

ASA 8.0: Configure LDAP Authentication for WebVPN Users

Contents

[Introduction](#)

[Prerequisites](#)

[Background Information](#)

[Configure LDAP Authentication](#)

[ASDM](#)

[Command Line Interface](#)

[Perform Multi-Domain Searches \(Optional\)](#)

[Verify](#)

[Test with ASDM](#)

[Test with CLI](#)

[Troubleshoot](#)

[Related Information](#)

[Introduction](#)

This document demonstrates how to configure the Cisco Adaptive Security Appliance (ASA) to use an LDAP server for authentication of WebVPN users. The LDAP server in this example is Microsoft Active Directory. This configuration is performed with Adaptive Security Device Manager (ASDM) 6.0(2) on an ASA that runs software version 8.0(2).

Note: In this example Lightweight Directory Access Protocol (LDAP) authentication is configured for WebVPN users, but this configuration can be used for all other types of remote access clients as well. Simply assign the AAA server group to the desired connection profile (tunnel group), as shown.

[Prerequisites](#)

A basic VPN configuration is required. In this example WebVPN is used.

[Background Information](#)

In this example, the ASA checks with an LDAP server in order to verify the identity of users that it authenticates. This process does not work like a traditional Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) exchange. These steps explain, at a high level, how the ASA uses an LDAP server in order to check user credentials.

1. The user initiates a connection to the ASA.
2. The ASA is configured to authenticate that user with the Microsoft Active Directory (AD)/LDAP server.
3. The ASA binds to the LDAP server with the credentials configured on the ASA (admin in this case), and looks up the provided username. The **admin** user also obtains the appropriate credentials to list contents within Active Directory. Refer to <http://support.microsoft.com/?id=320528> for more information about how to grant LDAP query privileges. **Note:** The Microsoft website at <http://support.microsoft.com/?id=320528> is managed by a third party provider. Cisco is not responsible for its content.
4. If the username is found, the ASA attempts to bind to the LDAP server with the credentials that the user provided at login.
5. If the second bind is successful, authentication succeeds and the the ASA processes the attributes of the user. **Note:** In this example the attributes are not used for anything. Refer to [ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example](#) in order to see an example of how the ASA can process LDAP attributes.

