.2.0.005** **Kernel Patch: XU*8.0*695**	REDACTED
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**	• REDACTED

Contents

Date	Description	Author(s)
05/2024	Updated version of KAAJEE SSOWAP **KAAJEE SSOWAP patch, XU*8.0*791**	REDACTED
12/2021	New version of KAAJEE SSOWAP for WL 12/2/Java 8 **KAAJEE SSOWAP patch, XU*8.0*747,** makes Technical Reference Model (TRM) compliance changes and upgrades/certification of a KAAJEE Single Sign-On Web Application Plugin (SSOWAP) component for the WebLogic 12.2/Java 1.8 platform and above.	REDACTED
	Kernel Patch: XU*8.0*504	
05/2006	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. **Software Version: 1.0.0.019** **Security Service Provider Interface (SSPI) Version: 1.0.0.010** **NOTE:** For a description of the current KAAJEE software version numbering scheme, please review the readme.txt file distributed with the KAAJEE software. In the future, the Development Technology Advisory Committee (DTAC) will be the authoritative source for determining future version numbering schemes for all HealtheVet-VistA software file and folder names.	• REDACTED

Patch Revisions

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

Contents

Figures

Tables

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 HealthVet-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. VistA M Server Installation Instructions
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.

Symbol	Description
	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.
	Instructions that only apply to Microsoft Windows operating systems (i.e., Microsoft Windows 2000 or XP) 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 7.0 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 19*g*—Database (e.g., Security Service Provider Interface [SSPI] or Standard Data Services [SDS] 19.0 (or higher) database/tables)
- Oracle SQL*Plus Software 13 (or higher)

This manual provides an overall explanation of the installation procedures and functionality provided by the Kernel Authentication & Authorization for J2EE Single Sign-On Web Application Plugin (KAAJEE SSOWAP) on Weblogic Application Server Versions 12.2 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.

Reference Materials

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

- *Kernel Systems Management Guide*
- *VistALink Installation Guide*
- *VistALink System Management Guide*
- *VistALink Developer Guide*

HealtheVet-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/

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

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

HealtheVet-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 HealtheVet-Veterans Health Information Systems and Technology Architecture (VistA) Kernel Authentication and Authorization for Java (2) Enterprise Edition Single SignOn Web Application Plugin (KAAJEE SSOWAP) and related software.

KAAJEE SSOWAP is *not* an application, but a framework. Users of the software need to understand how it integrates in their working environment. Thus, installing KAAJEE SSOWAP 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 SSOWAP provides secure two factor sign-on architecture for HealtheVet-VistA Web-based applications.

These HealtheVet-VistA Web-based applications are able to authenticate 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:

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

1.3 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: • Linux (i.e., Red Hat Enterprise ES 7.0 or higher)
Application Server Software	WebLogic Versions 12.2 and higher application servers.
SSPI Software	KAAJEE SSPI 8.0.748 and above
VistALink Software	Version 1.6.7
VistA Kernel Software	Patch XU*8*504
KAAJEE_SSOWAP_8.0.791_RN.PDF	**Release Notes** describes the changes to KAAJEE SSOWAP to include new features and enhancements.
KAAJEE_SSOWAP_8.0.791_IG.PDF	**Installation Guide**.
KAAJEE_SSOWAP_8.0.791_DEPL.PDF	**Deployment Guide** outlines the details of KAAJEE-related software and gives guidelines on how the software is used within HealtheVet-Veterans Health Information Systems and Technology Architecture (VistA). It contains the User Manual, Programmer Manual, and Technical Manual information for KAAJEE.
XU_8.0.791.zip	**KAAJEE SSOWAP Software.** The KAAJEE SSPI software download Zip file for installation on the application server.
XU_8.0.791.zip.MD5	**KAAJEE SSOWAP 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 Single SignOn Web Application Plugin (KAAJEE SSOWAP). The chapters that follow address the specific installations that comprise KAAJEE:

- VistA M Server Installation Instructions

> **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.

