UNIVERSAL TECHNICAL INSTITUTE

Auto
Diesel
Collision
Marine
Motorcycle

Chosen by Industry. Ready to Work.

UPGRADING TO XI 3.1 SP6 AND SINGLE SIGN ON

Chad Watson

Sr. Business Intelligence Developer

UPGRADING TO XI 3.1 SP6

What Business Objects Administrators should consider before installing a Service Pack.

SP6 Upgrade Considerations

- SAP BusinessObjects XI 3.1 Edge
- Upgraded from SP3 FP 5 to SP6
- The upgrade will overwrite any configuration files in the tomcat directory
- Back up any customizations you have made to any of the Business Objects applications
  - I like to back up the entire tomcat directory
- Back up any updates to the Tomcat Java Options settings (For example, if you use SSO)
- Back up the CMS and Audit databases, as well as the Input and Output repositories
- Make a snapshot of the server if it is virtual
- When upgrading to SP6 from SP3 you have to install SP 4 or 5 first, then you can install SP6

SINGLE SIGN ON (SSO) STEPS

1. Planning your Service account Configuration
2. Creating and preparing the service account for kerberos delegation
3. Steps to configure the CMC and map in AD groups
4. Steps to start the SIA/CMS under the service account
5. Logging into java apps
6. Configuring java for Infoview and CMC
7. Configuring and testing vintela SSO server side
8. Tracing tomcat, & packet scanning client SSO issues
9. Additional Steps - Cleanup tracing, add keytab, and forcing an AD site

A few key terms

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.

JAS – a take off from WAS - Web Application Server - but in this context we are referring to Java Application Servers ONLY in order to differentiate from IIS .net and other JAS (tomcat, Websphere, Weblogic, Jboss, Oracle App Server, etc)

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

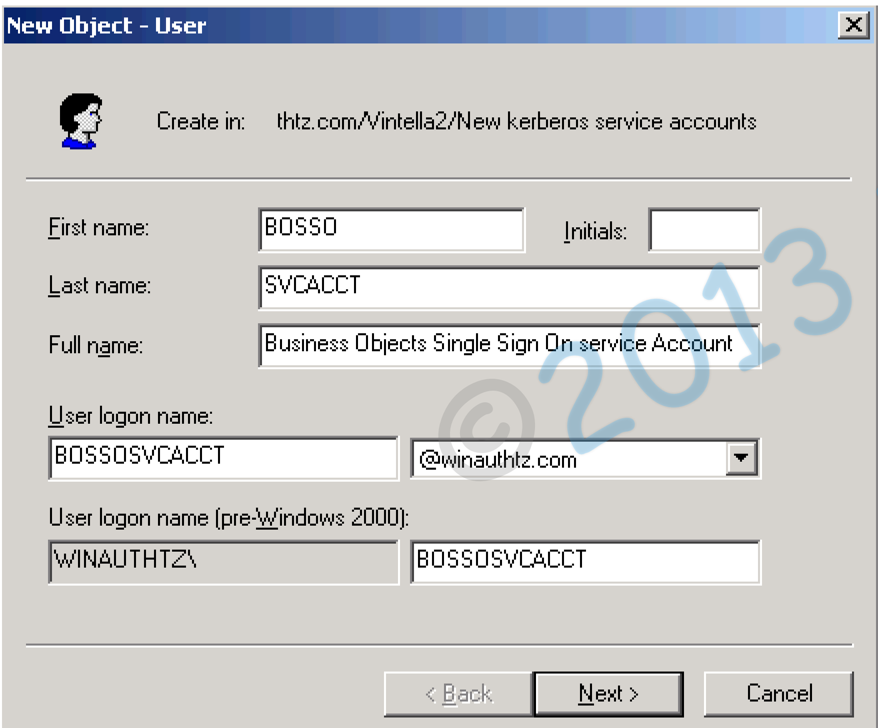
1. Planning your Service account Configuration

