Configuring Kerberos Manual Authentication and/or SSO in Distributed Environments (requires XI 3.1 SP3 or later)

Applies to:

Only XI 3.1 SP3 or later please see configuring Vintela SSO for earlier versions

Summary

This paper combines all the steps from the XI 3.1 admin guide(s) with the latest best practices and all the latest SAP KBs regarding vintela, kerberos and java AD configuration. **It is specifically written for XI 3.1 SP3 and will not work with earlier versions of XI.**

Author(s): Tim Ziemba BSEE, MCSE

Company: SAP Business Objects

Created on: 30 June 2010

Author Bio

IT/communications background prior to SAP/BO. Employed with SAP Business Objects Support in Lake Mary, FL since September 2005. Currently specializing in Authentication - XIR1, XIR2, XI 3.1 other areas include administration, migration, deployment and network troubleshooting.

Table of Contents

Please make sure you can perform the simple tests at the end of each section as they are designed in an order where 5 needs 4 which needs 3 which needs etc… Important notes are highlighted in RED code is in BLUE

Key Terms

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

AD – Active Directory – Microsoft's directory server based off LDAP

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

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

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

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

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

Vintela - 3rd party SSO tool packaged 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.

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

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 sam accountname except there can be multiple SPN's per account. The SPN is a primary access point for kerberos applications.

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

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

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

3rd Party Troubleshooting Tools

Kinit - Provided with java SDK and JRE, it can verify krb5.ini config by submitting AS requests to the KDC

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

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

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

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

NOTE: check out the references at the end of this document to links for the above tools and more.

Section 1- Planning your Service Account Configuration

Prior to configuring SSO you must create at least 1 service account. There are 3 completely separate roles for a service account. These roles can be combined on 1 account or shared across many. A best practice would be to use a common naming convention that will be introduced in this white paper. This can make troubleshooting easier and management simpler.

Role 1 - CMC – Query AD - Used by the CMS to perform LDAP searches against AD's directory servers (requires no delegation, no SPN, only read/query of AD). A typical domain user in AD will usually work. This account does not actually run any services or require any local permission unless combined with the CMS service account (if tracing the CMS then ensure this account can write to the logging directory). It is best if the password in of this account doesn't change in AD as when it does this functionality will be lost until the password is changed in the CMC.

Role 2 – SIA/CMS service account Used by the CMS to perform TGS requests against AD (Requires "act as part of the OS" policy, to be a member of the local Administrators group on every BOE server with a CMS, and an SPN is required but not delegation unless combined with role 3 or if used for SSO2DB.

Role 3 – java SSO account Used by tomcat or other java app server (enabled in web.xml) for launching the vintela filter. (Requires additional SPN's for all HTTP points of entry (web/apps, HLB, etc). This account does not actually run any services or require any local permission unless combined with role 2 above.

Naming Convention for service account(s) (only suggested but helpful for troubleshooting and administration)

A) **One service account for all 3 roles**/environments bossosvcacct

B) **One service accounts per role** (Use bocmcquery (1) bocmssvcacct (2) & bossoacct (3))

C) **One service account per environment** (Use bossosvcacctprod, bossosvcacctdev, bossosvcacctqa)

KEY to above naming convention - BO = Business Objects (all of the above), CMC = Central Management Console (just query account) SVC = Service (for accounts running the SIA), ACCT = account (all of the above), SSO = Single Sign On, PROD, QA, and DEV are just examples of customer environments as could be TEST or UAT as well.

You can have as many or as few service accounts as you would like. If SPN's are involved the less service accounts the less likely the chance for duplicate SPN's (this is an issue where AD cannot respond to kerberos requests due to conflict of the same aliases (SPN) created for multiple accounts). The per role option is excellent as well and will make tracing a little easier if packet scanning is required. **Questions can be posted on the SDN forums or open an incident with support component boj-bip-aut**

After planning you naming convention and service accounts then you are ready to create your service accounts. Service accounts will need to be created in Active Directory by a Domain Admin. For the rest of this document we will assume the all in 1 service account. Screenshots will be created with XI 3.1 SP3.

*****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 companies local AD/network Admins before attempting these steps**. The steps documented were tested in house, but your local AD admin is the only one familiar with your companies AD and its policies. If you admin has any questions arise please use the SDN forums or open a message with support.

Section 2 - Creating and preparing the service account

Suggestions for AD Domain Admin to create an account in AD. The following must be in place before you will be able to configure Business Objects for AD manual authentication or SSO.

NOTE: Since this document follows new workflows when enabling SSO. You should not combine the steps in this doc with any of our previous documents including my previous Vintela white papers unless specifically directed to another KB." This was designed for XI 3.1 SP3 and later only. Due to a different version of Vintela previous versions of XI will not work with this configuration..

On the next page screenshots depict the creation of an "all inclusive" service account

Account is bossosvcacct, password is set to never expire. Should a password expire, then the functionality dependant on that account will fail (see the roles above).

