LDAP/Active Directory Authentication in BBj

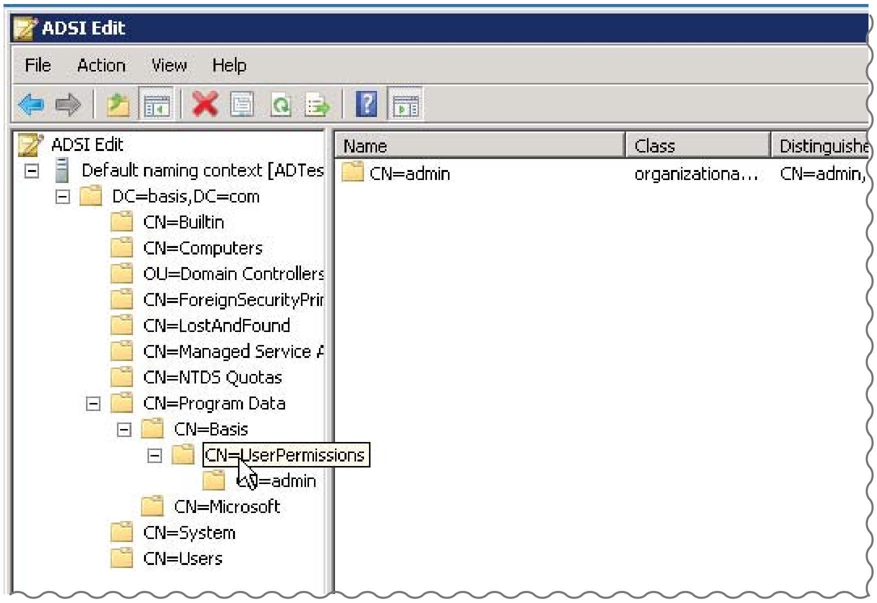
To help developers provide security for their applications and servers, BBj® provides a level of access control requiring a user name and password. While this is built in and very easy to use, it may make the job of system administrators easier if they can use existing user authentication mechanisms already available on their network. A simple BBj configuration change allows the use of other authentication mechanisms such as Microsoft's Active Directory.

Using Active Directory, administrators do not need to maintain multiple lists of user accounts, but rather, manage all user accounts from a single authentication source. This article takes a look at the two parts in the configuration that allow BBj to use Active Directory for authentication: the Active Directory server and the BBj Services installation.

What to do on the Active Directory Server

As a matter of convention, this article describes a convenient method for setting up the Active Directory server to interact with BBj properly. Follow these steps to ensure proper setup:

1. Using the ADSI Edit tool on the Active Directory server, create a directory structure as shown in **Figure 1**. The "Basis" and "UserPermissions" items should be of class type "container".
2. Next, add an object by right-clicking and then selecting "New Object" for the primary user account that will be used to administer BBj Services. Our example uses "admin" but you may choose "administrator", "jdoe", etc.; the object type should be "person".
3. Right click on the new user object and select "properties". Double-click the "description" attribute and enter "ALLOW_ALL" in the text field type, then click [Add] and [OK]. This grants all BBj permissions to this user for managing other users using the Enterprise Manager.
4. Right click on the BASIS object that we created earlier and select "Properties"and set the object's security to read/write for everyone. Repeat for the UserPermissions object. This allows BBj to update user information automatically rather than doing it manually for each user.



Name	Class	Distinguishe
CN=admin	organizationa...	CN=admin,

Figure 1. Create a sub directory structure with class type "container"

BBj Configuration

The BBj configuration involves two parts; the server information, and query information. The server information tells BBj how to connect to the Active Directory server to look up users and their permissions. The second part tells BBj how to find the information it needs once it is connected to the server.