2.1 VistA M Server

Kernel Patch XU*8*504 is the custodial patch for the M server installation of the KAAJEE SSOWAP software. In addition, ensure that the M server system is current with patches for KERNEL, VistALink, and Remote Procedure Call (RPC) Broker.

> **NOTE:** For information on the minimum software tools and files that are required to install the KAAJEE software, see the section titled "Application Server Environment Requirements" in this documentation.

2.2 WebLogic Server

WebLogic server will need to be configured with a security identity certificate for the server and added to the keystore along with intermediary and root certificates.

2.3 Deploy a J2EE Web-Based Application with the KAAJEE SSOWAP "Plug-In"

For details how to deploy a J2EE web-based application with the KAAJEE "plug-in," refer to the Kernel Authentication & Authorization for J2EE Single SignOn Web Application Plugin (KAAJEE SSOWAP) Deployment Guide for Weblogic Application Server Versions 12.2 and higher.

3 VistA M Server Installation Instructions

The installation instructions in this section are directed at the Information Resource Management (IRM) staff located at a site and are applicable for the Test/Production accounts in the VistA Caché environment.

NOTE: For additional information on the VistA M server installation of the KAAJEE software, see the description for Kernel Patch XU*8*504 located in the Patch Module on FORUM.

NOTE: For information on the minimum software tools and files required to install the KAAJEE software in its entirety (i.e., covering the Java 2 Enterprise Edition [J2EE] and VistA M installations), see the section titled "Application Server Environment Requirements" in this documentation.

3.1 Confirm/Obtain VistA M Server Distribution Files *(recommended)*

The following files and environment configuration are needed to install the Kernel Authentication and Authorization Java (2) Enterprise Edition (KAAJEE)-related VistA M Server software:

Table 3-1. KAAJEE-related VistA M Server distribution files and environment configuration

Minimum Software/Configuration	Description
Operating System Software	InterSystems Caché
Fully Patched M Accounts	You should have both a development Test account and a Production account for KAAJEE software. The account(s) *must* contain the *fully* patched versions of the following software: • Kernel 8.0 • Kernel Toolkit 7.3 • RPC Broker 1.1 • VA FileMan 22.2

Minimum Software/Configuration		Description
		• VistALink 1.6.7
VistALink Application Server Software	VistALink VistA Software	
Version 1.6.7	XOBV*1.6*7	
VistA Kernel Software		Patch XU*8*504
KAAJEE_SSOWAP_8.0.791_RN.PDF		**Release Notes** describes the changes to KAAJEE SSOWAP to include new features and enhancements.
KAAJEE_SSOWAP_8.0.747_IG.PDF		**Installation Guide** describes in detail the installation procedures for KAAJEE.
KAAJEE_SSOWAP_8.0.747_DEPL.PDF		**Deployment Guide** outlines the details of KAAJEE-related software and gives guidelines on how the software is used within HealtheVet-Veterans Health Information Systems and Technology Architecture (VistA). It contains the User Manual, Programmer Manual, and Technical Manual information for KAAJEE.

REF: For the KAAJEE software release, all distribution files, unless otherwise noted, are available for download from the Enterprise VistA Support (EVS) anonymous directories:

- Preferred Method REDACTED

  This method transmits the files from the first available FTP server.

3.2 Site Configuration *(required)*

The KERNEL SYSTEM PARAMETERS file (#8989.3) holds the site parameters for the installation of Kernel. This allows users to configure and fine tune Kernel for:

- Site-specific requirements and optimization needs.
- HealtheVet-VistA software application requirements.

Some parameters are defined by IRM during the Kernel software installation process (e.g., agency information, volume set multiple, default parameters). Other parameters can be edited subsequent to installation (e.g., spooling, response time, and audit parameters). Priorities can also be set for interactive users and for TaskMan. Defaults for fields (e.g., timed read, auto menu, and ask device) are defined for use when not otherwise specified for a user or device. The

values in the KERNEL SYSTEM PARAMETERS file (#8989.3) can be edited with the Enter/Edit Kernel Site Parameters option [XUSITEPARM].