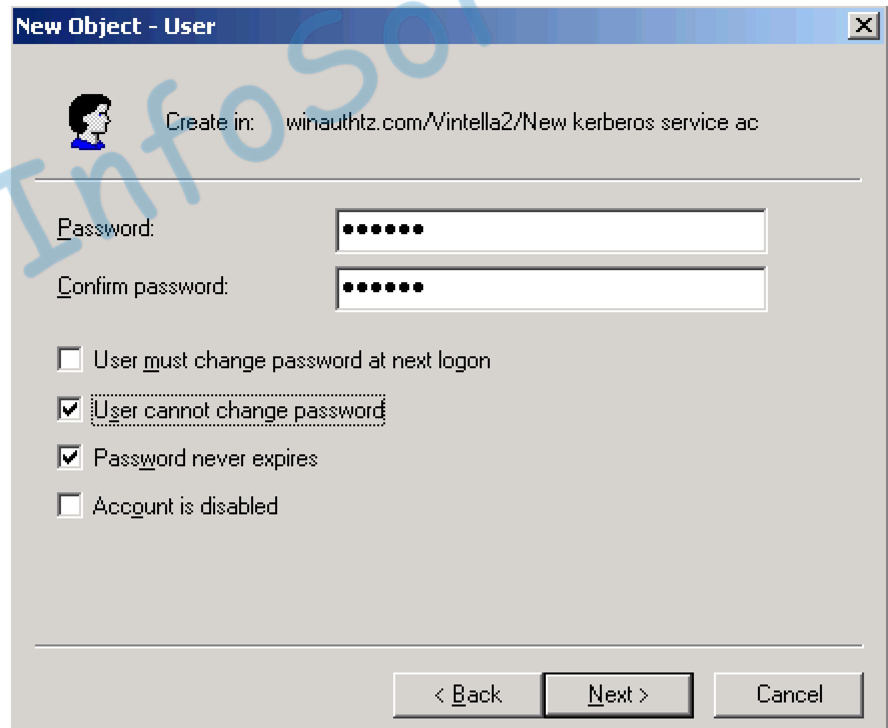
- **Role 1 – CMC – Query AD** Used by the CMS to perform LDAP searches against AD's directory servers
- **Role 2 – CMS/SIA service account** Used by the CMS to perform TGS requests against the KDC
- **Role 3 – Vintela SSO account** Used by JAS (enabled in web.xml) for launching the vintela filter

- **One service account can be used for all three roles. This makes troubleshooting easier.**

2. Creating and preparing the service account for kerberos delegation

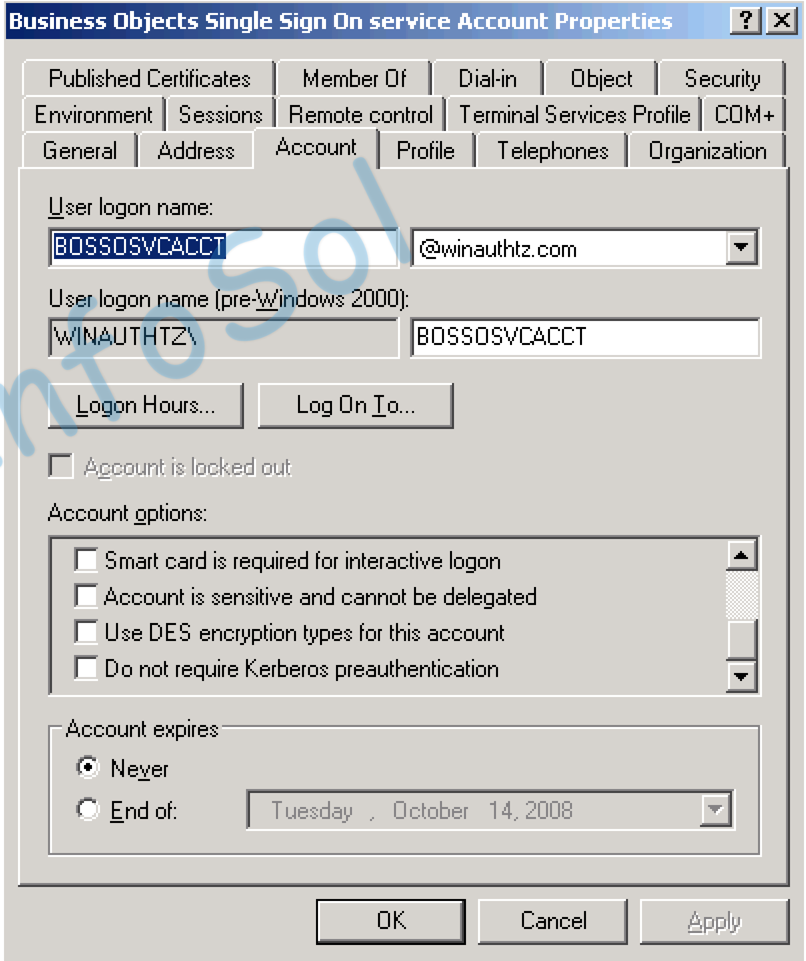
- Creation of an “all inclusive” service account
- Set password to never expire





Creating and preparing the service account for kerberos delegation (cont.)

