

# Configuring Active Directory Manual Authentication and SSO for BI4



## Applies to:

BI 4.0 or later

## Summary

This paper combines all the steps from the BI 4 Administrator's Guide with the latest best practices and all the latest SAP KBAs regarding vintela, kerberos and java AD configuration. **It is specifically written for BI 4 and will not work with earlier versions of XI.**

**Author(s):** Steve Fredell

**Company:** SAP Business Objects

**Created on:** 01 September 2011

## Author Bio



Educator and coach for 10 years prior to starting with SAP BusinessObjects Primary Support in March of 2007. Currently specializing in Authentication for the XIR2, XI 3.1 and BI 4 products.

## Table of Contents

Prerequisites .....	4
Section 1 - Planning your Service Account Configuration .....	4
Roles of the Service Account .....	4
Role 1 – Query Active Directory .....	4
Role 2 – Run the SIA/CMS and allow manual AD logins. ....	4
Role 3 – Allows Single Sign On .....	4
Section 2 - Creating and preparing the service account .....	5
Creating the Service Account .....	5
Create Service Principal Names for the Service Account.....	5
Background Information .....	5
Setspn Commands .....	6
To View all created SPN's.....	6
Delegation for the Service Account.....	7
Section 3 - Configure the AD Plugin Page in the CMC and map in AD groups .....	8
Section 4 — Steps to start the SIA/CMS under the service account.....	10
Verify the service account and AD logins are working.....	11
Section 5 –Configuring Manual AD authentication to Java Application Servers .....	12
Create the bscLogin.conf file .....	12
Create the krb5.ini file .....	12
Verify java can successfully receive a kerberos ticket.....	14
Section 6 – Configuring BI Launch Pad and CMC for manual AD login .....	15
Enable the Authentication dropdown for BI Launch Pad .....	15
Point your application server to the bscLogin.conf and krb5.ini files. ....	15
Verify the bscLogin.conf has been loaded by you application server .....	16
Common reasons why a manual login to BI Launch Pad would fail .....	16
Section 7 – Configuring Active Directory Single Sign On .....	17
Increase Tomcat's maxHttpHeaderSize .....	17
Create and configure a global.properties file .....	17
Configuring the application server's Java Options for AD Single Sign On .....	18
Verify the vintela filter has loaded successfully .....	19
If credentials are not obtained... ..	19
Testing AD Single Sign On .....	20
Browser Configuration .....	20
First SSO attempt .....	20
Section 8 – Additional information and settings.....	20
Ensure your .properties files are not overwritten after a patch or redeploy .....	20
Encrypting your service account password with a keytab .....	20
Configuring your system for end-to-end SSO to a DB.....	21
Setting up Constrained Delegation .....	21
Clean up tracing .....	21
Other information .....	22

Appendix .....	23
Key Terms.....	23
3 <sup>rd</sup> Party Troubleshooting Tools .....	23
Copyright.....	24

## Prerequisites

- Review the BI4 Product Availability Matrix (PAM) to ensure your client and server operating systems, browsers and Active Directory versions are supported.
- Windows AD authentication only works if the CMS is run on Windows. For single sign-on to the database, the reporting servers must also run on Windows. These Windows machines must be joined to the appropriate AD domain.
- At the time this document was written RC4 is the only tested and recommended encryption method. DES has known issues and AES encryption has not been fully tested.
- For multiple AD Forest environments please refer to KBA 1323391

**It is very important that you follow these sections in order and do not attempt to perform actions before they are requested or perform non-documented actions. For example, creating keytab files or enabling constrained delegation before simple SSO is working.**

## Section 1 - Planning your Service Account Configuration

Prior to configuring BI4 for Active Directory logins you must create an Active Directory service account. There are 3 roles for this service account.

### Roles of the Service Account

#### Role 1 – Query Active Directory

- This role is entered into the top portion of the Windows AD page in the CMC.
- This role is used by the CMS to perform LDAP searches against AD's directory servers.

#### Role 2 – Run the SIA/CMS and allow manual AD logins.

- Used by the CMS to perform Ticket Granting Server (TGS) requests against Active Directory.
- It requires the following:
  - “Act as part of the Operating System” policy
  - A member of the local Administrators group on every BI server with a CMS
  - An SPN without delegation unless Single Sign On or SSO to the database is required.

#### Role 3 – Allows Single Sign On

- Used by tomcat or other java application servers for launching the vintela filter.
- It requires additional SPN's for all HTTP points of entry (application servers, HLB, etc).

## Section 2 - Creating and preparing the service account

### Creating the Service Account

**\*\*\*READ THIS FIRST\*\*\***

Even though there will be screenshots with steps completed in Active Directory throughout the rest of this document, **please refer to your local AD and Network Administrators before attempting these steps.** The steps documented were tested in house on limited security environments. If your AD or Network Administrators have any questions please use the SDN forums or open a message with SAP support under the BI-BIP-AUT component.

**NOTE:** These steps involve 3rd party tools.

*SAP support can provide limited assistance with troubleshooting these applications.*

*Please see Microsoft for further assistance.*

1. Create a new AD account on the domain controller; for this whitepaper we'll be using bossosvcacct
2. Check 'Password never expires'. Should a password expire the functionality dependant on that account will fail (see the roles above).

NOTE: Some of our legacy Product Guides and Whitepapers suggested enabling additional encryption types, such as DES, on the service account. Ensure there are no additional encryption types selected.