3.2.1 Validate User Division Entries

During the authentication process for Web-based applications that are KAAJEE-enabled, KAAJEE displays a list of validated institutions to the user. KAAJEE uses the Standard Data Services (SDS) tables 13.0 (or higher) as the authoritative source to validate the list of station numbers that are stored in the <login-station-numbers> tag in the kaajeeConfig.xml file. After a user selects an institution from this validated list, the software follows the VistA authentication process (i.e., Kernel Signon).

NOTE: The validation of the VistA institution occurs *before* the actual login to the VistA M Server, but *after* the user selects the **Login** button on the KAAJEE Web login page. The selected institution is checked against the SDS 19.0 (or higher) tables for an entry and a VistA Provider. Also, KAAJEE checks that an entry exists in the KAAJEE configuration file.

The VistA authentication process (i.e., Kernel Signon) requires that each user be associated with at least one division/institution. The local DUZ(2) variable on the VistA M Server stores the Internal Entry Number (IEN) of the login institution. Entries in the DIVISION multiple (#16) in the NEW PERSON file (#200) permit users to sign onto the institution(s) stored in this field. If there are *no* entries in the DIVISION multiple (#16) of the NEW PERSON file (#200) for the user signing on, information about the login institution comes from the value in the DEFAULT INSTITUTION field (#217) in the KERNEL SYSTEM PARAMETERS file (#8989.3).

Therefore, sites running any application that is used to sign onto VistA *must* verify that the institution(s) are set up correctly for the application user, as follows:

- **Multi-divisional Sites:** The DIVISION multiple (#16) in the NEW PERSON file (#200) *must* be set up for all users. This assures that the application users have access to only those stations for which they are authorized.
- ***Non*-multi-divisional Sites:** Sites *must* verify that the value in the DEFAULT INSTITUTION field (#217) in the KERNEL SYSTEM PARAMETERS file (#8989.3) is correct.

3.2.2 Validate Institution Associations

KAAJEE uses the Standard Data Services (SDS) tables 19.0 (or higher) as the authoritative source for institution data. Data in the ASSOCIATIONS Multiple field (#14) in the local site's INSTITUTION file (#4) is uploaded to FORUM, which is then used to populate the SDS tables. Thus, in order to sign onto VistA the data in the ASSOCIATIONS Multiple field (#14) *must* have correct information.

The ASSOCIATIONS Multiple is used to link groups of institutions into associations. The ASSOCIATIONS Multiple consists of the following subfields:

- ASSOCIATIONS (#.01)—This field is a pointer to the INSTITUTIONS ASSOCIATION TYPES file (#4.05).
- PARENT OF ASSOCIATION (#1)—This field points back to the INSTITUTION file (#4) to indicate the parent of the association. This field is cross-referenced to find the children of a parent for an association type.

In the ASSOCIATIONS Multiple, child facilities point to their administrative parent. All clinics point to a division parent, all divisions point to a primary facility parent, primary facilities point to an HCS parent or VISN parent. HCS entries point to a VISN parent. Thus, all parent relationships eventually resolve to a VISN. The first entry (IEN=1) in the ASSOCIATIONS Multiple references the VISN to which the division belongs, so that the PARENT OF ASSOCIATION field in that entry *must* point to a VISN in the INSTITUTION file (#4), and the second entry (IEN=2) references the actual parent of the current institution.

Therefore, sites running any application that is used to sign onto VistA *must* verify that the ASSOCIATION Multiple field (#14) in the INSTITUTION file (#4) has a file entry for their own institution (and all child divisions if it's a multi-divisional site), and make sure that it is set up correctly. If changes are needed, use the IMF edit option [XUMF IMF ADD EDIT] to update those entries.

REF: For more information on the XUMF IMF ADD EDIT option as well as the ASSOCIATIONS Multiple and PARENT OF ASSOCIATION fields data requirements, please refer to the Institution File Redesign (IFR) supplemental documentation located on the VDL at the following Web address:

REDACTED

3.3 Do Not Run any KAAJEE-based Software During the Installation *(recommended)*

No HealtheVet-VistA Web-based and KAAJEE-enabled software should be running while the KAAJEE installation on the VistA M Server is taking place.