Some of our legacy Product Guides and Whitepapers required “Use DES encryption types for this account” to be enabled on kerberos service accounts (roles 2 and 3). **Do not select DES** as this white paper does not include the extra steps needed for DES to work and it is very weak encryption to begin with.

RC4 or AES will be used by default depending on the version and settings in AD.

Running setspn to create SPN’s for manual logon (CMS) and access points for SSO

Now we need to generate SPN(s) for all the SIA/CMS (to enable manual logon). No other SPN’s are needed if setting up manual logon only.

If using SSO clients, the web/app (if using a fixed IP) DNS redirects and hardware load balancers will also need SPN’s.

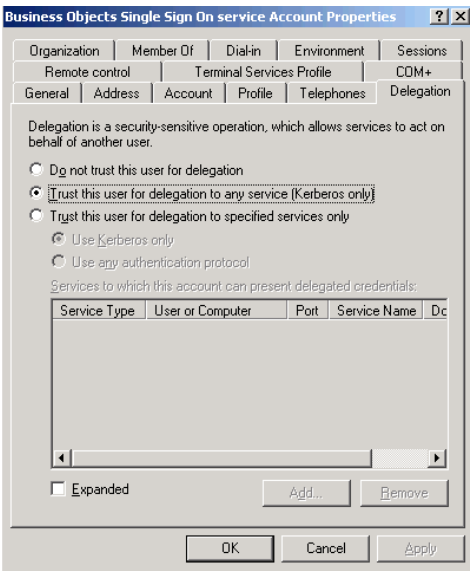
Background info: When an SSO client attempts to login to infoview it will use the URL (hostname/FQDN/IP) to generate a kerberos TGS HTTP/hostname/FQDN/IP requests respectively. In order for clients to make this request an SPN = to the hostname/FQDN/IP) must be added to the service account for it to succeed. Use the setspn command to create client SPN's or points of access for SSO. Format and examples provided on the next page

setspn –a BOCMS/serviceaccountname.serviceaccountdomain
The following SPN's are only needed for SSO
setspn –a HTTP/hostname of each tomcat or web/app server
setspn –a HTTP/FQDN of each tomcat tomcat or web/app server
Optional SPN's for server SSO and HLB's (if used)
setspn –a HTTP/ip.ip.ip.ip of each tomcat server to allow SSO to work on the server
setspn –a HTTP/otherFQDN/hostname/IP for any DNS redirects, or load balancers that will be used for SSO

Examples…

setspn –a BOCMS/bossosvcacct.vtiauth08.com bossosvcacct
The following SPN's are only needed for SSO
setspn –a HTTP/taz31 bossosvcacct
setspn –a HTTP/taz31.vtiauth08.com bossosvcacct
Optional SPN's for server SSO and HLB's (if used)
setspn –a HTTP/10.167.255.118 bossosvcacct
setspn –a HTTP/myloadbalancer bossosvcacct

HTTP SPN's are going to generally be needed in pairs (FQDN and hostname) or 3's (FQDN, hostname and IP). Each SPN acts as a point of entry for client requests. When performing SPNEGO (SSO) on the client the URL is used to generate a client TGS request. To note SSO always occurs on the client machine not BO or the web/app. If using SSO then delegation will need to be enabled.

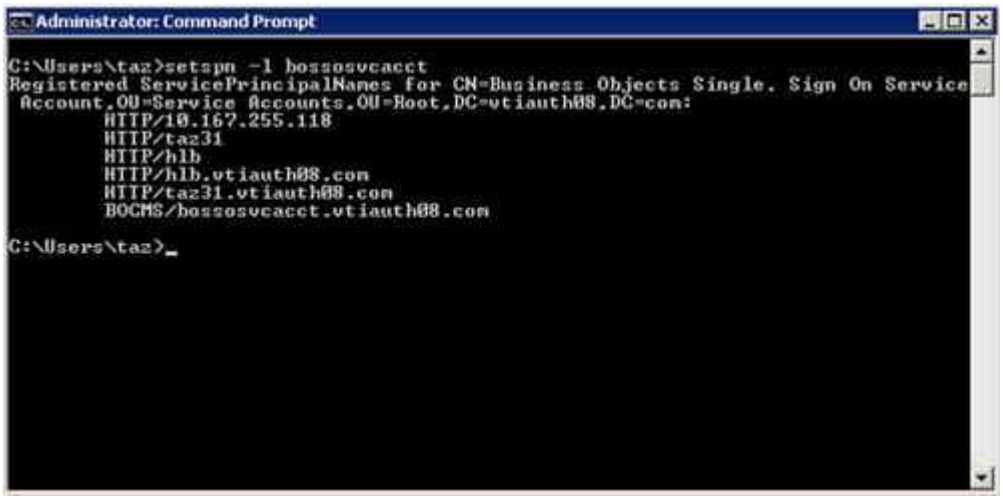


NOTE: This would also be a good time to verify delegation is enabled on the vintela SSO account. Screenshot above is in 2003 native. If using 2000 or mixed mode AD then look for a checkbox under the account properties. Delegation to specific services is referenced at the end of this document.

