Technical White Paper

Extending Microsoft Windows Active Directory Authentication to Access HPE Operations Bridge Reporter

For the Windows® Operation System

Software Version 10.00

Table of Contents

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

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 HPE Operations Bridge Reporter (OBR) reports, universes and the Administration Console.

Note: This document is applicable only for HPE Operations Bridge Reporter 10.x.

Goal

In your IT environment, if users are already using AD authentication it can be extended to access the OBR 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
OBRBOSERVER	BusinessObjects server installed along OBR
ADSERVER	Active Directory server configured to integrate the users or groups with OBR BOBJ Repository
ADBO_USER	Windows AD Service Account used to run BOBJ services
BOBJCMS/ OBRBOSERVER	Service Principle Name (SPN) to run BOBJ services using domain user account

To configure Microsoft Windows AD authentication for OBR 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 bscLogin.conf and Krb5.ini files
6. Configuring Tomcat Java Option
7. Configuring the AD Plug-in
8. Configuring BI LaunchPad to Enable Authentication
9. Configuring OBR Administration Console for AD Authentication

Sign up for updates
hp.com/go/getupdated

March 2016

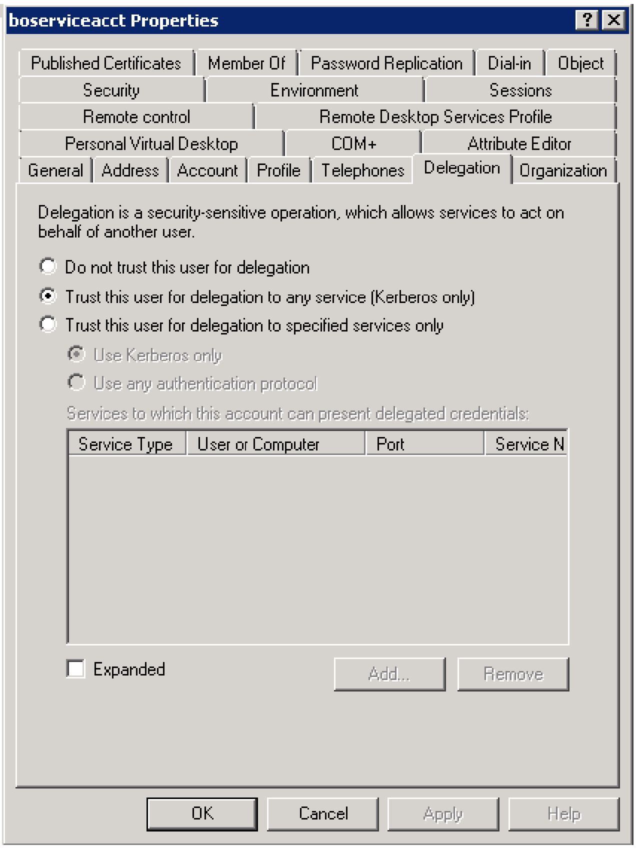
Configuring AD Authentication for OBR

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.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

● Trust this user for delegation to any service (Kerberos only)

○ Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

□ Expanded

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

March 2016

Hewlett Packard
Enterprise

Configuring Grants for the Service Account

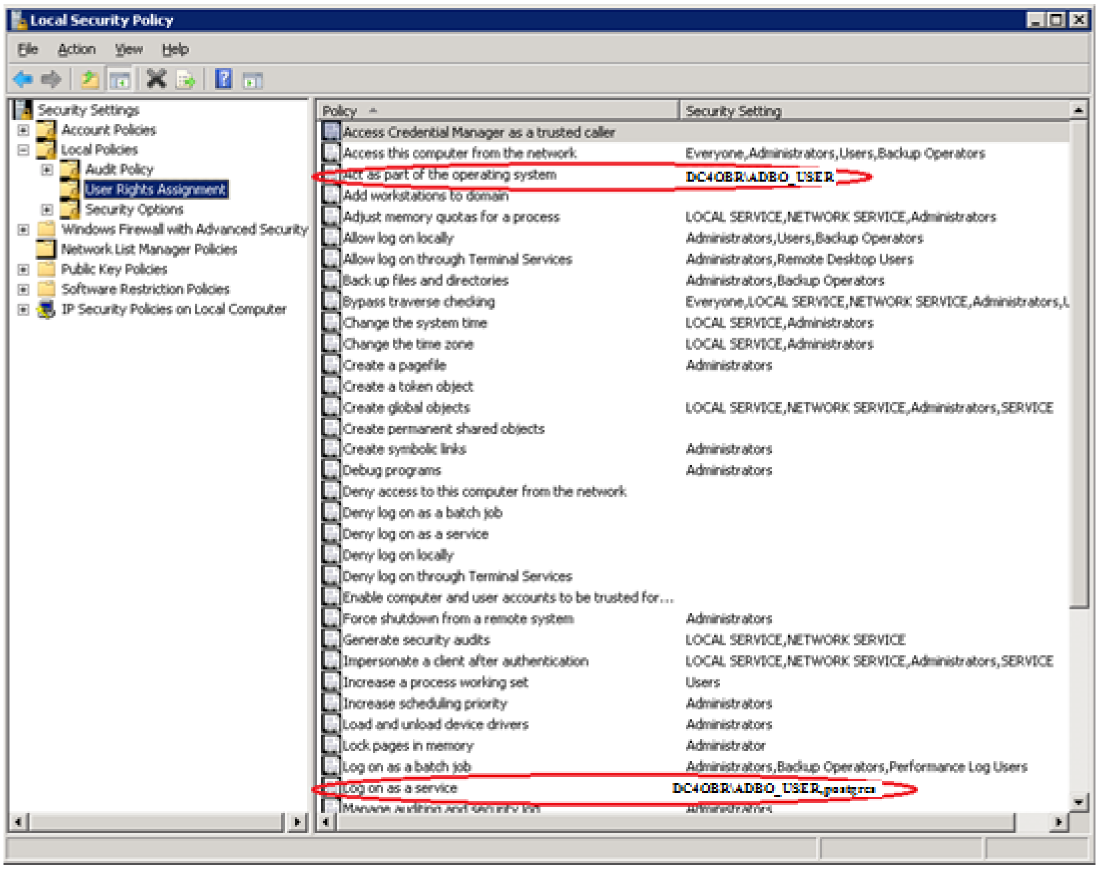
To support AD authentication, enable the service account to act as part of the operating system and log on as a service. This must be done on OBR BusinessObjects server (example: OBRBOSERVER) where the Server Intelligence Agent service is running.

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**.



Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,Users,Backup Operators
Act as part of the operating system	DC4OBR\ADBO_USER
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Administrators,Users,Backup Operators
Allow log on through Terminal Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,U
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Terminal Services	
Enable computer and user accounts to be trusted for...	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Increase a process working set	Users
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	Administrator
Log on as a batch job	Administrators,Backup Operators,Performance Log Users
Log on as a service	DC4OBR\ADBO_USER,postgres
Manage auditing and security log	Administrators

Sign up for updates
hp.com/go/getupdated

March 2016

Hewlett Packard
Enterprise

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

1. On the OBRBOSERVER 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. OBRBOSERVER Host name, for example OBRBOSERVER.XYZ.com.
   Where, `<serviceaccount>` is the name of the CMS service account. In this case, the `<serviceaccount>` is ADBO_USER.
   Example: setspn –A BOBJCMS /OBRBOSERVER.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 OBRBOSERVER, follow these steps:

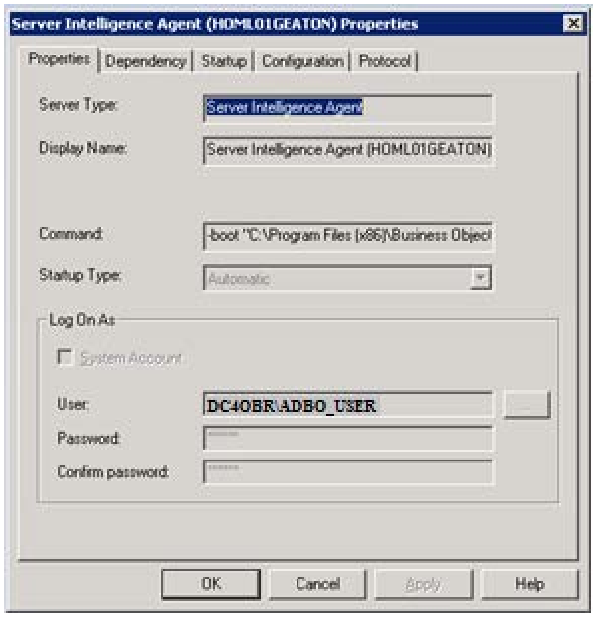
1. Start the Central Configuration Manager (CCM).
2. Stop the Server Intelligence Agent.
3. Double-click the **Server Intelligence Agent**. The **Server Intelligence Agent Properties** dialog box appears.
4. In the **Properties** tab:
   i. In the **Log On As**, uncheck **System Account** check box.
   ii. Type the user name and password for the service account.

Sign up for updates
hp.com/go/getupdated

March 2016

Hewlett Packard
Enterprise

iii. Click **Apply**, and then click **OK**.



Server Type: Server Intelligence Agent

Display Name: Server Intelligence Agent (HOML01GEATON)

Command: -boot "C:\Program Files (x86)\Business Object

Startup Type: Automatic

☐ System Account

User: DC4OBR\ADBO_USER

Password: ******

Confirm password: ******

5. Restart the Server Intelligence Agent.

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:\Windows folder on the OBR 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

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
```

Sign up for updates
hp.com/go/getupdated

```
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.DC4OBR.XYZ.COM.

Configuring Tomcat Java Option

To configure Tomcat java options, follow these steps:

1. Open command prompt in HPE OBR system and run the following commands:

   ```
   a. cd %PMDB_HOME%/BOWebServer/bin
   b. tomcat7w.exe //ES//BOE120Tomcat
   ```

   The **Business Objects Webserver Properties** windows is displayed.

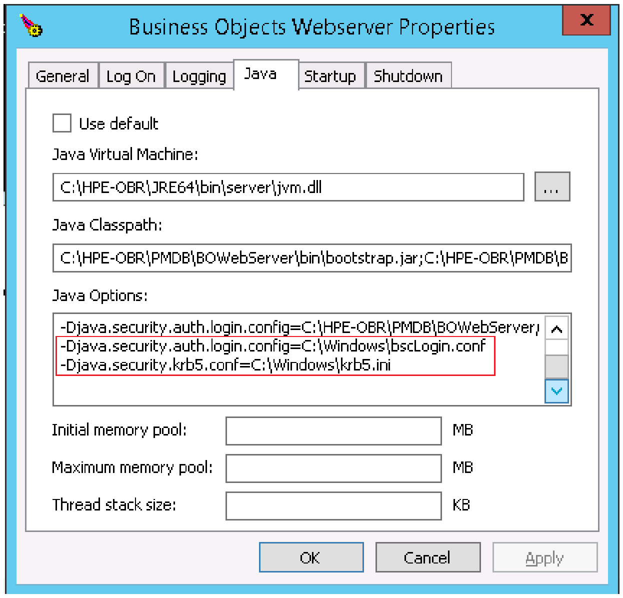
   Note: Once the AD users login to OBR Infoview page, based on the user roles you can provide them the permissions to access the OBR folders, universes and connections. This access will help the users to refresh OBR reports.

