WebSphere Portal 8.5

Manually Enable LDAP Security
Microsoft Active Directory

****

***** Table of Content *****

****

****

1 Information

This document will help with manually adding an Active Directory LDAP to the federated security of WebSphere Portal Server 8.5. The steps in the document can be used for other External User repository but the updated in the properties file may be different. To best determine the values, create LDIF files from the ldap and review the output.

Useful links:

- WebSphere Portal 8.5 Infocenter
  http://www-01.ibm.com/support/knowledgecenter/#!/SSHRKX_8.5.0/welcome/wp_welcome.html

- WebSphere Portal 8.5 Detailed System Requirements
  http://www-01.ibm.com/support/docview.wss?uid=swg27007791

- WebSphere Application Server 8.5.5 Infocenter
  http://www-01.ibm.com/support/knowledgecenter/?lang=en#!/SSAW57_8.5.5/as_ditamaps/was855_welcome_ndmp.html

This document is not written or supported by IBM Support

Name	Date	Version	Description
Loc Dang	Feb 21,2017	V1	Manually enabling AD LDAP to WebSphere Portal Server 8.5

2 Pre-requisites

1. Verify the WebSphere Portal system can ping the LDAP server

```
    ping <LDAP_HOSTNAME>
```

   Example: `ping my2008ad.ibm.com`

2. Verify the WebSphere Portal system can telnet to the LDAP Server port

```
    telnet <LDAP_HOSTNAME> <LDAP_PORT>
```

   Example: `telnet my2008ad.ibm.com 389`

   NOTE: If telnet is disabled on the system, either enable telnet or take the risk the firewall is open

3. If the LDAP is secure, import/install the WebSphere Portal environment through the WebSphere Application Server console or wsadmin command

3 WebSphere Portal Backup

1. Login to the WebSphere Portal file system
2. Run the following command on one line to backup the WebSphere Portal profile

```
        <WP_PROFILE>/bin/backupConfigEngine.(bat/sh) -nostop
```

Example:

```
WIN      E:\IBM\WebSphere\wp_profile\bin\backupConfig.bat -nostop
LINUX    /opt/IBM/WebSphere/wp_profile/bin/backupConfig.sh -nostop
AIX      /usr/IBM/WebSphere/wp_profile/bin/backupConfig.sh –nostop
SUN      /opt/IBM/WebSphere/wp_profile/bin/backupConfig.sh -nostop
```

NOTE: The backup file will be created in the directory it was ran

```
......................................................................
......................................................................
..............
ADMU5002I: 3,008 files successfully backed up
```

3. Verify the backup file was created

```
        WebSphereConfig_<DATE>.zip
```

Example: `WebSphereConfig_2017-02-14.zip`

4. Run the following command on one line to backup the WebSphere Portal property files

```
<WP_PROFILE>/bin/backupConfig.(bat/sh) backup-property-files-for-dbxfer
```

Example: WINDOW

```
E:\IBM\WebSphere\wp_profile\ConfigEngine\ConfigEngine.bat
                                       backup-property-files-for-dbxfer
```

Example: LINUX/SUN

```
/opt/IBM/WebSphere/wp_profile/ConfigEngine/ConfigEngine.sh
                                       backup-property-files-for-dbxfer
```

Example: AIX

```
/usr/IBM/WebSphere/wp_profile/ConfigEngine/ConfigEngine.sh
                                       backup-property-files-for-dbxfer
```

NOTE: The backup files will be created in a **backup** directory under the properties directory of the WebSphere Portal profile ConfigEngine

```
        <WP_PROFILE>/ConfigEngine/properties/backup/
```

Example:

```
WIN      E:\IBM\WebSphere\wp_profile\ConfigEngine\properties\backup
LINUX    /opt/IBM/WebSphere/wp_profile/ConfigEngine/properties/backup
AIX      /usr/IBM/WebSphere/wp_profile/ConfigEngine/properties/backup
SUN      /opt/IBM/WebSphere/wp_profile/ConfigEngine/properties/backup
```

4 Update Files

4.1 *wp_add_federated_ad.properties*

There are other variables that can be updated in this properties file. The ones in this document matches the updates that are done in the Configuration Wizard.

1. Login to the WebSphere Portal file system
2. Copy the helper file for the Active Directory LDAP to a temporary location

   FROM:

```
<WP_PROFILE>/ConfigEngine/config/helpers/wp_add_federated_ad.properties
```

   TO:

```
<TEMP>/wp_add_federated_ad.properties
```

Example: FROM - WINDOWS

```
E:\IBM\WebSphere\wp_profile\ConfigEngine\config\helpers\wp_add_federate
d_ad.properties
```

Example: FROM – LINUX/SUN

```
/opt/IBM/WebSphere/wp_profile/ConfigEngine/config/helpers/wp_add_federa
ted_ad.properties
```

Example: FROM – AIX

```
/usr/IBM/WebSphere/wp_profile/ConfigEngine/config/helpers/wp_add_federa
ted_ad.properties
```

3. Open the wp_add_federated_ad.properties with an editor

```
        <TEMP>/wp_add_federated_ad.properties
```

   Example:

```
WIN      F:\temp\wp_add_federated_ad.properties
LINUX    /opt/tmp/wp_add_federated_ad.properties
AIX      /usr/tmp/wp_add_federated_ad.properties
SUN      /opt/tmp/wp_add_federated_ad.properties
```