To View all created SPN's

When finished Run setspn –l bossosvcacct to view all created SPN's

Sample output below service account bossosvcacct has 3 SPN's for tomcat, 2 for an hlb, and 1 for the CMS

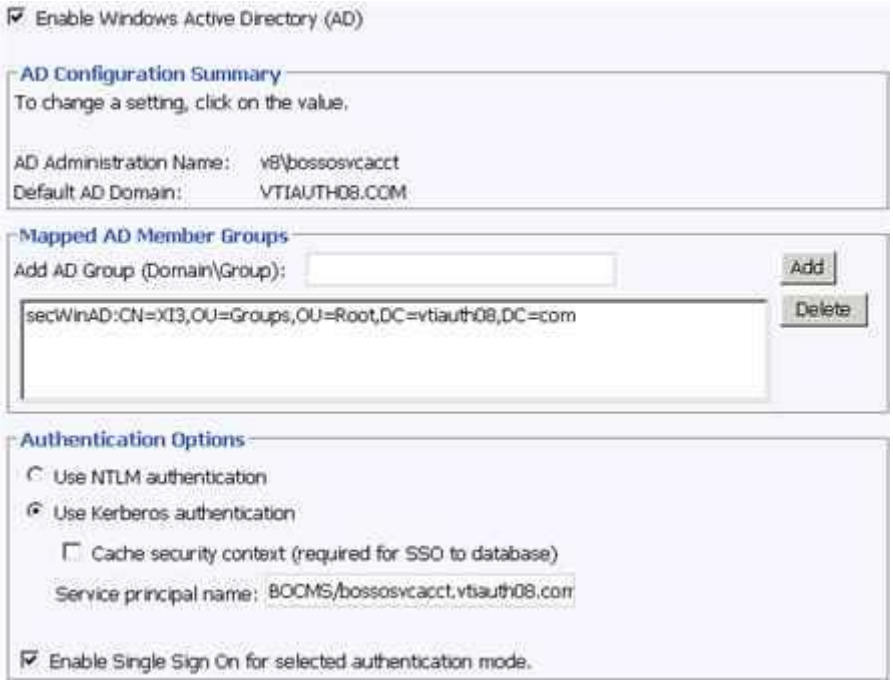


NOTE: When performing SPNEGO locally on a web/app it will default to NTLM and fail. A typical work around is to create an HTTP/ip.ip.ip.ip SPN and add it to the browsers **local intranet sites**. This will allow for testing SSO on the web/app.

At this point you can continue on to configure any and all Business Objects servers for manual authentication and /or SSO. The BOCMS/bossosvcacct.vtiauth08.com SPN can be used to configure manual AD authentication (CMC-SPN) and is also used for SSO (if needed).

Section 3 - Steps to configure the CMC and map in AD groups

The following steps are also explained in more detail on the XI3.1 Admin guide. Included are the key points in this document to verify they are complete and help avoid some common mistakes.



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 not 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. **Should exactly match default domain in the krb5.ini** mentioned later in the document.

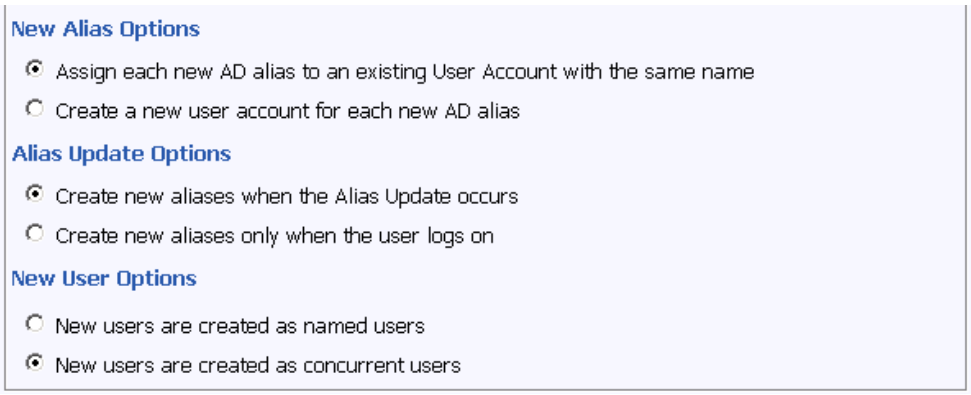
Mapped AD Member Groups If a group is in the default domain it can be usually be added with just the group name. If it's in another domain or (after 3.1 is released) another forest then it will need to be added in domain\group or DN format. Once added hit update and the groups will appear as above (secWinAD: DN) regardless of how they were entered (group, domain\group, or DN).

If having difficulty mapping in groups please see KB 1199995 for UseFQDNForDirectoryServers or KB 147634 for additional troubleshooting.