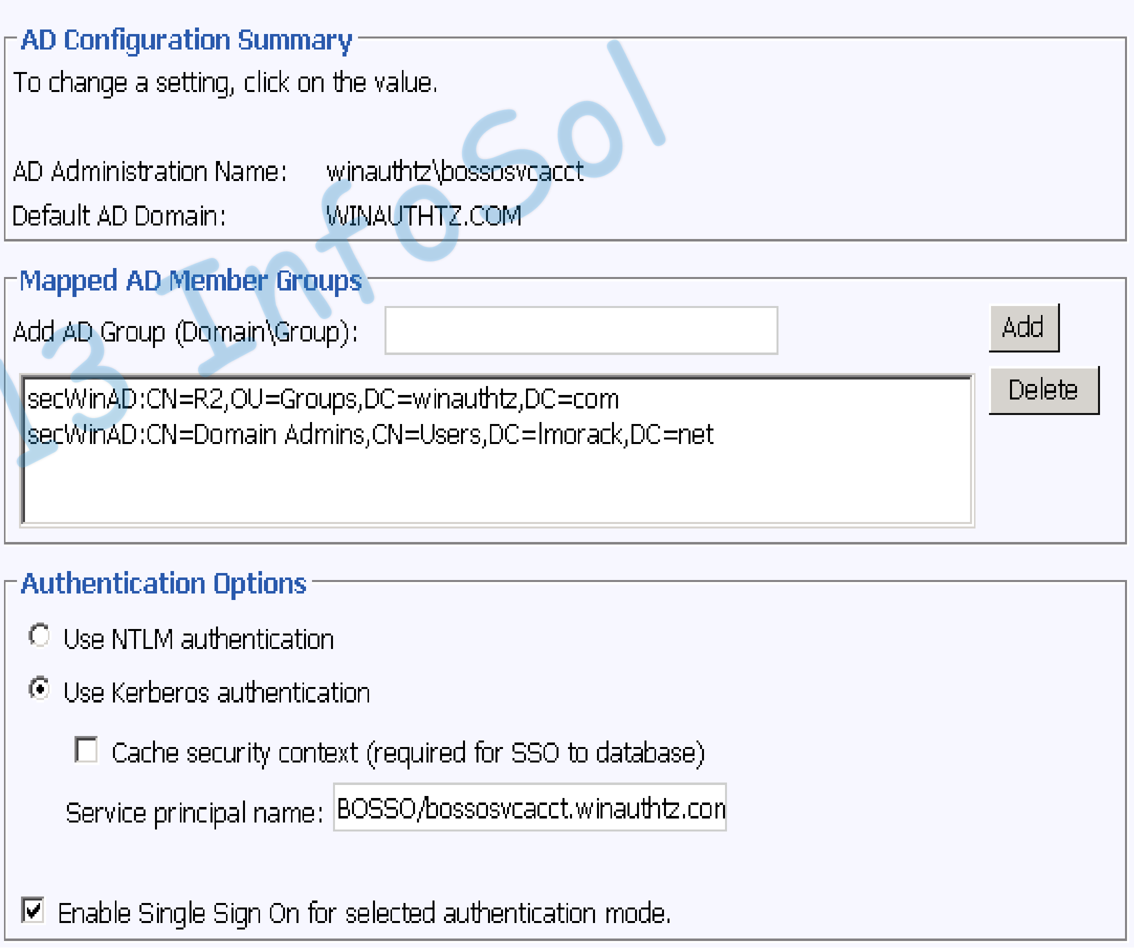
- Account is BOSSOSVCACCT, **password is set to never expire**. Should a password expire, then the functionality dependant on that account will fail. You will also need to enable delegation after running ktpass



