How to setup Kerberos SSO 6.7 on Windows 2008 R2 Server with Windows 7 Clients, Apache Tomcat Web Application.

First of all make a find and replace all information under “<>” with your own data. knowing that these information are case sensitive.

Repository name:	<repository_name>
Content Server:	<CS_ServerName>
Web Application Server:	<HTTP_ServerName>
Active Directory Server:	<AD_ServerName>
FQDN (Full Qualified Domain Name):	<ABC.ITU.CH>
fqdn:	<abc.itu.ch>
SSO HTTP User:	<DocumentumHTTP>
SSO HTTP User Password:	<PWD_HTTP>
SSO Content Server User:	<DocumentumCS>
SSO Content Server User Password:	<PWD_CS>
Web Application Name :	<taskspace>
Web Application Port :	<8093>
%CATALINA_HOME%:	<C:\Apache\taskspace_8093_p>

A - From your Active Directory Server

1) User Creation

Create these two users: <DocumentumHTTP> and <DocumentumCS>

Check:

Use Kerberos DES encryption types for this account
This account supports Kerberos AES 128 bit encryption.

2) Create Keytab

2.1) Keytab used by the Content Server

```
C:\>ktpass /pass <PWD_CS> -out <repository_name>.0001.keytab -princ CS/<repository_name>@<FQDN> -crypto ALL +DumpSalt -ptype KRB5_NT_PRINCIPAL /mapOp set /mapUser <DocumentumCS>@<FQDN>
```

2.1.1)From AD User Properties, Update **Delegation** for user <DocumentumCS>
check : Trust this user for delegation to any service (Kerberos only)

2.1.2)Copy this keytab file under <repository_name>.0001.keytab under \\<CS_ServerName>\%DOCUMENTUM%\dba\auth\kerberos\

2.2) Keytab used by all your web application.

```
C:\>ktpass /pass <PWD_HTTP>-out <DocumentumHTTP>.keytab -princ HTTP/<HTTP_ServerName>.<abc.itu.ch>@<ABC.ITU.CH> -crypto ALL +DumpSalt
-ptype KRB5_NT_PRINCIPAL /mapOp set /mapUser <DocumentumHTTP>@<ABC.ITU.CH>
```

2.2.1)From AD User Properties, Update **Delegation** for user <DocumentumHTTP>
check : Trust this user for delegation to any service (Kerberos only)

2.2.2) **Copy** Keytab file under \\<HTTP_ServerName> \%CATALINA_HOME%\<DocumentumHTTP>.keytab
This path will be named <HTTP_KEYTAB_PATH>

B - From your Web Application Server

Web Application Server : <HTTP_ServerName>
Update file webapps\<taskspace>\wdk\app.xml

```
<!-- Kerberos SSO authentication scheme configuration -->
  <kerberos_sso>
    <enabled>true</enabled>
    <browsers>
      <windows>
        <ieversions>6.0,7.0,8.0</ieversions>
        <firefoxversions>2.0,3.0,3.5</firefoxversions>
      </windows>
    </browsers>
    <!-- Enable login fall back to DocbaseLogin scheme -->
    <docbase_login_fallback>false</docbase_login_fallback>
    <!-- Mandatory configuration: Provide the kerberos realm / domian name. -->
    <domain><fqdn></domain>
  </kerberos_sso>
```

JASS Configuration file

Create file \\<HTTP_ServerName> \%CATALINA_HOME%\<taskspace>\webapps\<taskspace>\WEB-INF\krb5Login.conf

Warning1:

the bold red info must be replace by your <fqdn>, knowing that "." Must be replaced by "-"

Warning2:

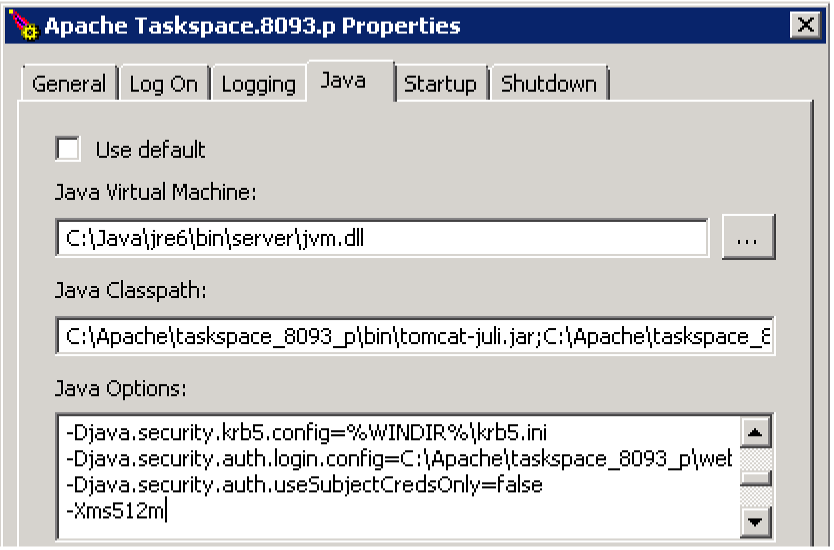
<**HTTP_KEYTAB_PATH**> **must be replace with you path related to your** <documentumHTTP>.keytab

Example : <**HTTP_KEYTAB_PATH**>=C\://Apache//taskspace_8093_p//<documentumHTTP>.keytab

```
HTTP-< HTTP_ServerName >- abc-itu-ch
{
com.sun.security.auth.module.Krb5LoginModule required
debug=true
principal="HTTP/< HTTP_ServerName >.<fqdn>@<fqdn>"
refreshKrb5Config=true
useKeyTab=true
storeKey=true
useTicketCache=false
isInitiator=false
keyTab="<HTTP_KEYTAB_PATH>";
};
```

