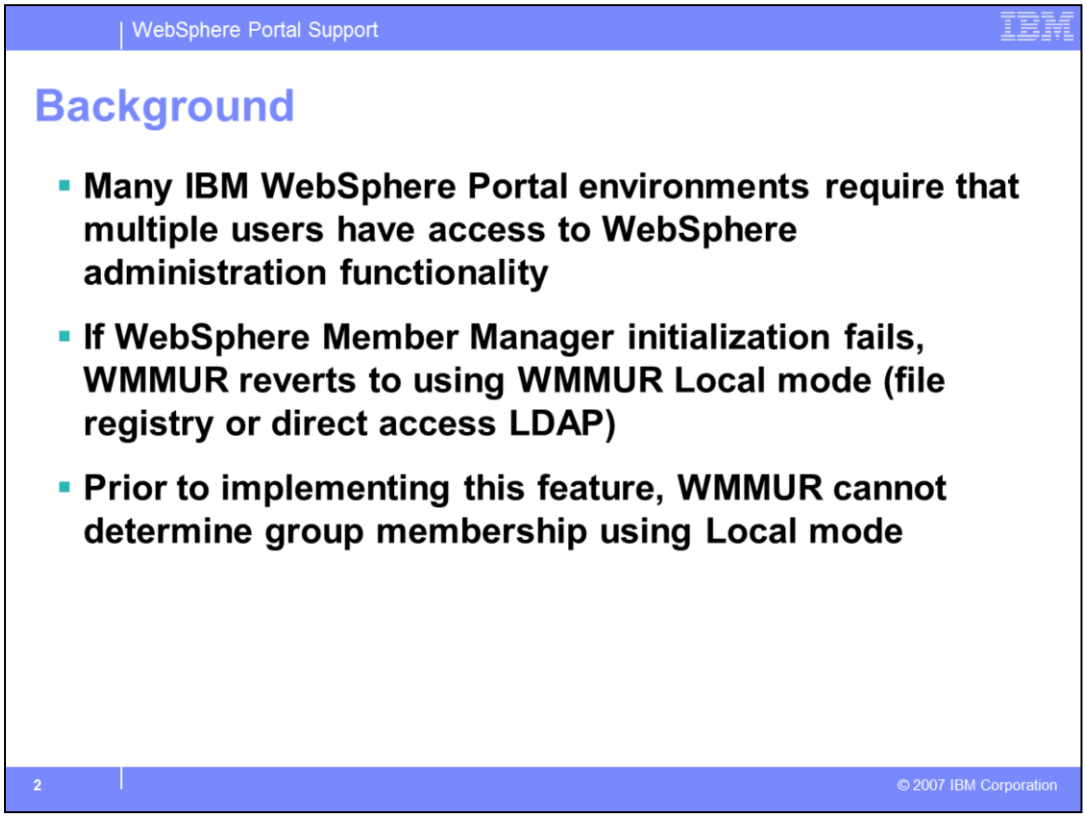
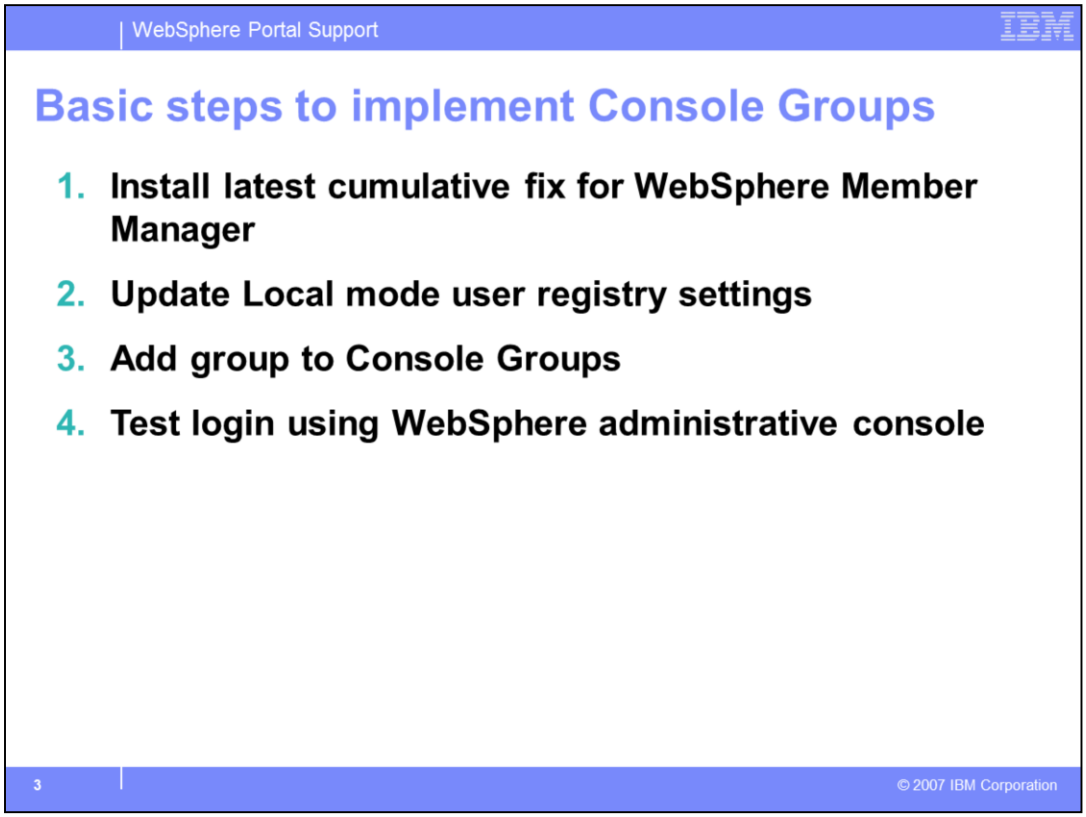
The presentation discusses the new IBM WebSphere® Member Manager user registry (WMMUR) group membership support feature recently added to WebSphere Member Manager.

