



# HP IT Executive Scorecard XS 9.50 Patch 04 Release Notes

Windows® operating system

Software version: September 2015

Documentation version: September 2015

The document includes the following topics:

	1
XS 9.50 Patch 04 for Windows .....	2
Installation Instructions for Patch 04 .....	2
Before you begin .....	2
Prerequisites .....	2
Patch Installation for single server configuration .....	3
Patch Installation for distributed configuration .....	3
Configure BOE and XS using the HTTPS proxy to access the report .....	4
Additional Steps Related to the CSA Content Update .....	6
Uninstallation Instructions for Patch 0004 .....	9
Defects Corrected in the XS 9.50 Patch 04 for Windows .....	10
Enhancements Added in the XS 9.50 Patch 04 for Windows .....	12
New Certifications .....	12
Documentation Changes Related to Patch 0004 .....	13
Update from a Trial License to a Permanent License in Distributed Environments .....	14
Activate the UCMDB Data Source .....	19
Activate the Integration .....	20
Connect to UCMDB on a Secured Connection .....	20
Consolidate Between BSM and UCMDB .....	20
Access and Deploy the UCMDB Push Adapter .....	21
Connect to CAC-enabled UCMDB Server .....	28
Configure CAC .....	39
Example of a CAC Configuration .....	51
Decimal Precision .....	57
XS 9.50 Patch 03 for Windows .....	59
Defects Corrected in the XS 9.50 Patch 03 for Windows .....	60

Enhancements Added in the XS 9.50 Patch 03 Revision 1 for Windows .....	61
New Certifications .....	61
XS 9.50 Patch 02 for Windows .....	62
Defects Corrected in the XS 9.50 Patch 02 for Windows .....	63
Enhancements Added in the XS 9.50 Patch 02 for Windows .....	64
New Certifications .....	64
XS 9.50 Patch 01 for Windows .....	65
Legal Notices .....	66
Documentation Updates .....	66
Support .....	67
About this PDF Version of Online Help .....	67

## XS 9.50 Patch 04 for Windows

This patch includes defects corrections as well as support for Cloud Service Automation (CSA) 4.5, SAP BusinessObjects Enterprise (BOE) 4.1 SP3, SAP BusinessObjects Data Services (BODS) 4.2 SP04, and Service Manager (SM) 9.41.

## Installation Instructions for Patch 04

### Before you begin

**Note:** Before installing XS 9.50 Patch 0004, you must upgrade SAP BusinessObjects Enterprise (BOE) and SAP BusinessObjects Data Services (BODS).

Review all instructions and the Hewlett-Packard SupportLine User Guide or your Hewlett-Packard support terms and conditions for precautions, scope of license, restrictions, and, limitation of liability and warranties, before installing this patch.

### Prerequisites

Before you install the patch, perform the following steps:

1. Back up your customized files.
2. Back up your databases.
3. Ensure Java 7 is installed.
4. Make sure XS is working before starting the patch installation.
5. Go to the HP Software Support Online web site at: <https://softwaresupport.hp.com/> go to **Product Information > Downloads**, and search and download HP IT Executive Scorecard 9.50 Patch 004.

## Patch Installation for single server configuration

### 1. Upgrade BOE and BODS:

- a. To upgrade SAP BusinessObjects Enterprise (BOE), double click **BIPLATSVR4103\_0-20010870.EXE** and follow the wizard.  
This procedure might take more than 2 hours.
- b. To upgrade SAP BusinessObjects Data Services (BODS), double click **DS4204\_0-20011165.EXE** and follow the wizard.
- c. To upgrade the BODS repository after the upgrade of the BODS service has completed, click **Start > SAP data services 4.2 > Data Services Repository Manager**. Log on and click the **Upgrade** button
- d. Restart the BOE server.

### 2. Install the Patch

**Note:** For an installation on 3 or 4 servers (distributed), install the patch (**HPXS\_9.50.0004.exe**) on each server including the BOE server.

- a. Run **HPXS\_9.50.0004.exe**.
- b. Once the patch is installed, restart the relevant server.

The patch installation is complete.

**Note:** If you had deployed a data source before you installed the patch, you must redeploy it using the following command:

```
$HPXS_HOME\agora\DataWarehouse\bin\dw_ds_automation.bat -task Redeploy -cp <CP_name> where CP_name is the name of the content pack you activated in ADMIN > Data Source Management.
```

## Patch Installation for distributed configuration

**Note:** Make sure that the patch is first installed on the BOE server, then on the DWH server, and last on the XS server, in that order.

### 1. Upgrade BOE and BODS:

**Note:** You must install the BOE upgrade and BODS upgrade on both the BOE and DWH server.

### 2. Upgrade BOE and BODS on the BOE Server:

- a. To upgrade SAP BusinessObjects Enterprise (BOE), double click **BIPLATSVR4103\_0-20010870.EXE** and follow the wizard.  
This procedure might take more than 2 hours.
- b. To upgrade SAP BusinessObjects Data Services (BODS), double click **DS4204\_0-20011165.EXE** and follow the wizard.
- c. Restart the BOE server.

### 3. Upgrade BOE and BODS on the DWH server:

- a. To upgrade SAP BusinessObjects Enterprise (BOE), double click **BIPLATSVR4103\_0-20010870.EXE** and follow the wizard.

This procedure might take more than 2 hours.

- b. To upgrade SAP BusinessObjects Data Services (BODS), double click **DS4204\_0-20011165.EXE** and follow the wizard.
- c. To upgrade the BODS repository after the upgrade of the BODS service has completed, click **Start > SAP data services 4.2 > Data Services Repository Manager**. Log on and click the **Upgrade** button
- d. Restart the DWH server.

### 4. Install the Patch

- **On the BOE server:**

- i. Run **HPXS\_9.50.0004.exe**.
- ii. Once the patch is installed, restart the BOE server.

- **On the DWH server:**

- i. Run **HPXS\_9.50.0004.exe**.
- ii. Once the patch is installed, restart the DWH server.

- **On the XS server:**

- i. Run **HPXS\_9.50.0004.exe**.
- ii. Once the patch is installed, restart the XS server.

The patch installation is complete.

## Configure BOE and XS using the HTTPS proxy to access the report

### For a single server configuration:

Proceed as follows:

1. Open **<BOE\_install\_driver>\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\server.xml**.
2. Remove the comment for the connector with port 8443 and modify it as below:

```
...
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="C:\HPXS\agora\jdk\jre\lib\security\cacerts"
keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />
...
```

3. Restart Tomcat in the Central Configuration Manager (CCM) of BOE.
4. Update the BO open docking port in **database**.

Change the BO open docking port in the management database using the command:

**UPDATE [dbo].[SETTINGS\_MANAGEMENT] set VALUE = 8443  
Where CONTEXT = 'bo' and NAME = 'bo.cms.opendoc.port'**

5. Change the BO open doc protocol TP HTTPS in the BO settings XML located at:

**<HPXS>\agora\glassfish\glassfish\domains\BTOA\config\settings\bo-settings.xml**

```
...
<setting name="bo.cms.protocol"
sectionKey="sections.bo"
nameKey="settings.bo.cms.protocol.name"
descKey="settings.bo.cms.protocol.desc"
refreshRate="Immediate"
displayInUI="false"
settingType="tenant">
<string>https</string>
</setting>
```

6. Restart the XS service.

#### For a distributed configuration:

- **On the BOE server:**

Proceed as follows:

- a. On the BOE server, run the following commands:
  - i. **c:\HPXS\agora\jdk\jre\bin\keytool -genkey -alias tomcat -keyalg RSA -keystore c:\ssl\keystore**
  - ii. **c:\HPXS\agora\webserver\bin\openssl genrsa -des3 -out c:\ssl\server.key 4096**
  - iii. **c:\HPXS\agora\webserver\bin\openssl req -new -key c:\ssl\server.key -out c:\ssl\server.csr**
  - iv. **c:\HPXS\agora\webserver\bin\openssl x509 -req -days 999 -in c:\ssl\server.csr -signkey c:\ssl\server.key -out c:\ssl\server.crt**
  - v. **c:\HPXS\agora\jdk\jre\bin\keytool -import -alias root -keystore <HPXS>\ssl\keystore -trustcacerts -file <HPXS>\ssl\server.crt**
- b. Open **<BOE install driver>:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\server.xml**.
- c. Remove the comment for the connector with port 8443 and modify it as below:

```
...
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="C:\ssl\keystore"
keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />
...
```

- d. Restart Tomcat in the Central Configuration Manager (CCM) of BOE.

- **Update the BO open docking port in database:**

Change the BO open docking port in the management database using the command:

**UPDATE [dbo].[SETTINGS\_MANAGEMENT] set VALUE = 8443**

**Where CONTEXT = 'bo' and NAME = 'bo.cms.opendoc.port'**

- **On the XS server:**
  - a. Change the BO open doc protocol TP HTTPS in the BO settings XML located at:
 

```
<HPXS>\agoralglassfish\glassfish\domains\BTOA\config\settings\bo-settings.xml
```

```
...
<setting name="bo.cms.protocol"
sectionKey="sections.bo"
nameKey="settings.bo.cms.protocol.name"
descKey="settings.bo.cms.protocol.desc"
refreshRate="Immediate"
displayInUI="false"
settingType="tenant">
<string>https</string>
</setting>
```
  - b. Restart the XS service.
  - c. Access the BOE CMC (for example: [https://<boe\\_name>.fpazsh.com/BOE/CMC](https://<boe_name>.fpazsh.com/BOE/CMC)), and install its certificate under **Intermediate Certification Authorities** and **Trusted Root Certification Authorities** by clicking the certification error, and then exporting the certification.

## Additional Steps Related to the CSA Content Update

If you want to work with the Patch 004 CSA Content Pack for CSA, perform the following steps:

1. If the CSA data source was activated in the system prior to installing the patch, perform the steps below to redeploy CSA content pack and reactivate CSA data source.
  - a. Open the cmd window in the DWH server, go to the DWH bin folder, using the following command:
 

```
cd %BTOA_HOME%\DataWarehouse\bin
```
  - b. Deactivate the CSA datasource, if it was previously activated, by executing the command:
 

```
dw_ds_automation.bat -task DeActivate -cp CSA
```
  - c. Re-deploy the CSA Content Pack by executing the command:
 

```
dw_ds_automation.bat -task Redeploy -cp CSA
```
  - d. Reactivate the CSA datasource by executing the command:
 

```
dw_ds_automation.bat -task Activate -cp CSA
```
2. **If you upgraded from XS 9.50 to XS 9.50 Patch 004**, it is recommended to clean the previous data of the CSA-related entities "BILLING" and "SUBSCRIPTION". To do so, perform the steps below:
  - a. Open the cmd window in the DWH server, go to the DWH bin folder, using the command:
 

```
cd %BTOA_HOME%\DataWarehouse\bin
```
  - b. Execute the command:
 

```
dw_abc_cleandata.bat -batch 1 -entity SUBSCRIPTION,BILLING
```
  - c. Log on to XS, click **Admin > ETL Management**.
  - d. In the DW ABC Streams Management page that opens, select **Show hidden streams**.

- e. Then run the **Cleandata** stream.

After this stream completes, the historical data for the entities "BILLING" and "SUBSCRIPTION" is cleaned up. You can now run a new ETL load to reload the data.

3. **If you upgraded from XS 9.50 patch 3**, execute the following SQL in the STAGING database:

```
INSERT INTO DWS.CSA_SUBSCRIPTIONUSER_TSNP (
    MD_BATCH_ID , MD_PROCESS_ID , MD_CP_ID ,
    MD_BUSINESS_KEY , SUBSCRIPTION_ID ,
    UPDATETIME, USER_IDENTIFIER )
SELECT T.MD_BATCH_ID , T.MD_PROCESS_ID , T.MD_CP_ID ,
    T.SUBSCRIPTION_ID + ':' + T.PERSON_ID AS MD_BUSINESS_KEY,
    T.SUBSCRIPTION_ID ,
    T.UPDATETIME , T.PERSON_ID
FROM DWS.CSA_SUBSCRIPTION_TSNP T ;
COMMIT;
```

4. **If you upgraded from XS 9.50**, perform the steps below to import one work flow into BODS:

- a. Open the cmd window on the DWH server, go to the DWH bin folder, and execute the command:

```
cd %BTOA_HOME%\DataWarehouse\bin
```

- b. Execute the command:

```
dw_bods_xml_import.bat -fromfile %BTOA_
HOME%\ContentPacks\Core\ETL\entities\BILLING\BILLING_MSI_WF.xml -verbose
```

5. **If you want to upload the upgraded CSA\_CAP or CSA\_CAP\_Demo CAPs**, you must upgrade the CAPs by performing the following steps:

- a. Logon to XS, and click **Admin > Content Acceleration Packs**.

- b. Deactivate the CSA\_CAP or CSA\_Demo\_CAP CAP if it is active. For details, see "Deactivate a CAP" in the *Guide to XS Content Acceleration Packs*.

- c. Delete the CAP.

- d. Upload the new CAP to XS from the following location:

- o CSA\_CAP: %BTOA\_
 HOME%\glassfish\glassfish\domains\BTOA\config\cap\import\languages\en\_
 US\CSA\_CAP.zip

- o CSA\_Demo\_CAP: %BTOA\_
 HOME%\glassfish\glassfish\domains\BTOA\config\cap\import\languages\en\_
 US\CSA\_Demo\_CAP.zip

For details, see "Upload a CAP" in the *Guide to XS Content Acceleration Packs*.

- e. Activate the CAP. For details, see "Activate a CAP" in the *Guide to XS Content Acceleration Packs*.

6. **If your XS was upgraded from 9.50 and CSA\_CAP was not activated** in the system prior to installing the patch, perform the steps below to update the CSA\_CAP.

- a. Log on to XS and click **Admin> Content Acceleration Pack**.

- b. Delete the CSA\_CAP.

- c. Upload the new CAP to XS from the following location:

- **CSA\_CAP: %BTOA\_  
HOME%\glassfish\glassfish\domains\BTOA\config\cap\import\languages\en\_  
US\CSA\_CAP.zip**
- **CSA\_Demo\_CAP: %BTOA\_  
HOME%\glassfish\glassfish\domains\BTOA\config\cap\import\languages\en\_  
US\CSA\_Demo\_CAP.zip**

For details, see "Upload a CAP" in the *Guide to XS Content Acceleration Packs*. Activate the CAP. For details, see "Activate a CAP" in the *Guide to XS Content Acceleration Packs*.



# Uninstallation Instructions for Patch 0004

**Note:** You cannot uninstall Patch 0004 once you have installed it.

# Defects Corrected in the XS 9.50 Patch 04 for Windows

XS 9.50 Patch 04 for Windows supersedes the XS 9.50 Patch 03, Patch 02, and Patch 01 for Windows.

XS 9.50 Patch 04 for Windows corrects the following:

Change Request	Description
QCCR8B20814	<p>XS 9.50 help seems refers to old HP Anywhere (HPA) software, not to the soon to be released new client.</p> <p>For the latest information about Executive Scorecard (XS) on mobile devices, see <i>Getting Started with the XS on Mobiles App Powered by Executive Scorecard</i> available at <a href="#">KM01081359</a></p>
QCCR8B21266	XS - CAP - activate CSA_CAP first and then activate the CSA_CAP_DEMO, the KPI calculation for CSA_CloudOptimization does not complete.
QCCR8B21334	Breakdown names are not displayed in components.
QCCR8B21374	SM KPI: <b>Mean Time To Resolve Customer Incident</b> formula is incorrect.
QCCR8B21375	SM KPI: <b>% Of Problems Reported By Customers</b> formula is incorrect.
QCCR8B21376	SM KPI: The name and formula of <b>% of Problems Resolved by Due Date</b> are not consistent.
QCCR8B21453	Application - Explorer - user should not be able to edit the annotations which are added by other users.
QCCR8B21569	CSA ETL; ABC aborts the source extraction job when it meets timeout issue instead of retrying it.
QCCR8B21573	<p>Application - Number of digits after Decimal Point configuration and presentation.</p> <p>By default, the total number of the digits displayed for KPI/Metric is up to 6 digits and the number of digits after the decimal point for KPI/Metric results is up to 5 digits.</p> <p>To work with a different default, click <b>Admin &gt; Scorecard &gt; XS Settings&gt;Total number of digits displayed for KPI/Metric results</b> setting and change the default to any number between 3 and 6. The new thresholds are then updated automatically for all KPIs.</p> <p>The <b>Admin &gt; Scorecard &gt; XS Settings &gt; Number of digits after decimal point for KPI/Metric results</b> was added to complement the capabilities. Change the default number of digits after the decimal point to any number between 0 and 5. For details, see "<a href="#">Decimal Precision</a>" on page 57 or <a href="#">KM01855072</a>.</p>
QCCR8B21948	SM PinkVerify - Add Breakdown <b>Location</b> for <b>Number of Opened requests</b> KPI.

Change Request	Description
QCCR8B22405	Source Extractor - AWS/AWSCW: AWS/AWSCW extractor failed after SDK update.
QCCR8B22592	Error occurs while running the billing report after configuring the LDAP authentication when the user name includes spaces.
QCCR8B22644	The <b>Additional Information</b> button is not enabled on Explorer pop-up dialog for KPIs.
QCCR8B22669	CSA - Limitation: The modification initial values are not calculated when the subscription is modified with different initial charges - only recurring charges are updated in the Showback report.
QCCR8B22703	CSA Webi report: The default period of the CSA BO report should not be from 1970 to 2010.
QCCR8B22757	Document: A note regarding the configuration of LDAP in a distributed environment was added to the documentation.
QCCR8B22851	More than one BO Webi report with input controls do not work well in the Google Chrome browser.
QCCR8B22866	FBI - AWSCW: The data cannot be extracted because of the endpoint.
QCCR8B23059	Scorecard - Configure Component Dialog Box - manual order arrows - there are 2 "down" arrows by default.
QCCR8B23116	BO report: 'Refresh on open' window pops up when opening the Webi Report View component in XS 9.50.
QCCR8B23129	Metrics: When using the page filter, the 'last closed period' is used for calculations and displays instead of the period set in the Metric configuration window in the Studio.
QCCR8B23222	Dashboard, Scorecard component: Missing scroll bar to display all items in the Scorecard component if there are many items.
QCCR8B23254	Unable to launch BO reports from <b>Additional Info</b> section on IE9 browsers.
QCCR8B23267	CSA KPI: Incorrect formula for <b>Service Subscription Lifespan</b> KPI.
QCCR8B23739	Dashboard: The name format of the breakdown displayed on the dashboard is <b>Entity+Dimension</b> and not the Breakdown name defined by the user in the Studio.
QCCR8B23840	Pop up Java Applet unreachable error when log on XS.
QCCR8B23966	XS cannot connect to UCMDB when it requires client authentication (CAC).
QCCR8B24022	XS cannot connect to CSA when CSA is configured to use client authentication.
QCCR8B24061	XS cannot be started by supervisor.
QCCR8B24087	DWH - PPM - ETL: XFR_FACT_JB failed for request is updated to support both dimensions and facts in SM, but in PPM it only support dimensions.