### Create Service Principal Names for the Service Account

#### Background Information

When a client attempts to login to BI Launch Pad via SSO it will use the URL to generate a kerberos ticket-granting ticket (TGT) to the ticket-granting server (TGS) requests. In order for clients to make this request an SPN equal to the application server's URL must be added to the service account.

For example: At the network level you can see that when the SSO user enters the url `http://Tomcat6:8080/BOE/BI` the client will send a TGS request to AD inquiring for a service account that has an SPN of `HTTP/Tomcat6`. The same applies if the user enters a fully qualified domain name (FQDN) or a load balancer URL.

Use the `setspn` command to create client SPN's or points of access for SSO. Format and examples provided below.

**NOTE:** These steps involve 3rd party tools.

*SAP support can provide limited assistance with troubleshooting these applications.*

*Please see Microsoft for further assistance.*

## Setspn Commands

Set a general SPN that we will enter into the SPN field of the AD page in the CMC

```
setspn -a BICMS/service_account_name.domain.com service_account_name
```

Example:

```
setspn -a BICMS/bossosvcacct.vtiauth08.com bossosvcacct
```

The following SPN's are only needed for SSO. See [Background information](#) above

```
setspn -a HTTP/hostname of each Tomcat or application server  
setspn -a HTTP/FQDN of each Tomcat or application server
```

Example:

```
setspn -a HTTP/Tomcat6 bossosvcacct  
setspn -a HTTP/Tomcat6.vtiauth08.com bossosvcacct
```

Optional SPN's for Hardware Load Balancers (HLBs) or server aliases if needed

```
setspn -a HTTP/otherFQDN/hostname for any DNS redirects, or load balancers that  
will be used for SSO
```

Example:

```
setspn -a HTTP/SAPreports bossosvcacct
```

### To View all created SPN's

When finished Run setspn -L bossosvcacct to view all created SPN's

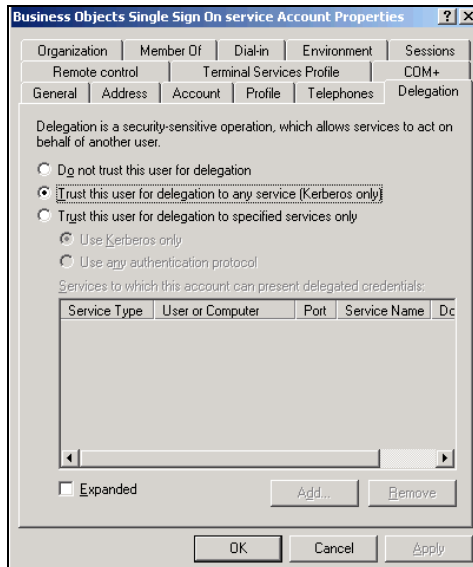
Sample output below shows the service account *bossosvcacct* has 1 SPN for the CMS , 2 for tomcat and 1 for an HLB.

```
C:\Users\Admin>setspn -L bossosvcacct  
Registered ServicePrincipalNames for  
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:  
    BICMS/bossosvcacct.domain.com  
    HTTP/Tomcat6  
    HTTP/Tomcat6.domain.com  
    HTTP/Load_Balancer.domain.com
```

## Delegation for the Service Account

If manual AD logins are all that is required there are no further actions be completed on the domain controller.

If AD SSO is required, navigate to the properties of the newly created service account and choose **Trust this user for delegation to any service (Kerberos only)** under the **Delegation** tab. If constrained delegation is required, the steps are provided at the end of this document. For troubleshooting reasons, please do not configure constrained delegation until AD SSO is working for non-constrained delegation.



## Section 3 - Configure the AD Plugin Page in the CMC and map in AD groups

The following steps are also explained in more detail on the BI4 Admin guide. Included are the key points in this document to verify they are complete and help avoid some common mistakes.

**Windows Active Directory**

☒ Enable Windows Active Directory (AD)

**AD Configuration Summary**  
To change a setting, click on the value.

AD Administration Name: v8\bossosvcacct  
Default AD Domain: VTIAUTH08.COM

**Mapped AD Member Groups**  
Add AD Group (Domain\Group):    
secWinAD:CN=VTIAUTH,OU=groups,OU=auth\_accts,DC=vtiauth08,DC=com

**Authentication Options**  
☐ Use NTLM authentication  
☒ Use Kerberos authentication  
☐ Cache security context (required for SSO to database)  
Service principal name: BICMS/bossosvcacct.vtiauth08.com  
☒ Enable Single Sign On for selected authentication mode.

**The AD administration Name** is the account mentioned in role 1 earlier in this doc. This account will be used to query AD for user/group information, and is the account that will need local permission to write to the Business Objects Enterprise xx\logging directory if tracing the CMS. Enter this account in domain\user or [user@domain.com](#) format only (it will likely fail without a domain name). Don't be confused by the word Administration, this is simply a role name created by our Product group. This account needs read/query access only and does not need to be an Admin in AD.

**The Default AD Domain** must be the **FULL DOMAIN NAME in ALL CAPS** or child domain name where the most users that will be logging into Business Objects. **This should exactly match default domain in the krb5.ini** mentioned later in the document.

**Mapped AD Member Groups** If a group is in the default domain it can be usually be added with just the group name. If it's in another domain or another forest then it will need to be added in domain\group or DN format. Once added hit update and the groups will appear as above (secWinAD: DN) regardless of how they were entered (group, domain\group, or DN).