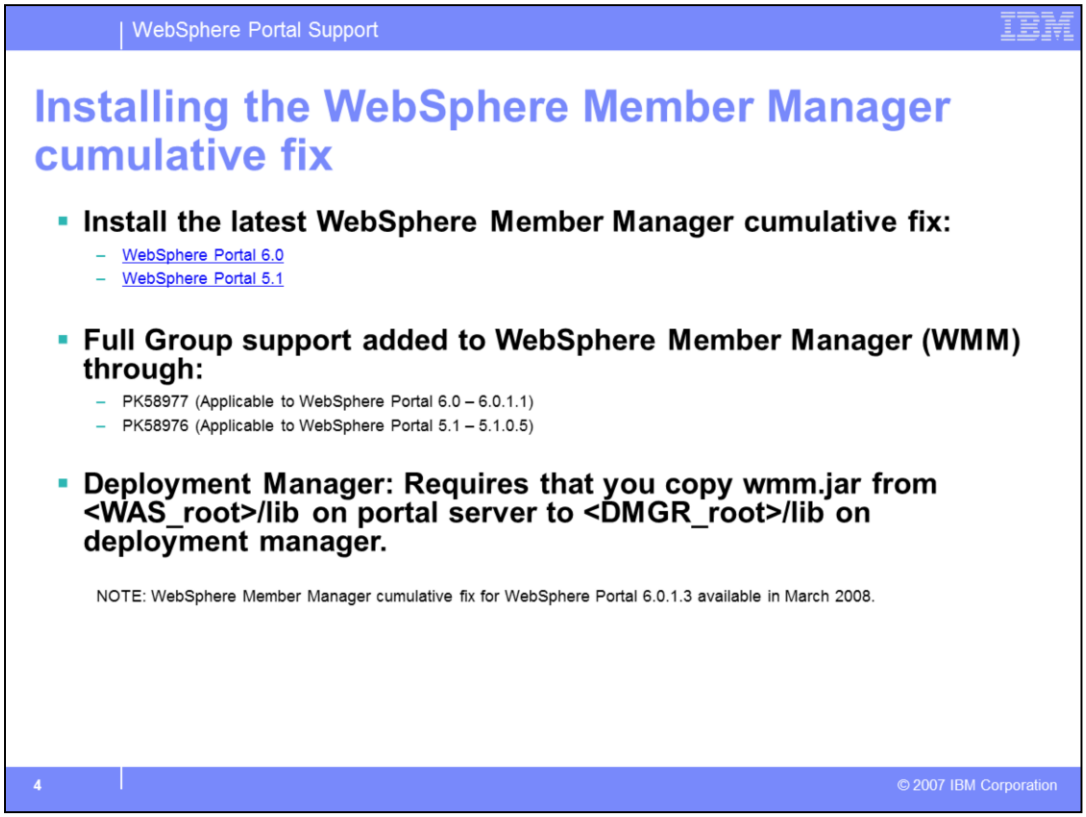


The WMMUR group membership support feature improves the efficiency of administering users who need access to various administrative functions in WebSphere Application Server. This feature pertains specifically to WebSphere Portal environments that use realm support security. Meaning that, if WebSphere Member Manager fails to initialize, or if the server cannot use wmm.xml properties to contact the LDAP server, WMMUR can use either the Local mode options of file registry or direct access LDAP to look up a user. Prior to implementing this feature, you have to add every user to Console Users to authorize them to access various functions of WebSphere Application Server administration. Now, you can create a group of users in the user registry which you can then reference in Console Groups.