Authentication Options Kerberos must be selected for manual java or SSO. NTLM is only supported for .net (IIS and non java client tools)

The Service Principal Name or SPN MUST be the value created on the service account that runs the SIA/CMS either via setspn (discussed in section 2 of this doc)

Enable Single Sign On should be selected if using SSO



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 infoview/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/groups, select the group you mapped in, and view 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 member AD groups).

Do not proceed to setting up the service account if users and or groups are not mapping in properly

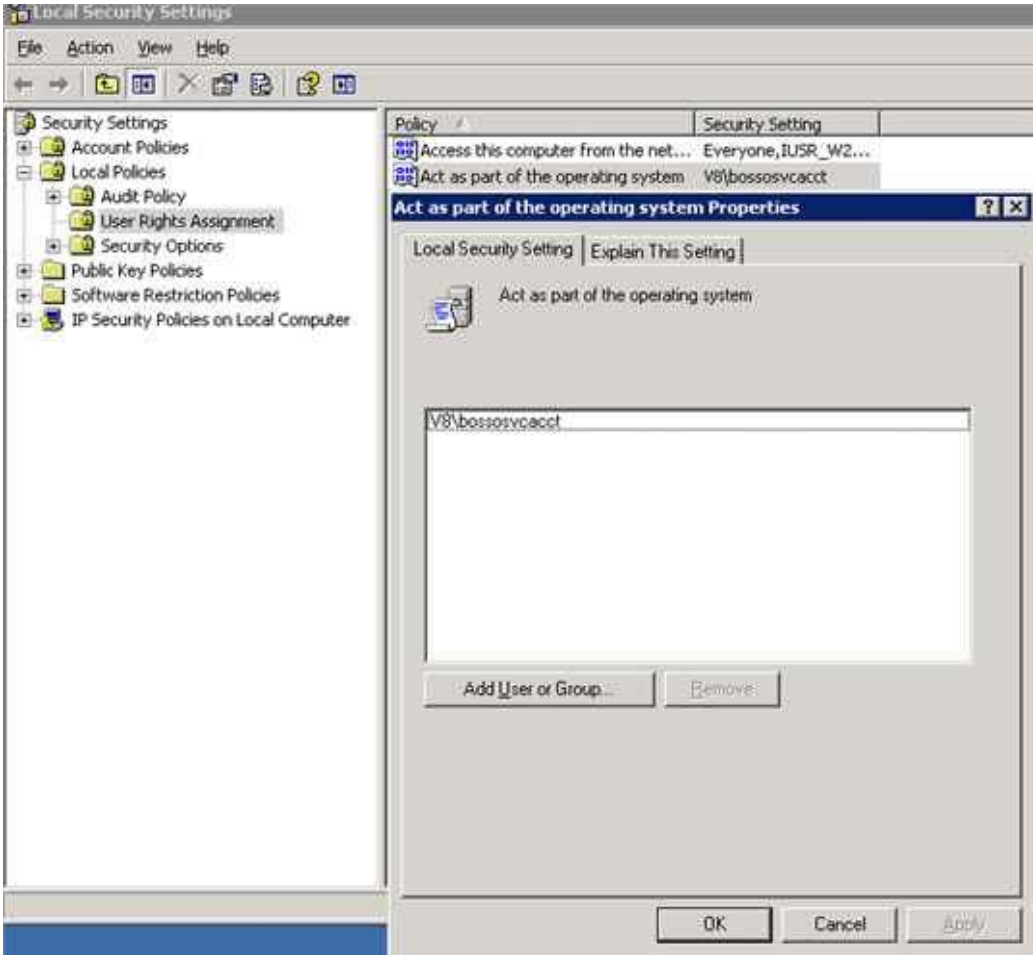
Section 4 — Steps to start the SIA/CMS under the service account

This service account was described in role2 (section1)

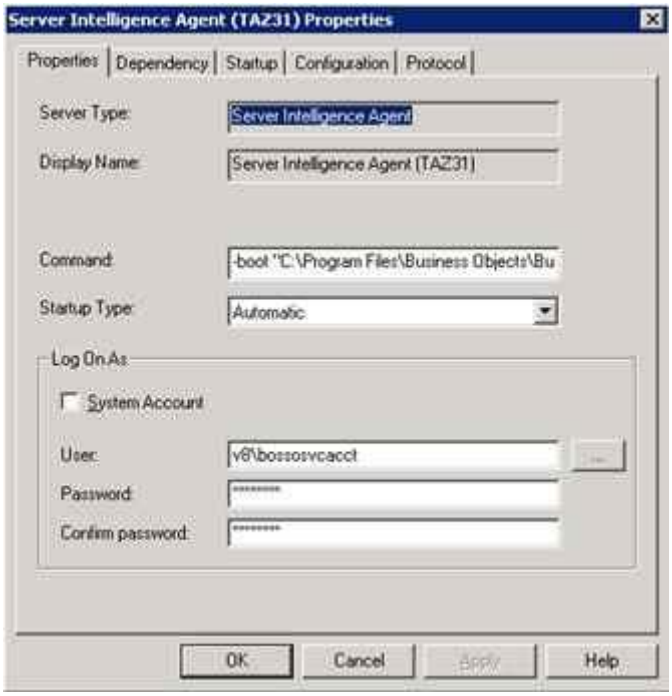
Add the service account to the **local administrator's group on any server where the service account will be running a SIA/CMS.**

NOTE: Is 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. Specific permissions other than administrator have not been calculated at this time.