3.4 Verify KIDS Install Platform *(required)*

Verify that the Kernel Installation and Distribution System (KIDS) platform on your system is ready to install VistA M Server patches.

3.5 Retrieve and Install the KAAJEE-related VistA M Server Patch *(required)*

Kernel Patch XU*8*504 is the custodial patch for the M server installation of the KAAJEE software. All VistA M Server patches are distributed in Kernel 8.0 KIDS format. Follow the normal procedures to obtain and install released patches.

Make sure that the Kernel, Kernel Toolkit, RPC Broker, VA FileMan, and VistALink software is fully patched. Patches must be installed in their published sequence.

REF: For more information on these patches, please refer to the Patch Module on FORUM.

Congratulations! You have now completed the installation of KAAJEE-related software on the VistA M Server.

3.6 Configure the security certificate on the WebLogic Server *(required)*

UPGRADES: Skip this step if you have already configured the certificate and the keystore, unless it is specifically noted that changes are required in the KAAJEE SSOWAP software release e-mail or Web site.

To configure the certificate, use the following steps:

1. Obtain the identity certificate from the certificate authority at VA - **yourServerCert.crt**

2. Obtain the intermediary and root certificates from the certificate authority at VA - **DigiCert-Global-G2-TLS-RSA-SHA256-2020-CA1.cer** and **DigiCert-Global-Root-G2.cer** in this example.

3. Add the identity cert and the intermediary/root certs to the same keystore. Below are the sample commands:

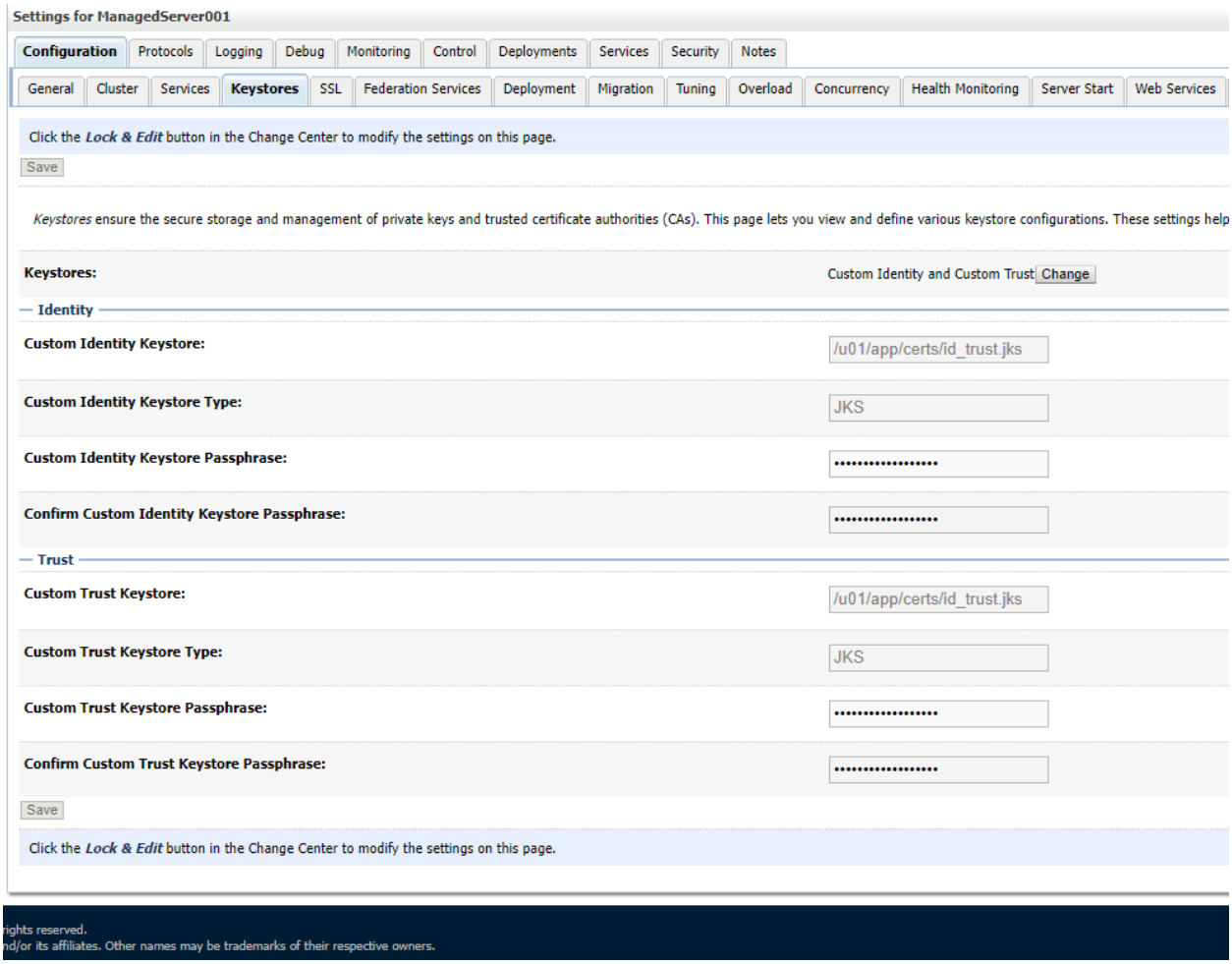
   keytool -import -alias DigiCert-Global-Root-G2 -file **DigiCert-Global-Root-G2.cer** -keystore **yourServerStore.jks** -storepass XXX ;

