HP Select Audit Software

for the Windows® operating system

Software Version: 1.02

PKCS11 Keystores Configuration Guide

Document Release Date: July 2007
Software Release Date: July 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

HP provides third-party products, software, and services that are not HP Branded “AS IS” without warranties or representations of any kind from HP, although the original manufacturers or third party suppliers of such products, software and services may provide their own warranties, representations or conditions. By using this software you accept the terms and conditions.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

HP Select Audit includes software developed by third parties. The software HP Select Audit uses includes:

- ANTLR Copyright 2005 Terrence Parr.
- commons-logging from the Apache Software Foundation.
- Install Anywhere, Copyright 2004 Zero G Software, Inc.
- Jasper Decisions Copyright 2000-2006 JasperSoft Corporation.
- JavaScript Tree, Copyright 2002-2003 Geir Landro.
- Legion of the Bouncy Castle developed by Bouncy Castle.
- log4J from the Apache Software Foundation.
- Microsoft SQL Server 2005 JDBC Driver
- OpenAdaptor from the Software Conservancy.
- Oracle JDBC Thin Driver
- Quartz, Copyright 2004 - 2005 OpenSymphony
- spring-framework from the Apache Software Foundation.
- Tomahawk from the Apache Software Foundation.
- treeviewjavascript from GubuSoft.
- Xalan-Java from the Apache Software Foundation.
- Xerces-Java version from the Apache Software Foundation.

Please check the `<install_dir>/3rd_party_license` folder for expanded copyright notices from such third party suppliers.

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP software support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To find more information about HP Passport, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Configuring Select Audit for PKCS11 Keystores

HP Select Audit software can digitally sign the audit data using keys stored on smart cards, USB tokens and HSMs. Integration with such devices requires a PKCS#11 provider which makes cryptographic operations of these devices accessible using the JCA/JCE framework.

Select Audit interoperates with the IAIK provider available at `https://jce.iaik.tugraz.at/sic/products/core_crypto_toolkits/pkcs_11_provider`. This PKCS11 provider is not included in Select Audit and must be acquired and licensed separately.

Download and expand the IAIK archive. In the instructions below `%IAIK%` refers to its expansion location on Windows and `$IAIK` to the expansion location on UNIX.

This document provides instructions for Windows systems only.

Adding IAIK PKCS#11 Provider to Select Audit

These instructions assume that the commands given below are executed in a Command window.

1 Create new folders for `PKCS11` files in your `BEA_HOME` directory.

```
mkdir %BEA_HOME%\PKCS11

mkdir %BEA_HOME%\PKCS11\lib

mkdir %BEA_HOME%\PCKS11\shlib

mkdir %BEA_HOME%\PCKS11\properties
```

2 Add the required IAIK `JAR` files to WebLogic's classpath using the following steps:

```
copy %IAIK%\provider\lib-signed\iaikPkcs11Provider.jar
%BEA_HOME%\PKCS11\lib

copy %IAIK%\provider\lib-signed\iaik_jce.jar %BEA_HOME%\PKCS11\lib

copy %IAIK%\provider\lib-signed\iaikPkcs11Wrapper.jar
%BEA_HOME%\PKCS11\lib
```

3 Add the PKCS11 `JAR` files to your Audit Server's classpath:

- If you are running a standalone WebLogic server instance, add:

  ```
  CLASSPATH=%BEA_HOME%\PKCS11\lib\iaikPkcs11Provider.jar;%BEA_HOME%\
  PKCS11\lib\iaik_jce.jar;%BEA_HOME%\PKCS11\lib\
  iaikPkcs11Wrapper.jar;%CLASSPATH%
  ```

  to your `startWebLogic.cmd`.

- If you are using a custom script or service to start WebLogic, modify its startup settings accordingly.

- If you are running a cluster, the classpath for managed servers must also be modified to include these JAR files.
  - If the servers are started using the provided startManagedWebLogic.cmd script, it has to be modified in the same way as startWebLogic.cmd (above).
  - If the servers are started using the Node Manager, the classpath can be modified to add:

    ```
    %BEA_HOME%\PKCS11\lib\iaikPkcs11Provider.jar;%BEA_HOME%\PKCS11\
    lib\iaik_jce.jar;%BEA_HOME%\PKCS11\lib\iaikPkcs11Wrapper.jar
    ```

    through the WebLogic Console, under **Servers → <myserver> → Remote Start**.

    If you are using the Console, the classpath will be replaced and not appended. Be sure to include everything that was previously on the classpath.

