

**Configuring Oracle® Hyperion
Enterprise Performance Management System 11.1.2.x
for Kerberos Authentication**

Assumptions

Knowledge of Kerberos and its configuration at the system level is assumed in this document, as it documents configuration steps needed at the application level. Before you start these procedures, please confirm that the prerequisites for these tasks are completed.

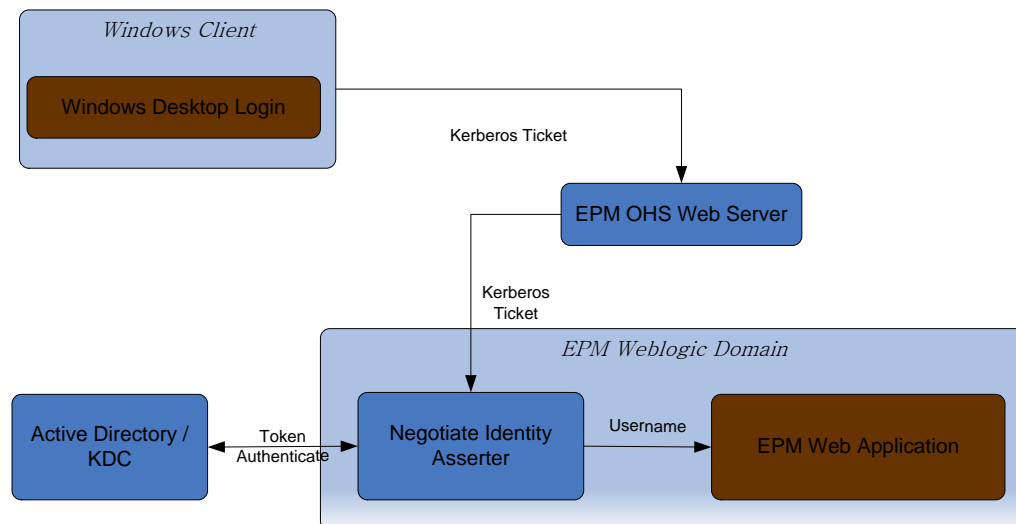
Note: The Oracle Hyperion Planning Web application for Release 11.1.2.1 is not supported for Kerberos.

Prerequisites Tasks

1. [Corporate Active Directory is configured for Kerberos authentication](http://www.microsoft.com/windowsserver2003/technologies/security/kerberos/default.mspx) (<http://www.microsoft.com/windowsserver2003/technologies/security/kerberos/default.mspx>)
2. [Windows client machines are configured for Kerberos authentication](http://support.microsoft.com/kb/295017) (<http://support.microsoft.com/kb/295017>).
3. The Client and Server are in Time Sync with a skew of not more than 5 minutes. ([http://technet.microsoft.com/en-us/library/cc780011\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc780011(W.S.10).aspx)).
4. Browsers are configured to negotiate using Kerberos tickets: IE (http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/sso.htm#i1102444) or Firefox (http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/sso-config-firefox.html)
5. IIS is set up if IIS is used as the front-end Web server - http://download.oracle.com/docs/cd/E12839_01/apirefs.1111/e14395/isapi.html#wp101184 and disable Windows Integrated Authentication - <http://support.microsoft.com/kb/215383>

Kerberos Authentication Flow Diagram for EPM System

The configuration of EPM System with Kerberos is supported using the WebLogic Negotiate Identity Asserter. The basic communication is as follows:

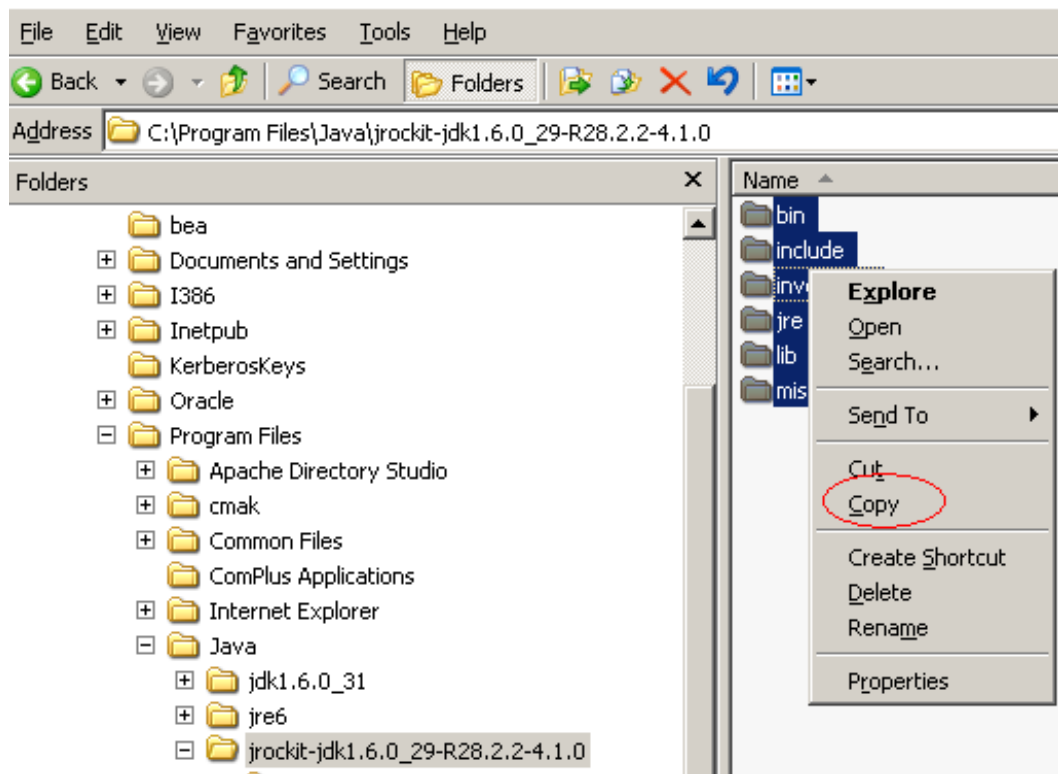


Step 1: Configure EPM System's WebLogic Domain for Kerberos Authentication

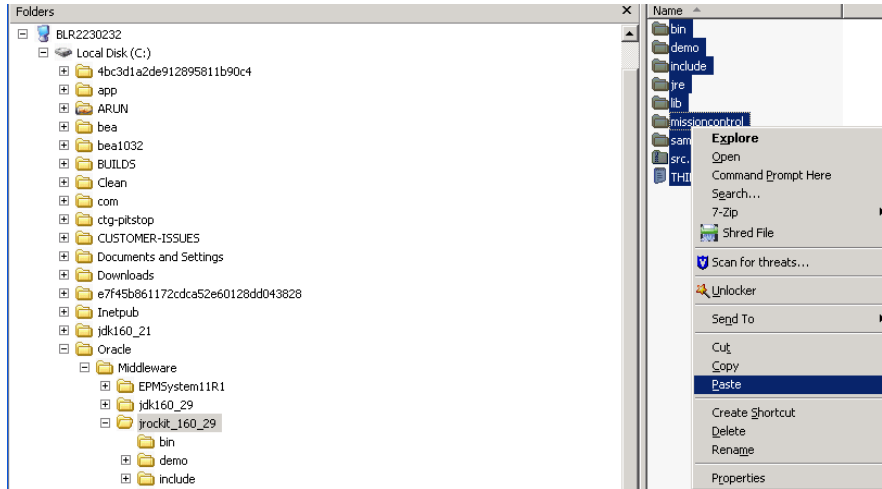
1. Install all the products you wish to use but only deploy and configure Foundation Services. This creates a WebLogic domain. The default domain name is EPMSystem.
2. Upgrade the deployed JRockit 1.6.29 under EPMSystem to JRockit 1.6.29 R28.2.2 to support RC4-HMAC encryption for both Web logic and IIS.

A common encryption type –RC4-HMAC, should be used for both Web logic and IIS installed on the same host; for example, MYHOST.

- a. Download and install the latest JRockit (Oracle JRockit 6 - R28.2.2) from <http://www.oracle.com/technetwork/middleware/jrockit/downloads/index.html>
- b. Stop all EPM Servers.
- c. Copy the contents of the newly installed JRockit R28.2.2.



