Technical White Paper

Extending Microsoft Windows Active Directory Authentication to Access HP Service Health Reporter

For the Windows® Operation System

Software Version 9.40

Table of Contents

Sign up for updates
hp.com/go/getupdated

May 2015

Introduction

This document aims at providing the steps to configure Microsoft Windows Active Directory (AD) authentication for SAP BusinessObjects (BO or BOBJ) using Kerberos that provides role based security for users to access HP Service Health Reporter (SHR) reports, universes and the Administration Console.

Note: This document is applicable for HP Service Health Reporter 9.3x and 9.40.

Goal

In your IT environment, if users are already using AD authentication it can be extended to access the SHR content.

Overview

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications. It uses secret-key cryptography where a user authenticates into an authentication server that creates a ticket. This ticket is sent to the application that recognizes the ticket and the user is granted access.

Acronyms used in this document:

Acronym	Expanded form
SHRBOSERVER	BusinessObjects server installed along SHR
ADSERVER	Active Directory server configured to integrate the users or groups with SHR BOBJ Repository
ADBO_USER	Windows AD Service Account used to run BOBJ services
BOBJCMS/SHRBOSERVER	Service Principle Name (SPN) to run BOBJ services using domain user account

To configure Microsoft Windows AD authentication for SHR BusinessObjects using Kerberos, follow these steps:

1. Setting Up a Service Account
2. Configuring Grants for the Service Account
3. Registering Service Principle Name (SPN)
4. Configuring SIA to Use the Service Account
5. Configuring the AD Plug-in
6. Configuring Tomcat web.xml File
7. Configuring bscLogin.conf and Krb5.ini files
8. Configuring Tomcat Java Option
9. Configuring SHR Administration Console for AD Authentication

May 2015

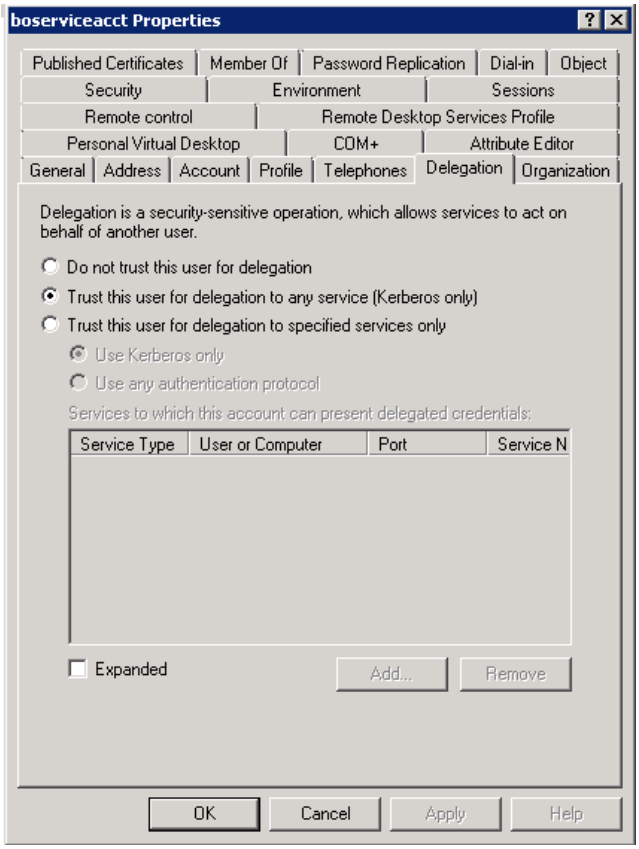
Configuring AD Authentication for SHR

Setting Up a Service Account

To configure BusinessObjects using Kerberos and Windows AD authentication, you must have a service account (domain account) that is trusted for delegation. You can either use an existing service account or create a new service account. The service account is used to run the BusinessObjects Enterprise servers.

To set up a service account, follow these steps:

1. Create a new AD service account (ADBO_USER) on the domain controller or use an existing account.
2. Select **Password never expires**. If the password expires, then the functionality dependent on that account will fail.
3. Select the AD service account, right-click and select **Properties**. The **Properties** window appears.
4. From the **Delegation** tab, click **Trust this user for delegation to any service (Kerberos only)** and then click **OK** to close the **Properties** window.



