KB 140177

How to configure LDAP Backend authentication with multiple subdomains in IDENTIKEY Authentication Server.

Creation date: 12/04/2017 Last Review: 12/05/2017 Revision number: 2

Document type: How To **Security status: EXTERNAL**

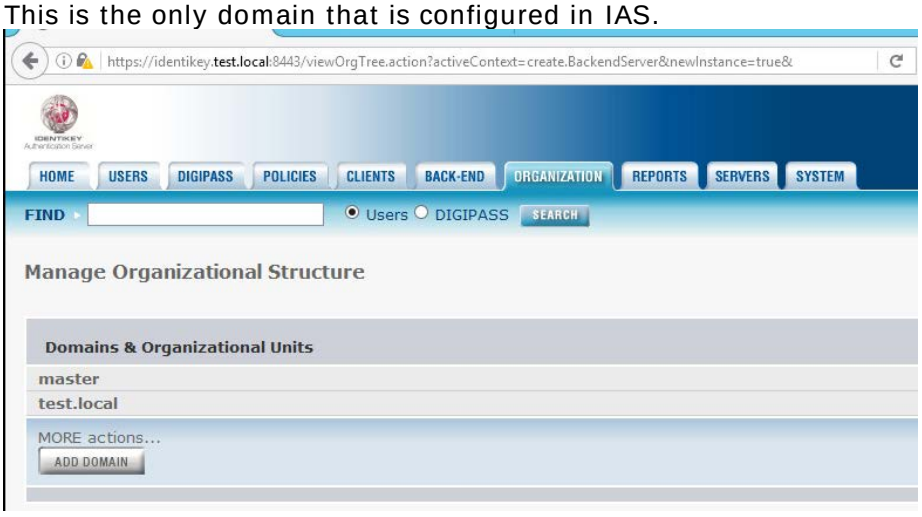
Summary

When you have more than 2 sub domains in Active Directory(AD) but only define the top level domain (for backend authentication) in IDENTIKEY Authentication Server(IAS), you get the error message "user not found" for the authentication.

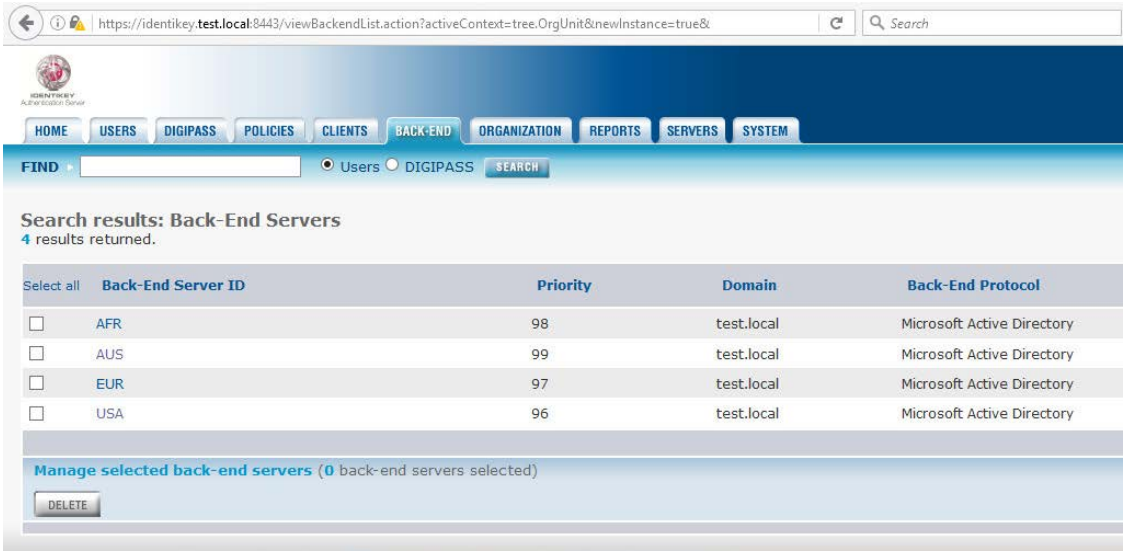
Detail

In the example of this KB article we will use the following AD domain configuration:

- Top level domain in AD: test.local.
  This is the only domain that is configured in IAS.