To configure the Active Directory information, click the "Users/Authentication" item in the Enterprise Manager navigator and then select the "Authentication Settings" tab shown in **Figure 2.**

Server Information

To configure the LDAP section of "Use LDAP/Active Directory Authentication,"

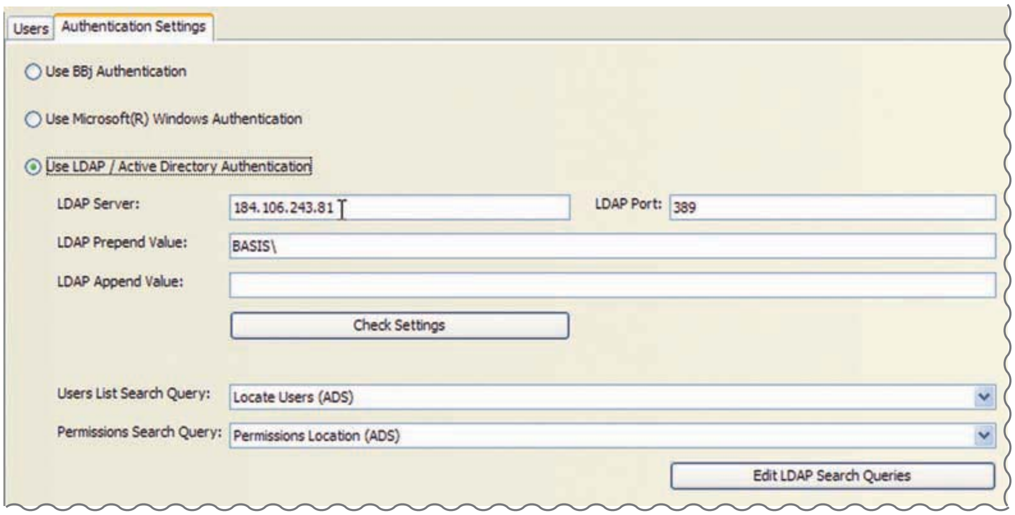
1. **LDAP Server:** Enter the IP address or host name for the Active Directory server.
2. **LDAP Port:** Enter the port number. The default port is 389 unless this was intentionally changed by the system administrator.
3. **LDAP Prepend Value:** Enter the domain of your Active Directory server. This is the string prepended to your user names when you log in to the Active Directory box. Our example uses `basis\`. This value prepends to all of the user names when sent through for authentication.
4. **LDAP Append Value:** Leave the field empty and click [Check Settings] to verify that all of the information is correct. You can authenticate using the user for whom you create an entry under UserPermissions in the ADSI Edit tool. >>

By Jeff Ash
Software Engineer

User List and Permissions Search Queries

The Query section of “Use LDAP/ Active Directory Authentication” can be a little trickier. You will provide two valid LDAP syntax search queries, one for looking up users, and the other for looking up user permissions.

1. Click [Edit LDAP Search Queries] button.
2. Click [Add].
3. Enter the information shown in **Figure 3** and click [Test] button to see the results of the query.
4. When satisfied with the results, click [OK] to save the query.
5. Click [Add] again.
6. Enter the information shown in **Figure 4** and click [Test] to check the results
7. Finally, click “OK” to save this query.



○ Use BBj Authentication

○ Use Microsoft(R) Windows Authentication

● Use LDAP / Active Directory Authentication

LDAP Server: 184.106.243.81

LDAP Port: 389

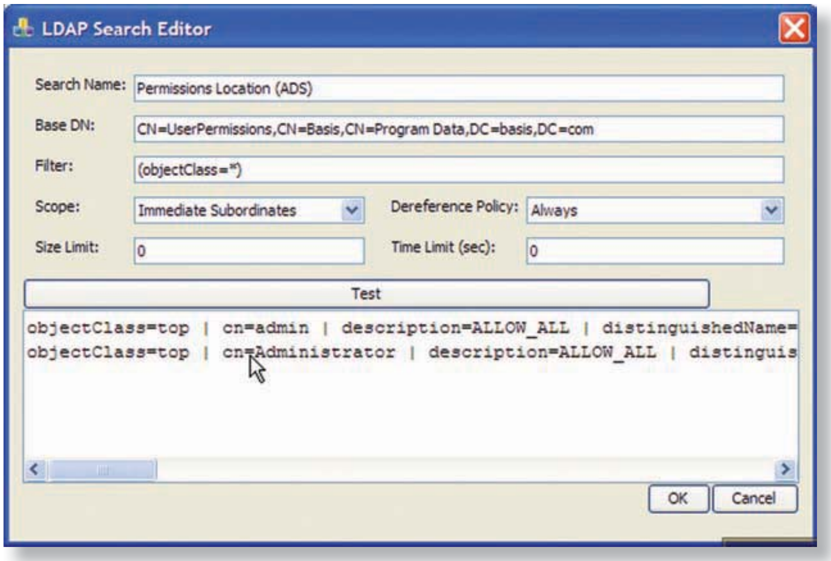
LDAP Prepend Value: BASIS\

LDAP Append Value:

Users List Search Query: Locate Users (ADS)

Permissions Search Query: Permissions Location (ADS)

Figure 2. Active Directory Authentication configuration in the Enterprise Manager



Search Name: Permissions Location (ADS)

Base DN: CN=UserPermissions,CN=Basis,CN=Program Data,DC=basis,DC=com

Filter: (objectClass=*)

Scope: Immediate Subordinates

Dereference Policy: Always

Size Limit: 0

Time Limit (sec): 0

```
objectClass=top | cn=admin | description=ALLOW_ALL | distinguishedName=
objectClass=top | cn=Administrator | description=ALLOW_ALL | distinguis
```

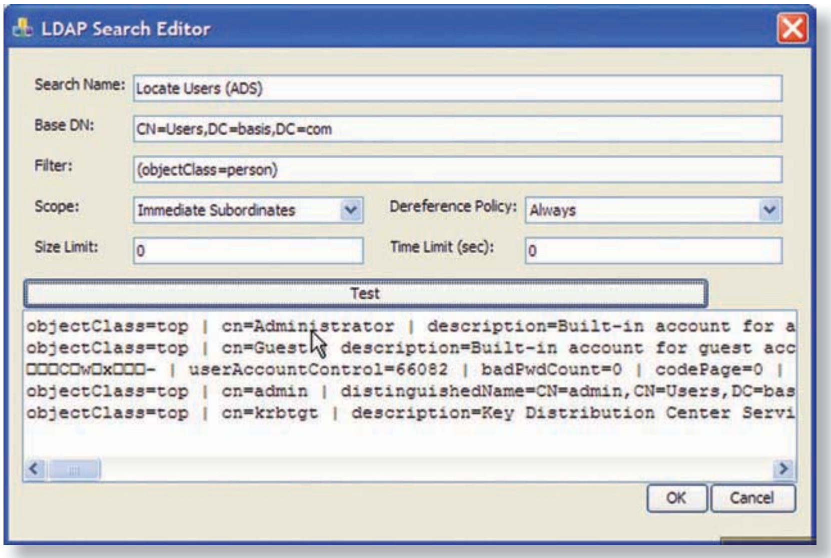
Figure 3. Sample text to enter in LDAP Search Queries

Now that the queries are created, select the “Locate Users” query for the “User List Search Query” dropdown, and select the “Permissions Location” query for the “Permissions Search Query” dropdown.

Configuration is now complete and ready to save. Click the save button at the bottom of the panel to save these changes. A login dialog will appear which will force a relogin to the system using the user account we setup in the Active Directory server UserPermissions section earlier.

If you make any mistakes during the configuration process, it may be necessary to manually change the BBj.properties file in order to get logged back into the Enterprise Manager. If this is necessary, open the BBj.properties file in your favorite text editor and make the following property change which will set everything back to using BBj authentication, but will not remove any of the Active Directory configuration setting put in place (make sure to restart BBj Services after making the change to the property). You can then go fix the issue and try again:

```
com.basis.auth.type=multiserver
```



Search Name: Locate Users (ADS)

Base DN: CN=Users,DC=basis,DC=com

Filter: (objectClass=person)

Scope: Immediate Subordinates

Dereference Policy: Always

Size Limit: 0

Time Limit (sec): 0

```
objectClass=top | cn=Administrator | description=Built-in account for a
objectClass=top | cn=Guest | description=Built-in account for guest acc
□□□C□w□x□□□- | userAccountControl=66082 | badPwdCount=0 | codePage=0 |
objectClass=top | cn=admin | distinguishedName=CN=admin,CN=Users,DC=bas
objectClass=top | cn=krbtgt | description=Key Distribution Center Servi
```

Figure 4. Data to test the query

Conclusion

Using Active Directory authentication can make the job of the system administrator much easier by eliminating the need to maintain multiple sources of users and passwords. If your organization does not use Active Directory, then it would probably not be worth the effort to only use it for BBj authentication. However, if Active Directory is already in use, it makes sense to take advantage of this feature of the BBj authentication system to simplify the initial installation and reduce the ongoing maintenance of replicating of the same or similar authentication information throughout the organization. ■