Configure an External AAA Server for VPN

About External AAA Servers

This ASA can be configured to use an external LDAP, RADIUS, or TACACS+ server to support Authentication, Authorization, and Accounting (AAA) for the ASA. The external AAA server enforces configured permissions and attributes. Before you configure the ASA to use an external server, you must configure the external AAA server with the correct ASA authorization attributes and, from a subset of these attributes, assign specific permissions to individual users.

Understanding Policy Enforcement of Authorization Attributes

The ASA supports several methods of applying user authorization attributes (also called user entitlements or permissions) to VPN connections. You can configure the ASA to obtain user attributes from any combination of:

- a Dynamic Access Policy (DAP) on the ASA
- an external RADIUS or LDAP authentication and/or authorization server
- a group policy on the ASA

If the ASA receives attributes from all sources, the attributes are evaluated, merged, and applied to the user policy. If there are conflicts between attributes, the DAP attributes take precedence.

The ASA applies attributes in the following order:

1. DAP attributes on the ASA—Introduced in Version 8.0(2), these attributes take precedence over all others. If you set a bookmark or URL list in DAP, it overrides a bookmark or URL list set in the group policy.
2. User attributes on the AAA server—The server returns these attributes after successful user authentication and/or authorization. Do not confuse these with attributes that are set for individual users in the local AAA database on the ASA (User Accounts in ASDM).

3. Group policy configured on the ASA—If a RADIUS server returns the value of the RADIUS CLASS attribute IETF-Class-25 (OU=*group-policy*) for the user, the ASA places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.

   For LDAP servers, any attribute name can be used to set the group policy for the session. The LDAP attribute map that you configure on the ASA maps the LDAP attribute to the Cisco attribute IETF-Radius-Class.

4. Group policy assigned by the Connection Profile (called tunnel-group in the CLI)—The Connection Profile has the preliminary settings for the connection, and includes a default group policy applied to the user before authentication. All users connecting to the ASA initially belong to this group, which provides any attributes that are missing from the DAP, user attributes returned by the server, or the group policy assigned to the user.

5. Default group policy assigned by the ASA (DfltGrpPolicy)—System default attributes provide any values that are missing from the DAP, user attributes, group policy, or connection profile.

Guidelines For Using External AAA Servers

The ASA enforces the LDAP attributes based on attribute name, not numeric ID. RADIUS attributes, are enforced by numeric ID, not by name.

For ASDM Version 7.0, LDAP attributes include the cVPN3000 prefix. For ASDM Versions 7.1 and later, this prefix was removed.

LDAP attributes are a subset of the Radius attributes, which are listed in the Radius chapter.

Configure Multiple Certificate Authentication

You can now validate multiple certificates per session with the AnyConnect Client SSL and IKEv2 client protocols. For example, you can make sure that the issuer name of the machine certificate matches a particular CA and therefore that the device is a corporate-issued device.

The multiple certificates option allows certificate authentication of both the machine and user via certificates. Without this option, you could only do certificate authentication of one or the other, but not both.

Note Because multiple certificate authentication requires a machine certificate and a user certificate (or two user certificates), you cannot use AnyConnect Client start before logon (SBL) with this feature.

The pre-fill username field allows a field from the second (user) certificate to be parsed and used for subsequent AAA authentication in a AAA and certificate authenticated connection. The username for both primary and secondary prefill is always retrieved from the second (user) certificate received from the client.

Beginning with 9.14(1), ASA allows you to specify which certificate the primary and secondary username should come from when configuring multiple certificate authentication and using the pre-fill username option for Authentication or Authorization. For information, see Configure Multiple Certificate Username, on page 3

With multiple certificate authentication, two certificates are authenticated: the second (user) certificate received from the client is the one that the pre-fill and username-from-certificate primary and secondary usernames are parsed from.

You can also configure multiple certificate authentication with SAML.