You should also grant the local policy **Act as Part of the operating system** as seen in the screenshot of the local policy editor on the next page.



After the above changes have been made then the service account can now run the SIA/CMS. This works best when the account is entered in domain\username format.



```
Command Prompt
C:\Documents and Settings\taz>SET
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\taz\Application Data
CLIENTNAME=MCON00458210A
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=TAZ31
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\taz
LOGONSERVER=\\W2K8DC1
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 29 Stepping 8, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=1d08
ProgramFiles=C:\Program Files
PROMPT=$P$G
SESSIONNAME=RDP-Tcp#1
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\taz\LOCALS~1\Temp\1
TMP=C:\DOCUME~1\taz\LOCALS~1\Temp\1
USERDNSDOMAIN=VTIAUTH08.COM
USERDOMAIN=V8
USERNAME=taz
USERPROFILE=C:\Documents and Settings\taz
windir=C:\WINDOWS

C:\Documents and Settings\taz>_
```

NOTE: If the SIA/CMS should fail to start look in the event viewer, search KBs, forums, or open a message with support.

To verify the service account is working

You should be able to login via client tools (deski, designer, business views, CCM, etc) at this point. If an error occurs please search our KB/notes if you have an error code or open a message with support**.**

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

Section 5 – Setting up the java SDK for AD

2 files need to be created when using java SDK.

These files need to be created from scratch (the 1st time) and should be placed in the C:\winnt directory on any windows WEB/APP. This path should be where the java SDK will look by default.

NOTE: C:\winnt does not exist by default and will need to be created in most cases
You can copy the default krb5.ini as well (but it will need to be modified with environment info)

bsclogin.conf – to load the java login module and trace login requests.

You can copy the default bsclogin file from below (replace sun with ibm is using websphere or when the web/app is on AIX)

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

krb5.ini – to configure the KDC's that will be used for the java SDK login requests

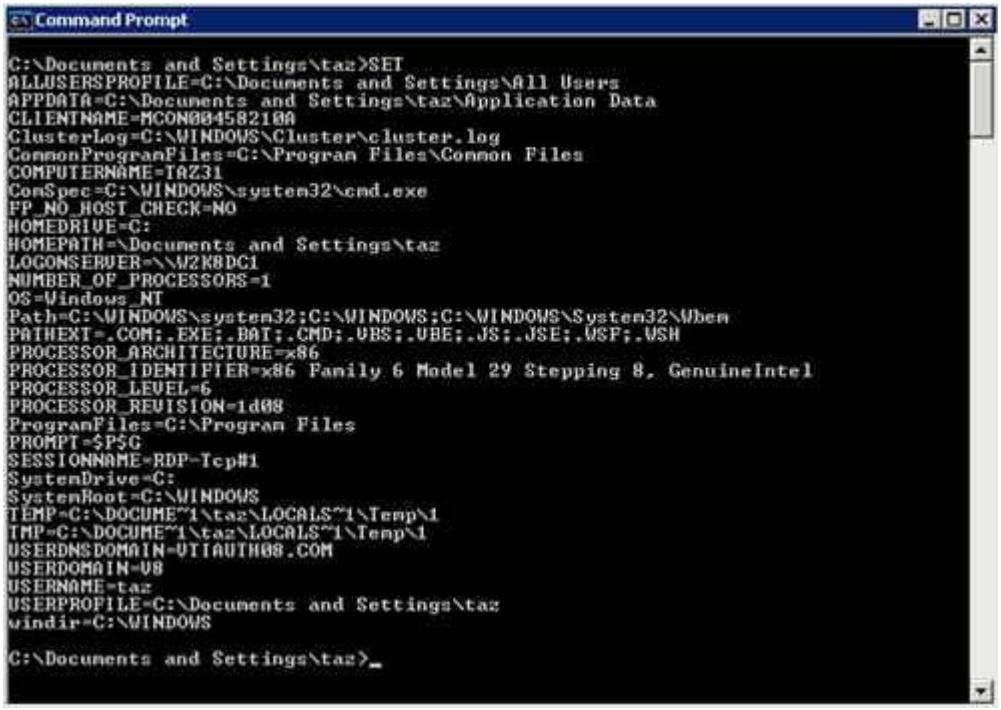
```
[libdefaults]
default_realm = MYDOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tgs_enctypes = rc4-hmac
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1
[realms]
MYDOMAIN.COM = {
kdc = MYDCHOSTNAME.MYDOMAIN.COM
default_domain = MYDOMAIN.COM
}
```

There are 4 values that need to be changed in the above file.