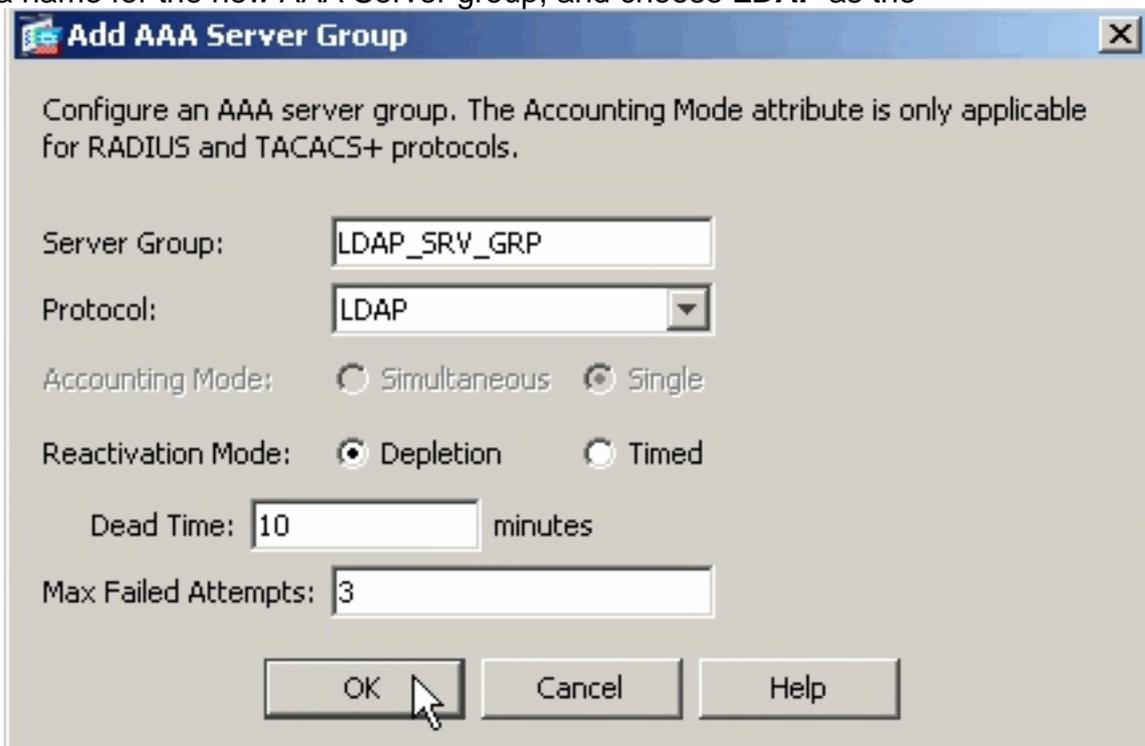
Configure LDAP Authentication

In this section, you are presented with the information to configure the ASA to use an LDAP server for the authentication of WebVPN clients.

ASDM

Complete these steps in the ASDM in order to configure the ASA to communicate with the LDAP server and authenticate WebVPN clients.

1. Navigate to Configuration > Remote Access VPN > AAA Setup > AAA Server Groups.
2. Click **Add** next to AAA Server Groups
3. Specify a name for the new AAA Server group, and choose **LDAP** as the



protocol.

4. Be sure that your new group is selected in the top pane, and click **Add** next to the **Servers** in

the Selected Group pane.

5. Provide the configuration information for your LDAP server. The subsequent screenshot illustrates an example configuration. This is an explanation of many of the configuration options:
Interface Name—the interface that the ASA uses in order to reach the LDAP server
Server Name or IP address—the address that the ASA uses in order to reach the LDAP server
Server Type—the type of LDAP server, such as Microsoft
Base DN—the location in the LDAP hierarchy where the server must begin to search
Scope—the extent of the search in the LDAP hierarchy that the server must make
Naming Attribute—the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server. **sAMAccountName** is the default attribute in the Microsoft Active Directory. Other commonly used attributes are CN, UID, and userPrincipalName.
Login DN—the DN with enough privileges in order to be able to search/read/lookup users in the LDAP server
Login Password—the password for the DN account
LDAP Attribute Map—an LDAP attribute map to be used with responses from this server. Refer to [ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example](#) for more information on how to configure LDAP attribute

