



## APPENDIX **E**

# Configuring an External Server for Authorization and Authentication

---

This appendix describes how to configure an external LDAP or RADIUS server to support the authentication and authorization of security appliance, VPN3000, and PIX users. Authentication determines who the user is and authorization determines what the user can do. Before you configure the security appliance to use an external server, you must configure the server with the correct security appliance authorization attributes and, from a subset of these attributes, assign specific permissions to individual users.

This appendix includes the following sections:

- [Selecting LDAP, RADIUS, or Local Authentication and Authorization](#)
- [Understanding Policy Enforcement of Permissions and Attributes](#)
- [Configuring an External LDAP Server](#)
- [Configuring an External RADIUS Server](#)

## Selecting LDAP, RADIUS, or Local Authentication and Authorization

To help you decide which authentication or authorization method is right for your platform, this section describes the LDAP and RADIUS support provided with the security appliance (ASA), PIX, and the VPN 3000 platforms.

- **LDAP Authentication**  
Supported on PIX 7.1.x and the security appliance only. VPN 3000 does not support native LDAP authentication. The LDAP server retrieves and searches for the username and enforces any defined attributes as part of the authorization function.
- **LDAP Authorization**  
Supported on PIX, VPN 3000, and the security appliance. The LDAP server retrieves/searches the username and enforces any defined attributes.
- **RADIUS Authentication**  
Supported on PIX, VPN 3000, and the security appliance. The RADIUS server retrieves/searches the username and enforces any defined attributes as it performs the authorization function.
- **RADIUS Authorization**

Supported on PIX, VPN 3000, and the security appliance. The RADIUS server retrieves/searches the username and enforces any defined attributes.

- Local Authentication

Supported on PIX, VPN 3000, and the security appliance. The Local/Internal server retrieves/searches the username and enforces any defined attributes as part of the authorization function.

- Local Authorization

Supported on PIX 7.1.x and the security appliance only. The Local/Internal server retrieves/searches the username and enforces any defined attributes.

## Understanding Policy Enforcement of Permissions and Attributes

You can configure the security appliance to receive user attributes from either the LOCAL/internal database, a RADIUS/LDAP authentication server, or a RADIUS/LDAP authorization server. You can also place users into group-policies with different attributes, but the user attributes will always take precedence. After the device authenticates the user and group(s), the security appliance combines the user and group attribute sets into one aggregate attribute set. The security appliance uses the attributes in the following order and applies the aggregate attribute set to the authenticated user.

1. User attributes—The server returns these after successful user authentication or authorization. These take precedence over all others.
2. Group policy attributes—These attributes come from the group policy associated with the user. You identify the user group policy name in the local database by the 'vpn-group-policy' attribute or from an external RADIUS/LDAP server by the value of the RADIUS CLASS attribute (25) in the format 'OU=GroupName;'. The group policy provides any attributes that are missing from the user attributes. User attributes override group policy attributes if both have a value.
3. Tunnel group default-group-policy attributes—These attributes come from the default-group-policy (Base group) that is associated with the tunnel group. After a lookup of that group policy, the Tunnel Group's default-group-policy provide any attributes that are missing from the user or group policy attributes. User attributes override group policy attributes if both have a value.
4. System default attributes—System default attributes provide any attributes that are missing from the user, group, or tunnel group attributes.

## Configuring an External LDAP Server



### Note

For more information on the LDAP protocol, see RFCs 1777, 2251, and 2849.

This section describes the structure, schema, and attributes of an LDAP server. It includes the following topics:

- [Reviewing the LDAP Directory Structure and Configuration Procedure](#)
- [Organizing the Security Appliance LDAP Schema](#)
- [Defining the Security Appliance LDAP Schema](#)

- [Loading the Schema in the LDAP Server](#)
- [Defining User Permissions](#)
- [Reviewing Examples of Active Directory Configurations](#)

## Reviewing the LDAP Directory Structure and Configuration Procedure

An LDAP server stores information as entries in a directory. An LDAP schema defines what types of information such entries store. The schema lists classes and the set of (required and optional) attributes that objects of each class can contain.

To configure your LDAP server to interoperate with the security appliance, define a security appliance authorization schema. A security appliance authorization schema defines the class and attributes of that class that the security appliance supports. Specifically, it comprises the object class (cVPN3000-User-Authorization) and all its possible attributes that may be used to authorize a security appliance user (such as access hours, primary DNS, and so on). Each attribute comprises the attribute name, its number (called an object identifier or OID), its type, and its possible values.

Once you have defined the security appliance authorization schema and loaded it on your server, define the security appliance attributes and permissions and their respective values for each user who will be authorizing to the server.

In summary, to set up your LDAP server:

- Design your security appliance LDAP authorization schema based on the hierarchical set-up of your organization
- Define the security appliance authorization schema
- Load the schema on the LDAP server
- Define permissions for each user on the LDAP server

The specific steps of these processes vary, depending on which type of LDAP server you are using.

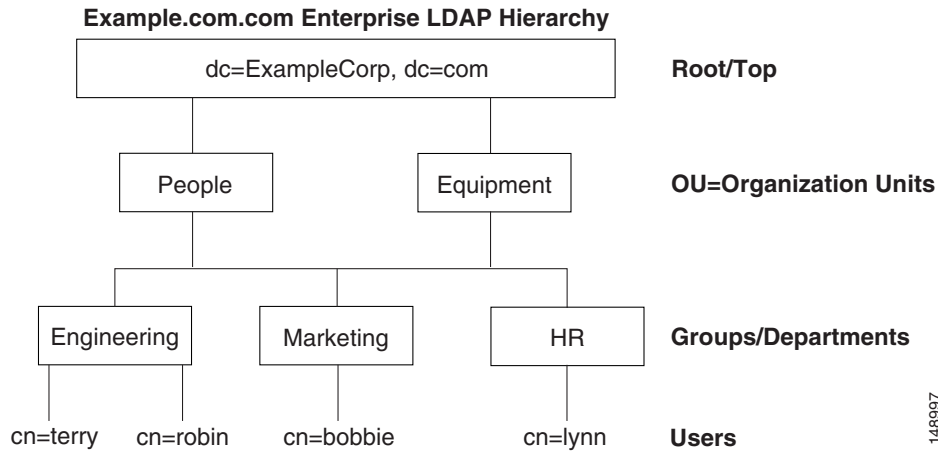
## Organizing the Security Appliance LDAP Schema

Before you actually create your schema, think about how your organization is structured. Your LDAP schema should reflect the logical hierarchy of your organization.

For example, suppose an employee at your company, Example Corporation, is named Terry. Terry works in the Engineering group. Your LDAP hierarchy could have one or many levels. You might decide to set up a shallow, single-level hierarchy in which Terry is considered a member of Example Corporation. Or, you could set up a multi-level hierarchy in which Terry is considered to be a member of the department Engineering, which is a member of an organizational unit called People, which is itself a member of Example Corporation. See [Figure E-1](#) for an example of this multi-level hierarchy.

A multi-level hierarchy has more granularity, but a single level hierarchy is quicker to search.

Figure E-1 A Multi-Level LDAP Hierarchy



## Searching the Hierarchy

The security appliance lets you tailor the search within the LDAP hierarchy. You configure the following three fields on the security appliance to define where in the LDAP hierarchy your search begins, its extent, and the type of information it is looking for. Together these fields allow you to limit the search of the hierarchy to just the part of the tree that contains the user permissions.

