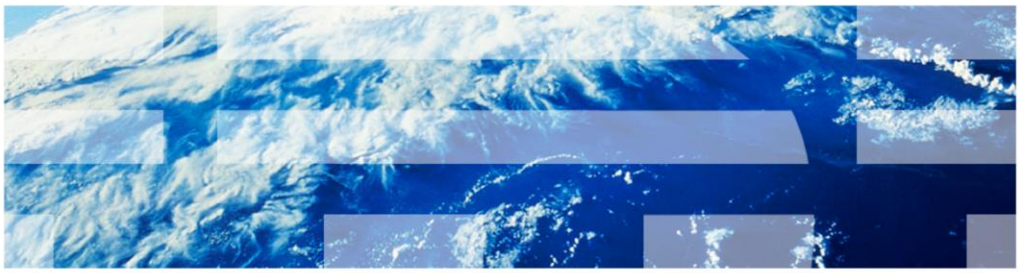
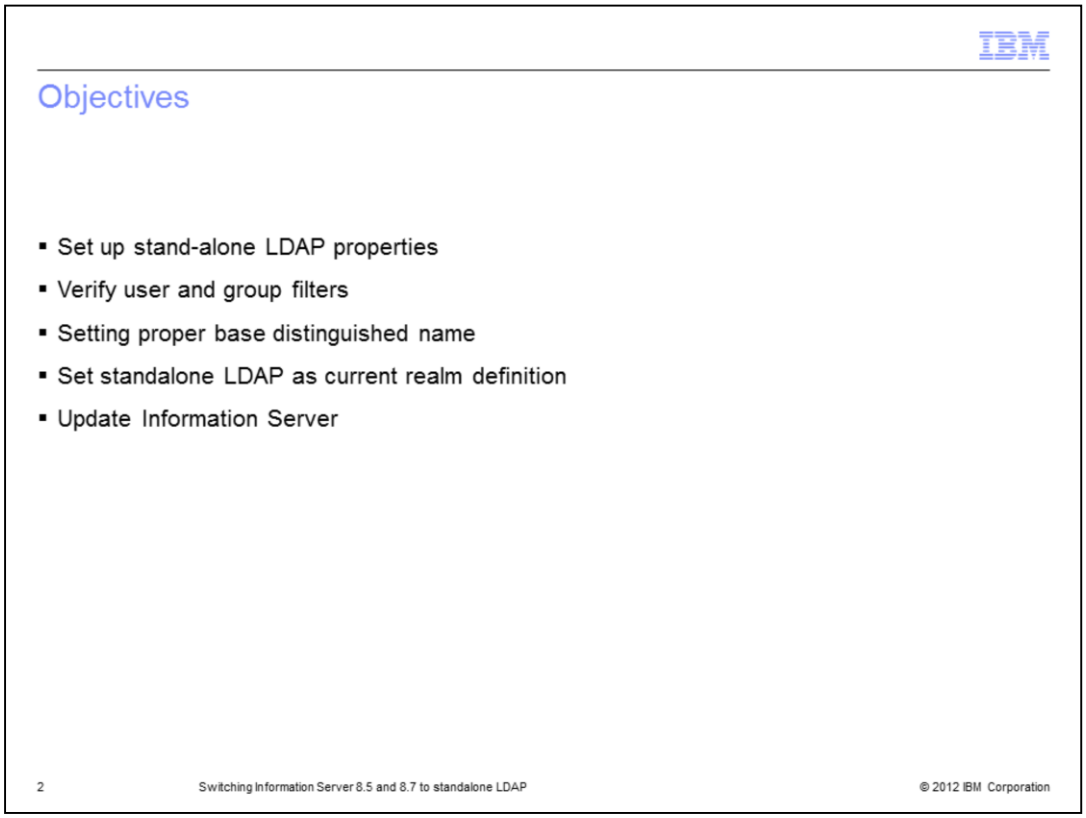
IBM