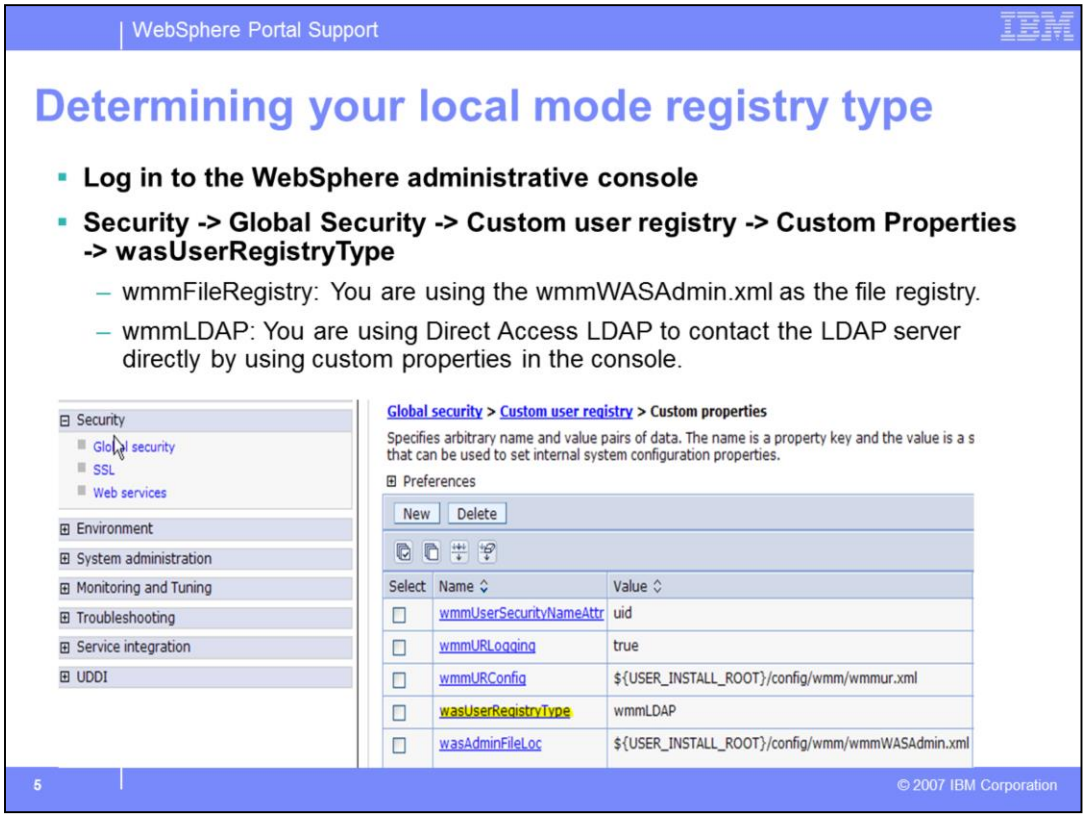


Here are the basic steps for implementing Console Groups through both registry options for WMMUR. First, install the latest cumulative fix for WebSphere Member Manager.

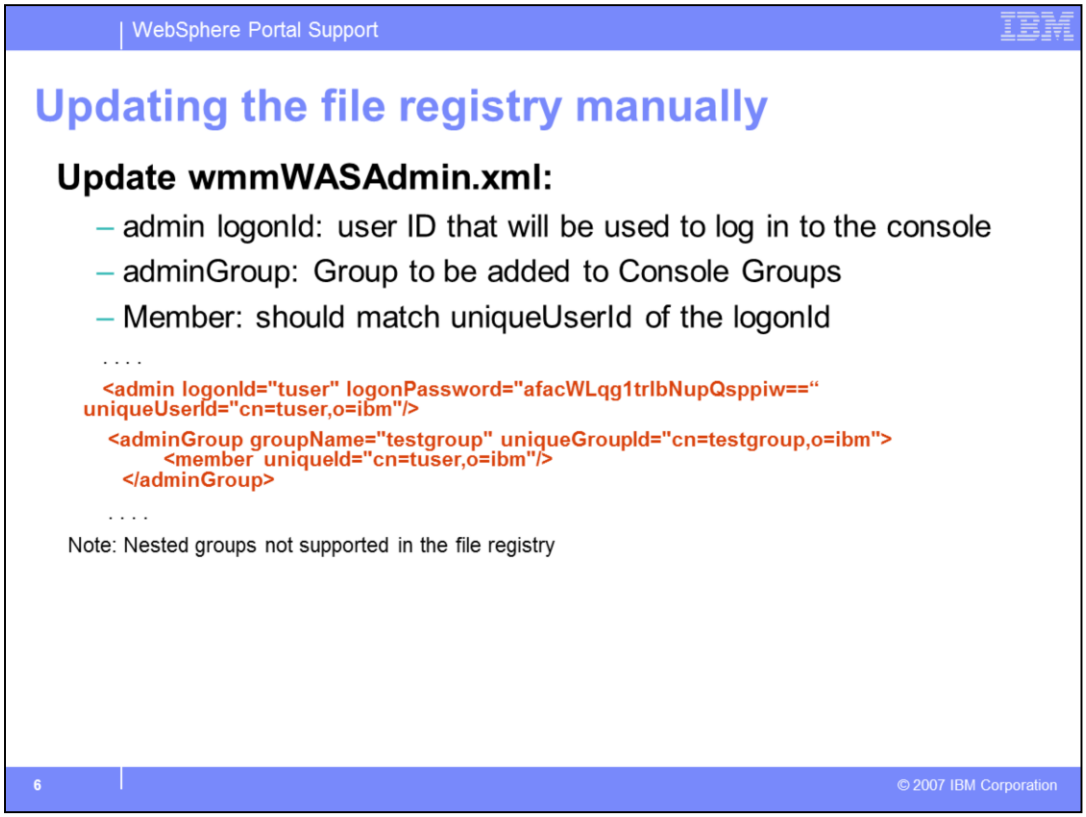
Next, update the appropriate user registry settings for your Local mode environment. Once your user registry is configured, you can add the Console Group through the WebSphere administrative console. Finally, to test the issue, log in to the console using a user ID from the group you just added.



For group membership support to function, you must update your WebSphere Member Manager code, as there are no current versions of WebSphere Portal that include the updated code. Here are links to the WebSphere Member Manager code for both WebSphere Portal version 5.1 and version 6.0. Also provided here are the APAR numbers of the fixes necessary for full WMMUR group membership support. You can compare these APAR numbers to your installed version of the WebSphere Member Manager cumulative fix. In a clustered environment, after you install the fix onto WebSphere Portal, you must copy the wmm.jar file from <WAS_root>/lib on the portal server over to the <DMGR_root>/lib on the deployment manager.