- LDAP Base DN defines where in the LDAP hierarchy the server should begin searching for user information when it receives an authorization request from the security appliance.
- Search Scope defines the extent of the search in the LDAP hierarchy. The search proceeds this many levels in the hierarchy below the LDAP Base DN. You can choose to have the server search only the level immediately below, or it can search the entire subtree. A single level search is quicker, but a subtree search is more extensive.
- Naming Attribute(s) defines the Relative Distinguished Name (RDN) that uniquely identifies an entry in the LDAP server. Common naming attributes are: cn (Common Name) and ui (user identification).

Figure E-1 shows a possible LDAP hierarchy for Example Corporation. Given this hierarchy, you could define your search in different ways. Table E-1 shows two possible search configurations.

In the first example configuration, when Terry establishes his or her IPsec tunnel with LDAP authorization required, the security appliance sends a search request to the LDAP server indicating it should search for Terry in the Engineering group. This search is quick.

In the second example configuration, the security appliance sends a search request indicating the server should search for Terry within Example Corporation. This search takes longer.

Table E-1 Example Search Configurations

#	LDAP Base DN	Search Scope	Naming Attribute	Result
1	group= Engineering,ou=People,dc=ExampleCorporation,dc=com	One Level	cn=Terry	Quicker search
2	dc=ExampleCorporation,dc=com	Subtree	cn=Terry	Longer search

## Binding the Security Appliance to the LDAP Server

Some LDAP servers (including the Microsoft Active Directory server) require the security appliance to establish a handshake via authenticated binding before they accept requests for any other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field defines the authentication characteristics of the security appliance; these characteristics should correspond to those of a user with administration privileges. An example Login DN field could be: `cn=Administrator, cn=users, ou=people, dc=example, dc=com`.

## Defining the Security Appliance LDAP Schema

Once you have decided how to structure your user information in the LDAP hierarchy, define this organization in a schema. To define the schema, begin by defining the object class name. The class name for the security appliance directory is `cVPN3000-User-Authorization`. The class has the object identifier (OID) `1.2.840.113556.1.8000.795.1.1`. Every entry or user in the directory is an object of this class.

Some LDAP servers (for example, the Microsoft Active Directory LDAP server) do not allow you to reuse the class OID once you have defined it. Use the next incremental OID. For example, if you incorrectly defined the class name as `cVPN3000-Usr-Authorization` with OID `1.2.840.113556.1.8000.795.1.1`, you can enter the correct class name `cVPN3000-User-Authorization` with the next OID, for example, `1.2.840.113556.1.8000.795.1.2`.

For the Microsoft Active Directory LDAP server, define the schema in text form in a file using the LDAP Data Interchange Format (LDIF). This file has an extension of `.ldif`, for example: `schema.ldif`. Other LDAP servers use graphical user interfaces or script files to define the object class and its attributes. For more information on LDIF, see RFC-2849.



### Note

- All LDAP attributes for all three appliances begin with the letters `cVPN3000`; for example: `cVPN3000-Access-Hours`.
- The appliances enforce the LDAP attributes based on attribute name, not numeric ID. RADIUS attributes, on the other hand, are enforced by numeric ID, not by name.
- Authorization refers to the process of enforcing permissions or attributes. An LDAP server defined as an authentication or authorization server will enforce permissions or attributes if they are configured.

For a complete list of attributes for the security appliance, the PIX Firewall and the VPN 3000, see [Table E-2](#).

All strings are case-sensitive and you must use an attribute name as capitalized in the table even if it conflicts with how a term is typically written. For example, use `cVPN3000-IETF-Radius-Class`, not `cVPN3000-IETF-RADIUS-Class`.

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-Access-Hours	Y	Y	Y	1	String	Single	Name of the time-range (i.e., Business-Hours)
cVPN3000-Simultaneous-Logins	Y	Y	Y	2	Integer	Single	0-2147483647
cVPN3000-Primary-DNS	Y	Y	Y	3	String	Single	An IP address
cVPN3000-Secondary-DNS	Y	Y	Y	4	String	Single	An IP address
cVPN3000-Primary-WINS	Y	Y	Y	5	String	Single	An IP address
cVPN3000-Secondary-WINS	Y	Y	Y	6	String	Single	An IP address
cVPN3000-SEP-Card-Assignment				7	Integer	Single	Not used
cVPN3000-Tunneling-Protocols	Y	Y	Y	8	Integer	Single	1 = PPTP 2 = L2TP 4 = IPSec 8 = L2TP/IPSec 16 = WebVPN. 8 and 4 are mutually exclusive (0 - 11, 16 - 27 are legal values)
cVPN3000-IPSec-Sec-Association	Y			9	String	Single	Name of the security association
cVPN3000-IPSec-Authentication	Y			10	Integer	Single	0 = None 1 = RADIUS 2 = LDAP (authorization only) 3 = NT Domain 4 = SDI 5 = Internal 6 = RADIUS with Expiry 7 = Kerberos/Active Directory
cVPN3000-IPSec-Banner1	Y	Y	Y	11	String	Single	Banner string
cVPN3000-IPSec-Allow-Passwd-Store	Y	Y	Y	12	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-Use-Client-Address	Y			13	Boolean	Single	0 = Disabled 1 = Enabled

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-PPTP-Encryption	Y			14	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Required Example: 15 = 40/128-Encr/Stateless-Req
cVPN3000-L2TP-Encryption	Y			15	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bit 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateless-Req
cVPN3000-IPSec-Split-Tunnel-List	Y	Y	Y	16	String	Single	Specifies the name of the network or access list that describes the split tunnel inclusion list.
cVPN3000-IPSec-Default-Domain	Y	Y	Y	17	String	Single	Specifies the single default domain name to send to the client (1-255 characters).
cVPN3000-IPSec-Split-DNS-Name	Y	Y	Y	18	String	Single	Specifies the list of secondary domain names to send to the client (1-255 characters).
cVPN3000-IPSec-Tunnel-Type	Y	Y	Y	19	Integer	Single	1 = LAN-to-LAN 2 = Remote access
cVPN3000-IPSec-Mode-Config	Y	Y	Y	20	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-User-Group-Lock	Y			21	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-Over-UDP	Y	Y	Y	22	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-Over-UDP-Port	Y	Y	Y	23	Integer	Single	4001 - 49151, default = 10000
cVPN3000-IPSec-Banner2	Y	Y	Y	24	String	Single	Banner string
cVPN3000-PPTP-MPPC-Compression	Y			25	Integer	Single	0 = Disabled 1 = Enabled

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-L2TP-MPPC-Compression	Y			26	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-IP-Compression	Y	Y	Y	27	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-IKE-Peer-ID-Check	Y	Y	Y	28	Integer	Single	1 = Required 2 = If supported by peer certificate 3 = Do not check
cVPN3000-IKE-Keep-Alive	Y	Y	Y	29	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-Auth-On-Rekey	Y	Y	Y	30	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-Required-Client- Firewall-Vendor-Code	Y	Y	Y	31	Integer	Single	1 = Cisco Systems (with Cisco Integrated Client) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (with Cisco Intrusion Prevention Security Agent)

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-Required-Client-Firewall-Product-Code	Y	Y	Y	32	Integer	Single	Cisco Systems Products: 1 = Cisco Intrusion Prevention Security Agent or Cisco Integrated Client (CIC)  Zone Labs Products: 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity  NetworkICE Product: 1 = BlackIce Defender/Agent  Sygate Products: 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
cVPN3000-Required-Client-Firewall-Description	Y	Y	Y	33	String	Single	String
cVPN3000-Require-Individual-User-Auth	Y	Y	Y	34	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-Require-HW-Client-Auth	Y	Y	Y	35	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-Authenticated-User-Idle-Timeout	Y	Y	Y	36	Integer	Single	1 - 35791394 minutes
cVPN3000-Cisco-IP-Phone-Bypass	Y	Y	Y	37	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-IPSec-Split-Tunneling-Policy	Y	Y	Y	38	Integer	Single	0 = Tunnel everything 1 = Split tunneling 2 = Local LAN permitted
cVPN3000-IPSec-Required-Client-Firewall-Capability	Y	Y	Y	39	Integer	Single	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = Policy from server