4 Make the appropriate shared library available to your WebLogic domain.

```
copy %IAIK%/lib/win32/pkcs11wrapper.dll %BEA_HOME\PKCS11\shlib
```

- If you are running a standalone WebLogic server instance, edit the startWebLogic.cmd and add the following line after all other set JAVA_OPTIONS lines in the startWebLogic.cmd file.

  ```
  set JAVA_OPTIONS=%JAVA_OPTIONS%
  -Djava.library.path=%BEA_HOME%\PKCS11\shlib
  ```

- If you are using a custom script or service to start WebLogic, modify its startup settings accordingly.
- If you are running a cluster, the JAVA_OPTIONS for managed servers must also be modified to include these shared libraries.
  - If the servers are started using the provided startManagedWebLogic.cmd script, it has to be modified in the same way as startWebLogic.cmd (above).
  - If the servers are started using the Node Manager, the Java arguments can be modified to add:

    ```
    -Djava.library.path=%BEA_HOME%\PKCS11\shlib
    ```

    through the WebLogic Console, under **Servers → <myserver> → Remote Start**.

    If you are using the Console, the arguments will be replaced and not appended. Be sure to include everything that was previously in the arguments.

5 In %BEA_HOME%\PCKS11\properties, create a file called iaik\pkcs\pkcs11\provider\IAIKPkcs11.properties which will contain the configuration for the provider (what hardware PKCS#11 module to use). For example, if you will use ActivCard on Windows, the file would contain:

```
PKCS11_NATIVE_MODULE = C:/Windows/System32/acpkcs.dll
```

You will have to install a driver for your ActivCard reader (whether USB2 or pmscia, or other) and the ActivCard Gold software.

6 Add the IAIKPkcs11.properties file to your Audit Server's classpath:

- If you are running a standalone WebLogic server instance, add the following to your startWebLogic.cmd:

  ```
  CLASSPATH=%BEA_HOME%\PKCS11\properties;%CLASSPATH%
  ```

- If you are using a custom script or service to start WebLogic, modify its startup settings accordingly.

- If you are running a cluster, the classpath for managed servers must also be modified to include these JAR files.
  - If the servers are started using the provided `startManagedWebLogic.cmd` script, it has to be modified in the same way as `startWebLogic.cmd` (above).
  - If the servers are started using the Node Manager, the classpath can be modified to add:

    `%BEA_HOME%\PKCS11\properties`

    through the WebLogic Console, under **Servers → <myserver> → Remote Start**.

    If you are using the Console, the classpath will be replaced and not appended. Be sure to include everything that was previously on the classpath.

Go to the `dist` directory of the Audit Server installation and create a temporary working directory and go into that directory.

```
cd C:\Program Files\HP Openview\Select Audit\auditserver\dist

mkdir temp

cd temp
```

7 Extract the `auditserver.ear` file into this directory.

```
%BEA_HOME%\jdk142_08\bin\jar -xvf ..\auditserver.ear
```

8 Go to the `APP-INF\lib` directory.

```
cd APP-INF\lib
```

9 Extract the contents of the `auditservercommon.jar` file.

```
%BEA_HOME%\jdk142_08\bin\jar -xvf auditservercommon.jar
```

10 Change to the security directory.

```
cd com\hp\ov\selectaudit\auditserver\common\security
```

11 Edit the `ProviderFactory.xml` file, add the highlighted sections (or uncomment) and save the file.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans SYSTEM "http://www.springframework.org/dtd/
spring-beans.dtd">
<beans>
   <bean id="BcProvider"
            lazy-init="true"
            class="com.hp.ov.selectaudit.auditserver.common.security
            .BCProviderEntry">
            <property name="defaultProvider" value="true"/>
   </bean>

   <bean id="IaikProvider"
            lazy-init="true"
            class="com.hp.ov.selectaudit.auditserver.common.
            security.IAIKProviderEntry">
   </bean>

   <bean id="ProviderFactory"
```

```
            lazy-init="true"
            class="com.hp.ov.selectaudit.auditserver.common
            .security.ProviderFactory">
            <property name="providerEntries">
                 <list>
                     <ref local="BcProvider"/>
                     <ref local="IaikProvider"/>
                 </list>
            </property>
   </bean>
</beans>
```

12 In the `com\hp\ov\selectaudit\auditserver\common\security`, create a file called `IAIKProviderEntry.java` containing the following:

This location must correspond to the "class" specified in the `IaikProvider` bean in `ProviderFactory.xml` above and must also be the same as that specified in the "package" line in the Java code below.