If there are issues mapping in groups please see KBA 1199995 for UseFQDNForDirectoryServers or KBA 147634 for additional troubleshooting.

**Authentication Options** Kerberos must be selected for manual AD or AD SSO.

**The Service Principal Name** or SPN *MUST* be the value created for the service account that runs the SIA/CMS via setspn (discussed in section 2 of this doc). Ensure there are no typos or white spaces before or after the SPN.

**Enable Single Sign On** should be selected if SSO is required



New Alias Options

☒ Assign each new AD alias to an existing User Account with the same name

☐ Create a new user account for each new AD alias

Alias Update Options

☒ Create new aliases when the Alias Update occurs

☐ Create new aliases only when the user logs on

New User Options

☐ New users are created as named users

☒ New users are created as concurrent users

**New Alias Options** determine how the user will be created if an existing user with the same name (LDAP/NT/Enterprise) already exists.

**Alias Update Options** determine if users will be added when pressing the update button or only after they have logged into BI Launch Pad/CMC/client tools

**New User Options** should be determined by your licensing options that can be viewed in CMC/license Keys. You can verify users/groups are added by going to CMC/users and groups.

### Verifying users

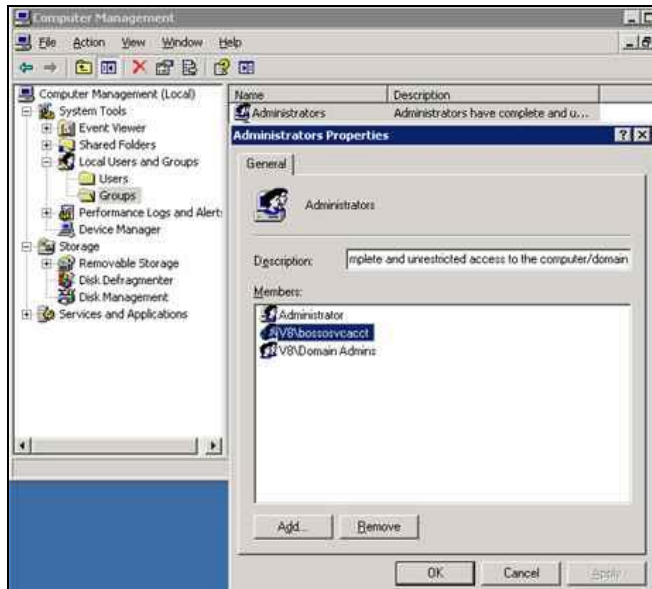
Go to **CMC>Users and Groups>Group Hierarchy** and select the AD group you mapped to view the users for that group. This will generate a live query to AD (using the CMC query account) and display the current users in that group. It will also display any nested users in that group (users that belong to nested AD groups).

**Do not proceed if users and/or groups are not mapping in properly!**

## Section 4 — Steps to start the SIA/CMS under the service account

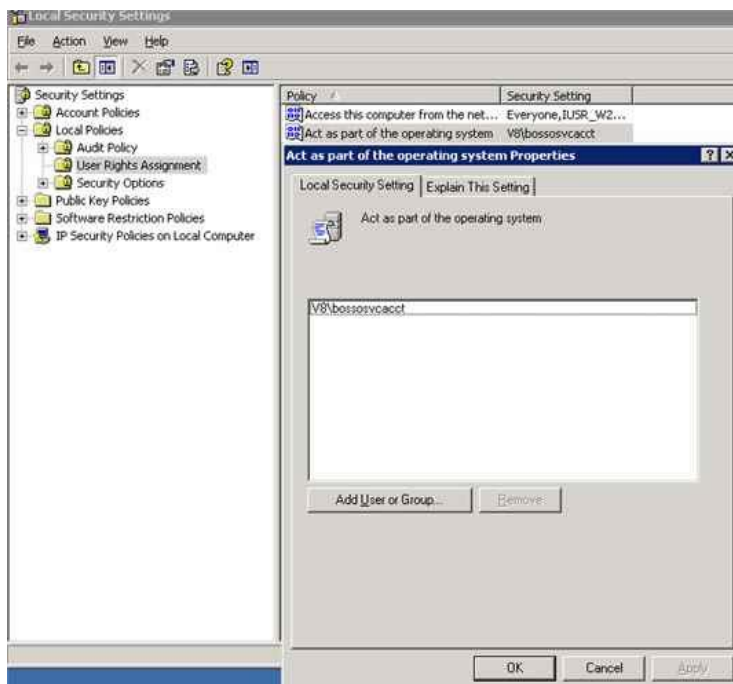
In order for the service account to run the SIA there are specific operating system settings that need to be set.

1. Add the service account to the local administrator's group on any server where the service account will be running a SIA/CMS.