Server Group: LDAP_SRV_GRP

Interface Name: inside

Server Name or IP Address: 192.168.1.2

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: Microsoft

Base DN: dc=ftwsecurity, dc=cisco, dc=com

Scope: All levels beneath the Base DN

Naming Attribute(s): sAMAccountName

Login DN: cn=admin, cn=users, dc=ftwsecurity, dc=cisco, dc=com

Login Password: *****

LDAP Attribute Map: -- None --

SASL MD5 authentication

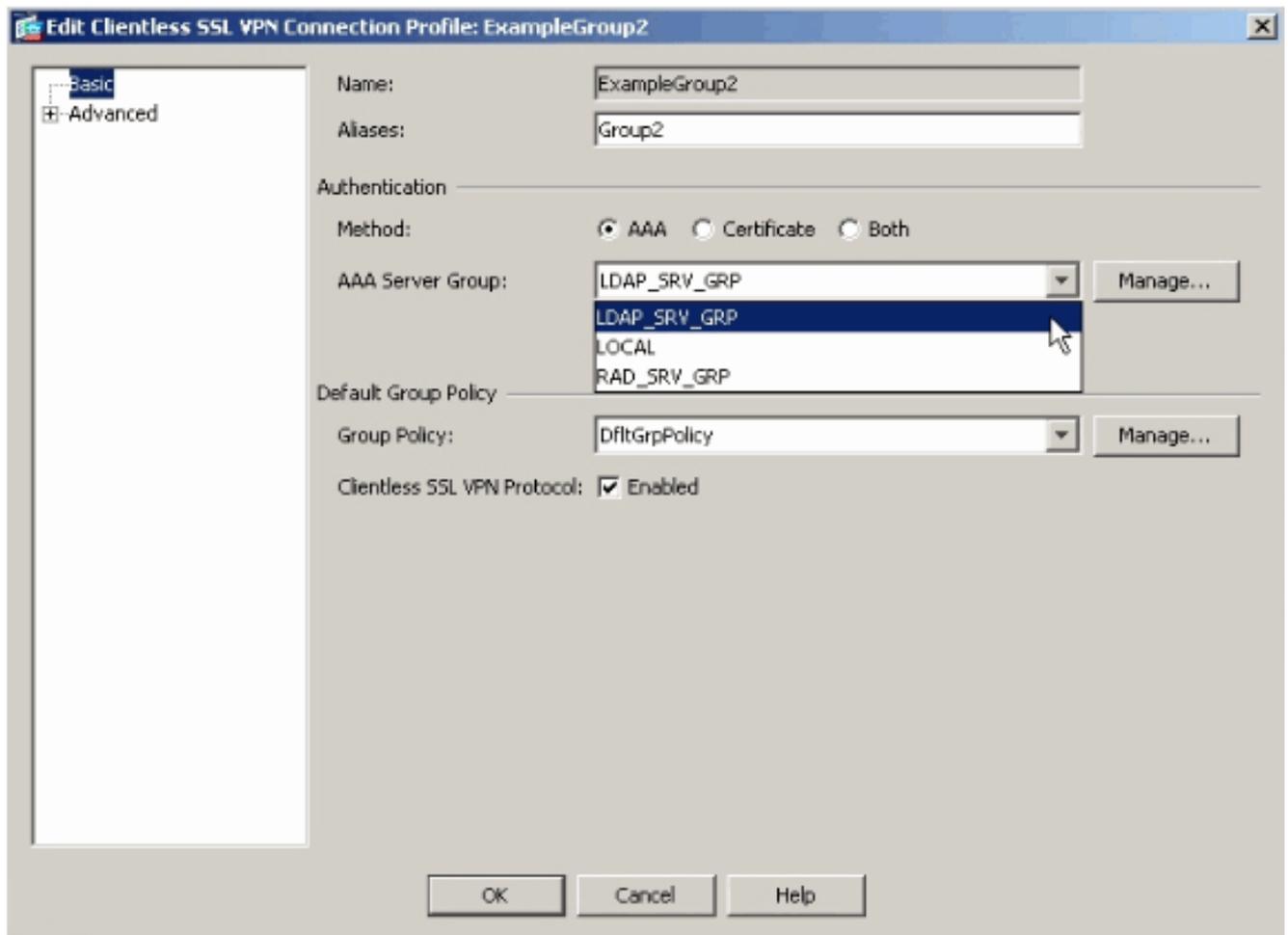
SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

maps.

6. Once you have configured the AAA server group and added a server to it, it is necessary to configure your connection profile (tunnel group) to use the new AAA configuration. Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.
7. Choose the connection profile (tunnel group) for which you want to configure AAA, and click **Edit**
8. Under **Authentication**, choose the LDAP server group that you created earlier.



Command Line Interface

Complete these steps in the command line interface (CLI) in order to configure the ASA to communicate with the LDAP server and authenticate WebVPN clients.

```

ciscoasa#configure terminal !--- Configure the AAA Server group.
ciscoasa(config)#aaa-server LDAP_SRV_GRP protocol ldap !--- Configure the AAA Server.
ciscoasa(config-aaa-server-group)#aaa-server LDAP_SRV_GRP (inside) host 192.168.1.2
ciscoasa(config-aaa-server-host)#ldap-base-dn dc=ftwsecurity, dc=cisco, dc=com
ciscoasa(config-aaa-server-host)#ldap-login-dn cn=admin, cn=users, dc=ftwsecurity,
dc=cisco, dc=com ciscoasa(config-aaa-server-host)#ldap-login-password *****
ciscoasa(config-aaa-server-host)#ldap-naming-attribute sAMAccountName
ciscoasa(config-aaa-server-host)#ldap-scope subtree ciscoasa(config-aaa-server-
host)#server-type microsoft ciscoasa(config-aaa-server-host)#exit !--- Configure the
tunnel group to use the new AAA setup. ciscoasa(config)#tunnel-group ExampleGroup2
general-att ciscoasa(config-tunnel-general)#authentication-server-group LDAP_SRV_GRP

