SAP BusinessObjects Mobile
Document Version: 4.2 Support Package 2 – 2016-03-07

# Mobile Server Deployment and Configuration Guide

# Content





© 2016 SAP SE or an SAP affiliate company. All rights reserved.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 1 Target Audience

This guide is designed to help the following end users:

- IT administrators who deploy and configure SAP BusinessObjects Mobile server.
- Business Intelligence administrators who:
  - Plan how Business Intelligence (BI) data and applications are deployed and managed.
  - Manage BI documents and folders for mobile users.
- IT security managers who perform the following tasks:
  - Guarantee that Business Intelligence data communicated through the Internet and wireless networks remains secure.
  - Manage mobile client access and the security policy of the Mobile server.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 2 What's New in the Mobile Server?

## Push Notifications on iOS Devices

The SAP BusinessObjects Mobile server pushes notifications to iOS devices of the SAP BusinessObjects Mobile application users. Notifications occur in the following scenarios:

- When the BI documents are downloaded on user's device have an update or a new instance available on the server.
- When a new document is received in user's BI Inbox.
- When the BI platform or BOE administrator broadcasts a message.

Notifications are automatically pushed to the device from the Mobile server through the Apple Push Notification Server (APNS). Users do not need to explicitly refresh the application home screen to fetch updates through an active connection. The "notification settings" should however be enabled in the application. For more information, refer to the *Mobile Server Deployment and Configuration Guide* for Mobile Server 4.2.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 3 Introducing the SAP BusinessObjects Mobile Solution

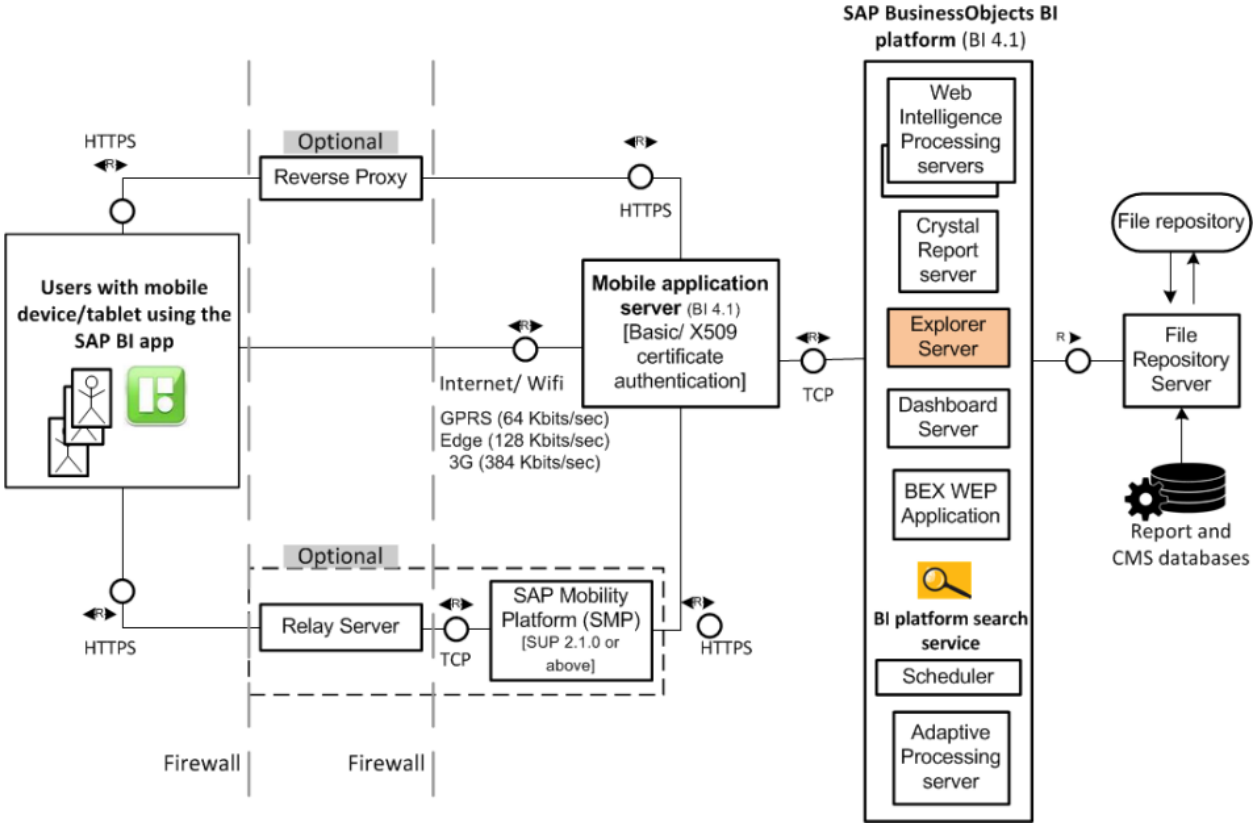
## 3.1 Solution Overview

The SAP BusinessObjects Mobile solution allows users to access and analyze business intelligence data using a mobile device and to help make analytical decisions while being on the move.

This solution comprises the following three major components:

- SAP BusinessObjects Mobile client
- SAP BusinessObjects Mobile server
- SAP BusinessObjects Business Intelligence (BI) platform

The above components and their inter-relation is displayed in the below figure:




### Related Information


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 3.1.1 SAP BusinessObjects Mobile Client

In this document, client refers to the SAP BusinessObjects Mobile application available for iOS platform. The application is designed specifically to optimize the display of Business Intelligence (BI) content while considering the space and interactivity constraints of the mobile device screens.

The following table summarizes the BI content types supported in the SAP BusinessObjects Mobile application on various mobile devices:

Table 1: BI Content Support Matrix for Mobile Devices

| BI Content Type | iPad | iPhone |
|---|---|---|
| Web Intelligence | Y | Y |
| Crystal Reports | Y | Y |
| Dashboards (Design Studio documents) | Y | N |
| Analysis applications | Y | Y |
| Explorer Information spaces/exploration views | Y | Y |
| Lumira artifacts | Y | N |
| Hyperlinks | Y | Y |

SAP BusinessObjects Mobile works on data infrastructures such as Edge, Wi-Fi and 3G networks.

> **Note**
>
> SAP BusinessObjects Mobile supports BI reports created using the SAP Business Warehouse. Depending on the document type, you can view, analyze, and interact with the data contained in the documents.

- For information about how to configure server settings for the SAP BusinessObjects Mobile application for iOS devices, refer to the *Administrator's Guide* available at http://help.sap.com/bomobileios.

## 3.1.2 SAP BusinessObjects Mobile Server

SAP BusinessObjects Mobile server is a Web application server. It performs the following functions:

- Receives requests sent by the SAP BusinessObjects Mobile client and passes them to the SAP BusinessObjects Business Intelligence (BI) platform server.
- Receives responses (For example: Web Intelligence document or Crystal report document) from the SAP BusinessObjects Business Intelligence (BI) platform server and sends them to the SAP BusinessObjects Mobile client.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The Mobile server can communicate with multiple SAP BusinessObjects Business Intelligence platform Central Management Servers (CMS). You specify the CMS name on the "Connection Settings" screen of the Mobile client application on each device. This means that different devices can connect to different CMS servers based on your deployment. The Mobile server forwards the connection request to the CMS as specified on the device.

## 3.1.3 SAP BusinessObjects Business Intelligence (BI) Platform

The SAP BusinessObjects BI platform server projects the data captured from corporate databases and data warehouses as business intelligence documents or reports. It handles all aspects of the document lifecycle, including creation, cataloging, refreshing, content delivery, and reporting interactivity.

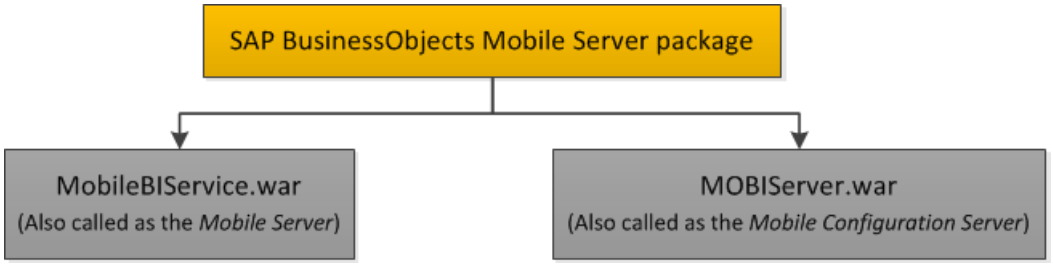
The SAP BusinessObjects BI platform server processes requests sent by the SAP BusinessObjects Mobile client through the SAP BusinessObjects Mobile server, and sends back responses (for example, a Web Intelligence document or a Crystal Report document).

> **Note**
>
> - If you are accessing the portal through a desktop computer, this portal is termed as the BI launch pad.
> - If you are accessing the portal as a mobile user, this portal is termed as the SAP BusinessObjects Business Intelligence Platform server


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 4 Deploying the SAP BusinessObjects Mobile Server Package

The SAP BusinessObjects Mobile server package includes 2 Web applications as shown in the below figure:




- **MobileBIService**: This Web application is **responsible for log on, listing and display of content on mobile devices**.
- **MOBIServer**: This Web application is an **optional piece of deployment**. It is **used for distributing the connection and policies to mobile devices**.

To install the Mobile server package on your Web application server, perform the following steps:

1. Configure your Web application server.
2. Deploy the Mobile server package.

You can also deploy the Mobile server package by auto deploying the Web applications. For more information on this, see the related topic of this chapter.

> **Note**
>
> - For the location of `MobileBIService`, and `MOBIServer` applications, refer to *Auto-deployment of Mobile Server*.
> - The SAP BusinessObjects Mobile server can be installed on the same Web application server on which other SAP BusinessObjects BI platform Web applications are deployed. It can also be installed on a separate Web application server.
> - Explicit configuration for the Tomcat Web application server is not required. However, for JBoss, NetWeaver, WebLogic and WebSphere application servers, you need to perform configuration settings to complete the installation.
> - Load balancing can be setup for MobileBIService using IP based affinity or cookie affinity (also referred to as sticky sessions).

## Related Information

Auto-Deployment of Mobile Server [page 14]

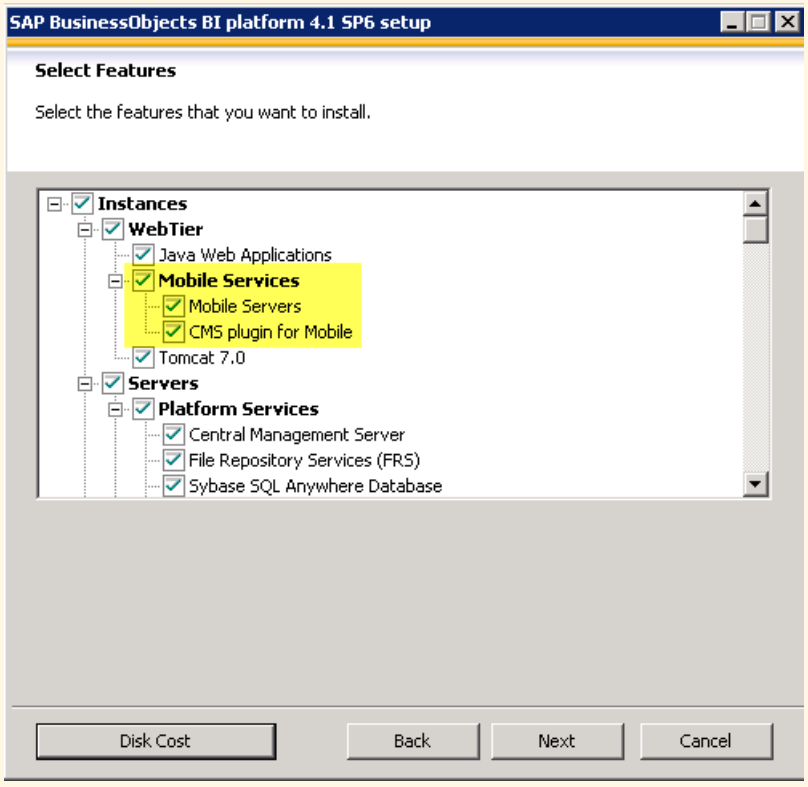

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 4.1 Pre-Installation Checklist

This checklist provides an overview of the steps you need to complete in order to deploy and configure SAP BusinessObjects Mobile. We advise you to read this checklist before beginning the server package deployment procedure.

- Check that your environment meets all the requirements for this version of the SAP BusinessObjects Mobile. To see a list of the supported platforms, visit our website https://support.sap.com/home.html
- Install and configure SAP BusinessObjects Business Intelligence platform.

> **Tip**
>
> Mobile services appear as a set up component (selected by default in the installer) when installing the SAP BusinessObjects BI platform. This is shown in the below figure:




For more information, see *SAP BusinessObjects Business Intelligence Platform Installation and Configuration Guide* .

- Check that the SAP BusinessObjects Enterprise CMS is running.
- Check that your application server is Java-compliant and supported by the latest version of SAP BusinessObjects Business Intelligence platform.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 4.2 Deploying Server Package using WDeploy

### Pre-requisite

- Before installing the SAP BusinessObjects Business Intelligence platform,
  - Your Web application server is installed and working.
  - You meet all the WDeploy prerequisites.

    > **Note**
    >
    > For information on WDeploy prerequisites, refer to the *Web Application Deployment Guide* for Unix and for Windows available at http://help.sap.com/bobip
- You have the Mobile server components selected while installing the Business Intelligence platform, on the same machine on which you have your required Web application server.