   keytool -import -alias DigiCert-Global-G2-TLS-RSA-SHA256-2020-CA1 -file **DigiCert-Global-G2-TLS-RSA-SHA256-2020-CA1.cer** -keystore **yourServerStore.jks** -storepass XXX ;

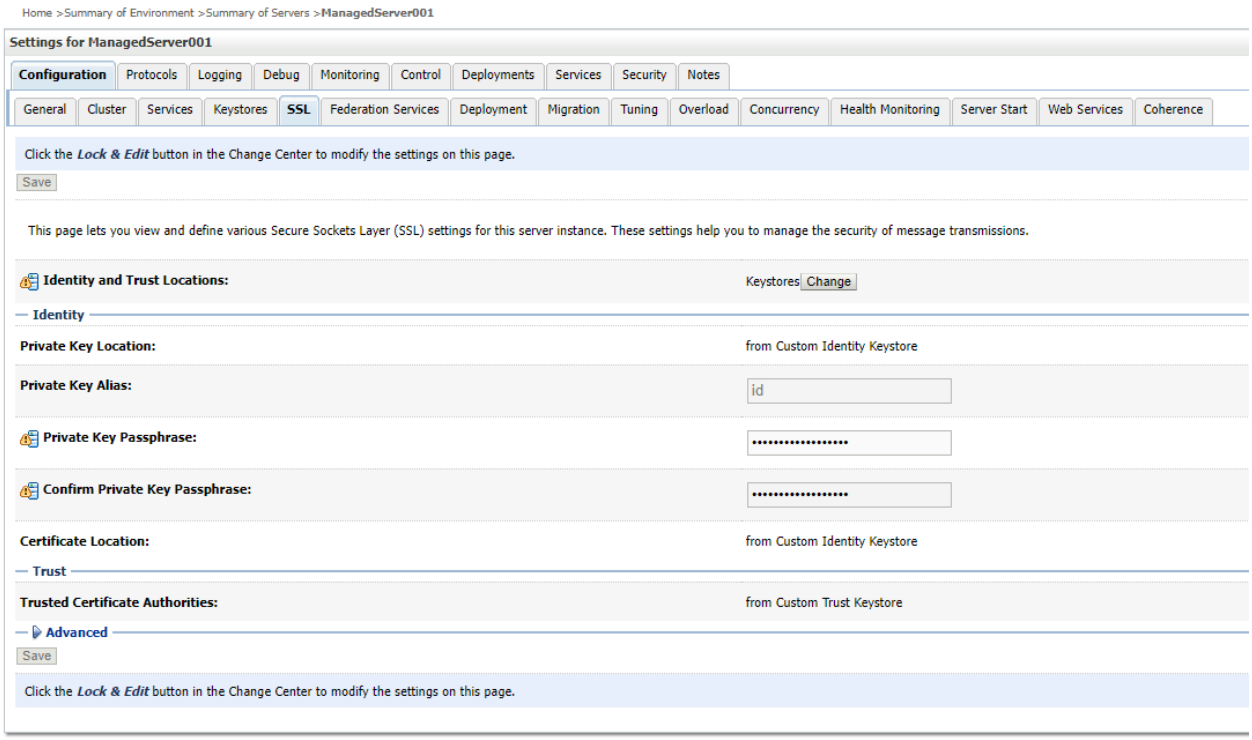
   keytool -import -alias id -file **yourServerCert.crt** -keystore **yourServerStore.jks** -storepass XXX ;