# Enhancements Added in the XS 9.50 Patch 04 for Windows

The enhancements added to the Patch are as follows:

Enhancement Request	Description
QCCR8B20473	Updating from trial to permanent license in distributed environment. <b>Workaround:</b> 1. HP Support need to provide the BO/BODS licenses. 2. The XS installation then needs to be run once only, on the DWH server.
QCCR8B20473	Documentation Enhancement Request: Updating from trial to permanent license in Distributed environments. For details, see <a href="#">"Update from a Trial License to a Permanent License in Distributed Environments"</a> on page 14 or <a href="#">KM01837431</a> .
QCCR8B23022	Enhancement: Enable CAC on XS. For details, see <a href="#">"Configure CAC"</a> on page 39 or <a href="#">KM01855433</a> .
QCCR8B23966	XS cannot connect to UCMDDB when it requires client authentication (CAC).
QCCR8B24022	XS cannot connect to CSA when CSA is configured to use client authentication

## New Certifications

Cloud Server Automation (CSA) 4.5 is supported.

**Note:** Make sure to install CSA 4.5 with CSA 4.50.0001 if you are planning to use the CSA-Billing Statement for Cloud Services report.

SAP BusinessObjects Enterprise (BOE) 4.1 SP3 & SAP BusinessObjects Data Services (BODS) 4.2 SP04 are certified.

Service Manager (SM) 9.41 is supported.

# Documentation Changes Related to Patch 0004

The documentation changes related to Patch 0004 are as follows:

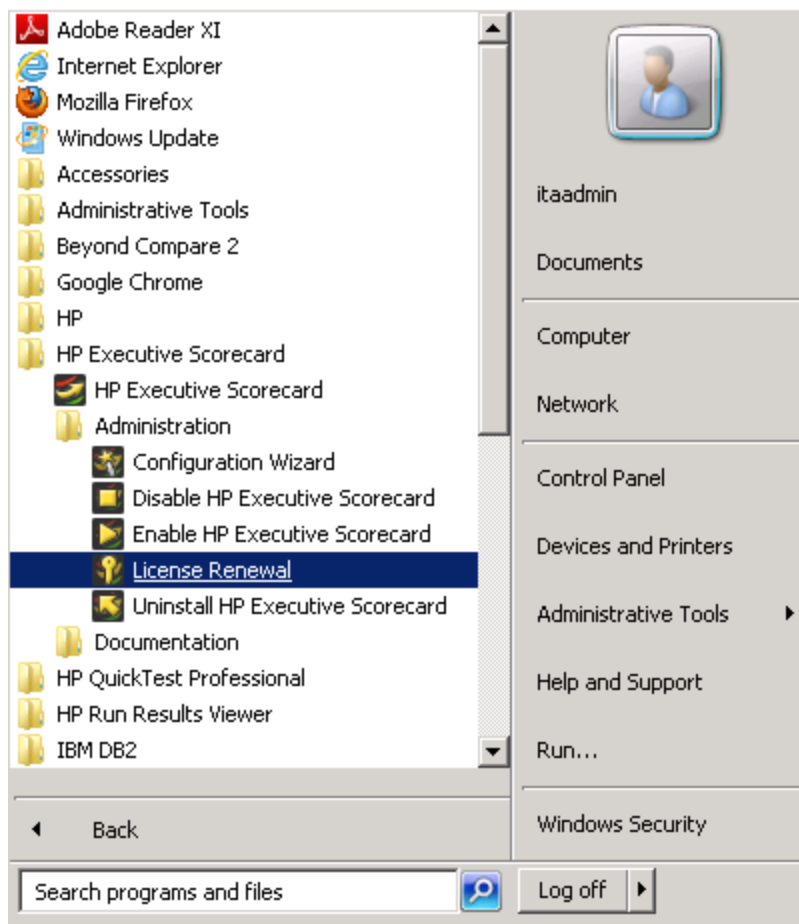
- The "[Update from a Trial License to a Permanent License in Distributed Environments](#)" on the next page (QCCR8B20473) section is new. It is also provided in the [KM01837431](#). It does **not** appear in the latest *Administrator Guide*.
- The "[Connect to CAC-enabled UCMDB Server](#)" on page 28 section was added to the "[Activate the UCMDB Data Source](#)" on page 19. The section is also provided in [KM01855061](#). It does **not** appear in the latest relevant *Content Reference Guide*.
- The "[Configure CAC](#)" on page 39 section describes how to enable CAC for XS. This section is new and is only provided in this document or in [KM01855433](#).
- The "[Decimal Precision](#)" on page 57 section (QCCR8B21573) provides details about the new setting: **Max number of digits after decimal point**. The setting is new and is only provided in this document or in [KM01855072](#).
- In XS installation, you do not have to configure the SQL server with Windows authentication. The *Installation Guide for XS 9.50* was fixed and republished. The information is also available in [KM01275262](#).
- Database Migration step - dw\_ds\_import.bat failed. For the corrected document, see [KM01837431](#).

# Update from a Trial License to a Permanent License in Distributed Environments

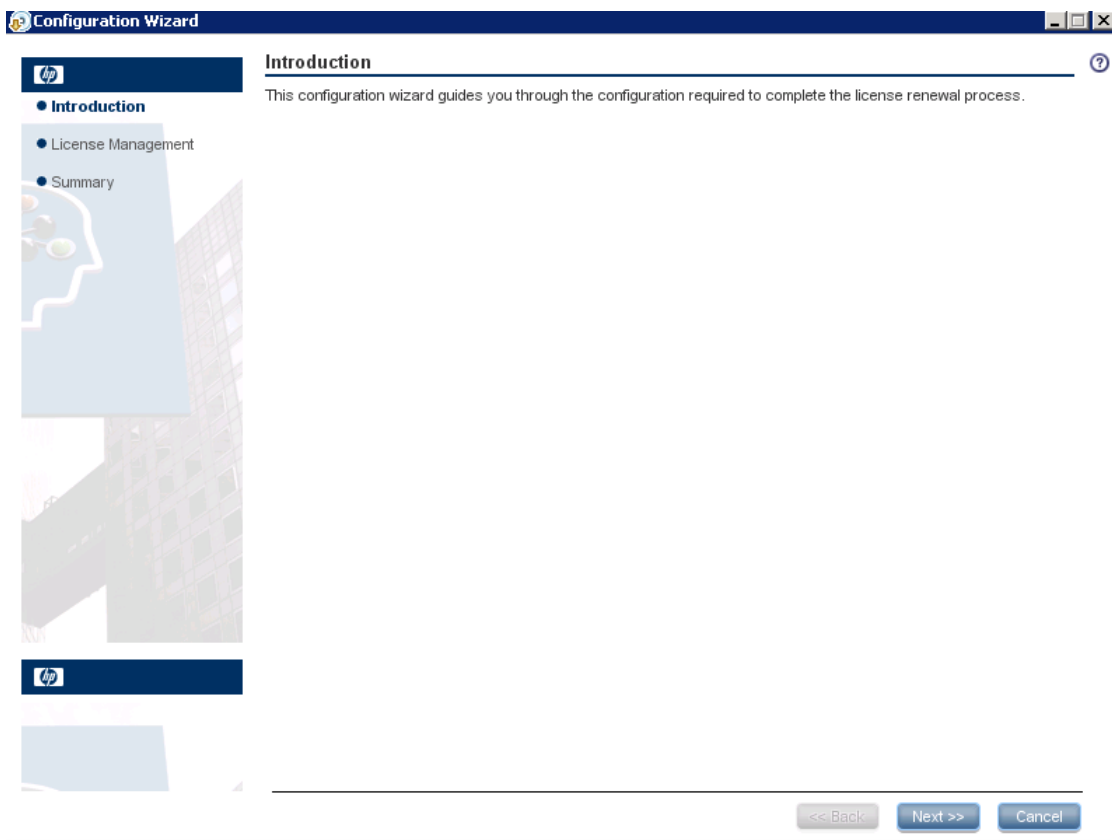
This section describes how to update from a trial to a permanent license in distributed environments.

**Note:** The license renewal must be performed on the server where DWH is installed.

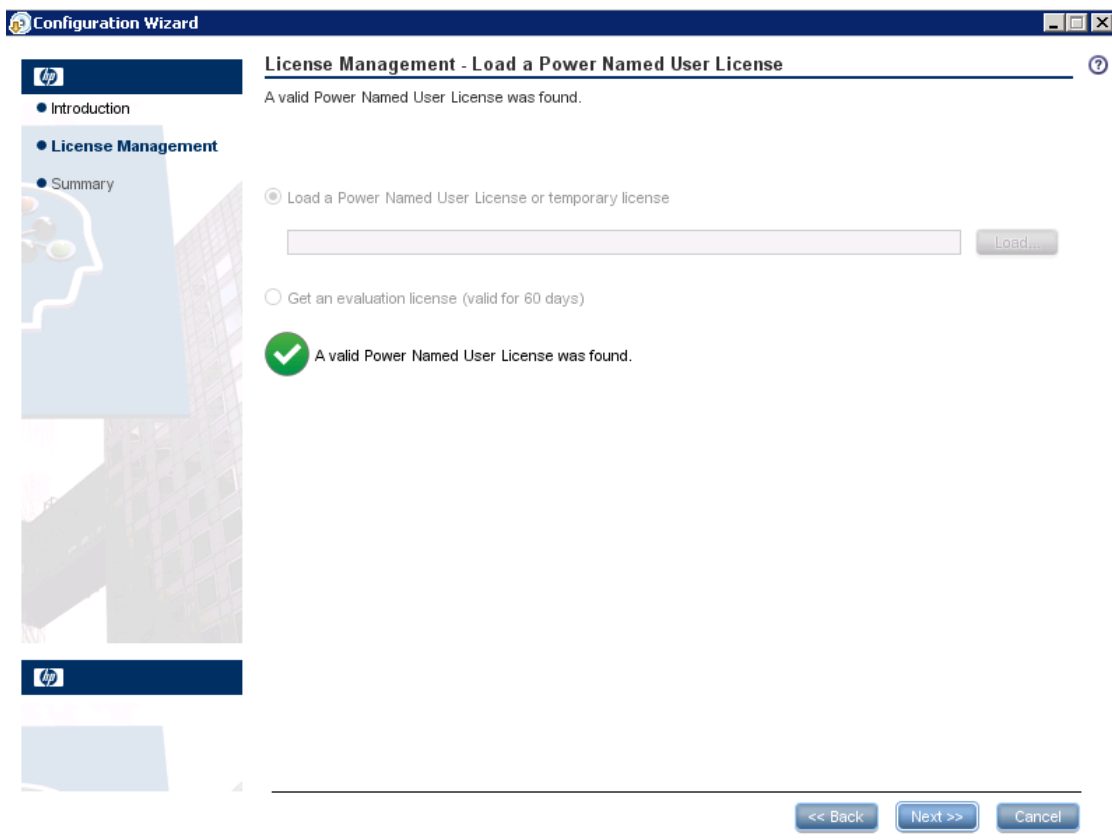
1. Log on to the XS (DWH) server.
2. In the start menu, click **Start > HP Executive Scorecard > Administration > License Renewal**.



3. In the **Introduction** page of the Configuration Wizard for the renewal of licenses, click **Next**.

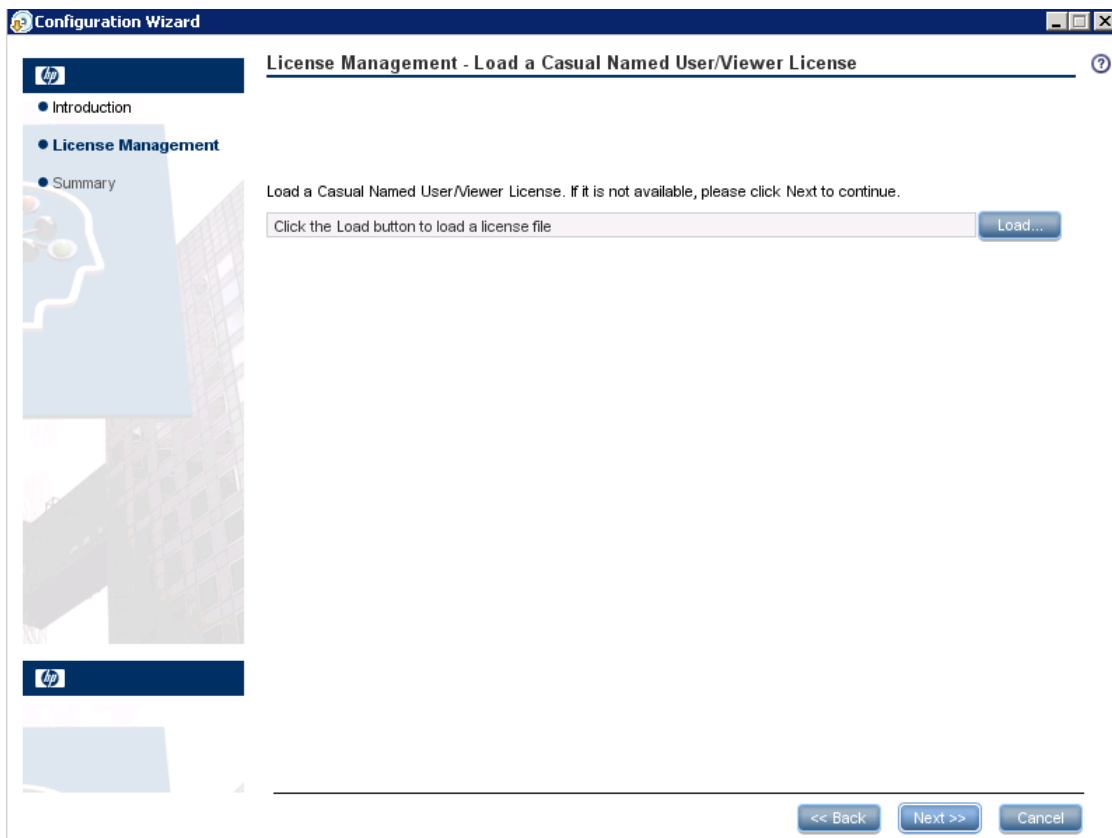


4. In the License Management - Load a Power Named User License page, click **Next**.

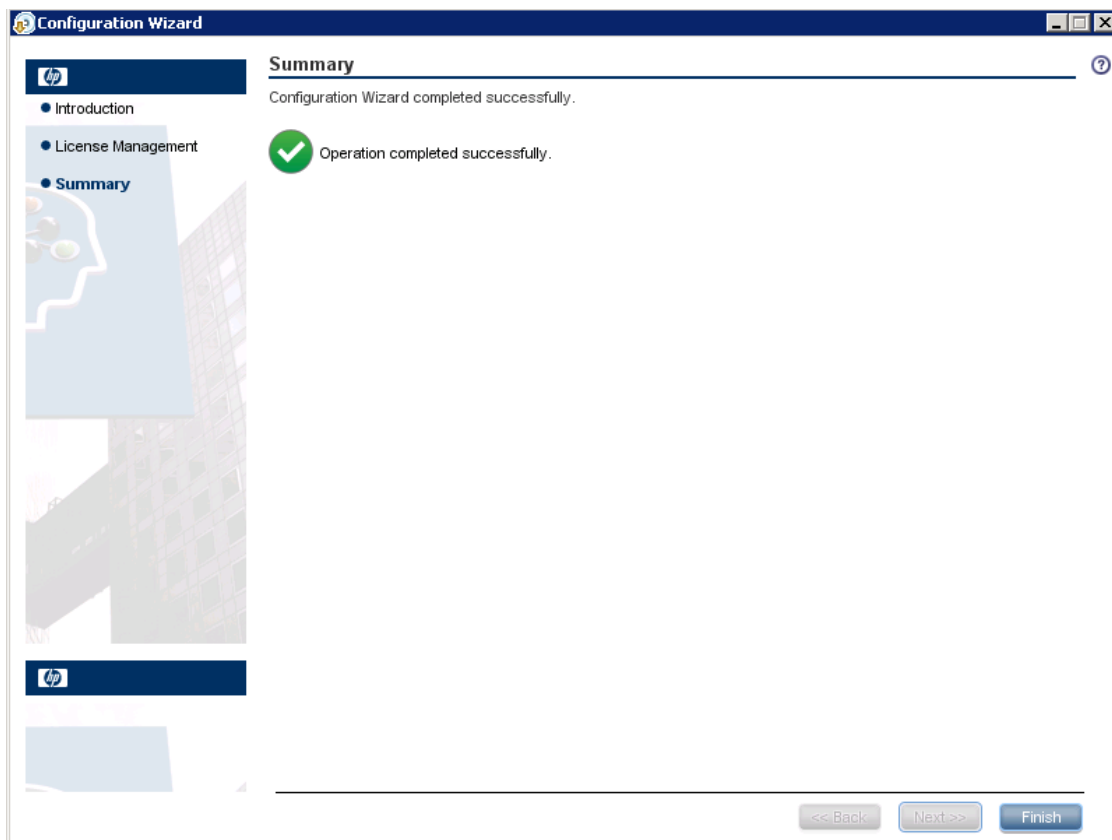


5. In the License Management - Load a Casual Named User/Viewer License page, click **Next**.





6. In the Summary page, click **Finish**.



Note that the license configuration wizard updates the log file located at:  
**%BTOA\_HOME%\confwizard\log\ConfigWizard.log.**

# Activate the UCMDB Data Source

The purpose of the integration of UCMDB as a data source is to bring quality management information into the Data Warehouse.

## To access:

Select **ADMIN > Data Management > Connect Data Source** then click **Add data source** and select **UCMDB** to activate the integration processes for the **UCMDB** data source.



## Learn More

- **Content Packs and their functionality**

To learn about Content Packs and their functionality, see *Connect the Data Source* in the *Administrator Guide*.

- **FBI Integration:**

An extractor using the File Based Integration mechanism that extracts entities from the UCMDB source and generates corresponding flat files. For details, see *Connect the Data Source* in the *Administrator Guide*. The UCMDB FBI extractor is used by both BSM and UCMDB.

- **UCMDB Push Adapter:**

A package installed on the UCMDB server that can push data into XS Data Warehouse database. The relevant XS information is set when you deploy the push adapter. You can then use the push adapter to access certain data based on the query you configure. For details, see "[Access and Deploy the UCMDB Push Adapter](#)" on page 21

### Important Information

- UCMDB supports multiple instances of the Content Pack.
- If you work with IT Financial Management (ITFM), this data source is not supported. When you activate this data source, the ITFM application displays **No data**.
- All fields are case-sensitive.