InfoSphere Information Server

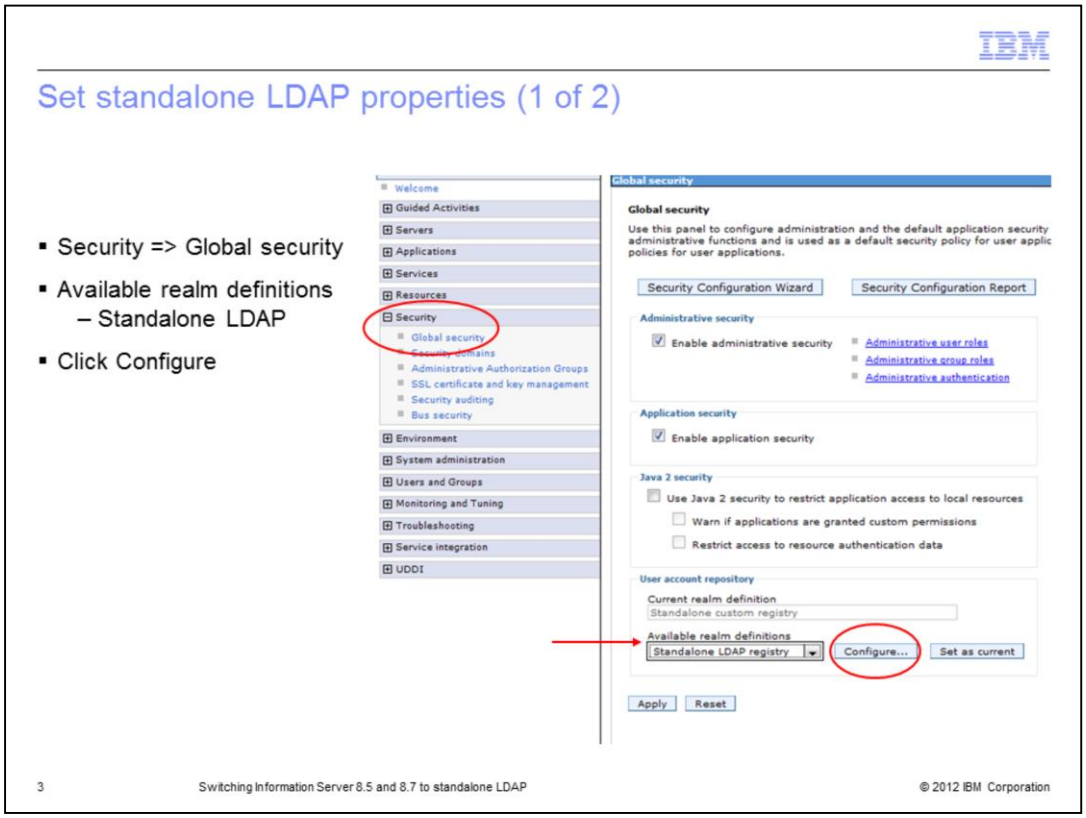
Switching Information Server 8.5 and 8.7 to standalone LDAP



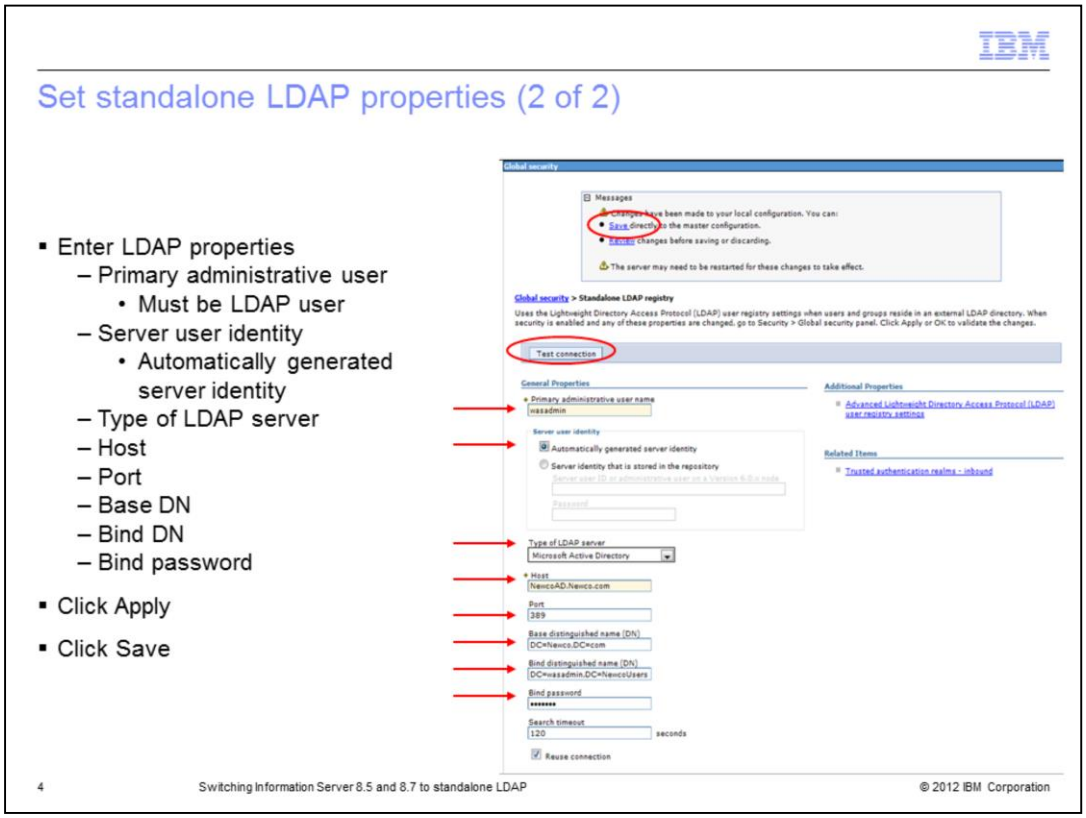
This presentation will discuss how to switch InfoSphere® Information Server 8.5 and 8.7 and WebSphere® 7.0 to use the stand-alone LDAP repository for authentication.