4. Update the following **VMM Federated LDAP Properties** variables

federated.ldap.id = ____

   Example: `myldapid`

```
(?) Specify a unique identifier for the repository within the cell.
The first time that you enable security, the ID can be an arbitrary
string.  The ID can contain only the following characters: Aphanumeric
(a-z, A-Z, 0-9, dash (-), and underscore (_).  The ID cannot start or
end with a dash (-) or an underscore (_), and must be a minimum of 3
characters and a maximum of 36 characters in length.
```

federated.ldap.host = ____

Example: `my2008ad.ibm.com`

```
(?) The host name of the primary LDAP server.  Enter either an IP
address or a domain name service (DNS) name.  If multiple load-balanced
LDAP servers are in use, type the hostname of the loca balancer.
During an update, the value of this entry must match the LDAP host name
of the existing repository that is entered in the LDAP ID.
```

federated.ldap.port = ____

Example: `389`

```
(?) Type the LDAP server port.  Typically port values for the LDAP
protocal are 389 for non-encrypted traffic, and 636 for encrypted
traffic.
```

federated.ldap.bindDN = ______________________________________

Example: `cn=ldapbind,cn=users,dc=ibm,dc=com`

```
(?) Type the DN that the application server uses to authenticate with
the LDAP server.  The ID is used for administrative operations, such as
conducting searches or creating user accounts.  The bind DN is used for
all operations to the LDAP server except validating individual user log
ins.  If you need to enable self enrllment or administration of new
users through the portal, the bind ID must have write authority to the
LDAP.  If the Bind DN and password are blan, the application server
binds anonymously.
```

NOTE: If the ldap.bindDN contains a '\', add an extra '\' after it. WebSphere Portal considers the \ as an escape character and requires another '\'.

Example:

```
LDAP DN = cn=bind \,ldap,cn=users,dc=ibm,dc=com
WP VALUE = cn=Bind \\,ldap,cn=users,dc=ibm,dc=com
```

federated.ldap.bindPassword = __________________________________

```
(?) Type the password for the bind DN user account.
```

federated.ldap.ldapServerType = ________________________________

Example: `AD`

```
(?) Select the LDAP server to integrate with.
```

federated.ldap.baseDN = ______________________________________

Example: `dc=ibm,dc=com`

```
(?) Specify the point in the LDAP directory information tree (DIT) that
serves as the "root" of the portal server's view.  WebSphere Portal has
visibility only of users and groups that are descendants of this point
in the DIT.
```

5. Update the following **Entity type Group** variables

federated.ldap.et.group.objectClasses = ____

Example: `group`

```
(?) Specify one or more object classes for the group entity type.
Separate multiple object classes with a semicolon(;).  Use object
classes that are unique to groups only.  If there are both users and
groups with an objectclass of 'top', then you cannot use the object
class 'top' here.
```

federated.ldap.et.group.objectClassesForCreate = ________________________________

```
(?) Type one or more object classes to use when an entity type is
created.  Separate multiple object classes with a semicolon (;).  If
the value of this field is the same as the LDAP group objectclasses,
then leave this field empty.  If your LDAP is read-only, meaning portal
is not allowed to write to it, then leave this field empty.
```

federated.ldap.et.group.searchBases = ____

Example: `ou=groups,dc=ibm,dc=com`

```
(?) VMM performs a search operation for each search base that you enter
in the field, which affects performance.  Minimize the number of search
bases.  Leave the field blank and use the baseEntries as the search
bases that are configured for this repository.  Specify one or more
search bases if you need to limit where VMM searches for groups to the
portion of the subtree below the baseEntries.  For example, if the base
Entries are high up in the LDAP tree and a search returns results that
should not be included.  Separate multiple search bases with a
semicolon (;).
```

6. Update the following **Entity type PersonAccount** variables

federated.ldap.et.personaccount.objectClasses = _________________________________

Example: `user`

(?) Type one or more object classes for the entity type. Use object classes that are unique to users. If there are both users and groups with an objectclass of ‘top’, then you cannot use the object class ‘top’ here. Separate multiple object classes with a semicolon (;)

federated.ldap.et.personaccount.objectClassesForCreate = ___________________________

(?) Specify one or more object classes to use when an entity type is created. If the value of this field is the same as the LDAP PersonAccount objectClasses field, leave this filed blank. If your LDAP is read-only, meaning portal is not allowed to it, leave this field blank. Separate multiple object classes with a semicolon(;).

federated.ldap.et.personaccount.searchBases = ____________________________________

Example: `cn=users,dc=ibm,dc=com`

NOTE: This field can be left blank

(?) VMM performs a search operation for each search base that you enter in the field, which affects performance. Minimize the number of search bases. Leave the field blank and use the baseEntries as the search bases that are configured for this repository. Specify one or more search bases if you need to limit where VMM searches for groups to the portion of the subtree below the baseEntries. For example, if the baseEntries are high up in the LDAP tree and a search returns results that should not be included. Separate multiple search bases with a semicolon (;).