The existing authentication webvpn attributes is modified to include an option for multiple-certificate authentication:

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml]
 | saml [certificate | multiple-certificate]}
```

With multiple-certificate authentication, you can make policy decisions based on the fields of a certificate used to authenticate that connection attempt. The user and machine certificate received from the client during multiple-certificate authentication is loaded into DAP to allow policies to be configured based on the field of the certificate. To add multiple certificate authentication using Dynamic Access Policies (DAP) so that you can set up rules to allow or disallow connection attempts, refer to *Add Multiple Certificate Authentication to DAP* in the appropriate release of the ASA VPN ASDM Configuration Guide.

Configure Multiple Certificate Username

A new command was introduced in ASA 9.14(1) to configure the certificate that ASA must use as the primary and secondary username for authentication or authorization. You can specify whether to use the machine certificate sent in SSL or IKE (first certificate) or the user certificate from client (second certificate) to get the authentication and authorization parameters. This option is available and can be configured for any tunnel groups irrespective of the authentication type (**aaa**, **certificate**, or **multiple-certificate**). However, the configuration takes effect only for Multiple Certificate Authentication (**multiple-certificate** or **aaa multiple-certificate**). When the option is not used for Multiple Certificate Authentication, the second certificate is used by default for authentication or authorization.

Procedure

Step 1 Specify whether to use the primary username from the first or second certificate:

username-from-certificate-choice {first-certificate | second-certificate}

Step 2 Specify whether to use the secondary username from the first or second certificate:

secondary-username-from-certificate-choice {first-certificate | second-certificate}

Example:

```
tunnel-group tg1 webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tg1 type remote-access
tunnel-group tg1 general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

Configure LDAP Authorization for VPN

After LDAP authentication for VPN access has succeeded, the ASA queries the LDAP server, which returns LDAP attributes. These attributes generally include authorization data that applies to the VPN session.

You may require authorization from an LDAP directory server that is separate and distinct from the authentication mechanism. For example, if you use an SDI or certificate server for authentication, no authorization information is passed back. For user authorizations in this case, you can query an LDAP directory after successful authentication, accomplishing authentication and authorization in two steps.

To set up VPN user authorization using LDAP, perform the following steps.

Procedure

Step 1 Create a AAA server group.

aaa-server *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}

Example:

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

Step 2 Create an IPsec remote access tunnel group named remotegrp.

tunnel-group *groupname*

Example:

```
hostname(config)# tunnel-group remotegrp
```

Step 3 Associate the server group and the tunnel group.

tunnel-group *groupname* **general-attributes**

Example:

```
hostname(config)# tunnel-group remotegrp general-attributes
```

Step 4 Assigns a new tunnel group to a previously created AAA server group for authorization.

authorization-server-group *group-tag*

Example:

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

Example

The following example shows commands for enabling user authorization with LDAP. The example then creates an IPsec remote access tunnel group named RAVPN and assigns that new tunnel group to the previously created LDAP AAA server group for authorization:

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

After you complete this configuration work, you can then configure additional LDAP authorization parameters such as a directory password, a starting point for searching a directory, and the scope of a directory search by entering the following commands:

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

Define the ASA LDAP Configuration

This section describes how to define the LDAP AV-pair attribute syntax and includes the following information:

- Supported Cisco Attributes for LDAP Authorization, on page 5
- Cisco AV Pair Attribute Syntax, on page 16
- Cisco AV Pairs ACL Examples, on page 16

Note The ASA enforces 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 enforces permissions or attributes if they are configured.

For ASA Version 7.0, LDAP attributes include the cVPN3000 prefix. For software Versions 7.1 and later, this prefix was removed.

Supported Cisco Attributes for LDAP Authorization

This section provides a complete list of attributes (see) for the ASA 5500, VPN 3000 concentrator, and PIX 500 series ASAs. The table includes attribute support information for the VPN 3000 concentrator and PIX 500 series ASAs to assist you in configuring networks with a combination of these devices.