To determine the WMMUR Local mode user registry type configured for your environment, you can log in to the WebSphere administrative console and navigate to Security -> Global Security -> Custom user registry -> Custom Properties. If you used the enable-security-wmmur-ldap task to enable security, you will have a custom property named "wasUserRegistryType" or "WASUSER_REGISTRY_TYPE". A value of "wmmFileRegistry“ indicates that your Local mode user registry is in the wmmWASadmin.xml, located in the <WP_root>/wmm for stand-alone systems and in <DMGR_profile_root>/config/wmm for clustered systems. A value of "wmmLDAP“ indicates that your Local mode user registry is Direct Access LDAP, meaning that WMMUR will use the defined custom properties to contact the LDAP directly.



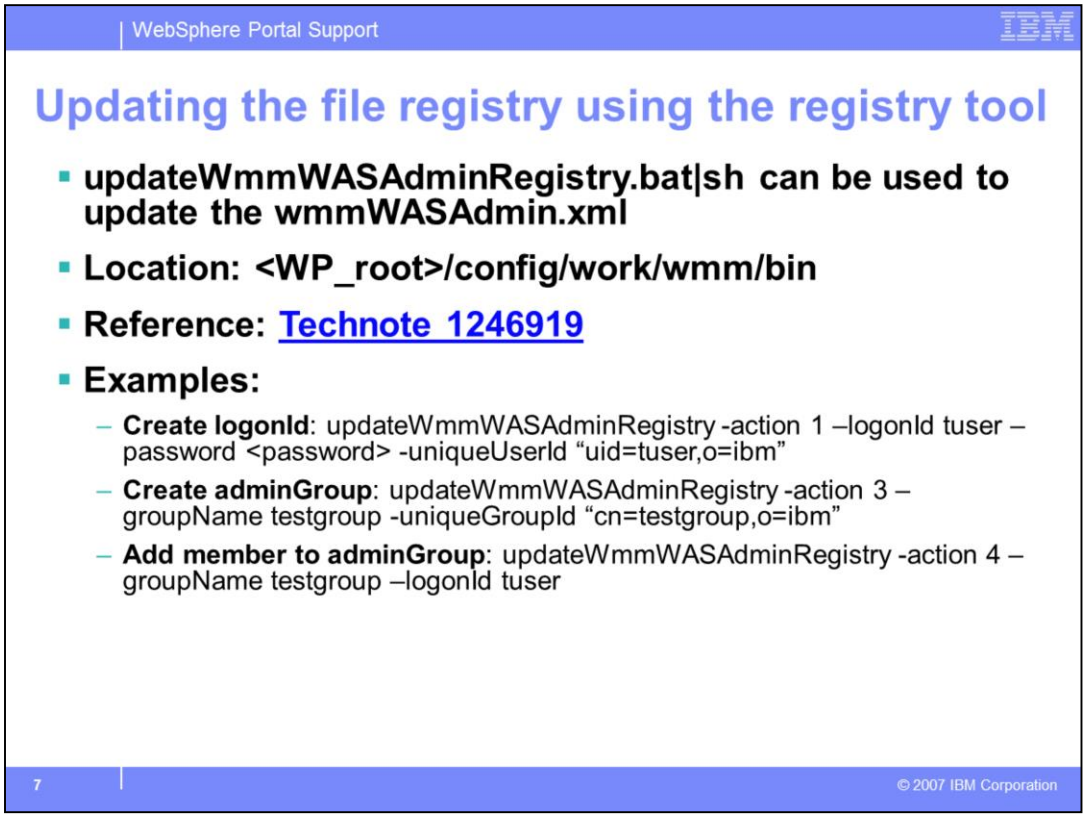
If you are using the Localmode file registry, then one option for updating the file registry settings is to manually modify the wmmWASAdmin.xml to include three entries:

-admin logonId, which includes password and uniqueId for the user that needs access to the WebSphere administrative console