The objectives of this presentation are to show how to set up the LDAP properties for standalone LDAP, how to verify the user and group filters and how to determine the best base distinguished name. This presentation will also show how to set standalone LDAP as your current realm definition and how to update Information Server with the new WebSphere Administrative ID.



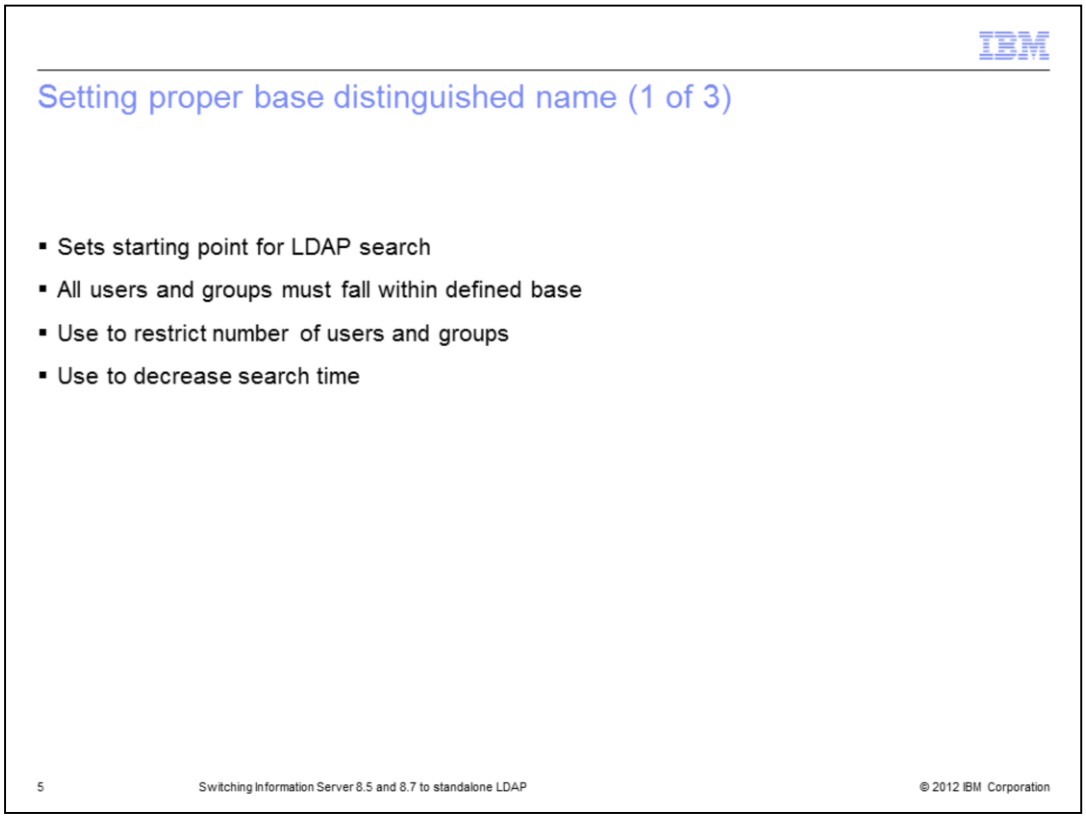
The first step in setting up the standalone LDAP registry is to open the WebSphere Administrative console. On the left side of the screen, click Security and then Global security. Next, click the drop down for the Available realm definitions and choose Standalone LDAP registry. Click Configure.