Note: If the **Delegation** tab does not appear, then complete the Registering Service Principle Name (SPN) **steps and continue with Step 4 of** Setting Up a Service Account.

Sign up for updates
hp.com/go/getupdated

May 2015

Configuring Grants for the Service Account

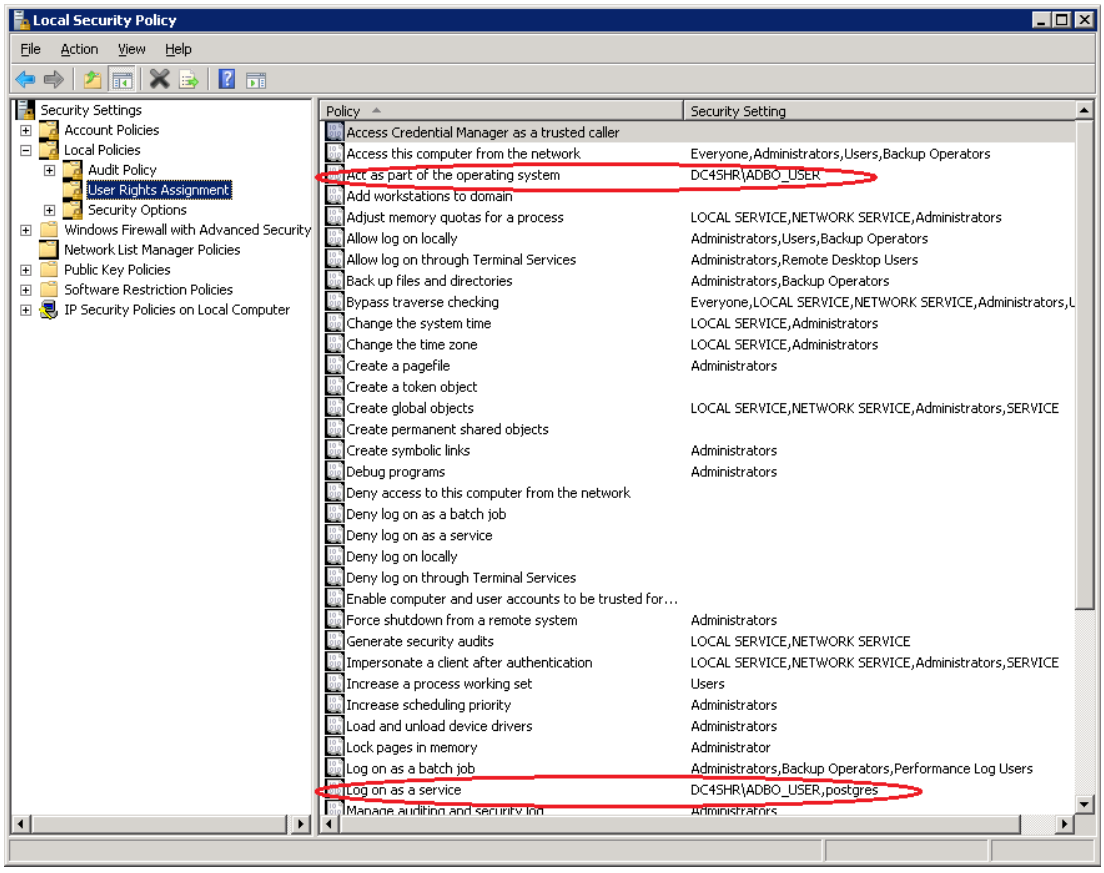
To support AD authentication, enable the service account to act as part of the operating system and log on as a service. This must be done on SHR BusinessObjects server (example: SHRBOSERVER) where the Server Intelligence Agent service is running.

To configure the grants for service account, follow these steps:

1. Go to **Start > Administrative Tools > Local Security Policy**.
2. In **Local Policies,** click **User Rights Assignment**.
3. Double-click **Act as a part of Operating System** and click **Add User** or **Group**.

   The user account (ADBO_USER) that is trusted for delegation is added.
4. Click **OK**.
5. Double-click **Logon as a service,** click **Add**, and then click **Add User** or **Group**.

   The user account that is trusted for delegation is added.
6. Click **OK**.