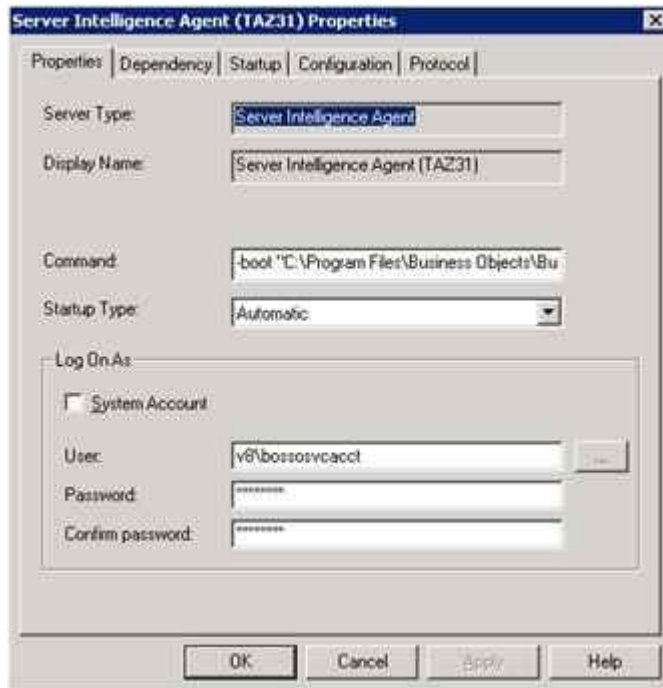


*NOTE: It has been observed that the SIA may start if this account does not have local Administrator permissions. In all cases local administrator is desired when the service account needs to run a service.*

2. You should also grant the local policy **Act as Part of the operating system** as seen in the screenshot below.



3. After the above changes have been made the service account can now run the Server Intelligence Agent (SIA). Navigate to the Central Configuration Manager (CCM), stop the SIA and on the properties tab enter the account in domain\username format.



**NOTE:** If the SIA/CMS should fail to start look in the event viewer, search KBAs, forums, or open a message with support. A common issue is the account running the SIA does not have rights to something local or the CMS database.

### Verify the service account and AD logins are working

You should be able to login via thick client tools at this point. The next steps will test an AD login with the Central Configuration Manager's Manage Servers tool.

1. While you have the CCM open, click on the Manage Servers icon
2. Ensure the System field is correct, choose Windows AD in the dropdown and login with an AD user who exists inside the CMC. AD users that do not reside in the default domain must login to client tools as domain\username
3. Don't worry if you just get a white screen and no services are visible. This is just a rights issue. As long as you do not get an error everything is working.
4. If you do get an error, navigate back to the AD plugin page in the CMC and switch from **Use Kerberos** to **Use NTLM** and click **Update**. If this works then you have a Kerberos issue. Using a tool like Wireshark (see appendix) capture a packet scan from the CMS server during a failed kerberos login to the CCM Manage Servers and in Wireshark filter on kerberos.

**Do not move on to the next section if you cannot login to client tools!**

## Section 5 –Configuring Manual AD authentication to Java Application Servers

**Please note, SAP Support provides these steps "as-is" and cannot assist further.  
Please see Oracle for further assistance with Sun Java  
Please see IBM for further assistance with IBM Java**

Two files need to be created when using java SDK. These files need to be created from scratch and should be placed in the C:\windows\ directory on any windows *application* server. This path is where the java will look by default on a windows server. For application servers on Unix the location will vary on the flavor of Unix, the application server used and the java type and version. Windows 2008 servers by default hide extension suffix for known extension types. When you create these files ensure they do not end with a .txt or other extension.

### Create the bscLogin.conf file

- bscLogin.conf is used to load the java login module and trace login requests.
- You can copy the default bscLogin.conf text from below (**replace sun with ibm when your web application server is using IBM's JDK.**)

```
com.businessobjects.security.jgss.initiate {  
com.sun.security.auth.module.Krb5LoginModule required debug=true;  
};
```

### Create the krb5.ini file

- **krb5.ini** is used to configure the KDC's (Kerberos Key Distribution Center aka domain controllers) that will be used for the java login requests
- You can copy the default krb5.ini text from below and then edit for your environment

```
[libdefaults]  
default_realm = MYDOMAIN.COM  
dns_lookup_kdc = true  
dns_lookup_realm = true  
default_tgs_enctypes = rc4-hmac  
default_tkt_enctypes = rc4-hmac  
udp_preference_limit = 1  
[realms]  
MYDOMAIN.COM = {  
kdc = MYDHOSTNAME.MYDOMAIN.COM  
default_domain = MYDOMAIN.COM  
}
```

- There are 4 bolded values that need to be changed in the above text.
- Replace **MYDOMAIN.COM** with the same domain of your service account. All DOMAIN info must be in ALL CAPS. You may list as many KDC's as you want but for initial configuration it is recommended to just have 1 to simplify testing.
- The **default\_realm** value must EXACTLY match the default domain value entered into the top of the AD page in the CMC.
- Replace **MYDHOSTNAME** with the hostname of a domain controller.
- If your AD admin is not immediately available you can use the steps below to find some of these values. However, it is strongly recommended that your AD and/or network team provide this information.

- To look up your information you can open a DOS window on the application server, execute the `set` command and then look for the `logonserver` and the `USERDNSDOMAIN`.
- Use these values for the `MYDCHOSTNAME` and `MYDOMAIN.COM` respectively.

```

Administrator: Command Prompt
C:\Users\taz>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\taz\AppData\Roaming
CLIENTNAME=DEWDFM0203
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
COMPUTERNAME=W2K8DC1
ComSpec=C:\Windows\system32\cmd.exe
DFSTRACINGON=FALSE
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\taz
LOCALAPPDATA=C:\Users\taz\AppData\Local
LOGONSERVER=\\W2K8DC1
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\ADMT;c:\
Program Files (x86)\Microsoft SQL Server\90\Tools\bin\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 29 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=1d01
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
PROMPT=$P$G
PUBLIC=C:\Users\Public
SESSIONNAME=RDP-Tcp#0
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\taz\AppData\Local\Temp\4
TMP=C:\Users\taz\AppData\Local\Temp\4
TRACE_FORMAT_SEARCH_PATH=\\winseqfe\release\Windows6.0\lh_sp2rtm\6002.18005.0904
10-1830\amd64fre\symbols.pri\TraceFormat
USERDNSDOMAIN=VTIAUTH08.COM
USERDOMAIN=U8
USERNAME=taz
USERPROFILE=C:\Users\taz
windir=C:\Windows