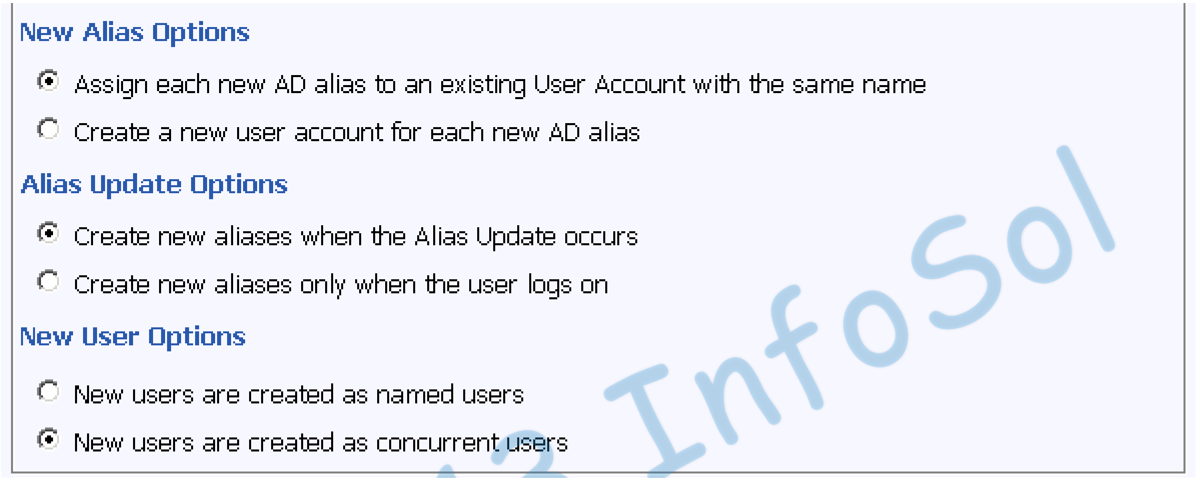
3. Steps to configure the CMC and map in AD groups

- **The AD administration Name** is the account mentioned in role 1 earlier
- **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

- **Mapped AD Member Groups** If a group is in the default domain it can be usually be added with just the group name.
- **Authentication Options** Kerberos must be selected java SSO does not support NTLM.
- **The Service Principal Name** or SPN MUST be the value created on the service account either by ktpass or setspn (discussed later in this doc)
- **Enable Single Sign On** should be selected as well.



Steps to configure the CMC and map in AD groups (cont.)

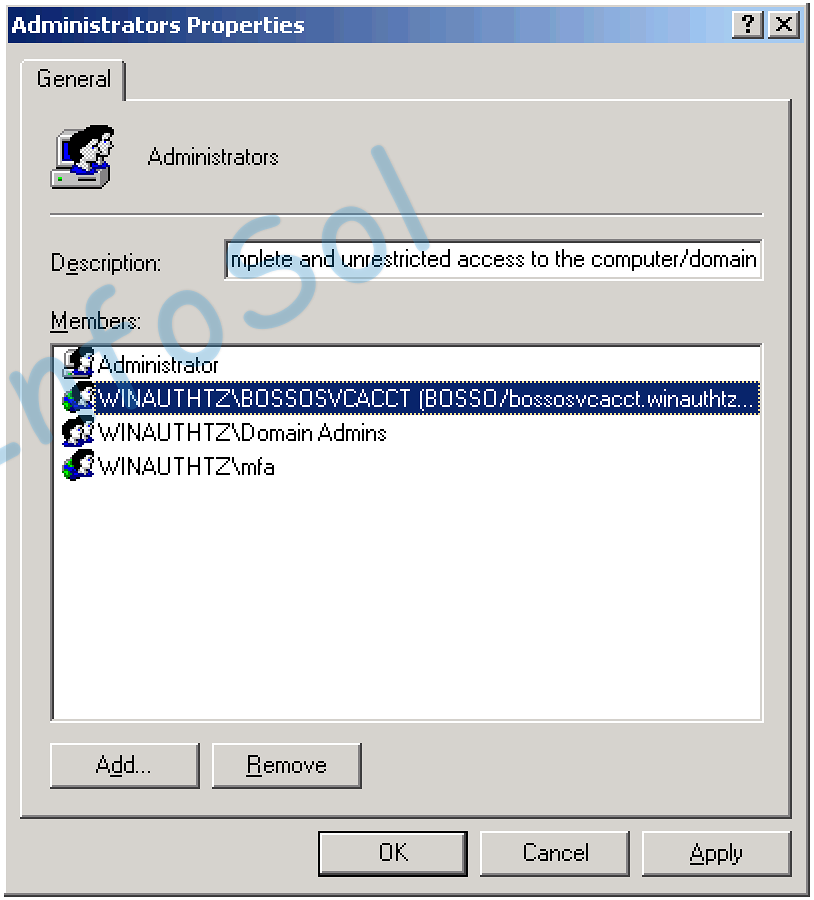


- **New Alias Options** determine how the user will be created if an existing user with the same name (LDAP/NT/Enterprise) already exists.
- **Alias Update Options** determine if users will be added when pressing the update button or only after they have logged into infoview/CMC/client tools
- **New 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.