## Tasks

This section includes:

- [Activate the Integration](#) .....20
- [Connect to UCMDB on a Secured Connection](#) .....20
- [Consolidate Between BSM and UCMDB](#) .....20
- [Access and Deploy the UCMDB Push Adapter](#) .....21

- [Connect to CAC-enabled UCMDB Server](#) .....28

## Activate the Integration

### 1. Important Note: First day of the week

In Data Warehouse, the first day of the week is set in the Post-Install wizard, and the Period tool is using is as an input to build PERIOD\_DIM days, weeks, months, and more, as well as relevant hierarchies.

After the administrator has installed Data Warehouse, the administrator selects the cooperation first-day-of-week. If the data source has a different first-day-of-week definition, the administrator should be aware that for weekly periodicity, the linkage to the period key uses the Data Warehouse week definition and not the data source week definition.

2. Select **ADMIN > Data Management > Connect Data Source** then click **Add data source**.
3. The Add Data Source page opens. Select the **UCMDB** data source type.
4. Select or enter the configuration parameters.
5. Click **Next** to proceed to the validation page.

**Note:** Before reactivating the UCMDB data source, click **Edit Settings** and enter the **Username** and **Password**.

## Connect to UCMDB on a Secured Connection

1. Export the UCMDB SSL certificate to a file. For details, see the UCMDB *Hardening Guide* available in the [HP Software Product Manual Site](http://support.openview.hp.com/selfsolve/manuals) (<http://support.openview.hp.com/selfsolve/manuals>).

2. Reveal the UCMDB certificate to Data Warehouse as follows:

Import the SSL certificate trusted by the UCMDB server into the JDK key store using a tool provided by the JDK called **keytool.exe** by running the command :

```
<HP-XS>\jdk\jre\bin\keytool -importcert -alias <alias> -file <file> -keystore
<HP-XS>\agora\jdk\jre\lib\security\cacerts -trustcacerts
```

**Note:** The default password for JVM keystore is a 'changeit'. If this password wasn't changed before, use the default keystore password for certificate import.

3. Restart the XS server.
4. Select **Is secured** in the activation parameters page.
5. Change the port to a secured port (default is 8080).

## Consolidate Between BSM and UCMDB

Business Services and Infrastructure Services are automatically consolidated between BSM and UCMDB during ETL.

**Note:** You must perform synchronization of BSM and UCMDB before each time you run the ETL,

to enable consolidation between these sources.

## Access and Deploy the UCMDB Push Adapter

The UCMDB push adapter enables you to access data links and nodes from UCMDB, which are then pushed into the Data Warehouse. You can deploy the push adapter on the UCMDB server and schedule the execution time of the adapter. You can also configure the adapter integration and add an integration point in the Integration Studio.

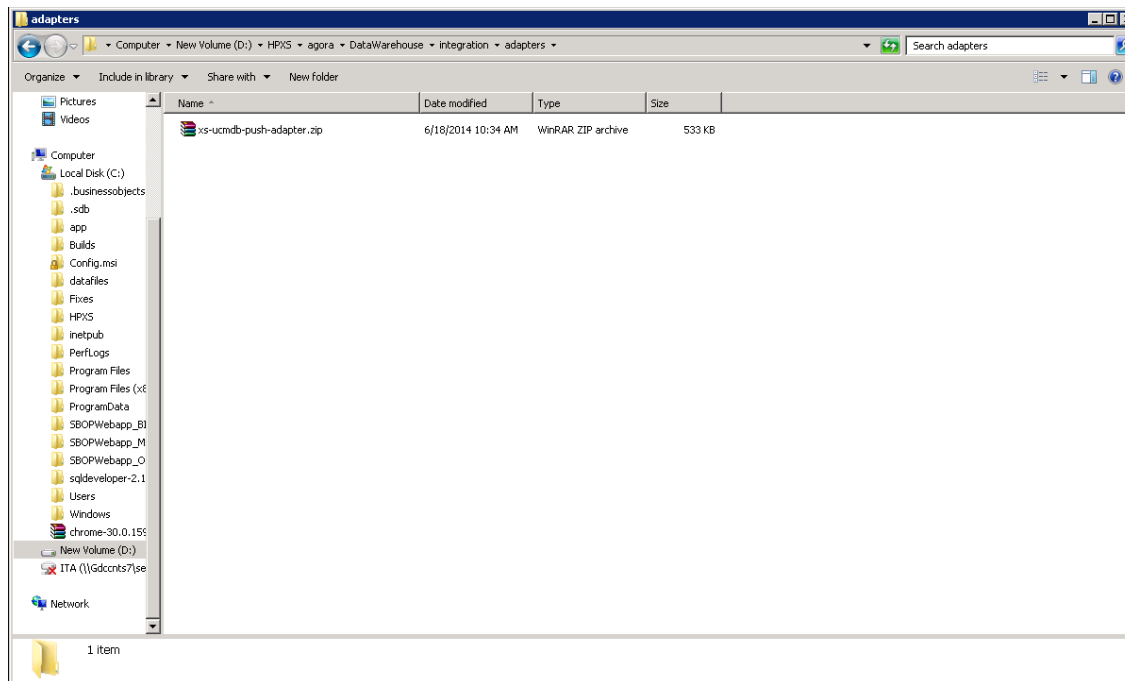
You must deploy the push adapter package when the UCMDB Content Pack is activated in the Connect Data Source UI, and before the first run of the ETL in order to get the Node, Application and Services topology from UCMDB.

This section includes:

### Deploy the push adapter package in Package Manager

1. In UCMDB, navigate to **Administration > Package Manager**.
2. Select **Deploy package to server (from local disk)** then click **Add**.
3. Select the XSpush adapter package from and then click **Open**.

The new adapter is deployed and displayed in the Adapters list.



### Deployment Limitation

If you deploy an incorrect version of the push adapter you need to redeploy as follows:

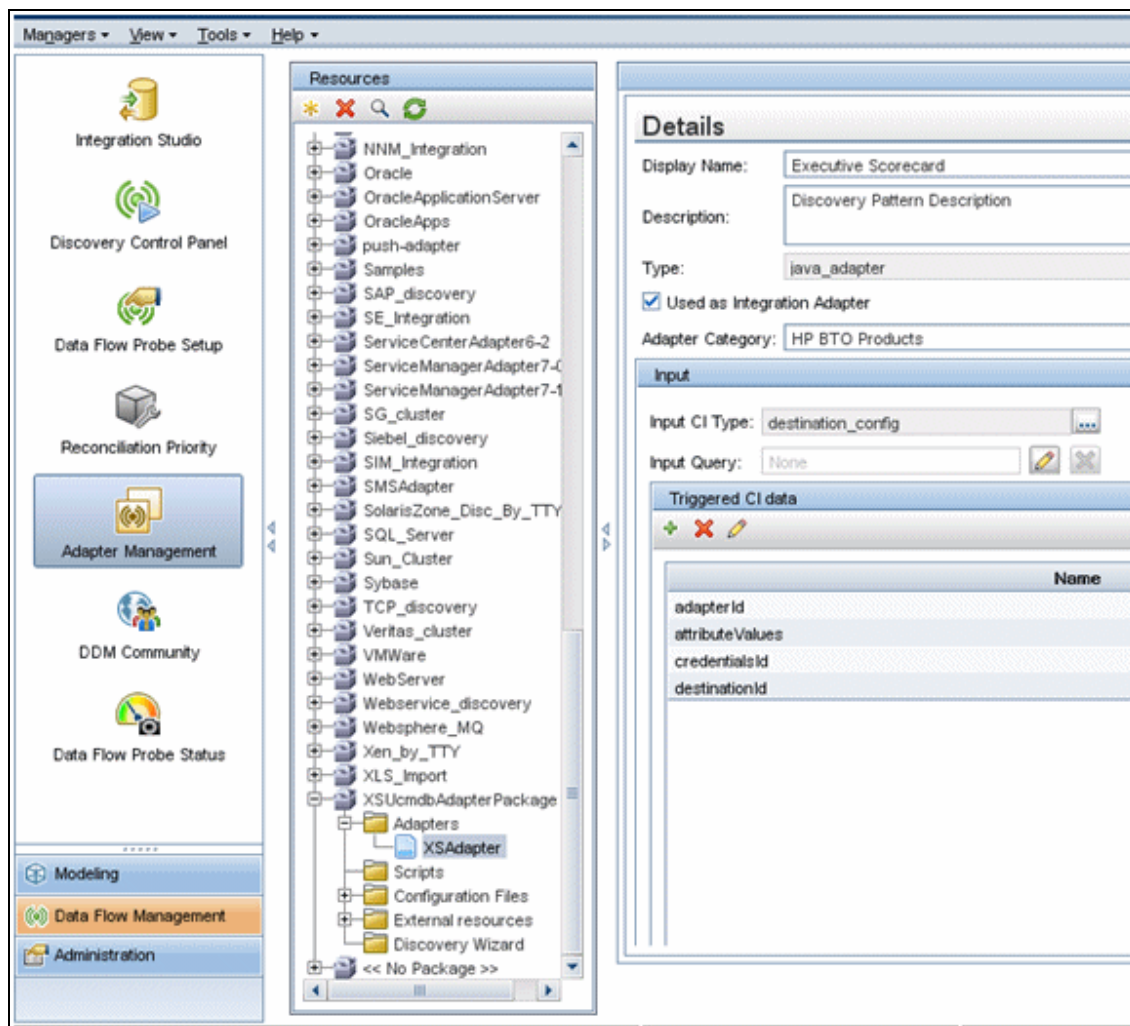
1. Delete the relevant Integration Point in **Data Flow Management > Integration Studio**.
2. Un-deploy the package in **Administration > Package Manager**. If necessary, delete the package

directory manually, as follows.

- a. Stop the UCMDB server: **Start > All Programs > HP UCMDB > Stop HP Universal CMDB Server.**
- b. Delete the XS adapter directory, for example, C:\hp\UCMDB\UCMDBServer\runtime\fcmdb\CodeBase\XSAdapter.
- c. Start the UCMDB server: **Start > All Programs > HP UCMDB > Start HP Universal CMDB Server.**
- d. Deploy the adapter package using the Package Manager.

### Locate the adapter in Adapter Management

1. In UCMDB, navigate to **Data Flow Management > Adapter Management.**
2. Select **XSUcmdbAdapter** in the Resources area.
3. Expand **Adapters** and select **XSAdapter** to check the adapter definition.



## Add the XS integration point in the Integration Studio

**Note:** For UCMDB version 10.0, see the procedure below.

1. In UCMDB, navigate to **Data Flow Management > Integration Studio**.
2. In the Integration Point area, select **New Integration Point**.
3. Enter the integration name, for example, XS.
4. Select **Executive Scorecard** from the **Adapter** list.
5. In Adapter Properties, enter the following.
  - **Hostname/IP:** The XS database.
  - **Port:** 1433.
  - **Database:** The XS DWH staging database name.
  - **Database Schema:** dws
  - **Credentials:** Browse to select **SQL protocol**, and add new credentials.
    - i. Enter a user, the Microsoft SQL Server for **Database Type**, leave default values for **Port Number** and **Connection Timeout**, and enter **User** and **Password** to connect to the XS DWH database.
    - ii. Click **OK**.
    - iii. Select the new created credential and click **OK**.
6. Click **Test Connection**.
7. Click **OK** in the New Integration Point dialog box.

The new integration point is created and added into Integration Point area.

**Note:** If the integration point already exists, a message appears accordingly.

#### Add an integration point using UCMDB version 10.0

1. In UCMDB, navigate to **Data Flow Management > Integration Studio**.
2. In the Integration Point area, select **New Integration Point**.
3. Enter the integration name, for example, XS.
4. Select **Executive Scorecard** and then select **XS push job and federation** from the **Adapter** list.
5. Select the **Is Integration Activated** checkbox.
6. In **Adapter Properties**, enter the following.
  - **Hostname/IP:** The XS database.
  - **Port:** 1433.
  - **Database:** The XS DWH staging database name.
  - **Schema:** dws
  - **Credentials ID:** Browse to select **SQL protocol**, and add new credentials.
    - i. Enter a user, the Microsoft SQL Server for **Database Type**, leave default values for **Port Number** and **Connection Timeout**, and enter **User** and **Password** to connect to the XS DWH database.
    - ii. Click **OK**.

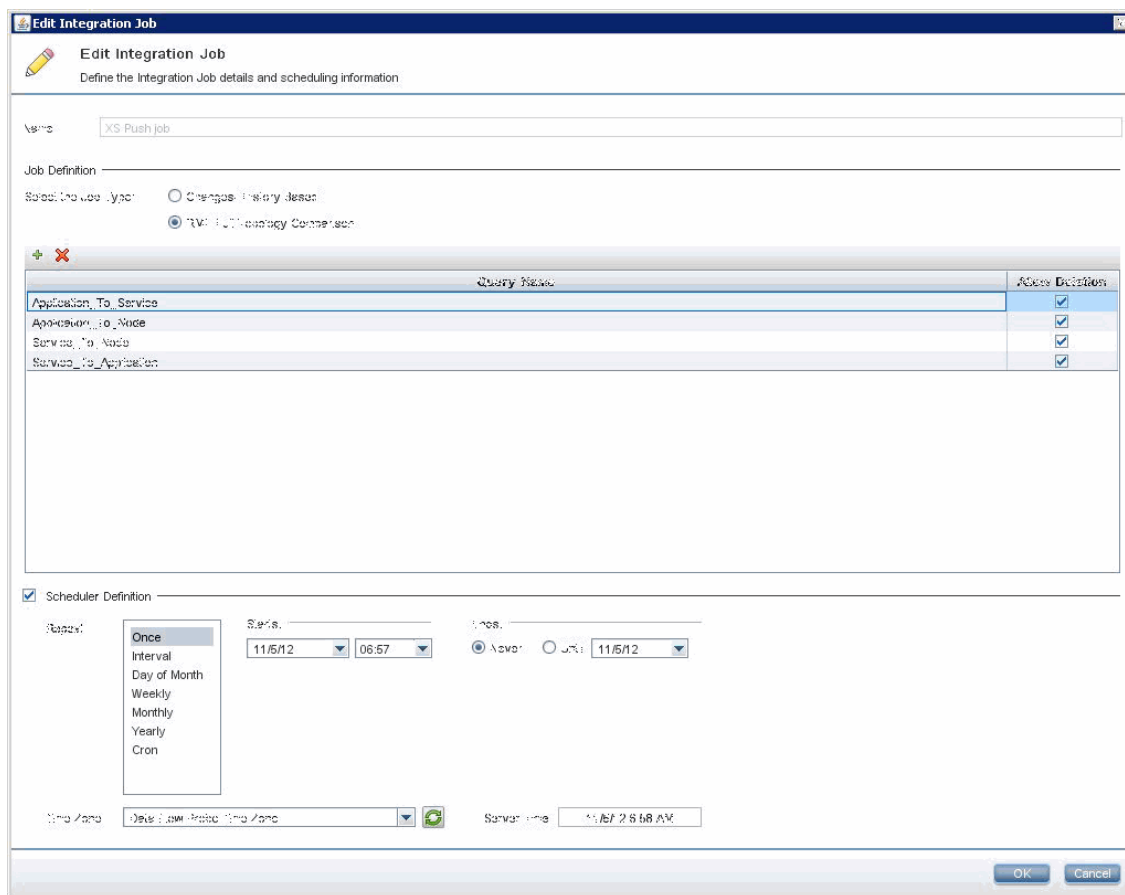


- iii. Select the new created credential and click **OK**.
  - **Data Flow Probe:** Select a Probe that has IP of the XS database in range.
7. Click **Test Connection**.
  8. Click **OK** in the New Integration Point dialog box.

The new integration point is created and added into Integration Point area.

### Edit a push job

1. In UCMDB, navigate to **Data Flow Management > Integration Studio**.
2. Select the job you want to edit from the Integration Point area.
3. Edit the properties and add queries, as required.
4. In the Scheduler Definition area, select the repeat frequency, start time, end time and time zone for the job and click **OK**. Make sure that the **Allow Deletion** checkbox is selected.

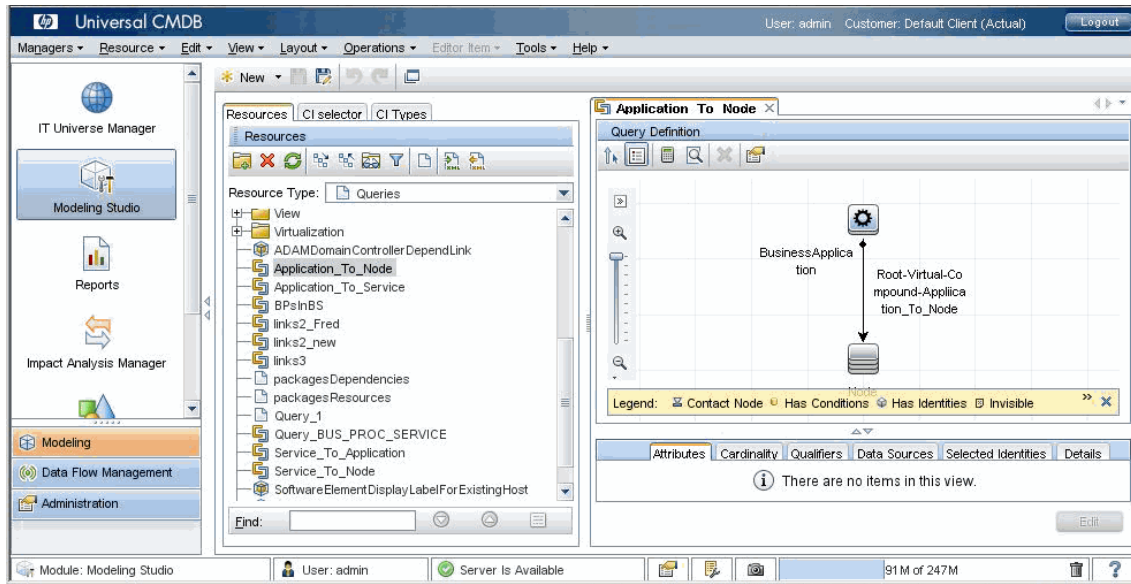


### Change or add TQL queries

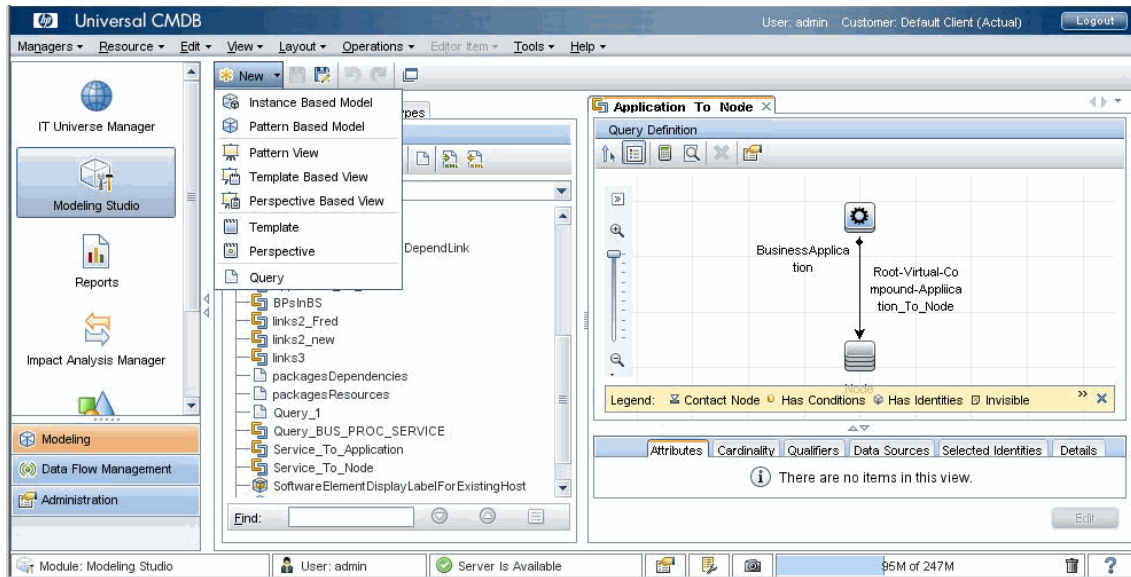
After the Push Adapter is deployed, Application\_To\_Node, Application\_To\_Service, Service\_To\_Application, Service\_To\_Node are added automatically. You can change these queries or add a new TQL query.