Table 1: ASA Supported Cisco Attributes for LDAP Authorization

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
Access-Hours	Y	Y	Y	String	Single	Name of the time-range (for example, Business-Hours)
Allow-Network-Extension-Mode	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	Y	Y	Y	Integer	Single	1 - 35791394 minutes
Authorization-Required	Y			Integer	Single	0 = No 1 = Yes
Authorization-Type	Y			Integer	Single	0 = None 1 = RADIUS 2 = LDAP
Banner1	Y	Y	Y	String	Single	Banner string for clientless and client SSL VPN, and IPsec clients.
Banner2	Y	Y	Y	String	Single	Banner string for clientless and client SSL VPN, and IPsec clients.
Cisco-AV-Pair	Y	Y	Y	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 the “Cisco AV Pair Attribute Syntax” section.”
Cisco-IP-Phone-Bypass	Y	Y	Y	Integer	Single	0 = Disabled 1 = Enabled
Cisco-LEAP-Bypass	Y	Y	Y	Integer	Single	0 = Disabled 1 = Enabled
Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
Client-Type-Version-Limiting	Y	Y	Y	String	Single	IPsec VPN client version number string
Confidence-Interval	Y	Y	Y	Integer	Single	10 - 300 seconds
DHCP-Network-Scope	Y	Y	Y	String	Single	IP address

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
DN-Field	Y	Y	Y	String	Single	Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, and use-entire-name.
Firewall-ACL-In		Y	Y	String	Single	Access list ID
Firewall-ACL-Out		Y	Y	String	Single	Access list ID
Group-Policy		Y	Y	String	Single	Sets the group policy for the remote access VPN session. For version 8.2 and later, use this attribute instead of IETF-Radius-Class. You can use one of the three following formats: • group policy name • OU= group policy name • OU= group policy name :
IE-Proxy-Bypass-Local				Boolean	Single	0 = Disabled 1 = Enabled
IE-Proxy-Exception-List				String	Single	A list of DNS domains. Entries must be separated by the new line character sequence (\n).
IE-Proxy-Method	Y	Y	Y	Integer	Single	1 = Do not modify proxy settings 2 = Do not use proxy 3 = Auto detect 4 = Use ASA setting
IE-Proxy-Server	Y	Y	Y	Integer	Single	IP address
IETF-Radius-Class	Y	Y	Y		Single	Sets the group policy for the remote access VPN session. For version 8.2 and later, use this attribute instead of IETF-Radius-Class. You can use one of the three following formats: • group policy name • OU= group policy name • OU= group policy name :
IETF-Radius-Filter-Id	Y	Y	Y	String	Single	Access list name that is defined on the ASA. The setting applies to VPN remote access IPsec and SSL VPN clients.

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
IETF-Radius-Framed-IP-Address	Y	Y	Y	String	Single	An IP address. The setting applies to VPN remote access IPsec and SSL VPN clients.
IETF-Radius-Framed-IP-Netmask	Y	Y	Y	String	Single	An IP address mask. The setting applies to VPN remote access IPsec and SSL VPN clients.
IETF-Radius-Idle-Timeout	Y	Y	Y	Integer	Single	Seconds
IETF-Radius-Service-Type	Y	Y	Y	Integer	Single	1 = Login 2 = Framed 5 = Remote access 6 = Administrative 7 = NAS prompt
IETF-Radius-Session-Timeout	Y	Y	Y	Integer	Single	Seconds
IKE-Keep-Alives	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Allow-Passwd-Store	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Authentication	Y	Y	Y	Integer	Single	0 = None 1 = RADIUS 2 = LDAP (authorization only) 3 = NT Domain 4 = SDI (RSA) 5 = Internal 6 = RADIUS with Expiry 7 = Kerberos or Active Directory
IPsec-Auth-On-Rekey	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Backup-Server-List	Y	Y	Y	String	Single	Server addresses (space delimited)
IPsec-Backup-Servers	Y	Y	Y	String	Single	1 = Use client-configured list 2 = Disabled and clear client list 3 = Use backup server list
IPsec-Client-Firewall-Filter-Name	Y			String	Single	Specifies the name of the filter to be pushed to the client as firewall policy.