To install Mobile server package (MobileBIService, and MOBIServer) using the WDeploy tool, perform the following steps:

1. Stop the Web application server.
2. Create configuration files.

   > **Note**
   >
   > For information on how to customize the WDeploy configuration files, refer to the *Web Application Deployment Guide* for Unix and for Windows available at http://help.sap.com/bobip
3. Deploy the Mobile server application files using the command line:
   - For Unix:
     - wdeploy command : <<BOE_INSTALL_DIR>>/sap_bobj/enterprise_xi40/wdeploy/wdeploy <WEB_APP_SERVER> -DAPP=MobileBIService deploy
     - wdeploy command : <<BOE_INSTALL_DIR>>/sap_bobj/enterprise_xi40/wdeploy/wdeploy <WEB_APP_SERVER> -DAPP=MOBIServer deploy
   - For Windows:
     - wdeploy command : <<BOE_INSTALL_DIR>>\SAP BusinessObjects Enterprise XI 4.0\wdeploy \wdeploy <WEB_APP_SERVER> -DAPP=MobileBIService deploy
     - wdeploy command : <<BOE_INSTALL_DIR>>\SAP BusinessObjects Enterprise XI 4.0\wdeploy \wdeploy.bat <WEB_APP_SERVER> -DAPP=MOBIServer deploy
4. Start Web application server.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 4.3 Configuring Your Web application Server

### 4.3.1 SAP NetWeaver Web Application Server

#### Prerequisites

The Mobile server package consists of the following web applications:

- MobileBIService
- MOBIServer

#### Context

To deploy Mobile server package on the SAP NetWeaver Web application server, perform the following steps:

#### Procedure

1. Edit the `SAP_metadata.properties` file.

   Using a text editor edit SAP_metadata.properties file for each of the three web applications and perform the following steps:
   1. Access the following location: `<BOE_Install_Folder>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\SLDSupport\NWSLD\ .`
   2. Set the counter and release to the version of the product.
      For example: If you are using 4.1, set the counter and release version to 4.1.
   3. Set the service level to match the current SP level.
      For example: If you are using SP4, set the service level to 4. If no service level is applied to this version, set it to 0.
   4. Set the patch level to the current patch level.
      For example: If you are using Patch 3, set the patch level to 3. If there is no patch applied to this SP level, set it to 0.
   5. If you have copied the metadata file from another web application, change the name of this file. The official names for each web application are below:
      - Web Application - name and scn values (change both)
      - MobileBIService - MOBILEBISERVICE
      - MOBIServer - MOBISERVER
   6. Save and exit the file.

   > **Note**
   >
   > If any folders are missing from the Mobile server package, you can create them using the naming scheme for the web applications shown above and copy the `SAP_metadata.properties` file to the new folder from an existing one.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

2. Deploy the mobile SCA files to SAP NetWeaver:
    1. MOVE (cut and paste) all the MOBI*.SCA files from `<BOE_INSTALL_DIR>/<Enterprise_DIR>/wdeploy/workdir/sapappsvr73/application/` to the `<Install_Drive>:\usr\sap\Trans\EPS\in` folder on your SAP NetWeaver host.
    2. Deploy the SCA file on SAP NetWeaver using the JSPM tool.
       To deploy the SCA file on SAP NetWeaver using the JSPM tool, perform the following steps:
        1. Open the `<Install_Drive>:\usr\sap\<AS_ID>\J00\j2ee\JSPM` folder to launch Java Support Manager (JSPM) tool.
        2. Run `go.bat`.
        3. On the Log on screen, enter the SAP NW administrator username and password.
        4. Choose *Log On*.
        5. On the Welcome > *Select Package Type* screen, select *New Software Components*.
        6. Choose Next.
        7. On the *New Software Component* > *Specify Queue* screen, Choose *Next*.
        8. On the *New Software Component* > *Check Queue screen*, Choose *Start*.

## 4.3.2 WebSphere Application Server

To view the Web Intelligence documents on the user's mobile device, launch the WebSphere Web Application Server and perform the following steps:

1. Go to *Enterprise Applications*.
2. Choose *MobileBIService* > *Manage Modules* > *Module*.
3. Under *Update*, select *Classes loaded with local class loader first (Parent Last)*.
4. *Save* configuration.
5. Start *MobileBIService.war* from the administrator console.

## 4.3.3 WebLogic Web Application Server

To deploy the SAP BusinessObjects Mobile on a WebLogic application server, perform the following steps:

1. Set the `<prefer-web-inf-classes>` element to true in weblogic.xml file.
2. Copy `MobileBIService` folder from `<BOE_Install_Folder>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps` to your system local drive.
3. Copy the weblogic.xml file configured in step 1 to the `MobileBIService\WEB-INF` folder.
4. Create a new war file `MobileBIService.war` with META-INF and modified WEB-INF.
5. Open the administration console of WebLogic and perform the following substeps:
    1. Choose *Deployments* > *Install*.
    2. In the *Path* field, access `MobileBIService.war` folder.
    3. Choose `MobileBIService.war`.
    4. Choose *Next*.
    5. Choose *Install this deployment as an application*.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

6. Choose *Next*.
7. Select the desired deployment targets.
8. Choose *Next*.
9. Choose *Next*.
10. Choose *Yes, take me to the deployment's configuration screen*.
11. Choose *Finish*.
12. Choose *Save*.

### 4.3.4 JBoss Web Application Server

For information on how to configure the `MobileBIService` on a JBoss Web Application Server, refer to the latest *Web application Deployment Guide for Windows* available at http://help.sap.com/bobip

## 4.4 Auto-Deployment of Mobile Server

As of release 4.1 SP4 of the SAP BusinessObjects Mobile server, the "MobileBIService.war" and "MOBIServer.war" files are auto-deployed.

If you are upgrading from versions BI 4.1 SP4, XI 3.x or XI R2 of the SAP BusinessObjects Mobile server, choose the auto-deployment scenario in the existing environment, to complete the installation of 4.1 SP5 on your system.

*Windows Operating System*

You can choose any of the following scenarios to auto deploy the .war files depending on the mode of the base installation performed on your server: If your base installation was performed in the:

- *Full Installation Mode*: Install the latest patch in the existing environment to auto-deploy the mobile server on the default application server. You find the mobile server web applications in the following locations:
  - In extracted form: `<Install_Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps`
  - In web archived form: `<Install_Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\tomcat6\application`
- *Custom Installation Mode*: Install the latest patch in the existing environment by choosing "Mobile Servers" and " Web-tier " along with default application server. The mobile server is auto-deployed on the default application server.

  > **Note**
  >
  > If the above mentioned server options are not selected appropriately after the latest patch installation in the existing environment, you need to perform the *Modify* installation on base installation.

- *Web-Tier Installation Mode*: Install the latest patch in the existing environment you need to perform the *Modify* installation in the base installation; the mobile servers are auto-deployed on the default application server.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Mobile servers are only auto-deployed after the *Modify installation*, if the base installation has Web-Tier components.

*Linux Operating System*

- Over BOE (<=4.0 SP05, XI 3.x, XI R2): Install the latest patch in the existing environment. You need to do a `<Modify installation>` over the base installation; the mobile servers are auto-deployed on the default application server.

  > **Note**
  >
  > Mobile servers are only auto-deployed after the *Modify installation*, if the base installation has Web-Tier components.

- Over BI platform 4.0 SP05 and above : To install the 4.1 SP5 Mobile server, choose from the following scenarios:
  - Mobile server installed: Install the latest patch in the existing environment by choosing "Mobile Servers" and "Web-tier" along with default application server. The mobile server is auto-deployed on the default application server.
  - No Mobile server installed : Install the latest patch in the existing environment you need to perform the *Modify installation* in the base installation; the mobile servers are auto-deployed on the default application server.

*AIX/Solaris Operating System*

Install the current patch in the existing environment. You need to perform the modify install on the base installation, to get the mobile server auto-deployed.

> **Note**
>
> Mobile servers are only auto-deployed after the *Modify* install in the base installation, if the base installation has Web-Tier components.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 5 Configuring MobileBIService (Mobile Server)

In MobileBIService, you can configure the following properties files:

Table 2: Configurable Properties Files on the Mobile Server

| File | Purpose |
|---|---|
| `mobi.properties` | Used to define the configuration parameters for mobile server. Server uses this information while responding back to mobile clients and for internal processing.<br>Some examples of these properties include BI document categories (personal/corporate/secure/mobiledesigned/featured), maximum image size, maximum document cache size and maximum displayed search results. |
| `clientsettings.properties` | Used to define the configuration parameters for mobile clients. Mobile clients use these parameter values to enable/disable features or to alter the behavior of the mobile application.<br>**Note**<br>These client settings can also be configured using the iOS or Android application SDK; however, if configured on the mobile server, they take precedence over the SDK configuration. For more information, see the *Developer's Guide* posted on http://help.sap.com/bomobileios or http://help.sap.com/bomobileandroid |
| `sup.properties` | Used to configure the mobile server for the SAP Mobility Platform (earlier known as the Sybase Unwired Platform). |
| `sso.properties` | Used to configure the mobile server for Single Sign On (SSO). |
| `authscheme.properties` | Used to configure the mobile server for Single Sign On (SSO). |

**Note**

The above properties files are located at `<WebApp root>\webapps\MobileBIService\WEBINF\config\default`, where `<WebAppsROOT>` is the folder on your specific application server, for example `C:\Program Files\Apache Software Foundation\Tomcat 6.0`

Besides the Mobile server, you can also use the Central Management Console (CMC) on the BI platform to specify values of mobile properties (mobi.properties) and client settings (clientsettings.properties). The parameter `mobile.server.configuration.location` in the Web application configuration file (located at `<WebApp root>\webapps\MobileBIService\WebContent\WEB-INF\web.xml`) specifies whether you are passing the values of mobile properties and client settings on the Mobile server (MobileBIService) or on the BI platform.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Source Code

```
<context-param>
<description>local-if configuration on server, boe-if configuration in CMC</
description>
 <param-name>mobile.server.configuration.location</param-name>
 <param-value>local</param-value>
</context-param>
```

Note

The default value of `mobile.server.configuration.location` is `boe`. This means that by default the server considers the client settings and mobile properties you specify in the files in MobileBIService. If you want to use the CMC to specify these values, you should update the `mobile.server.configuration.location` value to "boe".

## Configuration in mobi.properties

Following is a typical default configuration of the mobi.properties file:

Source Code

```
#default
default.corporateCategory=Mobile
default.personalCategory=Mobile
default.category.mobileDesigned=MobileDesigned
default.category.secure=Confidential
default.category.featured=Featured
#ipad
ipad.pagemode=true
#iphone
iphone.pagemode=true
#blackberry mobile
bbphone.pagemode=false
#blackberry Tablet
bbtablet.pagemode=false
#android tablet
#android phone
# for internal use
default.search.resultsPerPage=10
default.search.maxDocuments=500
default.search.maxInstanceOfDocument=5
default.save.maxPages=20
default.discover.maxrows=100
default.documents.cachesize=5
default.imageSize=1048576
```

The following table explains each property:


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Table 3: Understanding mobi.properties

| Property | Description | Default Value |
|---|---|---|
| default.corporateCategory | Specifies a corporate category for documents accessed via mobile. BI documents assigned to this category are considered to be "mobile ready" documents. Mobile users can access the BI documents assigned to this category using an SAP BusinessObjects Mobile application on iOS, Blackberry or Android devices. | Mobile |
| default.personalCategory | Specifies a personal category for BI documents. Documents assigned to this category are personal to the user and cannot be accessed by other mobile users. If there is more than one category name, specify the values, separating each with a comma. | Mobile |
| default.category.mobileDesigned | Specifies a category for documents specifically designed for the mobile application. BI documents assigned to this category are displayed on the mobile device according to the Page layout model.<br>**Note**<br>For more information on the Page layout and card layout models of display, refer to the *Mobile BI Report Designer's Guide* posted on http://help.sap.com/bomobileios | MobileDesigned |
| default.category.secure | Specifies a secure category. BI documents assigned to this category cannot be downloaded to user's mobile device. They can only be viewed on the device. | Confidential |
| default.category.featured | Specifies a category for featured or special BI documents. BI documents assigned to this category are automatically downloaded to user's mobile device when he/she connects to the Mobile server using the SAP BusinessObjects Mobile application on the device. | Featured |
| default.search.resultsPerPage | Specifies the number of search results to be displayed per page on the mobile device. | 10 |
| default.search.maxDocuments | Specifies the maximum number of documents to be displayed in search results when performing a search. | 500 |
| default.documents.cachesize | Specifies the number of documents that can be cached by the user per user session. | 5 |


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

| Property | Description | Default Value |
| --- | --- | --- |
| default.imageSize | Specifies the maximum size (in bytes) for an image that is displayed in the SAP BI app on mobile device. | 1048576 |

### Note

1. Properties with string values are case sensitive.
2. Once defined in mobi.properties, the mobile categories must be created in the BI LaunchPad and BI documents must be assigned to them based on requirements.
3. The "mobile", "featured" and "secure" categories also support sub-categories. In the BI LaunchPad, BI documents assigned to sub-categories of these categories carry the same property as those assigned to the root categories. However, note that in the mobi.properties file, you can only define the root category names.
4. The properties that are marked for internal use in the default configuration of the mobi.properties file must not be modified for their values.

## Configuration in clientsettings.properties

The following is a typical default configuration of the `clientsettings.properties` file:

```
savePassword=false

offlineStorage=false

offlineStorage.ttl=365

offlineStorage.appPwd=true
```

The following table describes each client setting:

| Feature (Client Setting) | Description | Default value |
| --- | --- | --- |
| savePassword | • If the value is 'true', the option to save connection password is enabled in the application by default. (Users can disable it when creating a server connection using the application.)<br>• If the value is 'false', the option to save connection password is disabled in the application by default. | false |
| offlineStorage | • If the value is 'true', users can download BI documents from the mobile server once they have added the server connection.<br>• If the value is 'false', users cannot download BI documents from the server. They can only view BI documents in the online mode. | false |
| offlineStorage.ttl | This setting specifies the time (in days) after which the downloaded BI content expires and is automatically removed from the user's device memory. | 365 |


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

| Feature (Client Setting) | Description | Default value |
| --- | --- | --- |
| offlineStorage.appPwd | • If the value is 'true', the application prompts users to create an application password when adding a connection, for protection of offline content (downloaded BI documents).<br>• If the value is 'false', the application prompts does not prompt users to create an application password when adding server connections. | true |

You can add the following features to the file if you need to customize some of these based on your requirements:

> **Note**
>
> The description of these client settings is available in the chapter *Customizing the Application Functionality* in the *Developer's Guide* for iOS available at http://help.sap.com/bomobileios, and the *Developer's Guide* for Android available at http://help.sap.com/bomobileandroid

- `feature.email.enabled`
- `feature.collaboration.enabled`
- `feature.annotation.enabled`
- `feature.streamwork.enabled`
- `feature.jam.enabled`
- `feature.jam.url`
- `feature.jam.consumer.key`
- `feature.jam.consumer.secret`
- `feature.jam.callback.urlverb`
- `feature.help.enabled`
- `feature.help.url`
- `feature.help.video.enabled`
- `feature.help.video.playlistfeed`
- `feature.webi.refresh.enabled`
- `feature.webi.reportTitle.enabled`
- `feature.rel.legacy.mode`
- `feature.webi.palette.enabled`
- `feature.dashboard.sup.enabled`
- `feature.qrcode.enabled`
- `feature.show.samples.enabled`
- `feature.webi.personal.view.update.enabled`
- `feature.home.doc.person.enabled`
- `feature.info.doc.person.enabled`
- `feature.notification.polling.interval`
- `feature.autoupdate.enabled`
- `feature.dashboards.prefer.cache.enabled`