7. Update the following **Group member attributes** variables

federated.ldap.gm.groupMemberName = ____________________________________

Example: `member`

(?) Type the LDAP attribute that is used as the group member attribute. This is the attribute within the group object that lists the members of that group.

federated.ldap.gm.objectClasses = ____

Example: `group`

(?) Type the group object class that contains the member attribute. If you do not enter a group object class, the member attribute applies to all group object classes.

federated.ldap.gm.scope = ____

Example: `direct`

> (?) The scope of the member attribute. This is similar to the scope setting for the membership attribute (which is the attribute on the user object that tells what groups the user is a member of), but in this case it tells VMM about the scope of the member record in the group object that tells what users are members of the group. Select **direct** if the LDAP member attribute in your LDAP server's group objects contains direct members only. Select **Nested** if the LDAP member attribute in your LDAP server's group objects contains direct memebers and nested members. Note: It is very unusual for this to be anything other then "Direct".

federated.ldap.gm.dummyMember = ____________________________________

NOTE: This field can be left blank

> (?) Many directory servers do not allow the creation of an empty group, meaning a group with no members. A dummy member enables group creation without requiring the creator to specify the first group member at the same time. When a group is created, a dummy member is created to satisfy the directory requirement. For Novell eDirectory, oracle Directory Server, and Windows Active Directory the dummy member must be empty or point to an existing emtry in LDAP.

8. Update the following **Advanced Properties** variables

federated.ldap.gc.name = ____

Example: `memberOf`

> (?) A membership attribute is an alternative way of getting group membershup information from the LDAP user registry. Leave the field empty if your LDAP does not support the group membership attribute. Group membership support consists of group objects that point at their members. For example, a groupOfUniqueNames object includes multiple uniqueMember records that contain the DNs of the users that are members of that group. Type the name of the attribute or virtual attribute in a user object that lists the group of which that user is a member.

federated.ldap.gc.scope = ____

Example: `direct`

> (?) Tell VMM how much information the LDAP server returns when portal requests the group membershup attribute value for a user object. The group membershup attribute is a value from the user object that contains the list of groups of which this user is a member. Select **All** if the LDAP server returns a complete list of all possible group memberships for a user. The list includes information for group nesting, dynamic memberships, and static direct group memberships. Select **Direct** if the LDAP server returns a list that contains only direct memberships. Select **Nested** if the LDAP server returns a list that contains both direct membershups and memberships from groups

```
nested within other groups, but does not include dynamic group
memberships.
```

federated.ldap.certificateMapMode = ____

Example: `EXACT_DN`

```
(?) Specify the filter certificate mapping property for the LDAP filter
if client certifucate autnetication is used for WebSphere Portal.  The
filter us used to map attributes in the client certificate to entried
within the LDAP repository.  You must select Certificate Filter as the
Certificate map mode to use the filter.  Filter syntasx: ${Client
certificate attribute}

This can be left blank if the federated.ldap.certificateMapMode is set
to EXACT_DN
```

federated.ldap.certificateFilter = ____

```
(?) Select the certificate map mode to use if client certificate
authentication is used for WebSphere Portal.  Select Certificate Filter
to specify a mapping filter between the client attribute and the LDAP
attribute.  If you select Certificate Filter, then you must also
specify the filter mapping in the Certificate filter field.  If DN in
the certificate must exactly match the user entry in the LDAP server,
including case and spaces, select Exact DN.
```

9. Save **wp_add_federated_ad.properties**

10. Change to the ConfigEngine directory of the WebSphere Portal profile

```
        <WP_PROFILE>/ConfigEngine
```

Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
SUN     /opt/IBM/WebSphere/wp_profile/ConfigEngine
```

11. Run the following command on one line to update the wkplc.properties with the information updated in the wp_add_federated_ad.properties

```
ConfigEngine.(bat/sh) -DparentProperties=<HELPER_FILE> -
DSaveParentProperties=true
```

Example: WINDOWS

```
ConfigEngine.bat
        -DparentProperties=F:\wp_add_federated_ad.properties
        -DSaveParentProperties=true
```

Example: LINUX/SUN

```
ConfigEngine.sh
        -DparentProperties=/opt/tmp/wp_add_federated_ad.properties
        -DSaveParentProperties=true
```

Example: AIX

```
ConfigEngine.sh
        -DparentProperties=/usr/tmp/wp_add_federated_ad.properties
        -DSaveParentProperties=true
```

12. Verify the script returns a BUILD SUCCESSFUL

4.2 wkplc.properties

1. Login to the WebSphere Portal file system

2. Open the wkplc.properties with an editor

```
<WP_PROFILE>/ConfigEngine/properties/wkplc.properties
```

Example: WINDOWS

```
E:\IBM\WebSphere\wp_profile\ConfigEngine\properties\wkplc.properties
```

Example: LINUX/SUN

```
/opt/IBM/WebSphere/wp_profile/ConfigEngine/properties/wkplc.properties
```

Example: AIX

```
/usr/IBM/WebSphere/wp_profile/ConfigEngine/properties/wkplc.properties
```

3. Verify/Update the following variables

personAccountParent = ______________________________________

Example:

```
FILEBASE        o=defaultWIMFileBasedRealm
LDAP            cn=users,dc=ibm,dc=com
```

NOTE: If the bind user does not have access to update the LDAP, set the personAccountParent to the file base repository

```
(?) Type the default parent of the entitype PersonAccount.  VMM creates
new users as a child of the parent when no other explicit parent is
specified.  This parent must be a descendent of the base DN of the LDAP
server.  It also must be a fully specified DN of the container,
including the base DN.  For example, if the base DN is
dc=yourco,dc=com, then the person account parent might be
cn=users,dc=yourco,dc=com.  It might also be
cn=users,ou=newPeopleGoHere,dc=yourco,dec=com.
```

groupParent = ____

Example:

```
FILEBASE        o=defaultWIMFileBasedRealm
LDAP            ou=groups,dc=ibm,dc=com
```

NOTE: If the bind user does not have access to update the LDAP, set the groupParent to the file base repository