**Note:** You must use the required naming convention, for example, **Application\_To\_Node**.

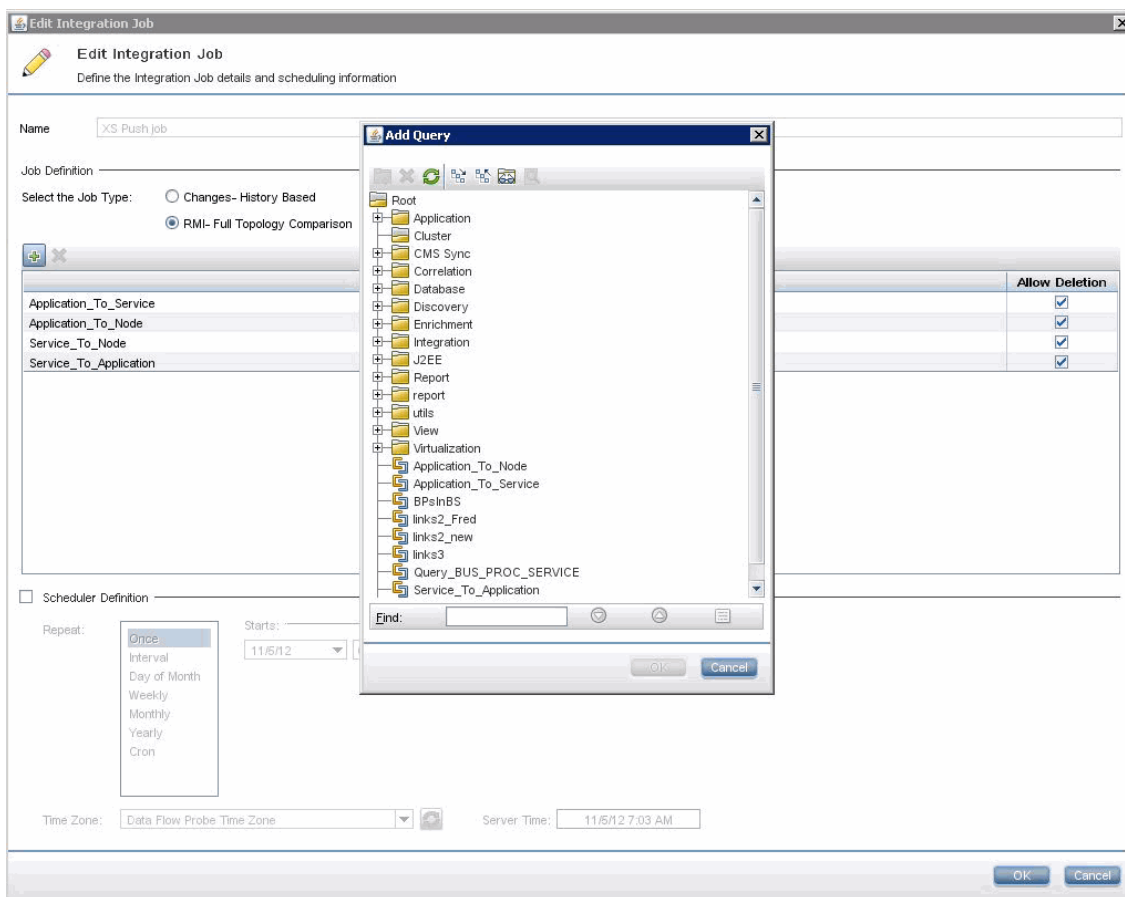
1. In UCMDB, view the XS push adapter list of OOTB queries in the Resources area of the Modeling Studio.
2. You can modify a query by opening the query definitions. Click **Save** and the changes are added to the adapter.



3. Create a new TQL query configuration by clicking .



4. Enter a new name and then proceed to editing the query in the XS push job you created in the Integration Studio.
5. Select the job you want to edit from the Integration Point area.
6. Click  to add the new query and click **Save**. The query is added to the XS list.

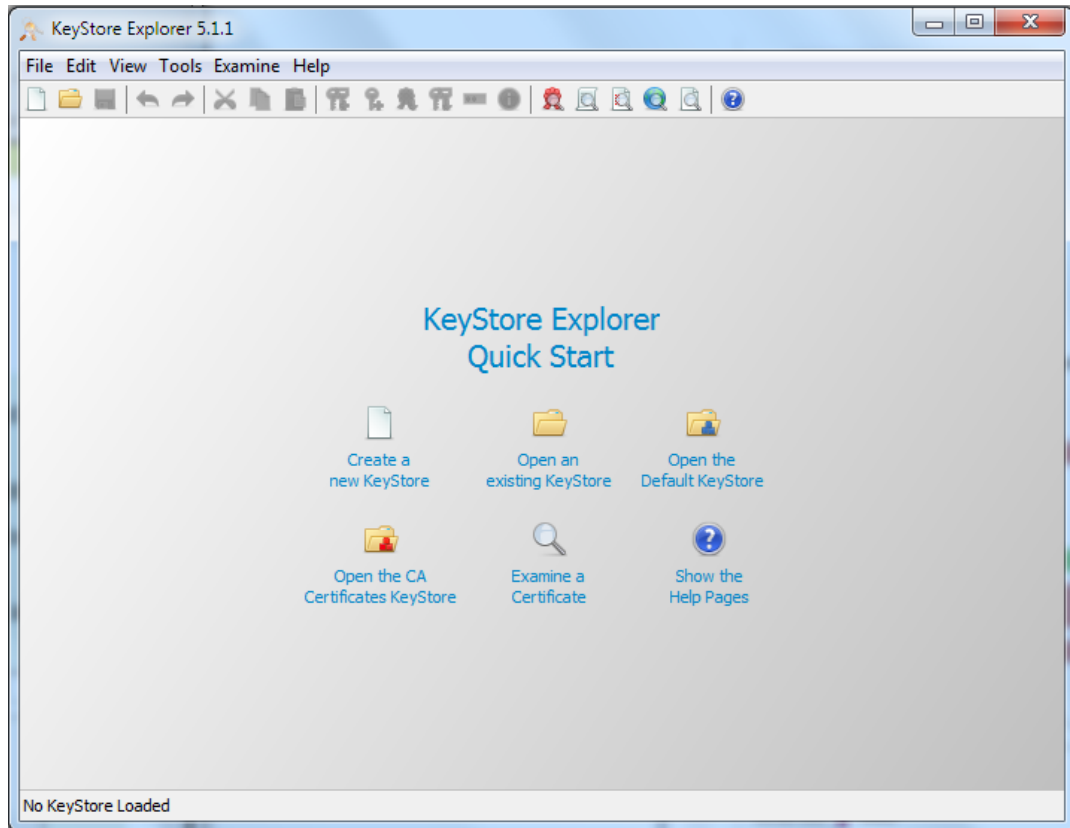


## Connect to CAC-enabled UCMDB Server

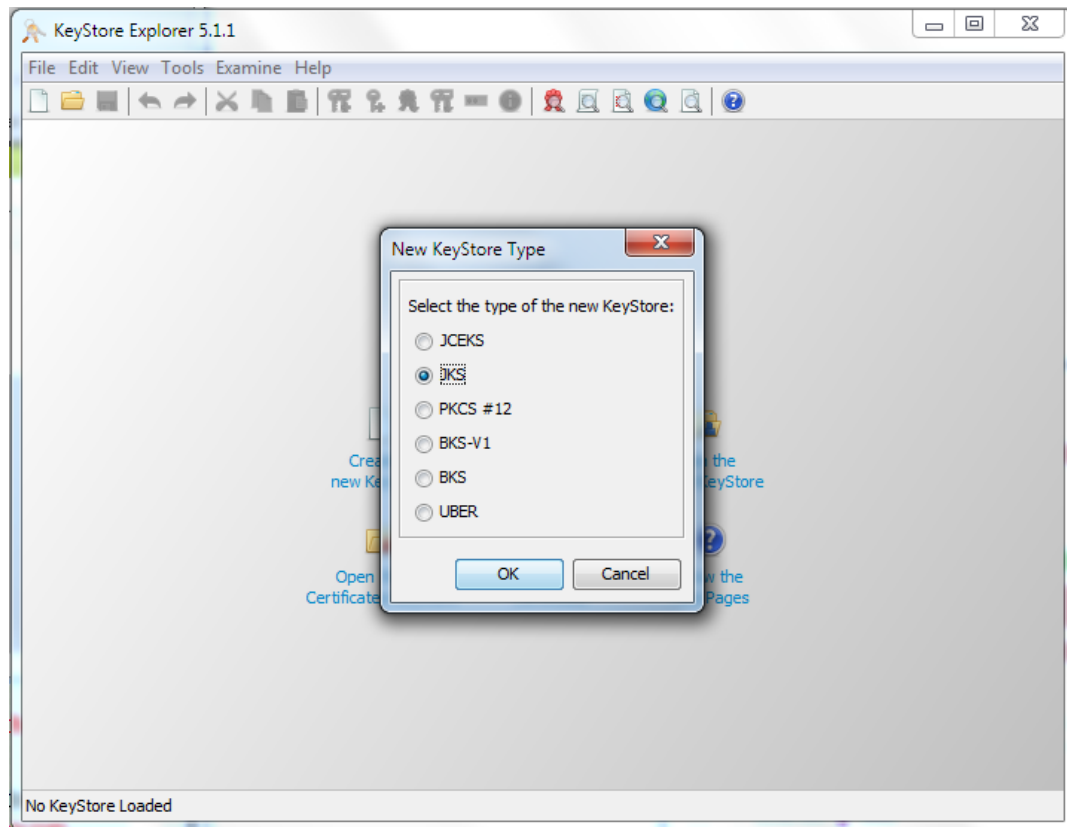
To connect XS with a Common Access Card-enabled UCMDB server, proceed as follows:

1. Import the UCMDB server certificate into XS jdk. (Like we import CSA certificate).  
 Steps for creating keystore files contains certain certificates with the p12 format:
  - a. Download **KeyStore Explorer 5.1** from [http://sourceforge.net/projects/keystore-explorer/?source=typ\\_redirect](http://sourceforge.net/projects/keystore-explorer/?source=typ_redirect) and run it as the Administrator on any server with Windows but

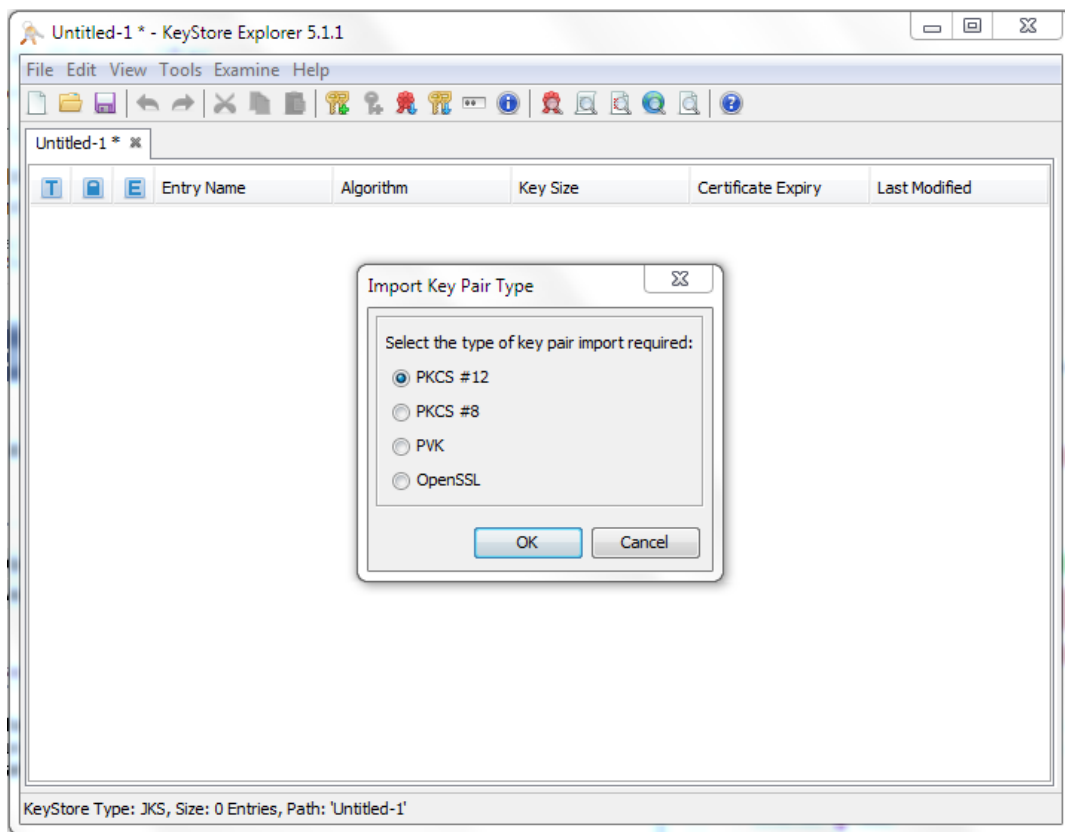
not on the XS server.



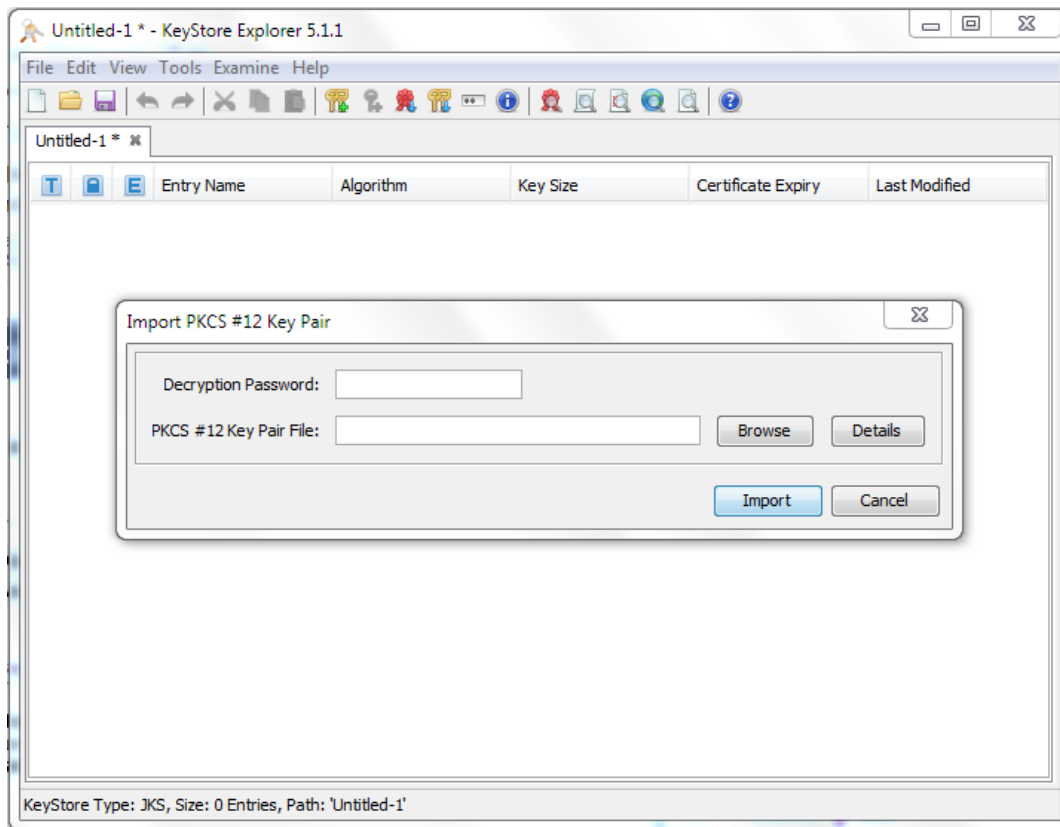
b. Click **File > New > JKS Radio button > OK.**



c. Click **Tools > Import Key Pair >**, select the **PKCS #12** radio button, and click **OK**.

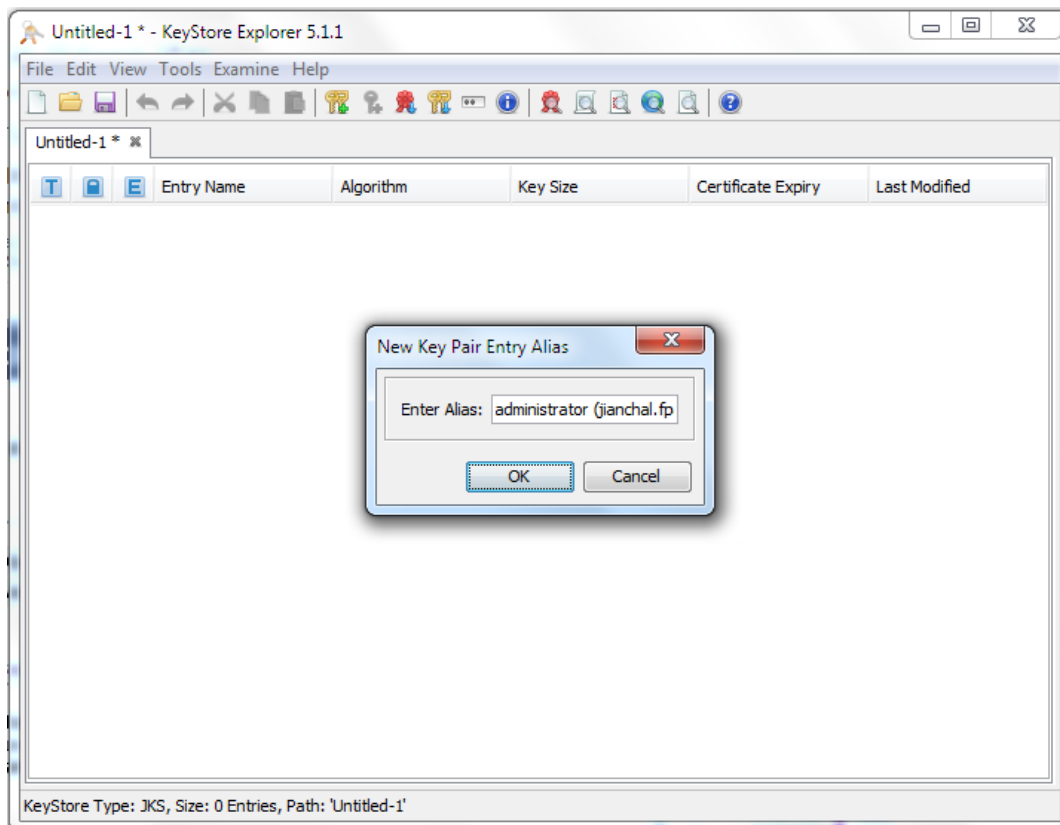


- d. In the dialog box that opens, click **Browse** to go to the relevant file Decryption Password (certificate's password), import de p12 key pair.