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-IPSec-Client-Firewall-Filter-Name	Y			40	String	Single	Specifies the name of the filter to be pushed to the client as firewall policy.
cVPN3000-IPSec-Client-Firewall-Filter-Optional	Y	Y	Y	41	Integer	Single	0 = Required 1 = Optional
cVPN3000-IPSec-Backup-Servers	Y	Y	Y	42	String	Single	1 = Use Client-Configured list 2 = Disabled and clear client list 3 = Use Backup Server list
cVPN3000-IPSec-Backup-Server-List	Y	Y	Y	43	String	Single	Server Addresses (space delimited)
cVPN3000-Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	44	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-MS-Client-Subnet-Mask	Y	Y	Y	45	String	Single	An IP address
cVPN3000-Allow-Network-Extension-Mode	Y	Y	Y	46	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-Strip-Realm	Y	Y	Y	47	Boolean	Single	0 = Disabled 1 = Enabled
cVPN3000-Cisco-AV-Pair	Y	Y	Y	48	String	Multi	An octet string in the following format:  [Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]  For more information, see <a href="#">“Cisco -AV-Pair Attribute Syntax.”</a>
cVPN3000-User-Auth-Server-Name	Y			49	String	Single	IP address or hostname
cVPN3000-User-Auth-Server-Port	Y			50	Integer	Single	Port number for server protocol
cVPN3000-User-Auth-Server-Secret	Y			51	String	Single	Server password
cVPN3000-Confidence-Interval	Y	Y	Y	52	Integer	Single	10 - 300 seconds
cVPN3000-Cisco-LEAP-Bypass	Y	Y	Y	53	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-DHCP-Network-Scope	Y	Y	Y	54	String	Single	IP address

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-Client-Type-Version-Limiting	Y	Y	Y	55	String	Single	IPsec VPN client version number string
cVPN3000-WebVPN-Content-Filter-Parameters	Y	Y		56	Integer	Single	1 = Java & ActiveX 2 = Java scripts 4 = Images 8 = Cookies in images Add the values to filter multiple parameters. For example: enter 10 to filter both Java scripts and cookies. (10 = 2 + 8)
cVPN3000-WebVPN-Enable-functions				57	Integer	Single	Not used - deprecated
cVPN3000-WebVPN-Exchange-Server-Address				58	String	Single	Not used - deprecated
cVPN3000-WebVPN-Exchange-Server-NETBIOS-Name				59	String	Single	Not used - deprecated
cVPN3000-Port-Forwarding-Name	Y	Y		60	String	Single	Name string (for example, "Corporate-Apps")
cVPN3000-IETF-Radius-Framed-IP-Address	Y	Y	Y	61	String	Single	An IP address
cVPN3000-IETF-Radius-Framed-IP-Netmask	Y	Y	Y	62	String	Single	An IP address
cVPN3000-IETF-Radius-Session-Timeout	Y	Y	Y	63	Integer	Single	1-35791394 minutes 0 = Unlimited
cVPN3000-IETF-Radius-Idle-Timeout	Y	Y	Y	64	Integer	Single	1-35791394 minutes 0 = Unlimited
cVPN3000-IETF-Radius-Class	Y	Y	Y	65	String	Single	Group name string. Use any of the these three formats: OU=Engineering OU=Engineering; Engineering
cVPN3000-IETF-Radius-Filter-Id	Y	Y	Y	66	String	Single	An access-list
cVPN3000-Authorization-Required	Y			67	Integer	Single	0 = No 1 = Yes
cVPN3000-Authorization-Type	Y			68	Integer	Single	0 = None 1 = RADIUS 2 = LDAP

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-DN-Field	Y	Y	Y	69	String	Single	Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name.
cVPN3000-WebVPN-URL-List		Y		70	String	Single	URL-list name
cVPN3000-WebVPN-Forwarded-Ports		Y		71	String	Single	Port-Forward list name
cVPN3000-WebVPN-ACL-Filters		Y		72	String	Single	Access-List name
cVPN3000-WebVPN-Homepage	Y	Y		73	String	Single	A url such as http://example-portal.com.
cVPN3000-WebVPN-Single-Sign-On-Server-Name		Y		74	String	Single	Name of the SSO Server (1 - 31 chars)
cVPN3000-WebVPN-URL-Entry-Enable	Y	Y		75	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-File-Access-Enable	Y	Y		76	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-File-Server-Entry-Enable	Y	Y		77	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-File-Server-Browsing-Enable	Y	Y		78	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-Port-Forwarding-Enable	Y	Y		79	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	Y		80	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-Port-Forwarding-HTTP-Proxy-Enable	Y	Y		81	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-Port-Forwarding-Auto-Download-Enable	Y	Y		82	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-Citrix-Support-Enable	Y	Y		83	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-Apply-ACL-Enable	Y	Y		84	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-SVC-Enable	Y	Y		85	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-WebVPN-SVC-Required-Enable	Y	Y		86	Integer	Single	0 = Disabled 1 = Enabled

Table E-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)

Attribute Name/ OID (Object Identifier)	VPN 3000	ASA	PIX	Attr. OID <sup>1</sup>	Syntax/ Type	Single or Multi- Valued	Possible Values
cVPN3000-WebVPN-SVC-Keep-Enable	Y	Y		87	Integer	Single	0 = Disabled 1 = Enabled
cVPN3000-IE-Proxy-Server	Y			88	String	Single	IP address
cVPN3000-IE-Proxy-Method	Y			89	Integer	Single	1 = No Modify 2 = No Proxy 3 = Auto Detect 4 = Other
cVPN3000-IE-Proxy-Exception-List	Y			90	String	Single	newline (\n)-separated list of DNS domains
cVPN3000-IE-Proxy-Bypass-Local	Y			91	Integer	Single	0 = None 1 = Local
cVPN3000-Tunnel-Group-Lock		Y	Y	92	String	Single	Name of the tunnel group or "none"
cVPN3000-Firewall-ACL-In		Y	Y	93	String	Single	Access list ID
cVPN3000-Firewall-ACL-Out		Y	Y	94	String	Single	Access list ID
cVPN3000-PFS-Required	Y	Y	Y	95	Boolean	Single	0 = No 1 = Yes
cVPN3000-WebVPN-SVC-Keepalive	Y	Y		96	Integer	Single	0 = Disabled n = Keepalive value in seconds (15 - 600)
cVPN3000-WebVPN-SVC-Client-DPD	Y	Y		97	Integer	Single	0 = Disabled n = Dead Peer Detection value in seconds (30 - 3600)
cVPN3000-WebVPN-SVC-Gateway-DPD	Y	Y		98	Integer	Single	0 = Disabled n = Dead Peer Detection value in seconds (30 - 3600)
cVPN3000-WebVPN-SVC-Rekey-Period	Y	Y		99	Integer	Single	0 = Disabled n = Retry period in minutes (4 - 10080)
cVPN3000-WebVPN-SVC-Rekey-Method	Y	Y		100	Integer	Single	0 = None 1 = SSL 2 = New tunnel 3 = Any (sets to SSL)
cVPN3000-WebVPN-SVC-Compression	Y	Y		101	Integer	Single	0 = None 1 = Deflate Compression

- To get the complete Object Identifier of each attribute, append the number in the column to the end of 1.2.840.113556.8000.795.2. Thus, the OID of the first attribute in the table, cVPN3000-Access-Hours, is 1.2.840.113556.8000.795.2.1. Likewise, the OID of the last attribute in the table, cVPN3000-WebVPN-SVC-Compression, is 1.2.840.113556.8000.795.2.115.