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.

Replace MYDCHOSTNAME with the hostname or a domain controller.

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



Using this set command the logonserver is W2K8DC1 and DNS Domain is VTIAUTH08.COM

Example of a populated krb5.ini on the next page

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

To verify the krb5.ini can successfully receive a ticket (this does not verify multi-domain issues)

navigate from DOS command line to the Boinstall\javasdk\bin directory. By default this is c:\program files\business objects\javasdk\bin

Run kinit username hit enter and type your password

If the KDC in the krb5.ini is correct you should receive a ticket

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

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. And Key Distribution Center (KDC) service must be running on port 88.

Common errors.

Preauthentication = invalid password

KDC for realm – means the KDC in the krb5.ini file did not respond

Client not found in kerberos database – bad username

See **KB 1476374** for additional troubleshooting and a list best practices

KB's 1245178 and **1429745** for advanced krb5.ini settings

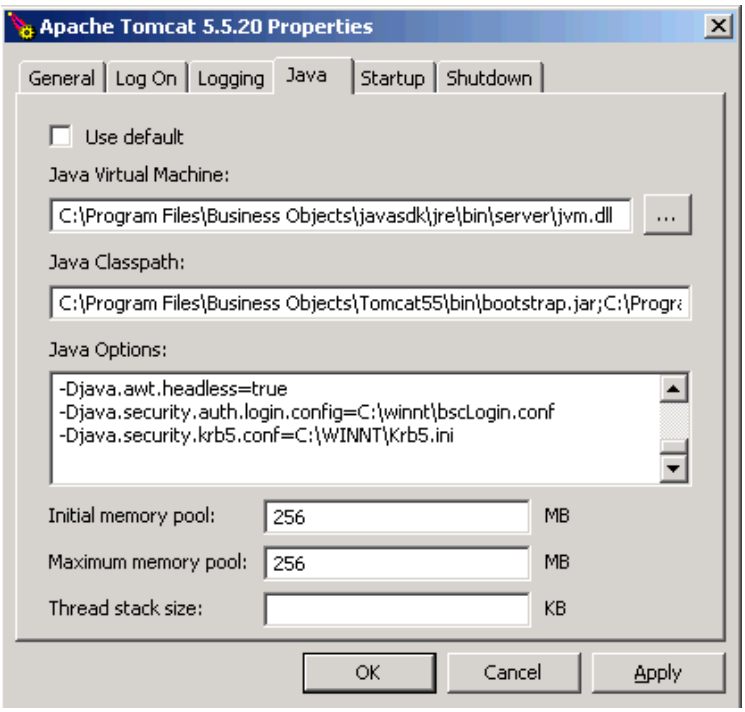
Only after you successfully get a ticket should you move on to configuring java infoview/CMC

Section 6 – Configuring java Infoview and CMC (3.1 or later)

In order for InfoView to work you must ensure your web/app has access to the bsclogin.conf and krb5.ini. The steps to accomplish this will vary depending on web/app. For this document we will assume the default tomcat is being used.

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

```
-Djava.security.auth.login.config=c:\winnt\bsclogin.conf
-Djava.security.krb5.conf=c:\winnt\krb5.ini
```



Verify bsclogin.conf was added properly

After the restart the bsclogin (with debug=true option from earlier) will force user logon attempts to show up in the std.out. This is a very un-intrusive level of tracing (leave this enabled during initial config or on test machines). To verify the path is correct attempt to logon to infoview (with AD selected in the drop down) then view the std.out, scroll to the end and the username should appear in username@REALM.COM

If you have a **commit succeeded** then the java SDK portion is working for infoview. At this point a successful test user will be able to login to java infoview and CMC.

If usernames are not showing up in the std.out then the bsclogin.conf is not loading properly. Look for typos, syntax errors, etc. You may need to enable java verbose tracing for additional errors in the troubleshooting section of this guide

If you can see the username and have a commit succeeded but still cannot login see **KB 1476374** for additional troubleshooting, **KB's 1245178** and **1429745** for advanced krb5.ini settings,post on the SDN forums or open a message with support under component boj-bip-aut.

Enable SDK tracing if needed with the following java option

-Dbobj.logging.log4j.config=verbose.properties

This logging creates a very large log file for general tomcat tracing. I have verified that it will log errors such as a typo in the bsclogin.conf file. Check the log after a manual logon attempt

The log files are located in documents and settings\tomcat user\.businessobjects

If having trouble finding the logs run tomcat under the service account

-Dsun.security.krb5.debug=true

The –Dsun logging will add additional levels of Kerberos trace information

If you only want manual AD logon then at this point you are done!

Do not proceed on to the next section unless manual logon is working!