4. Take a note of the alias under which the identity cert has been imported.

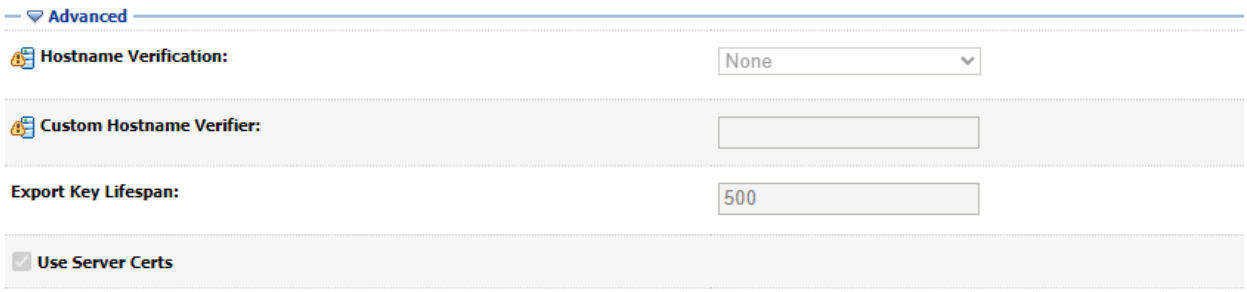
5. Install the **yourServerStore.jks** on the server by navigating to: Home >Summary of Environment >Summary of Servers >**ManagedServer001**



6. Configure the identity certificate for mutual SSL connection with the STS service; use the same alias id you have entered on step 4:



7. Make sure the **Use Server Certs** option is checked under the **Advanced** section:



Congratulations! You have now completed the installation of identity and root certs on the WebLogic Server.

3.7 Configure SDS 19.0 (or higher) JDBC Connections with the WebLogic Server *(required)*

UPGRADES: Skip this step if you have already configured the SDS tables, unless it is specifically noted that changes are required in the KAAJEE software release e-mail or Web site.

To configure the Standard Data Services (SDS) tables for a J2EE DataSource, please refer to the "Configuring for a J2EE DataSource" topic in the *SDS API Installation Guide*.

REF: The *SDS API Installation Guide* is included in the SDS software distribution ZIP files, which are available for download at the following Web address:

REDACTED

3.8 Ensure the Existence of, or Creation, of a SSOWAP_USER with Administrative Privileges *(required)*

For KAAJEE to execute correctly, the files web.xml and weblogic.xml has content that declares that KAAJEE will run with the needed privileges.

Check that your WebLogic server already has a user named "SSOWAP_USER" and is part of the **Administrators** group, or it is part of the **Admin** global security role. If there is such a user, your installation of the KAAJEE enable web application will execute properly.

WebLogic Security Realm:

If you need to create a new user in WebLogic, ensure that

1. It is named **SSOWAP_USER**
2. It is assigned to the **Administrators** group

Active Directory Authentication Provider:

If your WebLogic domain has integrated an Active Directory authentication provider, and you will be creating the user in Active Directory, ensure that

1. It is named **SSOWAP_USER**
2. The user is part of a group that can be mapped in the WebLogic security realm to the Global Security Role named **Admin**.