- d. Replace the contents of the JRockit folder under *EPM ORACLE_HOME* with the contents copied from JRockit R28.2.2 folder.



Note: Name of the root folder; jrockit_160_29; should be retained to ensure that the startup scripts work properly. Only the contents are upgraded to a newer version.

- e. Restart EPM Servers.
3. Configure the EPMSysystem domain for [Kerberos authentication](#)
 - a. Create an LDAP Authentication Provider - http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/atn.htm#i1216261.
 - b. Create a Negotiate asserter - http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/atn.htm#i1208059.
Note: Set the JAAS option to OPTIONAL for all of the Authenticators. See http://download.oracle.com/docs/cd/E12839_01/apirefs.1111/e13952/taskhelpp/security/SetTheJAASControlFlag.html for more details.
 - c. Create service principals and map them to user objects that represent the WebLogic server and Financial Management IIS Server – http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/sso.htm#i1101993.

An example of a Service Principal:

Create a User object; for example, EPM_HOST, in Active Directory to represent WebLogic server and IIS services running on host MYHOST. This service principal is used while enabling Kerberos on IIS for EPM products deployed on IIS. Refer to [Step 7](#) on how to configure IIS for Kerberos authentication.

An example of the command for creating the key tab file:

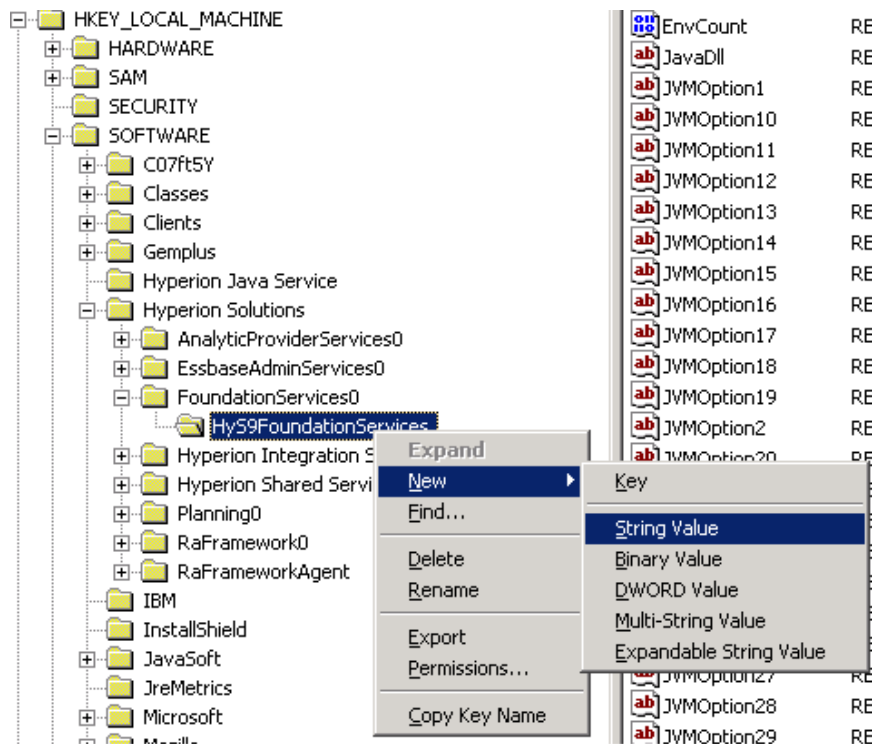
```
ktpass -princ HTTP/myhost.mydomain.com@MYHOST.MYDOMAIN.COM -pass password -mapuser EPM_HOST -out c:\myhost.keytab
```

- JDK5 onwards, the `com.sun.security.jgss.accept` package has changed to `com.sun.security.jgss.krb5.accept`.
- Use the Kerberos admin commands like `kinit`, `ktab`, create the `krb5.ini` file as described in http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/sso.htm#i1103676

- Configure WebLogic start scripts - http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/sso.htm#i1102021

i. In Windows environments the EPM Managed servers are run as Windows Services. The startup JVM options have to be set as described as follows for each of the EPM WebLogic managed servers. Perform this step for FoundationServices managed server only at this time

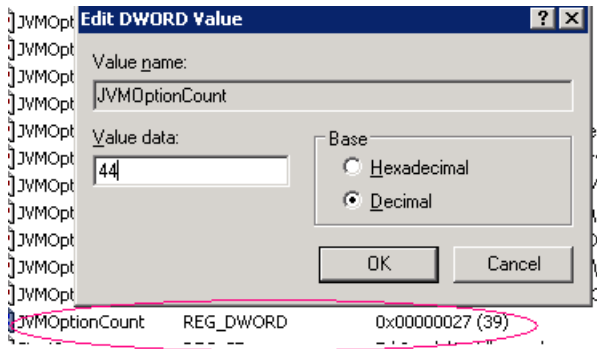
- Start the Windows regedit utility.
- Navigate to:
My Computer->HKEY_LOCAL_MACHINE->SOFTWARE
->Hyperion Solutions->FoundationServices0
->HyS9FoundationServices



- Create additional String values for JVMOptions; and add Kerberos JVM options as shown

JVMOption40	REG_SZ	-Djava.security.krb5.realm=KERBEROS.TEST.COM
JVMOption41	REG_SZ	-Djava.security.krb5.kdc=10.178.48.67
JVMOption42	REG_SZ	-Djava.security.auth.login.config=\\krb5login.conf
JVMOption43	REG_SZ	-Djavax.security.auth.useSubjectCredsOnly=false
JVMOption44	REG_SZ	-Dweblogic.security.enableNegotiate=true

- Modify the JVMOptionCount to reflect the new sum total of JVMOptions by adding 5 to the current OptionCount.



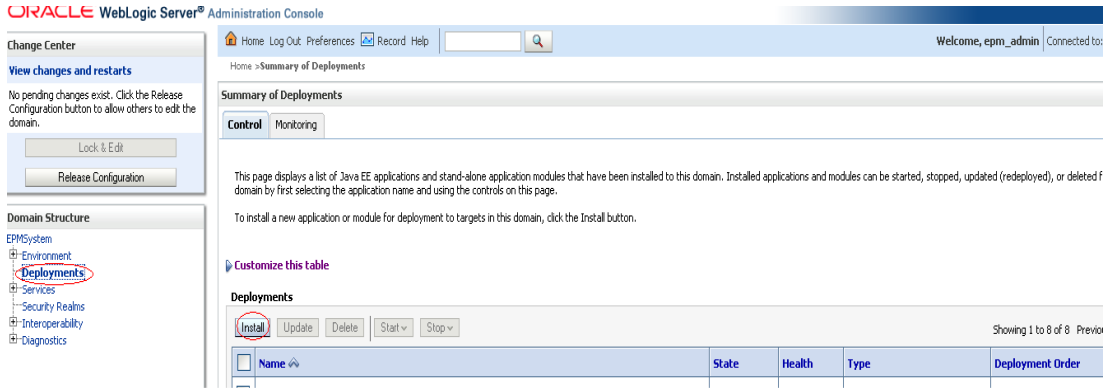
- Configure authorization policies for Active Directory users that will access the EPM products - http://download.oracle.com/docs/cd/E12839_01/web.1111/e13747/secejbwar.htm#i1242796. Refer to the section [Deploy Diagnostics Web App to test Kerberos Configuration](#) for an example of how to configure a Policy.