2. Enter the following to Java options in the **Java** tab :

   ```
   -Djava.security.auth.login.config=c:\Windows\bscLogin.conf
   ```

March 2016

```
-Djava.security.krb5.conf=c:\Windows\Krb5.ini
```



□ Use default

Java Virtual Machine: C:\HPE-OBR\JRE64\bin\server\jvm.dll

Java Classpath: C:\HPE-OBR\PMDB\BOWebServer\bin\bootstrap.jar;C:\HPE-OBR\PMDB\B

Java Options:

```
-Djava.security.auth.login.config=C:\HPE-OBR\PMDB\BOWebServer\
-Djava.security.auth.login.config=C:\Windows\bscLogin.conf
-Djava.security.krb5.conf=C:\Windows\krb5.ini
```

Initial memory pool: MB

Maximum memory pool: MB

Thread stack size: KB

3. Restart the Tomcat service.
4. Verify the Kerberos ticket:
   a. Open the command prompt on system where BO webserver is installed and navigate to *<BOE Install Direcotory>*\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`\jdk\bin` directory.

      For example, C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin.

   b. Run `kinit <username>` and press Enter.

      For example, kinit ADBO_USER

   c. Type the password.

      If the krb5.ini file was configured properly and the Java login module has been loaded, you should see the following message:

      ```
      New ticket is stored in cache file
      C:\Users\Administrator\krb5cc_Administrator
      ```

      Note: Do not continue with the AD Plug-in setup/configurations until you have successfully received a Kerberos ticket.

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:

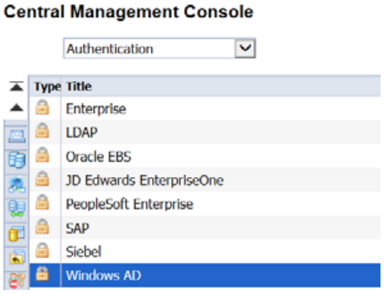
Sign up for updates
hp.com/go/getupdated

1. Log on to CMC as **Administrator** user and make ADBO_USER as member of '**Administrators**' group.

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

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

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



3. Select **Enable Windows Active Directory** check box.

4. In the **AD Configuration Summary**, click the link next to **AD Administration Name**.

5. Enter the credentials to read access to AD in the **Name** and **Password** textbox.

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

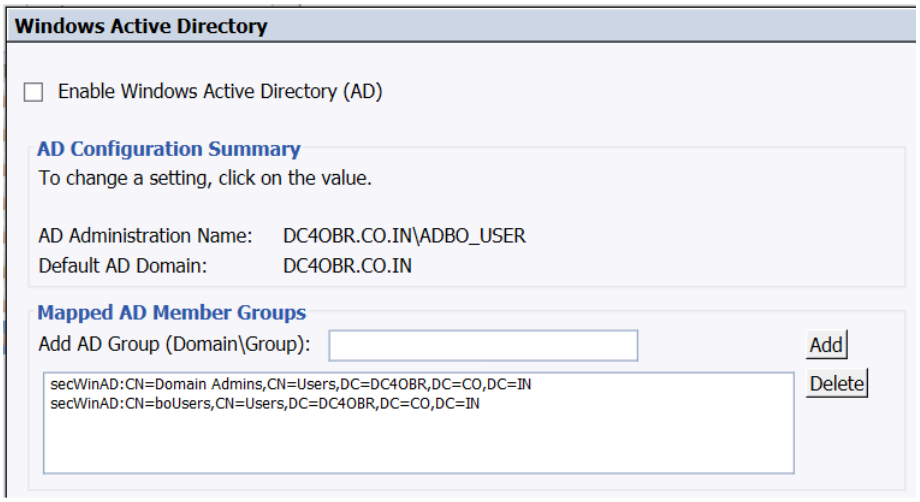
   Example: XYZ\ADBO_USER.

6. Enter the default domain in the **Default AD Domain** text box.

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

   Example: XYZ.COM.

7. 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**.


Windows Active Directory

□ Enable Windows Active Directory (AD)

AD Configuration Summary

To change a setting, click on the value.