Sign up for updates
hp.com/go/getupdated

May 2015

To add service account to the Administrators Group, follow these steps:

1. On the SHRBOSERVER machine, right-click **My Computer**, and then click **Manage**.
2. Go to **Configuration > Local Users > Groups > Groups**.
3. Right-click **Administrator** and then click **Add to Group**.
4. Click **Add** and type the logon name for the service account.
5. Click **Check Names** to ensure the account resolves.
6. Click **OK** and then click **OK** again.

Registering Service Principle Name (SPN)

BOBJ services use the Kerberos protocol for mutual authentication in a network, you must create a Service Principal Name (SPN) for the BOBJ services to run as a domain user account. The SETSPN utility is a program that manages the SPN for service accounts in Active Directory System.

To register Service Principle Name (SPN), follow these steps:

1. Run the following utility with required parameters on command line window :

   ```
   setspn –A BOBJCMS /<HOSTNAME> <serviceaccount>
   ```

   Where, <HOSTNAME> is a qualified domain name of the machine running the Content Management System (CMS) service, i.e. SHRBOSERVER Host name, for example SHRBOSERVER.XYZ.com.
   Where, <serviceaccount> is the name of the CMS service account. In this case, the <serviceaccount> is ADBO_USER.
   Example: setspn –A BOBJCMS /SHRBOSERVER.XYZ.com ADBO_USER

2. On successful registration of SPN, the screen displays the following message:

   ```
   Registering ServicePrincipalNames for CN=ServiceCMS, CN=Users, DC=DOMAIN,

   DC=COM BOBJCentralMS/HOSTNAME.DOMAIN.COM Updated object
   ```

To list the set of registered SPNs, run the following command:

```
setspn –L ADBO_USER
```

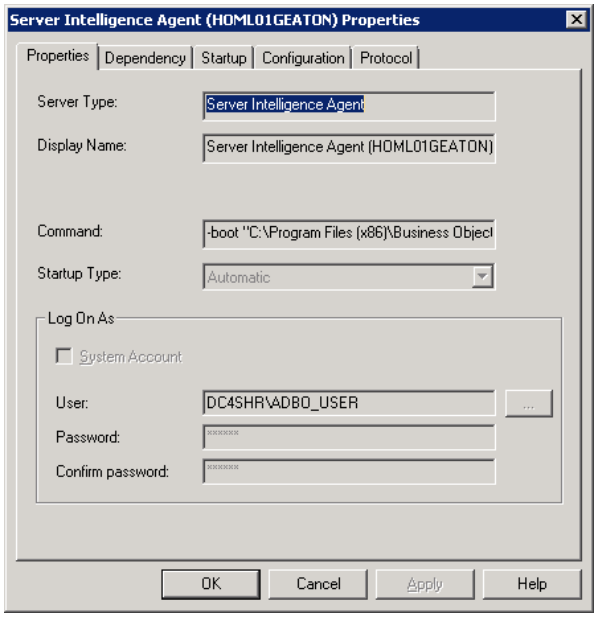
Configuring SIA to Use the Service Account

In order to support Kerberos, Server Intelligence Agent (SIA) must be configured in Central Configuration Manager (CCM) to log on as the service account.

To configure a Server Intelligence Agent on SHRBOSERVER, follow these steps:

1. Start the CCM.
2. Stop the Server Intelligence Agent.
3. Double-click the **Server Intelligence Agent**. The **Server Intelligence Agent Properties** dialog box appears.
4. In the **Properties** tab:

i. In the **Log On As**, uncheck **System Account** check box.
ii. Type the user name and password for the service account.
iii. Click **Apply**, and then click **OK**.



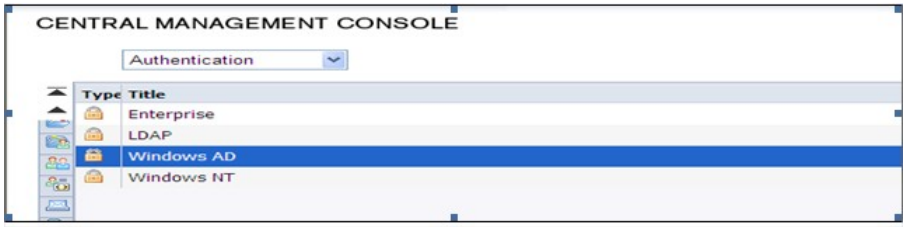
5. Restart the Server Intelligence Agent.