For a description of the properties in the `sup.properties`, `sso.properties` and `authscheme.properties` files, see the related topics of this chapter.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## Configuration in clientsettings.properties for push notification

| Feature (Client Setting) | Description | Default value |
|---|---|---|
| `Feature.Push.Notification` | This is a global notification parameter. To enable or disable push notification, admin has to explicitly configure this parameter at SAP BusinessObjects Mobile application object, in the Central Management Console (CMC). This property configuration must be set in the clientSettings of this object. | false |
| `Feature.Push.Post.Server.URL` | This is a POST server URL parameter. To make the push notification work, admin must configure this parameter. From APS mobile server, notification information gets posted to this URL, using this information the mobile server send information to the global port, for example: Apple Push Notifications (IOS), Google Could Messaging (android). | NULL<br>Example: http://<host_name>:PORT/MobileBIService/push |
| `Feature.Push.Inbox.Notification` | This is an optional configuration parameter for enabling or disabling Inbox notification. | true |
| `Feature.Push.DocUpdate.Notification` | This is an optional configuration parameter for enabling or disabling document update notification. | true |
| `Feature.Push.Polling.Interval` | This is an interval at which Adaptive Processing Server (APS) polls the Central Management System (CMS) repository to check for any updates available. This is an optional parameter. | `10 min` |
| `Feature.Push.Expiry.Interval` | This is an optional parameter to be configured by the administrator. This is the time interval at which Adaptive Processing Server (APS) considers the connection as idle or expired. Any connections, which have not been accessed during this time period gets cleaned up from the backend.<br>When user logs in the next time, notification related metadata are sent again to the APS and hence the data is restored at APS and user starts getting notification. | `30 days` |
| `Feature.Push.Broadcast.Notification` | This is an optional configuration parameter for enabling or disabling broadcase notification. | true |
| `Feature.Push.Post.HTTPSServer.CertParam` | This parameter is used to configure Java Key Store password in case of uses SSL based Mobile Server deployment. | changeit |

## Related Information

Connecting to the SAP Mobility Platform (SMP) [page 33]
Configuring Single Sign On (SSO) in SMP Environment [page 34]


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 5.1 Using the Central Management Console (CMC) For Mobile Server Configuration

### Context

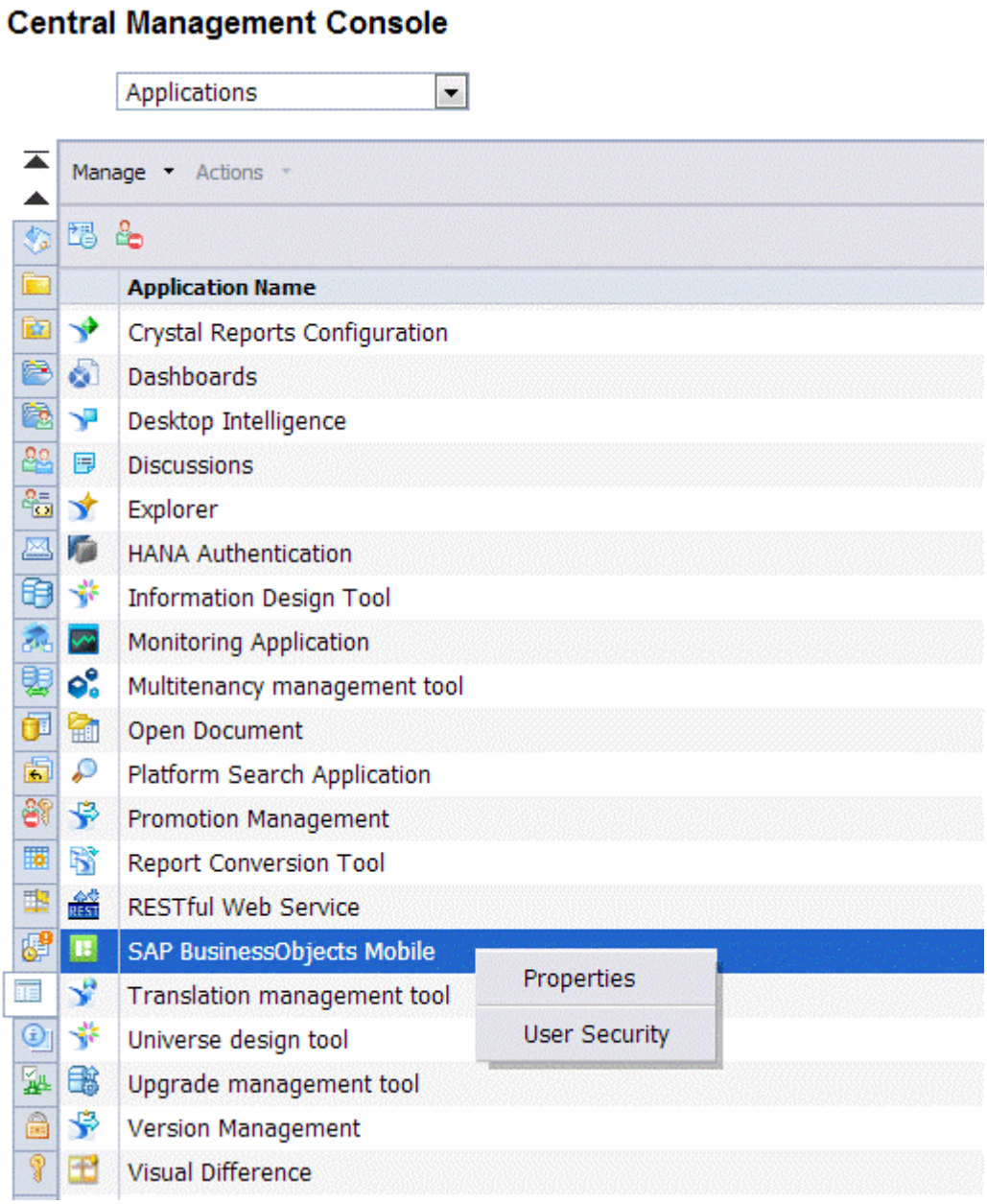
You can choose to customize the mobile server properties using the Central Management Console (CMC). CMC is the administrative console available on the BI platform.

To configure the Mobile server using the CMC, perform the following steps:

### Procedure

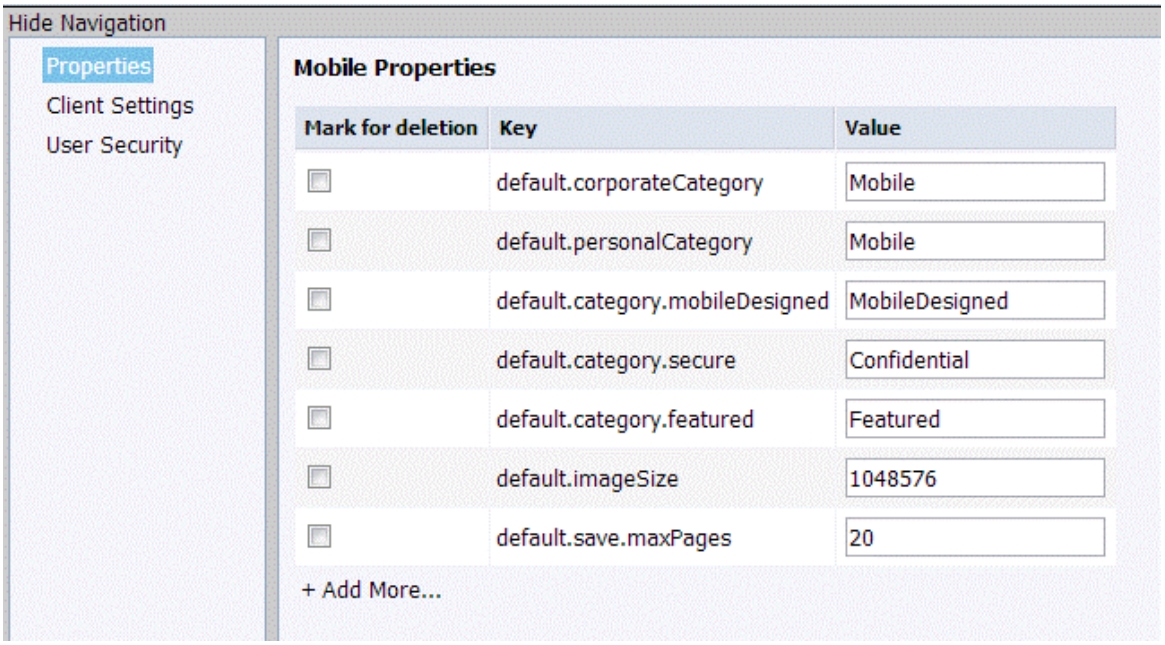
1. Log on to your BusinessObjects Enterprise (BOE)-> *Central Management Console* (CMC) application.
2. Select *Applications*.
3. Right click on *SAP BusinessObjects Mobile* and select *Properties* as shown in the below figure.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

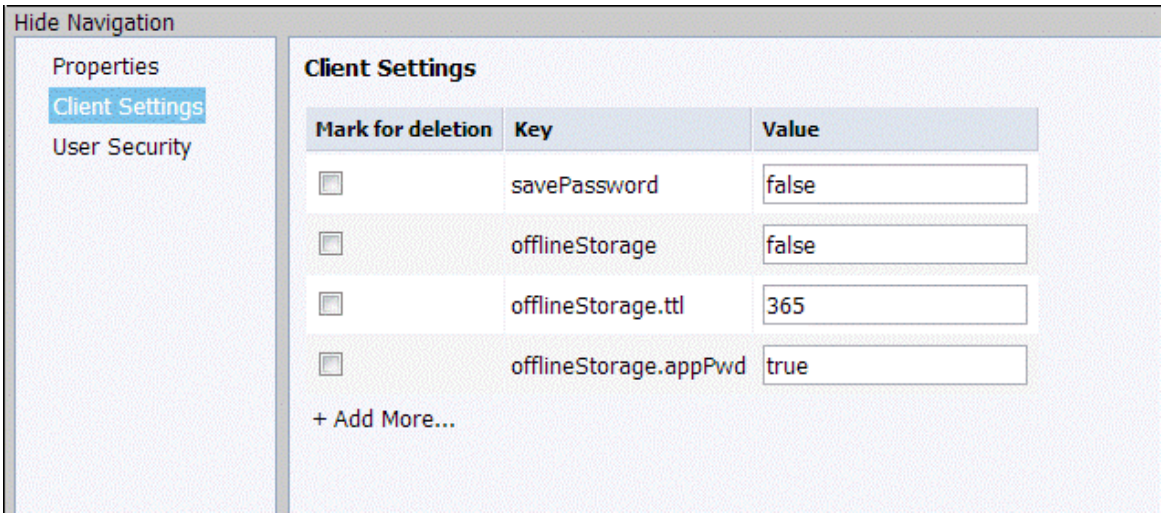



4. In the "Mobile Properties" window, select the required option in the left panel:
   - *Properties*: Select this option to customize the mobile server properties:


© 2016 SAP SE or an SAP affiliate company. All rights reserved.




- *Client Settings*: Select this option to customize the client settings:




5. Save the new values and exit from the CMC.

## 5.2 Push Notification

This is a functionality where server notifies (push) the mobile users for any updates. For example, when you receive a message to your Inbox, you are notified through a message on the mobile device (connected or not).

The benefits of this feature is that, this enables mobile users to receive notifications even when user session is not active or when application is not running on the mobile.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Following are the types of push notification supported in this release:

- BI Inbox
- Document Update
- Broadcast

> **Note**
>
> This feature can only be used on the SAP BusinessObjects Mobile 6.3 and above (Mobile Client).

For more information, watch Push Notification SAP BusinessObjects Mobile 6.3 Business Intelligence 4.2

## 5.2.1 BI Inbox Notification

When you receive a document in your BI inbox, you are notified through a message on your mobile device.

## 5.2.2 Document Update Notification

If the documents that you have downloaded on your mobile device, get modified or a new instance of it is created, you receive this notification..

## 5.2.3 Broadcast Notification

The SAP Business Intelligence Platform (BIP) has provided a new functionality known as broadcast notification, where the administrator can broadcast messages to a selected group of users. If you are one among the group of users, you receive broadcast notifications on your mobile device.

For more information, see **Configuration in clientsettings.properties for push notification** in Configuring MobileBIService (Mobile Server) [page 16]

## 5.2.4 Administrator Configuration

**Prerequisites:**

Mobile server sends notification information to Apple Push Notification Server (APNS) which in turn sends the notification to relevant mobile devices. The APNS port: "`gateway.push.apple.com, port 2195`" is the global port (provided by Apple) that must be open for the mobile server to get connected so as to send the notification.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

### Sample Code

To test if the APNS port is open or accessible, execute the following command on the terminal in the machine where mobile server is deployed.