```

Perform Multi-Domain Searches (Optional)

Optional. The ASA currently does not support the LDAP referral mechanism for multi-domain searches (Cisco bug ID CSCsj32153). Multi-domain searches are supported with the AD in Global Catalog Server mode. In order to perform multi-domain searches, setup up the AD server for Global Catalog Server mode, usually with the these key parameters for the LDAP server entry in the ASA. The key is to use an ldap-name-attribute that must be unique across the directory tree.

```

server-port 3268
ldap-scope subtree
ldap-naming-attribute userPrincipalName

```

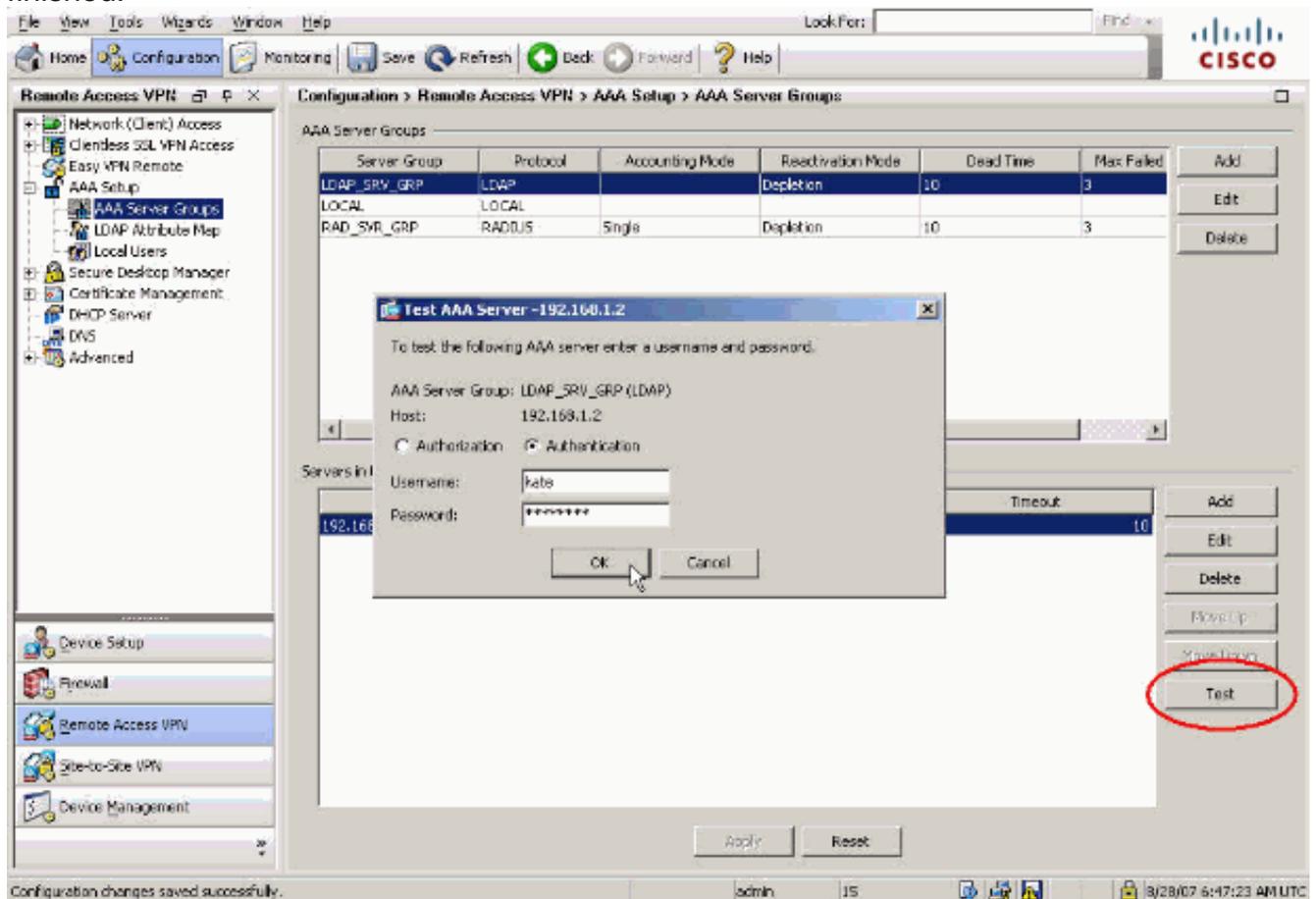
Verify

Use this section in order to confirm that your configuration works properly.

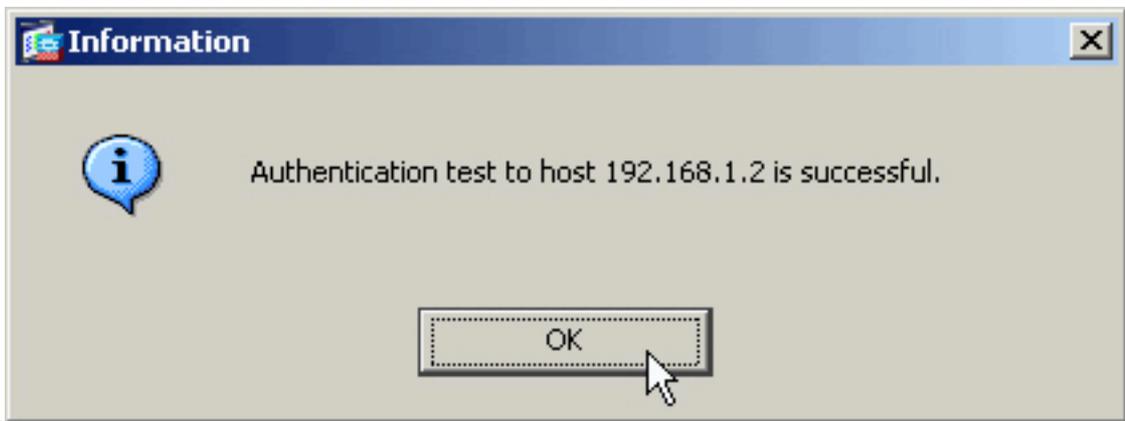
Test with ASDM

Verify your LDAP configuration with the **Test** button on the AAA Server Groups configuration screen. Once you supply a username and password, this button allows you to send a test authentication request to the LDAP server.

1. Navigate to Configuration > Remote Access VPN > AAA Setup > AAA Server Groups.
2. Select your desired AAA Server group in the top pane.
3. Select the AAA server that you want to test in the lower pane.
4. Click the **Test** button to the right of the lower pane.
5. In the window that appears, click the **Authentication** radio button, and supply the credentials with which you want to test. Click **OK** when finished.



6. After the ASA contacts the LDAP server, a success or failure message



appears.

Test with CLI

You can use the **test** command on the command line in order to test your AAA setup. A test request is sent to the AAA server, and the result appears on the command line.

```
ciscoasa#test aaa-server authentication LDAP_SRV_GRP host 192.168.1.2 username kate
password cisco123 INFO: Attempting Authentication test to IP address <192.168.1.2>
(timeout: 12 seconds) INFO: Authentication Successful
```

Troubleshoot

If unsure of the current DN string to use, you can issue the **dsquery** command on a Windows Active Directory server from a command prompt in order to verify the appropriate DN String of a user object.

```
C:\Documents and Settings\Administrator>dsquery user -samid kate !--- Queries Active
Directory for samid id "kate" "CN=Kate
Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com"
```

The **debug ldap 255** command can help to troubleshoot authentication problems in this scenario. This command enables LDAP debugging and allows you to watch the process that the ASA uses to connect to the LDAP server. This outputs show the ASA connect to the LDAP server as outlined in the [Background Information](#) section of this document.