The following shows the contents of the web.xml and weblogic.xml files as it pertains to the **KAAJEE** user.

REF: See the KAAJEE Deployment Guide for the contents of the web.xml and weblogic.xml files and additional details.

web.xml:
This file has a <run-as> tag, which causes it to run with the necessary administrative privileges. In addition, a corresponding security-role tag is defined. See the sample in Figure 3-1.

Figure 3-1. Sample excerpt from a web.xml file—Using the run-as and security-role tags

```
<servlet>
  <servlet-name>LoginController</servlet-name>
  <servlet-class>
          gov.va.med.authentication.kernel.servlet.ssowap.LoginController
  </servlet-class>
    <run-as>
     <role-name>adminuserrole</role-name>
    </run-as>
</servlet>

<security-role>
 <role-name>adminuserrole</role-name>
</security-role>
```

weblogic.xml:

This file has a <run-as> tag, which causes it to run as an administrative user whose username is "KAAJEE." In addition, a corresponding security-role tag is defined.

Figure 3-2. Sample excerpt from a weblogic.xml file—Using the run-as-role-assignment tag

```
<run-as-role-assignment>
  <role-name>adminuserrole</role-name>
  <run-as-principal-name>SSOWAP_USER</run-as-principal-name>
</run-as-role-assignment>
```

Important! The "SSOWAP_USER" user or alternate must exist in the WebLogic Application server and have system administration privileges.

3.9 Edit the KAAJEE Configuration File *(required)*

3.9.1 Locate the kaajeeConfig.xml File *(required)*

The EMC, or Application Server Administrator, must first locate the kaajeeConfig.xml file in the Web application ear or standalone war file, as follows:

Exploded Ear Files

Navigate to the WEB-INF directory in the sample application's exploded ear/war file—Locate the KAAJEE configuration file (i.e. kaajeeConfig.xml)

Ear Files

1. Unzip the application's ear file—Explode the artifact.
2. For any war file that implements KAAJEE authentication inside the ear file, unzip the war file.
3. Navigate to the WEB-INF directory—Locate the KAAJEE configuration file (i.e. kaajeeConfig.xml)

Standalone War Files

1. Unzip the application's war file that implements KAAJEE authentication.
2. Navigate to the WEB-INF directory—Locate the KAAJEE configuration file (i.e. kaajeeConfig.xml)

The following is a sample excerpt of the kaajeeConfig.xml file as distributed with KAAJEE SSOWAP:

Figure 3.9-1. Sample Station Number excerpt of the kaajeeConfig.xml file

```
<?xml version="1.0" encoding="UTF-8"?>
<kaajee-config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="kaajeeConfig.xsd">

    <!-- host application name, used for login page display and logging -->
    <host-application-name>SSOi Web Application Plugin (SWAP) 2FA release</host-application-name>

    <context-root-name>/swap</context-root-name>

    <!-- default target URL/URI in case weblogic fails to provide an authentication target -->
    <default-target-url>/swap</default-target-url>

    <!-- put each station number for KAAJEE login here -->
    <!-- taken out station 110, as it was causing production environment errors ARM 07/07/09 -->

    <!-- put the system announcement here. Use ~ for a line break, or ~ ~ for a
         paragraph break. -->
    <system-announcement>
    U.S. Government Computer System
    ~ ~
    U. S. government systems are intended to be used by authorized government network users for viewing and retrieving information only, except as otherwise exp
    ~ ~
    The data and documents on this system include Federal records that contain sensitive information protected by various Federal statutes, including the Privac
    ~ ~
    All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review and action inc
    ~ ~
    Unauthorized user attempts or acts to (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this syst
    </system-announcement>

    <sts-service-address>https://preprod.services.eauth.va.gov:9301/STS/RequestSecurityToken</sts-service-address>
    <!-- set to true to return a user's "New Person" division multiple as part
         of login -->
    <user-new-person-divisions retrieve="true" />

    <!-- set to true to return all children divisions of the login division's
         computing facility, as part of login -->
    <computing-facility-divisions retrieve="true" />

    <cactus-insecure-mode enabled="false" />

</kaajee-config>
```

3.9.2 Edit the Station Number List in the kaajeeConfig.xml File

With KAAJEE SSOWAP station numbers are retrieved from the VA Provisioning Services dynamically.
No manual editing of station numbers the kaajeeConfig.xml file is required.