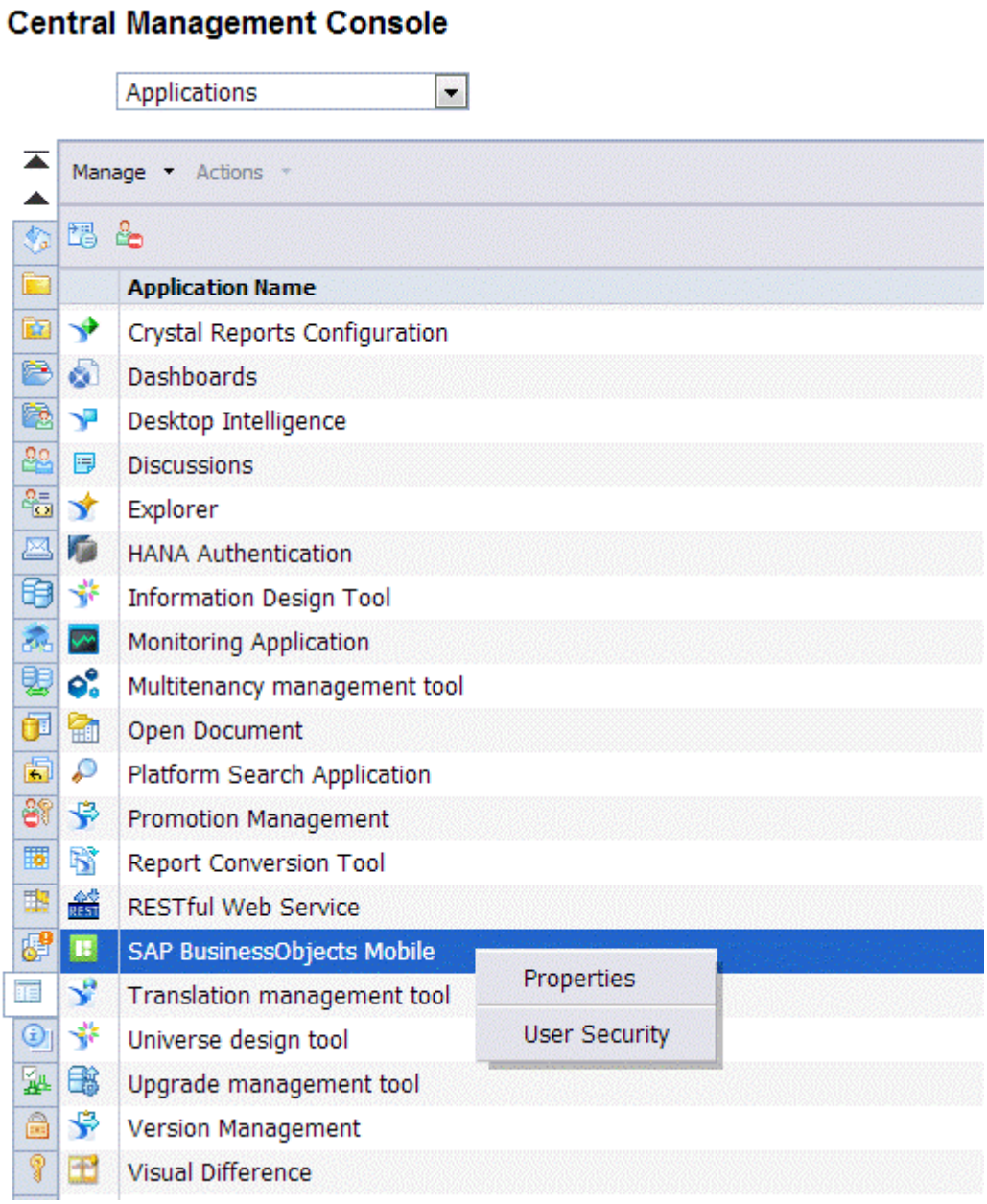
```
$ telnet gateway.push.apple.com 2195
Trying 17.110.226.155...
Connected to gateway.push-apple.com.akadns.net.
Escape character is '^]'.
```

## 5.2.4.1 Enabling Push Notification Feature

### Procedure

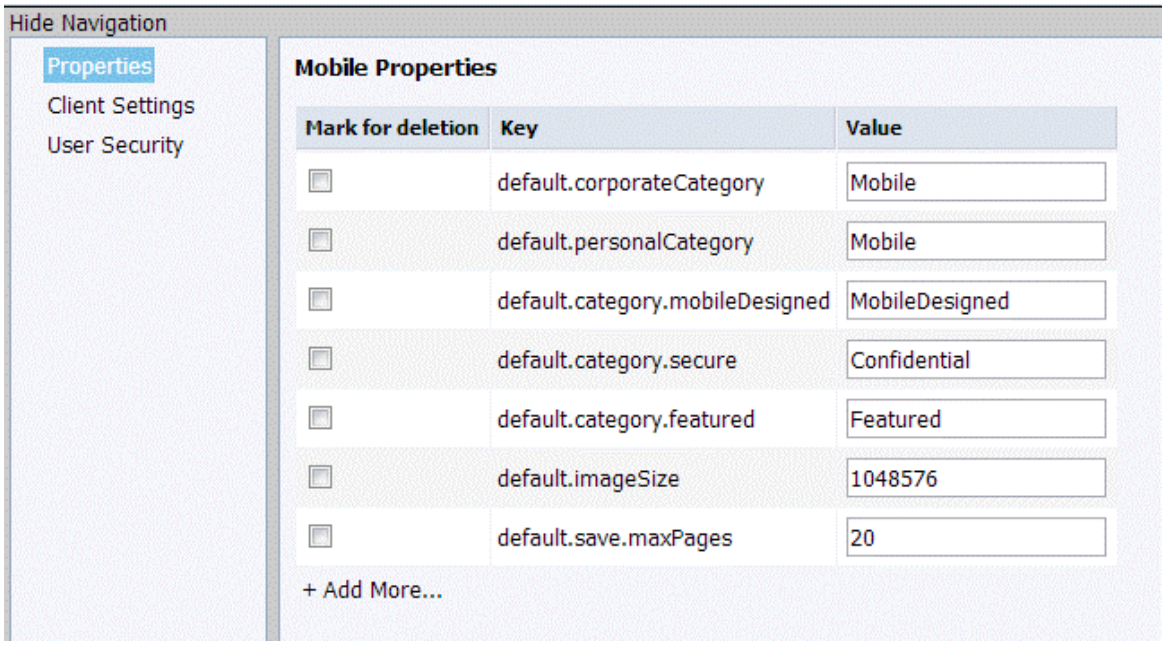
1. Deploy the `MobileBI Service` WAR file.
2. Ensure that the APNS port is open and also accessible from the machine where mobile server is deployed. For more information on how to test if the port is open, see *Administrator Configuration* section under *Push Notification* main section.
3. Log on to BusinessObjects Enterprise (BOE) > Central Management Console (CMC) application.
4. Select *Applications*.
5. Right click on *SAP BusinessObjects Mobile* and select *Properties* as shown in the below figure.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.




6. In the *Mobile Properties* window, select the required option in the left panel:
   - *Properties*: Select this option to customize the mobile server properties.

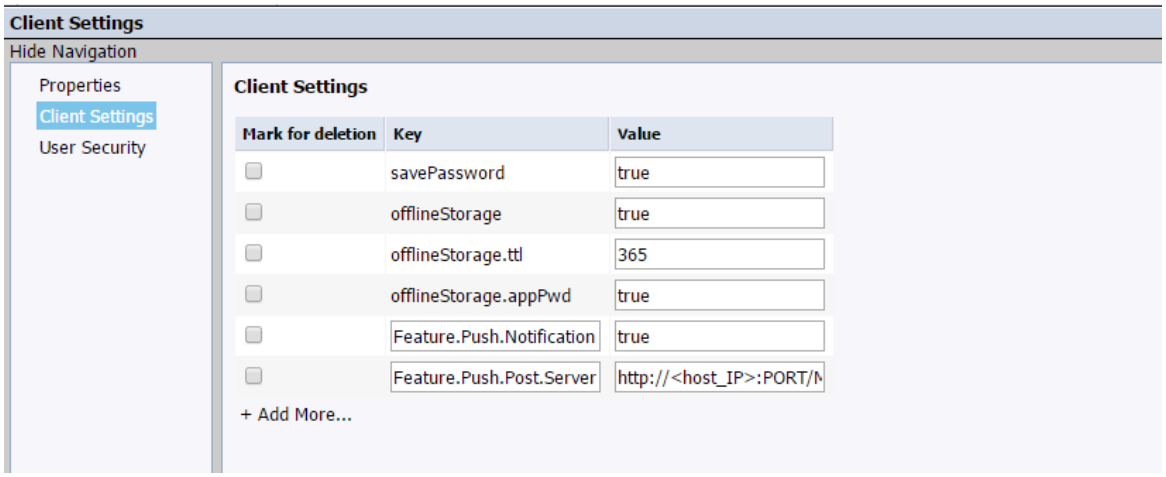

© 2016 SAP SE or an SAP affiliate company. All rights reserved.




- *Client Settings*: Select this option to customize the client settings.
  Add the following two new properties and their values in the *Client Settings* window, as shown in the figure:

  Table 4:

| Property Name | Value |
|---|---|
| `Feature.Push.Notification` | `true` |
| `Feature.Push.Post.Server.URL` | `http://<host_IP>:PORT/MobileBIService/push` |





© 2016 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> - `<Host_IP>` is the address of the service where `MobileBIService` is deployed.
> - The APS must be restarted when administrator changes the following properties:
>   - `Feature.Push.Notification`
>   - `Feature.Push.Polling.Interval`
> - There are other optional parameters that you can configure, refer *ClientSetting.configuration for push notification feature* section under *Configuring MobileBIService (Mobile Server)* main section .

7. Choose *Save* .

   Now, you have enabled push notification service on your mobile device.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 6 Configuring MOBIServer (Configuration Server)

## Context

Mobile users can add connections in the SAP BusinessObjects Mobile application on their devices in the following ways:

- Create connections manually using the application settings
- Add connections using the SAP BI URLs provided by the administrator
- Import connections from the mobile Configuration server

To enable users to import server connections to the application on their devices, you need to configure the Configuration server as described below.

## Procedure

1. Access the **server.properties** file from the following location: `<WebApp root>\MOBIServer\WEB-INF\config\default`, where `<WebAppsROOT>` is the folder on your specific application server, for example `C:\Program Files\Apache Software Foundation\Tomcat 6.0`
2. Copy `server.properties` from the `default` folder, create a folder named `custom` within <WebApp root>\MOBIServer\WEB-INF\config\, and paste the file to the `custom` folder.
3. Open the `server.properties` file in the custom folder, and add the line *mobi.connections*.

   **Tip**

   The mobile connections in the list are identified by mobi.connections values. For example, mobi.connections=connection1, connection2, connection3, means that three Mobile server connections are configured.

4. For each mobile connection, enter a value for its properties. The below table describes the properties:

   Table 5: Parameters for Defining Connections on the Configuration server

| Parameter | Name in server.properties | Basic | SSO | SUP | SMP | Possible Values |
|---|---|---|---|---|---|---|
| Name of connection | DisplayName | Y | | | | Any string value |


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

| Parameter | Name in server.properties | Basic | SSO | SUP | SMP | Possible Values |
|---|---|---|---|---|---|---|
| Type of connection | BOBJ_MOBILE_CONNECTION_TYPE_STRING | Y | | | | ○ "BOESMP" for SUP Rest Connection<br>○ "SUP" for SUP Legacy Connection<br>○ Unspecified value implies a basic BOE connection by default |
| CMS name or cluster | BOBJ_MOBILE_CMS | Y | | | | The CMS value entered on the connection screen of the mobile application. It can be IP, Qualified name or cluster name (@abc) |
| Mobile Server or SUP/SMP server URL | ○ BOBJ_MOBILE_URL (for Mobile Server)<br>○ BOBJ_MOBILE_SUP_SERVER (for SUP Server) | Y | | | | http://<IP address of the server>:port |
| Authentication Type | BOBJ_MOBILE_AUTH_METHOD | Y | | | | secEnterprise, secLDAP, secSAPR3, secWINAD |
| Is it an SSO connection? | BOBJ_MOBILE_SSO_ENABLED | | Y | | | 'true', 'false' |
| Type of SSO | BOBJ_MOBILE_SSO_TYPE | | Y | | | X509Certificate, SSO2COOKIE, SITEMINDER_BASIC, TRUSTED_AUTH_Basic, TRUSTED_AUTH_FORM, SSO_Form, SSO2COOKIE_QueryString |
| If X509 certificates are used, how are they configured | BOBJ_MOBILE_CERTIFICATE_REQUIRED_FOR_NETWORK | | Y | | | CertificateMandatory, CertificateOptional |
| URL to provide SSO2COOKIE | BOBJ_MOBILE_SSO_QUERY_URL | | Y | | | |
| Form that generates SSO2COOKIE | BOBJ_MOBILE_SSO_FORM_URL | | Y | | | |
| SSO cookie name (if other than the standard) | BOBJ_MOBILE_SSO_COOKIE_NAME | | Y | | | |
| SAP R3 system (in case of SSO) | BOBJ_MOBILE_SSO_SAP_SYSTEM | | Y | | | ABC^200, XYZ^100 etc. |
| SUP Farm ID | BOBJ_MOBILE_SUP_FARM_ID | | | Y | | |
| SUP/SMP security configuration name | BOBJ_MOBILE_SUP_SECURITY_CONFIG_NAME | | | Y | Y | |
| SUP port | BOBJ_MOBILE_SUP_PORT | | | Y | | |
| SUP/SMP application ID | BOBJ_MOBILE_SUP_APP_ID | | | Y | Y | |


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

| Parameter | Name in server.properties | Basic | SSO | SUP | SMP | Possible Values |
|---|---|---|---|---|---|---|
| SMP proxy connection name | BOBJ_MOBILE_SUP_PROXY_CONN | | | Y | | |

> **Note**
>
> The following policy line exists by default in server.properties:
>
> mobi.policy.APP_URL_LAUNCH_ENABLED=true
>
> The server policies are identified by mobi.policy.<policy name> = <policy value>.
>
> At the moment, only 1 policy (APP_URL_LAUNCH_ENABLED) is defined on the Mobile server, and it works for iOS and Android client applications. This policy ensures that `sapbi://` URLs created for sharing server connections and BI documents work in the SAP BusinessObjects Mobile application for iOS and Android. If this policy value is set to 'false', SAP BI URLs do not work in the application on devices.
>
> > **Tip**
> >
> > For more information on SAP BI URLs, refer to the *Administrator's Guide* available onhttp://help.sap.com/bomobileios

5. *Save* the properties file and deploy the MOBIServer.war again.
6. Execute the following URL to verify the configured properties:

   `http://<server>:<port>/MOBIServer/MobiConfigurationServlet?RequestType=ServerList`


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 7 Connecting to the SAP Mobility Platform (SMP)

To enable users of the mobile client applications to connect to the SAP BusinessObjects Mobile server using the SAP Mobility Platform (SMP), you need to perform certain configuration steps. These include the following:

1. Install SMP on a machine on your network.
2. Configure SMP for use with the SAP BusinessObjects Mobile server.
3. Configure the SAP BusinessObjects Mobile server to connect to the SMP server.

As of the current application release, the SAP BusinessObjects Mobile BI landscape supports two types of SMP connections:

- **SMP BOE Legacy** (IMO-based traditional connection)
  The following BI content types are supported for this connection type:
  - Web Intelligence (HTML and as PDFs)
  - Crystal Reports (as PDFs)
  - Dashboards
  - Explorer (information spaces and exploration views)
- **SMP BOE** (REST-based new and **recommended** connection)
  The following BI content types are supported for this connection type:
  - Web Intelligence (HTML and as PDFs)
  - Crystal Reports (HTML and as PDFs)
  - Dashboards
  - Explorer (information spaces and exploration views)
  - Analysis applications (created using the Design Studio)
  - Hyperlink objects

### Note

1. You can use REST-based connections (connection type: "SMP BOE Connection") only if your SAP Mobility Platform (SMP) version is:
   - SUP 2.2, Support Package 4, Patch 10391 or above
   - SUP 2.2, Support Package 5, Patch 10397 or above
   - SUP 2.3, Support Package 3, Patch 10398 or above
2. You can add multiple REST-based SMP connections in the application on an iOS device, but only a single IMO-based (legacy) SMP connection at a time.
3. **Do not add a combination of IMO- and REST-based connections** in the application, as this may cause issues in rendering HTML content in the application.
4. All configuration details in the sub-topics of this chapter likewise apply to both IMO- and REST-based SMP connections. However, **if you want to configure an SMP REST connection, you need to perform several additional steps of URL white-listing** while configuring SMP for use with the SAP BusinessObjects Mobile server. These steps are clearly listed in the second sub-chapter (*Configuring SMP for use with the SAP BusinessObjects Mobile server*).


