LDAP Setup Notes for WTI Products

The samples in this document are based on most common Windows Server LDAP settings.
Shown below, is a common setup for a Windows Server LDAP configuration:

```
LDAP:
1.  Enable:                      Off
2.  Primary Host:                192.168.100.246
3.  Secondary Host:              (undefined)
4.  LDAP Port:                   389
5.  TLS/SSL:                     On
    50. Check Certificate:       Off
    51. Import Certificate:
6.  Bind Type:                   None
7.  Search Bind DN:              cn=wti1600,ou=Network Admin,ou=WTI_MIS,dc=wti,dc=com
8.  Search Bind Password:        (defined)
9.  User Search Base DN:         ou=WTI_TECH_SUPPORT,dc=wti,dc=com
10. User Search Filter:          sAMAccountName=%s
11. Group Membership Attribute:  memberOf
12. Group Membership Value Type: Name
13. Fallback:                    On
14. LDAP Group Setup
15. LDAP Kerberos Setup
16. Debug:                       Off
```

A few notes on setup:

When using TLS/SSL and Check Certificate is ON, the Primary Host (and secondary if defined) needs to be the fully qualified name defined in the certificate and at least one DNS server needs to be defined to do the name lookup.

If using Kerberos with LDAP, the time on the unit needs to match almost exact to the Kerberos server, so the NTP should be turned on and active.

Fallback should be turned On during setup, just in case.

The debug on the above screen is separate from the “/z9” type of debug. The debug on the LDAP screen is to fill the Linux type of logs in the WTI unit (i.e. /bash type /var/log/auth.log). The “/z9” debug is to direct the LDAP debugging info out Serial Port 1. Remember when logging in with LDAP and the /z9 option is on, there will be a long pause on the login session because of all the LDAP debug stuff being printed through the serial port. There must be a device attached to the serial port if the /z9 is enabled and an LDAP sign in is attempted.

LDAP configuration options are discussed on the next page.

Options:

1. **Enable:** Turn LDAP on/off
2. **Primary Host:** IP or fully qualified names of the LDAP server
3. **Secondary Host:** IP or fully qualified names of the LDAP server
4. **LDAP Port:** The number of the port that the LDAP server is listening on.
5. **TLS/SSL:** Turn LDAP encryption on.
    50. **Check Certificate:** Make sure the FCN entered in 2 or 3 is the name in the certificate that was uploaded to prevent spoofing.
    51. **Import Certificate:** Where the public PEM based (text) certificate gets uploads that would be generated from the server.
6. **Bind Type:** Essentially 1 (None) and 2 (Simple) are the same. Option 3 (Kerberos) turns on the Kerberos protocol.
7. **Search Bind DN:** This is the path to the user you are using to search the LDAP Tree for User lookup and Group lookup. This username must have sufficient rights to search the LDAP tree.
8. **Search Bind Password:** Password for the Search Bind DN user in item number 7
9. **User Search Base DN:** This is the starting point of our User and Group Search Activity. For debugging you could put this at the top of the tree, although this is time consuming on a full search and the rights of the Search Bind DN must be sufficient to do so.
10. **User Search Filter:** This is who the Username is matched to find the user and to find the user's Groups he is associated with.
11. **Group Membership Attribute:** This is the piece of text we use in a search to see where the group names are located. Usually in the LDAP tree they will be stored as [memberOf: CN=WTI_Users,OU=WTI_AAA_Groups,DC=nemc,DC=wti,DC=com] , as we go down the LDAP tree we see the attribute memberOf and we match against the Group Membership Attribute, then we compare against this string any group names that are in the LDAP Group Setup section
12. **Group Membership Value Type:** This item is compared against the group names. If you choose DN it will add a = prefix and a , suffix to the search. For example, if the group name is WTI_Users the real search criteria will be =WTI_Users, looking for a match. If the Name is chosen, the entire group for just that search term will be matched, so if you have WTI, any group name that has WTI will be matched.
13. **Fallback:** If On, will search on the WTI box for users if the LDAP login fails.

Note: *The /z9 command and the debug option under the LDAP options are two different things. The /z9 debug LDAP option is for internal WTI debug information coming mostly from the main WTI server program, detailing the group matching mechanism. The debug option in the LDAP section (option 16) enables Linux LDAP debug messages to be sent to the /var/log/auth.log which mostly has to do with technical LDAP information for initial login and startup.*