Step 2: Deploy Diagnostics Web Application to Test the Kerberos Configuration

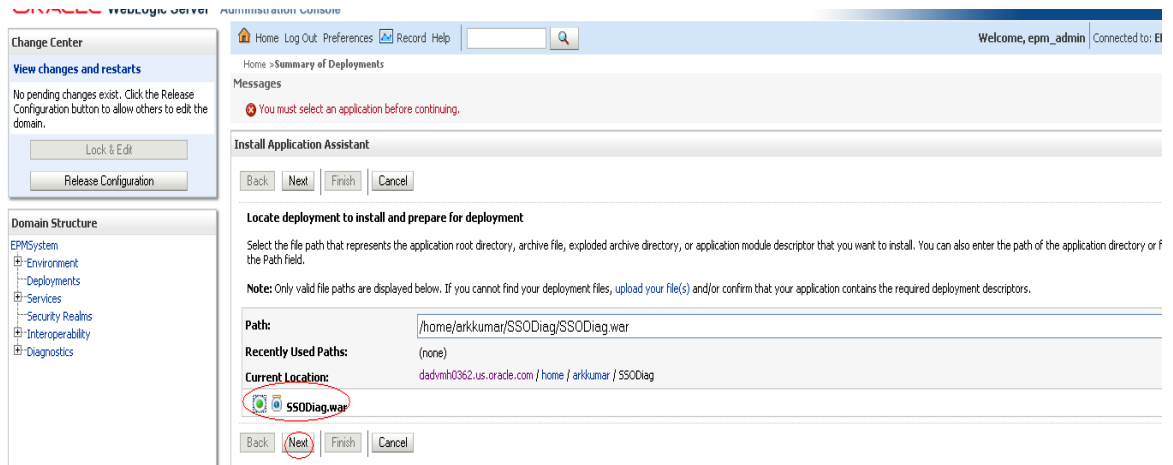
EPM System provides a test Web Application that can be used to test whether WebLogic is properly configured for Kerberos authentication.

For 11.1.2.0, download the patch 11678653 from <http://support.oracle.com> and apply it, which contains the Diagnostics Web App `SSODiag.war`. Launch the EPM domain WebLogic admin console to deploy the reference implementation `SSODiag.war` web application to the Foundation Services managed server.

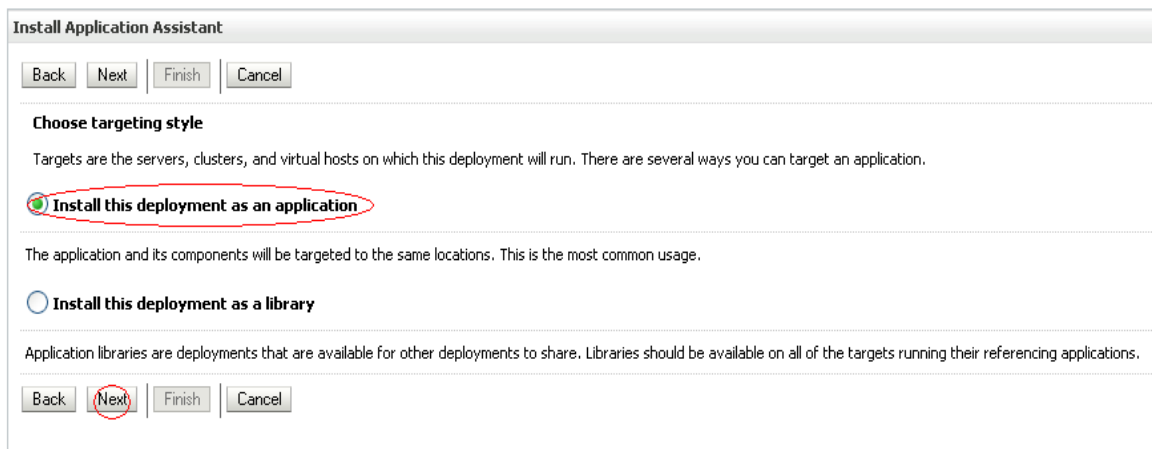
1. Deploy `SSODiag.war`.
 - a. Log in to WebLogic admin console, and select **Install**.



b. Select **SSODiag.war**.



c. Select **Install this deployment as an application**, and then click **Next**.



d. Deploy the **SSODiag.war** application to the **FoundationServices** managed server.

Servers
<input type="checkbox"/> AdminServer

Clusters
<input type="checkbox"/> AnalyticProviderServices <input type="radio"/> All servers in the cluster <input type="radio"/> Part of the cluster <input type="checkbox"/> AnalyticProviderServices0
<input type="checkbox"/> EssbaseAdminServices <input type="radio"/> All servers in the cluster <input type="radio"/> Part of the cluster <input type="checkbox"/> EssbaseAdminServices0
<input checked="" type="checkbox"/> FoundationServices <input checked="" type="radio"/> All servers in the cluster <input type="radio"/> Part of the cluster <input type="checkbox"/> FoundationServices0
<input type="checkbox"/> Planning

e. Select **Custom Roles and Policies** as the security model.

Security

What security model do you want to use with this application?

DD Only: Use only roles and policies that are defined in the deployment descriptors.

Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.

Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.

Advanced: Use a custom model that you have configured on the realm's configuration page.

Source accessibility

f. Complete the deployment.

Install Application Assistant

Back Next Finish Cancel

Review your choices and click Finish

Click Finish to complete the deployment. This may take a few moments to complete.

Additional configuration

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

Yes, take me to the deployment's configuration screen.

No, I will review the configuration later.

Summary

Deployment: /home/arkkumar/SSODiag/SSODiag.war

Name: SSODiag

Staging mode: Use the defaults defined by the chosen targets

Security Model: CustomRolesAndPolicies: Ignore all roles and policies in deployment descriptors. Create custom roles and policies later.

Target Summary

Components	Targets
SSODiag	FoundationServices

Back Next Finish Cancel

2. Configure Oracle HTTP Server (OHS) and add a forwarding request for SSODiag URL.

3. Add the following lines into

`EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/mod_wl_ohs.conf` to forward request to WebLogic Server from OHS. Restart OHS after updating `mod_wl_ohs.conf`.

```
<LocationMatch ^/SSODiag/>
  SetHandler weblogic-handler
  WeblogicCluster HSS_Server_Name:HSS_port
</LocationMatch>
```

4. Protect the URL by creating a policy in the WebLogic admin console for the URL http://OHS_server_name:port/SSODiag/krbssodiag

The screenshot shows the WebLogic Admin Console interface. The breadcrumb navigation path is: Home > Summary of Deployments > SSODiag > Roles > Policies. The main title of the dialog is "Create a New Stand-Alone Web Application URL Pattern Scoped Policy". It contains "OK" and "Cancel" buttons at the top. The section "Create a New Policy URL Pattern" includes the instruction: "The following property will be used to identify your new Policy URL pattern." Below this, it asks "What would you like to name your new Policy URL pattern?" with a text input field containing a forward slash (/). It then asks "What Authorizer Provider would you like to select?" with a dropdown menu showing "XACMLAuthorizer". At the bottom, there are "OK" and "Cancel" buttons, with the "OK" button circled in red.

The screenshot shows the WebLogic Admin Console interface. The breadcrumb navigation path is: Home > Summary of Deployments > SSODiag > Roles > Policies > Edit a Stand-Alone Web Application URL Pattern Scoped P. The main title of the dialog is "Edit a Stand-Alone Web Application URL Pattern Scoped Policy". It contains "Back", "Next", "Finish", and "Cancel" buttons at the top. The section "Choose a Predicate" includes the instruction: "Choose the predicate you wish to use as your new condition." Below this, it states: "The predicate list is a list of available predicates which can be used to make up a security policy condition". At the bottom, there is a "Predicate List:" dropdown menu with "User" selected. Below the dropdown are "Back", "Next", "Finish", and "Cancel" buttons.

Edit a Stand-Alone Web Application URL Pattern Scoped Policy

Back Next Finish Cancel

Edit Arguments

On this page you will fill in the arguments that pertain to the predicate you have chosen.