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 7.1 Configuring Single Sign On (SSO) in SMP Environment

### Context

To configure SSO in SMP environment, ensure that you have:

1. The SAP BusinessObjects BI platform configured for X509 SSO authentication.
2. The SAP Mobility Platform (version 2.2.4 and above) configured for X509 authentication.

You need to configure the SMP server, MobileBIService (Mobile server) and MOBIServer (Configuration server) for SSO. The sub-topics explain how to perform the SSO configuration.

## 7.2 Installing the SAP Mobility Platform (SMP)

For detailed information on installing the SAP Mobility Platform, access http://infocenter.sybase.com/help/index.jsp?docset=/com.sybase.infocenter.pubs.docset-SUP-2.1.1/doc/html/title.html, and navigate to *Sybase Unwired Platform 2.1 ESD #1* > *Installation Guide for Runtime*.

## 7.3 Configuring SMP for Use With the Mobile Server

### Context

To configure SMP for use with the mobile server, you need to perform the following sub-tasks:

### Procedure

1. Create a Security configuration.
2. Create an application.
3. Create an application connection template.
4. White-list the application end-point URL.

   The sub-topics of this topic describe the above sub-tasks.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 7.3.1 Creating a Security Configuration

### Context

To connect to a Mobile server, you need to create a security configuration. To do this, perform the following steps:

### Procedure

1. On the SMP server, launch the *Mobility Server Cluster Management View* (SAP Control Center).
2. In the *Mobility Platform Cluster* panel that appears on the left, select *Security*.
3. Choose *New* in the *General* tab in the panel on the right.
   The *Create Security Configuration* window appears.
4. Enter a name for the new Security Configuration (for example `<MobiSec>`) and choose *OK*.
   The new security configuration appears in the *Security* folder in the panel on the left.

   > **Note**
   >
   > Make a note of the Security Configuration name. You need this name to configure the SMP connection on the client application.

5. Select the new security configuration in the *Mobility Platform Cluster* panel.
6. Select the *Authentication* tab in the right panel and choose *New*.
   The *Add Provider* window appears.
7. In the Authentication Provider dropdown list, select *HttpAuthenticationLoginModule*.
8. In the properties that appear below the dropdown list, enter a URL with the following format:`http://<Mobile BI Server>/MobileBIService/SUP/VerifyUser/<Security Config name>` (For example, `http://10.10.10.10:8080/MobileBIService/SUP/VerifyUser/MobiSec`)
9. Choose OK to close the *Add Provider* window.
   The authentication provider you have added appears in the Authentication tab of the new Security Configuration.
10. Go to the General tab and choose *Validate*. This allows you to validate the changes to the security configuration before applying them to the SMP server. Then choose *Apply*.
    The security configuration you have added is saved on the Mobility platform server.

    > **Tip**
    >
    > You can connect to multiple Mobile servers by creating a security configuration for each one.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 7.3.2 Creating an Application

### Procedure

1. On the SMP server machine, launch the *Mobility Server Cluster Management View*.
2. In the *Mobility Platform Cluster* panel on the left, select *Applications*.
3. Choose *New* in the *Applications* tab in the panel on the right
   The *Application Creation* window appears.
4. In the Application ID field, enter MobiApp.
5. In the Display name field, enter a display name.
6. Select the security configuration from the dropdown list (`<MobiSec>` configured in step one).
7. Choose *Finish* to complete the procedure.

## 7.3.3 Creating an Application Connection Template

### Context

To create a connection between your Mobile server and the Application ID (MobiApp), you need to create an application connection template.

> **Note**
>
> You can either create a (new) application connection template or *edit* the existing application connection template that is automatically created when you create the application (in the last procedure).

To create an application connection template, perform the following steps:

### Procedure

1. In the *Mobility Platform Cluster* panel on the left, choose *Applications*.
2. Choose *Application Connection Template*.
3. Choose *New*.
   The Template popup appears.
4. In the *Template name* field, enter the name for the template.
5. In the *Base template* field, choose Default.
6. Choose *Application Settings*, and perform the following sub-steps:
   a. In the *Application Identifier* field, choose MobiApp as the value.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

b. In the *Domain* field, choose Default as the value.
c. In the *Security Configuration* field, choose the security configuration you want to connect to.

   Since you are creating a new application connection template, the *Security Configuration* should be different from the value (Mobisec) configured while creating the application. If the Application identifier (application ID), the Domain and the Security Configuration values that you enter in this step are the same as the ones you specified while creating the application, the system does not allow you to proceed.

7. Select *Proxy*, in the *Application Endpoint*, enter the URL of the Mobile Server provided by your administrator. The value should have the following format: `http://<Mobile BI Server>/MobileBIService/MessageHandlerServlet` For example, `http://10.10.10.10:8080/MobileBIService/MessageHandlerServlet`
8. Choose *Ok*.

## 7.3.4 Whitelisting the Application Endpoint URL for an SMP BOE Legacy connection

### Context

This section applies to you if you are using the SMP server version 2.2. If your SMP server version is 2.2, you need to "white-list" the application end point URL.

To white-list a URL, perform the following steps

### Procedure

1. After creating the application connection template, choose *Domains*> *Default*>*Connections* in the "Mobility Server Cluster Management View".
2. In the *Manage Connections* section that appears in the Connections tab on the right of the window, choose *New*.
3. The *Add Connection Pool* window appears.
4. Perform the following sub-steps in the *Add Connection Pool* window:
   a. Enter a name for the Connection pool name.
   b. Select "Proxy" for the Connection pool type.
   c. Specify the Application Endpoint URL in the Address field and choose *Ok*.

      The value of Address (Application Endpoint URL) should have the following format: `http://<Mobile BI Server>/MobileBIService`


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 7.3.5 Whitelisting the Application Endpoint URL for a REST (SMP BOE) connection

### Context

This section applies to you if you are using the SMP server version 2.2. If your SMP server version is 2.2, you need to "white-list" the application end point URL.

To white-list a URL, perform the following steps

### Procedure

1. After creating the application connection template, choose *Domains*> *Default*>*Connections* in the "Mobility Server Cluster Management View".
2. In the *Manage Connections* section that appears in the Connections tab on the right of the window, choose *New*.
   The *Add Connection Pool* window appears.
3. Perform the following sub-steps in the *Add Connection Pool* window:
   a. Enter a name for the Connection pool name.
   b. Select "Proxy" for the Connection pool type.
   c. Specify the Application Endpoint URL in the Address field and choose *Ok*.

      The value of Address (Application Endpoint URL) should have the following format: `http://<Mobile BI Server>/MobileBIService`
4. In the panel on the left, select *Security* in the default domain, and choose *Assign*.
   The list of security configurations that have not been assigned to the default domain yet appear on the *Assign Security Configurations* screen.
5. Select the required security configuration, and choose *OK*.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 7.4 Configuring Mobile Server to Connect to the SMP Server

### Context

To configure the SAP BusinessObjects Mobile server to connect to the Sybase Unwired Platform, perform the following steps:

### Procedure

1. Deploy the `MobileBIService.war` file (version 4.0.3/ 4.0.2.13 or later) on your Web application server.
2. Locate the `WEB_INF\sup.properties` file.

   > **Note**
   >
   > The file location of `sup.properties` is the same as for `mobi.properties`.

3. Insert the following lines in the file: `MobiSec.cms=11.22.33.44 MobiSec.auth=secEnterprise`

   > **Note**
   >
   > - You will notice that these lines have already been placed as comments in the `sup.properties` file. You can change the lines from comments to code and update the values of the parameters.
   > - You can connect to multiple CMS by providing the CMS address along with the security configuration in the `sup.properties`.
   >   For Example:
   >
   >   ```
   >   MobiSec_another.cms=11.42.44.55
   >   MobiSec_another.auth=secEnterprise
   >   MobiSec_another_another.cms=11.66.22.77
   >   MobiSec_another_another.auth=secEnterprise
   >   ```
   >
   > - Note that MobiSec is the name that you specified for the security configuration setting when you added it to the SUP server with the Sybase Control Center.
   > - Possible values for authentication are: `<secEnterprise>`, `<secLDAP>`, `<secWinAD>`, `<secSAPR3>`. You also need to make sure that the specified IP address of the CMS is correct.

   The browser displays an authentication dialog. If you enter a valid user name and password for the CMS mentioned in the configuration, you should see an empty page. (MobiSec is the security configuration name in this particular example. Change it to the name that you used in your settings.)


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 8 Configuring Single Sign On (SSO) in SMP Environment

## Context

To configure SSO in SMP environment, ensure that you have:

1. The SAP BusinessObjects BI platform configured for X509 SSO authentication.
2. The SAP Mobility Platform (version 2.2.4 and above) configured for X509 authentication.

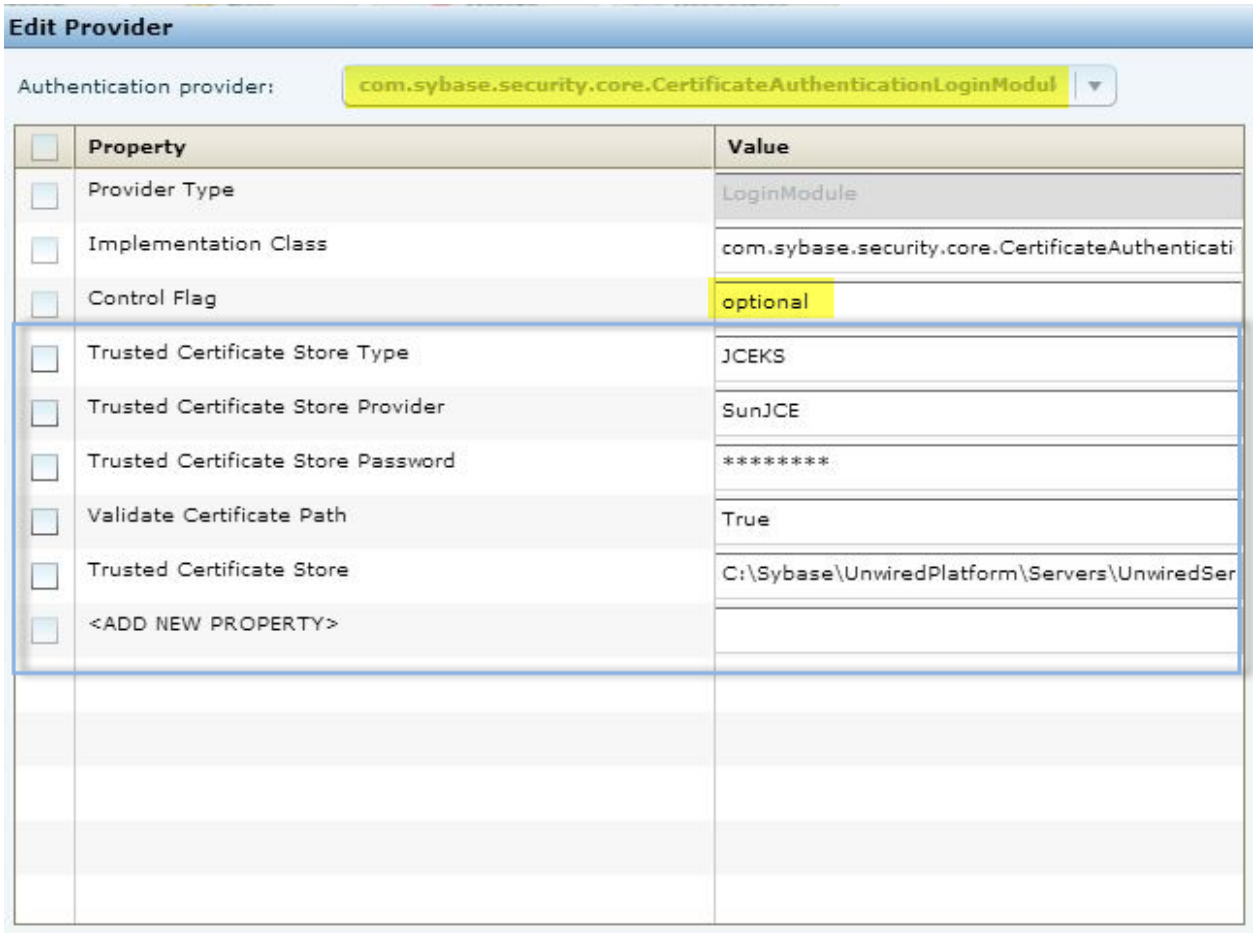
You need to configure the SMP server, MobileBIService (Mobile server) and MOBIServer (Configuration server) for SSO. The sub-topics explain how to perform the SSO configuration.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 8.1 Configuring the SMP Server for X509 Authentication-Based SSO

### Context

Configure the SMP server for use with the SAP BusinessObjects Mobile server as described in an earlier chapter, with only the following **difference in step 7 of creating a security configuration**:




- In the *Authentication Provider* drop-down, instead of selecting HttpAuthenticationLoginModule, select CertificateAuthenticationLoginModuleand set the control flag as "Optional". Then add the following properties:

```
Trusted Certificate Store Type=JCEKS
Trusted Certificate Store Provider=SunJCE
Trusted Certificate Store Password=******
Validate Certificate Path=”True”
Trusted Certificate Store=DREVE:\Sybase\UnwiredPlatform\Servers\UnwiredServer
\Repository\Security
```


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 8.2 Configuring MobileBIService (Mobile Server) for SSO Using X509 Authentication

### Context

You need to modify the `authscheme.properties` and `sso.properties` files on the Mobile server.