Configuring the AD Plug-in

To use Kerberos authentication, you have to configure the Windows AD security plug-in in the Central Management Console (CMC).

To configure the Windows AD security plug-in for Kerberos, follow these steps:

1. In CMC, go to the **Authentication** management page and click the **Windows AD** tab.



2. Select **Enable Windows Active Directory** check box.
3. In the **AD Configuration Summary**, click the link next to **AD Administration Name**.
4. Enter the credentials to read access to AD in the **Name** and **Password** textbox.

   Note: Use the format Domain\Account in the **Name** field.

   Example: XYZ\ADBO_USER.
5. Enter the default domain in the **Default AD Domain** text box.

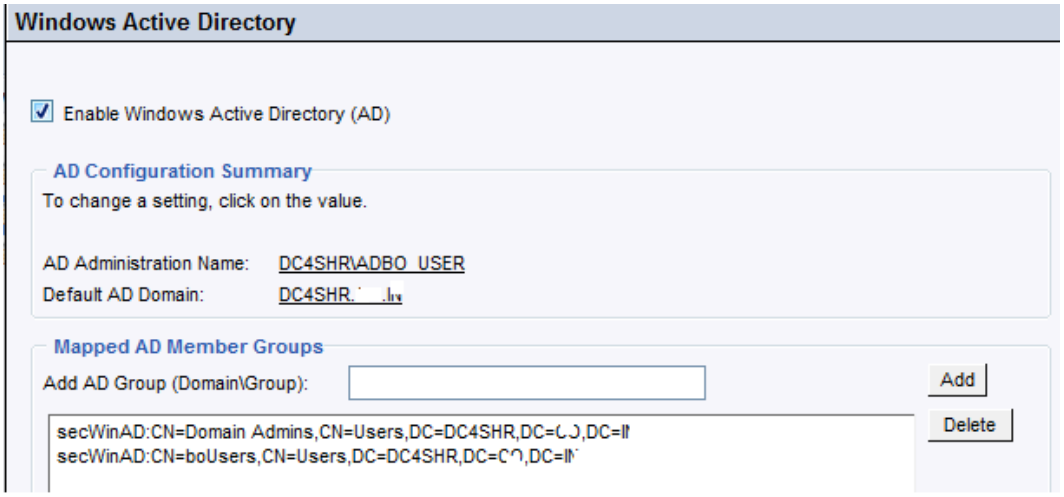
   Note: Use FQDN format and enter the domain in uppercase.

Sign up for updates
hp.com/go/getupdated

May 2015

Example: XYZ.COM.

6. In **Mapped AD Member Groups**, type the name of the domain or group in the **ADD AD Group (Domain\Group)** text box, and then click **Add**.



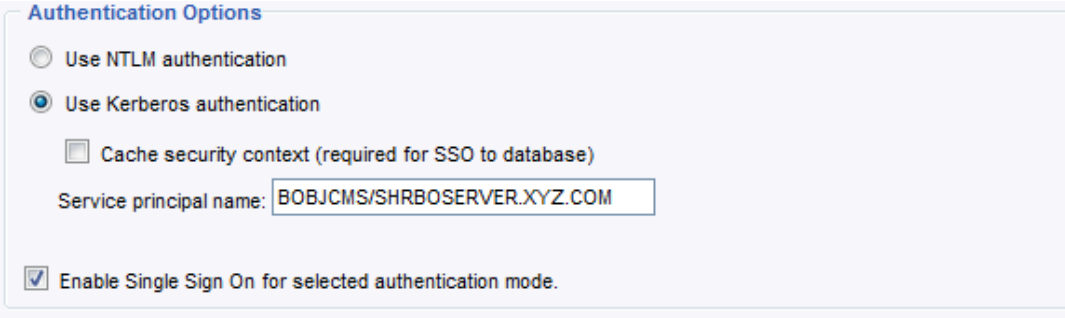
Mapped AD Member Groups:

- If a group is in the default domain it can be added with just the group name. If it is in another domain then it requires to be added in domain/group format or DomainName (DN) format.
- Click **Update** and the groups will appear as shown in the above figure (secWinAD: DN) regardless of how they were entered (group, domain/group, or DN).
- To add all users from the default domain, specify **Domain Users** as the group name.