AD Administration Name: DC4OBR.CO.IN\ADBO_USER

Default AD Domain: DC4OBR.CO.IN

Mapped AD Member Groups

Add AD Group (Domain\Group):

```
secWinAD:CN=Domain Admins,CN=Users,DC=DC4OBR,DC=CO,DC=IN
secWinAD:CN=boUsers,CN=Users,DC=DC4OBR,DC=CO,DC=IN
```

Sign up for updates
hp.com/go/getupdated

March 2016

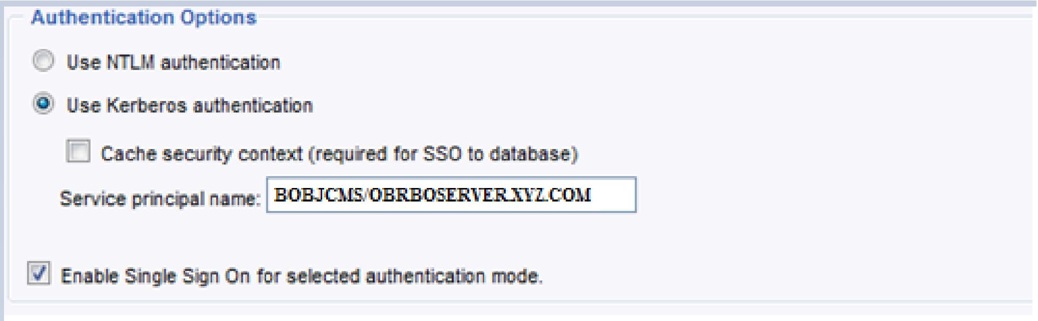
Mapped AD Member Groups:

- 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.

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

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

9. 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/OBRBOSERVER.XYZ.COM.



Authentication Options

○ Use NTLM authentication

● Use Kerberos authentication

□ Cache security context (required for SSO to database)

Service principal name: BOBJCMS/OBRBOSERVER.XYZ.COM

☑ Enable Single Sign On for selected authentication mode.

   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.

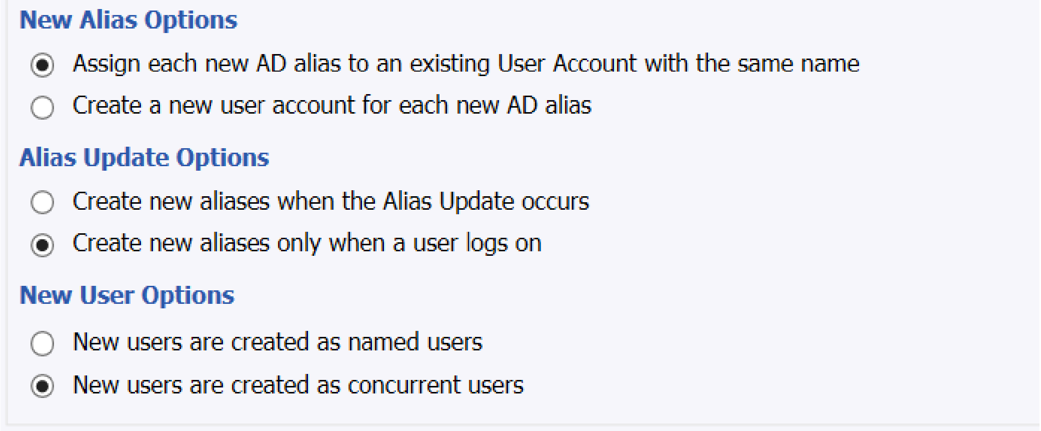
10. Select **Enable Single Sign On for selected authentication mode** (not required for manual AD authentication).

11. New User Alias Options:

    - **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.

March 2016

- **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 OBR.