```
package com.hp.ov.selectaudit.auditserver.common.security;
import iaik.pkcs.pkcs11.provider.IAIKPkcs11;
import iaik.security.provider.IAIK;

import java.security.Security;

import
com.hp.ov.selectaudit.auditserver.common.security.ProviderInterface;

public class IAIKProviderEntry implements ProviderInterface {
       protected boolean isDefaultProvider;
       protected String providerName1;
       protected String providerName2;

       public void loadProvider() throws Exception {
           IAIK p1 = new IAIK();
           providerName1 = p1.getName();
           Security.addProvider(p1);

           IAIKPkcs11 p2 = new IAIKPkcs11();
           providerName2 = p2.getName();
           Security.addProvider(p2);
       }

       public void removeProvider() throws Exception {
           if (providerName2 != null) {
                   Security.removeProvider(providerName2);
           }
```

```
            if (providerName1 != null) {
                    Security.removeProvider(providerName1);
            }
        }

        public boolean isDefaultProvider() {
            return isDefaultProvider;
        }

        public void setDefaultProvider(boolean isDefaultProvider) {
            this.isDefaultProvider = isDefaultProvider;
        }
}
```

13 Compile this Java code using the following command:

```
%BEA_HOME%\jdk142_08\bin\javac -classpath "C:\Program Files\HP
OpenView\Select Audit\auditserver\dist\temp\APP-INF\lib\
auditservercommon.jar;%BEA_HOME%\PKCS11\lib\iaikPkcs11Provider.jar;
%BEA_HOME%\PKCS11\lib\iaikPkcs11Wrapper.jar;%BEA_HOME%\PKCS11\lib\
iaik_jce.jar" IAIKProviderEntry.java
```

14 Change back to the `APP-INF\lib` directory.

```
cd C:\Program Files\HP
OpenView\SelectAudit\auditserver\dist\temp\APP-INF\lib
```

15 Create a new `auditservercommon.jar` file.

```
%BEA_HOME%\jdk142_08\bin\jar -cvf auditservercommon.jar com
```

16 Remove the `com` directory tree.

17 Create a new `ear` file.

```
cd C:\Program Files\HP OpenView\SelectAudit\auditserver\dist\temp
```

```
%BEA_HOME%\jdk142_08\bin\jar -cvf ..\auditserver.ear *
```

18 Connect to your Select Audit database using an SQL client and run the following SQL (remember to commit the changes).

```
delete from SACFGATTRIBUTE where AttributeName =
'dataSignatureCryptoProvider';
```

```
insert into SACFGATTRIBUTE values ('AuditServerConfig',
'dataSignatureCryptoProvider', 'IAIK PKCS#11:1');
```

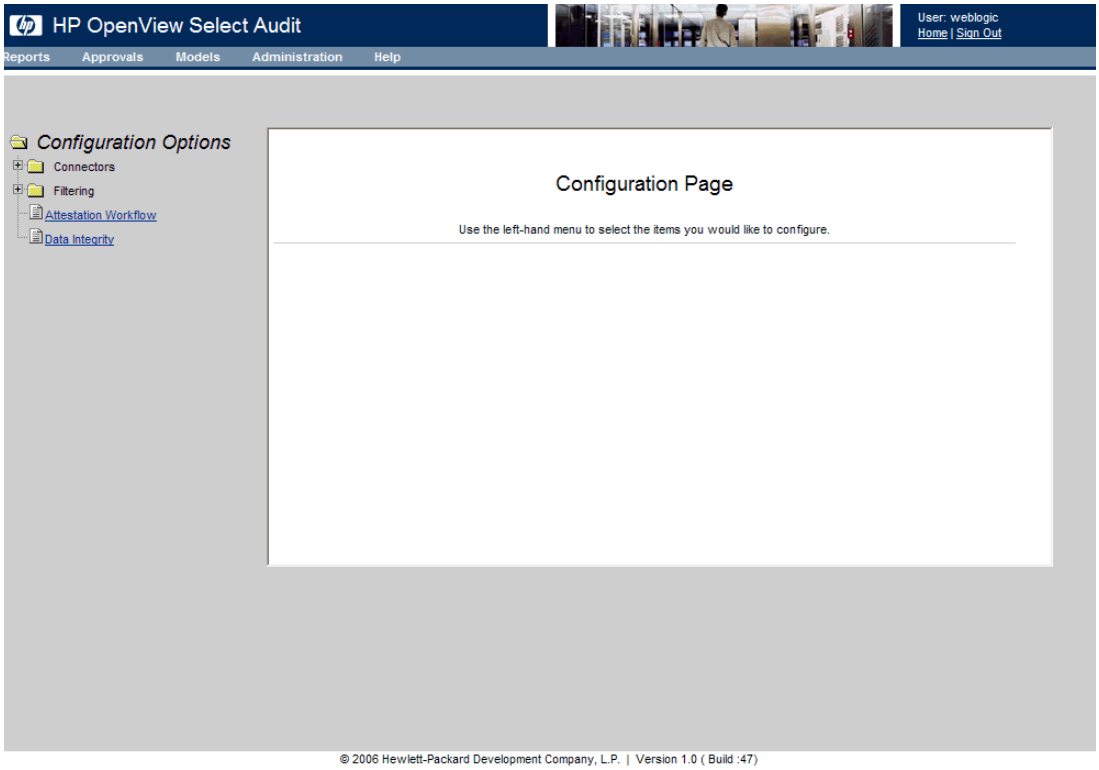
```
delete from SACFGATTRIBUTE where AttributeName =
'dataSignatureSecurityProvider';
```