This debug shows a successful authentication:

```
ciscoasa#debug ldap 255 [7] Session Start [7] New request Session, context
0xd4b11730, reqType = 1 [7] Fiber started [7] Creating LDAP context with
uri=ldap://192.168.1.2:389 [7] Connect to LDAP server: ldap://192.168.1.2:389, status
= Successful [7] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [7]
supportedLDAPVersion: value = 3 [7] supportedLDAPVersion: value = 2 [7]
supportedSASLMechanisms: value = GSSAPI [7] supportedSASLMechanisms: value = GSS-
SPNEGO [7] supportedSASLMechanisms: value = EXTERNAL [7] supportedSASLMechanisms:
value = DIGEST-MD5 !--- The ASA connects to the LDAP server as admin to search for
kate. [7] Binding as administrator [7] Performing Simple authentication for admin to
192.168.1.2 [7] LDAP Search: Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter =
[sAMAccountName=kate] Scope = [SUBTREE] [7] User DN = [CN=Kate
Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com] [7] Talking to Active Directory
server 192.168.1.2 [7] Reading password policy for kate, dn:CN=Kate Austen,CN=Users,
DC=ftwsecurity,DC=cisco,DC=com [7] Read bad password count 1 !--- The ASA binds to
the LDAP server as kate to test the password. [7] Binding as user [7] Performing
Simple authentication for kate to 192.168.1.2 [7] Checking password policy for user
kate [7] Binding as administrator [7] Performing Simple authentication for admin to
192.168.1.2 [7] Authentication successful for kate to 192.168.1.2 [7] Retrieving user
```

```
attributes from server 192.168.1.2 [7] Retrieved Attributes: [7] objectClass: value =
top [7] objectClass: value = person [7] objectClass: value = organizationalPerson [7]
objectClass: value = user [7] cn: value = Kate Austen [7] sn: value = Austen [7]
givenName: value = Kate [7] distinguishedName: value = CN=Kate
Austen,CN=Users,DC=ftwsecurity, DC=cisco,DC=com [7] instanceType: value = 4 [7]
whenCreated: value = 20070815155224.OZ [7] whenChanged: value = 20070815195813.OZ [7]
displayName: value = Kate Austen [7] uSNCreated: value = 16430 [7] memberOf: value =
CN=Castaways,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7] memberOf: value =
CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7] uSNChanged: value = 20500
[7] name: value = Kate Austen [7] objectGUID: value = ..z...yC.q0..... [7]
userAccountControl: value = 66048 [7] badPwdCount: value = 1 [7] codePage: value = 0
[7] countryCode: value = 0 [7] badPasswordTime: value = 128321799570937500 [7]
lastLogoff: value = 0 [7] lastLogon: value = 128321798130468750 [7] pwdLastSet: value
= 128316667442656250 [7] primaryGroupID: value = 513 [7] objectSid: value =
.....Q..p..*p?E.Z... [7] accountExpires: value = 9223372036854775807 [7]
logonCount: value = 0 [7] sAMAccountName: value = kate [7] sAMAccountType: value =
805306368 [7] userPrincipalName: value = kate@ftwsecurity.cisco.com [7]
objectCategory: value = CN=Person,CN=Schema,CN=Configuration,
DC=ftwsecurity,DC=cisco,DC=com [7] dSCorePropagataionData: value = 20070815195237.OZ
[7] dSCorePropagataionData: value = 20070815195237.OZ [7] dSCorePropagataionData: value
= 20070815195237.OZ [7] dSCorePropagataionData: value = 16010108151056.OZ [7] Fiber
exit Tx=685 bytes Rx=2690 bytes, status=1 [7] Session End
```

