

This is a guide to troubleshooting LDAP integration in AC-Hunter. If you're running into problems using LDAP to authenticate web requests in AC-Hunter, please go through the following checks.

Please confirm that each check passes before moving on to the next. If you have questions or run into problems, please contact AC-Hunter support with one of the methods on <https://portal.activecountermeasures.com/support/>. Please:

- include any error messages you receive.
- let us know if your AC-Hunter users can log in with the original static username (commonly "welcome@activecountermeasures.com") and password.
- tell us how far you got through this checklist, and which step failed (along with how it failed)
- tell us what type of authentication you use on AD (password only, password + smartcard or token, etc.)
- include the "Authorization" section of `/etc/AC-Hunter/config.yaml` from your AC-Hunter system. Feel free to redact anything you're not comfortable sharing.
- tell us what kind of LDAP server you use, and on what operating system and version.

Please remember that any changes you make in `/etc/AC-Hunter/config.yaml` *do not take effect* until you run:

```
hunt up -d --force-recreate
```

1. Are you running AC-Hunter 6.1.0 or lower?

If not, please upgrade to 6.1.0 or higher as LDAP authentication was added in 6.1.0. We strongly recommend upgrading to 6.2.0 as it fixed some bugs in 6.1.0's LDAP code.

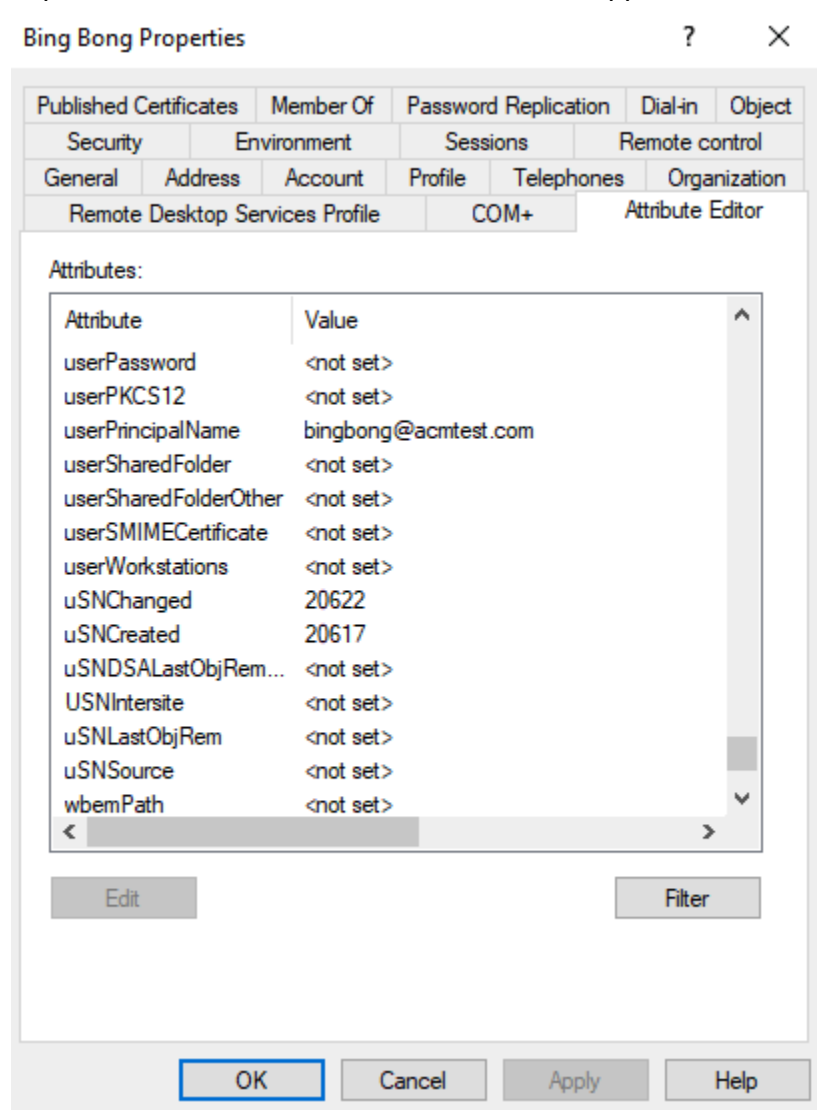
2. What LDAP server are you running?