NOTE: There is a new configuration setting being introduced: <sts-service-address> - this is a required setting and KAAJEE SSOWAP will not work without it.

3.9.3 Redeploy and Test the Web Application with the Updated kaajeeConfig.xml File *(required)*

Use WebLogic to redeploy the Web application ear or standalone war file with the updated kaajeeConfig.xml file on all appropriate application servers. Test the redeployed application.

Exploded Ear Files

Leave application as an exploded ear file.

Packaged Ear Files

1. Zip any unzipped war files that implements KAAJEE authentication into a war, replacing the old war file.
2. Zip up the application ear file.

Standalone War Files

Zip any unzipped war files into a war, replacing the old war file.

3.10 (Linux/Windows) Configure log4j for All J2EE-based Application Log Entries *(required)*

UPGRADES: Skip this step if you have already configured log4j *and* added the KAAJEE-specific logger information to the active log4j configuration file on the application server, unless it is specifically noted that changes are required in the KAAJEE software release e-mail or Web site.

In order to provide a unified logger and consolidate all log/error entries into one file, all J2EE-based application-specific loggers *must* be added to the same log4j configuration file, which should be the active log4j configuration file for the server. After locating the active log4j configuration file used on the server you are configuring (e.g., mylog4j.xml file), add in the KAAJEE (and Fat-client Kernel Authentication and Authorization, or FatKAAT) loggers to that file.

To locate the active log4j configuration file, look for the"-Dlog4j.configuration=" argument in the startup script file (i.e., setDomainEnv.sh/.cmd). The "-Dlog4j.configuration=" should be set to the absolute location of the configuration file (e.g., c:/mydirectory/mylog4j.xml). If no such argument is present, look for a file named "log4j.xml" in a folder on the server classpath.

You *must* configure log4j for the first time, if all three of the following conditions exist:

- The "-Dlog4j.configuration=" argument does *not* exist in the WebLogic JVM startup script files.
- The "log4j.xml" file does *not* exist in the classpath.
- There is no pre-existing log4j configuration file in the folder placed on the classpath of the WebLogic Application Server containing the configuration files for all HealtheVet-VistA J2EE applications (e.g., <HEV CONFIGURATION FOLDER>).

For first time log4j configuration procedures, please refer to the "log4j Configuration File" topic in the *VistALink Installation Guide (1.6)*. Also, sample log4j configuration files are included with the VistALink 1.6 software distribution.

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

Once the log4j file is initially configured, you need to configure the file specifically for KAAJEE log entries as outlined below.

REF: For more information on log4j guidelines, please refer to the Application Structure & Integration Services (ASIS) *Log4j Guidelines for HealtheVet-VistA Applications* document available at the following Web address:

http://vista.med.va.gov/vistaarch/healthevet/Documents/Log4j%20Guidance%201.0.doc

3.10.1 Configure Application for log4j

KAAJEE SSOWAP has been updated with the log4j2 API. Follow the Log4J instructions (https://logging.apache.org/log4j/log4j-2.1/manual/configuration.html) to configure your application for Log4J.

Congratulations! You have now completed the installation and configuration of KAAJEE-related software on the WebLogic Application Server.

This page is left blank intentionally.

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

J2EE Application Server

The Java component in KAAJEE SSOWAP is not a stand-alone Web application. It is an embedded set of Java components and a Java library to be embedded within a consuming Web application. Therefore, there is no back-out/roll-back procedure specific to KAAJEE SSOWAP. Each consuming application would have to devise their own back-out/roll-back procedure.

This page is left blank intentionally.