User Argument Description

User Argument Name:

 Add

krbuser1

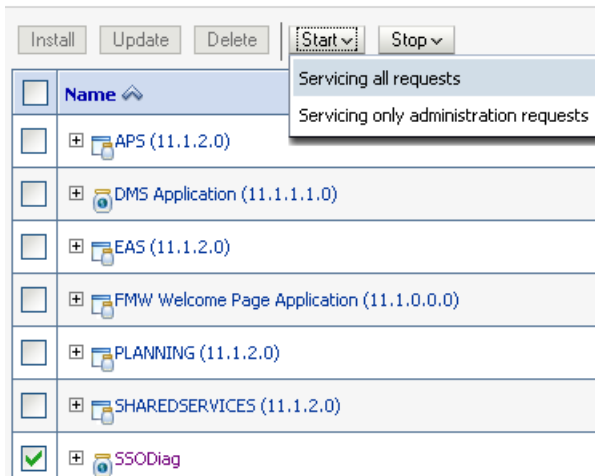
Remove

Back Next **Finish** Cancel

krbuser1 is the AD user who will authenticate to the Desktop

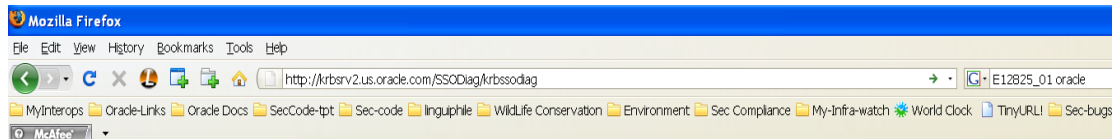
krbuser1 is a sample domain user that will access the browser from the Desktop. This can be an Active Directory user ID or an Active Directory group.

5. Start Foundation Services and the SSODiag utility.



6. Login as a valid provisioned active directory user into the client machine configured for Kerberos authentication and access the page http://OHS_server_name:port/SSODiag/krbssodiag from a browser.

If the Kerberos configuration is done correctly the following page is shown.

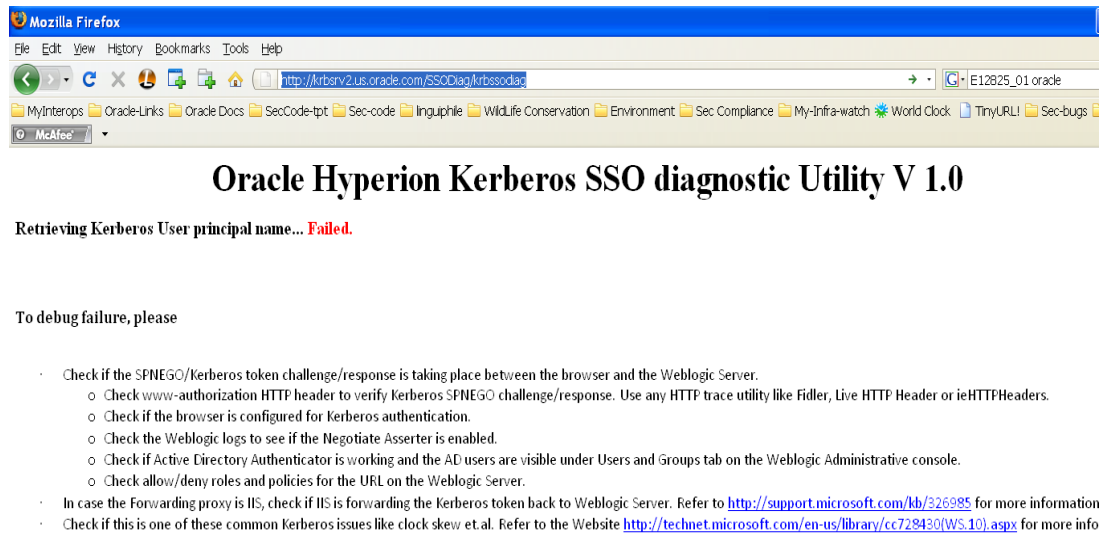


Oracle Hyperion Kerberos SSO diagnostic Utility V 1.0

Retrieving Kerberos User principal name... Success.

Kerberos Principal name retrieved... bea_sso_ad.

If the Kerberos configuration is not done correctly the following page is seen. Take corrective steps.



After Kerberos Diagnostics Utility is run successfully, go to Step 3

Step 3: Configure and deploy the rest of EPM System to this domain.

Configure all EPM System products and deploy them to the EPM domain using the EPM System Configurator.

Step 4: Configure EPM products for Kerberos authentication

In Windows environments, EPM managed servers are run as Windows services. You must set the startup JVM options for each EPM WebLogic managed server.

Here is a comprehensive list of EPM WebLogic managed servers for which you must set the startup JVM options in non-compact deployment mode:

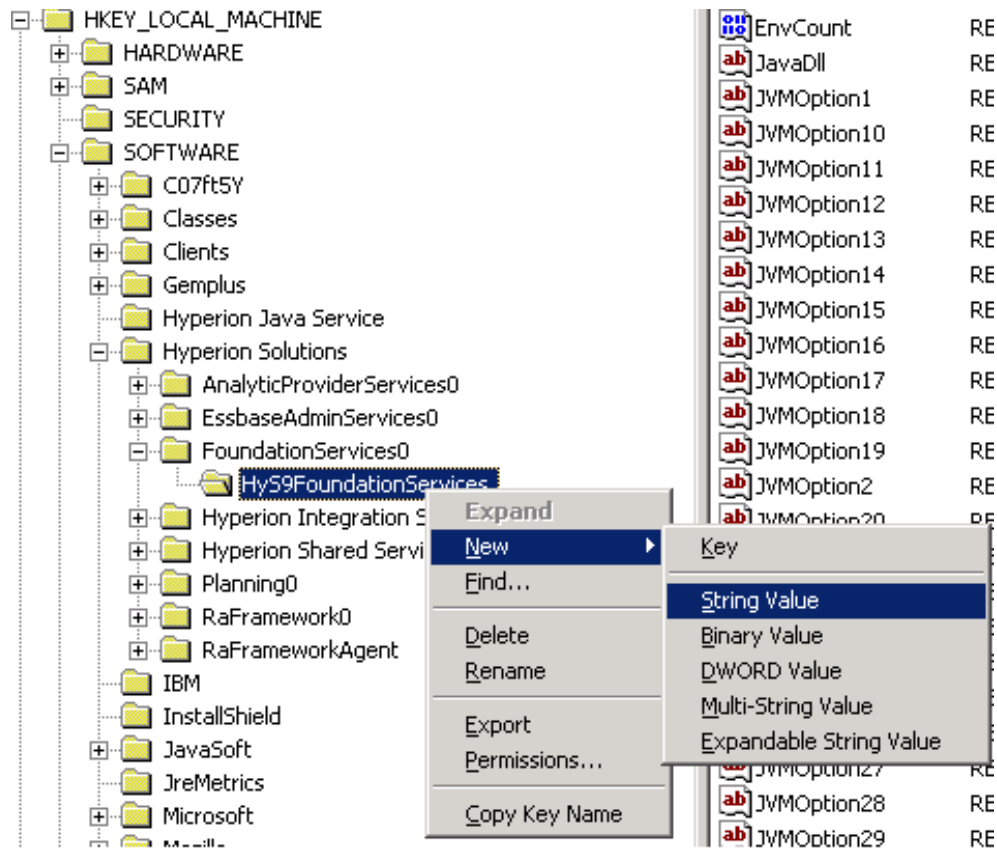
AnalyticProviderServices0	CalcMgr0	DisclosureManagement0
EpmaDataSync0	EpmaWebReports0	ErpIntegrator0
EssbaseAdminServer0	FinancialReporting0	FMWebServices0
FoundationServices0	HpsAlerter0	HpsWebReports0
hsfweb0	Planning0	Profitability0
RaFramework0	WebAnalysis0	

If web applications are deployed in the compact deployment mode, you need to update the startup JVM options of EPMSystem0 managed server only. If you have multiple compact managed servers, you must update the startup JVM options for all managed servers.

1. Configure WebLogic start scripts - http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/sso.htm#11102021

The following example describes how to set the startup JVM options for the FoundationServices managed server. You need to perform this task for each WebLogic managed server in the deployment.

- a. Start the Windows regedit utility.
- b. Navigate to My Computer -> HKEY_LOCAL_MACHINE->SOFTWARE->Hyperion Solutions ->HyS9FoundationServices.