7. In **Authentication Options**, click **Use Kerberos authentication**.

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

8. In the **Service principal name** text box, type the account and domain of the service account or the SPN mapping to the service account. For example, BOBJCMS/SHRBOSERVER.XYZ.COM.



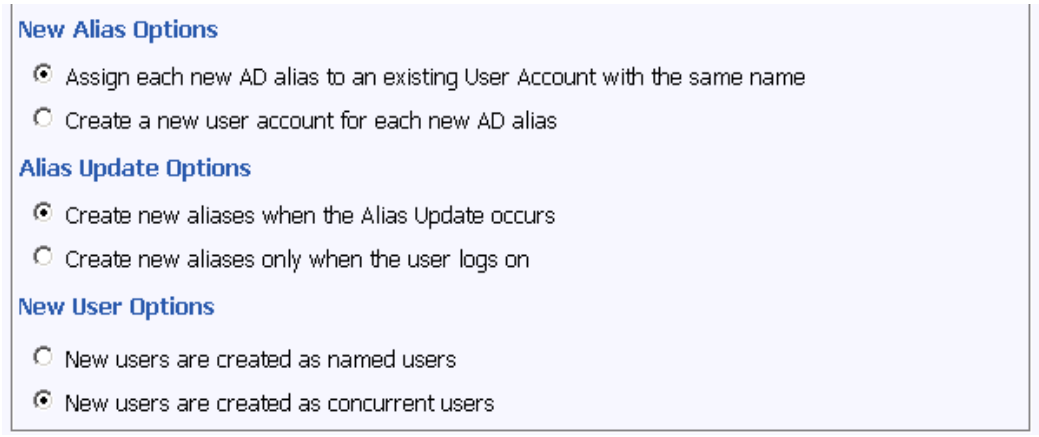
   The **Service Principal Name** must be the value created for the service account that runs the SIA or CMS using SETSPN. For more details, see Registering Service Principle Name (SPN). Ensure that there are no mistakes or white spaces before or after the SPN.

9. Select **Enable Single Sign On for selected authentication mode** (not required for manual AD authentication).
10. New User Alias Options:

Sign up for updates
hp.com/go/getupdated

May 2015

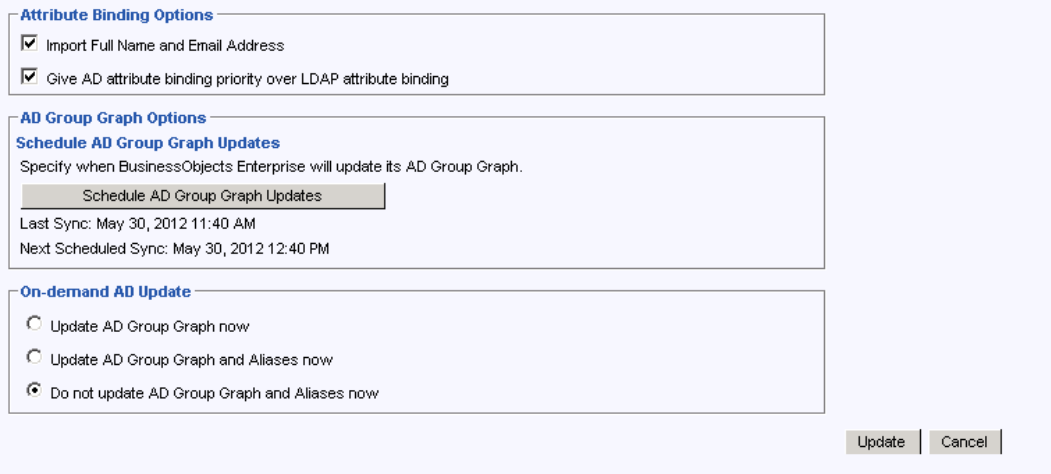
- **New Alias Options** determine how the user will be created if there is an existing user with the same name (LDAP or NT or Enterprise).
- **Alias Update Options** determine if users will be added when clicking the update button or only after they have logged into CMC or client tools.
- **New User Options** should be determined by your licensing options that can be viewed in CMC or license keys. Click **New Users are created as concurrent users** as it is a supported option for BO license within SHR.