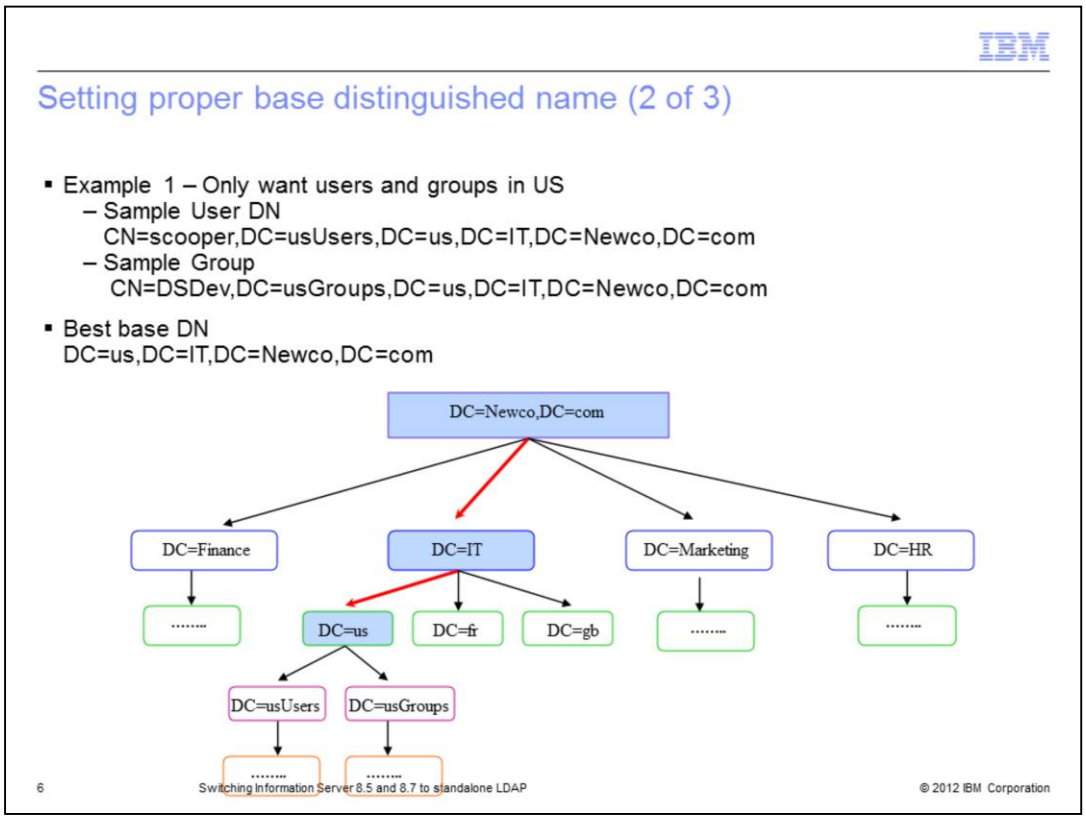
Under the General properties page, enter the name of your primary administrative user. This user must be a valid LDAP user. Next, make sure the Server user identity is set to Automatically generated server identity. Choose the type of LDAP server you are authenticating against. Next, enter the LDAP server name, Port, and Base distinguished name. The base distinguished name defines the starting point for LDAP searches. Making this value more restrictive will limit the number of users and groups returned to Information Server. Be sure that all the users and groups all fall with in the defined base. The next slide will discuss the base DN in more detail.

Next, enter your bind distinguished name and password. This is the distinguished name of the user that is used to bind to the directory service. It does not have to be the same user as the primary administrative user. If your directory service support is an anonymous bind, you can leave these fields blank.

