Scan Business Systems, Inc.

LDAP Integration Document

Café web portal is now able to provide single sign-on capability with Microsoft Active Directory. Users can now login in to the Cafeweb portal using their active directory credentials and gain access to their information. The following details the system requirements to set up this authentication process. Please understand that it is our recommended best practice to utilize the SYUSER creation program to generate usernames and passwords for new accounts and use the output file to create the Active Directory accounts, thus maintaining username integrity that originates from the scanfilev5 database SYUSER table. Any user who is logging in to the Cafeweb portal will still need an account in the SYUSER table, however, a password would no longer be required in the SYUSER table thus allowing users to keep one password in Active directory and the usernames would be synchronized and theoretically would not change between systems. It should also be noted that the users logging in do not have to have an Active directory account to log in as long as there is a username and password for them and their account is not inactive in SYUSER.

The following WebApp Config items need to be configured in the System Administration Module:

LDAP_BASE_1 - Example: ou=Student Logins,dc=students,dc=public,dc=myschooldomain,dc=edu

The LDAP base should be read from right to left as a search string: *'in the edu domain, search for the myschooldomain. Within the myschooldomain, search for the public domain. In the public domain, search for the students domain. Within the students domain, search the organizational unit Student Logins for the username to be authenticated.'* It is valid to list more than one organizational unit (ou) depending on how your LDAP solution is configured. *Note: order matters when constructing the LDAP base.*

Once a username is located in the organizational unit, the related properties, such as the password, are collected and the authentication procedure is ready to proceed to validate the user's credentials.

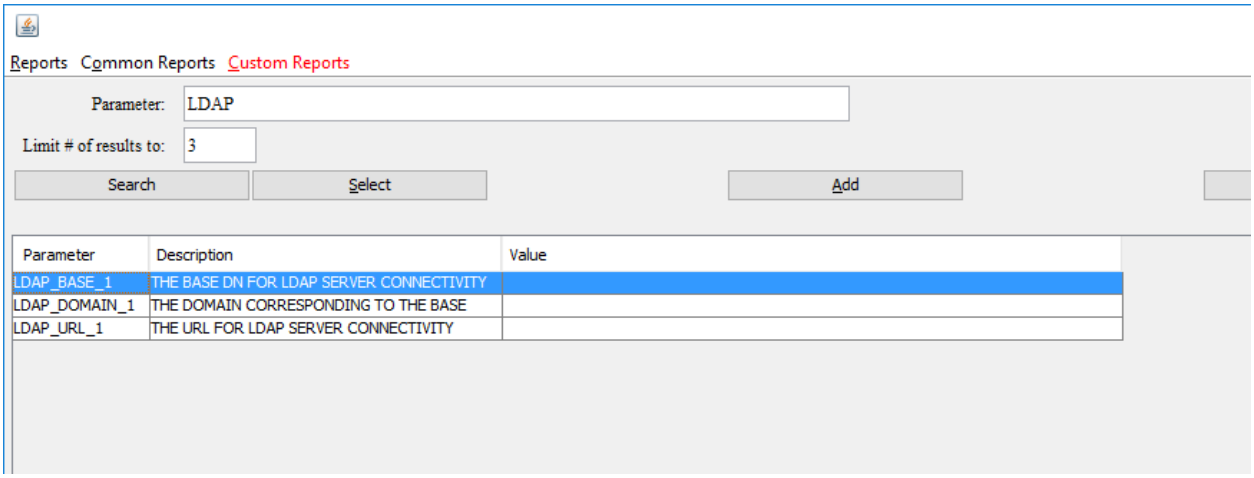
LDAP_DOMAIN_1 - Example: students.public.myschooldomain.edu

Note that the LDAP domain matches the domain components listed in the base above (excepting the organizational unit or units).

LDAP_URL_1 – Example: ldap://10.0.0.1

The URL may be identified via Internet protocol address or domain name. Note the trailing numbers in each identifier; if your institution has deployed more than one LDAP service, you may add further criteria. For example, for a second LDAP server, create parameters LDAP_BASE_2, LDAP_DOMAIN_2, and LDAP_URL_2.