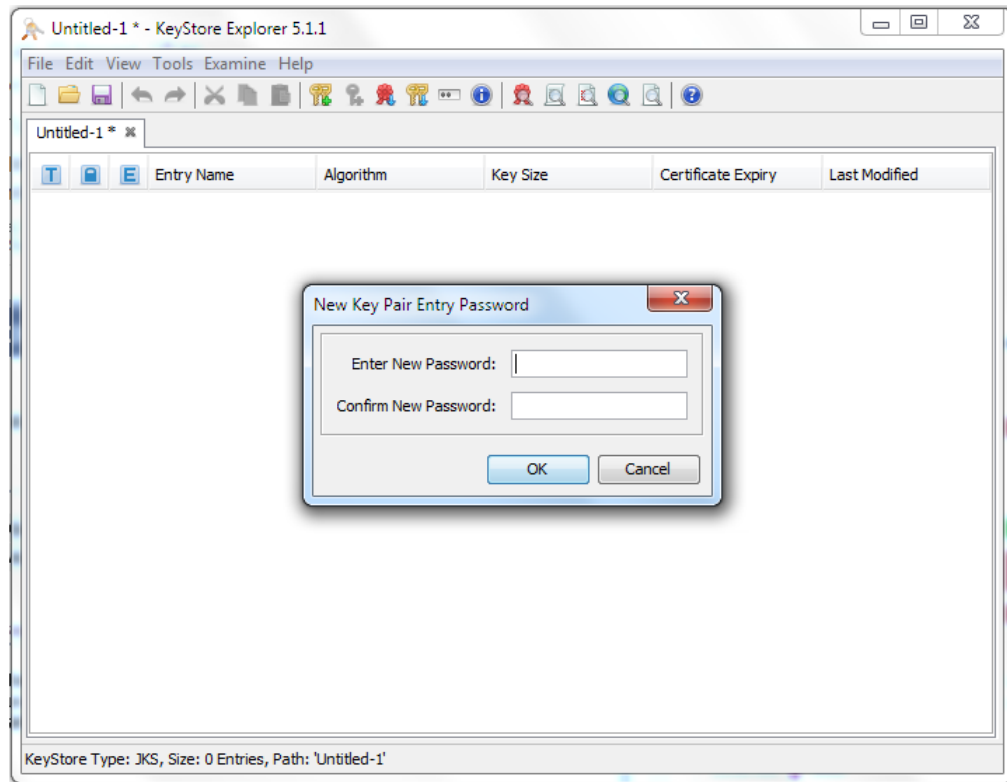




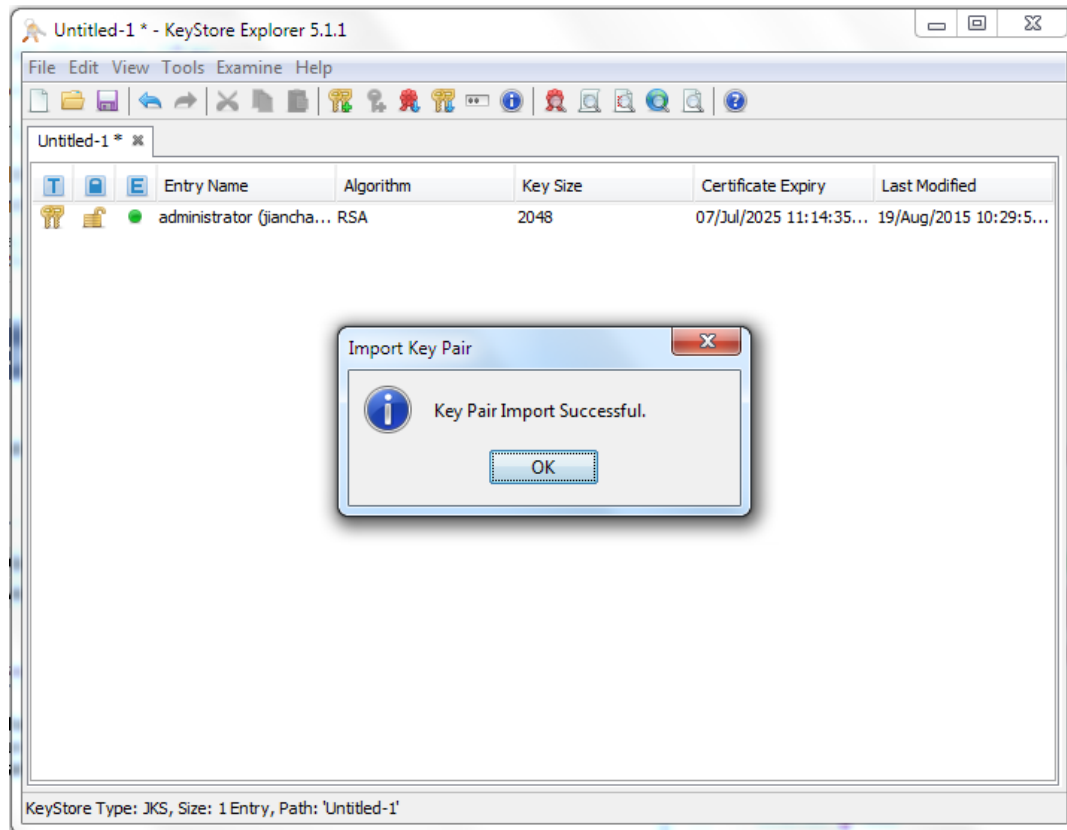
- e. In the New Key Pair Entry Alias dialog box, click **OK** for the default alias.



- f. Enter the password for the new key pair and click **OK**.



g. The following message is displayed when the Key Pair is imported successfully.



h. Save the keystore (enter the same password from step f). When you Import the converted keystore you must enter the same password.

**Note:**

- The keystore used for client SDK must be in Java Keystore format (JKS).
- The Java Cryptography Extension KeyStore (JCEKS) or other formats are not supported.
- The keystore used for SDK must contain only one key-pair and nothing else. The password for this key-pair must be the same as the one for the keystore.

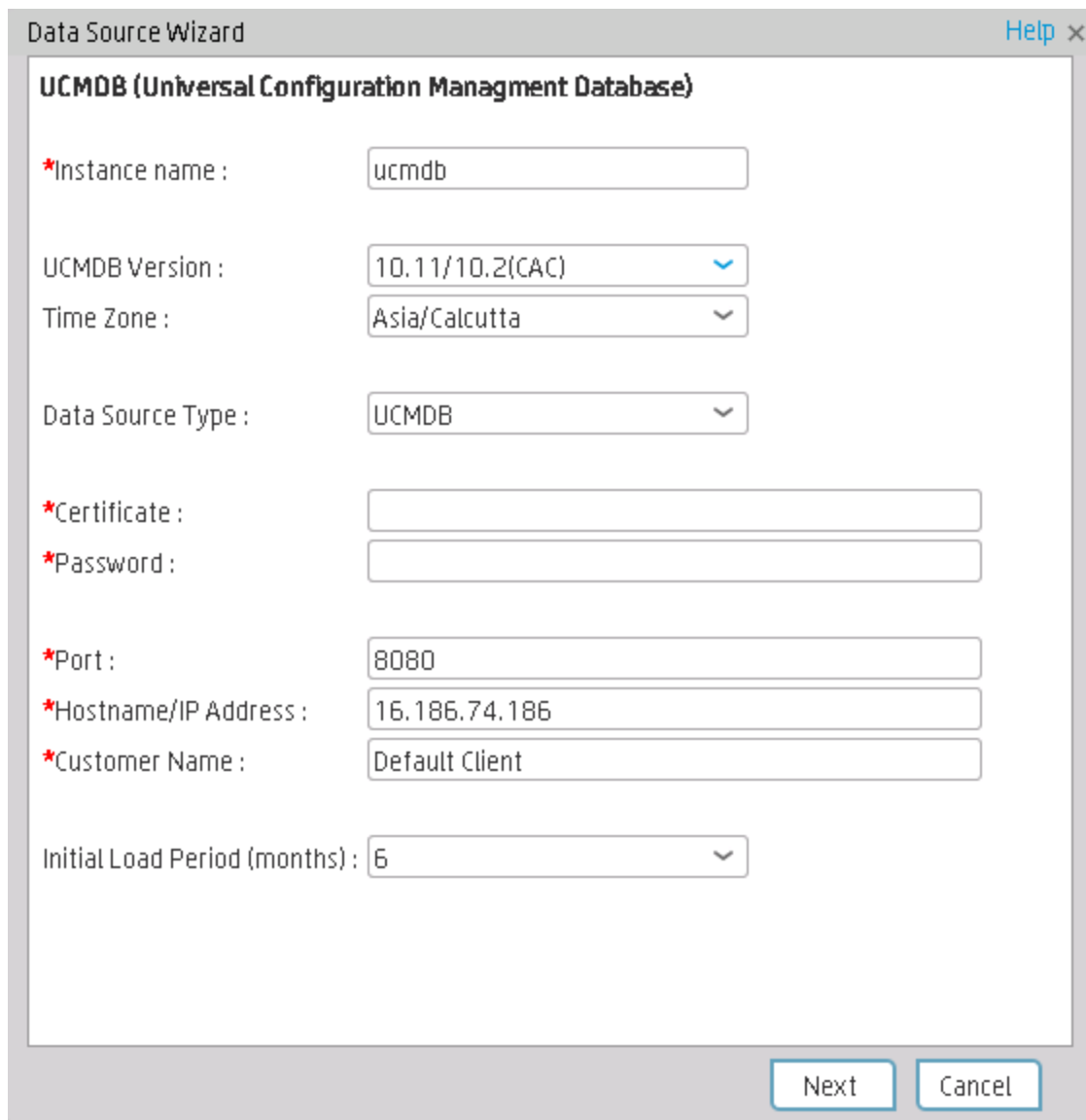
2. Select **ADMIN > Data Management > Connect Data Source** then click **Add data source** and select **UCMDB** to activate the integration processes for the **UCMDB** data source.
3. Enter the relevant information, and select **CAC ENABLED** to enable the CAC feature.
4. Provide the path to the Client Certificate. The client certificate can be located in the XS server. Once you have provided the path, XS uses it to setup a 2-way SSL authentication with the UCMDB server.
5. Click **Next** to test the connection.

## UI Description

### UCMDB Activation Page

The data warehouse is connected to UCMDB through high-level integration processes. A set of database views enables the extraction of the main UCMDB objects.

- With CAC:



The screenshot shows a 'Data Source Wizard' window titled 'UCMDB (Universal Configuration Management Database)'. The window contains several input fields and dropdown menus for configuring the data source. The fields are as follows:

Field Name	Value
*Instance name :	ucmdb
UCMDB Version :	10.11/10.2(CAC)
Time Zone :	Asia/Calcutta
Data Source Type :	UCMDB
*Certificate :	
*Password :	
*Port :	8080
*Hostname/IP Address :	16.186.74.186
*Customer Name :	Default Client
Initial Load Period (months) :	6

At the bottom right of the window, there are two buttons: 'Next' and 'Cancel'. A 'Help' link with a close icon is located in the top right corner of the window.

- Without CAC:

The screenshot shows a 'Data Source Wizard' window titled 'UCMDB (Universal Configuration Management Database)'. The window contains several input fields and dropdown menus. Mandatory fields are marked with a red asterisk. The fields are: Instance name (text box with 'ucmdb'), UCMDB Version (dropdown with '10.0x/10.1x/10.2(NON\_C...)'), Time Zone (dropdown with 'Asia/Calcutta'), Data Source Type (dropdown with 'UCMDB'), Username (text box with 'admin'), Password (text box), Is Secured (checkbox), Port (text box with '8080'), Hostname/IP Address (text box with '16.186.74.186'), Customer Name (text box with 'Default Client'), and Initial Load Period (months) (dropdown with '6'). At the bottom right, there are 'Next' and 'Cancel' buttons.

Mandatory fields are marked with a red asterisk.

User interface elements are described below:

UI Element	Description
Instance name	Enter a name for the data source instance you are activating.
UCMDB Version	Select the relevant UCMDB version. For details, see the <i>Support Matrix</i> . You can select to work with CAC or not.
Time Zone	Select the time zone for the data source.
Data Source Type	<b>UCMDB</b> . This parameter is read only.

UI Element	Description
<b>Certificate</b>	The location of the UCMDB server's certificate file.
Password	The password of the certificate file.
<b>Username</b>	Enter the user name used to log on to CMDB. You must create a new integration user in UCMDB for integration with XS.
<b>Password</b>	Enter the password used to log on to CMDB. You must create a new integration password in UCMDB for integration with XS.
<b>Is Secured</b>	Select if the server host is secured.
<b>Port</b>	The port number. The default value is 8080.
<b>Hostname/IP Address</b>	Enter the server hostname or IP address of the server where the UCMDB is installed.
<b>Customer Name</b>	Used for tenant client purposes. If no username is given, then <b>Default Client</b> is displayed.
<b>Initial Load Period (months)</b>	Select the number of months from which you want the initial data loaded.

## Reference

### List of Entities

List of Entities in Excel format

This document is available in the PDFs directory in the Installation DVD, is accessible from the Help Center page in the online Help Center (documentation library), or from the [HP Software Product Manual Site](http://h20230.www2.hp.com/selfsolve/manuals) (<http://h20230.www2.hp.com/selfsolve/manuals>).

# Configure CAC

This section explains how to configure Common Access Card (CAC) (Smart Card/PKI Authentication) on XS.

**Note:** In a distributed environment, the Administrator must configure both the DWH server and the XS server using the procedure provided below.

## 1. Prepare certificates.

To prepare the root Certificate Authority (CA) certificate and client certificates for the XS server, copy the root CA certificate to the following path in the XS server:

**\$HPXS\_HOME\agora\conf\keys**

**Note:** Apache uses PEM format certificates, so that the root certificate provided by the customer must obey this rule.

If your certificate is DER binary format, please convert the binary certificate file into PEM format using one of the following methods:

- Convert DER to PEM using: **\$ openssl x509 -inform der -in certificate.cer -out certificate.pem**
- Convert it with the online tool: <https://www.sslshopper.com/ssl-converter.html>

## 2. Configure the root CA in the XS Server.

Edit the **%HPXS\_HOME%\agora\webserver\conf\extra\httpd-ssl.conf** configuration file. In the file, add following lines to enable the SSL authentication:

```
SSLCertificateFile "../conf/keys/ca.cer "  
JkOptions +ForwardSSLCertChain  
<Location /bsf >  
    SSLVerifyClient optional  
    SSLVerifyDepth 10  
    SSLOptions +StdEnvVars +ExportCertData  
</Location>
```

The highlighted values can vary depending on your CA certificate file name and verification depth.

Make sure the CA certificate (ca.cer file) is located in the **%HPXS\_HOME%\agora\conf\keys** folder.

## 3. Enable CAC mode in the XS Server.

In the XS server, edit the **%HPXS\_HOME%\agora\glassfish\glassfish\domains\BTOA\config\confcac.properties** property file.

- a. Enable CAC mode.

Mark the following flag as true to enable CAC. The default value is false.

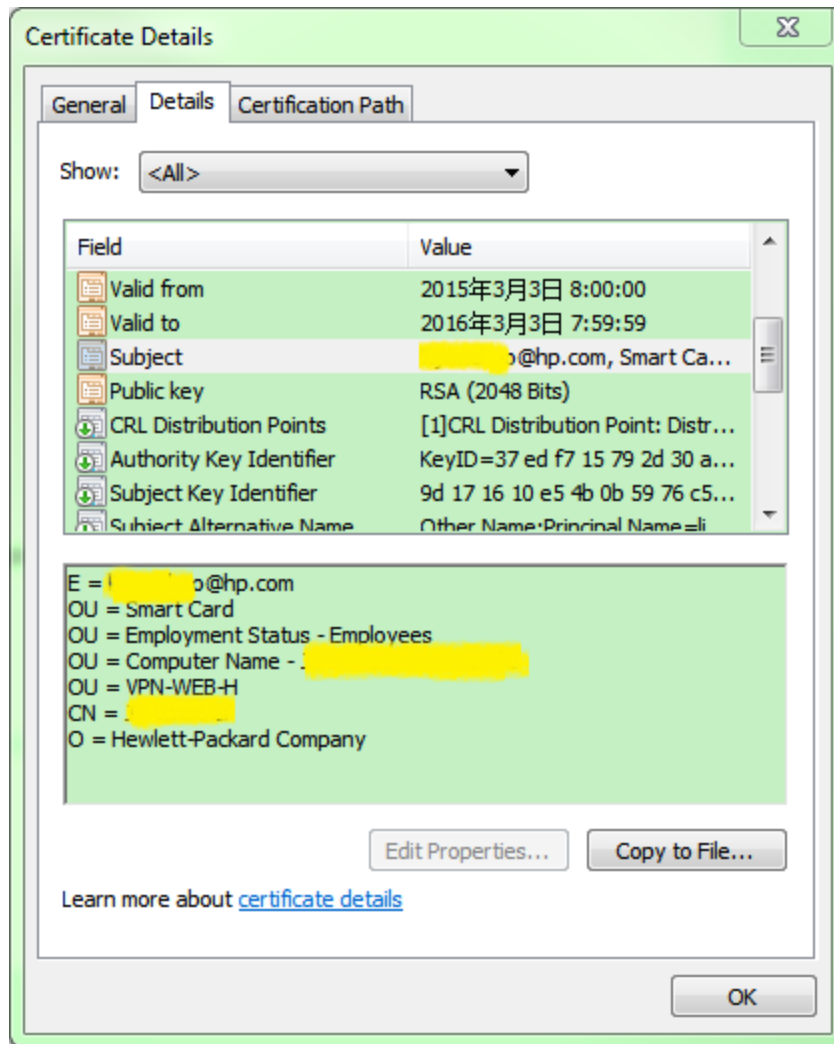
**isCACEnabled=true**

- b. Set the Distinguished Name (DN) field for certificate extraction.