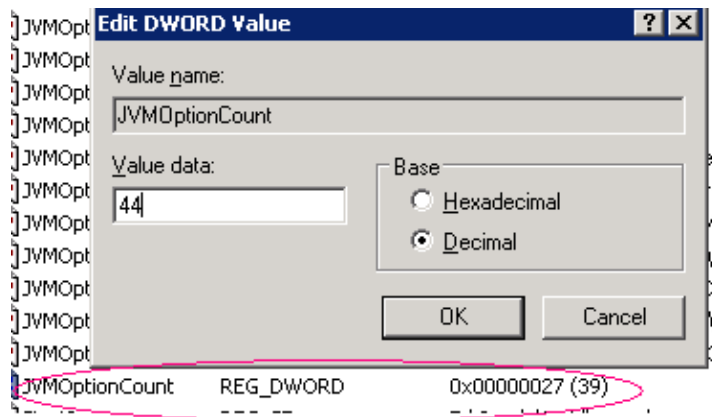


- c. Create String values for the JVMOptions shown below.

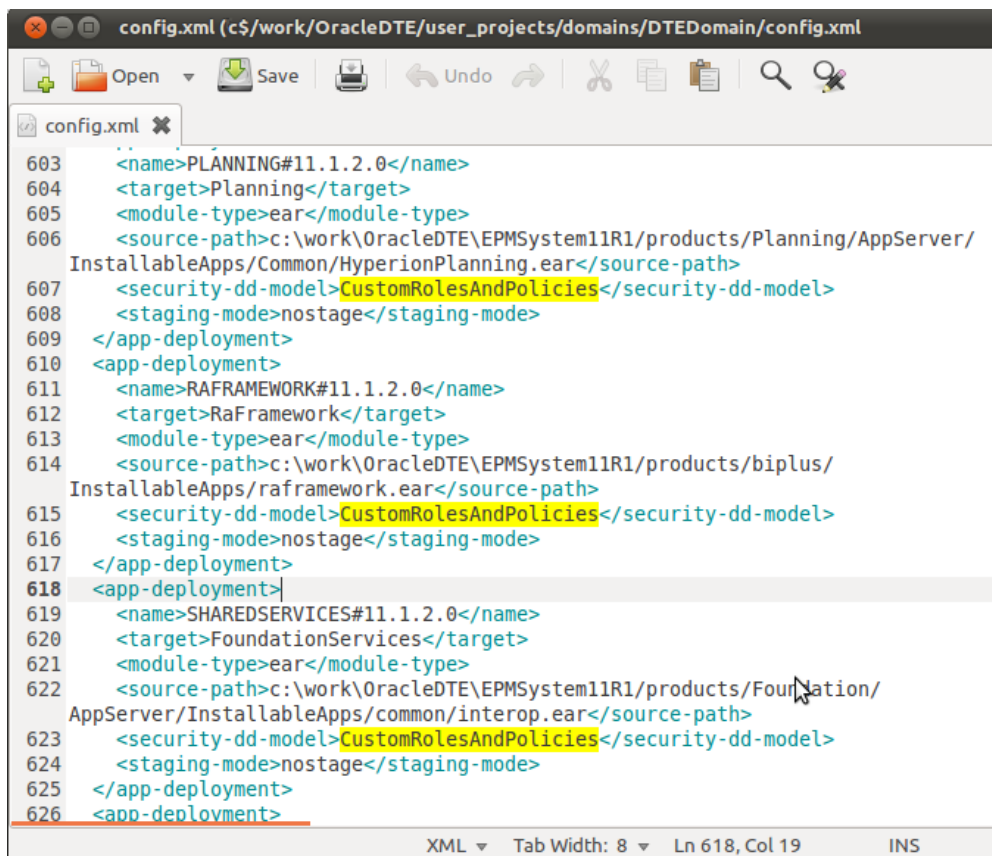
Be sure to replace `krb5.realm` with your Kerberos domain name, `krb5.kdc` with your domain controller IP address.

JVMOption40	REG_SZ	-Djava.security.krb5.realm=KERBEROS.TEST.COM
JVMOption41	REG_SZ	-Djava.security.krb5.kdc=10.178.48.67
JVMOption42	REG_SZ	-Djava.security.auth.login.config=f:\krb5login.conf
JVMOption43	REG_SZ	-Djavax.security.auth.useSubjectCredsOnly=false
JVMOption44	REG_SZ	-Dweblogic.security.enableNegotiate=true

- d. Modify the JVMOptionCount to reflect the new sum total of JVMOptions by adding 5 to the current OptionCount.



- e. Configure authorization policies for Active Directory users that will access the EPM products - http://download.oracle.com/docs/cd/E12839_01/web.1111/e13747/secejbwar.htm#i1242796. Refer to the section – [Deploy Diagnostics Web App to test Kerberos Configuration](#) - for an example of how to configure a policy.
2. Edit `EPM_ORACLE_INSTANCE/domains/EPMSysystem/config/config.xml` to change the default security model from `DDOnly` to `CustomRolesAndPolicies` (case-sensitive).



If EPM System is not deployed in compact mode, you must change the default security model from `DDOnly` to `CustomRolesAndPolicies` for each EPM System web application recorded in `config.xml`. The preceding screenshot lists a partial list of the entries only.

The following is a comprehensive list of EPM System WebLogic enterprise applications that may be identified in `config.xml`.

AIF	APS	CALC
DISCLOSUREMANAGEMENT	EAS	EPMADATASYNCHRONIZER
EPMAWEBTIER	FINANCIALREPORTING	HPSAlerter
HPSWebReports	HSFWEB	PLANNING
PROFITABILITY	RAFRAMEWORK	SHAREDSEVICES
WEBANALYSIS	WORKSPACE	

3. Create a URL protection policy, for each EPM System enterprise application.
 - a. Log in to the WebLogic admin console as an admin.
 - b. Click Deployments.
 - c. Create a URL protection policy for each deployed EPM System enterprise application.

AIF	APS	CALC
DISCLOSUREMANAGEMENT	EAS	EPMADATASYNCHRONIZER
EPMAWEBTIER	FINANCIALREPORTING	HPSAlerter
HPSWebReports	HSFWEB	PLANNING
PROFITABILITY	RAFRAMEWORK	SHAREDSEVICES
WEBANALYSIS	WORKSPACE	

view changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

- DTEDomain
 - Environment
 - Deployments**
 - Services
 - Security Realms
 - Interoperability
 - Diagnostics

How do I...

- Install an Enterprise application
- Configure an Enterprise application
- Update (redeploy) an Enterprise application
- Start and stop a deployed Enterprise application
- Monitor the modules of an Enterprise application
- Deploy EJB modules
- Install a Web application

System Status

Health of Running Servers

- Failed (0)
- Critical (0)
- Overloaded (0)
- Warning (0)
- OK (11)

Summary of Deployments

Control Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Customize this table

View

Number of rows displayed per page: 100

Exclude libraries when displaying deployments

Apply Reset

Deployments

Install Update Delete Start Stop

Showing 1 to 24 of 24 Previous Next

Name	State	Health	Type	Deployment Order
AIF (11.1.2.0)	Active	Warning	Enterprise Application	100
APS (11.1.2.0)	Active	OK	Enterprise Application	100
CALC (11.1.2.0)	New		Enterprise Application	100
DISCLOSUREMANAGEMENT (11.1.2.0)	New		Enterprise Application	100
DMS Application (11.1.1.1.0)	Active	OK	Web Application	5
EAS (11.1.2.0)	Active	OK	Enterprise Application	100
em	Active	OK	Enterprise Application	400
EPDATASYNCHRONIZER (11.1.2.0)	Active	OK	Enterprise Application	100
EPMAWEBTIER (11.1.2.0)	New		Enterprise Application	100
FINANCIALREPORTING (11.1.2.0)	New		Enterprise Application	100
FMW Welcome Page Application (11.1.0.0.0)	Active	OK	Enterprise Application	5
FMWEBSERVICES (11.1.2.0)	Active	OK	Enterprise Application	100
HPSAlerter (11.1.2.0)	New		Enterprise Application	100
HPSWebReports (11.1.2.0)	New		Enterprise Application	100
HSFWEB (11.1.2.0)	Active	OK	Enterprise Application	100
PLANNING (11.1.2.0)	Active	OK	Enterprise Application	100
PROFITABILITY (11.1.2.0)	Active	OK	Enterprise Application	100
proxyservlet (11.1.2.2)	Active	OK	Enterprise Application	100
RAFRAMEWORK (11.1.2.0)	Active	OK	Enterprise Application	100

- d. Expand an enterprise application such as PLANNING (11.1.2.0), and then select the web application; for example, HyperionPlanning.