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
IPsec-Client-Firewall-Filter-Optional	Y	Y	Y	Integer	Single	0 = Required 1 = Optional
IPsec-Default-Domain	Y	Y	Y	String	Single	Specifies the single default domain name to send to the client (1 - 255 characters).
IPsec-Extended-Auth-On-Rekey		Y	Y	String	Single	String
IPsec-IKE-Peer-ID-Check	Y	Y	Y	Integer	Single	1 = Required 2 = If supported by peer certificate 3 = Do not check
IPsec-IP-Compression	Y	Y	Y	Integer	Single	0 = Disabled 1 = Enabled
IPsec-Mode-Config	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Over-UDP	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Over-UDP-Port	Y	Y	Y	Integer	Single	4001 - 49151; The default is 10000.
IPsec-Required-Client-Firewall-Capability	Y	Y	Y	Integer	Single	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = Policy from server
IPsec-Sec-Association	Y			String	Single	Name of the security association
IPsec-Split-DNS-Names	Y	Y	Y	String	Single	Specifies the list of secondary domain names to send to the client (1 - 255 characters).
IPsec-Split-Tunneling-Policy	Y	Y	Y	Integer	Single	0 = Tunnel everything 1 = Split tunneling 2 = Local LAN permitted
IPsec-Split-Tunnel-List	Y	Y	Y	String	Single	Specifies the name of the network or access list that describes the split tunnel inclusion list.
IPsec-Tunnel-Type	Y	Y	Y	Integer	Single	1 = LAN-to-LAN 2 = Remote access

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
L2TP-Encryption	Y			Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bit 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateless-Req
L2TP-MPPC-Compression	Y			Integer	Single	0 = Disabled 1 = Enabled
MS-Client-Subnet-Mask	Y	Y	Y	String	Single	An IP address
PFS-Required	Y	Y	Y	Boolean	Single	0 = No 1 = Yes
Port-Forwarding-Name	Y	Y		String	Single	Name string (for example, “Corporate-Apps”)
PPTP-Encryption	Y			Intger	Single	Bitmap: 1 = Encryption required 2 = 40 bit 4 = 128 bits 8 = Stateless-Req Example: 15 = 40/128-Encr/Stateless-Req
PPTP-MPPC-Compression	Y			Integer	Single	0 = Disabled 1 = Enabled
Primary-DNS	Y	Y	Y	String	Single	An IP address
Primary-WINS	Y	Y	Y	String	Single	An IP address
Privilege-Level				Integer	Single	For usernames, 0 - 15
Required-Client-Firewall-Vendor-Code	Y	Y	Y	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)

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
Required-Client-Firewall-Description	Y	Y	Y	String	Single	—
Required-Client-Firewall-Product-Code	Y	Y	Y	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
Require-HW-Client-Auth	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
Require-Individual-User-Auth	Y	Y	Y	Integer	Single	0 = Disabled 1 = Enabled
Secondary-DNS	Y	Y	Y	String	Single	An IP address
Secondary-WINS	Y	Y	Y	String	Single	An IP address
SEP-Card-Assignment				Integer	Single	Not used
Simultaneous-Logins	Y	Y	Y	Integer	Single	0 - 2147483647
Strip-Realm	Y	Y	Y	Boolean	Single	0 = Disabled 1 = Enabled
TACACS-Authtype	Y	Y	Y	Integer	Single	—
TACACS-Privilege-Level	Y	Y	Y	Integer	Single	—
Tunnel-Group-Lock		Y	Y	String	Single	Name of the tunnel group or “none”

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
Tunneling-Protocols	Y	Y	Y	Integer	Single	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 and 4 are mutually exclusive (0 - 11, 16 - 27, 32 - 43, 48 - 59 are legal values).
Use-Client-Address	Y			Boolean	Single	0 = Disabled 1 = Enabled
User-Auth-Server-Name	Y			String	Single	IP address or hostname
User-Auth-Server-Port	Y	Y	Y	Integer	Single	Port number for server protocol
User-Auth-Server-Secret	Y			String	Single	Server password
WebVPN-ACL-Filters		Y		String	Single	Webtype access list name
WebVPN-Apply-ACL-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled With Version 8.0 and later, this attribute is not required.
WebVPN-Citrix-Support-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled With Version 8.0 and later, this attribute is not required.
WebVPN-Enable-functions				Integer	Single	Not used - deprecated
WebVPN-Exchange-Server-Address				String	Single	Not used - deprecated
WebVPN-Exchange-Server-NETBIOS-Name				String	Single	Not used - deprecated
WebVPN-File-Access-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
WebVPN-File-Server-Browsing-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Entry-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Forwarded-Ports		Y		String	Single	Port-forward list name
WebVPN-Homepage	Y	Y		String	Single	A URL such as http://www.example.com
WebVPN-Macro-Substitution-Value1	Y	Y		String	Single	See the SSL VPN Deployment Guide for examples at the following URL: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution-Value2	Y	Y		String	Single	See the SSL VPN Deployment Guide for examples at the following URL: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Auto-Download-Enable	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Enable	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-Single-Sign-On-Server-Name	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-SVC-Client-DPD	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-SVC-Compression	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-SVC-Enable	Y	Y		Boolean	Single	0 = Disabled 1 = Enabled