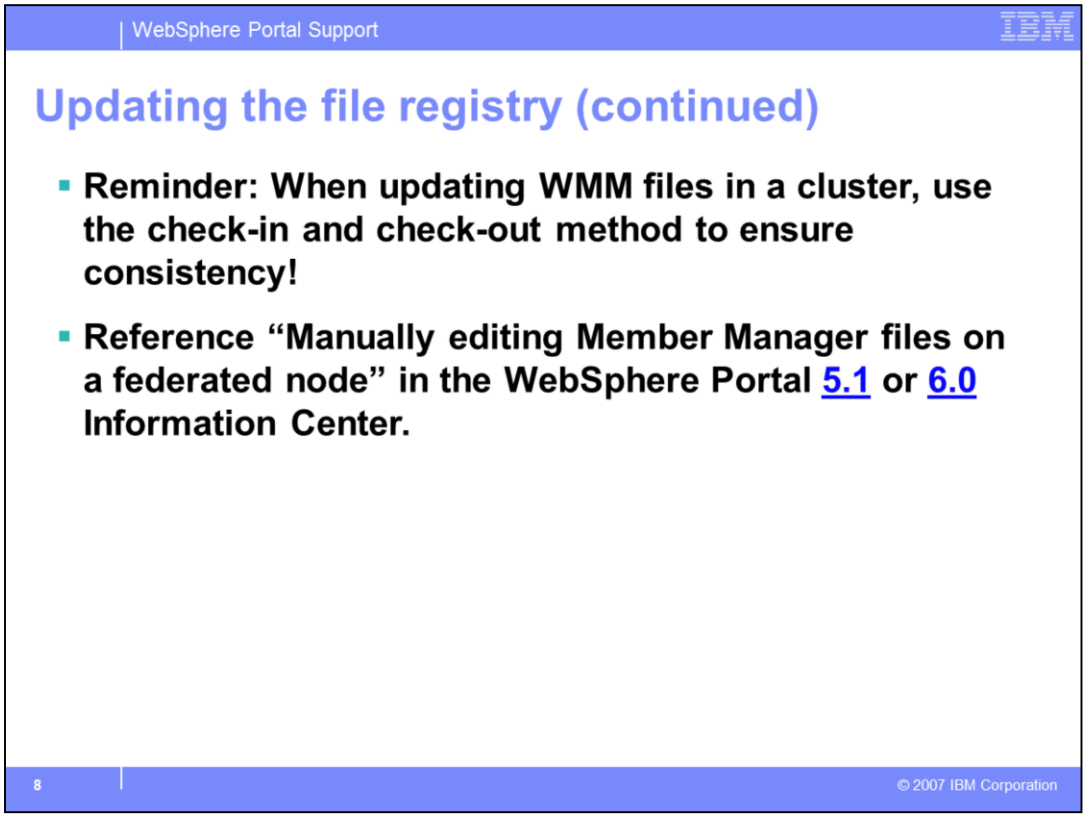
-adminGroup, which includes the groupName and uniqueGroupId for the group to be added to Console Groups.

-member, which includes the uniqueId of the user that needs access to the console.

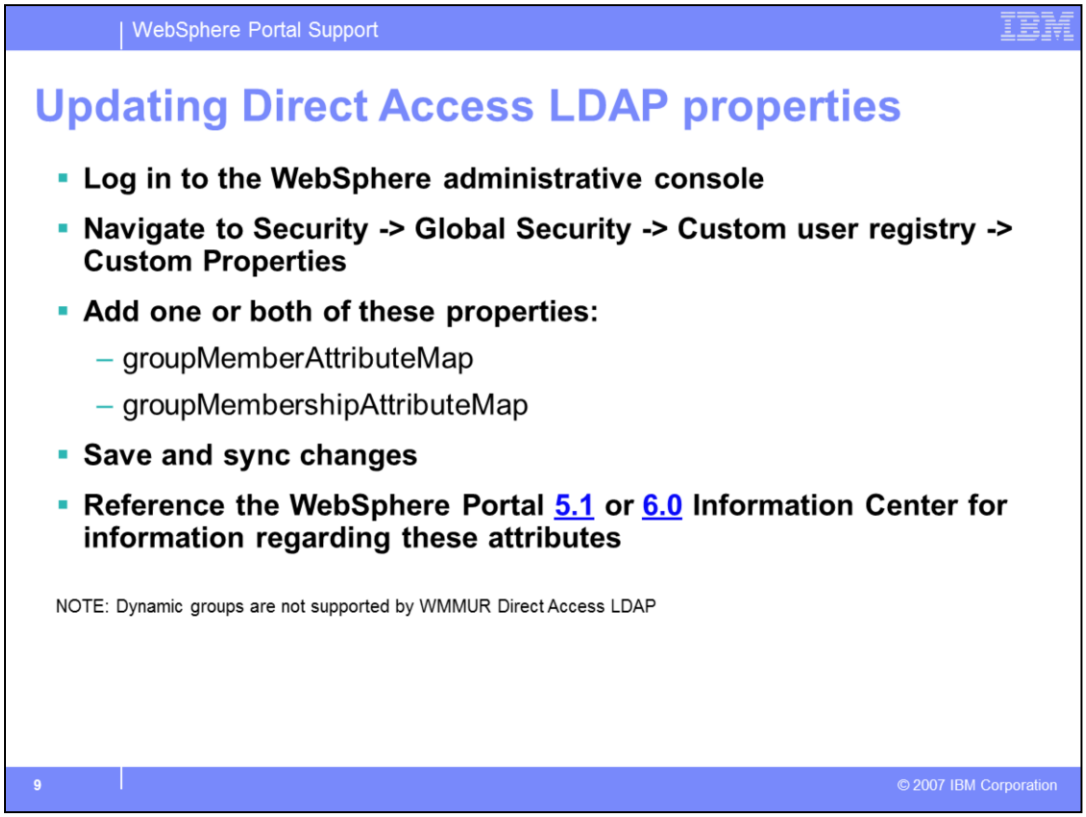
Note that the file registry option does not allow you to use nested groups, so you cannot put an adminGroup within an adminGroup.