On the Apache Setting

Update Apache Service Properties



□ Use default

Java Virtual Machine: C:\Java\jre6\bin\server\jvm.dll

Java Classpath: C:\Apache\taskspace_8093_p\bin\tomcat-juli.jar;C:\Apache\taskspace_8

Java Options:

```
-Djava.security.krb5.config=%WINDIR%\krb5.ini
-Djava.security.auth.login.config=C:\Apache\taskspace_8093_p\wet
-Djava.security.auth.useSubjectCredsOnly=false
-Xms512m
```

Add

```
-Djava.security.krb5.config=%WINDIR%\krb5.ini
-Djava.security.auth.login.config=<C:\Apache\taskspace_8093_p>\webapps\taskspace\WEB-INF\krb5Login.conf
-Djava.security.auth.useSubjectCredsOnly=false
```

C – On your Web Application Server and Content Server

Create a File krb5.ini. You will have to store it under "c:\windows\" of the Content Server and the Web Application Server.

```
[libdefaults]
default_realm = <ABC.ITU.CH>
forwardable = true
ticket_lifetime = 24h
clockskew = 72000
default_tkt_enctypes = aes128-cts des-cbc-md5 des-cbc-crc des3-cbc-sha1
default_tgs_enctypes = aes128-cts des-cbc-md5 des-cbc-crc des3-cbc-sha1
permitted_enctypes = aes128-cts des-cbc-md5 des-cbc-crc des3-cbc-sha1

[realms]
<ABC.ITU.CH> = {
kdc = <AD_ServerName>.<abc.itu.ch>
admin_server= <AD_ServerName>.<abc.itu.ch>
}

[domain_realm]
.<abc.itu.ch> = <abc.itu.ch>
```

D – How to debug it

Update service **Documentum Docbase Service** <repository_name> in order to add **-otrace_authentication,** this will allow you to manage log file in a trace mode for Kerberos authentication

```
C:\Documentum\product\6.7\bin\documentum.exe -docbase_name <repository_name> -security acl -otrace_authentication -init_file
C:\Documentum\dba\config\<repository_name>\server.ini -run_as_service -install_owner dmadmin -logfile C:\Documentum\dba\log\<repository_name>.log
```

Update file
\\<HTTP_ServerName> \%CATALINA_HOME%\<taskspace>\webapps\<taskspace>\WEB-INF\classes\log4j.properties

In order to get all Debug information under Taskspace_8093_p.log

```
log4j.rootCategory=DEBUG, file, stdout
log4j.appender.file.File=C:\\Apache\\taskspace_8093_p\\logs\\Taskspace_8093_p.log
```

Update file \\<HTTP_ServerName> \%CATALINA_HOME%\<taskspace>\webapps\<taskspace>\WEB-INF\classes\com\documentum\debug\TraceProp.properties
In order to get more detailed debug information

```
com.documentum.web.formext.Trace.SESSION=true
```

Check Java Version

```
C:\Windows\system32>java -version
java version "1.6.0_22"
Java(TM) SE Runtime Environment (build 1.6.0_22-b02)
Java HotSpot(TM) 64-Bit Server VM (build 16.3-b01, mixed mode)
```

Java Version must be 1.6.0_20
Uninstall existing Java version
Download Archive: Java[tm] Technology Products Download from : http://www.oracle.com/technetwork/java/archive-139210.html
Select : **JDK/JRE -6**
Select : **6 Update 20**
Archive: Download Java Platform Standard Edition (Java SE) 6 Update 20
Download Java SE development Kit 6u20 for Windows x64
Copy file under c:\temp\jdk-6u20-windows-x64.exe
Install JDK 1.6.0_20 under c:\java\

Update each Apache Instances
Update Java Virtual Machine from C:\Java\jdk1.6.0_22\jre\bin\server\jvm.dll
To C:\Java\jdk1.6.0_20\jre\bin\server\jvm.dll
Update **JAVA_HOME** Variable
C:\Java\jdk1.6.0_20

To test with **Firefox**
Type about:config under the browser
Under Filter, type network.n

Update value **network.negotiate-auth.trusted-uris**

With : http://<HTTP_ServerName>.<abc.itu.ch>

Test URL : http://<HTTP_ServerName>.<abc.itu.ch>:<8093>/<taskspace>/appname=CORE

Check Log files : <C:\Apache\taskspace_8093_p>\logs\Taskspace_8093_p.log

To test Kerberos Password

From your Content Server

```
C:\>kinit CS/<repository_name>
Password for CS/<repository_name>@<FQDN>:
New ticket is stored in cache file C:\Users\dmadmin\krb5cc_dmadmin
```

From your Web Application Server

```
C:\Java\jdk1.6.0_20\bin>kinit HTTP/<HTTP_ServerName>.<abc.itu.ch>
Password for HTTP/<HTTP_ServerName>.<abc.itu.ch>:
New ticket is stored in cache file C:\Users\dmadmin\krb5cc_dmadmin
```

E – List of existing EMC White papers

- EMC Documentum Kerberos SSO Authentication (A Detailed Review) May 2011 and August 2010
- Troubleshooting EMC Documentum WEBTOP KERBEROS SSO ENVIRONMENTS
- EMC Documentum Web Development Kit and Webtop Version 6.7 Deployment Guide (Chapter 11 : Configuring Kerberos Authentication)
- EMC Documentum My Documentum for Microsoft Sharepoint