## Cisco -AV-Pair Attribute Syntax

The syntax of each Cisco-AV-Pair rule is as follows:

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]:

Field	Description
Prefix	A unique identifier for the AV pair. For example: <code>ip:inacl#1=</code> (used for standard ACLs) or <code>webvpn:inacl#</code> (used for WebVPN ACLs). This field only appears when the filter has been sent as an AV pair.
Action	Action to perform if rule matches: deny, permit.
Protocol	Number or name of an IP protocol. Either an integer in the range 0-255 or one of the following keywords: icmp, igmp, ip, tcp, udp.
Source	Network or host that sends the packet. It is specified as an IP address, a hostname, or the keyword “any”. If specified as an IP address, the source wildcard mask must follow.
Source Wildcard Mask	The wildcard mask applied to the source address.
Destination	Network or host that receives the packet. It is specified as an IP address, a hostname, or the keyword “any”. If specified as an IP address, the source wildcard mask must follow.
Destination Wildcard Mask	The wildcard mask applied to the destination address.
Log	Generates a FILTER log message. You must use this keyword to generate events of severity level 9.
Operator	Logic operators: greater than, less than, equal to, not equal to.
Port	The number of a TCP or UDP port in the range 0-65535.

For example:

```
ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log
```

```
webvpn:inacl#1=permit url http://www.cnn.com
webvpn:inacl#2=deny smtp any host 10.1.3.5
webvpn:inacl#3=permit url cifs://mar_server/peopleshare1
```

**Note**

- Use Cisco-AV pair entries with the ip:inacl# prefix to enforce ACLs for remote IPsec and SSL VPN Client (SVC) tunnels.
- Use Cisco-AV pair entries with the webvpn:inacl# prefix to enforce ACLs for WebVPN clientless (browser-mode) tunnels.

Table E-3 lists the tokens for the Cisco-AV-Pair attribute:

**Table E-3 Security Appliance-Supported Tokens**

Token	Syntax Field	Description
ip:inacl#Num=	N/A (Identifier)	(Where <i>Num</i> is a unique integer.) Starts all AV pair access control lists. Enforces ACLs for remote IPsec and SSL VPN (SVC) tunnels.
webvpn:inacl#Num=	N/A (Identifier)	(Where <i>Num</i> is a unique integer.) Starts all WebVPN AV pair access control lists. Enforces ACLs for WebVPN clientless (browser-mode) tunnels.
deny	Action	Denies action. (Default)
permit	Action	Allows action.
icmp	Protocol	Internet Control Message Protocol (ICMP)
1	Protocol	Internet Control Message Protocol (ICMP)
IP	Protocol	Internet Protocol (IP)
0	Protocol	Internet Protocol (IP)
TCP	Protocol	Transmission Control Protocol (TCP)
6	Protocol	Transmission Control Protocol (TCP)
UDP	Protocol	User Datagram Protocol (UDP)
17	Protocol	User Datagram Protocol (UDP)
any	Hostname	Rule applies to any host.
host	Hostname	Any alpha-numeric string that denotes a hostname.
log	Log	When the event is hit, a filter log message appears. (Same as permit and log or deny and log.)
lt	Operator	Less than value
gt	Operator	Greater than value
eq	Operator	Equal to value
neq	Operator	Not equal to value
range	Operator	Inclusive range. Should be followed by two values.

## Example Security Appliance Authorization Schema

This section provides a sample of an LDAP schema. This schema supports the security appliance class and attributes. It is specific to the Microsoft Active Directory LDAP server. Use it as a model, with [Table E-2](#), to define your own schema for your own LDAP server.

## Schema 3k\_schema.ldif

```

dn:
CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Access-Hours
attributeID: 1.2.840.113556.1.8000.795.2.1
attributeSyntax: 2.5.5.3
cn: cVPN3000-Access-Hours
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Access-Hours
distinguishedName:

CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
  CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Access-Hours
showInAdvancedViewOnly: TRUE

.....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Primary-DNS
attributeID: 1.2.840.113556.1.8000.795.2.3
attributeSyntax: 2.5.5.3
cn: cVPN3000-Primary-DNS
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Primary-DNS
distinguishedName:
  CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
  CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Primary-DNS
showInAdvancedViewOnly: TRUE

.....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation
,DC=com
changetype: add
adminDisplayName: cVPN3000-Confidence-Interval
attributeID: 1.2.840.113556.1.8000.795.2.52
attributeSyntax: 2.5.5.9
cn: cVPN3000-Confidence-Interval
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Confidence-Interval
distinguishedName:

```

```

CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation
,DC=com
objectCategory:

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

dn:
CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,
DC=com
changetype: add
adminDisplayName: cVPN3000-User-Authorization
adminDescription: Cisco Class Schema
cn: cVPN3000-User-Authorization
defaultObjectCategory:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,
DC=com
defaultSecurityDescriptor:
  D:(A;;RPWPCRCDDCLCLORCWOWSDDDTDSW;;;DA)(A;;RPWPCRCDDCLCLORCWOWSDDDTDSW;;;SY)
  (A;;RPLCLORC;;;AU)
governsID: 1.2.840.113556.1.8000.795.1.1
instanceType: 4
LDAPDisplayName: cVPN3000-User-Authorization

mustContain: cn
mayContain: cVPN3000-Access-Hours
mayContain: cVPN3000-Simultaneous-Logins
mayContain: cVPN3000-Primary-DNS
...
mayContain: cVPN3000-Confidence-Interval
mayContain: cVPN3000-Cisco-LEAP-Bypass

distinguishedName:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,
DC=com
objectCategory:
  CN=Class-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: classSchema
objectClassCategory: 1
possSuperiors: organizationalUnit
name: cVPN3000-User-Authorization
rDNAttID: cn
showInAdvancedViewOnly: TRUE
subClassOf: top
systemOnly: FALSE

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
systemOnly: FALSE

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

```

## Loading the Schema in the LDAP Server



### Note

The directions in this section are specific to the Microsoft Active Directory LDAP server. If you have a different type of server, refer to your server documentation for information on loading a schema.

To load the schema on the LDAP server, enter the following command from the directory where the schema file resides: `ldifde -i -f Schema Name`. For example: `ldifde -i -f 3k_schema.ldif`

## Defining User Permissions



### Note

The directions in this section are specific to the Microsoft Active Directory LDAP server. If you have a different type of server, see your server documentation to define and load user attributes.

For each user authorizing to your LDAP server, define a user file. A user file defines all the security appliance attributes and values associated with a particular user. Each user is an object of the class `cVPN3000-User-Authorization`. To define the user file, use any text editor. The file must have the extension `.ldif`. (For an example user file, see [Robin.ldif](#).)

To load the user file on the LDAP server, enter the following command on the directory where your version of the `ldap_user.ldif` file resides: `ldifde -i -f ldap_user.ldif`. For example: `ldifde -i -f Robin.ldif`

After you have created and loaded both the schema and the user file, your LDAP server is ready to process security appliance authorization requests.

## Example User File

This section provides a sample user file for the user Robin.