```

Example of a populated `krb5.ini`

```

[libdefaults]
default_realm = VTIAUTH08.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tgs_encypes = rc4-hmac
default_tkt_encypes = rc4-hmac
udp_preference_limit = 1
[realms]
VTIAUTH08.COM = {
kdc = W2K8DC1.VTIAUTH08.COM
default_domain = VTIAUTH08.COM
}

```

## Verify java can successfully receive a kerberos ticket

AKA – Kinit test

Note: This does not verify multi-domain issues

1. From DOS command line navigate to the jdk\bin directory. By default this is:

*C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64\_x64\jdk\bin*

2. Run *kinit username* hit enter and type your *password*

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin>kinit sfredell
Password for sfredell@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

- If the KDC and other configurations in the krb5.ini are correct you should receive a ticket.
- If an error occurs please search our KBAs or open a message with support if necessary.

**NOTE:** java, kinit, krb5.ini, kerberos, AD, etc are not SAP components and thus SAP can provide limited support with troubleshooting these 3<sup>rd</sup> party applications.

### Some quick tips...

The KDC should be an AD domain controller with global catalog services enabled, requests will be sent to port 88 by default. A KDC service must be running on port 88.

### Common errors

**Preauthentication** = invalid password

**KDC for realm** = The KDC in the krb5.ini file did not respond

**Client not found in kerberos database** = bad username

See **KBA 1476374** for additional troubleshooting and a list of best practices

See **KBA 1245178** for advanced krb5.ini settings

**If you cannot successfully get a ticket do not proceed.**

## Section 6 – Configuring BI Launch Pad and CMC for manual AD login

### Enable the Authentication dropdown for BI Launch Pad

The Authentication dropdown on the BI Launch Pad page is hidden by default.

We no longer use xml files. BI4 now uses *.properties* files that are stored in a *custom* folder that does not get overwritten during patching.

1. Navigate to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOEWEB-INF\config\custom
2. Create a file named *BIlaunchpad.properties* with the following text inside:  

```
authentication.visible=true  
authentication.default=secWinAD
```
3. Restart Tomcat to see if the dropdown is visible

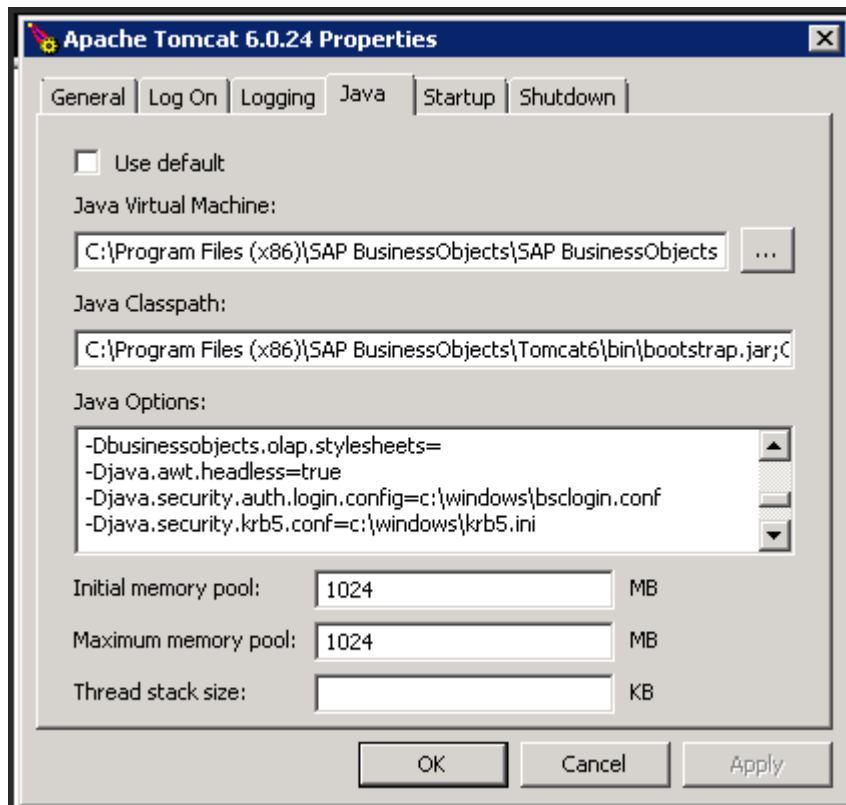
### Point your application server to the bscLogin.conf and krb5.ini files.

In order for AD users to login to BI Launch Pad and the CMC you must ensure your application server has access to the bscLogin.conf and the krb5.ini.

Below are the steps for Tomcat 6.0.24. Steps will vary depending on the application server.