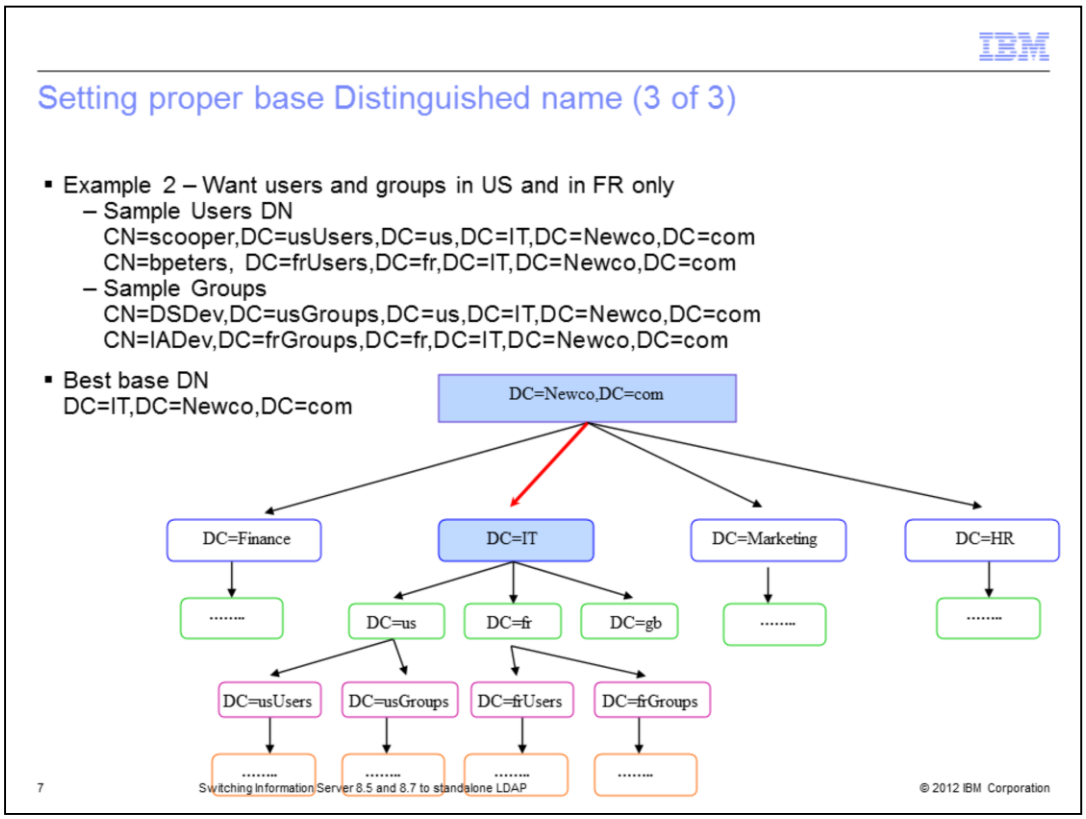
When the information has been entered, click Apply at the bottom of the screen and then click Save in the message box at the top. Click Test Connection to make sure your connection to your LDAP server is working properly.



The base distinguished name sets the starting point for LDAP searches in the directory service. Setting this appropriately for your user and group search can help to limit the number of users and groups returned to Information Server and decrease the search time. The appropriate value for this field depends on the layout of your directory service.



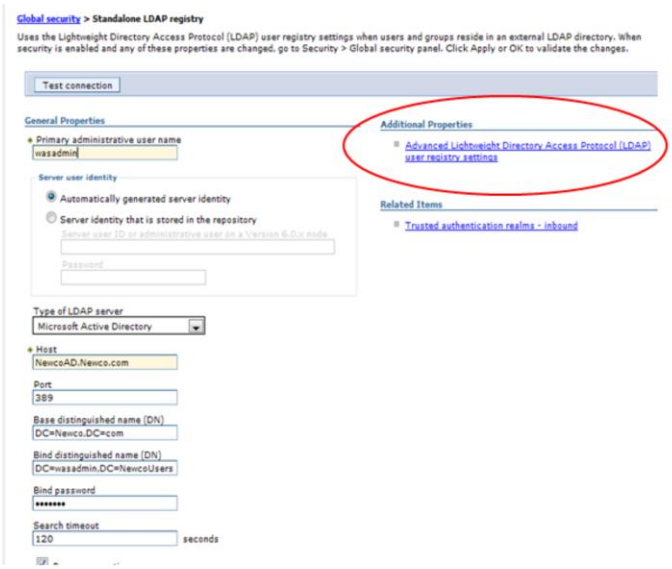
In the example displayed on this slide, the company Newco only wants their US users and groups to appear in Information Server. This slide displays an example distinguished name for user scooper and group DSDev. If Newco uses DC=Newco,DC=com for their base DN, whenever they do an LDAP lookup or attempt to get a list of users and groups, LDAP will have to search all four branches. Searching the four branches, Finance, IT, Marketing, and HR, can be time consuming in a large directory service and will return thousands of unwanted users and groups. Since all of the users and groups are under the DC=us branch, it is much more efficient to make the base DN DC=us,DC=IT,DC=Newco,DC=com. In this case, if an LDAP search, user list, or group list is requested, the search will begin at the DC=us branch making the search much more efficient.