Section 7 – Configuring and testing SSO server side (web.xml and server.xml)

Server.xml — For Tomcat servers it is necessary to increase the default HTTP Header size in the server.xml. Kerberos login requests contain group information and this requires a larger header size. 16384 is usually large enough but if your AD contains users that are a member of many groups (50 or more AD groups). You may need to increase this size to 32768.

Default path is c:\program files\business objects\tomcat55\conf\server.xml

NOTE: Make a backup copy of any XML files prior to editing

In the server.xml you will want to define any "non-SSL HTTP/1.1 Connector on port 8080" or "SSL HTTP/1.1 Connector on port 8443" (if using SSL) have **maxHttpHeaderSize="16384"** or higher (if needed).

Sample

```
<!—Define a non-SSL HTTP/1.1 Connector on port 8080 →

<Connector URIEncoding="UTF-8" acceptCount="100" connectionTimeout="20000"
disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="16384"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="8080" redirectPort="8443"/>
```

Web.xml – This is where the vintela filter is enabled. The changes below consider a default web.xml.

Default path is c:\program files\business objects\tomcat55\InfoViewApp\WEB-INF\web.xml

In most cases when using SSO you will want to change your authentication default to secWinAD, siteminder, must be set to false, and vintela to true

Sample

```
<context-param>
   <param-name>authentication.default</param-name>
   <param-value>secWinAD</param-value>
</context-param>

<context-param>
   <param-name>siteminder.enabled</param-name>
   <param-value>false</param-value>
</context-param>

<context-param>
   <param-name>vintela.enabled</param-name>
   <param-value>true</param-value>
</context-param>
```

On the next page

1. Remove open and close comments from auth filter (bold <!-- →)
2. Set the idm.realm to your service account domain. MUST be in ALL CAPS
3. Set your idm.princ to the service account
4. Comment out the legacy logging (bold <!-- →)

```
<!—
<filter>
   <filter-name>authFilter</filter-name>
   <filter-class>com.businessobjects.sdk.credential.WrappedResponseAuthFilter</filter-class>
   <init-param>
      <param-name>idm.realm</param-name>
      <param-value>VTIAUTH08.COM</param-value>
   </init-param>
   <init-param>
      <param-name>idm.princ</param-name>
      <param-value>bossosvcacct</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>
<!—
   <init-param>
      <param-name>idm.logger.name</param-name>
      <param-value>simple</param-value>
      <description>
         The unique name for this logger.
      </description>
   </init-param>
   <init-param>
      <param-name>idm.logger.props</param-name>
      <param-value>error-log.properties</param-value>
      <description>
         Configures logging from the specified file.
      </description>
   </init-param>
 →
   <init-param>
      <param-name>error.page</param-name>
      <param-value>../logonNoSso.jsp</param-value>
      <description>
         The URL of the page to show if an error occurs during authentication.
      </description>
   </init-param>
</filter>
 →
```

You must also remove the comments from the filter mapping (separate section)

```
<!--
<filter-mapping>
   <filter-name>authFilter</filter-name>
   <url-pattern>/logon/logonService.do</url-pattern>
</filter-mapping>
-->
```

Save the web.xml

NOTE: If in the same cluster deployed on the exact same version/patch then this file can be copied between machines. It may be copied from different environments again if the product/version are exactly the same and the CMS name is modified to = the destination environment.

It may not be copied if any patch is different, or any different/additional products (that modify the .war files) have been installed

Verifying web.xml settings

If the settings don't seem to have an effect, open the web.xml with a browser such as IE. Review the changed settings (the values what are uncommented should show up in dark text. Commented values will appear grayed out).

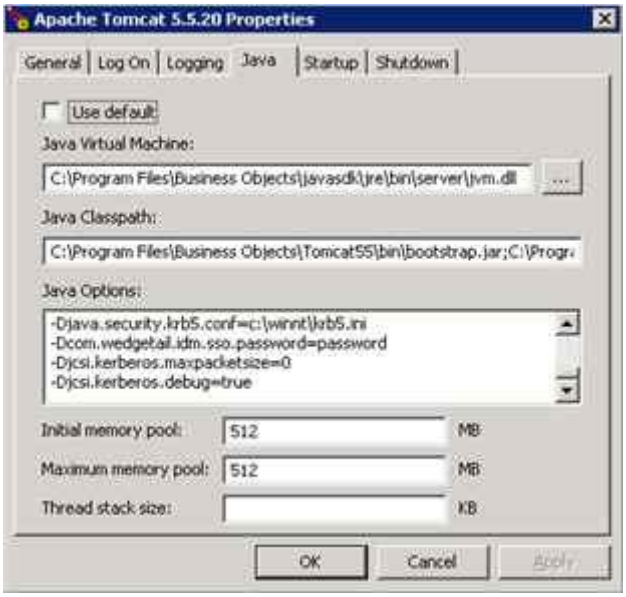
Configuring Java Options for vintela server components

Then 2 more options must be added to the tomcat java options

The wedgetail.sso.password is the password for the vintela SSO account

The DJCSI.kerberos.debug options will enable a start up trace of the vintela filter.

