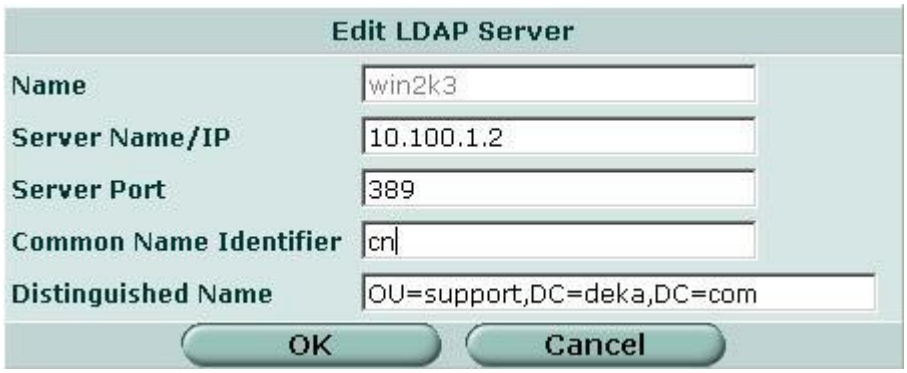
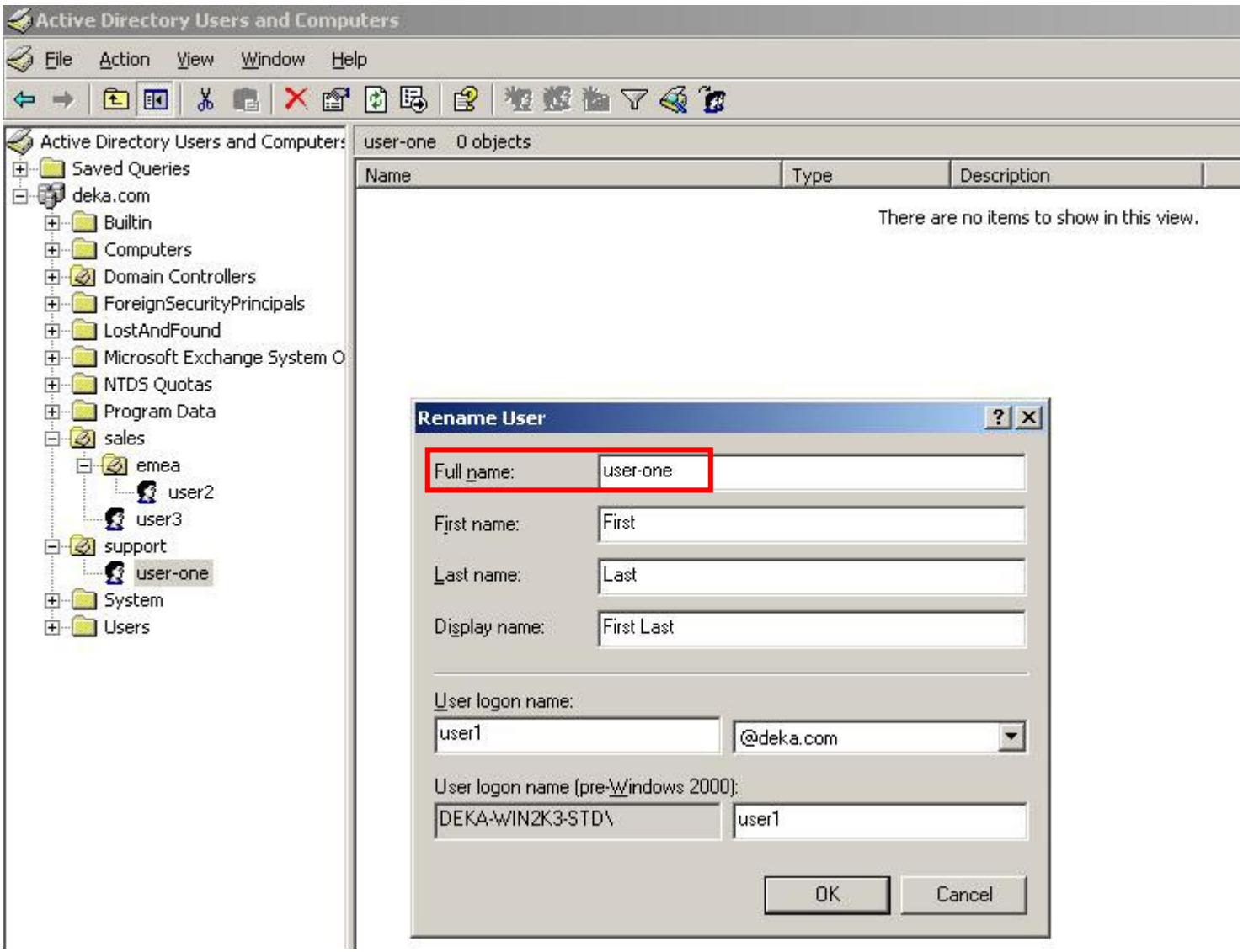
Fortigate LDAP Server configuration examples, for use with Microsoft Active Directory