4. Steps to start the SIA/CMS under the service account

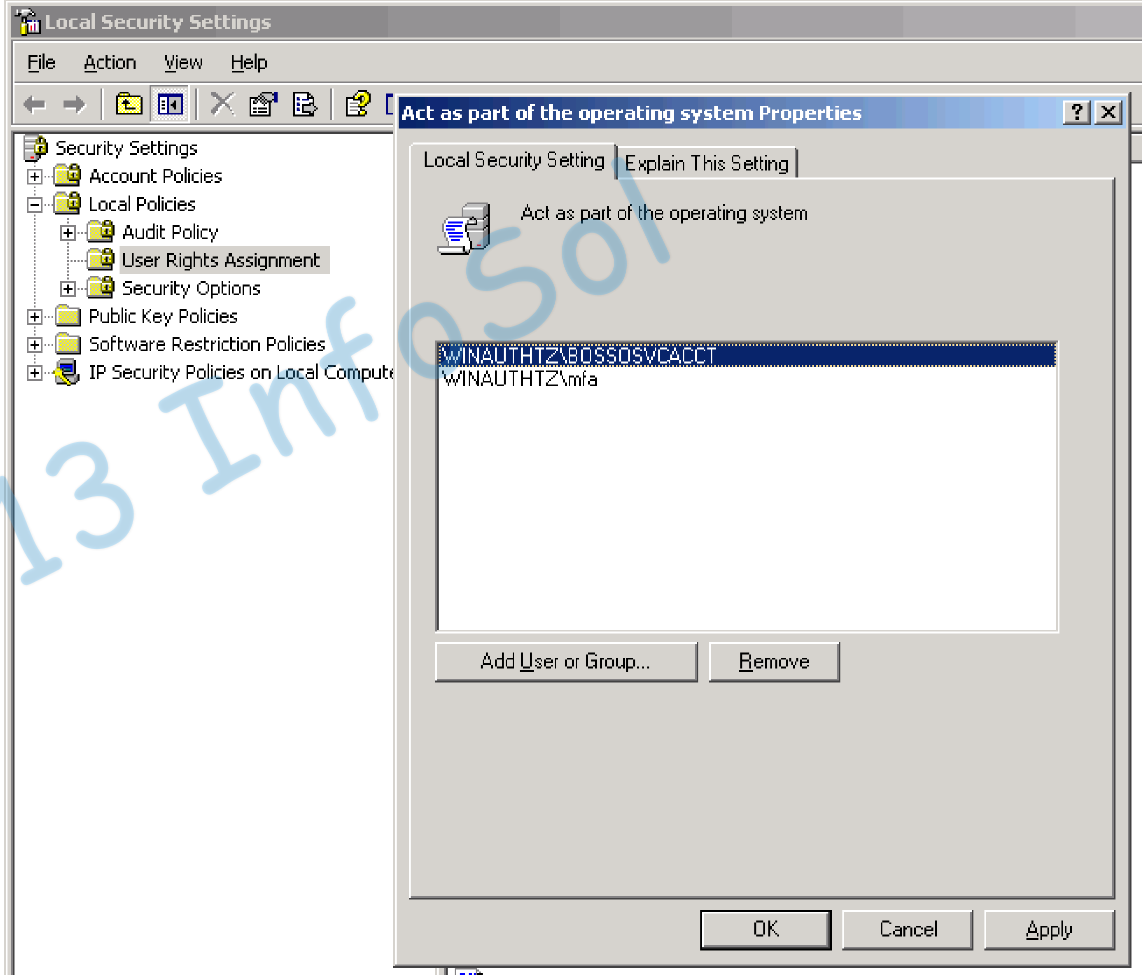
This service account was described in Role 2 (Planning section)