In the example displayed on this slide, the company Newco, only wants both their US and France users. The base DN will have to be less restrictive and use DC=IT,DC=Newco,DC=com so that it will include both the user and groups from the US and France. Since the Great Britain users are also under the IT branch, DC=gb will always be searched as well. Even with this being the case, the search will still be more efficient than searching the entire Newco domain. If you want to use multiple base DNs for searching, you have to set WebSphere up to use federated repositories.

Verify filters (1 of 2)

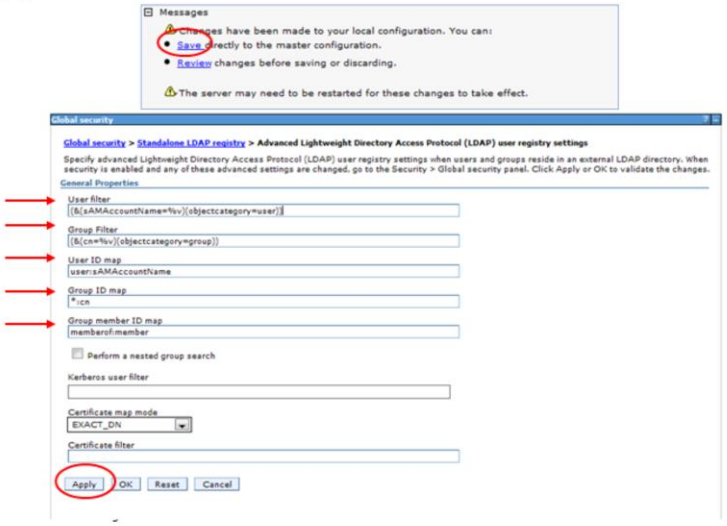
- Verify user and group filters
  - Additional Properties
    - Advanced Lightweight Directory Access Protocol (LDAP) user registry settings



The next step in setting up the standalone repository is to verify that the default user and group filters are correct. While in the General Properties screen for the LDAP repository, click Advanced Lightweight Directory Access Protocol user registry settings under Additional Properties.

Verify filters (1 of 2)

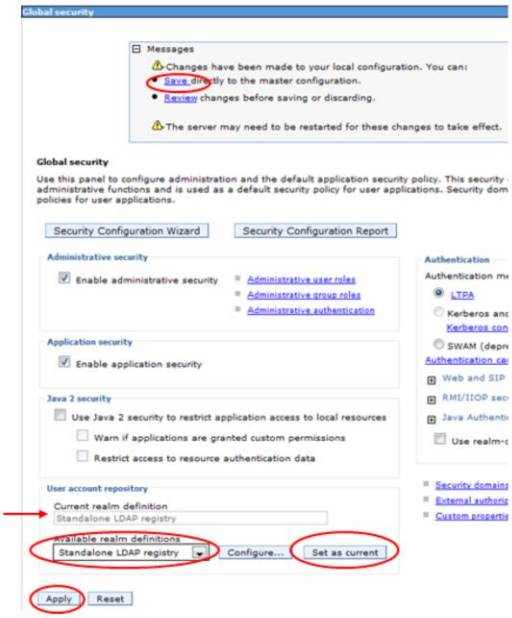
- Verify/update user and group filters
- Click Apply and save