The examples below illustrate various ways to configure the Fortigate's LDAP Server settings, and how they relate to Microsoft's Active Directory (Windows Server 2000 or 2003) implementation. The Fortigate's LDAP Server configuration can be used to authenticate users via HTTP, FTP or Telnet prior to accessing a resource or can be used with VPN authentication.

If the FortiGate's "Common Name Identifier" is left to default of "cn", then the (Windows Server) user's 'Full Name' must be used to authenticate. The FortiGate's "Distinguished Name" field must also point to the correct level within Active Directory. This restricts authentication of users within an Active Directory structure, based on their position within AD.





A Windows Server 2003 “dsquery” command example output, which can be used to determine the correct ‘Distinguished Name’ setting to use on a Fortigate for any particular user:

```
C:\ >dsquery user
"CN=Administrator,CN=Users,DC=deka,DC=com"
"CN=Guest,CN=Users,DC=deka,DC=com"
"CN=user-one,OU=support,DC=deka,DC=com"
"CN=user2,OU=emea,OU=sales,DC=deka,DC=com"
"CN=user3,OU=sales,DC=deka,DC=com"
```

Example shown below is with the Fortigate’s HTTP web authentication feature:

If the Fortigate’s “Common Name Identifier” and “Distinguished Name” fields are left blank, then the (Windows Server) ‘UPN’ (Universal Principal Name) OR ‘Display Name’ information can be used to authenticate. This method allows all users defined in an Active Directory to be authenticated, regardless of their position within the AD structure.

Example 1:

Example 2:

The following Fortigate debug command ‘`diag deb appl authd 99`’ can be activated on the Fortigate to assist in troubleshooting. Examples are provided below:

```
Fortigate-100 # diag deb appl authd 99

Fortigate-100 # diag deb en

fam_authenticate(): 3 user3 pass3
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=cn=user3,OU=sales,DC=deka,DC=com pw=pass3
Bind succ
Authentication of user user3 on 10.100.1.2 was successful!

Fortigate-100 # message_loop:258 misc=0, domain_info=4, grp_info=0 cerb_info=0, vf=0
fam_authenticate(): 3 user3 pass3
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=user3 pw=pass3
Bind succ
Authentication of user user3 on 10.100.1.2 was successful!

Fortigate-100 # fam_authenticate(): 3 user1@deka.com pass1
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=user1@deka.com pw=pass1
Bind succ
Authentication of user user1@deka.com on 10.100.1.2 was successful!

message_loop:258 misc=0, domain_info=4, grp_info=0 cerb_info=0, vf=0
fam_authenticate(): 3 user1 pass1
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=user1 pw=pass1
User:user1 Radius or LDAP authentication failed!

Fortigate-100 # fam_authenticate(): 3 First Last pass1
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=First Last pw=pass1
Bind succ
Authentication of user First Last on 10.100.1.2 was successful!

Fortigate-100 login: message_loop:258 misc=0, domain_info=4, grp_info=0 cerb_info=0, vf=0
fam_authenticate(): 3 user-one pass1
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=user-one pw=pass1
User:user-one Radius or LDAP authentication failed!

Fortigate-100 login: fam_authenticate(): 3 user-one pass1
host=10.100.1.2 port=389
ldap_simple_bind_s(): dn=cn=user-one,OU=support,DC=deka,DC=com pw=pass1
Bind succ
Authentication of user user-one on 10.100.1.2 was successful!
```

See also:
http://kc.forticare.com/default.asp?id=432&Lang=1
http://kc.forticare.com/default.asp?id=592&Lang=1