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



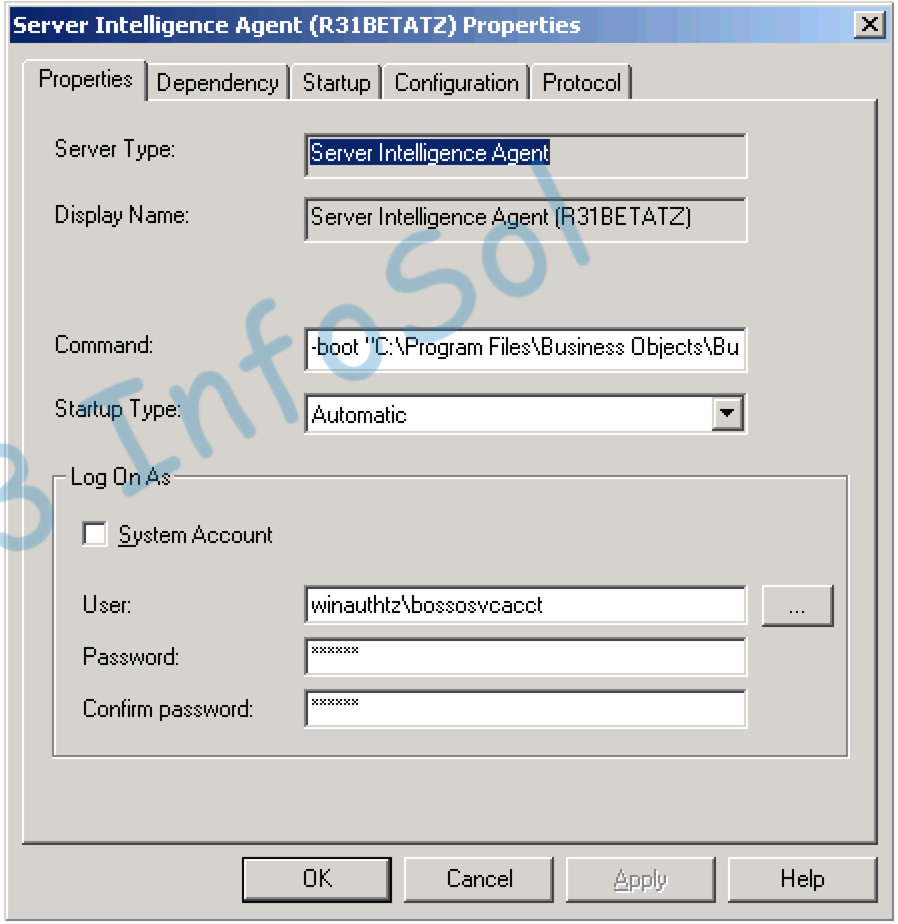
Steps to start the SIA/CMS under the service account (cont.)

- You should also grant the local policy **Act as Part of the operating system**



Steps to start the SIA/CMS under the service account (cont.)

- The service account can now run the SIA/CMS
- This works best when the account is entered in domain\username format.
- You should be able to log into client tools using the service account to validate that the account is working properly.



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

5. Logging into java apps

Two additional files are needed for logging into a java apps.

- These files need to be created from scratch (the 1st time) and should be placed in the **C:\winnt** directory. 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

- **bsclogin.conf** – to load the java login module and trace login requests. (replace sun with ibm if using websphere)