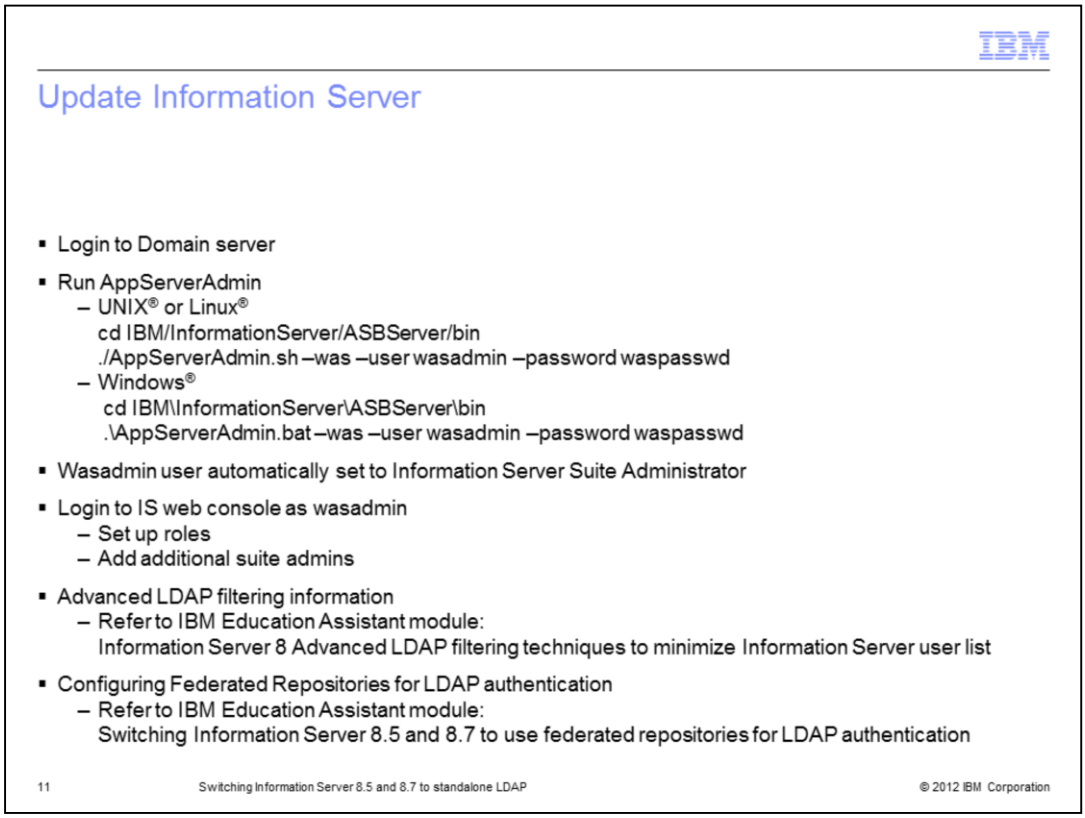
Verify that the filters match what was supplied to you by your LDAP administrator. If the values do not match, make the appropriate changes and click Apply and Save.

Set current realm definition

- Set Available realm definitions
  - Standalone LDAP registry
- Click Set as current
- Click Apply
- Click Save
- Restart WebSphere



The last step in WebSphere is to set the standalone LDAP repository as the current realm definition. Be sure that Standalone LDAP registry is selected under Available realm definitions and click Set as current. The current realm definition should change to Standalone LDAP registry. Next, click Apply. If no error appears in the message box at the top, click Save. If a message appears, you need to review your LDAP properties and filters. You also need to restart WebSphere for the changes to take effect.



On the Information Server side, you need to run the AppServerAdmin command line utility to update Information Server with your new wasadmin user and password. cd into the InformationServer/ASBServer/bin directory and run the AppServerAdmin command as displayed on this slide.

Once that has completed successfully, you are ready to go into the Information Server web console. The first time you login to the Information Server Web console, you need to use the primary administrative user you specified on slide four. This user will automatically be an Information Server suite administrator. Once you open the Information Server Web console, you can then go in and set the user roles and add any additional users as suite admins.

For information on more advanced LDAP filtering techniques, see the IBM Education Assistant module “Information Server 8 Advanced LDAP filtering techniques to minimize Information Server user list”.

For more information on how to configure Information Server and WebSphere to use federated repositories, see the IBM Education Assistant module “Switching Information Server 8.5 and 8.7 to use federated repositories for LDAP authentication”.

Trademarks, disclaimer, and copyright information