11. In **Attribute Binding Options**, select **Import Full Name and Email Address** and **Give AD attribute binding priority over LDAP attribute binding**
12. In the **On-demand AD Update**, select **Update AD Group Graph and Aliases now** and click **Update**.

    On successful update of AD plug-in users or groups are synchronized with the BO repository.

    Verify if users or groups are added by going to CMC or users and groups.



Sign up for updates
hp.com/go/getupdated

May 2015

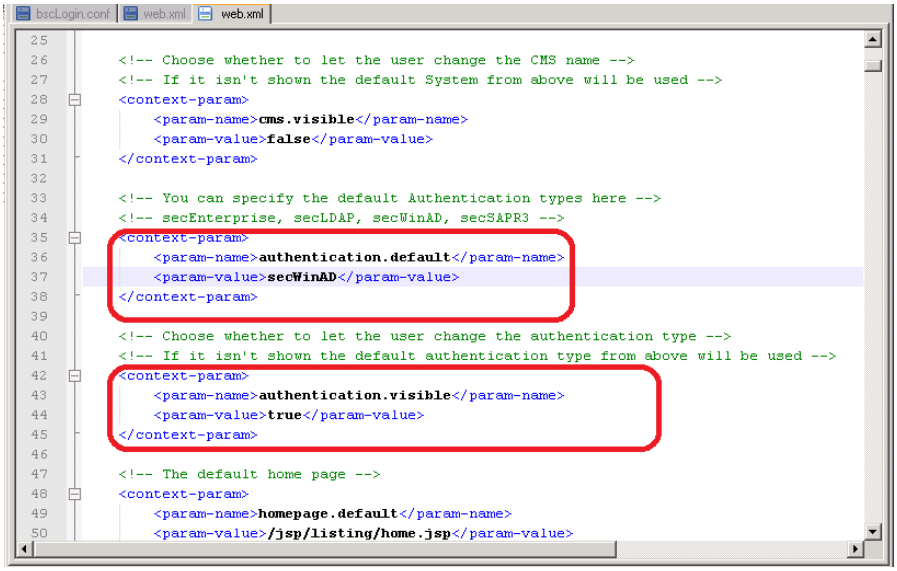
Configuring Tomcat web.xml File

To enable manual AD login, you have to configure Tomcat web.xml file for InfoView and CMC.

The Authentication dropdown in the InfoView and CMC login page is hidden by default.

To enable the dropdown box, follow these steps:

1. Open the file %PMDB_HOME%/BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml.
2. Set the **authentication.visible** flag to **True**.
3. Set the **authentication.default** to **secWinAD**.
4. Save the changes.



Configuring bscLogin.conf and Krb5.ini files

To configure bscLogin.conf and Krb5.ini files, follow these steps:

The two files bscLogin.conf and Krb5.ini should be created under the c:\winnt folder on the SHR server.

Note: The file names are case-sensitive.

a. Create the bscLogin.conf file

`bscLogin.conf` is used to load the Java Login Module and trace log on requests.

Create this file using the following code:

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

b. Create the Krb5.ini file

Sign up for updates
hp.com/go/getupdated

May 2015

Krb5.ini is used to configure the KDC's (Kerberos Key Distribution Center also known as domain controllers) that will be used for the Java log on requests.

c. Copy the default Krb5.ini and edit the following:

```
[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 = DCHOSTNAME.MYDOMAIN.COM
default_domain = MYDOMAIN.COM
}
```

The highlighted parameters in the above code should to be modified as the following:

a. Replace **MYDOMAIN.COM** with the same domain of your service account. All DOMAIN information must be in uppercase.

b. The default_realm value must exactly match the default domain value entered into the top of the AD page in the CMC.

c. Replace **MYDCHOSTNAME** with the hostname of a domain controller. For example, DCHOSTNAME is ADSERVER.DC4SHR.XYZ.COM.