- If you're running Microsoft's Active Directory LDAP server on Windows server 2016 or higher you'll need AC-Hunter 6.1.0 or higher.
- If you're running Microsoft's Active Directory LDAP server on Windows server 2012 you'll need AC-Hunter 6.2.0 or higher.
- If you're running Redhat's LDAP server, you'll need AC-Hunter 6.2.0 or higher.

3. Have you created a read-only user account on the AD/LDAP server that's used for AC-Hunter to make requests?

If not, please create one. The account should be in the form "[username@domain.name](#)". The userPrincipalName must also be set in the user attributes (see "Active Directory Users & Computers" with "Advanced Features" view enabled (see

image). It needs to use password authentication only, as opposed to authentication that requires a smartcard, token, or authenticator app.



4. Is your LDAP server running on port 389 (if using plaintext LDAP) or port 636 (TLS-encrypted LDAPS)?

If not, AC-Hunter will not be able to reach the LDAP service.

5. Can you reach that port from the AC-Hunter system?

From the command line on the AC-Hunter system, please try to connect to the LDAP/LDAPS port. If you're using TLS-encrypted LDAPS, you'll need to check that you can

reach port 636. If you're not able to use TLS encryption, you'll need to check that you can reach port 389 (be aware that this sends the LDAP password in plaintext).

Here are some example commands for connecting to port 636; start at the top and work your way down until you find a command that's installed on your system:

```
echo | ncat ldap.server.hostname.or.ip.address 636
echo | nc ldap.server.hostname.or.ip.address 636
echo | netcat ldap.server.hostname.or.ip.address 636
telnet ldap.server.hostname.or.ip.address 636
```

Similar commands if you're running LDAP on port 389:

```
echo | ncat ldap.server.hostname.or.ip.address 389
echo | nc ldap.server.hostname.or.ip.address 389
echo | netcat ldap.server.hostname.or.ip.address 389
telnet ldap.server.hostname.or.ip.address 389
```

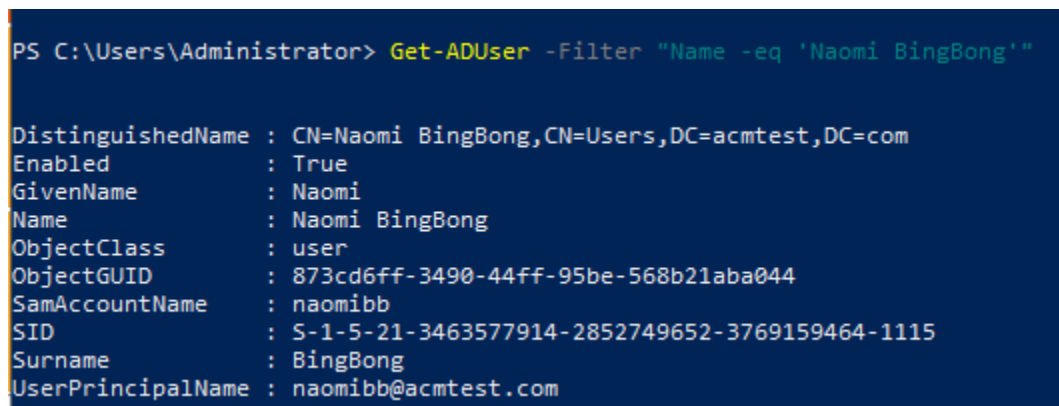
With all of the above, you're looking for an error to say that the port is closed or the host is unreachable - that means you can't reach the port. If the command runs but just sits there, that's fine; we're not constructing an actual ldap request, so the server is just twiddling its thumbs waiting for you.