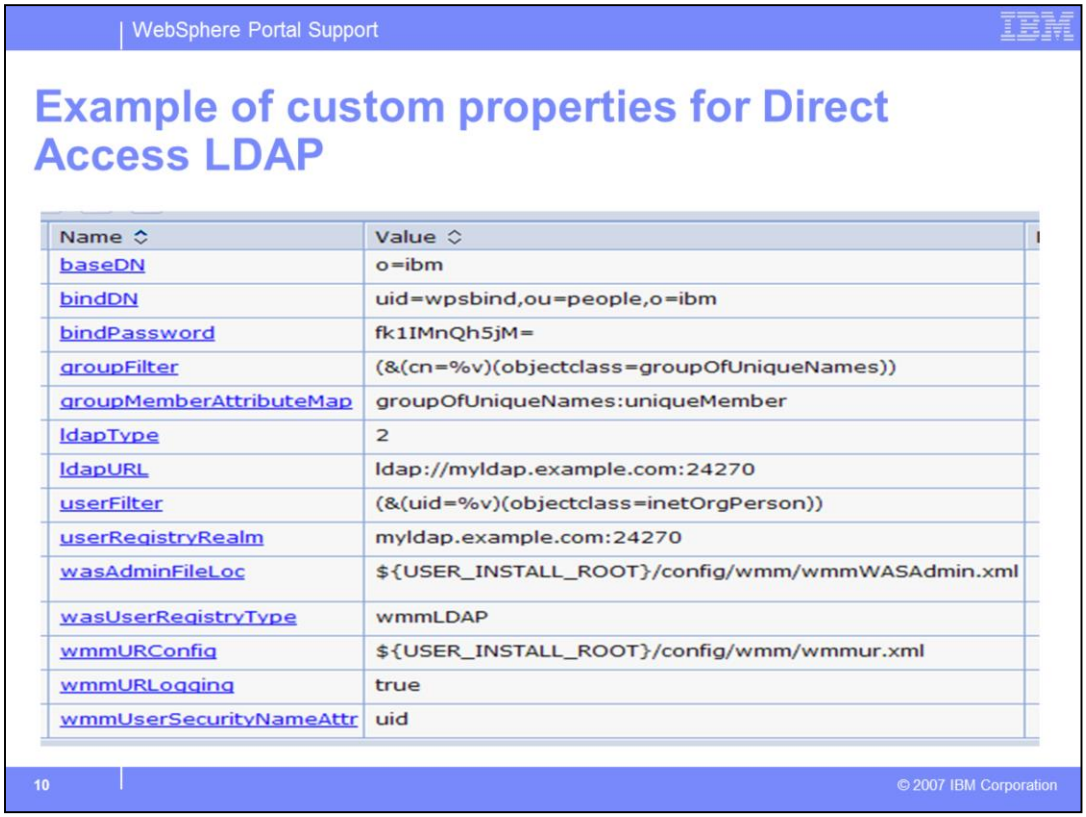
An alternate way of updating the wmmWASAdmin.xml is through the updateWmmWASAdminRegistry tool. You can reference Technotes 1246919 for details on how to use the tool. Or you can type updateWmmWASAdminRegistry at a command prompt to see all of the options. Provided here are examples of the three commands necessary to implement the group membership functionality.



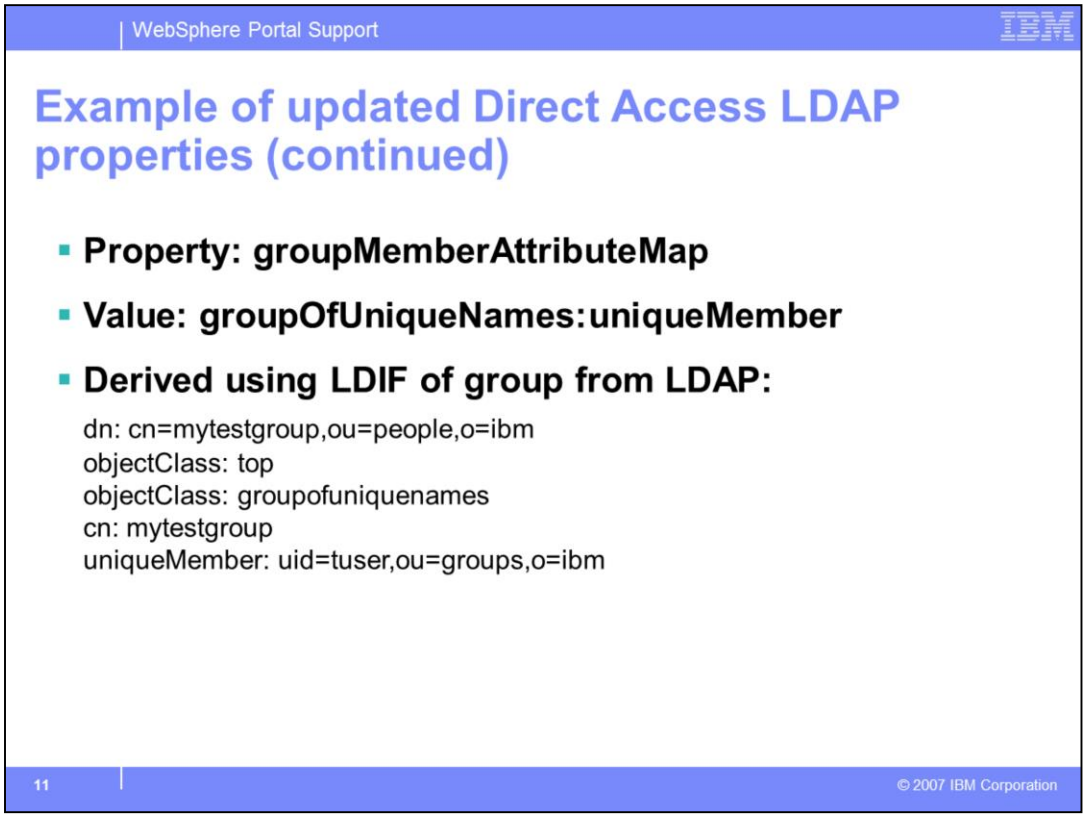
When you update any WebSphere Member Manager file, including the wmmWASAdmin.xml in a cluster, you must use the check-in and check-out method as documented in the Information Center topics linked here. Otherwise, you risk inconsistencies between nodes and possibly having your updates fail to take effect. This is an important and often overlooked point.