New Alias Options

● Assign each new AD alias to an existing User Account with the same name

○ Create a new user account for each new AD alias

Alias Update Options

○ Create new aliases when the Alias Update occurs

● Create new aliases only when a user logs on

New User Options

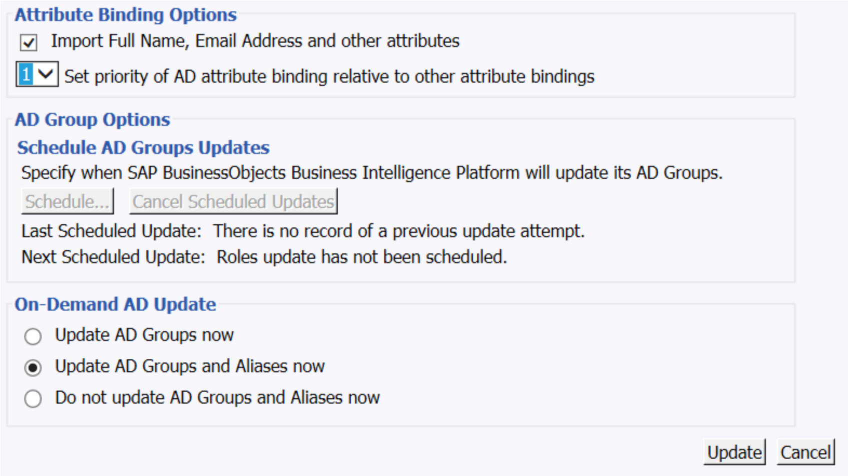
○ New users are created as named users

● New users are created as concurrent users

12. In **Attribute Binding Options**, select **Import Full Name and Email Address and other attributes** and select priority from drop down for **Set priority of AD attribute binding relative to other attribute bindings**.
13. 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 and groups are synchronized with the BO repository.

    Verify if users or groups are added in CMC or users and groups.



Attribute Binding Options

☑ Import Full Name, Email Address and other attributes

1 Set priority of AD attribute binding relative to other attribute bindings

AD Group Options

Schedule AD Groups Updates

Specify when SAP BusinessObjects Business Intelligence Platform will update its AD Groups.

Last Scheduled Update: There is no record of a previous update attempt.

Next Scheduled Update: Roles update has not been scheduled.

On-Demand AD Update

○ Update AD Groups now

● Update AD Groups and Aliases now

○ Do not update AD Groups and Aliases now

Configuring BI LaunchPad to Enable Authentication

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

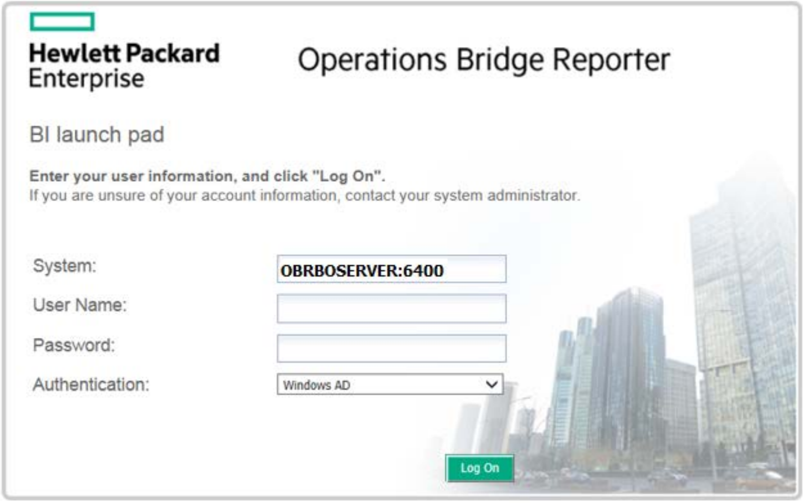
The Authentication dropdown in the InfoView and CMC login page is hidden by default.

To enable the dropdown box, follow these steps:

Sign up for updates
hp.com/go/getupdated

March 2016

1. Create a file **BIlaunchpad.properties** in **%PMDB_HOME%/BOWebServer/webapps/BOE/WEB-INF/config/custom** with the following entries:
   - **authentication.visible=True**
   - **authentication.default=secWinAD**
2. Save the changes.



BI launch pad

Enter your user information, and click "Log On".
If you are unsure of your account information, contact your system administrator.

System: OBRBOSERVER:6400
User Name:
Password:
Authentication: Windows AD

Configuring OBR Administration Console for AD Authentication

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\:\\Windows\\Krb5.ini

   java.security.auth.login.config=C\:\\Windows\\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 HPE_PMDB_Platform_Administrator service.

Sign up for updates
hp.com/go/getupdated

March 2016

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

March 2016

Hewlett Packard
Enterprise