### Robin.ldif

```
dn: cn=Robin,OU=People,DC=ExampleCorporation,DC=com
changetype: add
cn: Robin
CVPN3000-Access-Hours: Corporate_time
cVPN3000-Simultaneous-Logins: 2
cVPN3000-IPSec-Over-UDP: TRUE
CVPN3000-IPSec-Over-UDP-Port: 12125
cVPN3000-IPSec-Banner1: Welcome to the Example Corporation!!!
cVPN3000-IPSec-Banner2: Unauthorized access is prohibited!!!!
cVPN3000-Primary-DNS: 10.10.4.5
CVPN3000-Secondary-DNS: 10.11.12.7
CVPN3000-Primary-WINS: 10.20.1.44
CVPN3000-SEP-Card-Assignment: 1
CVPN3000-IPSec-Tunnel-Type: 2
CVPN3000-Tunneling-Protocols: 7
cVPN3000-Confidence-Interval: 300
cVPN3000-IPSec-Allow-Passwd-Store: TRUE
objectClass: cVPN3000-User-Authorization
```



```
hostname(config-aaa-server-host) # ldap-naming-attribute cn
hostname(config-aaa-server-host) # ldap-login-password anypassword
hostname(config-aaa-server-host) # ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host) # ldap-attribute-map LdapSvrName
hostname(config-aaa-server-host) #
```

**Step 4** Create a tunnel group that specifies SDI Authentication and LDAP authorization, as shown in the following example commands:

```
hostname(config) # tunnel-group ipsec-tunnelgroup type ipsec-ra
hostname(config) # tunnel-group ipsec-tunnelgroup general-attributes
hostname(config) # authentication-server-group sdi-group
hostname(config) # authorization-server-group ldap-authorize-group
hostname(config) #
```



**Note**

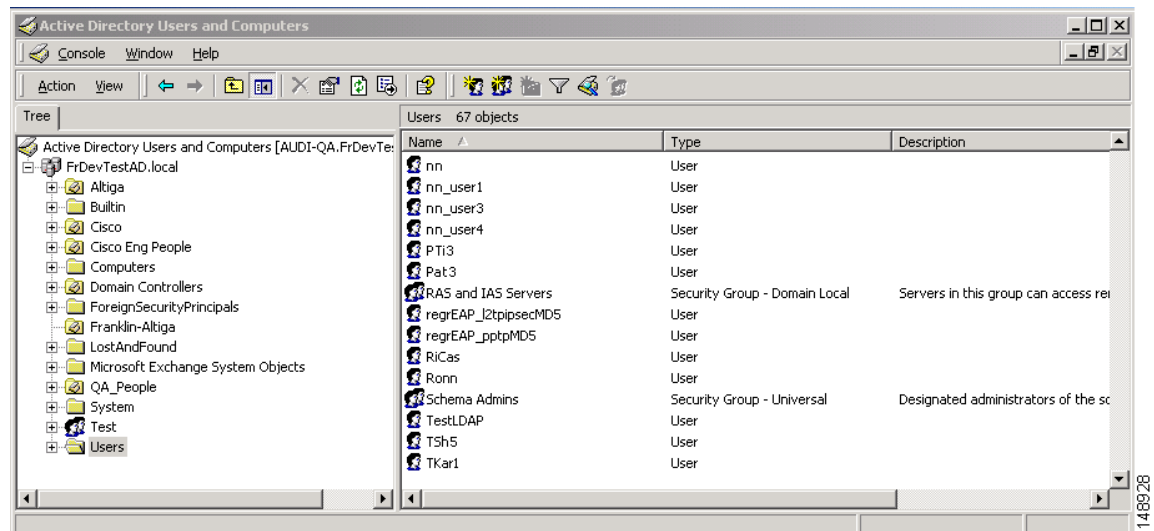
This example does not show the configuration for sdi-group.

## Example 2: Configuring LDAP Authentication with Microsoft Active Directory

This example presents a configuration procedure for LDAP authentication with Microsoft Active Directory. To secure the user credentials during transmission, this procedure configures the security appliance to exchange messages with the LDAP directory over a SSL connection. It also configures the security appliance to interpret the department attribute in the Microsoft AD user record as the group policy to which the user is assigned. The authorization attributes for this group are retrieved from a RADIUS server.

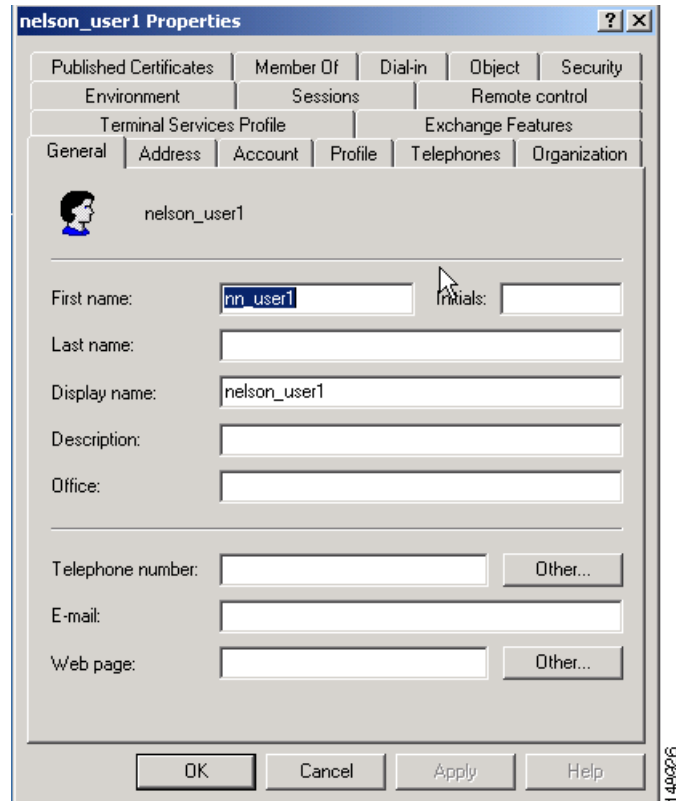
View the user records by clicking the User folder in the Active Directory Users and Computers window as shown in [Figure E-3](#).

**Figure E-3** Active Directory Users and Computers Window Showing User Folder



Review specific user attributes and values by right-clicking the username and clicking Properties. The Username Properties dialog box appears as shown in Figure E-4.

**Figure E-4** The Username Properties Dialog Box



**Note** The department attribute is configured under the Organization tab in the Active Directory Users and Computers window.

To configure this example, perform the following steps on the security appliance:

**Step 1** Create a aaa-server record for the LDAP authentication server and use the ldap-base-dn to specify the search location for the Active Directory user records as shown in the following example commands:

```
hostname(config)# aaa-server ldap-authenticate-grp protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap-authenticate-grp host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn cn=Users,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host)#
```

**Step 2** Create an LDAP mapping table entry to map the AD attribute department to the Cisco attribute cVPN3000-IETF-Radius-Class as shown in the following example commands:

```
hostname(config)# ldap attribute-map ActiveDirectoryMapTable
```

```
hostname(config-ldap-attribute-map) # map-name department cVPN3000-IETF-Radius-Class
hostname(config-ldap-attribute-map) #
```

**Step 3** Configure the name of the LDAP attribute map as shown in the following example command:

```
hostname(config-aaa-server-host) # ldap-attribute-map ActiveDirectoryMapTable
hostname(config-aaa-server-host) #
```

**Step 4** Specify a secure LDAP connection as follows:

```
hostname(config-aaa-server-host) # ldap-over-ssl enable
hostname(config-aaa-server-host) #
```

**Step 5** Create an external group policy that associates the group-name with the RADIUS server. In this example, the user is assigned to the group Engineering as shown in the following example command:

```
hostname(config-aaa-server-host) # group-policy Engineering external server-group
radius-group password anypassword
hostname(config-aaa-server-host) #
```