The following flag is used to indicate which field is "login name".

**certificateFieldExtractDN=<certificate\_standard>**

where **<certificate\_standard>** can be either **SUBJECT.E** or **SUBJECT.CN**.  
See the following example:



- c. Enforce the client certificate validation using the following flag:  
**validationEnforced=<true|false>**
  - o **true.** all validation strategies are enforced.
  - o **false.** the following validation strategies are ignored: LOCAL\_CRL, ONLINE\_CRL and so on.
- d. Choose validation strategy.  
For example: **validationStrategy=<validation\_strategy>**  
where **<validation\_strategy>** can be:
  - o **LOCAL\_CRL.** Local Certificate Revocation Location (CRL) validation. Then make sure that CRLStoreLocation is set as shown below.
  - o **ONLINE\_CRL.** Online CRL validation. Then make sure that CRLDownloadURL is set as shown below.



- o **OCSP OCSP.** Validation. Then make sure that OCSPResponderURL is set as shown below. OCSP stands for Online Certificate Status Protocol.
- o **CER\_TYPE.** Smart card certificate validation.
- o **EXPIRATION.** Certificate expiration validation.

**Note:** The validation strategy can be a combination of these values and the delimiters are commas. For example:  
validationStrategy=CER\_TYPE, EXPIRATION

- e. Set the root certificate path.  
**RootCertPath=<root\_certificate\_path>**  
where <root\_certificate\_path> is used for validation strategy. It can be: **LOCAL\_CRL**, **ONLINE\_CRL**, or **OCSP**.
- f. Set the store path.  
**CRLStoreLocation=LOCAL\_CRL**  
This is used for validation strategy.
- g. Set the online CRL URL Path.  
**CRLDownloadURL=ONLINE\_CRL**  
This is used for validation strategy.
- h. Set the OCSP Responder URL.  
**OCSPResponderURL=OCSP**  
This is used for validation strategy.
- i. Set the OCSP Server cert.  
**OCSPServerCertPath=OCSP**  
This is used for validation strategy. If the value is not set, the OCSP Server cert used RootCert instead.

#### 4. Customize the content of the splash screen.

Once CAC is enabled, you **MUST** configure the splash screen to show a popup dialog that displays agreement terms to the end user. The end user **MUST** agree to the terms to continue after choosing the certificate for login.

The customized splash screen can be configured with pure html code in the following file:

**%HPXS\_  
HOME%\agora\glassfish\glassfish\domains\BTOA\applications\bsf\splashScreen.html**

The splash screen with the default content is as follows:

### HP IT Executive Scorecard

HP IT Executive Scorecard is a strategy enabler that enables executives to continuously improve their business by measuring what happened and what is happening, analyzing that information, and planning new strategies using the gathered information. This enables a better strategy execution resulting in a reduction of cost and risk, and an increase in quality and value.

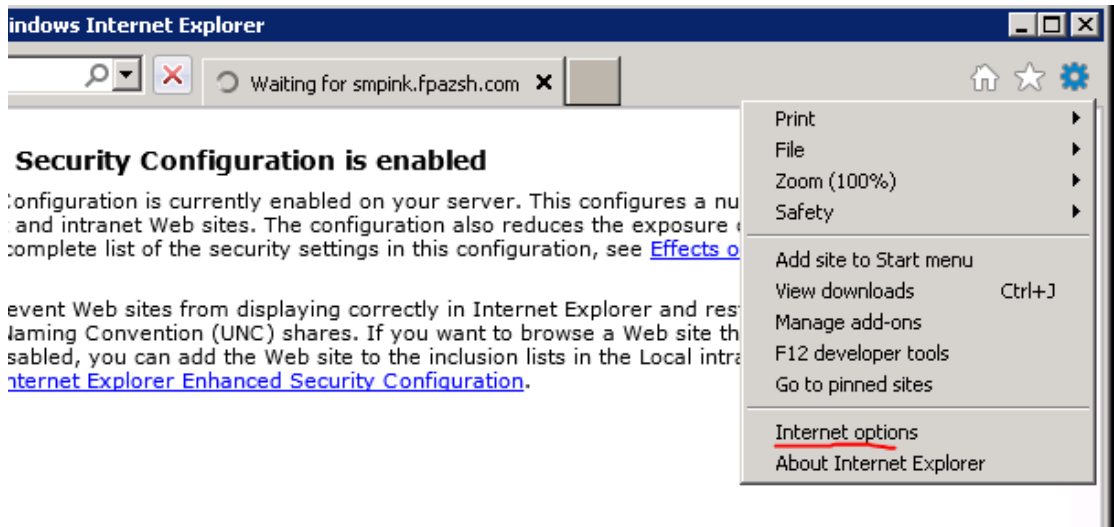
**The following topics provide the main steps to follow to get started with the Studio and the Dashboard:**

- Learn about how the Executive Dashboard can help the challenges facing Executives.
- Make sure the HP IT Executive Scorecard settings are configured.
- Make sure the HP IT Executive Scorecard users and permissions are configured.
- Create and activate Scorecards, Perspectives, Objectives, Metrics, and KPIs.
- Enrich the Dashboard contents with Metric Breakdowns and KPIs, overrides, Cascading Scorecards, and more.
- Review the out-of-the-box Executive pages, add components to pages, create your own components, or create your own pages.
- The Executive user can now view and analyze the relevant business objectives.
- Perform the maintenance of HP IT Executive Scorecard.

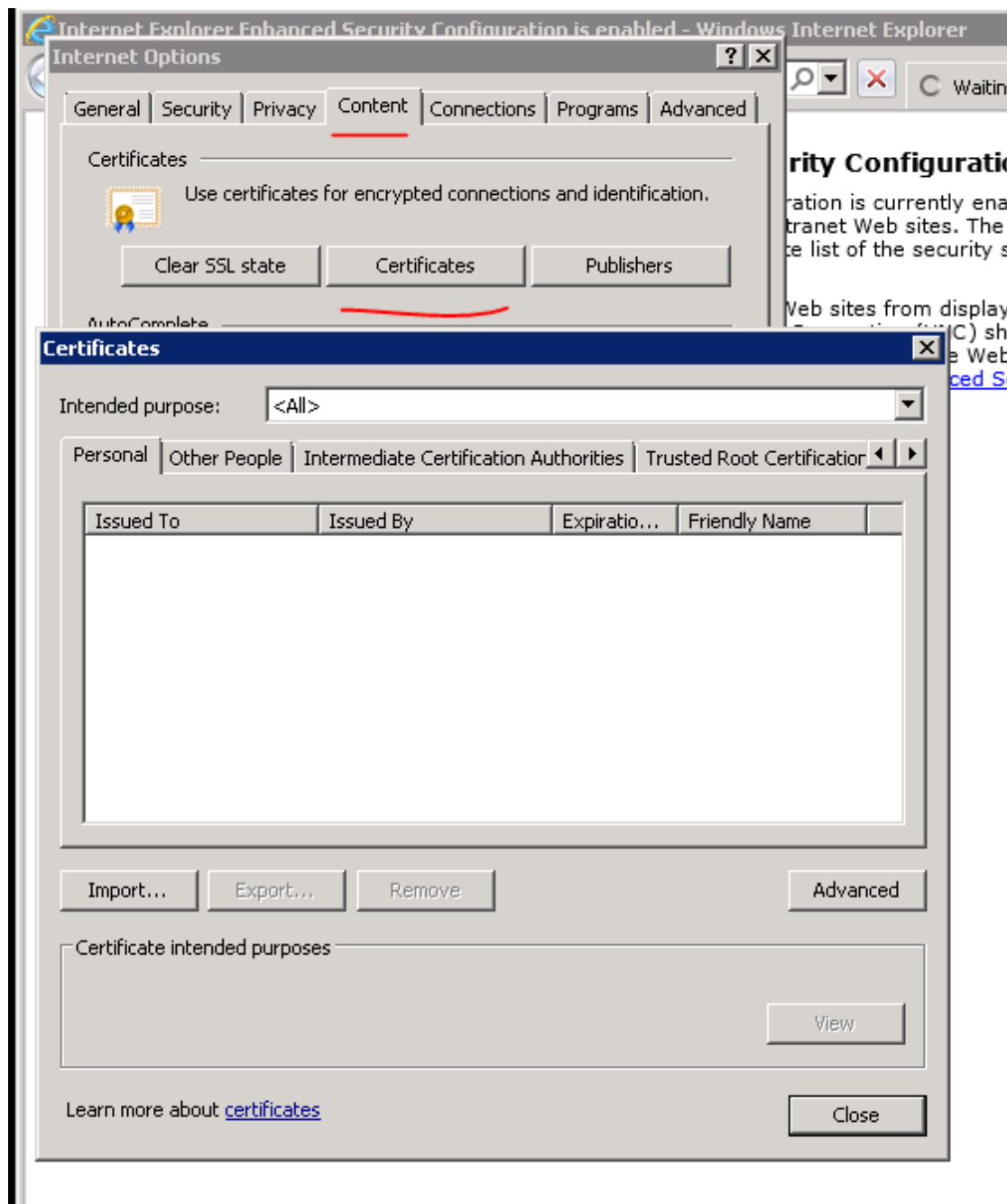
Accept

5. Install the client certificate in the client browser.

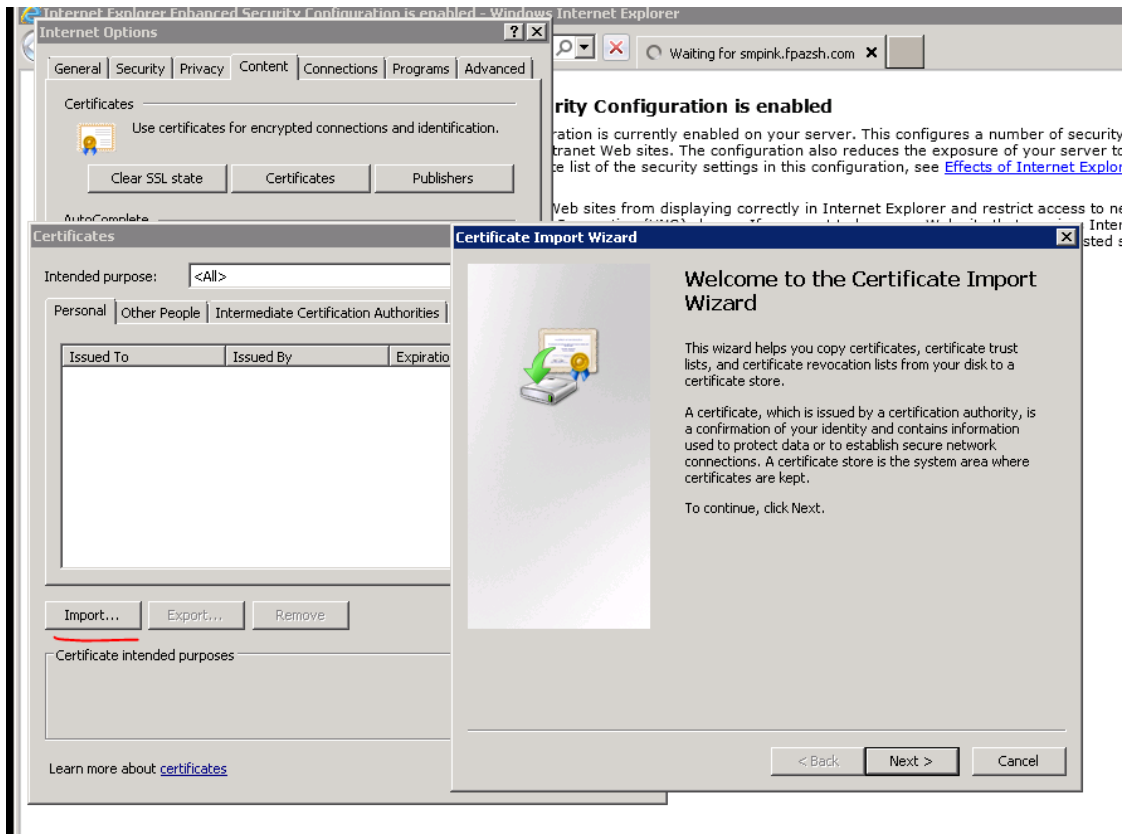
In the client browser, select **Internet Options**.



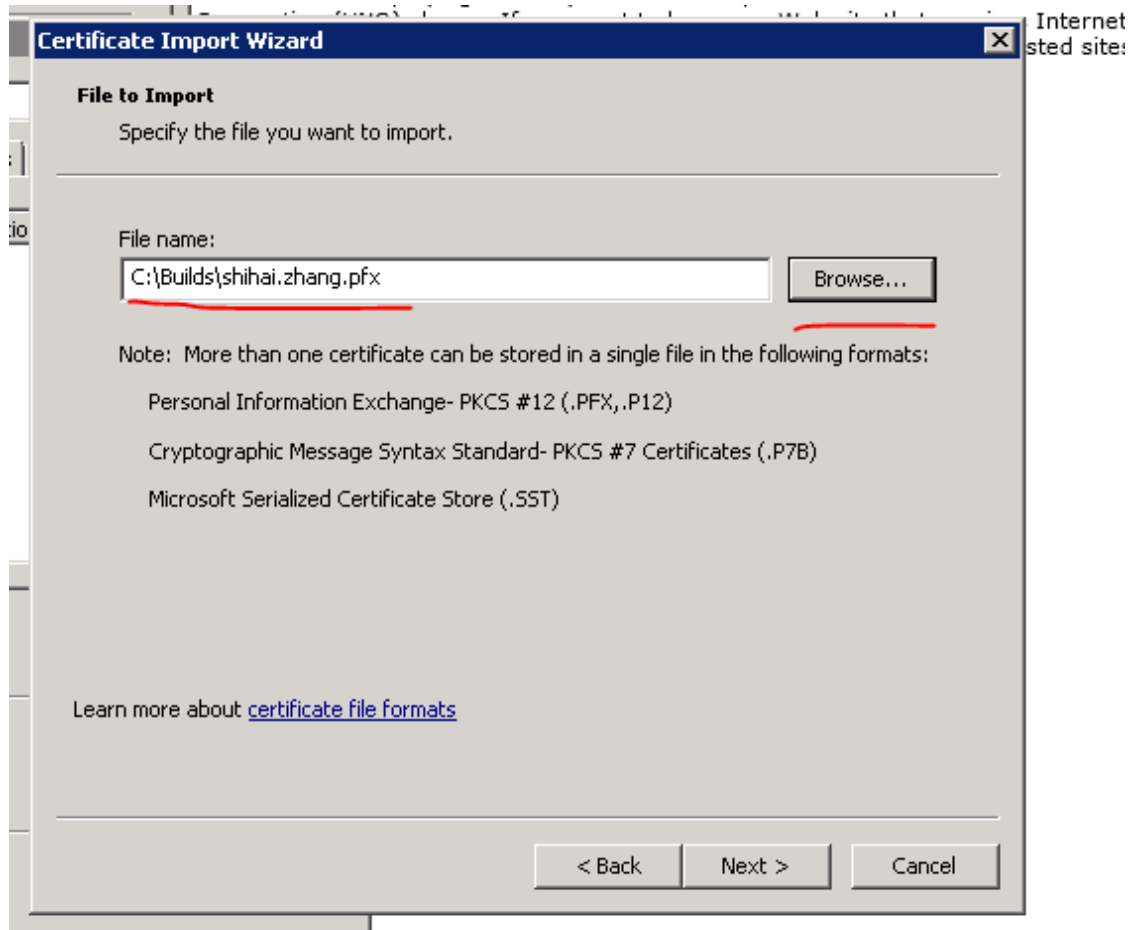
Click **Content > Certificates**:



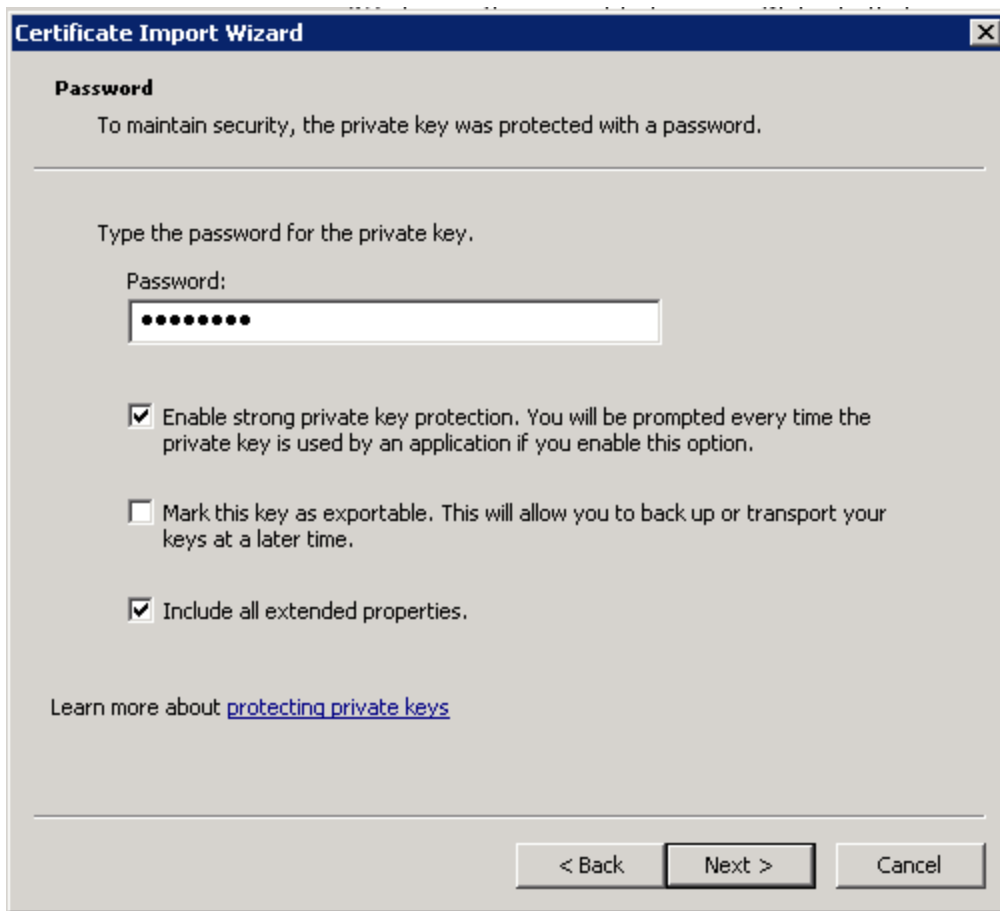
Click **Import**:



Enter the path to the file you want to import:



Enter the password:



**Certificate Import Wizard** [X]

**Password**

To maintain security, the private key was protected with a password.