1. Add the following lines to the tomcat java options. Tomcat must be restarted to test.  

```
-Djava.security.auth.login.config=c:\windows\bscLogin.conf  
-Djava.security.krb5.conf=c:\windows\krb5.ini
```



## Verify the bscLogin.conf has been loaded by your application server

After the restart the bscLogin.conf (with *debug=true* option from earlier) will force user login attempts to show up in the application server logs. This is a very un-intrusive level of tracing (leave this enabled during initial configuration or on test environments).

- To verify the bscLogin.conf has been loaded by your application server attempt to logon to BI Launch Pad (with AD selected in the drop down).

A successful login should look like this:

```
Debug is true storeKey false useTicketCache false useKeyTab false doNotPrompt false ticketCache is
null isInitiator true KeyTab is null refreshKrb5Config is false principal is null tryFirstPass is
false useFirstPass is false storePass is false clearPass is false

[Krb5LoginModule] user entered username: sfredell@VTIAUTH08.COM
Acquire TGT using AS Exchange
principal is sfredell@VTIAUTH08.COM
EncryptionKey: keyType=23 keyBytes (hex dump)=0000: 88 46 F7 EA EE 8F B1 17 AD 06 BD D8 30 B7 58
6C .F.....0.X1
Commit Succeeded
```

## Common reasons why a manual login to BI Launch Pad would fail

### bscLogin.conf failing to load

- If usernames are not showing up you can check the logs in C:\SBOPWebapp\_BIlaunchpad\_IP\_PORT.
- If there is a typo in the bscLogin.conf file you may see:  
Cannot create LoginContext. No LoginModules configured for com.businessobjects.security.jgss.initiate
- If user login attempts are not being logged there may be a typo in the web application server's java options related to the bsclogin.conf file.

### Krb5.ini failing to load

We know the contents of the krb5.ini are good from the [Kinit test](#) above however, if the path specified in the application server's java options is incorrect you will see an error similar to the following in the application server logs or in the C:\SBOPWebapp\_BIlaunchpad\_IP\_PORT directory:

*Could not load configuration file <directory path>\krb5.ini (The system cannot find the path specified)*

**Do not proceed to the next section until manual logins to BI Launch Pad are working!**



## Section 7 – Configuring Active Directory Single Sign On

### Increase Tomcat's maxHttpHeaderSize

For Tomcat servers it is necessary to increase the default HTTP Header size in the server.xml. Kerberos login requests contain, amongst other things, group information. The more AD groups a user is a member of the larger the http header must be to accommodate the size of the kerberos packet. 16384 is usually large enough but if your mapped users are a member of many groups (50 or more AD groups) you may need to increase this size to 32768, 65536 or more (multiples of 16384).

**NOTE:** Make a backup copy of server.xml file prior to editing

- Default path for the server.xml:  
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\conf\server.xml
- The line should look like this after adding the bold text and single space:

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443"
compression="on" URIEncoding="UTF-8" compressionMinSize="2048"
noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,text/json,application/json" maxHttpHeaderSize="65536" />
```

**Note:** Do not copy/paste. Also, this file is case sensitive.

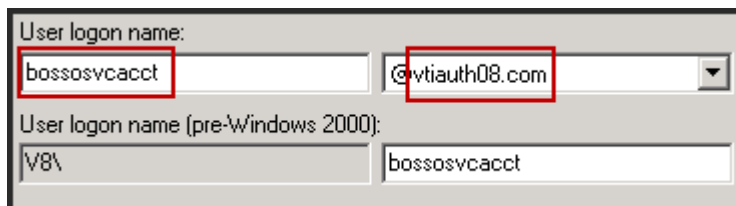
### Create and configure a global.properties file

We no longer use xml files. BI4 now uses .properties files that are stored in a *custom* folder that does not get overwritten during patching.

1. Navigate to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom
2. Create a file named **global.properties** with the following text inside:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=VTIAUTH08.COM
idm.princ=bossosvcacct
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.logger.props=error-log.properties
```

- For the values in **bold** above replace them with the values for your service account from Section 2 above.



The screenshot shows a 'User logon' dialog box. It has two main sections. The top section is for 'User logon name' and includes a text input field containing 'bossosvcacct' and a dropdown menu showing '@vtiauth08.com'. The bottom section is for 'User logon name (pre-Windows 2000)' and includes a text input field containing 'V8\bossosvcacct'.

- Best practices suggest you enter the username with exact lowercase and capitals as seen in AD.
- Your domain should be entered in ALL CAPS.
- Ensure there are no white spaces at the end of any line and the file does not end with .txt extension.

## Configuring the application server's Java Options for AD Single Sign On

In the above step we have given your application server the name and domain of your service account. In the options below we will provide the application server with the password to that account as well as enable tracing.