**Step 6** Create a tunnel group that specifies LDAP authentication as shown in the following example commands:

```
hostname(config) # tunnel-group ipsec-tunnelgroup type ipsec-ra
hostname(config) # tunnel-group ipsec-tunnelgroup general-attributes
hostname(config-tunnel-general) # authentication-server-group ldap-authenticate-grp
hostname(config-tunnel-general) #
```



**Note**

---

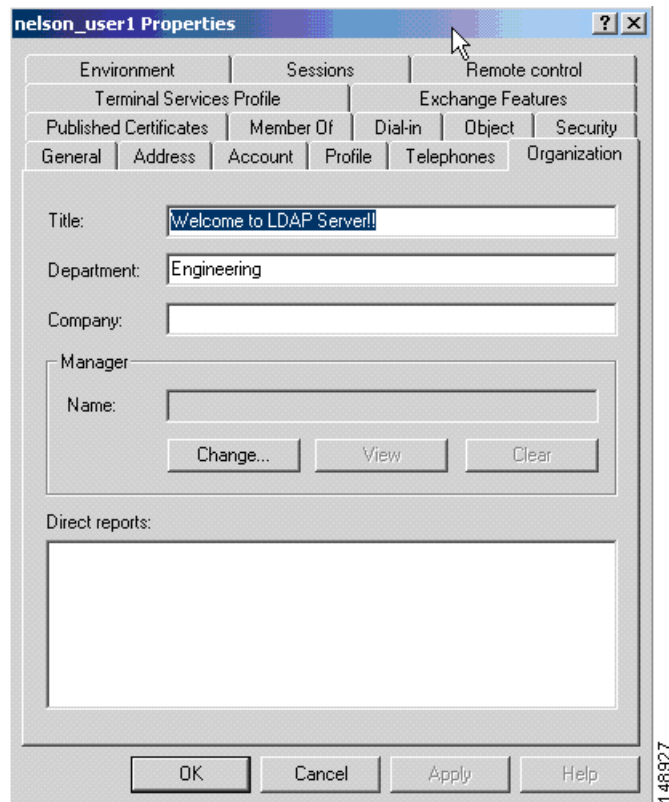
The configuration for radius-group is not shown in this example.

---

### Example 3: LDAP Authentication and LDAP Authorization with Microsoft Active Directory

This example presents the procedure for configuring both authentication and authorization using LDAP and Microsoft Active Directory. In the Microsoft user record, the department attribute is interpreted as the group-name for the user. The authorization attributes for this group-name are retrieved from the Active Directory server.

The department attribute is configured under the Organization tab in the Active Directory Users and Computers dialog box as shown in [Figure E-5](#).

**Figure E-5** The Organization Tab of the Active Directory Users and Computer Dialog

To configure this example, perform the following steps on the security appliance:

- Step 1** Create an LDAP mapping table entry to map the Active Directory attribute department to the Cisco attribute cVPN3000-IETF-Radius-Class as shown in the following example commands:
- ```
hostname(config)# ldap attribute-map ActiveDirectoryMapTable
hostname(config-ldap-attribute-map)# map-name department cVPN3000-IETF-Radius-Class
```
- Step 2** Create a aaa-server record for the LDAP authentication server and use the ldap-base-dn to specify the search location for the Active Directory user records as shown in the following example commands:
- ```
hostname(config)# aaa-server ldap-authenticate protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap-authenticate host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn cn=Users,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host)#
```
- Step 3** Configure the name of the LDAP attribute map as shown in the following example command:
- ```
hostname(config-aaa-server-host)# ldap-attribute-map ActiveDirectoryMapTable
hostname(config-aaa-server-host)#
```

**Step 4** Specify a secure LDAP connection as follows:

```
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

**Step 5** Create an aaa-server record to configure the LDAP authorization server and use the ldap-base-dn to specify the search location for the Cisco cVPN3000-User-Authorization records as shown in the following example commands:

```
hostname(config-aaa-server-host)# aaa-server ldap-authorize protocol ldap
hostname(config-aaa-server-host)# aaa-server ldap-authorize host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn ou=Franklin-Altiga,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host)#
```

**Step 6** Create an external group policy that associates the group-name with the LDAP authorization server. In this example, the user is assigned to the group Engineering as shown in the following command:

```
hostname(config-aaa-server-host)# group-policy engineering external server-group
ldap-authorize
hostname(config-aaa-server-host)#
```

**Step 7** Create a tunnel group that specifies LDAP authentication as shown in the following example commands:

```
hostname(config)# tunnel-group ipsec-tunnelgroup type ipsec-ra
hostname(config)# tunnel-group ipsec-tunnelgroup general-attributes
hostname(config-tunnel-general)# authentication-server-group ldap-authenticate
hostname(config-tunnel-general)#
```

## Configuring an External RADIUS Server

This section presents an overview of the RADIUS configuration procedure and defines the Cisco RADIUS and TACACS+ attributes. It includes the following topics:

- [Reviewing the RADIUS Configuration Procedure](#)
- [Security Appliance RADIUS Authorization Attributes](#)
- [Security Appliance TACACS+ Attributes](#)

### Reviewing the RADIUS Configuration Procedure

This section describes the RADIUS configuration steps required to support authentication and authorization of the security appliance users. Follow the steps below to set up the RADIUS server to interoperate with the security appliance.

**Step 1** Load the security appliance attributes into the RADIUS server. The method you use to load the attributes depends on which type of RADIUS server you are using:

- If you are using Cisco ACS: the server already has these attributes integrated. You can skip this step.

- If you are using a FUNK RADIUS server: Cisco supplies a dictionary file that contains all the security appliance attributes. Obtain this dictionary file, `cisco3k.dct`, from Software Center on CCO or from the security appliance CD-ROM. Load the dictionary file on your server.
- For other vendors' RADIUS servers (for example, Microsoft Internet Authentication Service): you must manually define each security appliance attribute. To define an attribute, use the attribute name or number, type, value, and vendor code (3076). For a list of security appliance RADIUS authorization attributes and values, see [Table E-4](#).

**Step 2** Set up the users or groups with the permissions and attributes to send during IPSec/WebVPN tunnel establishment. The permissions or attributes might include access hours, primary DNS, banner, and so forth.

## Security Appliance RADIUS Authorization Attributes



### Note

Authorization refers to the process of enforcing permissions or attributes. A RADIUS server defined as an authentication server enforces permissions or attributes if they are configured.

[Table E-4](#) lists all the possible security appliance supported attributes that can be used for user authorization.

**Table E-4** Security Appliance Supported RADIUS Attributes and Values

| Attribute Name        | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                                      |
|-----------------------|----------|-----|-----|---------|-------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Access-Hours          | Y        | Y   | Y   | 1       | String      | Single                 | Name of the time range, for example, Business-hours                                                                                       |
| Simultaneous-Logins   | Y        | Y   | Y   | 2       | Integer     | Single                 | An integer 0 to 2147483647                                                                                                                |
| Primary-DNS           | Y        | Y   | Y   | 5       | String      | Single                 | An IP address                                                                                                                             |
| Secondary-DNS         | Y        | Y   | Y   | 6       | String      | Single                 | An IP address                                                                                                                             |
| Primary-WINS          | Y        | Y   | Y   | 7       | String      | Single                 | An IP address                                                                                                                             |
| Secondary-WINS        | Y        | Y   | Y   | 8       | String      | Single                 | An IP address                                                                                                                             |
| SEP-Card-Assignment   |          |     |     | 9       | Integer     | Single                 | Not used                                                                                                                                  |
| Tunneling-Protocols   | Y        | Y   | Y   | 11      | Integer     | Single                 | 1 = PPTP<br>2 = L2TP<br>4 = IPSec<br>8 = L2TP/IPSec<br>16 = WebVPN<br>4 and 8 are mutually exclusive;<br>0-11 and 16-27 are legal values. |
| IPSec-Sec-Association | Y        |     |     | 12      | String      | Single                 | Name of the security association                                                                                                          |

Table E-4 Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name           | VPN 3000 | ASA | PIX | Attr. # | Syntax/ Type | Single or Multi-Valued | Description or Value                                                                                                                                           |
|--------------------------|----------|-----|-----|---------|--------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPSec-Authentication     | Y        |     |     | 13      | Integer      | Single                 | 0 = None<br>1 = RADIUS<br>2 = LDAP (authorization only)<br>3 = NT Domain<br>4 = SDI<br>5 = Internal<br>6 = RADIUS with Expiry<br>7 = Kerberos/Active Directory |
| Banner1                  | Y        | Y   | Y   | 15      | String       | Single                 | Banner string                                                                                                                                                  |
| IPSec-Allow-Passwd-Store | Y        | Y   | Y   | 16      | Boolean      | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                    |
| Use-Client-Address       | Y        |     |     | 17      | Boolean      | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                    |
| PPTP-Encryption          | Y        |     |     | 20      | Integer      | Single                 | Bitmap:<br>1 = Encryption required<br>2 = 40 bits<br>4 = 128 bits<br>8 = Stateless-Required<br>15 =<br>40/128-Encr/Stateless-Req                               |
| L2TP-Encryption          | Y        |     |     | 21      | Integer      | Single                 | Bitmap:<br>1 = Encryption required<br>2 = 40 bit<br>4 = 128 bits<br>8 = Stateless-Req<br>15 =<br>40/128-Encr/Stateless-Req                                     |
| IPSec-Split-Tunnel-List  | Y        | Y   | Y   | 27      | String       | Single                 | Specifies the name of the network/access list that describes the split tunnel inclusion list                                                                   |
| IPSec-Default-Domain     | Y        | Y   | Y   | 28      | String       | Single                 | Specifies the single default domain name to send to the client (1-255 characters)                                                                              |

Table E-4 Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name          | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                  |
|-------------------------|----------|-----|-----|---------|-------------|------------------------|---------------------------------------------------------------------------------------|
| IPSec-Split-DNS-Names   | Y        | Y   | Y   | 29      | String      | Single                 | Specifies the list of secondary domain names to send to the client (1-255 characters) |
| IPSec-Tunnel-Type       | Y        | Y   | Y   | 30      | Integer     | Single                 | 1 = LAN-to-LAN<br>2 = Remote access                                                   |
| IPSec-Mode-Config       | Y        | Y   | Y   | 31      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| IPSec-User-Group-Lock   | Y        |     |     | 33      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| IPSec-Over-UDP          | Y        | Y   | Y   | 34      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| IPSec-Over-UDP-Port     | Y        | Y   | Y   | 35      | Integer     | Single                 | 4001 - 49151, default = 10000                                                         |
| Banner2                 | Y        | Y   | Y   | 36      | String      | Single                 | A banner string. Banner2 string is concatenated to Banner1 string if configured.      |
| PPTP-MPPC-Compression   | Y        |     |     | 37      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| L2TP-MPPC-Compression   | Y        |     |     | 38      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| IPSec-IP-Compression    | Y        | Y   | Y   | 39      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| IPSec-IKE-Peer-ID-Check | Y        | Y   | Y   | 40      | Integer     | Single                 | 1 = Required<br>2 = If supported by peer certificate<br>3 = Do not check              |
| IKE-Keep-Alives         | Y        | Y   | Y   | 41      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |
| IPSec-Auth-On-Rekey     | Y        | Y   | Y   | 42      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                           |

Table E-4 Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                        | VPN 3000 | ASA | PIX | Attr. # | Syntax/ Type | Single or Multi-Valued | Description or Value                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|----------|-----|-----|---------|--------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Required-Client-Firewall-Vendor-Code  | Y        | Y   | Y   | 45      | Integer      | Single                 | 1 = Cisco Systems (with Cisco Integrated Client)<br>2 = Zone Labs<br>3 = NetworkICE<br>4 = Sygate<br>5 = Cisco Systems (with Cisco Intrusion Prevention Security Agent)                                                                                                                                                                                  |
| Required-Client-Firewall-Product-Code | Y        | Y   | Y   | 46      | Integer      | Single                 | Cisco Systems Products:<br>1 = Cisco Intrusion Prevention Security Agent or Cisco Integrated Client (CIC)<br>Zone Labs Products:<br>1 = Zone Alarm<br>2 = Zone AlarmPro<br>3 = Zone Labs Integrity<br>NetworkICE Product:<br>1 = BlackIce Defender/Agent<br>Sygate Products:<br>1 = Personal Firewall<br>2 = Personal Firewall Pro<br>3 = Security Agent |
| Required-Client-Firewall-Description  | Y        | Y   | Y   | 47      | String       | Single                 | String                                                                                                                                                                                                                                                                                                                                                   |
| Require-HW-Client-Auth                | Y        | Y   | Y   | 48      | Boolean      | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                                                                                              |
| Required-Individual-User-Auth         | Y        | Y   | Y   | 49      | Integer      | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                                                                                              |
| Authenticated-User-Idle-Timeout       | Y        | Y   | Y   | 50      | Integer      | Single                 | 1-35791394 minutes                                                                                                                                                                                                                                                                                                                                       |
| Cisco-IP-Phone-Bypass                 | Y        | Y   | Y   | 51      | Integer      | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                                                                                              |
| IPSec-Split-Tunneling-Policy          | Y        | Y   | Y   | 55      | Integer      | Single                 | 0 = No split tunneling<br>1 = Split tunneling<br>2 = Local LAN permitted                                                                                                                                                                                                                                                                                 |

Table E-4 Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                            | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                               |
|-------------------------------------------|----------|-----|-----|---------|-------------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| IPSec-Required-Client-Firewall-Capability | Y        | Y   | Y   | 56      | Integer     | Single                 | 0 = None<br>1 = Policy defined by remote FW Are-You-There (AYT)<br>2 = Policy pushed CPP<br>4 = Policy from server |
| IPSec-Client-Firewall-Filter-Name         | Y        |     |     | 57      | String      | Single                 | Specifies the name of the filter to be pushed to the client as firewall policy                                     |
| IPSec-Client-Firewall-Filter-Optional     | Y        | Y   | Y   | 58      | Integer     | Single                 | 0 = Required<br>1 = Optional                                                                                       |
| IPSec-Backup-Servers                      | Y        | Y   | Y   | 59      | String      | Single                 | 1 = Use Client-Configured list<br>2 = Disable and clear client list<br>3 = Use Backup Server list                  |
| IPSec-Backup-Server-List                  | Y        | Y   | Y   | 60      | String      | Single                 | Server Addresses (space delimited)                                                                                 |