```
insert into SACFGATTRIBUTE values ('AuditServerConfig',
'dataSignatureSecurityProvider', 'IAIK PKCS#11:1');
```

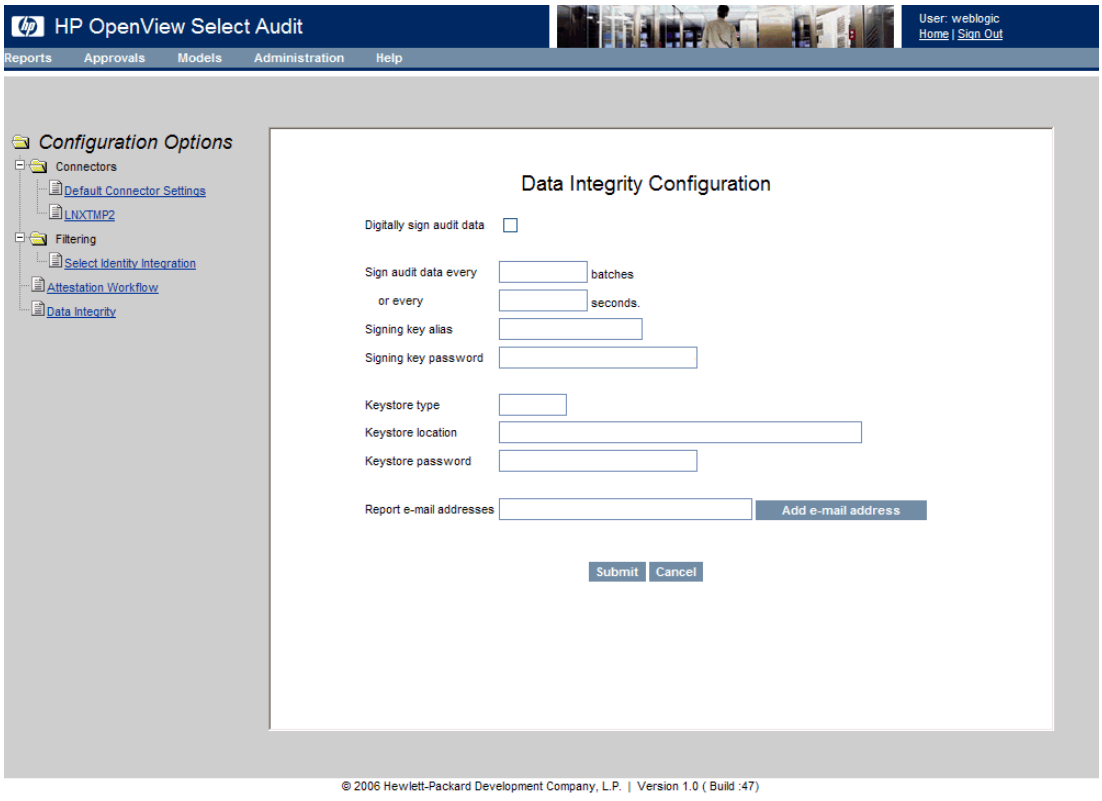
19 In the WebLogic console, deploy the new `auditserver.ear`. Restart WebLogic from the console of the machine where it is running as there may be issues with accessing the ActivCard reader when WebLogic is started from a Remote Administration window.

20 To configure Data Signing using a `PKCS11` keystore on an ActivCard, log on to the Select Audit Portal

21 In Select Audit, click **Administration** → **Configuration**. The **Configuration** screen opens.



22 Click **Data Integrity.** The **Data Integrity** screen opens.



23 On the **Data Integrity** screen, complete the fields as described in Table 1.

Table 1 Data Integrity Fields

Field	Data Entered
Signing key alias	Type your signing key alias.
Signing key password	Leave this field blank.
Keystore type	Type `pkcs11`.
Keystore location	Leave this field blank.
Keystore password	Type your Active Card's PIN.

24 Type the email address of the person who will receive the report in the **Report e-mail addresses** field and click **Add e-mail address**.

When you initially configure Data Integrity, you can type a semicolon separated list of email addresses. The email addresses will be saved when you click **Submit**. After Data Integrity is configured, you can add email addresses using **Add email address** without resaving the other parameters of the Data Integrity configuration.

25 Click **Submit**. The message **Successfully submitted** is shown at the bottom of the screen.