Configuring Tomcat Java Option

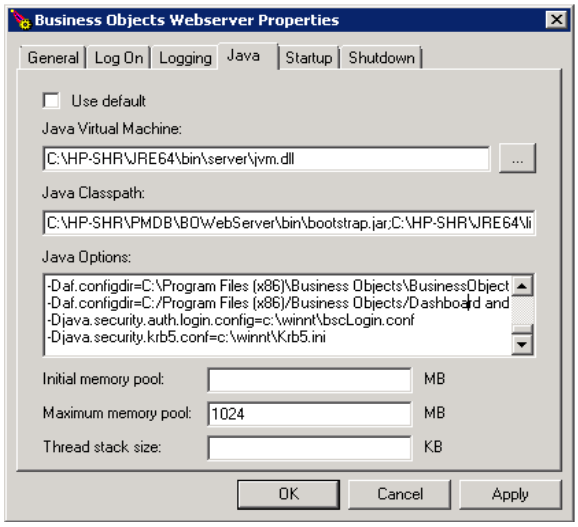
To configure Tomcat java options, follow these steps:

1. Stop the Tomcat service on SHR server.
2. Go to **Start > Programs >Tomcat >Tomcat Configuration**.
3. Enter the following to Java options in the **Java** tab :

```
-Djava.security.auth.login.config=c:\winnt\bscLogin.conf
-Djava.security.krb5.conf=c:\winnt\Krb5.ini
```

Sign up for updates
hp.com/go/getupdated

May 2015

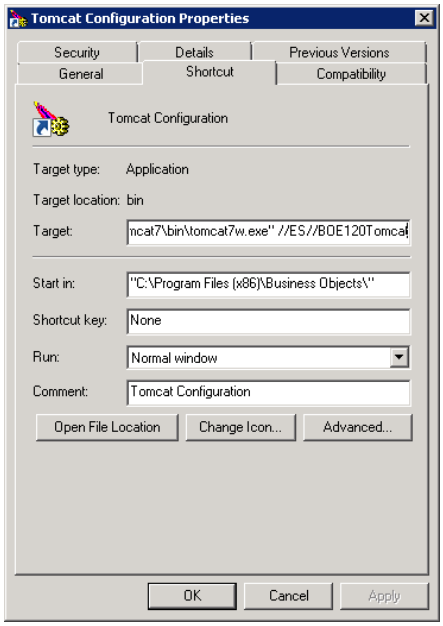


4. Restart the Tomcat service.

Tomcat configuration changes for SHR 9.40

To make the Tomcat configuration changes for SHR 9.40, follow these steps:

1. Right-click on **Tomcat Configuration** program in **Programs** menu.
2. Click on **Properties**.
3. Modify the path in **Target**. Replace **//ES//BOE120Tomcat7** with **//ES//BOE120Tomcat**.



4. Follow Step 1 of Configuring Tomcat Java Option.

Note: Once the AD users login to SHR Infoview page, based on the user roles you can provide them the permissions to access the SHR folders, universes and connections. This access will help the users to refresh SHR reports.

Sign up for updates
hp.com/go/getupdated

May 2015

For more details on how to create report User Accounts and Groups and Access Level Restrictions, see **SHR - Managing User Accounts and Groups** using the following URL:

https://hpln.hp.com/node/19476/attachment

Configuring SHR Administration Console for AD Authentication

AD authentication for SHR Administration Console is supported for versions SHR 9.31 onwards. Ensure that SHR is upgraded to SHR 9.31 or later version before you follow these steps:

1. Make the following changes to %PMDB_HOME%/data/config.prp:
   I. Set `bo.authType=secWinAD`
   II. Add the following lines of code to specify the location of the files bscLogin.conf and Krb5.ini:

   `java.security.auth.login.config=`*<absolute path of bscLogin.conf file>*

   `java.security.krb5.conf=`*<absolute path of Krb5.ini file>*

   Example: java.security.krb5.conf=C\:\\winnt\\Krb5.ini

   java.security.auth.login.config=C\:\\winnt\\bscLogin.conf

2. Enter the following command in **packagemgrSilent.ini** file located at %PMDB_HOME%/config/startup:

   `jargs=-Xmx256m -Dbsmr.home={bsmr.home} -DDPIPE_HOME={bsmr.home} -Dpmdb.home={bsmr.home} -Djava.security.auth.login.config=`*<absolute path of bscLogin.conf file>* `-Djava.security.krb5.conf=`*<absolute path of Krb5.ini file>*

3. Restart the SHR_PMDB_Platform_Administrator service.

Sign up for updates
hp.com/go/getupdated

May 2015

References

http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/40f4abf5-4d67-2e10-e48b-8db2cac73f8c?QuickLink=index&overridelayout=true&50968377367535

Sign up for updates
hp.com/go/getupdated

May 2015