| DHCP-Network-Scope                        | Y        | Y   | Y   | 61      | String      | Single                 | IP Address                                                                                                         |
| Intercept-DHCP-Configure-Msg              | Y        | Y   | Y   | 62      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                        |
| MS-Client-Subnet-Mask                     | Y        | Y   | Y   | 63      | Boolean     | Single                 | An IP address                                                                                                      |
| Allow-Network-Extension-Mode              | Y        | Y   | Y   | 64      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                        |
| Authorization-Type                        | Y        | Y   | Y   | 65      | Integer     | Single                 | 0 = None<br>1 = RADIUS<br>2 = LDAP                                                                                 |
| Authorization-Required                    | Y        |     |     | 66      | Integer     | Single                 | 0 = No<br>1 = Yes                                                                                                  |
| Authorization-DN-Field                    | Y        | Y   | Y   | 67      | String      | Single                 | Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name                    |
| IKE-KeepAlive-Confidence-Interval         | Y        | Y   | Y   | 68      | Integer     | Single                 | 10-300 seconds                                                                                                     |
| WebVPN-Content-Filter-Parameters          | Y        | Y   |     | 69      | Integer     | Single                 | 1 = Java ActiveX<br>2 = Java Script<br>4 = Image<br>8 = Cookies in images                                          |

Table E-4 Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                 | VPN 3000 | ASA | PIX | Attr. # | Syntax/ Type | Single or Multi-Valued | Description or Value                                                                                                                  |
|--------------------------------|----------|-----|-----|---------|--------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| WebVPN-URL-List                |          | Y   |     | 71      | String       | Single                 | URL-List name                                                                                                                         |
| WebVPN-Port-Forward-List       |          | Y   |     | 72      | String       | Single                 | Port-Forward list name                                                                                                                |
| WebVPN-Access-List             |          | Y   |     | 73      | String       | Single                 | Access-List name                                                                                                                      |
| Cisco-LEAP-Bypass              | Y        | Y   | Y   | 75      | Integer      | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                           |
| WebVPN-Homepage                | Y        | Y   |     | 76      | String       | Single                 | A URL such as<br>http://example-portal.com                                                                                            |
| Client-Type-Version-Limiting   | Y        | Y   | Y   | 77      | String       | Single                 | IPsec VPN version number string                                                                                                       |
| WebVPN-Port-Forwarding-Name    | Y        | Y   |     | 79      | String       | Single                 | String name (example, "Corporate-Apps").<br><br>This text replaces the default string, "Application Access," on the WebVPN home page. |
| IE-Proxy-Server                | Y        |     |     | 80      | String       | Single                 | IP address                                                                                                                            |
| IE-Proxy-Server-Policy         | Y        |     |     | 81      | Integer      | Single                 | 1 = No Modify<br>2 = No Proxy<br>3 = Auto detect<br>4 = Use Concentrator Setting                                                      |
| IE-Proxy-Exception-List        | Y        |     |     | 82      | String       | Single                 | newline (\n) separated list of DNS domains                                                                                            |
| IE-Proxy-Bypass-Local          | Y        |     |     | 83      | Integer      | Single                 | 0 = None<br>1 = Local                                                                                                                 |
| IKE-Keepalive-Retry-Interval   | Y        | Y   | Y   | 84      | Integer      | Single                 | 2 - 10 seconds                                                                                                                        |
| Tunnel-Group-Lock              |          | Y   | Y   | 85      | String       | Single                 | Name of the tunnel group or "none"                                                                                                    |
| Access-List-Inbound            |          | Y   | Y   | 86      | String       | Single                 | Access list ID                                                                                                                        |
| Access-List-Outbound           |          | Y   | Y   | 87      | String       | Single                 | Access list ID                                                                                                                        |
| Perfect-Forward-Secrecy-Enable | Y        | Y   | Y   | 88      | Boolean      | Single                 | 0 = No<br>1 = Yes                                                                                                                     |
| NAC-Enable                     | Y        |     |     | 89      | Integer      |                        | 0 = No<br>1 = Yes                                                                                                                     |
| NAC-Status-Query-Timer         | Y        |     |     | 90      | Integer      |                        | 30 - 1800 seconds                                                                                                                     |
| NAC-Revalidation-Timer         | Y        |     |     | 91      | Integer      |                        | 300 - 86400 seconds                                                                                                                   |
| NAC-Default-ACL                | Y        |     |     | 92      | String       |                        | Access list                                                                                                                           |

**Table E-4** Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                          | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value        |
|-----------------------------------------|----------|-----|-----|---------|-------------|------------------------|-----------------------------|
| WebVPN-URL-Entry-Enable                 | Y        | Y   |     | 93      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-File-Access-Enable               | Y        | Y   |     | 94      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-File-Server-Entry-Enable         | Y        | Y   |     | 95      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-File-Server-Browsing-Enable      | Y        | Y   |     | 96      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Port-Forwarding-Enable           | Y        | Y   |     | 97      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Outlook-Exchange-Proxy-Enable    | Y        | Y   |     | 98      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Port-Forwarding-HTTP-Proxy       | Y        | Y   |     | 99      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Auto-Applet-Download-Enable      | Y        | Y   |     | 100     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Citrix-Metaframe-Enable          | Y        | Y   |     | 101     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Apply-ACL                        | Y        | Y   |     | 102     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-SSL-VPN-Client-Enable            | Y        | Y   |     | 103     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-SSL-VPN-Client-Required          | Y        | Y   |     | 104     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-SSL-VPN-Client-Keep-Installation | Y        | Y   |     | 105     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| Strip-Realm                             | Y        | Y   | Y   | 135     | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled |

**Note**

RADIUS attribute names do not contain the cVPN3000 prefix to better reflect support for all three security appliances (VPN 3000, PIX, and the ASA). Cisco Secure ACS 4.x supports this new nomenclature, but attribute names in pre-4.0 ACS releases still include the cVPN3000 prefix. The appliances enforce the RADIUS attributes based on attribute numeric ID, not attribute name. LDAP attributes are enforced by their name, not by the ID.

## Security Appliance TACACS+ Attributes

The security appliance provides support for TACACS+ attributes. TACACS+ separates the functions of authentication, authorization, and accounting. The protocol supports two types of attributes: mandatory and optional. Both the server and client must understand a mandatory attribute, and the mandatory attribute must be applied to the user. An optional attribute may or may not be understood or used.


**Note**

To use TACACS+ attributes, make sure you have enabled AAA services on the NAS.

[Table E-5](#) lists supported TACACS+ authorization response attributes for cut-through-proxy connections. [Table E-6](#) lists supported TACACS+ accounting attributes.

**Table E-5 Supported TACACS+ Authorization Response Attributes**

| Attribute | Description                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| acl       | Identifies a locally configured access list to be applied to the connection.                                                                        |
| idletime  | Indicates the amount of inactivity in minutes that is allowed before the authenticated user session is terminated.                                  |
| timeout   | Specifies the absolute amount of time in minutes that authentication credentials remain active before the authenticated user session is terminated. |

**Table E-6 Supported TACACS+ Accounting Attributes**

| Attribute    | Description                                                                                                                                                            |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bytes_in     | Specifies the number of input bytes transferred during this connection (stop records only).                                                                            |
| bytes_out    | Specifies the number of output bytes transferred during this connection (stop records only).                                                                           |
| cmd          | Defines the command executed (command accounting only).                                                                                                                |
| disc-cause   | Indicates the numeric code that identifies the reason for disconnecting (stop records only).                                                                           |
| elapsed_time | Defines the elapsed time in seconds for the connection (stop records only).                                                                                            |
| foreign_ip   | Specifies the IP address of the client for tunnel connections. Defines the address on the lowest security interface for cut-through-proxy connections.                 |
| local_ip     | Specifies the IP address that the client connected to for tunnel connections. Defines the address on the highest security interface for cut-through-proxy connections. |
| NAS port     | Contains a session ID for the connection.                                                                                                                              |
| packs_in     | Specifies the number of input packets transferred during this connection.                                                                                              |
| packs_out    | Specifies the number of output packets transferred during this connection.                                                                                             |
| priv-level   | Set to the user's privilege level for command accounting requests or to 1 otherwise.                                                                                   |
| rem_addr     | Indicates the IP address of the client.                                                                                                                                |
| service      | Specifies the service used. Always set to "shell" for command accounting only.                                                                                         |
| task_id      | Specifies a unique task ID for the accounting transaction.                                                                                                             |
| username     | Indicates the name of the user.                                                                                                                                        |