If you cannot connect, please check that the two systems have a path to each other and that any firewalls, routers, and IPS's in between allow LDAP traffic.

6. Can you place an actual query to the ldap server?

First, we need to find a "Distinguished Name" - a block of text that looks like an oddly formatted email address. If you're not sure what that is in your LDAP environment, the simplest way to find one is to run the following command in a powershell window on the AD server:

```
Get-ADUser -Filter "Name -eq 'User's full name'"
```



```
PS C:\Users\Administrator> Get-ADUser -Filter "Name -eq 'Naomi BingBong'"
DistinguishedName : CN=Naomi BingBong,CN=Users,DC=acmtest,DC=com
Enabled           : True
GivenName        : Naomi
Name             : Naomi BingBong
ObjectClass      : user
ObjectGUID       : 873cd6ff-3490-44ff-95be-568b21aba044
SamAccountName   : naomibb
SID              : S-1-5-21-3463577914-2852749652-3769159464-1115
Surname         : BingBong
UserPrincipalName : naomibb@acmtest.com
```

Now that you have the Distinguished Name, you'll enter that same text in the "ldapwhoami" command in a terminal on the AC-Hunter server. To perform this step you may need to install the openldap-clients package with one of the following. The first is for Centos (and other rpm-based distributions), the second is for Ubuntu (and other apt-based distributions):

```
sudo yum -y install openldap-clients
sudo apt -y install ldap-utils
```

With ldapwhoami now installed, run the following, placing the Distinguished Name you found above in the double quotes:

```
ldapwhoami -x -h ldap.server.hostname.or.ip.address -D "cn=Naomi
BingBong,cn=Users,dc=acmtest,dc=com" -W -v
```

If all is working well, you'll see something like this:

```
naomi@test:~$ ldapwhoami -x -h 192.168.0.190 -D "CN=Naomi BingBong,CN=Users,DC=acmtest,DC=com" -W -v
ldap_initialize( ldap://192.168.0.190 )
Enter LDAP Password:
u:ACMTEST\naomibb
Result: Success (0)
```

7. Please carefully check the file /etc/AC-Hunter/config.yaml on the AC-Hunter server.

The yaml file format is particularly unforgiving about the spacing used at the beginning of each line; these need to be spaces, not tabs, and any lines you've added should be indented the same amount as other lines around it. Also, if there's any chance you've edited this on a Windows machine, please double check that the lines all end in the Unix format line feed and not the Windows "carriage return plus line feed".

The "SearchDN" value in that file is similar to the Distinguished Name we used above ("cn=Naomi BingBong,cn=Users,dc=acmtest,dc=com"), but is missing the first "cn=Users Name," piece. Here's an example:

```
SearchDN: CN=Users,DC=acmtest,DC=com
```