- Subdomains in AD: eur.test.local, afr.test.local, aus.test.local, usa.test.local. The backend authentication is configured in IAS for every subdomain.



When we want to do an authentication for users in the 2 subdomains with the highest priority. The authentication will succeed.

But when we want to do an authentication for users in the 2 subdomains with the lowest priority. The authentication will fail.
When you check the IAS FULL tracing you can see that the authentication process stops after TRYING 2 backend authentication records;

```
[2016/11/10|14:12:42.325479UTC][S0/P584/T01284][INFO
][LdapADBackEndAuthenticator::authenticate] > Attempting search on and bind to LDAP
server(s)
[2016/11/10|14:12:42.325479UTC][S0/P584/T01284][DEBUG][BackEndStatus::isServerAvailable] >
Server <192.168.20.2:389> is available (no failures yet)
[2016/11/10|14:12:42.325479UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::operator ()] > Attempting LDAP bind before LDAP
search...
[2016/11/10|14:12:42.325479UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnBind::bind] > Realm:
[2016/11/10|14:12:42.325479UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnBind::bind] > Username: ldapAUS
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnBind::bind] > LDAP bind result: Success (0)
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::operator ()] > Attempting LDAP search...
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::search] > Base distinguished name:
CN=Users,DC=EUR,DC=test,DC=local
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::search] > Filter:
(&(objectClass=user)(sAMAccountName=jimmyaus))
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::search] > LDAP search result: Success (0)
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapADBackEndAuthenticator::authenticate] > Search for user found none on LDAP server
'192.168.20.2'
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][DEBUG][BackEndStatus::isServerAvailable] >
Server <192.168.20.4:389> is available (no failures yet)
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::operator ()] > Attempting LDAP bind before LDAP
search...
```