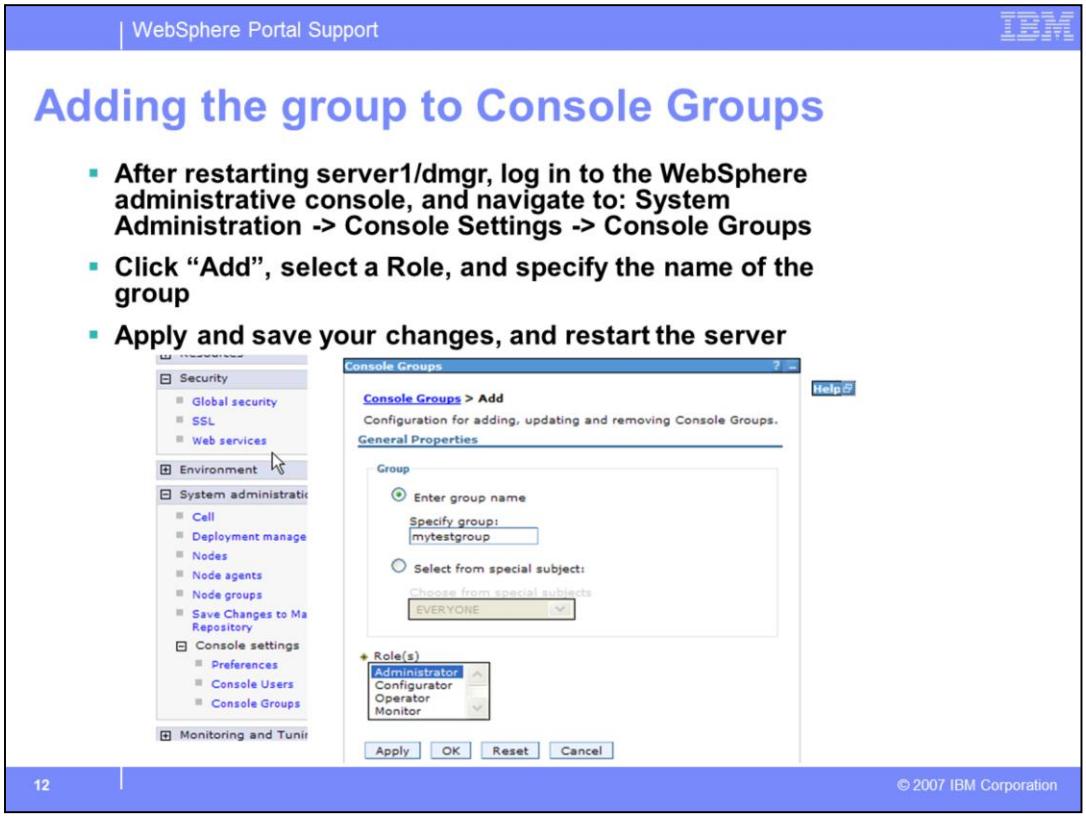
If you are using the Local mode Direct Access LDAP registry, perform the updates using the WebSphere Administrative console. After you log in, navigate to Security -> Global Security -> Custom user registry -> Custom Properties, where you should see several properties which allow you to search the LDAP server. However, to add the ability to determine group membership, you must add the groupMemberAttributeMap property, the groupMembershipAttributeMap property, or both. Refer to the WebSphere Portal Information Center for more details on these attributes and to determine which one (if not both) your LDAP can support. Typically, at least groupMemberAttributeMap will be supported. It should be pointed out that nested groups are supported in this type of Local mode registry; however, it cannot support dynamic groups.