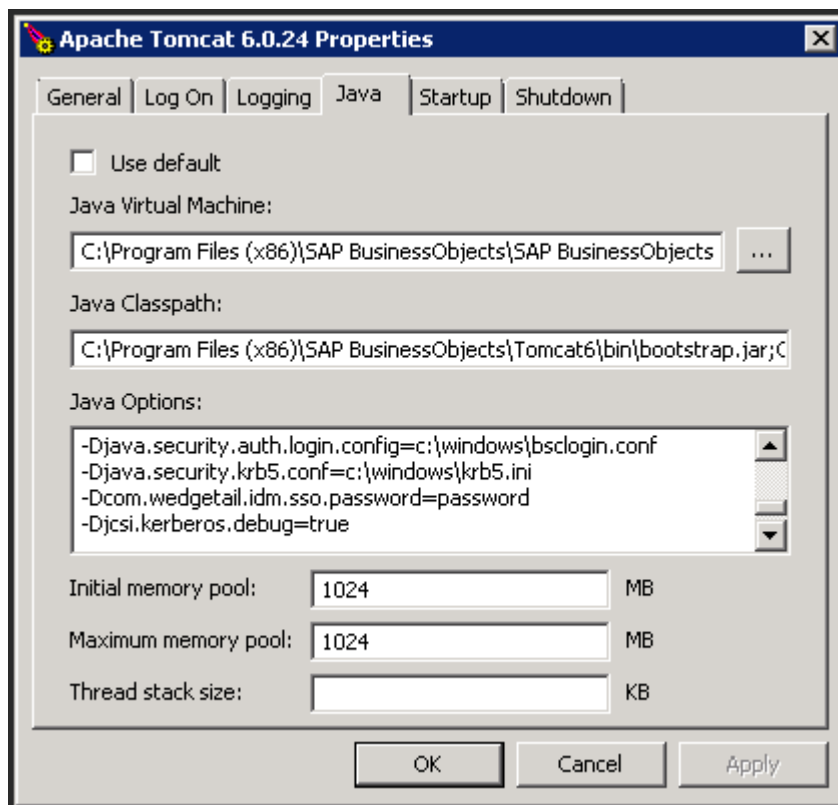
**Note:** Later in this document we explain how to use a keytab file to store and encrypt your service account's password if you so desire. For now, please use the java password option until SSO is working for all users, in all domains and in all forests.

Below are the steps for Tomcat 6.0.24. Steps will vary depending on the application server.

1. Add the following lines to the tomcat java options. Tomcat must be restarted to test.

```
-Dcom.wedgetail.idm.sso.password=password  
-Djcsi.kerberos.debug=true
```

- The wedgetail.sso.password is the password for your service account from [Section 2](#) above.
- The DJCSI.kerberos.debug options will enable a start up trace of the vintela filter.



## Verify the vintela filter has loaded successfully

1. Stop Tomcat
2. Delete or backup the logs in the following folders
  - C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\logs\
  - C:\SBOPWebapp\_Bllaunchpad\_IP\_PORT\
3. Restart Tomcat
4. Open C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\logs\**stderr.log** and look for the following line. This will let you know that Tomcat has fully started.
  - INFO: Server startup in ##### ms
5. Open C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\logs\**stdout.log** and look for the following line(s). The number of SPNs you have registered for this account will determine how many times this line is displayed.
  - jcsi.kerberos: \*\* credentials obtained .. \*\*.

If this line is seen the vintela filter is loading successfully. You may skip down to the section titled: [Testing AD Single Sign On](#)

### If credentials are not obtained...

If credentials are not obtained then you can test the service account by running kinit (See [Kinit test](#) above).

1. From DOS command line navigate to the jdk\bin directory. By default this is:
  - C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64\_x64\jdk\bin

2. Run *kinit service-acct-name* hit enter and type the *password*

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\jdk\bin>kinit bossosvcacct
Password for bossosvcacct@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

If an error occurs please search our KBAs or open a message with support if necessary.

**NOTE:** java, kinit, krb5.ini, kerberos, AD, etc are not SAP components and thus SAP can provide limited support with troubleshooting these 3<sup>rd</sup> party applications.

## Testing AD Single Sign On

If all the above steps are successful, including manual logons you can continue with testing AD SSO.

### Browser Configuration

Make sure the browser is setup properly for client side testing KBA 1379894 (IE) and KBA 1263764 (Firefox)

### First SSO attempt

Attempt to test SSO from a client workstation. Be sure the client workstation is on the same domain and a user has logged into the workstation as an AD user that can manually login to BI Launch Pad.

- If your environment will have users from multiple operating systems and/or browsers please test them now.
- If your environment will have users from multiple domains/forests please test them now.
- Troubleshooting client side SSO issues must be done with 3rd party tools since SSO occurs externally to Business Objects and the application server. KBA 1370926 will assist with creating network log files. Open a message with SAP support if you need help interpreting them under the component BI-BIP-AUT.

**NOTE:** SSO will not work from the Tomcat server.

## Section 8 – Additional information and settings

**Note:** DO NOT perform these steps until SSO is working via the above instructions.

### Ensure your .properties files are not overwritten after a patch or redeploy

1. Copy the Bllaunchpad.properties and global.properties files from:  
*C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom*
2. Paste the .properties files in the folder below:  
*C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom*

### Encrypting your service account password with a keytab

An alternative to hard-coding the service account's password in the java options we can encrypt the password in a keytab file.

**Note:** ktpass and Active Directory are not SAP components and thus SAP can provide limited support with troubleshooting these 3rd party applications.

1. Create a keytab with the ktpass command
  - ktpass can be found on domain controllers (DC's) or can be downloaded from Microsoft

```
ktpass -out bosso.keytab -princ service-account-name@REALM.COM -pass service-account-password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Sample:

```
ktpass -out bosso.keytab -princ bossosvcacct@VTIAUTH08.COM -pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

2. Copy the bosso.keytab to the c:\windows\ directory of the application server
3. Add the following line to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\global.properties
  - `idm.keytab=C:/WINDOWS/<your keytab file name>` (note the FORWARD slashes)

4. Remove the wedgetail.password option from the application server's java options.
5. Restart Tomcat and ensure you still see *jcsi.kerberos: \*\* credentials obtained .. \*\** in the application server logs per the directions in the section above titled **Verify the vintela filter has loaded successfully.**

See **KBA 1359035** to test the keytab separately if SSO stops working after these changes.