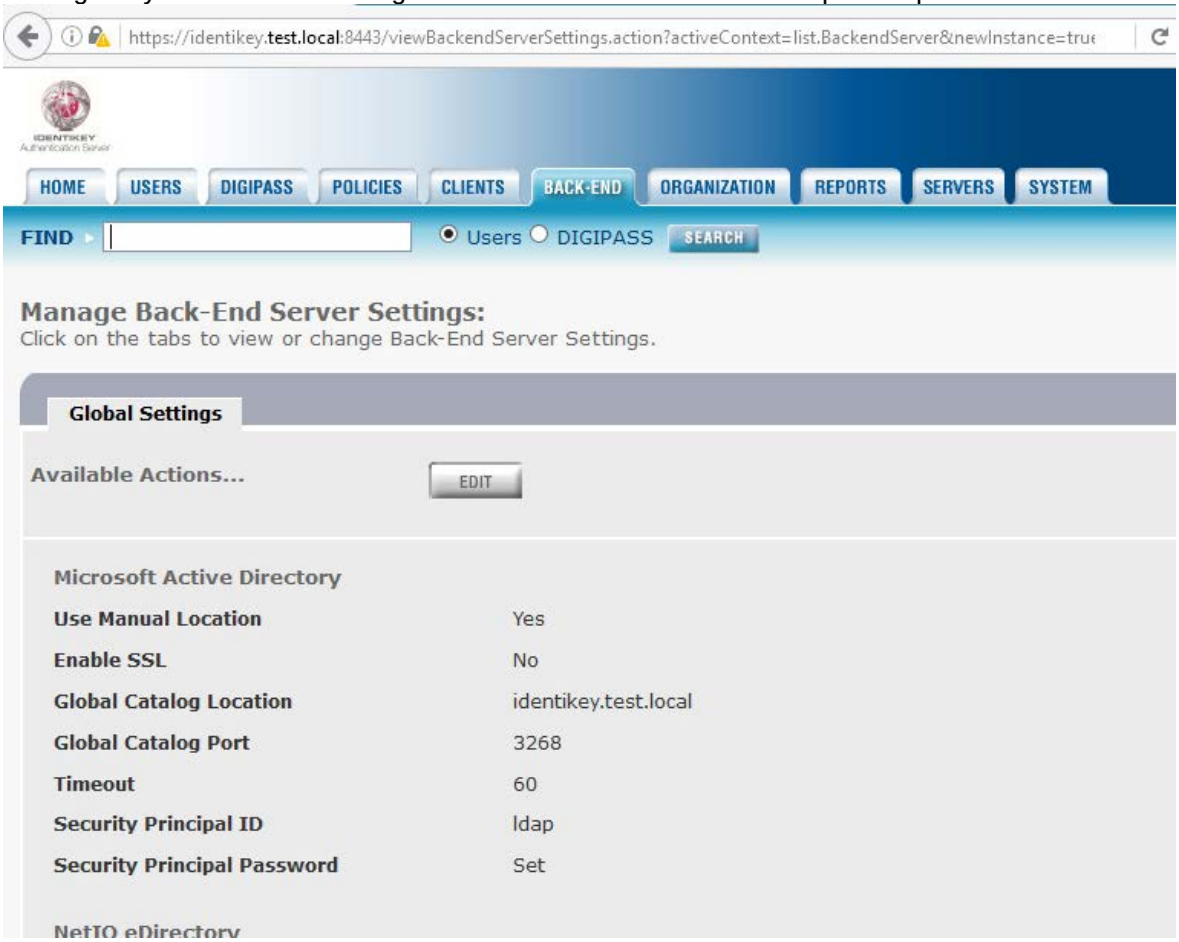
```
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnBind::bind] > Realm:
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnBind::bind] > Username: ldapAFR
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnBind::bind] > LDAP bind result: Success (0)
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::operator ()] > Attempting LDAP search...
[2016/11/10|14:12:42.341133UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::search] > Base distinguished name:
CN=Users,DC=AFR,DC=test,DC=local
[2016/11/10|14:12:42.356640UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::search] > Filter:
(&(objectClass=user)(sAMAccountName=jimmyaus))
[2016/11/10|14:12:42.356640UTC][S0/P584/T01284][INFO
][LdapBackEndAuthenticatorImpl::FnSearch::search] > LDAP search result: Success (0)
[2016/11/10|14:12:42.356640UTC][S0/P584/T01284][INFO
][LdapADBackEndAuthenticator::authenticate] > Search for user found none on LDAP server
'192.168.20.4'
[2016/11/10|14:12:42.356640UTC][S0/P584/T01284][INFO
][BackEndAuthenticationChecks::backEndVerification] > Setting m_backEndAuthState to [Fail]
[2016/11/10|14:12:42.356640UTC][S0/P584/T01284][DEBUG][AuthenticateRequest::calculateExitSt
ate] > User checks state is [User Exists], local auth state is [Password locally verified],
backend auth state is [Fail]
[2016/11/10|14:12:42.356640UTC][S0/P584/T01284][INFO ][AuthenticateRequest::dbUpdate] >
Fast authentication is <false>
```

Solution

When you have a similar configuration you can't define a backend authentication record for every subdomain. You MUST configure the global catalog option in Identikey Authentication Server:

1. Go to backend authentication – Settings

2. Configure your Global Catalog server with the environment specific parameters



IMPORTANT: It is important to know that the Security Principal ID must be the same in every subdomain with the same password.
So in our example you need to define the user ldap with e.g. password Test1234 in all the domains and the top level domain. If this ldap bind user is not present in the domains. Backend authentications will fail.

For more Details on how to configure LDAP Back-end authentication with Global Catalog, please check KB article KB 140178.