Attribute Name	VPN 3000	ASA	PIX	Syntax/Type	Single or Multi-valued	Possible Values
WebVPN-SVC-Gateway-DPD	Y	Y		Integer	Single	0 = Disabled n = Dead peer detection value in seconds (30 - 3600)
WebVPN-SVC-Keepalive	Y	Y		Integer	Single	0 = Disabled n = Keepalive value in seconds (15 - 600)
WebVPN-SVC-Keep-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SVC-Rekey-Method	Y	Y		Integer	Single	0 = None 1 = SSL 2 = New tunnel 3 = Any (sets to SSL)
WebVPN-SVC-Rekey-Period	Y	Y		Integer	Single	0 = Disabled n = Retry period in minutes (4 - 10080)
WebVPN-SVC-Required-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled
WebVPN-URL-Entry-Enable	Y	Y		Integer	Single	0 = Disabled 1 = Enabled
WebVPN-URL-List		Y		String	Single	URL list name

URL Types Supported in ACLs

The URL may be a partial URL, contain wildcards for the server, or include a port.

The following URL types are supported.

any All URLs	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

Guidelines for Using Cisco-AV Pairs (ACLs)

- Use Cisco-AV pair entries with the ip:inacl# prefix to enforce access lists for remote IPsec and SSL VPN Client (SVC) tunnels.
- Use Cisco-AV pair entries with the webvpn:inacl# prefix to enforce access lists for SSL VPN clientless (browser-mode) tunnels.
- For webtype ACLs, you do not specify the source because the ASA is the source.

Table 2: ASA-Supported Tokens

Token	Syntax Field	Description
ip:inacl# *Num* =	N/A (Identifier)	(Where *Num* is a unique integer.) Starts all AV pair access control lists. Enforces access lists for remote IPsec and SSL VPN (SVC) tunnels.
webvpn:inacl# *Num* =	N/A (Identifier)	(Where *Num* is a unique integer.) Starts all clientless SSL AV pair access control lists. Enforces access lists for 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 occurs, 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.

Cisco AV Pair Attribute Syntax

The Cisco Attribute Value (AV) pair (ID Number 26/9/1) can be used to enforce access lists from a RADIUS server (like Cisco ACS), or from an LDAP server via an LDAP attribute map.

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]

Table 3: AV-Pair Attribute Syntax Rules

Field	Description
Action	Action to perform if the rule matches a deny or a permit.
Destination	Network or host that receives the packet. Specify it as an IP address, a hostname, or the **any** keyword. If using an IP address, the source wildcard mask must follow.
Destination Wildcard Mask	The wildcard mask that applies 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 of 0 - 65535.
Prefix	A unique identifier for the AV pair (for example: ip:inacl#1= for standard access lists or webvpn:inacl# = for clientless SSL VPN access lists). This field only appears when the filter has been sent as an AV pair.
Protocol	Number or name of an IP protocol. Either an integer in the range of 0 - 255 or one of the following keywords: **icmp** , **igmp** , **ip** , **tcp** , **udp** .
Source	Network or host that sends the packet. Specify it as an IP address, a hostname, or the **any** keyword. If using an IP address, the source wildcard mask must follow. This field does not apply to Clientless SSL VPN because the ASA has the role of the source or proxy.
Source Wildcard Mask	The wildcard mask that applies to the source address. This field does not apply to Clientless SSL VPN because the ASA has the role of the source or proxy.

Cisco AV Pairs ACL Examples

This section shows examples of Cisco AV pairs and describes the permit or deny actions that result.