Install a Web application

System Status

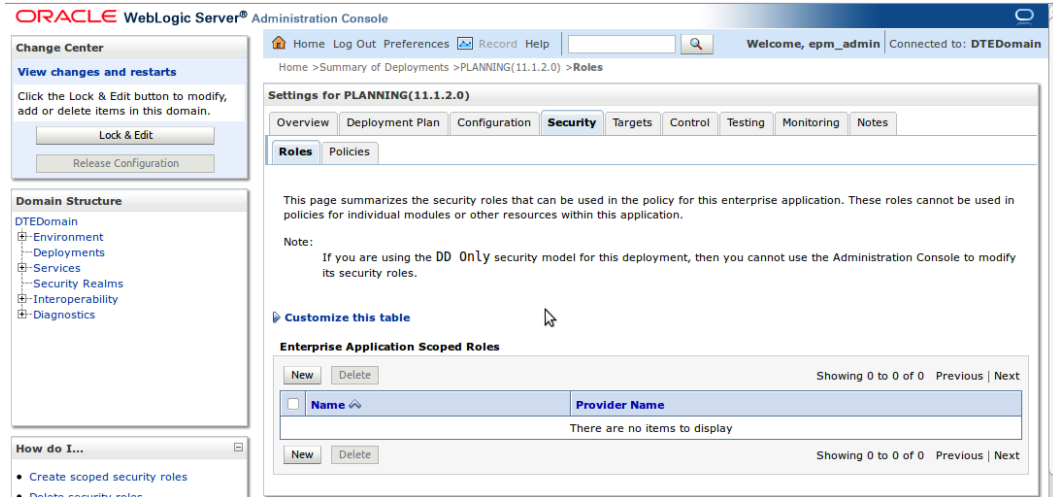
Health of Running Servers

- Failed (0)
- Critical (0)
- Overloaded (0)
- Warning (0)
- OK (11)

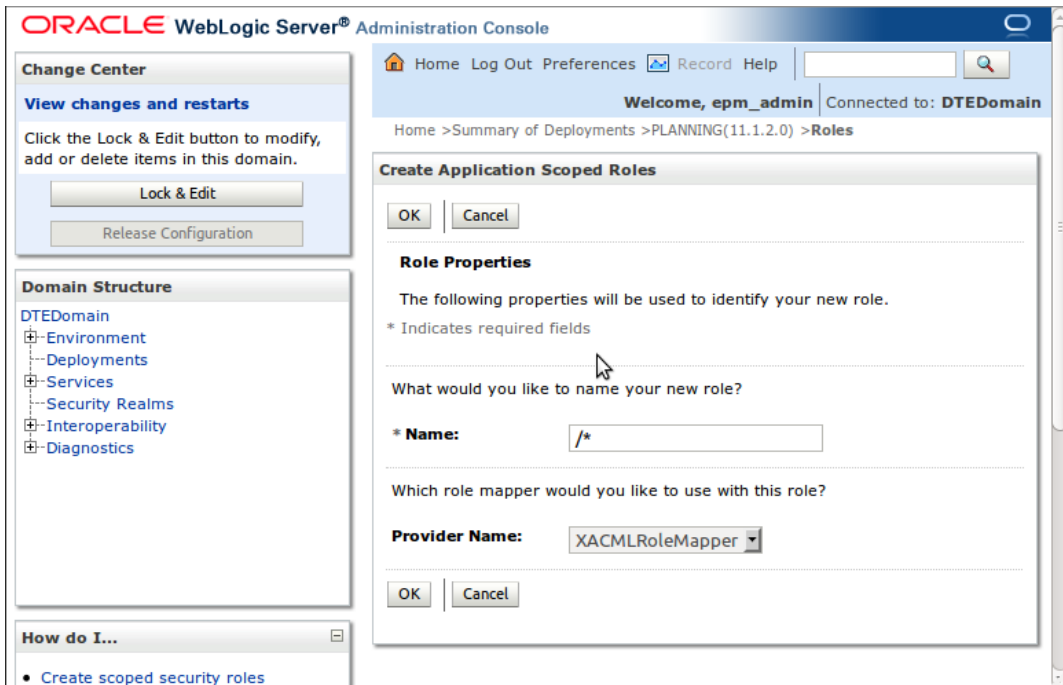
EPDATASYNCHRONIZER (11.1.2.0)	Active	OK	Enterprise Application	100
EPMAWEBTIER (11.1.2.0)	New		Enterprise Application	100
FINANCIALREPORTING (11.1.2.0)	New		Enterprise Application	100
FMW Welcome Page Application (11.1.0.0.0)	Active	OK	Enterprise Application	5
FMWEBSERVICES (11.1.2.0)	Active	OK	Enterprise Application	100
HPSAlerter (11.1.2.0)	New		Enterprise Application	100
HPSWebReports (11.1.2.0)	New		Enterprise Application	100
HSFWEB (11.1.2.0)	Active	OK	Enterprise Application	100
PLANNING (11.1.2.0)	Active	OK	Enterprise Application	100
Modules				
HyperionPlanning			Web Application	
EJBs			None to display	
Web Services			None to display	
PROFITABILITY (11.1.2.0)	Active	OK	Enterprise Application	100
proxyservlet (11.1.2.2)	Active	OK	Enterprise Application	100

http://rchakrav8:7001/console/console...g.war;HyperionPlanning;<none>;WEBAPP")

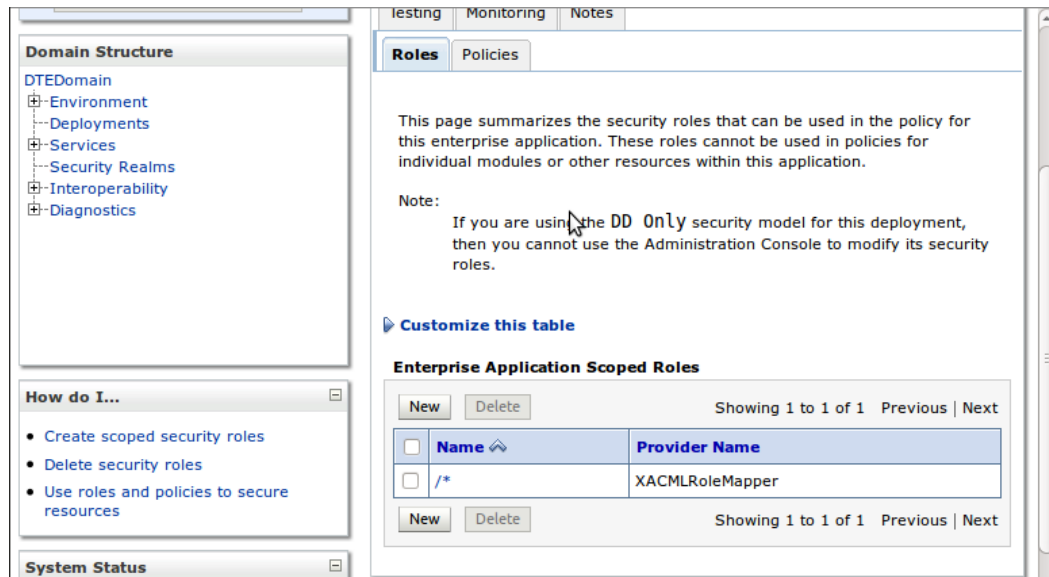
- e. Click the Security tab and select New Role.
 If the following message is displayed, it means that the security model of the web application was not changed from DDOnly to CustomRolesAndPolicies. Complete [step 2](#).
 If you are using the DD Only security model for this deployment, then you cannot use the Administration Console to modify its security roles.