> **Note**
>
> 1. By default, these properties files are deployed at the following location on the server machine: `<WebAppsROOT>\webapps\MobileBIService\WEB-INF\config\default`, where <WebAppsROOT> is the folder on your specific application server, for example `C:\Program Files\Apache Software Foundation\Tomcat 6.0`
> 2. We recommended that you back up these properties files before modifying them. Save the files in a custom folder, and then modify them. For example, `<WebAppsROOT>\webapps\MobileBIService\WEB-INF\config`**\custom**

### Procedure

1. Open the authscheme.properties file and un-comment the following line:
   `TRUST_X509=com.businessobjects.mobilebi.server.logon.impl.TrustedAuthX509`
2. Save and close the authscheme.properties file.
3. Open the `sso.properties` file and define your CMS alias with the properties for your SAP BusinessObjects back end (for SSO via trusted authentication).

   For this step, uncomment the lines and specify the required parameters as described in the following table:

| File (sso.properties) Parameter | Purpose | Example |
|---|---|---|
| `default.cms.identifier` | Specifies the default CMS ID | `default.cms.identifier = cms1` |
| `<id>.aliases` | Specifies the IP address/qualified name/alias for your CMS | `cms1.aliases = 10.X.X.X`<br>**Note**<br>You can pass the FQN of the SAP BusinessObjects back-end server as well. |
| `<id>.authentication.scheme` | Specifies the authentication scheme. | `<id>.authentication.scheme = cms1.authentication.scheme =TRUST` |


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

| File (sso.properties) Parameter | Purpose | Example |
|---|---|---|
| `<id>.trusted.auth.sharedsecret` | Specifies the secret key that is generated on the BI platform server for trusted authentication . | `cms1.trusted.auth.sharedsecret=<Shared secret key configured with Business Objects Backend>` |
| `<id>.trusted.auth.user.retrieval` | Specifies the mechanism of retrieving user ID. | `cms1.trusted.auth.user.retrieval=X509` |
| `<id>.product.locale` | Specifies the default product locale | `cms1.product.locale=en` |
| `<id>.preferred.viewing.locale` | Specifies the preferred viewing locale | `cms1.preferred.viewing.locale=en` |
| `<id>.authentication.type` | Specifies the authentication type (such as 'secLDAP'/ 'secWinAD'/ 'secEnterprise'/'secSAPR3') | `cms1.authentication.type=secEnterprise` |

4. Save and close the sso.properties file.

## 8.3 Configuring MOBIServer (Configuration Server) for SSO Using X509 Authentication

### Context

Users can add single sign-on (SSO) connections in the application only by importing connections from the configuration server. (Users cannot manually create them.) So that users can import SSO connections via X509 authentication in the application, you need to create the required connections on the mobile Configuration server. Connections on the configuration server are created by updating the `server.properties file` file.

To create connections on the Configuration server, perform the following steps:

### Procedure

1. Access the `server.properties file` available at `<WebAppsROOT>\webapps\MOBIServer\WEB-INF\config\default`

   Before modifying the properties file, it is recommended to take a back up of the existing file. Create a copy of the server.properties file in a custom folder (`<WebAppsROOT>\MobileBIService\WEB-INF\config\custom`) and then do your modifications.
2. Add (or modify the values of) the following lines in the file and save it:
   SUPSMP_X509.DisplayName:SUP_SSO_REST_X509
   SUPSMP_X509.BOBJ_MOBILE_CONNECTION_TYPE_STRING=BOESMP
   SUPSMP_X509.BOBJ_MOBILE_SUP_SERVER = https://10.208.107.23:8002
   SUPSMP_X509.BOBJ_MOBILE_SUP_PROXY_CONN =X509
   SUPSMP_X509.BOBJ_MOBILE_SUP_SECURITY_CONFIG_NAME =X509


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

SUPSMP_X509.BOBJ_MOBILE_SSO_ENABLED=true
SUPSMP_X509.BOBJ_MOBILE_SSO_TYPE:X509Certificate
SUPSMP_X509.BOBJ_MOBILE_CERTIFICATE_REQUIRED_FOR_NETWORK:CertificateMandatory

> **Note**
>
> 1. The following parameters are mandatory for specifying a single sign-on X509authentication-based connection:
>    - `BOBJ_MOBILE_SSO_ENABLED:true`
>    - `BOBJ_MOBILE_SSO_TYPE:X509Certificate`
> 2. To access Design Studio content (Analysis applications) while using the SAP BI application in a REST-based SMP environment, you need to have one of the following **SMP server versions**:
>    - SUP 2.2, Support Package 4, Patch 10391
>    - SUP 2.2, Support Package 5, Patch 10397
>    - SUP 2.3, Support Package 3, Patch 10398

## 8.4 Configuring Push Notification While using Trusted Form Based Authentication (SSO or Two Factor)

### Context

If your deployment supports trusted or form based authentication, you can perform the steps mentioned in this section to enable `/push` notification feature.

> **Note**
>
> The `/push` must not have authentication constraints. To exclude authentication challenge for `/push` inside `MobileBIService`, you must edit the `web.xml` file. The following is the procedure to edit the `web.xml` file.

### Procedure

1. Navigate to `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\MobileBIService\WEB-INF`.
2. Edit the `web.xml` by adding the following code at the end:


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

**Sample code that depicts "how to exclude authentication challenges for `\push` notification feature:**

Sample Code

```
<security-constraint>
    <web-resource-collection>
    <web-resource-name>Wildcard means whole app requires authentication</web-
resource-name>
    <url-pattern>/push</url-pattern>
// excludes authentication for '/push' (push notification)

<http-method>GET</http-method>
    <http-method>POST</http-method>
    </web-resource-collection>
</security-constraint>
<security-constraint>
    <web-resource-collection>
    <web-resource-name>Wildcard means whole app requires authentication</web-
resource-name>
    <url-pattern>/*</url-pattern>
// This enables authentication for all resources
    <http-method>GET</http-method>
    <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint>
    <role-name>BOE</role-name>
    </auth-constraint>
        <user-data-constraint>
        <!-- transport-guarantee can be CONFIDENTIAL, INTEGRAL, or NONE -->
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
</security-constraint>
    <login-config>
    <auth-method>FORM</auth-method>
    <form-login-config>
    <form-login-page>/login.html</form-login-page>
    <form-error-page>/login-failed.html</form-error-page>
    </form-login-config>
    </login-config>
```

## 8.5 Configuring Push Notification in SSL Scenarios

### Context

When you implement Single Sign On (SSO) or Two Factor authentication on mobile server using mandatory `x509` Certificate, the push notification does not work. This is because the the certificate authentication is enabled at application server level and not at URL level. Hence, when Adaptive Processing Server (APS) tries to post the data to `MobileBIService`, it receives authentication errors.

Work around:

As an administrator, for `x509` Certificate based set up on `MobileBIService`, perform the following steps:


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

### Procedure

1. Deploy `MobileBIService` on two separate machines.

   Machine 1: Configure Machine1 to perform user workflows such as, logon, listing, configuring notifications, sending device token and so on.

   Machine 2: Use Machine 2 only to POST notification from the APS to mobile service that is deployed on this machine. However, the POST from APS mobile service is not a user workflow, so you need not use `X509 certificate based 2-factor` or `SSO` authentication on this machine. You need to open an external `APNS` port from Machine 2.
2. Use the push POST URL of Machine 2 in the Central Management Console (CMC) against the property `Feature.Push.Post.Server.URL` to send the notifications. For example, use URL: http://machine2:port/MobileBiService/push to send notifications to the APNS.

## 8.5.1 X-509 One-Way Authentication

### Context

When you implement Single Sign On (SSO) or Two Factor authentication on mobile server using mandatory `x509` Certificate, the push notification does not work. This is because the the certificate authentication is enabled at application server level and not at URL level. Hence, when Adaptive Processing Server (APS) tries to post the data to `MobileBIService`, it receives authentication errors.

Work around:

As an administrator, for `x509` Certificate based set up on `MobileBIService`, perform the following steps:

### Procedure

1. Deploy `MobileBIService` on two separate machines.

   Machine 1: Configure Machine1 to perform user workflows such as, logon, listing, configuring notifications, sending device token and so on.

   Machine 2: Use Machine 2 only to POST notification from the APS to mobile service that is deployed on this machine. However, the POST from APS mobile service is not a user workflow, so you need not use `X509 certificate based 2-factor` or `SSO` authentication on this machine. You need to open an external `APNS` port from Machine 2.
2. Use the push POST URL of Machine 2 in the Central Management Console (CMC) against the property `Feature.Push.Post.Server.URL` to send the notifications. For example, use URL: http://machine2:port/MobileBiService/push to send notifications to the APNS.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 8.5.2 Password Setting for the Key Store

Java Key Store password can be configured using `Feature.Push.Post.HTTPSServer.CertParam` parameter in `SAP BusinessObject Mobile application` object under *Client Settings*.

For more information, see section *Using the Central Management Console (CMC) For Mobile Server Configuration* under *Configuring MobileBIService (Mobile Server)* main section.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 9 Configuring Kerberos in SSO Environment

Kerberos is an authentication mechanism in which passwords are not transmitted over the network. The server depends on a trusted ticket issued by a ticket granting server, which the client sends in the request from the client to the server.

In order to enable Kerberos-based authentication for the Mobile iOS application, a few steps need to be executed on both the iOS device and the Mobile server.

> **Note**
>
> - The BOE landscape should be configured for Kerberos-based Authentication.
> - Kerberos is not supported via SMP and SUP Connections.
> - If you are using Apache Tomcat 8.0.21, in `catalina.properties` add the parameter `org.apache.catalina.core.ApplicationContext .GET_RESOURCE_REQUIRE_SLASH = true`

## 9.1 Configuring the iOS Device

### Configuring the iOS Device

On iOS, Kerberos is controlled by a configuration profile, which guides iOS framework in handling Kerberos tickets. This profile can be installed from any MDM tool and should have a `.mobileconfig` extension. Given


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

below is a sample configuration, which indicates the values that you should update.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple/DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
  <dict>
   <key>PayloadDisplayName</key>
   <string>SSO Settings</string>
   <key>PayloadType</key>
   <string>com.apple.sso</string>
   <key>PayloadVersion</key>
   <integer>1</integer>
   <key>PayloadUUID</key>
   <string>d3fe4709-0cc6-4f51-afed-839c6ab1451c</string>
   <key>PayloadIdentifier</key>
   <string>com.sap.example.sso</string>
   <key>Name</key>
   <string>username@EXAMPLE.COM</string>
   <key>Kerberos</key>
   <dict>
    <key>PrincipalName</key>
    <string>username</string>
    <key>Realm</key>
    <string>EXAMPLE.COM</string>
    <key>URLPrefixMatches</key>
    <array>
     <string>https://example.com/</string>
     <string>https://example.com:443/</string>
    </array>
    <key>AppIdentifierMatches</key>
    <array>
     <string>com.apple.mobilesafari</string>
     <string>com.sap.*</string>
    </array>
   </dict>
  </dict>
 </array>
 <key>PayloadOrganization</key>
 <string>SAP</string>
 <key>PayloadDisplayName</key>
 <string>SSO for SAP</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
 <key>PayloadUUID</key>
 <string>f4544183-fc96-495f-a384-435cdb66e5b9</string>
 <key>PayloadIdentifier</key>
 <string>com.sap.example.sso.profile</string>
 <key>PayloadDescription</key>
 <string>SSO Configuration profile</string>
 <key>PayloadType</key>
 <string>Configuration</string>
</dict>
</plist>
```

The table below gives details of payload content.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Table 6: Payload content

| Parameter | Description |
|---|---|
| *PayloadDisplayName | Do not modify this string. |
| *PayloadType | Do not modify this string. |
| *PayloadVersion | Do not modify this string. |
| *PayloadUUID | This should be a unique ID which you can generate online. |
| *PayloadIdentifier | You should modify this to reflect your company domain. |
| *Name | Any name for the profile that you are creating. |
| *PrincipalName | The Kerberos login occurs with this winAD user name. |
| *Realm | This should be the Kerberos Realm. In case of Active Directory, an AD domain. |
| *URLPrefixMatches | iOS appends the service ticket to this URL. It can have multiple entries of which at least one should have the format: http://<FQDNof BOE>:<port where Mobile Server is deployed> FQDN: Fully Qualified Domain Name. |
| *AppIdentifierMatches | This is the list of applications eligible to use Kerberos Based Authentication. Do not modify this string. |
| *PayloadOrganization | Name of your organization. |
| *PayloadDisplayName | Name of this SSO payload. Here you can enter any string. |
| *PayloadVersion | Do not modify this string. |
| *PayloadUUID | This should be a unique Id which you can generate online. |
| *PayloadIdentifier | This should be modified to reflect your company domain. Example: com.<your company name>.mobi.sso.profile |
| *PayloadDescription | Description of payload profile. |
| *PayloadType | Do not modify this string. |


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 9.2 Configuring the Import Connection Server

### Configuring the Import Connection Server

Since Kerberos is an SSO connection, the following configuration should be maintained on the import connection server.