---

Type the password for the private key.

Password:  
[.....]

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

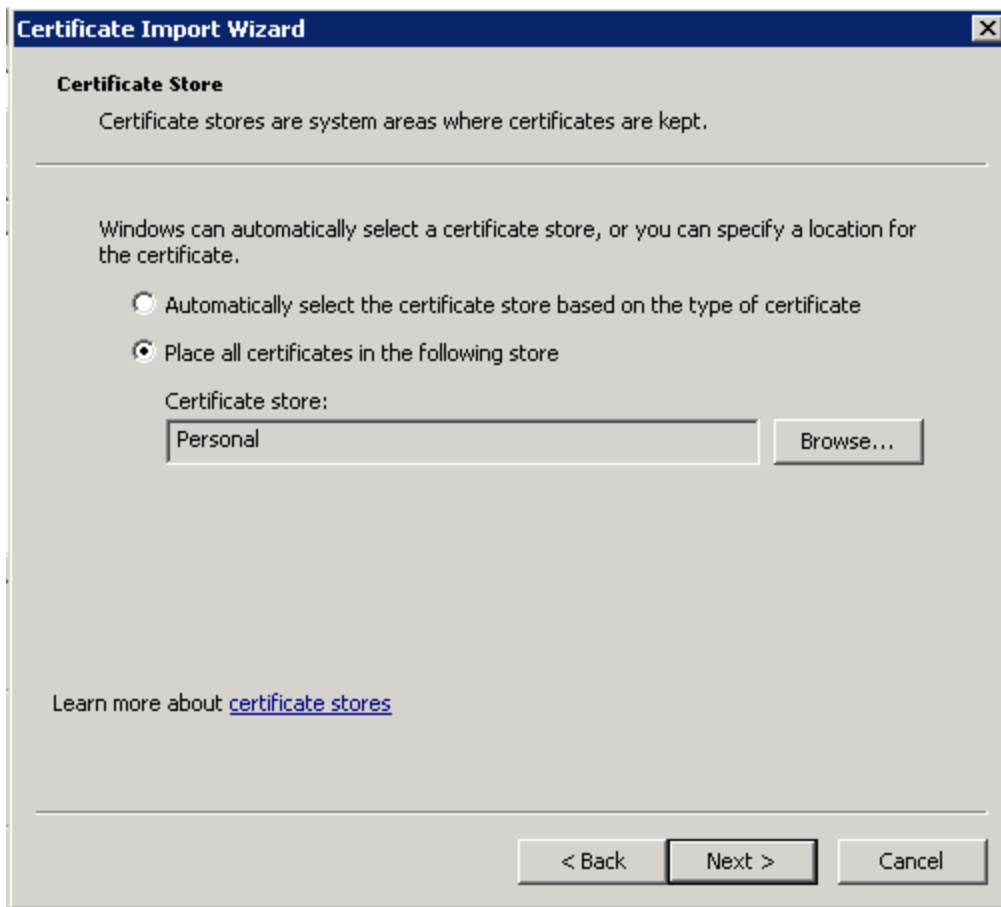
Include all extended properties.

Learn more about [protecting private keys](#)

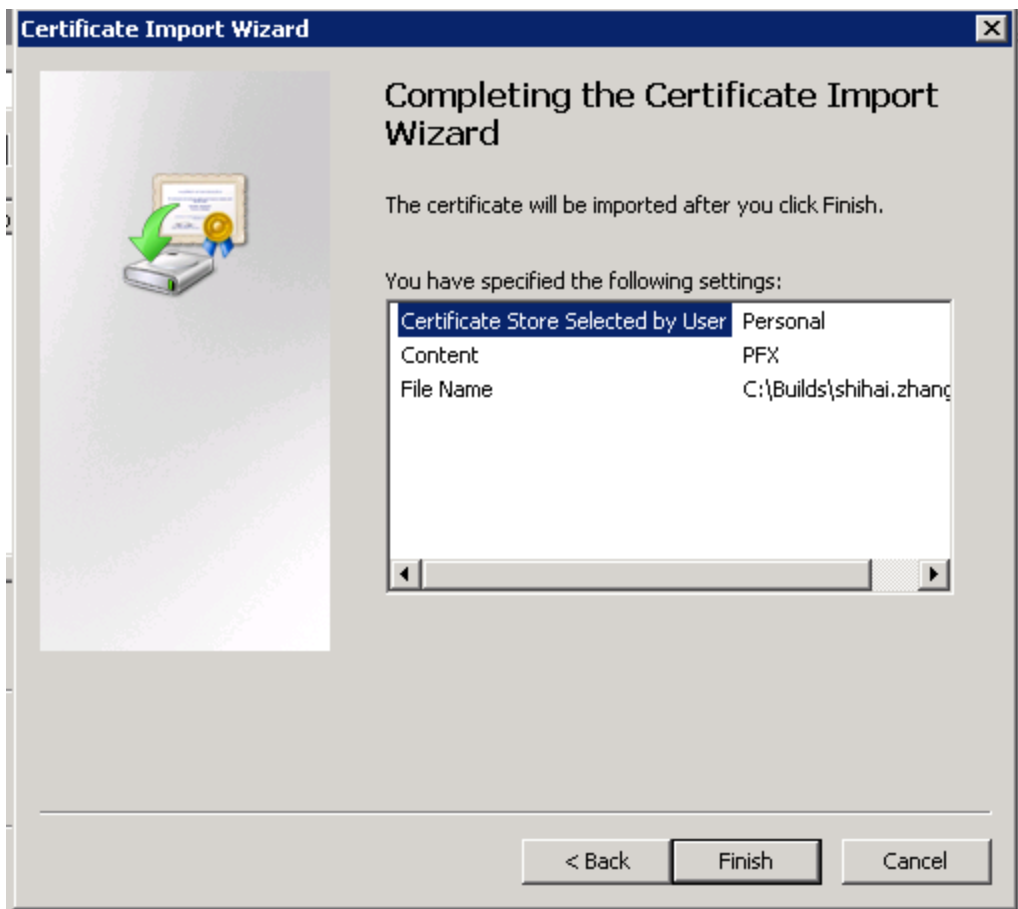
---

< Back    Next >    Cancel

Click **Next**.

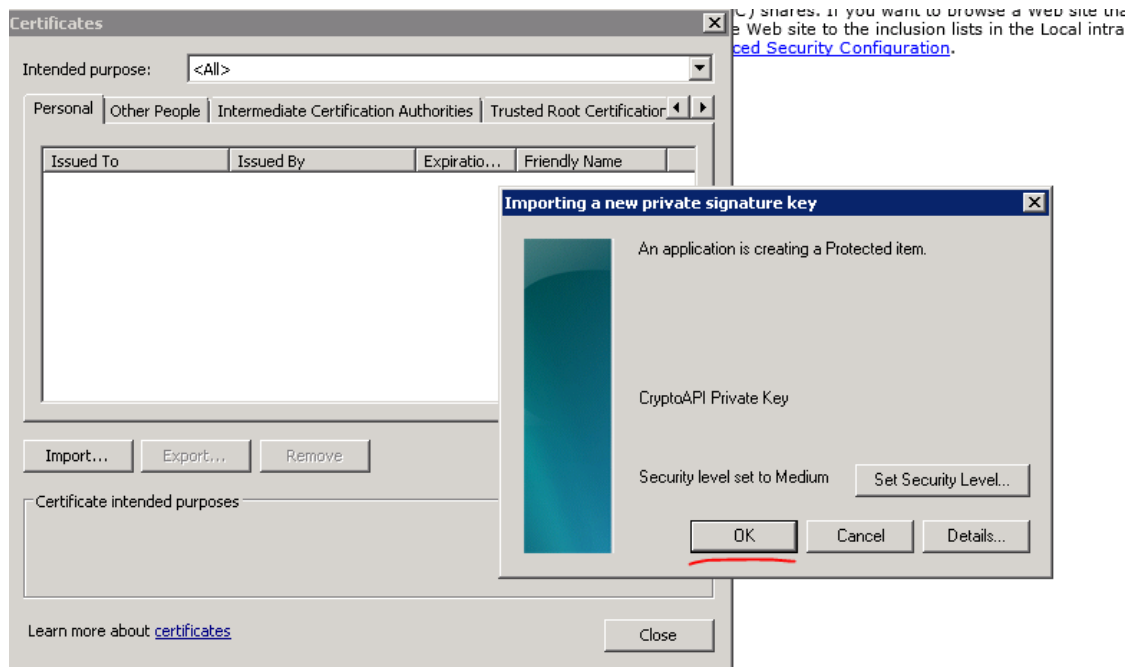


Click **Next**.

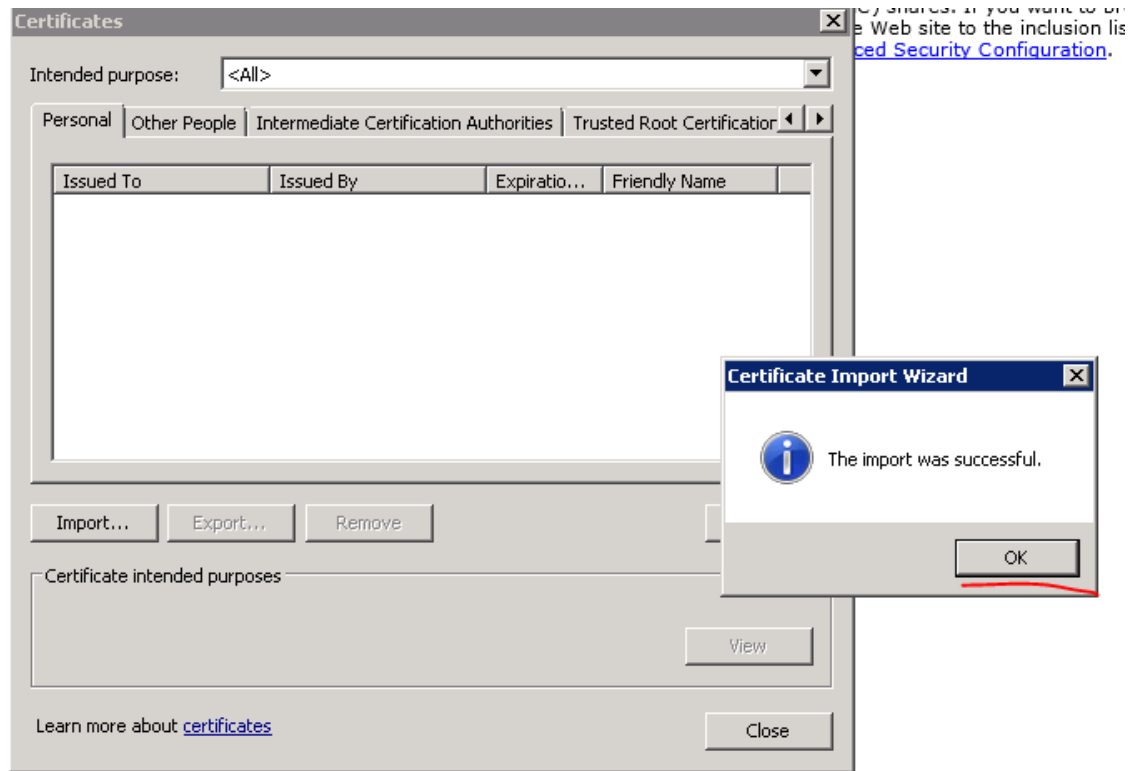




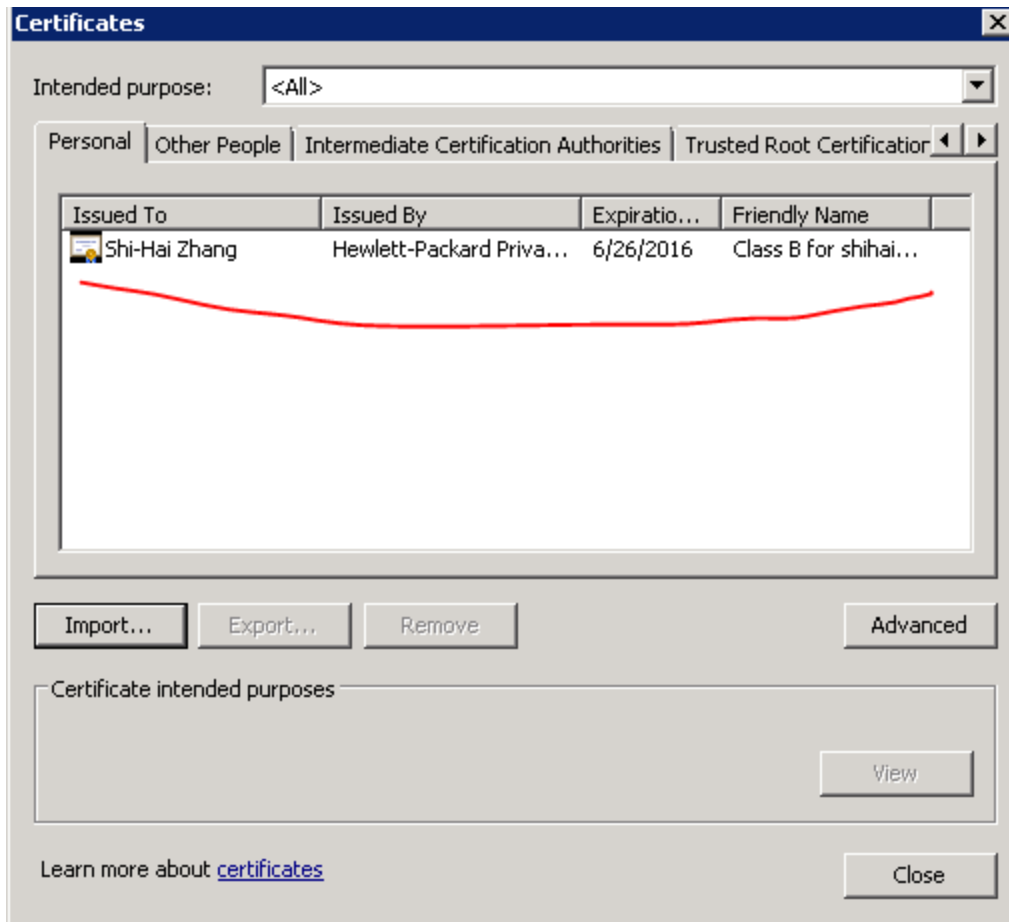
Click **Next**.



Click **Next**.

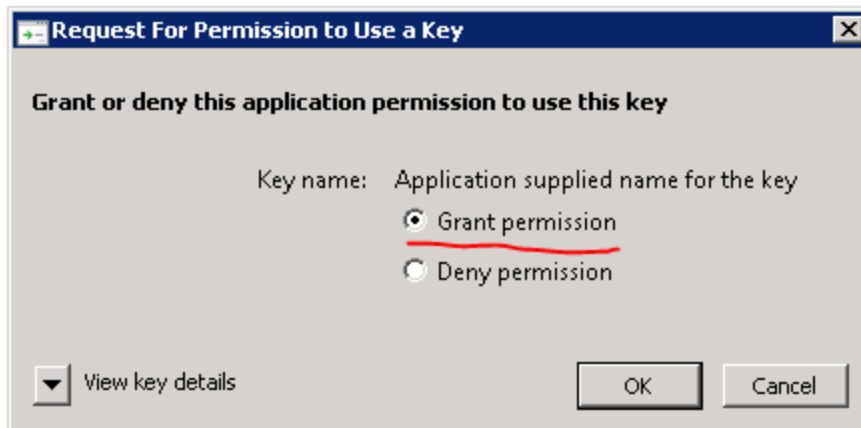


Click **Next**.



6. **Restart the XS server.**

When performing a logon, the end user is now required to provide CAC credentials before accessing the XS application from a browser.



Note that if you work with Chrome or Firefox you must make sure to follow a similar procedure for these browsers.

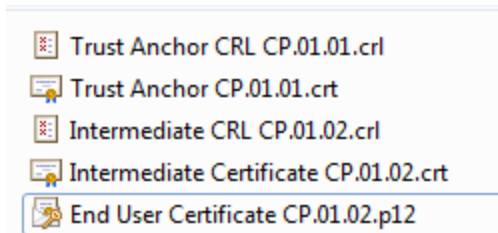
**Note:** The <HPXS>\agora\glassfish\glassfish\domains\BTOA\logs\cac.log is issued when the user certification is revoked.