Following is a screen shot of the configuration items:



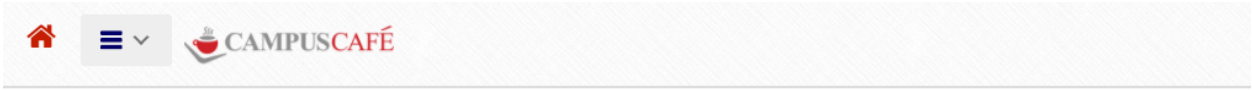
In addition to these configuration elements for the LDAP, you must also set two MSPARMS.

WEBUSRNAME-1-1 Value=MIXED

WEBPASSWORD-1-6 Value=MIXED

Setting both of these parameters to mixed effectively removes any conversion of the username or password to UPPER or LOWER case, essentially the signing in to the portal becomes case sensitive and therefore, more secure. It would be our recommended best practice to make sure that both the samAccountName and the SYUSER.USERNAME values always be stored in lower case so users logging into the system do not need to worry about typing anything in uppercase.

Screenshots follow:

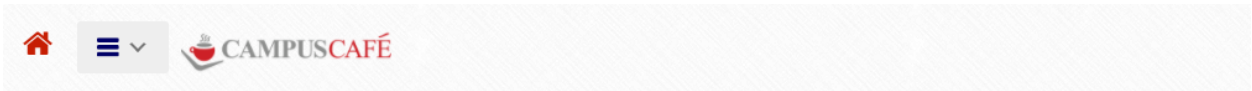


MSParm Detail Program Id: WEBUSRNAME Seq Num: 1

Information that is red is required

Context: GLOBAL - MSPARM CONTEXT GLOBAL

Parameter Value 1:	MIXED
Description 1:	CONVERT TO CASE (LOWER, UPPER, MIXED)
Default Value 1:	upper
Parameter Value 2:	
Description 2:	MAKE USERNAME FIELD INTO A PASSWORD TYPE (MASKED)
Default Value 2:	N
Parameter Value 3:	
Description 3:	
Default Value 3:	
Parameter Value 4:	
Description 4:	
Default Value 4:	



MSParm Detail Program Id: WEBPASSWRD Seq Num: 1

Information that is red is required

Context: GLOBAL - MSPARM CONTEXT GLOBAL

Parameter Value 1:	5
Description 1:	MIN LENGTH
Default Value 1:	5
Parameter Value 2:	15
Description 2:	MAX LENGTH
Default Value 2:	10
Parameter Value 3:	4
Description 3:	MIN NUMBER OF ALPHA CHARS
Default Value 3:	4
Parameter Value 4:	1
Description 4:	MIN NUMBER OF NUMERIC CHARS
Default Value 4:	1
Parameter Value 5:	0
Description 5:	MIN NUMBER OF NON ALPHA-NUMERIC CHARS
Default Value 5:	0
Parameter Value 6:	mixed
Description 6:	CONVERT TO CASE (LOWER,UPPER,MIXED)
Default Value 6:	upper
Parameter Value 7:	
Description 7:	
Default Value 7:	

There should also be an understanding by the IT administrator of how the underlying process works. The following details the process that is undertaken when a user signs in:

1. The user puts in a username and password.
2. Upon submission, the entries are trimmed and checked for being blank, if blank the user is prompted to reenter, otherwise,
3. LDAP connectivity parameters are looked up in SYWCFG and if not blank, LDAP authentication is attempted on NON-CONVERTED username and password. If LDAP is successful in authenticating the user, a flag is set in the code to indicate this.
4. The conversion rules are applied to both the username and password (as before).
5. The user record is looked up in the database by the username. If not found an error is reported to the user.
6. The disabled account check runs and if disabled, an error is reported to the user.
7. If the flag indicating LDAP success is true, the password is not checked in SYUSER. Otherwise (if LDAP failed to authenticate for any reason), the password is checked in SYUSER and if matching, the user gets logged in, otherwise, the user gets an error.