This debug shows an authentication that fails due to an incorrect password:

```
ciscoasa#debug ldap 255 [8] Session Start [8] New request Session, context
0xd4b11730, reqType = 1 [8] Fiber started [8] Creating LDAP context with
uri=ldap://192.168.1.2:389 [8] Connect to LDAP server: ldap://192.168.1.2:389, status
= Successful [8] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [8]
supportedLDAPVersion: value = 3 [8] supportedLDAPVersion: value = 2 [8]
supportedSASLMechanisms: value = GSSAPI [8] supportedSASLMechanisms: value = GSS-
SPNEGO [8] supportedSASLMechanisms: value = EXTERNAL [8] supportedSASLMechanisms:
value = DIGEST-MD5 !--- The ASA connects to the LDAP server as admin to search for
kate. [8] Binding as administrator [8] Performing Simple authentication for admin to
192.168.1.2 [8] LDAP Search: Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter =
[sAMAccountName=kate] Scope = [SUBTREE] [8] User DN = [CN=Kate
Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com] [8] Talking to Active Directory
server 192.168.1.2 [8] Reading password policy for kate, dn:CN=Kate Austen,CN=Users,
DC=ftwsecurity,DC=cisco,DC=com [8] Read bad password count 1 !--- The ASA attempts to
bind as kate, but the password is incorrect. [8] Binding as user [8] Performing
Simple authentication for kate to 192.168.1.2 [8] Simple authentication for kate
returned code (49) Invalid credentials [8] Binding as administrator [8] Performing
Simple authentication for admin to 192.168.1.2 [8] Reading bad password count for
kate, dn: CN=Kate Austen,CN=Users, DC=ftwsecurity,DC=cisco,DC=com [8] Received
badPwdCount=1 for user kate [8] badPwdCount=1 before, badPwdCount=1 after for kate
[8] now: Tue, 28 Aug 2007 15:33:05 GMT, lastset: Wed, 15 Aug 2007 15:52:24 GMT,
delta=1122041, maxage=3710851 secs [8] Invalid password for kate [8] Fiber exit
Tx=788 bytes Rx=2904 bytes, status=-1 [8] Session End
```

This debug shows an authentication that fails because the user can not be found on the LDAP server:

```
ciscoasa#debug ldap 255 [9] Session Start [9] New request Session, context
0xd4b11730, reqType = 1 [9] Fiber started [9] Creating LDAP context with
uri=ldap://192.168.1.2:389 [9] Connect to LDAP server: ldap://192.168.1.2:389, status
= Successful [9] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [9]
supportedLDAPVersion: value = 3 [9] supportedLDAPVersion: value = 2 [9]
supportedSASLMechanisms: value = GSSAPI [9] supportedSASLMechanisms: value = GSS-
SPNEGO [9] supportedSASLMechanisms: value = EXTERNAL [9] supportedSASLMechanisms:
value = DIGEST-MD5 !--- The user mikhail is not found. [9] Binding as administrator
[9] Performing Simple authentication for admin to 192.168.1.2 [9] LDAP Search: Base
DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=mikhail] Scope =
```

```
[SUBTREE] [9] Requested attributes not found [9] Fiber exit Tx=256 bytes Rx=607
bytes, status=-1 [9] Session End
```

The debugs show this error message when the connectivity between the ASA and the LDAP authentication server does not work:

```
ciscoasa# debug webvpn 255
INFO: debug webvpn enabled at level 255.
ciscoasa# webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
...not resuming [2587]
webvpn_portal.c:http_webvpn_kill_cookie[787]
webvpn_auth.c:http_webvpn_pre_authentication[2327]
WebVPN: calling AAA with ewsContext (-847917520) and nh (-851696992)!
webvpn_auth.c:webvpn_add_auth_handle[5118]
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[5158] WebVPN: AAA status = (ERROR)
webvpn_portal.c:ewaFormSubmit_webvpn_login[2162] ewaFormSubmit_webvpn_login: tgCookie
= NULL ewaFormSubmit_webvpn_login: cookie = 1 ewaFormSubmit_webvpn_login: tgCookieSet
= 0 ewaFormSubmit_webvpn_login: tgroup = NULL ...resuming [2564]
webvpn_auth.c:http_webvpn_post_authentication[1506] WebVPN: user: (utrcd01) auth
error.
```

[Related Information](#)

- [Technical Support & Documentation - Cisco Systems](#)