```
SSO_Kerberos.DisplayName:SSO_Kerberos
SSO_Kerberos.BOBJ_MOBILE_URL :< your mobile server URL>
SSO_Kerberos.BOBJ_MOBILE_CMS :< your CMS URL>
SSO_Kerberos.BOBJ_MOBILE_SSO_ENABLED: true
SSO_Kerberos.BOBJ_MOBILE_SSO_TYPE: kerberos
```

The following table gives the description of various parameters.

Table 7: Parameter table

| Parameter | Descrription |
|---|---|
| `SSO_Kerberos.DisplayName` | This string is the name of your connection. |
| `SSO_Kerberos.BOBJ_MOBILE_URL` | This is the mobile server URL. The URL here and the URL in the `URLPrefixMatches` of the iOS configuration profile must be the same. (URLs should be Fully Qualified Domain Name) |
| `SSO_Kerberos.BOBJ_MOBILE_CMS` | This should be the Fully Qualified Domain Name of CMS. |
| `SSO_Kerberos.BOBJ_MOBILE_SSO_ENABLED` | Retain this value as true. |
| `SSO_Kerberos.BOBJ_MOBILE_SSO_TYPE` | Retain this value as Kerberos. |

## 9.3 Configuring the Mobile server

### Configuring the Mobile Server

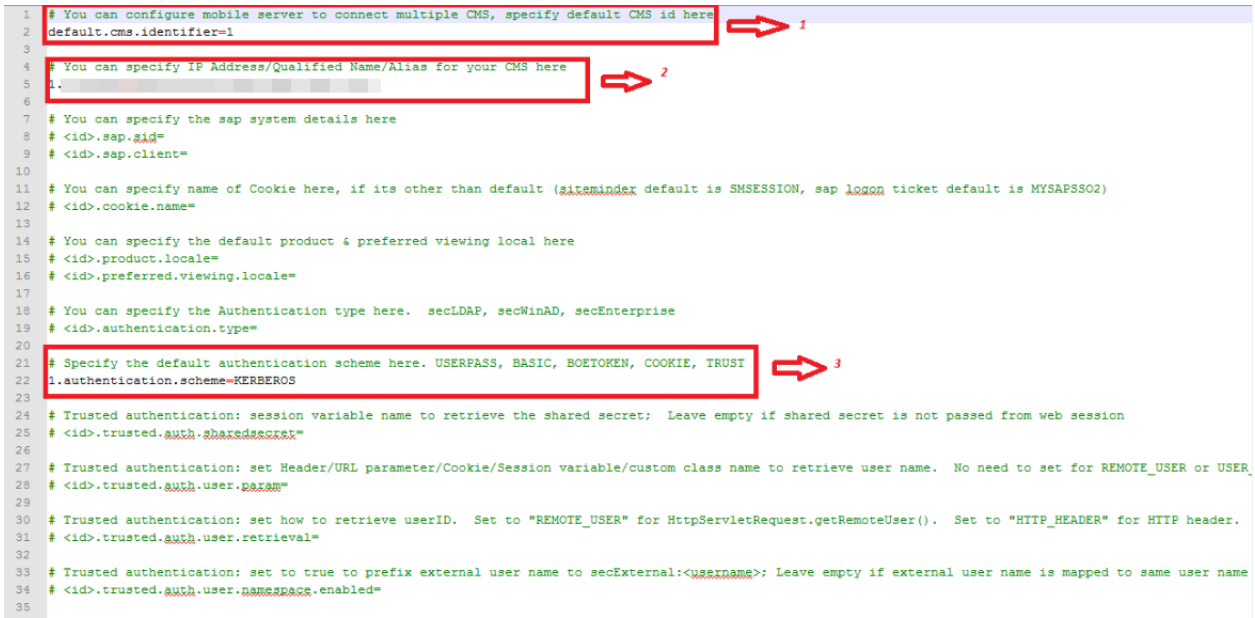
Mobile server must be enabled for Kerberos based authentication. Follow the steps as given below:

1. Stop Tomcat server
2. Modify sso.properties, authscheme.properties and web.xml
3. Clean Start tomcat server.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## Changes for sso.properties

Make the changes in sso.properties as indicated in the figure below.



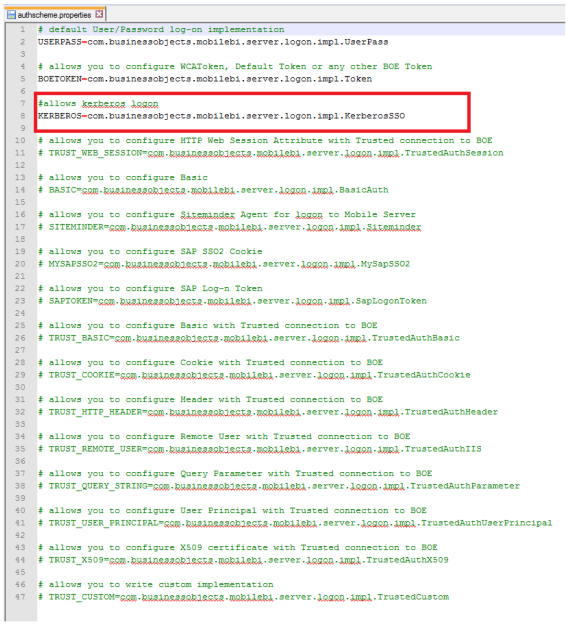

```
# You can configure mobile server to connect multiple CMS, specify default CMS id here
default.cms.identifier=1

# You can specify IP Address/Qualified Name/Alias for your CMS here
1.

# You can specify the sap system details here
# <id>.sap.sid=
# <id>.sap.client=

# You can specify name of Cookie here, if its other than default (siteminder default is SMSESSION, sap logon ticket default is MYSAPSSO2)
# <id>.cookie.name=

# You can specify the default product & preferred viewing local here
# <id>.product.locale=
# <id>.preferred.viewing.locale=

# You can specify the Authentication type here.  secLDAP, secWinAD, secEnterprise
# <id>.authentication.type=

# Specify the default authentication scheme here. USERPASS, BASIC, BOETOKEN, COOKIE, TRUST
1.authentication.scheme=KERBEROS

# Trusted authentication: session variable name to retrieve the shared secret;  Leave empty if shared secret is not passed from web session
# <id>.trusted.auth.sharedsecret=

# Trusted authentication: set Header/URL parameter/Cookie/Session variable/custom class name to retrieve user name.  No need to set for REMOTE_USER or USER_
# <id>.trusted.auth.user.param=

# Trusted authentication: set how to retrieve userID.  Set to "REMOTE_USER" for HttpServletRequest.getRemoteUser().  Set to "HTTP_HEADER" for HTTP header.
# <id>.trusted.auth.user.retrieval=

# Trusted authentication: set to true to prefix external user name to secExternal:<username>; Leave empty if external user name is mapped to same user name
# <id>.trusted.auth.user.namespace.enabled=

```

1. Uncomment `default.cms.identifier` and assign the value 1.
2. Uncomment aliases and assign the same value given for `SSO_Kerberos.BOBJ_MOBILE_CMS`.
3. Uncomment authentication.scheme and assign the value KERBEROS.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## Changes for `authscheme.properties`

Uncommont the KERBEROS property that is highlighted in the figure below.




## Configuring web.xml

You must provide values to few parameters specific to your environment, as mentioned below. The values for each of these keys are found in `global.properties`, which is created while setting up BOE with `kerberos.global.properties` under `<BIP_INST_DIR>\tomcat\webapps\BOE\WEB-INF\config\custom\global.properties`.

Add the following lines after the end filter tag of CompressionFilter.

```
<filter>
<filter-name>KerberosFilter</filter-name>
<filter-class>com.businessobjects.mobilebi.server.filters.KerberosFilter</filter-
class>
<init-param>
<param-name>sso.enabled</param-name>
<param-value>true</param-value>
    </init-param>
<init-param>
<param-name>siteminder.enabled</param-name>
<param-value>false</param-value>
    </init-param>
<init-param>
<param-name>vintela.enabled</param-name>
<param-value>true</param-value>
    </init-param>
<init-param>
<param-name>idm.realm</param-name>
<param-value>{your-realm-name-here}</param-value>
```


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

```
</init-param>
<init-param>
<param-name>idm.princ</param-name>
<param-value>{your-principal-name-here}</param-value>
</init-param>
<init-param>
<param-name>idm.allowUnsecured</param-name>
<param-value>true</param-value>
    </init-param>
<init-param>
<param-name>idm.allowNTLM</param-name>
<param-value>false</param-value>
<init-param>
<param-name>idm.logger.name</param-name>
<param-value>simple</param-value>
</init-param>
<init-param>
<param-name>idm.logger.props</param-name>
<param-value>error-log.properties</param-value>
</init-param>
  </filter>
<filter-mapping>
<filter-name>KerberosFilter</filter-name>
<servlet-name>VintelaServlet</servlet-name>
<dispatcher>REQUEST</dispatcher>
<dispatcher>FORWARD</dispatcher>
<dispatcher>INCLUDE</dispatcher>
</filter-mapping>
```

Add the following after the end servlet tag of LumiraServlet.

```
<servlet>
<description>HandleKerberosLogon</description>
<servlet-name>VintelaServlet</servlet-name>
<servlet-class>com.businessobjects.mobilebi.server.http.VintelaServlet</servlet-
class>
</servlet>
```

Add the following after the end servlet-mapping tag of lumiraservlet.

```
<servlet-mapping>
<servlet-name>VintelaServlet</servlet-name>
<url-pattern>/VintelaServlet</url-pattern>
  </servlet-mapping>
```


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 10 Understanding the User Data Protection and Privacy Parameters

User data is data or information that is specific to an individual user. This includes downloaded reports and the user's application log on credentials. To guarantee the security of user data, SAP BusinessObjects Mobile implements certain security measures.

These include the following:

- Users have the option of saving their password for a connection in the application. In the default configuration, this option is disabled (`savePassword=false`). However, if a user enables the Save Password option while configuring the connection on his or her device, the password is encrypted using the FIPS compliant AES algorithm.
- If users do not choose to save their password, they are prompted for it whenever they access the application, regardless of whether they are in online or offline mode.
- In the default configuration for the application, the option to download and view documents locally on the device is disabled. (`offlineStorage=false`). Users can only access the documents available on the server in online mode.
  Based on requirements, the administrator can enable this option in the server configuration file or using the Central Management Console. (See the related topic of this chapter for more information on how to configure the Mobile server using the CMC.)
- If offline storage of documents is enabled, there is a "Time to Live" parameter in the server configuration file, with a default value of 365 days (`offlineStorage.ttl=365`). This means that the downloaded documents expire after 365 days and are automatically removed from the device's local memory.
- For Web Intelligence documents containing private or confidential data, you can secure the documents by assigning them to a "Confidential" category in the document designing tool. A secure document can be accessed by users only while connected to the Mobile server. Once users log off from the server, the secure document is deleted from the device memory.

The parameters (`savePassword`, `offlineStorage` and `offlineStorage.ttl`) explained above can be found in the following file on the Mobile server:

Based on your specific security requirements, you can change the values of these parameters in the `ClientSettings.properties` file.

> **Note**
>
> For more information about the security measures implemented in the application and in the mobile system landscape, see the *SAP BusinessObjects Mobile System Security Guide* available at at the SAP Help portal: http://help.sap.com/boall_en

## Related Information

Using the Central Management Console (CMC) For Mobile Server Configuration [page 22]


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 11 Setting Mobile Specific Document Properties for BI Inbox Documents

To enable mobile users to view the BI documents sent or published to their BI Inbox, you need to set mobile specific properties in the BI LaunchPad.

To set mobile specific properties for BI Inbox documents, follow the below procedure:

1. On the *Documents* tab, expand the *Folders* drawer, and select the object.
2. Right-click the object and select*Mobile Properties*. The *Mobile Properties* dialog box appears.
3. Choose one or more properties for an object from the following options:

| Option | Enables you to |
|---|---|
| Display on mobile | View the document on the mobile device. |
| Disable saving on mobile | Access the document while you are connected to Mobile server. You cannot save a local copy of the document. |
| Designed for mobile | View the document in page layout mode on the mobile device.<br>**Note**<br>This is only applicable to Web Intelligence documents. |

> **Note**
>
> To view the BI Inbox documents on the mobile documents, ensure to set the above properties before assigning the document to BI Inbox.

4. (Optional) Select *Show as PDF*, to view the document in PDF format on the mobile device.

> **Note**
>
> This is only applicable to Web Intelligence documents.

5. (Optional) Enter a numeric value for *Time to Live*, to specify the number of days the document after which the document expires.
6. Click *Save & Close*.

> **Remember**
>
> The above work-flow for setting mobile specific properties for BI Inbox documents is required because documents once sent to the Inbox do not have any category associated with them. Hence, the standard way of making BI documents mobile-ready and mobile-designed (which is assignment to the "mobile" and "mobiledesigned" categories) does not work for them.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 12 Administrative and Security Rights

## 12.1 Managing Document Access and Other Rights for Mobile Users

Administrators can set up security rights for mobile users and groups on the SAP BusinessObjects Business Intelligence Platform Central Management Console (CMC), using the standard SAP BusinessObjects Business Intelligence platform security rules.

> **Note**
>
> For complete information on configuring rights, see the *SAP BusinessObjects Business Intelligence Platform Administrator's Guide*.

### Mobile Rights for Users and Groups

To set the rights for the user or groups, perform the following steps:

1. Log on to the Central Management Console application.
2. Under *Manage* category, choose *Applications*.
3. Select SAP BusinessObjects Mobile from the list and click on Manage User Security icon.
   The User Security: SAP BusinessObjects Mobile popup appears.
4. Select *Add Principles*.
   The Add Principles popup appears.
5. To assign appropriate rights, choose Users or Groups.
6. Select *Add and assign security* and perform following substeps:
   1. In the *Access level* tab, select the access levels.

      > **Note**
      >
      > The minimum access level that you can assign is View.

   2. In the *Advanced* tab, Select Add/ Remove Rights.
      The Add/Remove Rights popup appears.
   3. You can set, grant or deny rights for each listed application right.
      SAP BusinessObjects Mobile supports the following application rights for selected users and groups:


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

| Right | Description |
| --- | --- |
| Log on to SAP BusinessObjects Mobile application | Allows you to log on to SAP BusinessObjects Business Intelligence platform (using the Mobile application) and view documents. |
| Subscribe to document alerts | Allows you to subscribe to document/recurring alerts.<br>**Note**<br>If you previously had granted the "Subscribe to document alerts" right and access is currently denied, you will still receive subscribed alerts. To stop recieving alerts, you have to explicitly unsubscribe from them.<br>**Note**<br>To subscribe to document alerts (or recurring instances) for schedules, a user must have "Full Control" security access for the "System Events" folder under "Events" in the Central Management Console (CMC). |
| Save documents locally to device | Allows you to save documents on the Mobile device.<br>**Note**<br>If you saved documents on the device when you had the "Save documents locally to device" right, the documents still exist on the device even if you are currently not authorized to save. However, these documents are not synced during the synchronization process. |
| Send documents on device as an e-mail | Allows you to send reports by e-mail. |

4. Select *Ok*.

In the default settings, users belonging to the administrators group have full access rights whereas all other users are only granted the "Log on to SAP BusinessObjects Mobile application" right (unless these rights are explicitly denied).

The Mobile application rights did not exist in releases XI R2 and XI 3.x. If you are upgrading or migrating from an XI R2 or XI 3.x system to a 4.1 system, rights for users and groups therefore need to be configured in the 4.1 system.

## Authentication

SAP BusinessObjects Mobile supports the following authentication methods:


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

- Enterprise
- Windows AD
- LDAP
- SAP R/3

## 12.2 Mobile Category and Document Access

We recommend having your Enterprise administrator create a category in the BI Launch pad named *Mobile* under corporate categories and assign mobile-related documents to this category. If the administrator groups all mobile documents under the same category, mobile users only access the content designed for mobile consumption through the *Home* page. This reduces the number of clicks required to access documents at each log on.

As an administrator, you can deny or grant specific groups in the Mobile deployment access to the documents and sub-categories within the Mobile category.

## 12.3 Working with CORBA SSL Enabled CMS

If your SAP BusinessObjects Business Intelligence platform CMS is configured to use CORBA SSL, then additional configuration is required to enable the Web application servers (WAS) to work with CORBA SSL.

Add the following entry to the Java options of any Web application server:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl
-DtrustedCert=cacert.der
-DsslCert=clientcert.der
-DsslKey=client.key
-Dpassphrase=passphrase.txt
```

The following table shows the descriptions that correspond to these examples:

| Example | Description |
|---|---|
| <DcertDir=d:\ssl> | The directory to store all the certificates and keys. |
| <DtrustedCert=cacert.der> | Trusted certificate file. If specifying more than one, separate with semicolons. |
| <DsslCert=clientcert.der> | Certificate used by the SDK. |
| <DsslKey=client.key> | Private key of the SDK certificate. |
| <Dpassphrase=passphrase.txt> | The file that stores the passphrase for the private key. |

For information about configuring servers for SSL, see *SAP BusinessObjects Business Intelligence Platform Administrator's* Guide.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 13 Auditing

Auditing enables you to keep record of significant events on SAP BusinessObjects Business Intelligence platform servers and applications, giving you a picture of what, how and who is accessing the information. This information is recorded in a database called the Auditing Data Store (ADS). Once the data is in the ADS, you can design custom reports in accordance with your specific requirements.