Note Each ACL # in inacl# must be unique. However, they do not need to be sequential (for example, 1, 2, 3, 4). That is, they could be 5, 45, 135.

Table 4: Examples of Cisco AV Pairs and Their Permitting or Denying Action

Cisco AV Pair Example	Permitting or Denying Action
`ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log`	Allows IP traffic between the two hosts using a full tunnel IPsec or SSL VPN client.
`ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log`	Allows TCP traffic from all hosts to the specific host on port 80 only using a full tunnel IPsec or SSL VPN client.
`webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share`	Allows clientlessSSL VPN traffic to the URL specified, denies SMTP traffic to a specific server, and allows file share access (CIFS) to the specified server.
`webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log`	Denies Telnet access and permits SSH access on non-default ports 2323 and 2222, respectively, or other application traffic flows using these ports for clientless SSL VPN.
`webvpn:inacl#1=permit url ssh://10.86.1.2webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 logwebvpn:inacl#48=deny url telnet://10.86.1.2webvpn:inacl#100=deny tcp 10.86.1.6 eq 23`	Allows clientless SSL VPN SSH access to default port 22 and denies Telnet access to port 23, respectively. This example assumes that you are using Telnet or SSH Java plug-ins enforced by these ACLs.

Active Directory/LDAP VPN Remote Access Authorization Examples

This section presents example procedures for configuring authentication and authorization on the ASA using the Microsoft Active Directory server. It includes the following topics:

- Policy Enforcement of User-Based Attributes, on page 17
- Enforce Static IP Address Assignment for AnyConnect Client Tunnels, on page 19
- Enforce Dial-in Allow or Deny Access, on page 21
- Enforce Logon Hours and Time-of-Day Rules, on page 23

Other configuration examples available on Cisco.com include the following TechNotes.

- ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example
- PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login

Policy Enforcement of User-Based Attributes

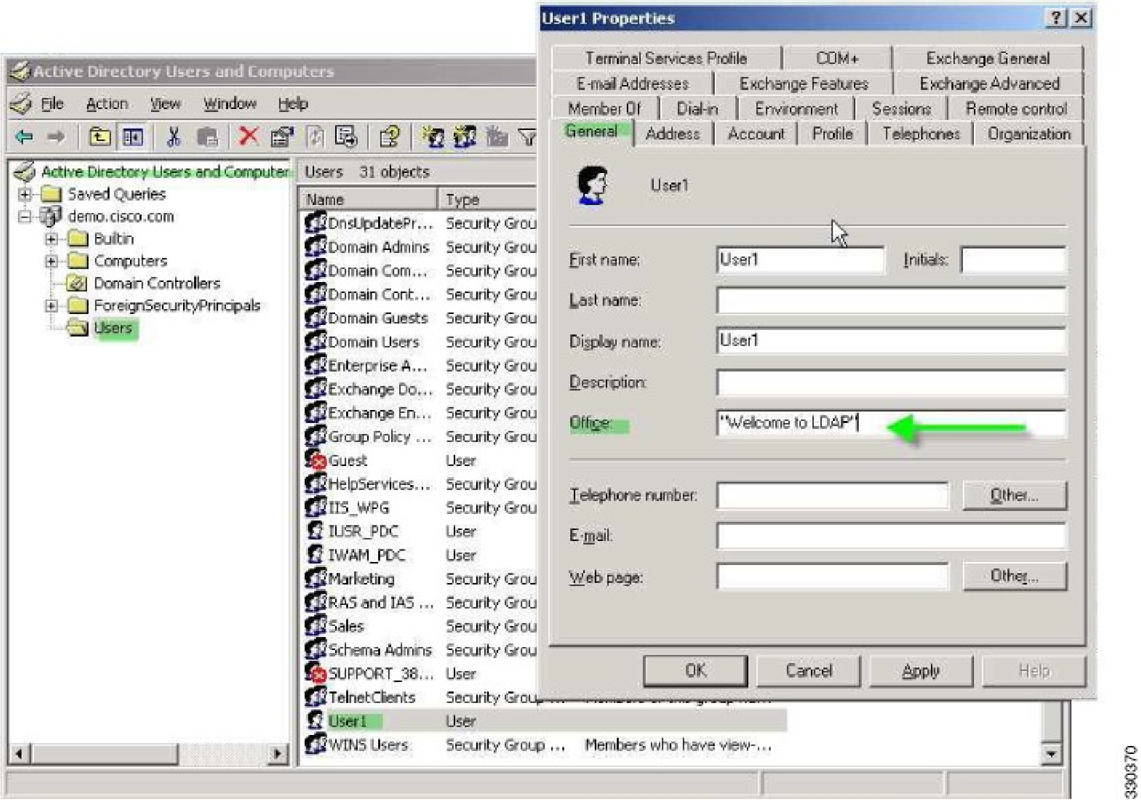
This example displays a simple banner to the user, showing how you can map any standard LDAP attribute to a well-known Vendor-Specific Attribute (VSA), and you can map one or more LDAP attribute(s) to one or more Cisco LDAP attributes. It applies to any connection type, including the IPsec VPN client and AnyConnect Client.