### Configuring your system for end-to-end SSO to a DB

If you desire to use end-to-end SSO you'll need to run the ktpass command differently than above.

**Note:** ktpass and Active Directory are not SAP components and thus SAP can provide limited support with troubleshooting these 3rd party applications.

1. Create a keytab with the ktpass command
  - ktpass can be found on domain controllers (DC's) or can be downloaded from Microsoft

```
ktpass -out bosso.keytab -princ BICMS/service-account-name@REALM.COM -mapuser service-account-name@REALM.COM -pass service-account-password -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Sample:

```
ktpass -out bosso.keytab -princ BICMS/bossosvcacct@VTIAUTH08.COM -mapuser bossosvcacct@VTIAUTH08.COM -pass password -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

2. Copy the bosso.keytab to the c:\windows\ directory of the application server
3. Modify the following line in C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\global.properties
 

From:

  - idm.princ=bossosvcacct

to:

  - idm.princ=BICMS/bossosvcacct
4. Add the following line to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\global.properties
  - idm.keytab=C:/WINDOWS/<your keytab file name> (note the FORWARD slashes)
5. Remove the wedgetail.password option from the application server's java options.
6. Restart Tomcat and ensure you still see *jcsi.kerberos: \*\* credentials obtained .. \*\** in the application server logs per the directions in the section above titled **Verify the vintela filter has loaded successfully.**

See **KBA 1359035** to test the keytab separately if SSO stops working after these changes.

### Setting up Constrained Delegation

**Note:** DO NOT perform these steps until SSO is working via the above instructions.

See **KBA 1184989** for setting up **constrained delegation** most steps are to be completed within Microsoft with one edit in the **custom\global.properties** file.

### Clean up tracing

You should have completed and tested each section (1-7). You can remove any tracing that was enabled such as:

- debug=true in the bscLogin.conf (Set by default in section 5. Set to false or remove.)
- -Djcsi.kerberos.debug=true java option (Set by default in section 7. Set to false or remove.)

## Other information

Detailed troubleshooting and best practices can be found in KBA 1476374

How to enable trace logging for BI40 Web applications found in KBA 1613472

For manual logon use <http://server:PORT/BOE/BI/logonNoSso.jsp>

## References

BI 4 Documentation: <http://service.sap.com/bosap-support>

ADEplorer <http://technet.microsoft.com/en-us/sysinternals/bb963907>

Netmon 3.4: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f>

Wireshark <http://www.wireshark.org/download.html>

kerbtray - <http://www.microsoft.com/downloads/details.aspx?FamilyID=4e3a58be-29f6-49f6-85be-e866af8e7a88&displaylang=en>

SAP SDN Business Objects User forums (requires free registration) <https://www.sdn.sap.com/irj/sdn/businessobjects-forums>

## Appendix

### Key Terms

Some terms or acronyms we will be referring to throughout this document

**AD Plugin** – The area in the CMC where the query account is entered, SPN is set, and group mapping rules are configured

**AD** – Active Directory – Microsoft's directory server

**CCM** – Utility found on Business Objects Enterprise servers that can view Business Objects server/services/processes

**CMC** – Web Admin tool used to configure the CMS service and other parameters for Business Objects Enterprise

**CMS** – Windows service that is responsible for authorization when using vintela SSO

**FQDN** – The Fully Qualified Domain Name. For example, the FQDN of your Tomcat server may be Tomcat01.SAP.COM

**HLB** – Refers to Hardware Load Balancers (used to split the load between APPLICATION SERVER) DNS redirects generally will follow the same rules as an HLB.

**KDC** - Kerberos Key Distribution Center - A network service that supplies session tickets and temporary session keys to users and computers within an Active Directory domain. The KDC runs on each domain controller as part of Active Directory Domain Services (AD DS).

**SPN** – Service Principal Name refers to an additional alias and attribute to an AD account. Various tools can be used to add an SPN to an AD account. It's much like a UPN or samAccountName except there can be multiple SPN's per account. The SPN is a primary access point for kerberos applications.

**SSO** - Single Sign-On – The ability to access an application without entering login credentials also known as silent sign-on, automatic logon, etc

**Sam Account Name** – common logon name in AD (i.e. domain\user)

**Service account** – Refers to an Active Directory user with special permissions (such as a fixed, non-changing password or SPN)

**UPN** – User Principal Name in AD (i.e. user@domain.com).

**Vintela** - 3rd party SSO tool embedded in with Business Objects products since XIR2 SP2 to provide quick, easy SSO configuration. Since it is OEM'd no external products need to be installed for SSO to work.

### 3<sup>rd</sup> Party Troubleshooting Tools

**AD Explorer** – tool created by Microsoft Sysinternals, used to search and verify AD account attributes

**Kerbtray** – Microsoft utility used to display or purge kerberos tickets on a client workstation

**Kinit** - Provided with java SDK and JRE, it can verify krb5.ini configurations by submitting Authentication Service (AS) requests to the KDC

**MMC** - Microsoft Management Console can be accessed from any windows 2000/2003 server

**Packet Scanner** – The built in Microsoft Netmon, free 3rd party Wireshark, or other utility that can trace and record network packets between various hosts.

## Copyright

© Copyright 2011 SAP AG. 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 AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group 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.