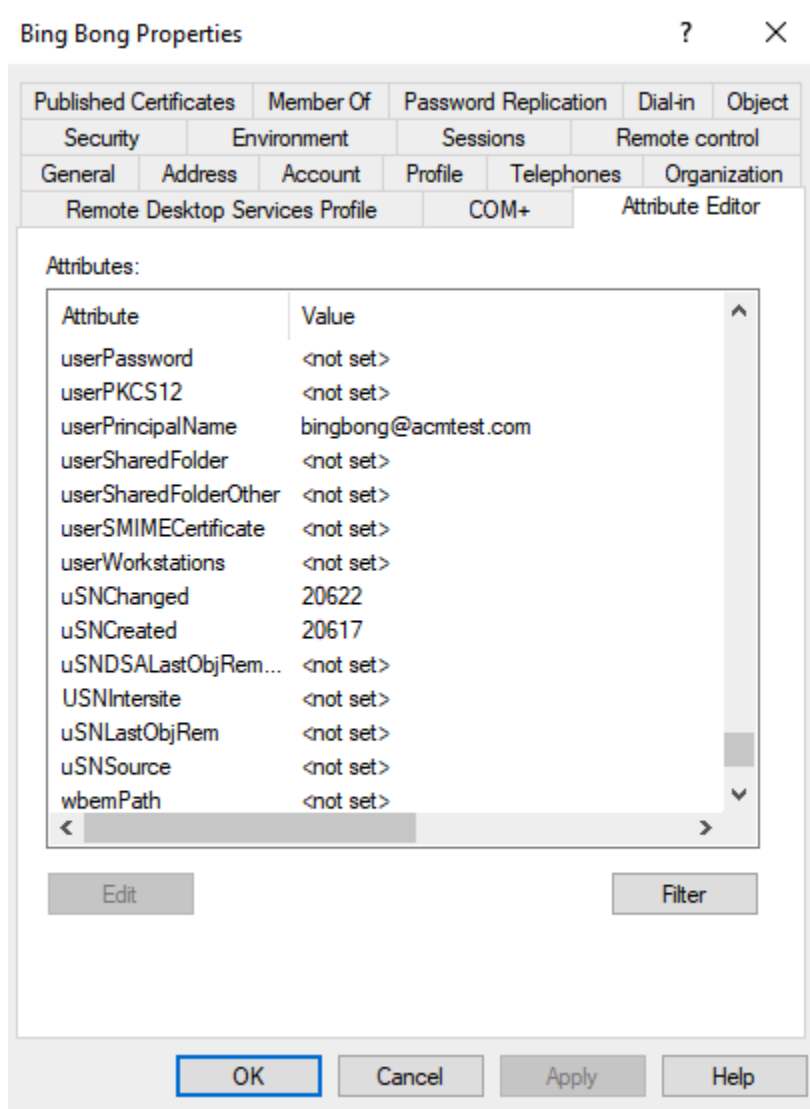
To check that the yaml file is correctly formatted, please use a tool like <http://www.yamllint.com/> (note, this is a free service not run by Active Countermeasures. You may want to redact any sensitive information in the file before uploading it.) This will report on any formatting issues in the file.

8. Are your AC-Hunter administrators in a security group called "AC-Hunter Users" on your Active Directory server?

If you're using a different group name, make sure you've edited the
AuthorizationGroup: "..."
line in /etc/AC-Hunter/config.yaml * to match it.

Like the read-only account AC-Hunter uses, your AC-Hunter administrator accounts need the following settings:

The userPrincipalName must also be set in the user attributes (see "Active Directory Users & Computers" with "Advanced Features" view enabled (see image)). They need to use password authentication only, as opposed to authentication that requires a smartcard, token, or authenticator app.



9. If you're using LDAPS/TLS, please check the certificate verification settings. If "VerifyCertificate" (in /etc/AC-Hunter/config.yaml, see Authorization:, Providers:, LDAP, then TLS) is set to true, please change it to "false" and run:

```
hunt up -d --force-recreate
```

Now try to log in again; does the login now succeed? This may mean that the "CAPath" field is not correctly set to your certificate file. Please see https://portal.activecountermeasures.com/support/faq/?Display_FAQ=4571 for the steps needed

to configure your certificate; once these are done, change "VerifyCertificate" back to "true" and rerun

```
hunt up -d --force-recreate
```

If all is good, you should now be able to log in.

10. Do your users use anything more than just a password to log into AD?

As of version 6.1.0, we only support password logins.

References:

- LDAP setup: see "Authenticating AC-Hunter User Accounts with Active Directory" in the User Guide for setup instructions.

- End-of-line differences between Linux and Windows: <https://en.wikipedia.org/wiki/Newline>

* After making any changes to /etc/AC-Hunter/config.yaml, make sure you run

```
hunt up -d --force-recreate
```

to load them.

Document date: Sep 20, 2023 00:10

If you find errors, omissions, or sections that are unclear, we'd appreciate it if you'd let us know at support@activecountermeasures.com.

Many thanks to Naomi for all her help with preparing these troubleshooting steps.