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



Verifying the vintela filter is loaded successfully

stop tomcat, delete, or move the C:\program file\business objects\tomcat55\logs*.*

restart tomcat, wait 10-20 seconds or so (to allow the vintela filter to initialize). Search the std.out for "credentials obtained" (without the "") for the bossosvcacct@VTIAUTH08.COM.

If the credentials are obtained then vintela filter is loading successfully. You may proceed attempt to test SSO from the client machines or from the server with the IP

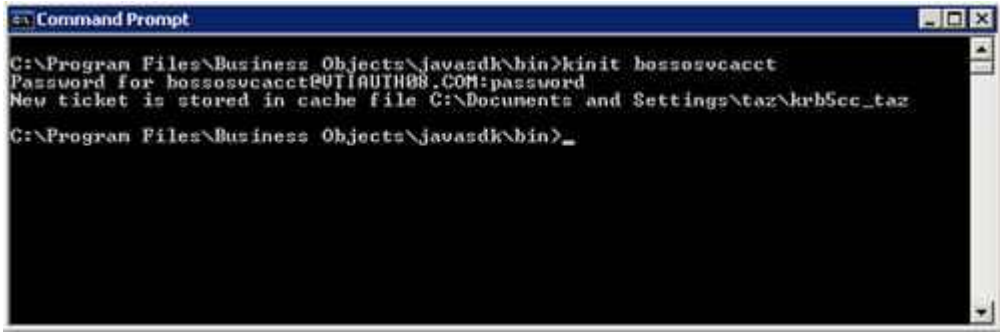
NOTE: must have an IP SPN defined in section 2 and use the IP address in the URL

Verifying a valid vintela idm.princ@IDM.REALM

If credentials are not obtained then you can test by running kinit (same steps as earlier)

```
C:\program files\business objects\javasdk\bin\kinit bossosvcacct
```

Sample success in the screenshot below



If you receive any errors please search our KBs, the forums, or open a message with support

When kinit works, and credentials are obtained in the std.out then we can finish the configuration by testing SSO from the client side

Make sure the browser is setup properly for client side testing **KB 1379894** (IE) and **KB 1263764** (firefox)

Troubleshooting client side issues must be done with 3rd party tools since SSO occurs external to business Objects and the web/app. **KB 1370926** will create log files. Open a message with support if you need help interpreting them under boj-bip-aut

Section 8 – Additional information and settings

Detailed troubleshooting and best practices can be found in **KB 1476374**

For manual logon use http://server:port/InfoViewApp/logonNoSso.jsp

If using multiple forests check **KB 1323391**

Additional Steps - Cleanup tracing, add keytab, Constrained Delegation

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

debug=true in the bsclogin.conf (set by default in section 5 you can also leave this on it's non-intrusive)

-Dbobj.logging.log4j.config=verbose.properties (may have been added to java options turn it off)

-Djcsi.kerberos.debug=true java option (set by default in section 7 also turn off when not needed)

Dcom.wedgetail.idm.sso.password=pw (**only remove when you have a valid keytab configured below**)

Switch Tomcat 5.5 back to local system (if running under service account for verbose tracing)

Do not setup constrained delegation or the keytab until SSO is verified working as troubleshooting is much more difficult when trying to add these too.

Encrypting your service account password with a keytab

Create a keytab with ktpass (found on DC's and can be downloaded from Microsoft)

```
ktpass -out bosso.keytab -princ serviceaccount@REALM.COM –pass user_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
```

Copy the bosso.keytab to the c:\winnt directory then add the following 4 lines in the web.xml (after the idm.princ setting). Once this is added you can remove the wedgetail.password option from the tomcat java options. At this point your vintela SSO account password will now be encrypted with RC4.

```
<init-param>
<param-name>idm.keytab</param-name>
<param-value>c:\winnt\bosso.keytab</param-value>
</init-param>
```

If you receive RC4 errors then you may need to get a newer version of ktpass from Microsoft. Please consult Microsoft regarding ktpass errors

See **KB 1359035** to test the keytab separately if SSO stops upon adding this setting

Setting up Constrained Delegation

See **KB 1184989** for setting up **constrained delegation** most steps are in Microsoft 1 in the web.xml

References

XI 3.1 Admin Guide http://help.sap.com/businessobject/product_guides/boexir3/en/xi3_bip_admin_en.pdf

ADExplorer http://technet.microsoft.com/en-us/sysinternals/bb963907

Netmon 3.2 http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=f4db40af-1e08-4a21-a26b-ec2f4dc4190d&displaylang=en

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

Additional Notes

AD 2008 functional level 2003 BO server Windows 2008 server SP2 for the CMS and tomcat (3rd party)

XI 3.1 SP3 Tomcat 5.5 (integrated) Java 1.5 (integrated) VSJ 3.3 (integrated)

Copyright