To enforce a simple banner for a user who is configured on an AD LDAP server use the Office field in the General tab to enter the banner text. This field uses the attribute named physicalDeliveryOfficeName. On the ASA, create an attribute map that maps physicalDeliveryOfficeName to the Cisco attribute Banner1.

During authentication, the ASA retrieves the value of physicalDeliveryOfficeName from the server, maps the value to the Cisco attribute Banner1, and displays the banner to the user.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **General** tab and enter banner text in the Office field, which uses the AD/LDAP attribute physicalDeliveryOfficeName.



Name	Type
DnsUpdatePr...	Security Grou
Domain Admins	Security Grou
Domain Com...	Security Grou
Domain Cont...	Security Grou
Domain Guests	Security Grou
Domain Users	Security Grou
Enterprise A...	Security Grou
Exchange Do...	Security Grou
Exchange En...	Security Grou
Group Policy ...	Security Grou
Guest	User
HelpServices...	Security Grou
IIS_WPG	Security Grou
IUSR_PDC	User
IWAM_PDC	User
Marketing	Security Grou
RAS and IAS ...	Security Grou
Sales	Security Grou
Schema Admins	Security Grou
SUPPORT_38...	User
TelnetClients	Security Group ...
User1	User
WINS Users	Security Group ... Members who have view-...

User1

First name: User1 Initials:

Last name:

Display name: User1

Description:

Office: "Welcome to LDAP"

Telephone number:

E-mail:

Web page:

Step 2 Create an LDAP attribute map on the ASA.

Create the map Banner and map the AD/LDAP attribute physicalDeliveryOfficeName to the Cisco attribute Banner1:

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP, and associate the attribute map Banner that you previously created:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

Step 4 Test the banner enforcement.