```
(?) Type the default parent of the entity type group.  When an explicit
parent is not specified for a new group, VMM uses the default parent
that is specified here.  The parent must be a decendent of the base DN
of the LDAP server.  It also must be a fully specified DN of the
container, including the base DN value.
```

personAccountRdnProperties = ____

Example: `uid`

```
(?) The RDN attribute is the first attribute in the Distinguished Name.
Usually the attribute is "uid" or "cn", but it depends on how the DNs
in your LDAP server are set up.  It is possible to specify multiple
attribute names that are separated by semicolons, but this is highly
unusual.  Do not leave this property blank.
```

groupRdnProperties = ____

Example: `cn`

```
(?) The RDN attribute is the first attribute in the Distinguished Name.
Usually the attribute is "cn" for the group entity type, but it depends
on how the DNs in your LDAP server are set up.  It is possible to
specify mutliple attributes names that are are separated by semicolons,
but this is highly unusual.  Do not leave this property blank.
```

4. Save the wkplc.properties

5 Validate LDAP Server Settings

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

   Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
SUN     /opt/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) validate-federated-ldap -DWasPassword=<WASPWD>
```

4. Verify the script returns a BUILD SUCCESSFUL

6 Add LDAP User Registry to Existing Federated Repository

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

   Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) wp-create-ldap recycle-dmgr-if-cluster -
DWasPassword=<WASPWD>
```

4. Verify the script returns a BUILD SUCCESSFUL

7 Register WebSphere Application Server scheduler Task

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

   Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) stop-portal-server start-portal-server
reregister-scheduler-tasks -DWasPassword=<WASPWD> -
DPortalAdminPwd=<WPPWD>
```

4. Verify the script returns a BUILD SUCCESSFUL

8 Update User Registry Where New Users and Groups are Stored

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
SUN     /opt/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) wp-set-entitytypes -DWasPassword=<WASPWD>
```

4. Verify the script returns a BUILD SUCCESSFUL

9 Replace Portal and WAS Administrator User and Group (OPTIONAL)

This section is optional. The WebSphere Portal Administrator and WebSphere Application Server Administrator can stay in the File Base repository.

If the WebSphere Application Server Administrator and the WebSphere Portal Administrator are different users the 2 ConfigEngine command can be ran separately.

```
        wp-change-portal-admin-user
        wp-change-was-admin-user
```

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
SUN     /opt/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) wp-change-portal-admin-user wp-change-was-admin-
user -DnewAdminGroupId=<NEW_ADMINGRP> -DnewAdminId=<NEW_ADMIN> -
DnewAdminPw=<NEW_ADMINPWD> -DWasPassword=<WASPWD> -
DsaveParentProperties=true
```

Example:

```
ConfigEngine.(bat/sh) wp-change-portal-admin-user wp-change-was-admin-
user -DnewAdminGroupId=cn=portaladmins,ou=groups,dc=ibm,dc=com -
DnewAdminId=cn=portaladmin,cn=users,dc=ibm,dc=com -DnewAdminPw=passw0rd
-DWasPassword=passw0rd
```

NOTE: The user and group must exist in the External User repository (LDAP).

4. Verify the script returns a BUILD SUCCESSFUL

NOTE:

- Anything referencing <WASADMIN> will be using the new WebSphere Application Server Administrator
- Anything referencing <WPADMIN> will be using the new WebSphere Portal Server Administrator
- Anything referencing <WASPWD> will be using the new WebSphere Application Server Administrator password
- Anything referencing <WPPWD> will be using the new WebSphere Portal Server Administrator passw0rd

10 Recycle Servers After security Change

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

Example:

```
WIN      E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX    /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX      /usr/IBM/WebSphere/wp_profile/ConfigEngine
SUN      /opt/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) recycle-servers-after-security-change -
DWasPassword=<ORIGINAL_WASPWD> -DWasUserid=<ORIGINAL_WASADMIN>
```

Example:

```
ConfigEngine.(bat/sh) recycle-servers-after-security-change -
DWasPassword=passw0rd -DWasUserid=wpadmin
```

4. Verify the script returns a BUILD SUCCESSFUL

11 Update the Search Administration User

This section only needs to be completed if the WebSphere Portal Server has been updated.

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

   Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) start-portal-server action-fixup-after-security-
change-portal-wp.search.webscanner -DWasPassword=<WASPWD> -
DPortalAdminPwd=<WPPWD>
```

4. Verify the script returns a BUILD SUCCESSFUL

5. Run the following command on one line

```
ConfigEngine.(bat/sh) recycle-servers-after-security-change start-
portal-server -DWasPassword=<WASPWD> -DPortalAdminPwd=<WPPWD>
```

6. Verify the script returns a BUILD SUCCESSFUL

12 Verify All Defined Attributes

1. Login to the WebSphere Portal file system
2. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

   Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
```

3. Run the following command on one line

```
ConfigEngine.(bat/sh) wp-validate-federated-ldap-attribute-config -
DWasPassword=<WASPWD>
```

4. Verify the script returns a BUILD SUCCESSFUL

13 MemberFixer

This section only needs to be completed if the WebSphere Portal Administrative user has been updated.