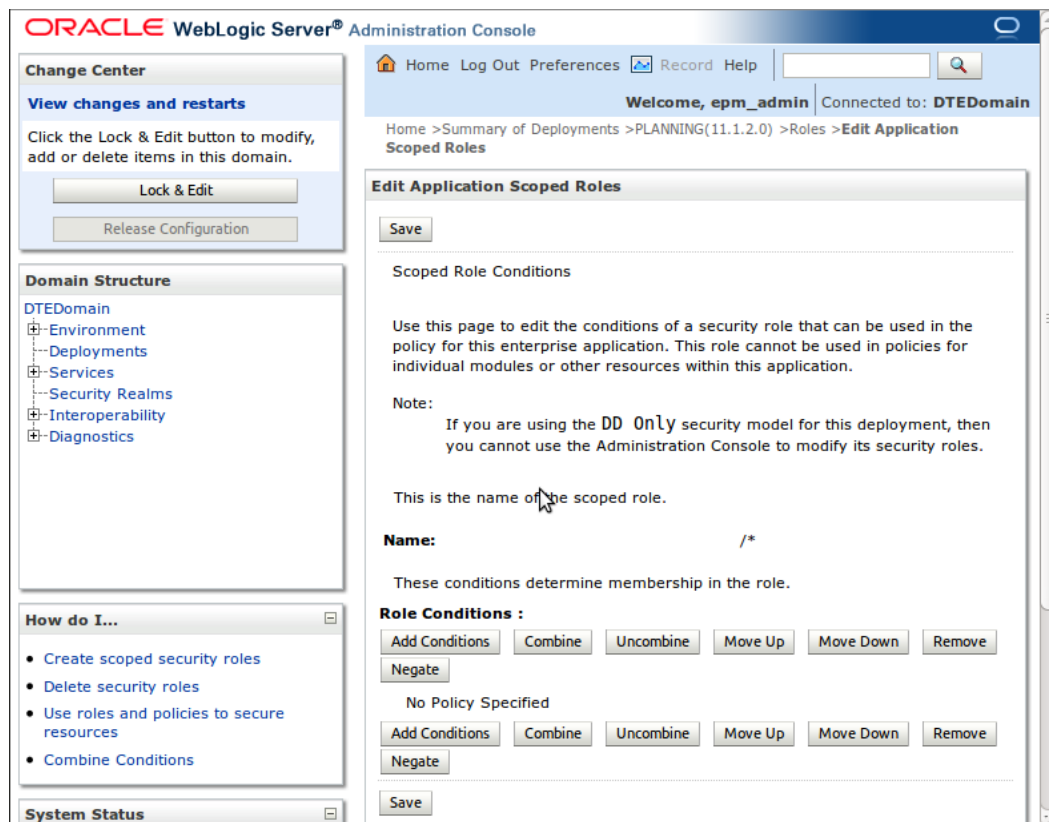
- f. In Name, type /*, and then click OK.



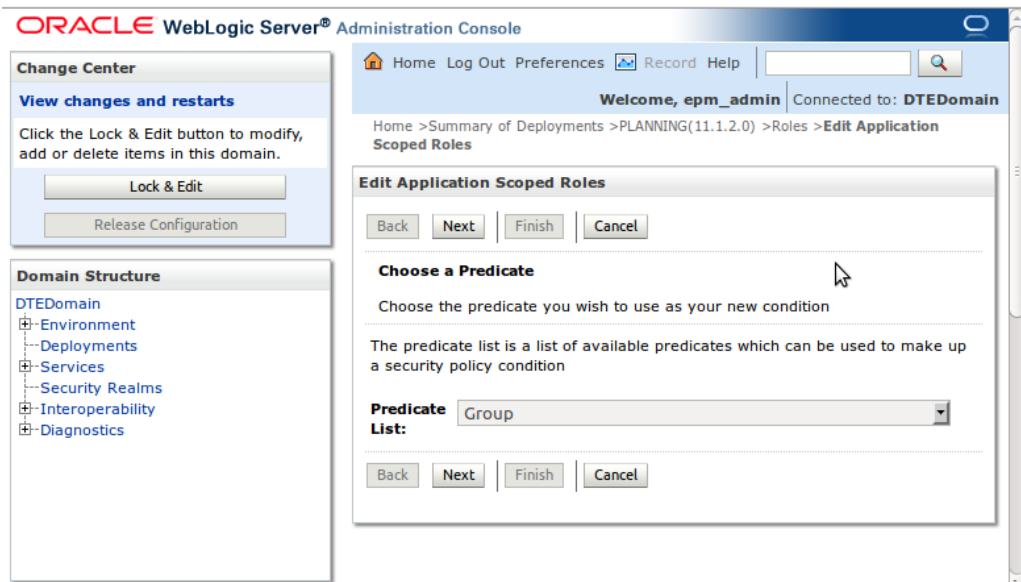
g. Click the /* link.



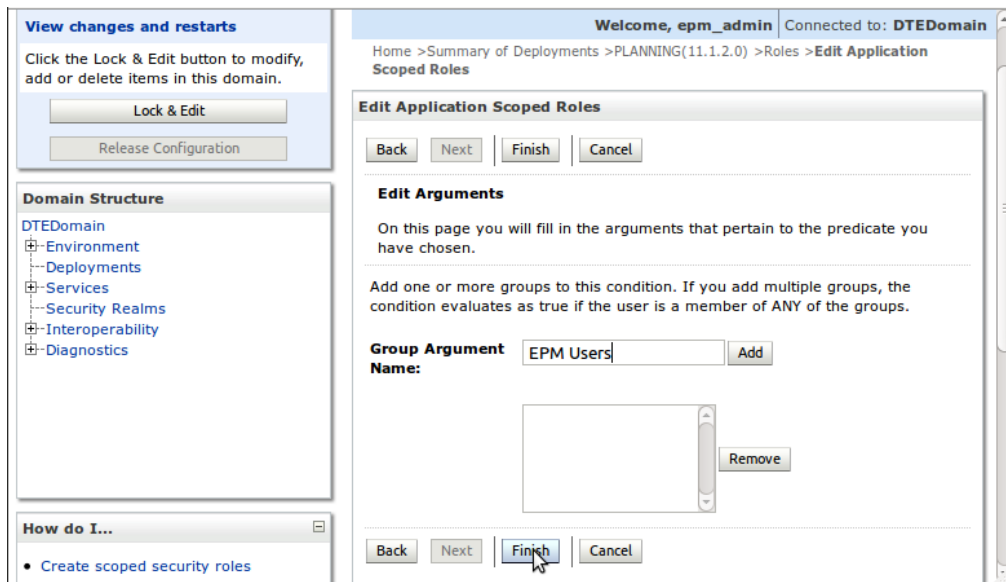
h. Choose Add Conditions under Role Conditions.



i. Choose a predicate list to be an Active Directory group or user, and click Next. These are the users who will be granted privileges to access this EPM web application.



- j. Type in the name of the Active Directory group and click Finish. Choose an Active Directory group contains all the users that will access EPM products. Check with your Active Directory admin to get the exact group name. It should match the name in AD. WebLogic displays an error after you click the Finish button if the group cannot be found.



- k. Repeat the preceding steps to create the policy for each web application.

Step 5: Modify EPM Web Applications to Enable Client Cert Based Authentication in WebLogic

Note: This step is required for EPM versions 11.1.2.1.00 or earlier only.