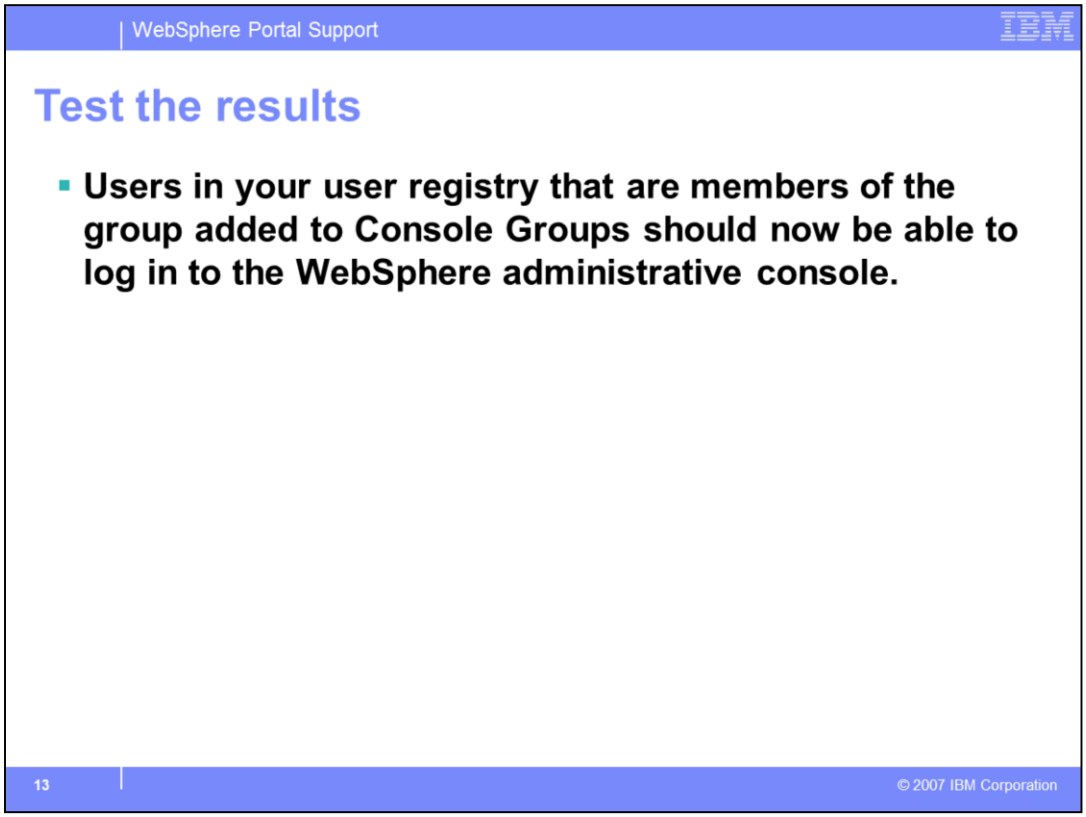
Here you see an image of a test system which implements Local mode Direct Access LDAP. There are 14 parameters defined; however, that can vary depending on the environment including the type of LDAP server. This image shows that only groupMemberAttributeMap is implemented . The LDAP in this scenario is Sun Java Directory Server.



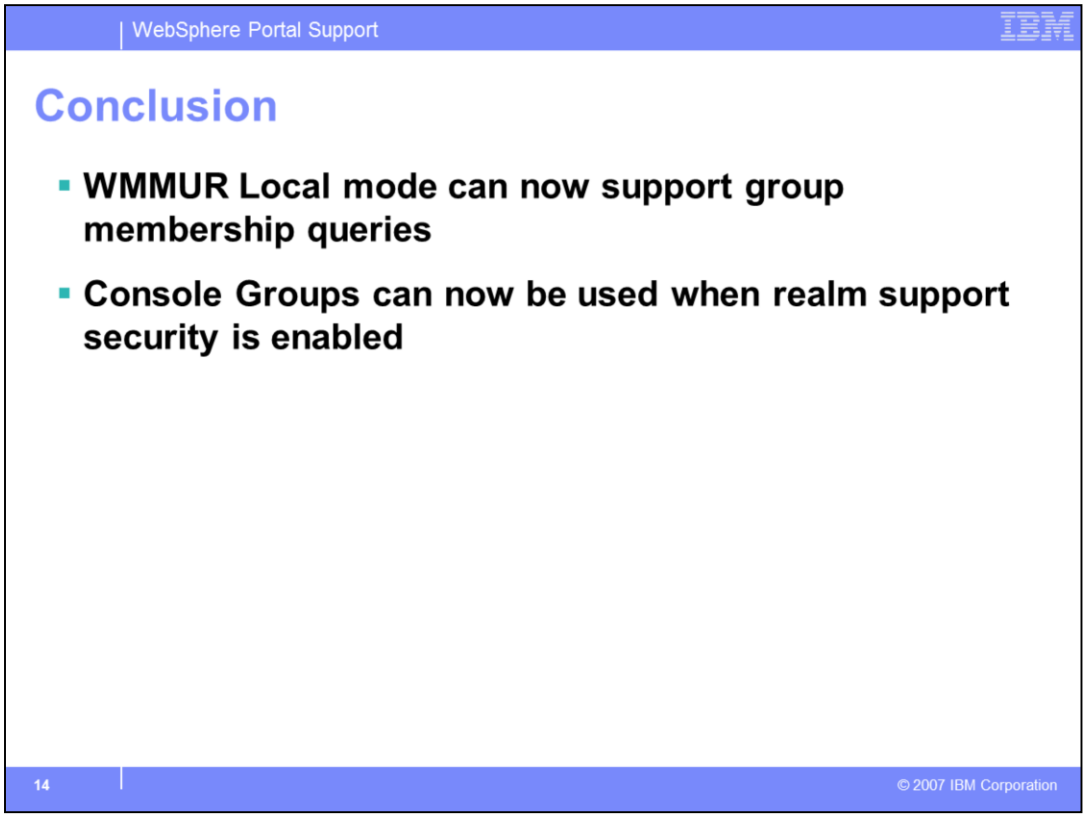
To determine the proper values to use for groupMemberAttributeMap, you can look at an LDIF of the group you want to add to Console Groups. The LDIF shown here indicates that the “groupOfUniqueNames” objectclass and the “uniqueMember” attribute can be used to form the correct value.



After making the changes to either Local mode user registry, you must restart the deployment manager or server1. Then log in to the WebSphere administrative console and navigate to System Administration -> Console Settings -> Console Groups, select the proper role for your group, and specify your group name to add the entry. Save the changes and restart the server once again.



You can test the results by logging in to the WebSphere administrative console as a member of the Console Group that you just defined.



In conclusion, WMMUR Local mode can now be used to support group membership. Meaning that, Console Groups can be used through the WebSphere administrative console even if you have enabled security in WebSphere Portal with realm support.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere

Access, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.