1. Login to the WebSphere Portal file system
2. Open the MemberFixerModule.properties with an editor

```
<WP_PROFILE>/PortalServer/wcm/shared/app/config/wcmservices/
                                           MemberFixerModule.properties
```

Example: WINDOWS

```
E:\IBM\WebSphere\wp_profile\PortalServer\wcm\shared\app\config\wcmservi
ces\MemberFixerModule.properties
```

Example: LINUX/SUN

```
/opt/IBM/WebSphere/wp_profile/PortalServer/wcm/shared/app/config/wcmser
vices/MemberFixerModule.properties
```

Example: AIX

```
/usr/IBM/WebSphere/wp_profile/PortalServer/wcm/shared/app/config/wcmser
vices/MemberFixerModule.properties
```

3. Add the following on one line

```
<OLD_WPADMIN> -> <NEW_WPADMIN>
```

Example:

```
uid=wpadmin,o=defaultWIMFileBasedRealm ->
cn=portaladmin,cn=users,dc=ibm,dc=com
```

4. Save MemberFixerModule.properties

5. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

Example:

```
WIN     E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX   /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX     /usr/IBM/WebSphere/wp_profile/ConfigEngine
```

6. Run the following command on one line

```
ConfigEngine.(bat/sh) -DallLibraries=true -Dfix=true -DaltDn=update -
DmismatchedId=update -DinvalidDn=update -DnoRealmDn=true run-wcm-admin-
task-member-fixer -DWasPassword=<WASPWD> -DPortalAdminPwd=<WPPWD>
```

7. Verify the script returns a BUILD SUCCESSFUL

8. Run the following command on one line

```
ConfigEngine.(bat/sh) stop-portal-server start-portal-server -
DWasPassword=<WASPWD>
```

9. Verify the script returns a BUILD SUCCESSFUL

14 Map Attributes

1. Login to the WebSphere Portal file system
2. Open the **wkplc.properties** file with an editor

```
        <WP_PROFILE>/ConfigEngine/properties/wkplc.properties
```

Example: WINDOWS

```
E:\IBM\WebSphere\wp_profile\ConfigEngine\properties\wkplc.properties
```

Example: LINUX/SUN

```
/opt/IBM/WebSphere/wp_profile/ConfigEngine/properties/wkplc.properties
```

Example: AIX

```
/usr/IBM/WebSphere/wp_profile/ConfigEngine/properties/wkplc.properties
```

3. Update the following variables

```
federated.ldap.attributes.nonSupported=certificate,members

federated.ldap.attributes.nonSupported.delete=

federated.ldap.attributes.mapping.ldapName=mail,title

federated.ldap.attributes.mapping.portalName=ibm-primaryEmail,ibm-
jobTitle

federated.ldap.attributes.mapping.entityTypes=PersonAccount
```

4. Save **wkplc.properties**
5. Change to the ConfigEngine of the WebSphere Portal Server

```
        <WP_PROFILE>/ConfigEngine
```

Example:

```
WIN      E:\IBM\WebSphere\wp_profile\ConfigEngine
LINUX    /opt/IBM/WebSphere/wp_profile/ConfigEngine
AIX      /usr/IBM/WebSphere/wp_profile/ConfigEngine
```

6. Run the following command on one line

```
ConfigEngine.(bat/sh) wp-update-federated-ldap-attribute-config -
DWasPassword=<WASPWD>
```

7. Verify the script returns a BUILD SUCCESSFUL
8. Restart all Java Process

Standalone: WebSphere_Portal

```
<WP_PROFILE>/bin/stopServer.(bat/sh) WebSphere_Portal -user <WASADMIN>
-password <WASPWD>

<WP_PROFILE>/bin/startServer.(bat/sh) WebSphere_Portal
```

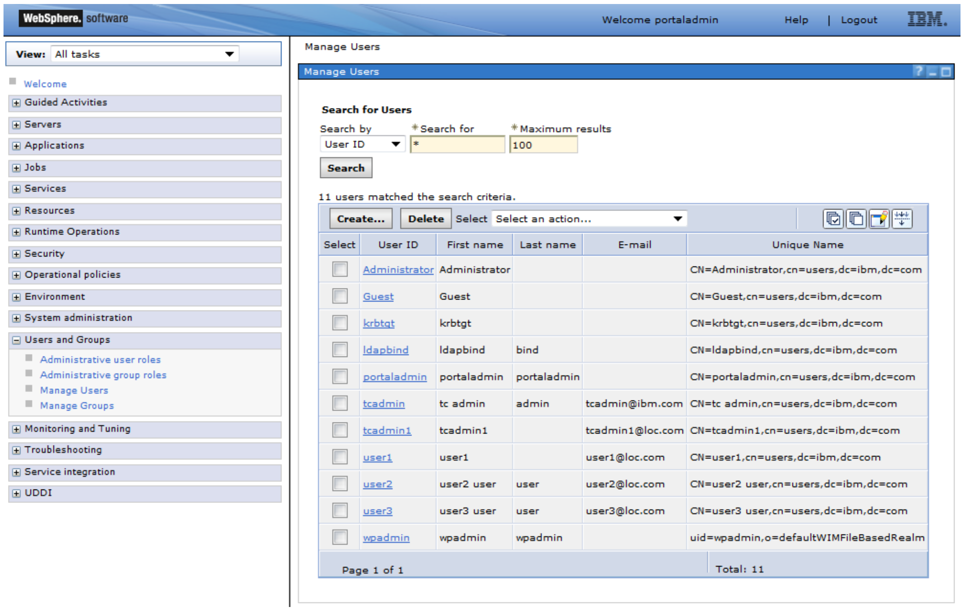
Cluster: Deployment Manager, Nodeagents, WebSphere_Portal

```
<WP_PROFILE>/bin/stopServer.(bat/sh) WebSphere_Portal –user <WASADMIN>
-password <WASPWD>

<WP_PROFILE>/bin/stopNode.(bat/sh) –user <WASADMIN> -password <WASPWD>

<DMGR_PROFILE>/bin/stopManager.(bat/sh) –user <WASADMIN> -password
<WASPWD>

<DMGR_PROFILE>/bin/startManager.(bat/sh) –user <WASADMIN> -password
<WASPWD>

<WP_PROFILE>/bin/startNode.(bat/sh)

<WP_PROFILE>/bin/startServer.(bat/sh) WebSphere_Portal
```

15 Validate

15.1 WebSphere Application Server

Verify WebSphere Application Server can list the LDAP user and groups.