To modify EPM Web Applications to Enable Client Cert Based Authentication in WebLogic, you must modify the following application archives (located in *EPM_ORACLE_HOME/EPMSystemR11/products*) to insert a `login-config` entry:

- DisclosureManagement/AppServer/InstallableApps/common/DisclosureManagement.ear
- Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear
- FinancialDataQuality/AppServer/InstallableApps/aif.ear
- financialreporting/InstallableApps/HReports.ear
- Foundation/AppServer/InstallableApps/common/interop.ear
- hsf/AppServer/InstallableApps/hsf.ear
- PerformanceScorecard/AppServer/InstallableApps/common/webapps/HPSAlert.ear
- PerformanceScorecard/AppServer/InstallableApps/common/webapps/HPSWebReports.ear
- Planning/AppServer/InstallableApps/Common/HyperionPlanning.ear
- Profitability/AppServer/InstallableApps/common/profitability.ear

1. Stop EPM System products and processes.
2. Using 7 Zip, extract the contents of each enterprise archive.
3. Using 7 Zip, open the .war file inside the enterprise archive.
4. Using a text editor, open the `web.xml` file under the `WEB-INF` folder inside the .war file.
5. Add the following lines just above the `</web-app>` tag at the end of the file

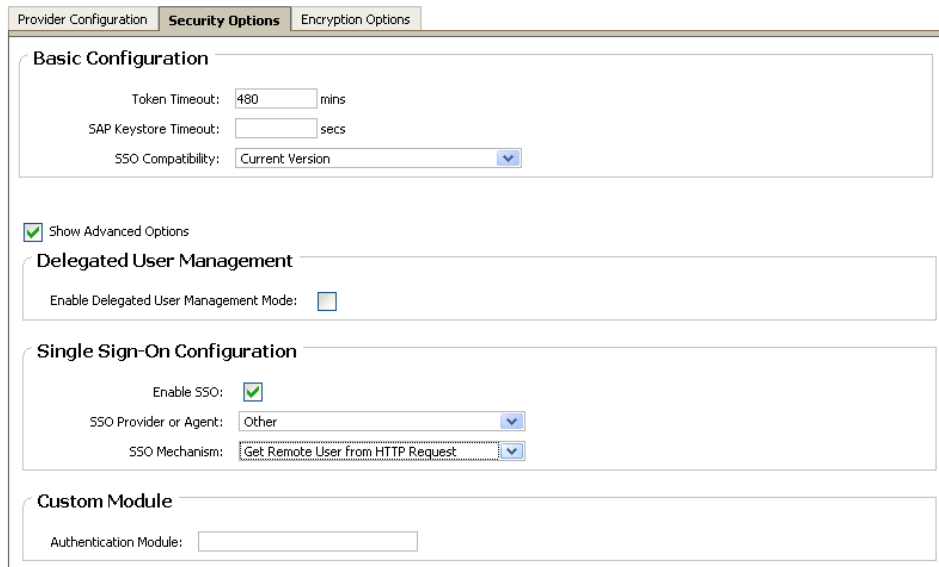
```
<login-config>
  <auth-method>CLIENT-CERT</auth-method>
</login-config>
```
6. Save `web.xml` file. 7zip queries whether you want to update the archive. Choose Yes.
7. Close 7zip.

Step 6: Enable Shared Services the Security Configuration to Perform SSO with Kerberos-enabled WebLogic

1. Launch Shared Services and login as an Administrator user.
2. Add the Active Directory domain that is configured for Kerberos authentication as an external user directory.

Ensure that the login attribute you set (for example, `samAccountName`) is identical to that you set in WebLogic authenticator configuration.

- On the Security Options tab, enable single sign-on configuration, and choose Get Remote User from HTTP Request as the SSO mechanism.

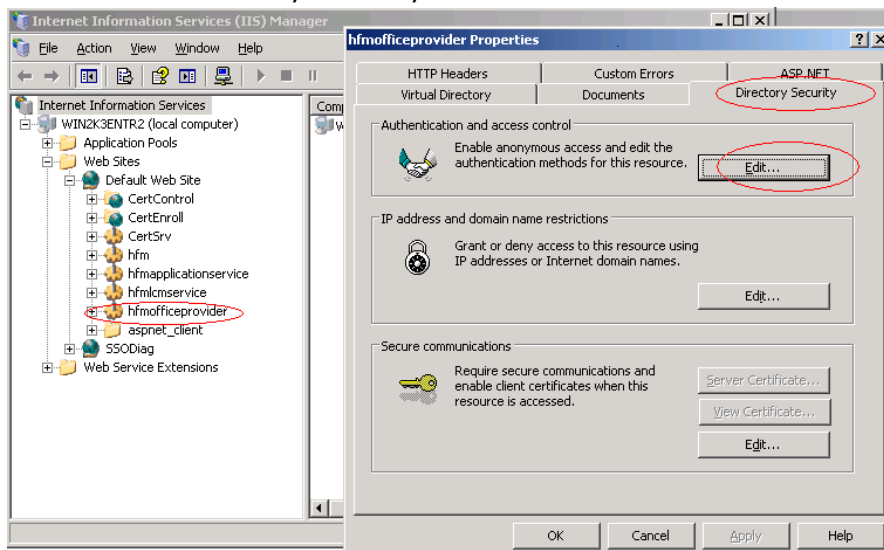


- Restart EPM System products and processes.
- Test the configuration by accessing Shared Services Console.
If Kerberos is configured properly, Shared Services does not prompt you for your user name and password to access the Shared Services Console.

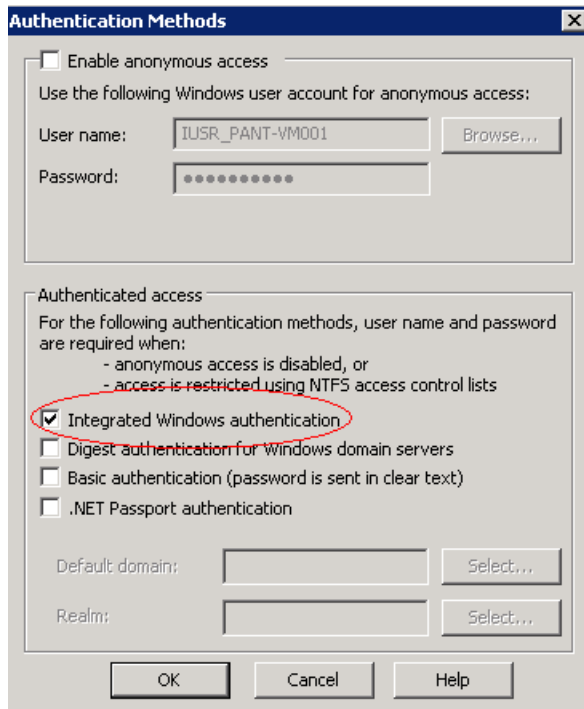
Step 7: Configuring Financial Management IIS Servers for Kerberos Authentication

Perform this step on all Financial Management IIS Servers.

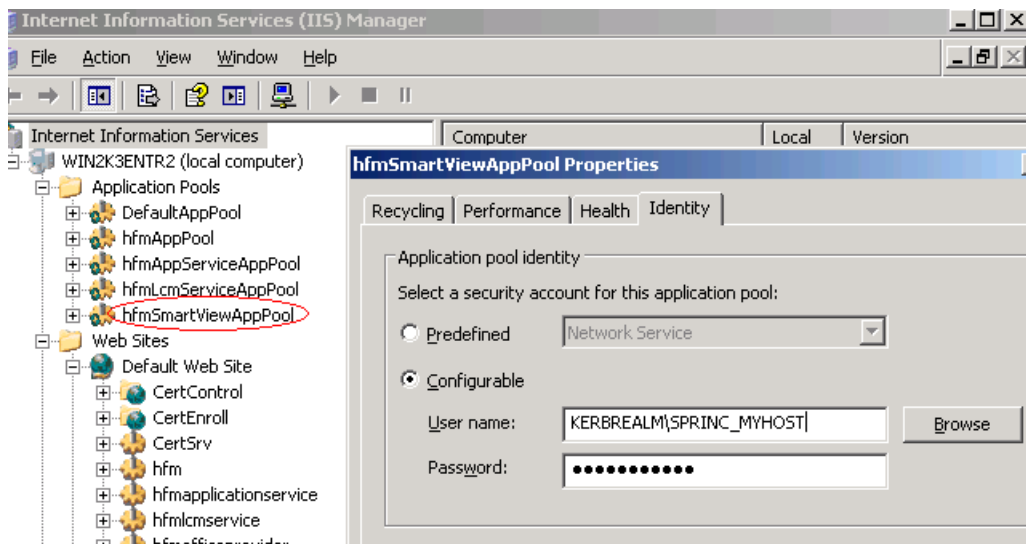
- Launch Internet Information Services Manager.
- Right click on Financial Management web site `hfmoofficeprovider`, and then select `Properties`.
- Click `Edit` on `Directory Security` tab.



4. Enable Integrated Windows Authentication.



5. On the corresponding Application pool, right click, select Properties. On the Properties tab, add the Kerberos Service Principal created in Step 1 as the Pool Identity.



6. Restart IIS and Financial Management.

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited. The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS:

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services