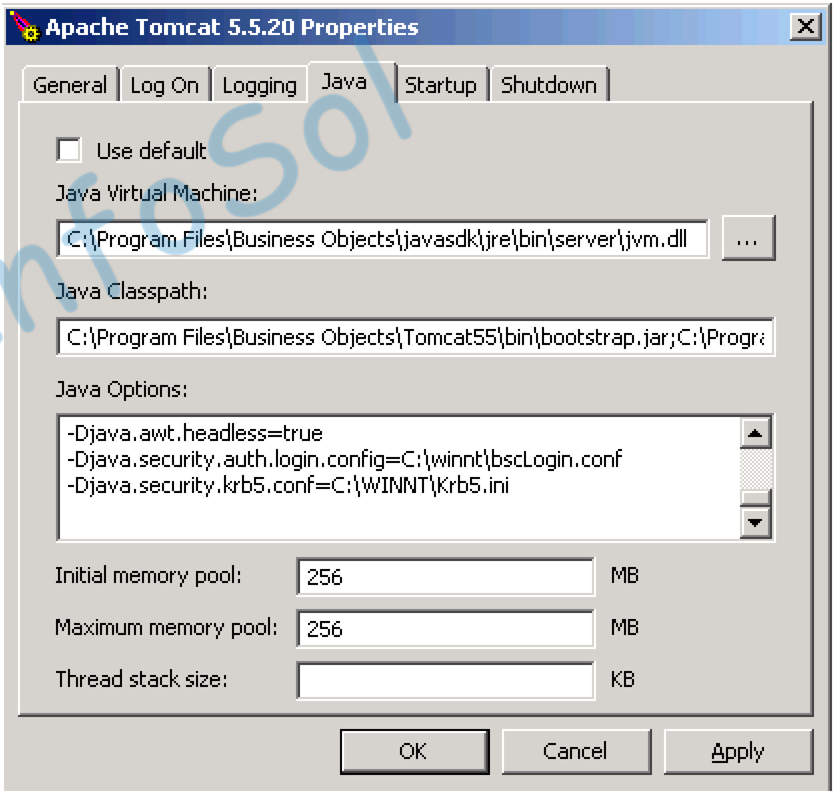
```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required debug=true;
};
```

- **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
udp_preference_limit = 1
[realms]
MYDOMAIN.COM = {
kdc = MYDCHOSTNAME.MYDOMAIN.COM
default_domain = MYDOMAIN.COM
}
```

6. Configuring java for Infoview and CMC

- 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**



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

NOTE: Make a backup copy of any XML files prior to editing to insure default values can always be retrieved

- **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 than default 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.
- Default path is c:\program files\business objects\tomcat**55**\conf\server.xml
- 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”/>
```

Configuring and testing vintela SSO server side (web.xml and server.xml) (cont.)

NOTE: Make a backup copy of any XML files prior to editing to insure default values can always be retrieved

- **Web.xml** – This is where the vintela filter is enabled. The changes below consider a default 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>
```

Configuring and testing vintela SSO server side (web.xml and server.xml) (cont.)

- Remove open and close comments from auth filter (bold <!-- -->)
- Set the idm.realm to your default REALM (the one from the ktpass step) MUST be in ALL CAPS
- Set your idm.princ to the default SPN (also from the ktpass step)

```
<!--
<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>WINAUTHTZ.COM</param-value>
        </init-param>
        <init-param>
                <param-name>idm.princ</param-name>
                <param-value>BOSSO/bossosvcacct.winauthtz.com</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>
```

Configuring and testing vintela SSO server side (web.xml and server.xml) (cont.)