Search for Users

Search by: User ID
* Search for: *
* Maximum results: 100

Search

11 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
□	Administrator	Administrator			CN=Administrator,cn=users,dc=ibm,dc=com
□	Guest	Guest			CN=Guest,cn=users,dc=ibm,dc=com
□	krbtgt	krbtgt			CN=krbtgt,cn=users,dc=ibm,dc=com
□	ldapbind	ldapbind	bind		CN=ldapbind,cn=users,dc=ibm,dc=com
□	portaladmin	portaladmin	portaladmin		CN=portaladmin,cn=users,dc=ibm,dc=com
□	tcadmin	tc admin	admin	tcadmin@ibm.com	CN=tc admin,cn=users,dc=ibm,dc=com
□	tcadmin1	tcadmin1		tcadmin1@loc.com	CN=tcadmin1,cn=users,dc=ibm,dc=com
□	user1	user1		user1@loc.com	CN=user1,cn=users,dc=ibm,dc=com
□	user2	user2 user	user	user2@loc.com	CN=user2 user,cn=users,dc=ibm,dc=com
□	user3	user3 user	user	user3@loc.com	CN=user3 user,cn=users,dc=ibm,dc=com
□	wpadmin	wpadmin	wpadmin		uid=wpadmin,o=defaultWIMFileBasedRealm

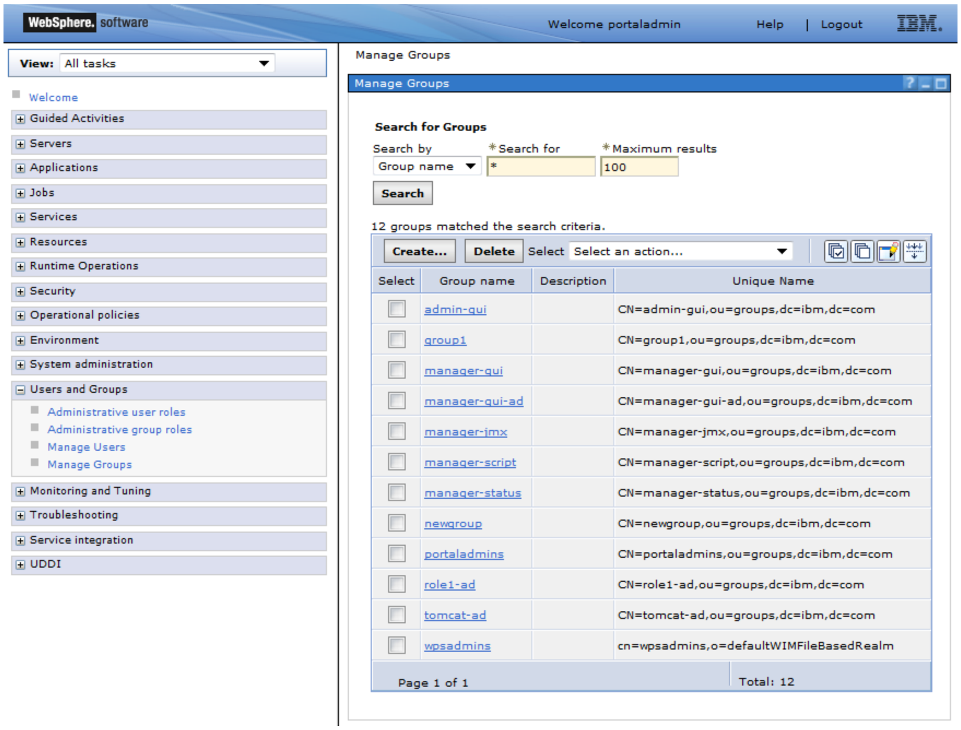
Page 1 of 1   Total: 11

1. Open a browser and set the URL to the WebSphere Application Server console
   `http://<HOSTNAME>:<PORT>/ibm/console`

   Example:

Standalone `http://wps85-64.ibm.com:10041/ibm/console`
Cluster `http://mydmgr.ibm.com:9043/ibm.console`

2. Login as the WebSphere Application Server Administrator
3. Navigate to Users and Groups > Manage Users
4. Verify there are LDAP users in the list