> **Note**
>
> To record the information in ADS, ensure to enable the audit function on your SAP BusinessObjects Enterprise server. For information on the list of auditing events and details, the auditing database and schema, and to understand how auditing works, see the "Auditing" chapter in the SAP BusinessObjects Business Intelligence Platform Administrator's Guide.

## 13.1 Auditing Events

SAP BusinessObjects Mobile obeys the following auditing events supported on the SAP BusinessObjects Enterprise server based on the settings of the Business Intelligence (BI) artifacts:

| Event Name | Description |
|---|---|
| View | This event is triggered when Mobile users attempt to view a BI document in the Mobile client |
| Refresh | This event is triggered when Mobile users attempt to refresh a BI document in the client. |
| Prompt | This event is triggered when Mobile users attempt to select value for a promptin the client. |
| Retrieve | This event is triggered when Mobile users attempt to retrieve a BI document from CMS |
| Log on | This event is triggered when Mobile users attempt to logon to the client application. |
| Logout | This event is triggered when Mobile users attempt to logout of the client application. |

However, you can identify the events specific to the Mobile application by querying the ADS using the Application_Type_Name = "SAP BusinessObjects Mobile".


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 13.2 Creating Custom Auditing Reports

Auditing reports help you identify, troubleshoot, and detect underlying system errors. You can use the SAP Crystal Reports or SAP BusinessObjects Web Intelligence to create custom auditing reports for user and system actions specific to Mobile.

Using the following information in ADS, the Administrator generates mobile specific auditing report:

- Client IP address and Host ID: This information is sent by client to establish a connection to the Mobile server and in turn to SAP BusinessObjects Enterprise server.
- Mobile server UID: This information is the unique ID of the server.

### Example

**SQL for generating report for Mobile application 'View' event**

```
select distinct d.Session_ID, d.Start_Time, a.Event_ID, b.Event_Detail_Type_Name,
a.Event_Detail_Value, d.Event_Type_ID, c.Event_Type_Name, d.Service_Type_ID,
e.Service_Type_Name, d.Client_Type_ID
From
ADS_EVENT_DETAIL as a, ADS_EVENT_DETAIL_TYPE_STR as b, ADS_EVENT_TYPE_STR as c,
ADS_SERVICE_TYPE_STR as e, ADS_EVENT as d,
Where
a.Event_Detail_Type_ID = b.Event_Detail_Type_ID and b.Language = 'EN' and
a.Event_ID = d.Event_iD and d.Session_ID in ( select distinct Session_ID from
ADS_EVENT where Client_Type_ID = 'ASF9FYol7kRAuW.u1ikmU20' ) and d.Event_Type_ID
= c.Event_Type_ID and c.Language = 'EN' and  d.Service_Type_ID =
e.Service_Type_ID and e.Language = 'EN'   order by d.Session_ID, d.Start_Time asc
```

#### Note

When generating a Save event report, use a.event type id= `1088` . Tracking auditing information specific to Mobile application and generate report.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# 14 Troubleshooting Information

## 14.1 Logging and Tracking Mobile Server Errors

The main types of server errors that you need to capture in your deployment are:

- SAP BusinessObjects Business Intelligence platform errors, reported directly to the Mobile client. For more information, see the *Error Messages Explained* guide.
- Mobile server errors:

  Generic errors

  Authentication errors such as invalid credentials or session errors

  Networking errors such as Remote site unreachable, Cannot resolve the address, Local database access errors or Connection to the application server lost

  HTTPS errors

### 14.1.1 Defining the Log Level

The procedure enables the Mobile application to record information about execution of the application. This log information helps you to identify issues if the application fails or encounters a problem.

To set log levels for the Mobile server component, you need to create three environment variables:

- BO_TRACE_LOGDIR: Specifies the path to the folder where logs are generated.
- BO_TRACE_CONFIGFILE: Specifies the path to BO_trace.ini.
- BO_TRACE_CONFIGDIR: Specifies the path to the folder where BO_trace.ini is located.
- BO_trace.ini is the configuration file where multiple log levels can be set. There are different log level types: trace_none, trace_debug, trace_path, trace_information and trace_error.

The following table describes the logging level importance in decreasing order of detail:

| Severity | Configuration Value |
|---|---|
| NONE | trace_none |
| DEBUG | trace_debug |
| PATH | trace_path |
| INFO | trace_information |
| ERROR | trace_ error |

To set the log level, perform the following steps:

1. Open the BO_Trace.ini file for editing.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

2. Set the required logging level for each unit.

For detailed information on how to configure server tracing using the `BO_trace.ini` file, see the section *To configure server tracing using the BO_trace.ini file* in the latest *Business Intelligence Platform Administrator Guide* available at http://help.sap.com/bobip41?current=bobip41

> **Note**
>
> If you do not set the importance for any unit, the default importance that you set for the global parameter is applied.

### Sample BO_trace.ini

```
sap_trace_level = trace_none; // Developer log information
sap_log_level = log_none;     // Administrator log information
size = 10;                    // Size of log file
keep = false;                 // Retain the log file
```

### Set dedicated folder for server logs

By default, the path to BO_trace file location is accessed from BO_TRACE_CONFIGFILE. However, It can also be configured in web.xml by specifying a new context parameter "mobi.trace" and specifying the path value "/WEB-INF/conf/BO_Trace.ini".

## 14.1.2 Viewing Build Numbers

After installing the Mobile server and the client, you can access the build number of the Mobile application for both the server and client. The build number enables you to identify which version of the Mobile application you have installed. It is also useful for troubleshooting any Mobile server and client problems.

You can access the build number of the Mobile server from the log files on log level DEBUG. These are located in the *MANIFEST* file, which is located in the *MobileBIService.war* file.

To view the build number of the Mobile client application you can perform either one of the following:

- Look at the splash screen when you start the Mobile client application on the device.
- Open the device menu and choose *Preferences* > *About*.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## 14.2 Network Unavailable Errors

Mobile devices that connect to SAP BusinessObjects Mobile need to be configured for Internet access. Ensure that all devices in your deployment can connect to the Internet, so that they can access the Mobile server.

If TCP and APN settings are not correctly configured on the device, the user might receive *Open-tunnel failure* or *Network unavailable errors*. To resolve these errors configure the device for Internet access. These can also be caused by:

| Cause | Resolution |
| --- | --- |
| Incorrect network configuration for device | Check the data subscription<br>Check the carrier settings (TCP)<br>Check the IT policy<br>Check the application rights (can use HTTP and socket connection) |
| Incorrect connection settings | Mobile server name<br>Mobile port number<br>CMS name |
| Device cannot connect to the Mobile server | Device cannot connect to the BES<br>BES cannot connect to the Mobile Server<br>Mobile Server cannot connect to the SAP BusinessObjects Business Intelligence platform Server<br>Device cannot connect to the internet or to the proxy server (if your deployment includes a proxy server)<br>The proxy server cannot connect to the Mobile Server (if your deployment includes a proxy server)<br>The Mobile Server cannot connect to the SAP BusinessObjects Business Intelligence platform Server |

## 14.3 HTTPS errors

Errors explained in this section are generated on the server side of the Mobile solution, yet they are encountered while working with the applicatio on user's Android and iOS devices.

Most errors occurring on the server are caused by HTTP errors such as HTTP 503, HTTP 400, HTTP 404, HTTP 500 and others. Whenever the application (client) receives an HTTP error code from the server, the code is included in the error message displayed by the application. This helps the administrator identify the server error and take the required action to fix it.

For example, consider the following error:

"Connection to the server could not be established; try again or contact your administrator (MOB06005)"

If during the occurrence of this error, the application receives HTTP 503 error from the server, the error message is displayed as:

"Connection to the server could not be established; try again or contact your administrator (MOB06005) (HTTP 503)"


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Sometimes, instead of the HTTP code, the server may return a zero error code ('0'). In this case, the application does not append anything to the error message.

Commonly encountered mobile server errors are described below:

## An internal server error occurred while processing the client request (MOB00022)

### Cause

This error occurs when the user does content Search on server using the SAP BI application on iPad. It is a limitation of server configuration.

### Action

To resolve this issue, take the following steps:

1. Stop the Web application server on which the MobileBIService.war is installed.
2. Locate MobiService.jar file in the following directory: `<WEB_APP_ROOT>\MobileBIService\WEB-INF\lib`
3. Open MobiService.jar as a zip file (using Winrar or Winzip).
4. Extract command_factories.properties file from the MobiService.jar
5. Open command_factories.properties using a text editor and add the following lines at the end of file:

```
com.businessobjects.mobilebi.server.messages.AdvancedSearchRequest=com.businessob
jects.mobilebi.server.commands.impl.AdvancedSearchFactory
com.businessobjects.mobilebi.server.messages.AdvancedSearchDataRequest=com.busine
ssobjects.mobilebi.server.commands.impl.AdvancedSearchDataFactory
```

6. Save the command_factories.properties file.
7. Update MobiService.jar with the updated command_factories.properties file.
8. Restart the Web application server.

## Connection to the server could not be established; contact your administrator if the problem persists (MOB06004)

### Cause

The proxy information configured on the device might be incorrect or the application server might be down.

### Action

1. Verify that the proxy server settings are configured correctly on your device.
2. Verify the connectivity to the application servers on which the Mobile WebApp and the BusinessObjects Enterprise (BI platform) is deployed. You should also make sure that these servers are up and running.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## Connection to the server could not be established; try again or contact your administrator (MOB06005)

**Cause**

This error occurs when there is a problem in redirecting the request to the Web proxy server. The server is unable to handle the request temporarily, due to an overload of the request. This error arises due to HTTP 503 response from the server.

**Action**

Trying again after sometime resolves the issue.

## The request has timed out; try again or contact your system administrator (MOB06006)

**Cause**

This error occurs when user's HTTP request to the server has timed out. This can be due to slow speed of the network or because of connectivity problems between the client and server.

**Action**

Verify the connectivity of user's mobile device to the mobile server.

## You are not authorized for this request (MOB06008)

**Cause**

The file for which the user has requested the server requires access rights and permissions.

**Action**

Check if the user is authorized to view or access the requested document on the BI platform.

## Your request is invalid; verify the connection details or contact your administrator (MOB06009)

**Cause**

The request which the user has made to the server is incorrect. This message may also be displayed due to an HTTP 404 error.

**Action**

Ask the user to try again after some time. If user's request invokes a document from the server, verify if the requested document is accessible on the BI platform server.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## Internal server error occurred while processing your request; try again or contact your system administrator (MOB06010)

**Cause**

This error indicates that the Web application server has encountered some unexpected condition. This can also arise due to improperly configured proxy servers.

**Action**

Verify that the proxy server settings are configured correctly on user's device. If this does not resolve the problem, try restarting the Web application server.

## Missing prompt value; select at least one value for the prompt (MOB06011)

**Cause**

This error appears when the user has not entered any values in the prompt which appears while refreshing a Web Intelligence document using the app.

**Action**

Ask the user to ensure that he/she has selected at least one value for each prompt that appears on refreshing a document.

## Verify network connectivity (MOB06021)

**Cause**

This error is encountered when the openDocument link of a webintelligence document is not able to fetch or retrieve the target document.

**Action**

Verify that the network connectivity is fine. You can do so by trying to access the internet from the browser on user's device.

## Connection to the server could not be established; try again or contact your administrator (MOB06031)

**Cause**

This error occurs when the network within which users are working does not have connectivity with the SAP BusinessObjects Mobile server.

**Action**


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Verify the server connection details in the app on user's device, such as the IP address or syntax of the connection URL.

## Server returned an error while downloading the document (MOB06060)

**Cause**

This error may appear when the user is trying to download a document. It occurs due to following reasons:

- There are connectivity issues between the Mobile server and the CMS (BI platform server).
- The document which the user is trying to download is corrupt.

**Action**

Ask the user to try downloading the document again. If the problem persists, check if the document is opening and behaving as expected on the BI platform.

## This action cannot be performed; verify network connectivity (MOB08002)

**Cause**

This error occurs due to following reasons:

- Connection to the BI platform server is lost.
- The device has lost its connectivity to the Wifi network.

**Action**

Verify the following:

- Application's connectivity to the BI platform.
- Device connectivity to the Wifi network.

## An internal server error occurred while processing your request on hierarchical data; the document will be closed; contact your administrator for more information (MOB09001)

**Cause**

This error is encountered when users are working with reports based on hierarchical report parts or hierarchical prompts. It occurs because the Web Intelligence server is unable to fetch data from a hierarchical data source (such as OLAP and BW).

**Action**

None. This is a known limitation of the application.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

## There was a problem in opening the document; download the document again or contact your administrator (MOB06061)

### Cause

This error appears when users are trying to open a document that is either corrupt or is not downloaded completely.

### Action

Ask the user to download the document again and to download it completely. Also, check if the document is opening and behaving as expected on the BI platform.

## Maximum character file size limit exceeded. The document is too large to be processed by the server. Contact your BusinessObjects administrator (WIS 30272)

### Cause

When users view a Web Intelligence document in HTML format, the Web Intelligence server generates character based output, which is then interpreted by the Web browser. This errors occurs, if the size of the character output is greater than the maximum size specified by you on the Web Intelligence server.

### Action

As the application administrator, you can change the value for Maximum Character Stream Size (MB) in the Web Intelligence Processing (WIP) server properties via the CMC (Central Management Console). However, increasing the maximum binary output (Binary Stream Maximum Size (MB)) can affect the performance.


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

# Important Disclaimers and Legal Information

## Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

## Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

## Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

## Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).


© 2016 SAP SE or an SAP affiliate company. All rights reserved.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

**go.sap.com/registration/contact.html**

© 2016 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.
Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.
These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.
SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.
Please see http://www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.