```
    </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>
-->
```

Configuring and testing vintela SSO server side (web.xml and server.xml) (cont.)

- 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

- You can also do this to other applications, such as the OpenDocument web.xml to use SSO when you use an OpenDocument call.

Student Information System OpenDocument Call with SSO.

Web.ini location:

Program Files\Business Objects\Tomcat55\webapps\OpenDocument

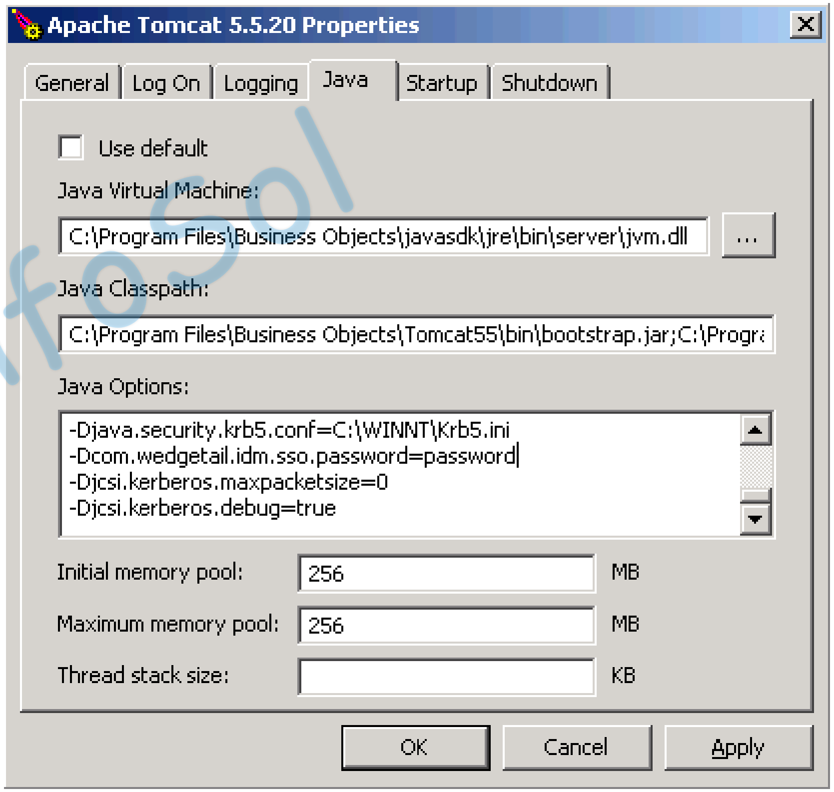
Open Document Call:

http://BOESERVER/OpenDocument/opendoc/
openDocument.jsp?
iDocID=AZZKrwZADnXzI2MqYQ
&sIDType=CUID

SIS Demonstration

Configuring and testing vintela SSO server side (web.xml and server.xml) (cont.)

- Then 3 more options must be added to the tomcat java options
- The wedgetail.sso.password is the password for the vintela SSO account (ktpass step earlier)
- The max packet size will force SSO clients to use TCP
- The DJCSI.kerberos.debug options will enable a start up trace of the vintela filter.
  - **-Dcom.wedgetail.idm.sso.password=*password***
  - **-Djcsi.kerberos.maxpacketsize=0**
  - **-Djcsi.kerberos.debug=true**



8. Tracing tomcat, & packet scanning client SSO issues

At this point you should have manual AD authorization working for all applications (including infoview), the vintela filter loaded, and tested on the server. If not please finish the earlier sections before attempting to troubleshoot SSO

The following tracing options were tested in 3.1 with tomcat 5.5

In order to create a jce_verbose log in XI 3.x(tomcat 5.5) add the following to the tomcat java options

-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. For best results check the log after a logon attempt

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

You may also try… (the XIR2 verbose option)

-Dcrystal.enterprise.trace.configuration=verbose

The logs are much smaller, and called jce_default

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

Newly added to the 3.1 admin guide is

-sun.security.krb5.debug=true

This logging is fantastic for java AD (AKA manual logon). It shows much more than the **debug=true** that we add to the bsclogin.conf

For vintela we still use (when you see djcsi think vintela) both on XIR2 and XI 3.x

-Djcsi.kerberos.debug=true

For this logging to work you must not have a keytab file in the web.xml (or cached web.xml in tomcat 5.5). It will only trace when using the tomcat password option for vintela **(-Dcom.wedgetail.idm.sso.password=mypassword**) and the keytab is commented out

9. Additional Steps - Cleanup tracing, add keytab, and forcing an AD site

At this point you have completed and tested each section (1-7) . You can now remove any tracing that was enabled
Remove the following(if they exist)…
Debug =true in the bsclogin.conf (set by default in section 5)
-Dbobj.logging.log4j.config=verbose.properties (may have been added to java options)
-Dcrystal.enterprise.trace.configuration=verbose (may have been added to java options)
-Djcsi.kerberos.debug=true java option (set by default in section 7)
Dcom.wedgetail.idm.sso.password=mypassword (only remove if you have a valid keytab configured)
Switch Tomcat 5.5 back to local system (if running under service account for verbose tracing)

Encrypting your service account password

Copy the vinsso.keytab (created during ktpass step) to the c:\winnt directory then specify the following in the web.xml (after the idm.princ setting). Once this is added you can remove the wedgetail.passowrd 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\vinsso.keytab</param-value>
</init-param>
```

Setting up an AD site

In large deployments it may also be necessary to use the idm.ad.site parameter to force vintela to login to a set of specific DC's. If so add this section next and add the following option to the tomcat java options
This may be required if vintela is trying to authenticate against DC's that are non local or on the other side of a firewall(discovered in packet scanning or Djcsi tracing).

```
<init-param>
    <param-name>idm.ad.site</param-name>
    <param-value>mysite</param-value>
</init-param>
```

Java options
-Djcsi.kerberos.site=mysite

SSO Guide (pdf download)

Configuring Vintela SSO in Distributed Environments – Complete Guide

A compilation of support experience and steps from the XI 3.1 Admin guide condensed into a single easy to follow step by step document with troubleshooting steps built in

http://scn.sap.com/docs/DOC-10636

Questions?