Search for Groups

Search by: Group name
* Search for: *
* Maximum results: 100

Search

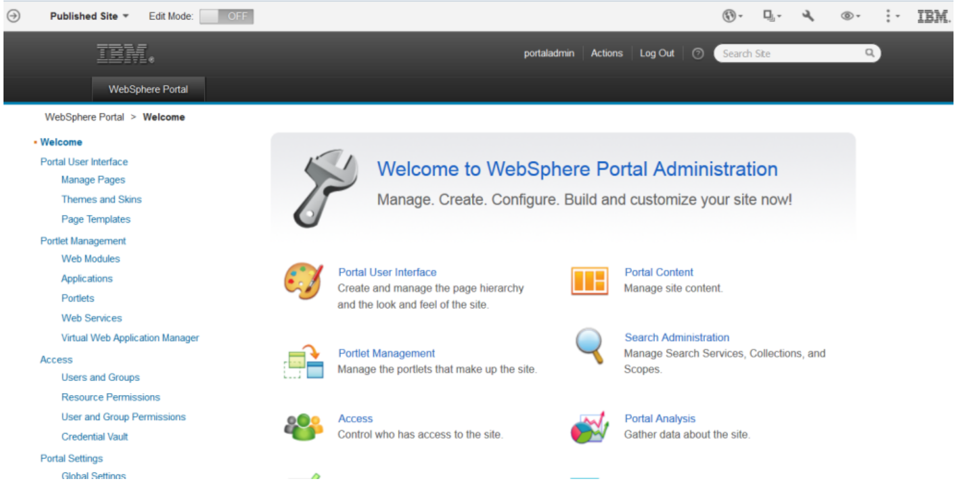
12 groups matched the search criteria.

Select	Group name	Description	Unique Name
□	admin-gui		CN=admin-gui,ou=groups,dc=ibm,dc=com
□	group1		CN=group1,ou=groups,dc=ibm,dc=com
□	manager-gui		CN=manager-gui,ou=groups,dc=ibm,dc=com
□	manager-gui-ad		CN=manager-gui-ad,ou=groups,dc=ibm,dc=com
□	manager-jmx		CN=manager-jmx,ou=groups,dc=ibm,dc=com
□	manager-script		CN=manager-script,ou=groups,dc=ibm,dc=com
□	manager-status		CN=manager-status,ou=groups,dc=ibm,dc=com
□	newgroup		CN=newgroup,ou=groups,dc=ibm,dc=com
□	portaladmins		CN=portaladmins,ou=groups,dc=ibm,dc=com
□	role1-ad		CN=role1-ad,ou=groups,dc=ibm,dc=com
□	tomcat-ad		CN=tomcat-ad,ou=groups,dc=ibm,dc=com
□	wpsadmins		cn=wpsadmins,o=defaultWIMFileBasedRealm

Page 1 of 1 Total: 12

5. Navigate to Users and Groups > Manage Groups
6. Verify there are LDAP groups in the list

15.2 WebSphere Portal Server



Welcome to WebSphere Portal Administration

Manage. Create. Configure. Build and customize your site now!

Portal User Interface: Create and manage the page hierarchy and the look and feel of the site.

Portal Content: Manage site content.

Portlet Management: Manage the portlets that make up the site.

Search Administration: Manage Search Services, Collections, and Scopes.

Access: Control who has access to the site.

Portal Analysis: Gather data about the site.

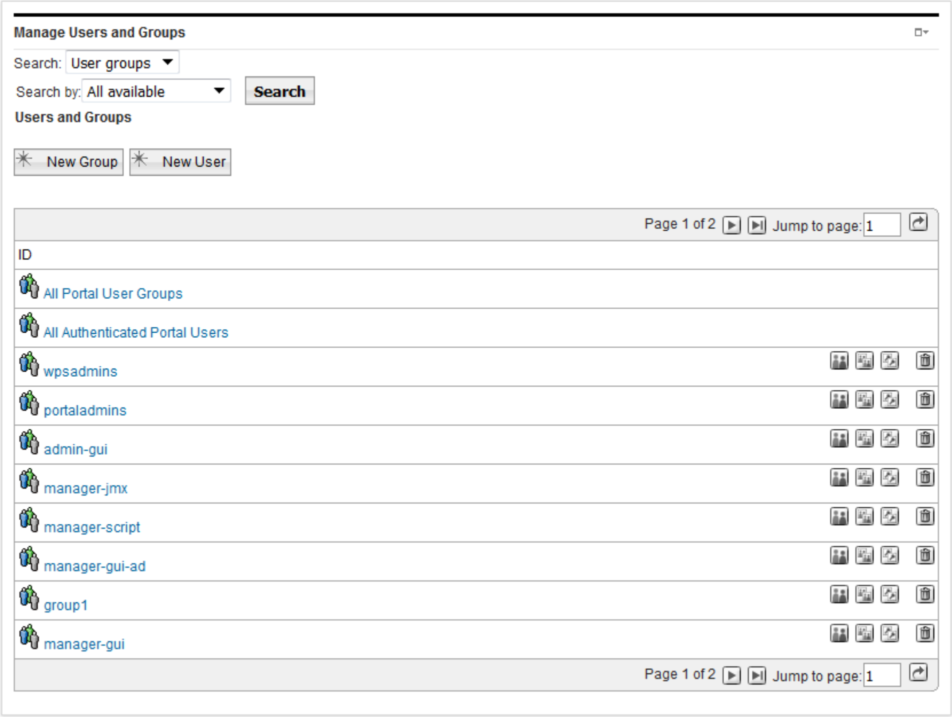
1. Open a browser and set the URL to the WebSphere Portal Server Administration page

```
http://<HOSTNAME>:<PORT>/wps/myportal/Administration
```