## Example of a CAC Configuration

### Precondition:

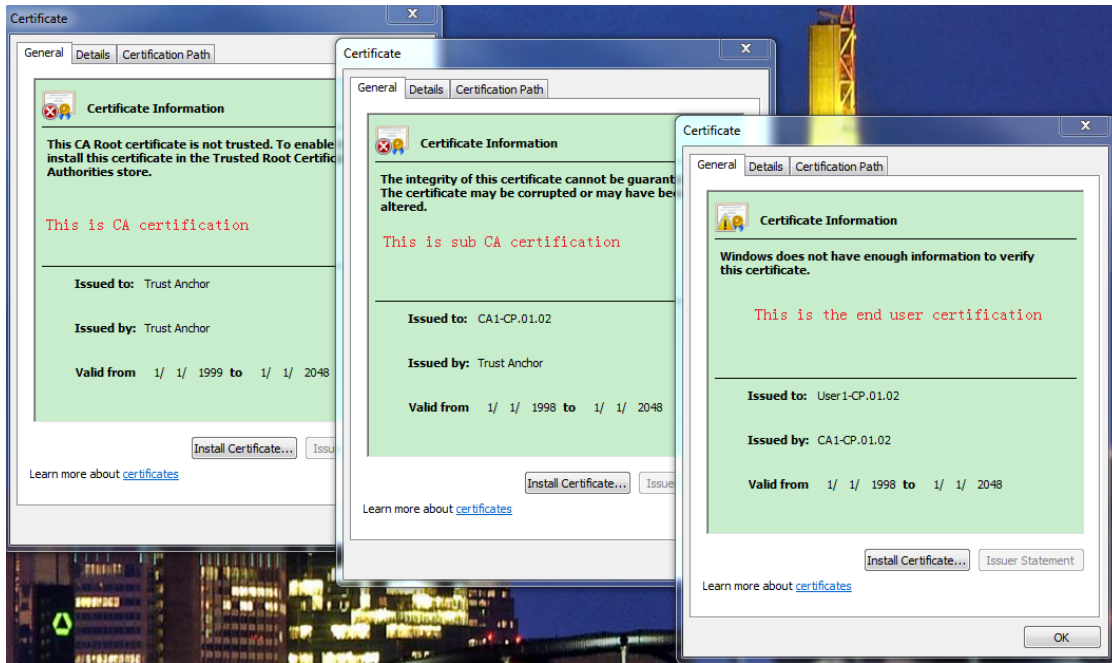
#### 1. Certification files:

We have the following certification files.



where:

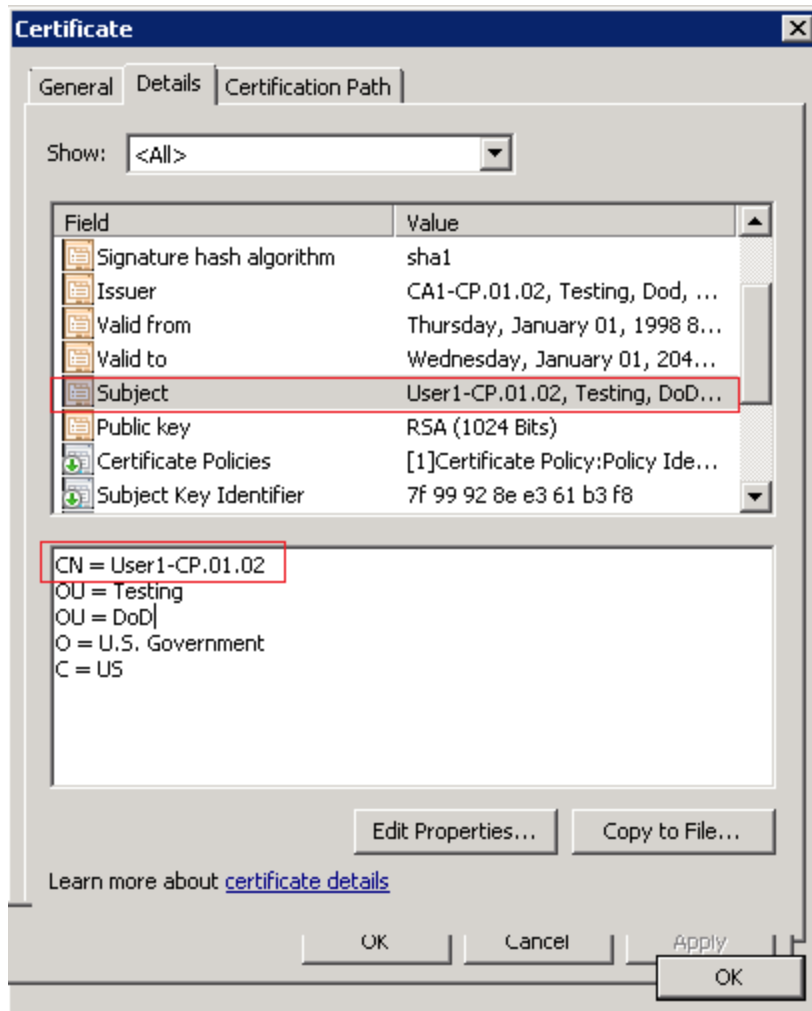
- **Trust Anchor CP.01.01.crt:** The CA certification.
  - **Trust Anchor CRL CP.01.01.crl:** The certification revocation list by CA certification.
  - **Intermediate Certificate CP.01.02.crt:** The sub CA certification, which is issued by above CA.
  - **Intermediate CRL CP.01.02.crl:** The certification revocation list by the sub CA certification.
  - **End Certificate CP.01.02.p12:** The end user certification, which is issued by the sub CA certification. If the end user certification is issued by CA certification, the sub certification is not needed.
2. **Relations:** The end user is issued by sub CA, sub CA is issued by CA.



### 3. End User Certification:

**Note:** The SUBJECT.CN for the end user certification is : **User1-CP.01.02**. It is the logon name in this example, so make sure you have such a logon user in already in the XS application.

- End User certification details:



- XS application logon user:

ID	LOGIN_NAME	PASSWRD	UNIQUE_ID
917504	User1-CP.01.02	{SSHA256}IKBA...	24395
1146880	George	{SSHA256}Ro6X...	34908
*	NULL	NULL	NULL

### Configure CA certification

On the XS application server (Do the following on the XS application server if you have a distributed configuration)

1. Copy the above certification files to %HPXS\_HOME%\agora\conf\keys.
2. Edit the %HPXS\_HOME%\agora\webserver\conf\extra\httpd-ssl.conf configuration file, as shown below.

```

22
23 JkMountCopy On
24
25 SSLEngine on
26
27 SSLCertificateFile "../conf/keys/btoa.host.hp.com.cert.pem"
28
29 SSLCertificateKeyFile "../conf/keys/btoa.host.hp.com.key.pem"
30
31 SSLCACertificateFile "../conf/keys/Trust Anchor CP.01.01.crt"
32 JkOptions +ForwardSSLCertChain
33 <Location /bsf >
34     SSLVerifyClient optional
35     SSLVerifyDepth 10
36     SSLOptions +StdEnvVars +ExportCertData
37 </Location>
38
39 #BrowserMatch ".*MSIE.*" \
40 #     nokeepalive ssl-unclean-shutdown \
41 #     downgrade-1.0 force-response-1.0
42
43
44 CustomLog "../webserver/logs/ssl_request.log" \
45     "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
46
47 </VirtualHost>
48

```

3. Enable the CAC mode:

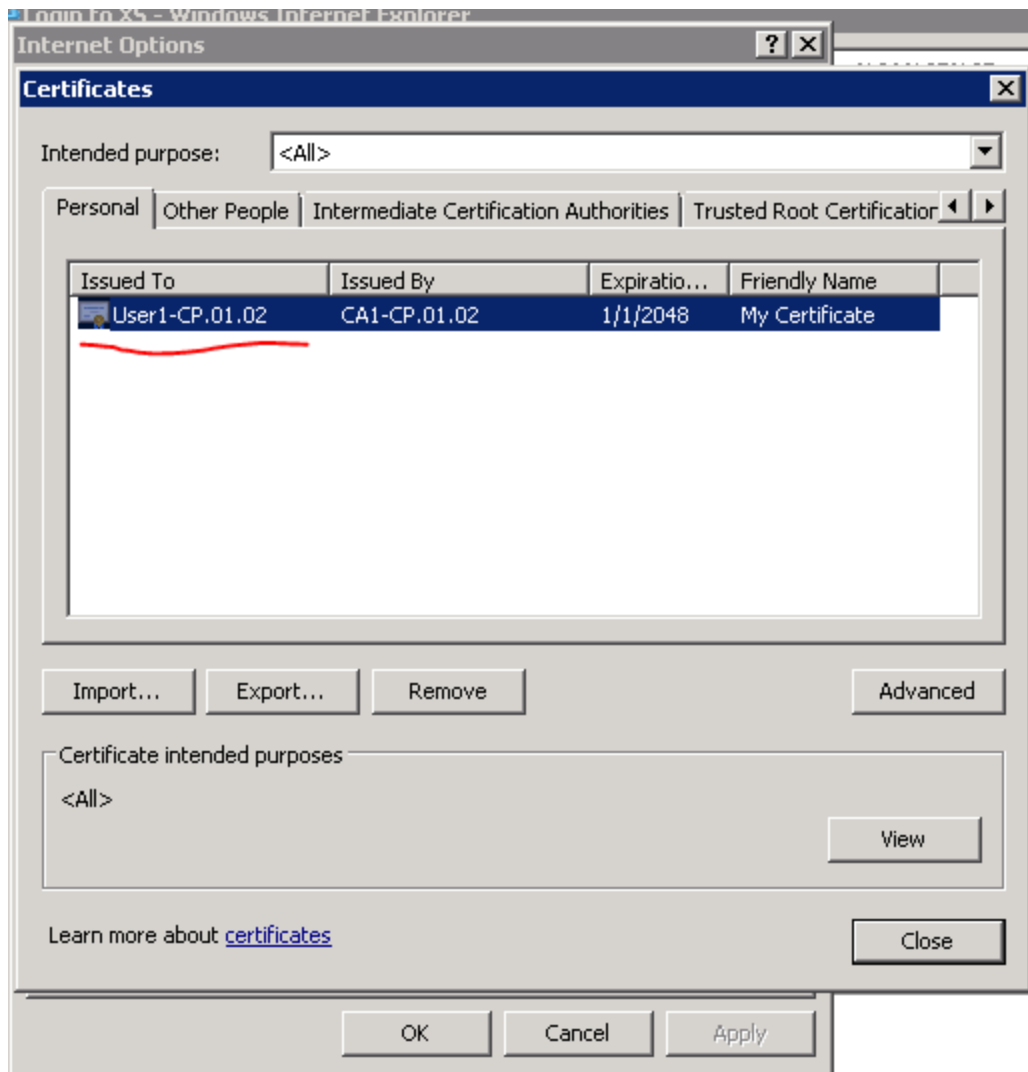
Edit the **%HPXS\_HOME%\agora\glassfish\glassfish\domains\BTOA\config\conf\cac.properties** property file, as shown below:

```

C:\HPXS\agora\glassfish\glassfish\domains\BTOA\config\conf\cac.properties - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd-ssl.conf cac.properties
1 # The flag used to open CAC mode
2 #==== Default value - false
3 isCAEnabled=True
4
5 # The flag used to indicate which field is "login name"
6 certificateFieldExtractDN=SUBJECT.CN
7
8 #oidMap an OID map, where each key is an object identifier in String form
9 #eg:"E:1.2.840.113549.1.9.1" mutiple mappings separated by comma
10 certificateOIDMapping=
11
12 # The flag used to indicate the requirement of validation
13 #==== Default value - true
14 validationEnforced=true
15
16 # validation strategy
17 # optional values :LOCAL_CRL,ONLINE_CRL,OCSP,CER_TYPE,EXPIRATION
18 # Delimiters is comma.eg:CER_TYPE,EXPIRATION
19 validationStrategy=EXPIRATION,LOCAL_CRL
20
21 #Root Cert Path
22 #==== This value is used for validation strategy:LOCAL_CRL,ONLINE_CRL,OCSP.
23 RootCertPath=C:/HPXS/agora/conf/keys/Trust Anchor CP.01.01.crt,C:/HPXS/agora/conf/keys/Intermediate Certificate CP.01.02.crt
24
25 #CRL store path
26 #==== This value is used for validation strategy:LOCAL_CRL
27 CRLStoreLocation=C:/HPXS/agora/conf/keys/Trust Anchor CRL CP.01.01.crl,C:/HPXS/agora/conf/keys/Intermediate CRL CP.01.02.crl
28
29 #online CRL URL Path
30 #==== This value is used for validation strategy:ONLINE_CRL
31 CRLDownloadURL=
32
33 #OCSP Responder URL
34 #==== This value is used for validation strategy:OCSP
35 OCSPResponderURL=
36
37 #OCSP Server cert
38 #==== This value is used for validation strategy:OCSP
39 #==== if this value is not indicated ,it would use RootCert instead
40 OCSPServerCertPath=

```

4. Restart the XS service.
5. Install the **End Certificate CP.01.02.p12** certification to your browser according to the steps that mentioned above:



You can now log on to the XS application using the end user certification via CAC.



# Decimal Precision

The decimal precision used in displays in Business Analytics is as follows:

- **Studio/Dashboard/Explorer.** By default, the values of KPIs and Metrics are displayed with a maximum of 6 digits (default) (for example: 123456) and if needed a decimal point (123.456).  
Digits after the decimal point are rounded to 5 digits maximum. For example: 456.7893 is rounded to 456.789.  
Digits before the decimal point are rounded to 3 digits maximum. If there are more than 3 digits before the decimal point, K, M, or T are used to indicate the correct value. For example: 3300122.111 is displayed as 3.300 M, and 999999 is displayed as 999.999 K.



- **Thresholds in Studio.**

Because the threshold fields in the Studio are where you enter the threshold values, the thresholds display all the digits before the decimal point. Nevertheless, if you configure a KPI threshold with more than 3 digits after the decimal point, they are rounded to 3 digits. For example:



The Administrator can change the default using one of the following options:

- in **Admin > Settings > Dashboard Settings**, you can specify a total number of digits (between 3 and 6) in the **Total number of digits displayed for KPI/Metric results** setting. Note that the number of digits before the decimal point is up to 3 with a K, M, or T indication when needed.
- in **Admin > Settings > Dashboard Settings**, you can specify the number of digits (between 0 and 5) after the decimal point in the **Max number of digits after decimal point** setting.

Note that the two settings must work together. The **Total number of digits displayed for KPI/Metric results** setting decides the total number of digits that is displayed while the **Max number of digits after decimal point** setting provides the number of digits that is displayed after the decimal point depending on the number of digits of the number.

Settings	Number		
	123.123456	1.123456	12345.123456
Total number of digits displayed for KPI/Metric results = 6 Max number of digits after decimal point = 5	123.123	1.12345	12.3451 K
Total number of digits displayed for KPI/Metric results = 3 Max number of digits after decimal point = 5	123	1.12	12.3 K
Total number of digits displayed for KPI/Metric results = 6 Max number of digits after decimal point = 2	123.12	1.12	12.34 K

# XS 9.50 Patch 03 for Windows

## Defects Corrected in the XS 9.50 Patch 03 for Windows

XS 9.50 Patch 03 for Windows supersedes the XS 9.50 Patch 02 for Windows and the XS 9.50 Patch 01 for Windows.

XS 9.50 Patch 03 for Windows corrects the following:

<b>Change Request</b>	<b>Description</b>
QCCR8B21176	DWH - SM - PERSON/ORG/NODE/APPLICATION/CI/ASSET/MODEL/LOCATION.MD_BUSINESS_KEY should support non-sensitive case.
QCCR8B21252	DWH - SM-backfill control has performance issues.
QCCR8B21333	LDAP - The User/RootGroups/SearchGroups/ list is blank when the results set is larger than the MaxPageSize configure of LDAP server.
QCCR8B21452	SM - Update MSI template to update the Datetime lookup method should be '=' to resolve performance issue.
QCCR8B21536	LDAP- We cannot add view role to the ldap groups in the UserManagement page.
QCCR8B21537	Login Error- An error message (Google java null point error) pops up when first time logon XS after configure LDAP.
QCCR8B21587	Date format is always in US format.
QCCR8B21682	DWH - SM - If the foreign key points to PERSON/ORG/NODE/APPLICATION/CI/ASSET/MODEL/LOCATION.MD_BUSINESS_KEY, it is always equal to -2.
QCCR8B21704	The KPI View component incorrectly displayed after it is changed to a historical chart when wiring from the Objective in Perspective (containing more than two Objectives) of Cascading Scorecard.
QCCR8B22091	'Generate URL' for dashboard page disappears in IE9 and IE10.

# Enhancements Added in the XS 9.50 Patch 03 Revision 1 for Windows

The enhancements added to the Patch are as follows:

Change Request	Description
QCCR8B20938	<p>SM PinkVerify</p> <p>New KPIs, compliant with PinkVERIFY™, were added to Patch 03 Revision 1 for Windows. Refer to "List of KPIs and Metrics" in the <i>SM Content Acceleration Pack Guide</i> that is part of the patch package for a detailed description of these new KPIs. Note that some of these KPIs have a version limitation that is provided in the detailed description.</p> <p>The documents that accompany the patch are (click go to download the document from the <a href="#">Support Site</a> (<a href="https://softwaresupport.hp.com/group/software-support/home">https://softwaresupport.hp.com/group/software-support/home</a>)):</p> <ul style="list-style-type: none"><li>• <i>HP IT Executive Scorecard XS 9.50 Patch 03 Revision 1 for Windows</i> -- <a href="#">go</a></li><li>• <i>CAP_SM Content Acceleration Pack Guide</i> -- <a href="#">go</a></li><li>• <i>Content Reference Guide for the Integration with HP Service Manager</i> -- <a href="#">go</a></li><li>• <i>Support Matrix</i> -- <a href="#">go</a></li></ul> <p>The patch is available at: <a href="#">go</a></p>
QCCR8B20943	SA 10.2 support
QCCR8B21572	Page filter to affect 'Scorecard component

## New Certifications

**Supported Integrations:** HP Service Manager 9.40 and HP Server Automation 10.2.

# XS 9.50 Patch 02 for Windows

## Defects Corrected in the XS 9.50 Patch 02 for Windows

XS 9.50 Patch 02 for Windows supersedes the XS 9.50 Patch 01 for Windows.

XS 9.50 Patch 02 for Windows corrects the following:

<b>Change Request</b>	<b>Symptoms</b>
QCCR8B20895	Context Designer: Excel file loading issue.
QCCR8B20934	Log Portal does not work on distribution model.
QCCR8B20936	Initial load has performance issue.
QCCR8B20941	CSA billing is incorrect if the XS ETL is not set to run daily.
QCCR8B21023	XS950 doesn't perform the calculation for the option initial_price and recurring_price in CSA.
QCCR8B21104	XS950 will use the resource provider of the parent node if the current node doesn't have resource provider in CSA design.
QCCR8B21122	XS950 only support English in the Scorecard component.
QCCR8B21145	XS950 will get a hang issue during a KPI calculation.
QCCR8B21250	Missing org page in CSA and CSA_CSP_DEMO.
QCCR8B21251	XS950 filter the consumer from userlist.
QCCR8B21302	XS950 will produce a Java Applet unreachable error when log on XS.
QCCR8B21325	XS950 application is getting stuck on Loading Data API after login.
QCCR8B21326	Cannot run insecure content of XS in Chrome.

## Enhancements Added in the XS 9.50 Patch 02 for Windows

The enhancements added to the XS 9.50 Patch 02 for Windows are as follows:

<b>Change Request</b>	<b>Description</b>
QCCR8B20907	Android platforms are now supported.
QCCR8B20935	The JDBC Driver was updated to 4.0.
QCCR8B20937	Delta load was optimized.
QCCR8B20942	Data filter in CSA bundle pages and reports by organization name and consumer name is now supported.
QCCR8B20972	The one server design in CSA is now supported.
QCCR8B21119	KPIs can be sorted in the Studio and in Explorer.
QCCR8B21127	The sorting for Perspectives, Objectives and Child KPIS is now supported in the Cascade Scorecard.

## New Certifications

**Client Environments and Optional Software:** Microsoft Exchange 2013

**Supported Integrations:** HP Server Automation10.1, HP Cloud Service Automation4.2 and 4.1.

**Report tool:** Xcelsius Reports Viewer component supports the new SAP® Business Objects Dashboards 4.1 (Xcelsius dashboards) format.xlf.



# XS 9.50 Patch 01 for Windows

XS 9.50 Patch 01 for Windows corrects security issues.

# 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.

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 Notice

© Copyright 2011-2015 Hewlett-Packard Development Company, L.P.

## Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

AMD is a trademark of Advanced Micro Devices, Inc.

Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

# Documentation Updates

The title page of this document 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: **<https://softwaresupport.hp.com>**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **<https://hpp12.passport.hp.com/hppcf/createuser.do>**

Or click the **Register** link at the top of the HP Software Support page.

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

Visit the HP Software Support Online web site at: <https://softwaresupport.hp.com>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web 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 register for an HP Passport ID, go to:

<https://hpp12.passport.hp.com/hppcf/createuser.do>

To find more information about access levels, go to:

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

**HP Software Solutions Now** accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

## About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

### Document Change Notes

The following table provides details of any changes introduced in this version of this document.

<b>Date</b>	<b>Change</b>
August 2015	Original release of this document