Example:

```
http://wps85-64.ibm.com:10039/wps/myportal/Administration
```

2. Login as the WebSphere Application Server Administrator
3. Navigate to Access > users and Groups



Manage Users and Groups

Search: User groups

Search by: All available

Users and Groups

Page 1 of 2 Jump to page: 1

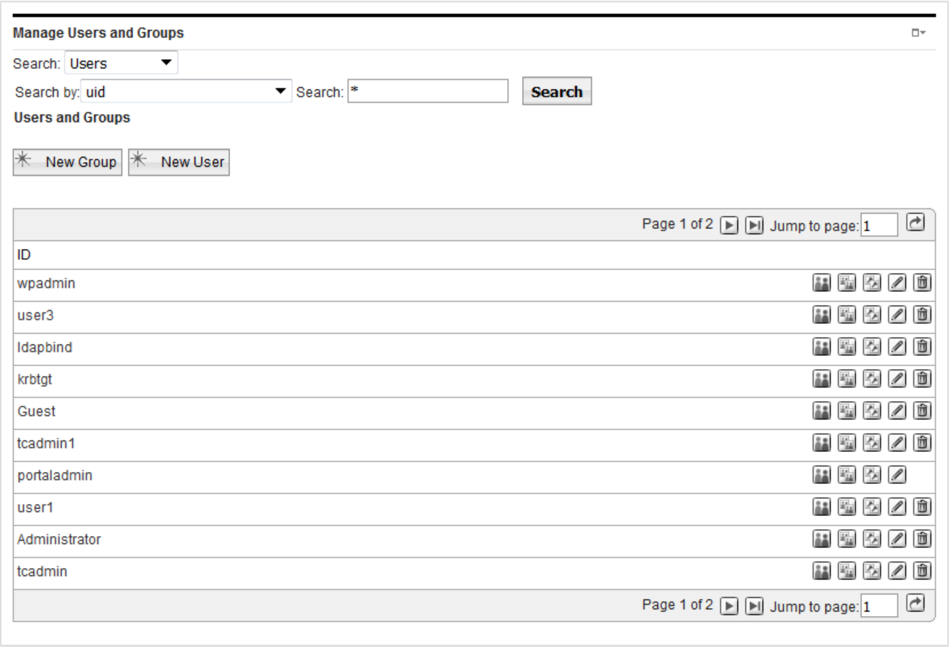
ID
All Portal User Groups
All Authenticated Portal Users
wpsadmins
portaladmins
admin-gui
manager-jmx
manager-script
manager-gui-ad
group1
manager-gui

Page 1 of 2 Jump to page: 1

4. In the **Search** dropdown, select User groups
5. In the **Search by** dropdown, select **All available**
6. Click Search

NOTE: If there are too many groups, this may result in a to many group message. Under **Search by**, selected a category and search for something more specific

- cn
- changeType
- seeAlso
- displayName
- businessCategory
- description



Manage Users and Groups

Search: Users

Search by: uid Search: * **Search**

Users and Groups

New Group New User

Page 1 of 2 Jump to page: 1

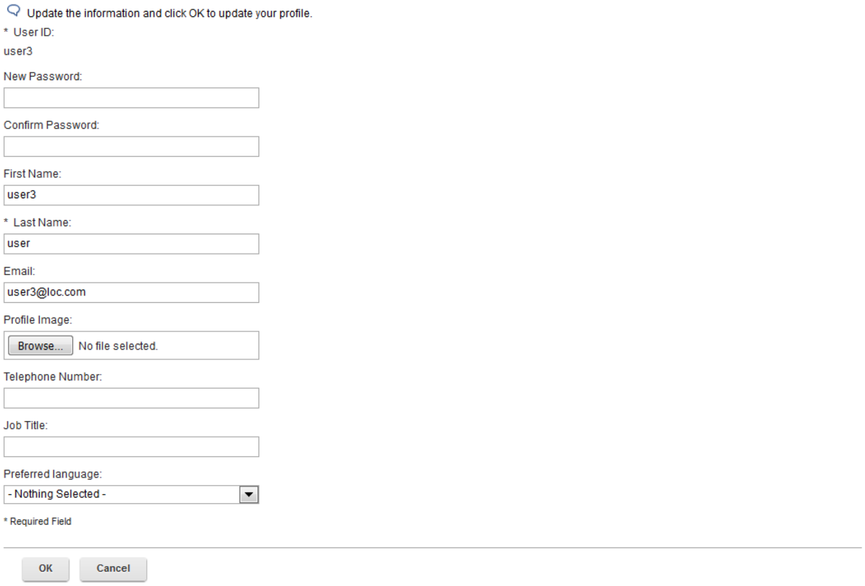
ID
wpadmin
user3
ldapbind
krbtgt
Guest
tcadmin1
portaladmin
user1
Administrator
tcadmin

Page 1 of 2 Jump to page: 1

7. In the **Search** dropdown, select **Users**
8. In the **Search by**, select one of the following categories. In the example, **uid** was selected
9. Under the **Search** field, enter a search criteria.

   NOTE: If there are too many users that meet the search criteria, this may result in a to many user message. Set the search criteria to something more exact.

10. Click on the edit icon ✎ right of one of the ldap user. In the example, **user3** was selected.



Update the information and click OK to update your profile.

* User ID:
user3

New Password:

Confirm Password:

First Name:
user3

* Last Name:
user

Email:
user3@loc.com

Profile Image:
Browse... No file selected.

Telephone Number:

Job Title:

Preferred language:
- Nothing Selected -

* Required Field

OK Cancel

11. Verify the Email field has a value. If it does not, check the LDAP to verify if the user has a mail attribute.