Enforce Static IP Address Assignment for AnyConnect Client Tunnels

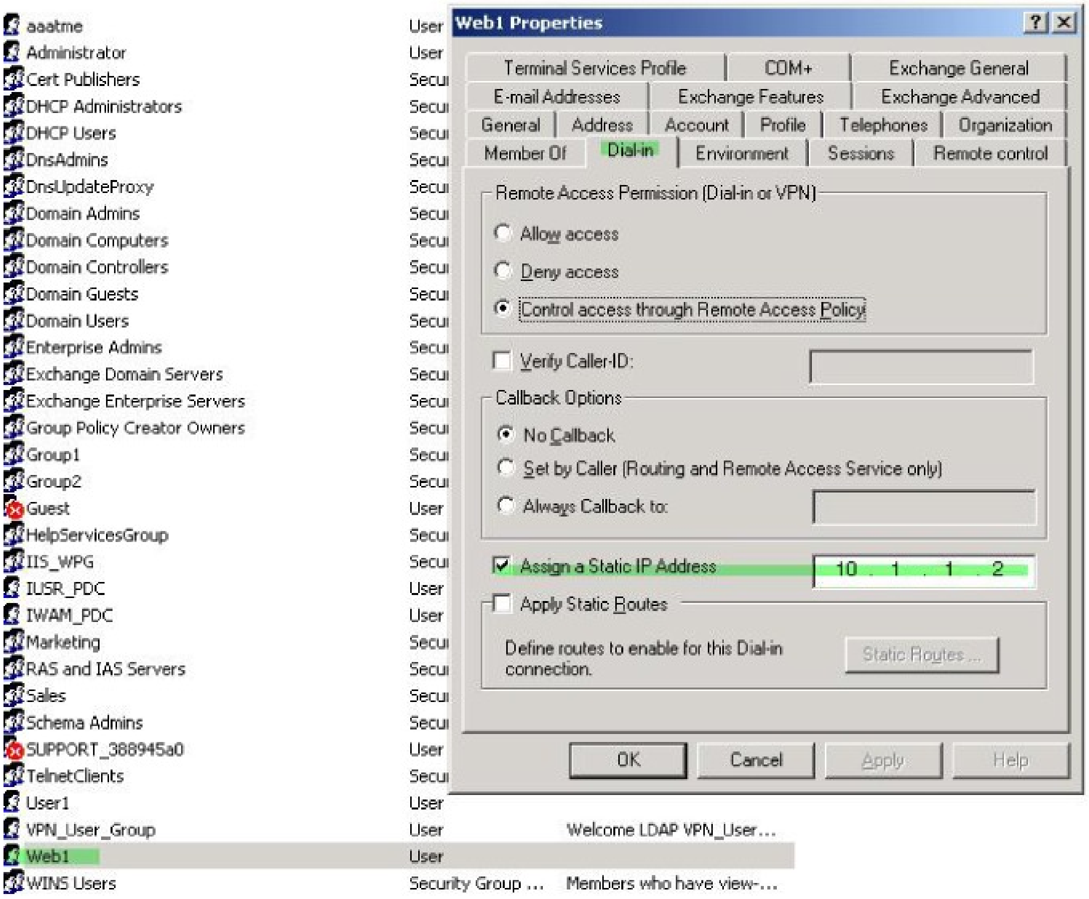
This example applies to full-tunnel clients, such as the IPsec client and the SSL VPN clients.

To enforce static AnyConnect Client static IP assignments configure the AnyConnect Client user Web1 to receive a static IP address, enter the address in the Assign Static IP Address field of the Dialin tab on the AD LDAP server (this field uses the msRADIUSFramedIPAddress attribute), and create an attribute map that maps this attribute to the Cisco attribute IETF-Radius-Framed-IP-Address.

During authentication, the ASA retrieves the value of msRADIUSFramedIPAddress from the server, maps the value to the Cisco attribute IETF-Radius-Framed-IP-Address, and provides the static address to User1.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **Dial-in** tab, check the **Assign Static IP Address** check box, and enter an IP address of 10.1.1.2.



Web1 Properties

Remote Access Permission (Dial-in or VPN)

○ Allow access
○ Deny access
● Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback
○ Set by Caller (Routing and Remote Access Service only)
○ Always Callback to:

☑ Assign a Static IP Address 10 . 1 . 1 . 2

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

330373

Step 2 Create an attribute map for the LDAP configuration shown.

Map the AD attribute msRADIUSFramedIPAddress used by the Static Address field to the Cisco attribute IETF-Radius-Framed-IP-Address:

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP, and associates the attribute map static_address that you previously created in:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

Step 4 Verify that the **vpn-address-assignment** command is configured to specify AAA by viewing this part of the configuration:

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
```

```
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

Step 5 Establish a connection to the ASA with the AnyConnect Client. Observe that the user receives the IP address configured on the server and mapped to the ASA.

Step 6 Use the **show vpn-sessiondb svc** command to view the session details and verify the address assigned:

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Enforce Dial-in Allow or Deny Access

This example creates an LDAP attribute map that specifies the tunneling protocols allowed by the user. You map the allow access and deny access settings on the Dialin tab to the Cisco attribute Tunneling-Protocol, which supports the following bitmap values:

Value	Tunneling Protocol
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	Clientless SSL
32	SSL client—AnyConnect Client or SSL VPN client
64	IPsec (IKEv2)

[1] (1) IPsec and L2TP over IPsec are not supported simultaneously. Therefore, the values 4 and 8 are mutually exclusive.

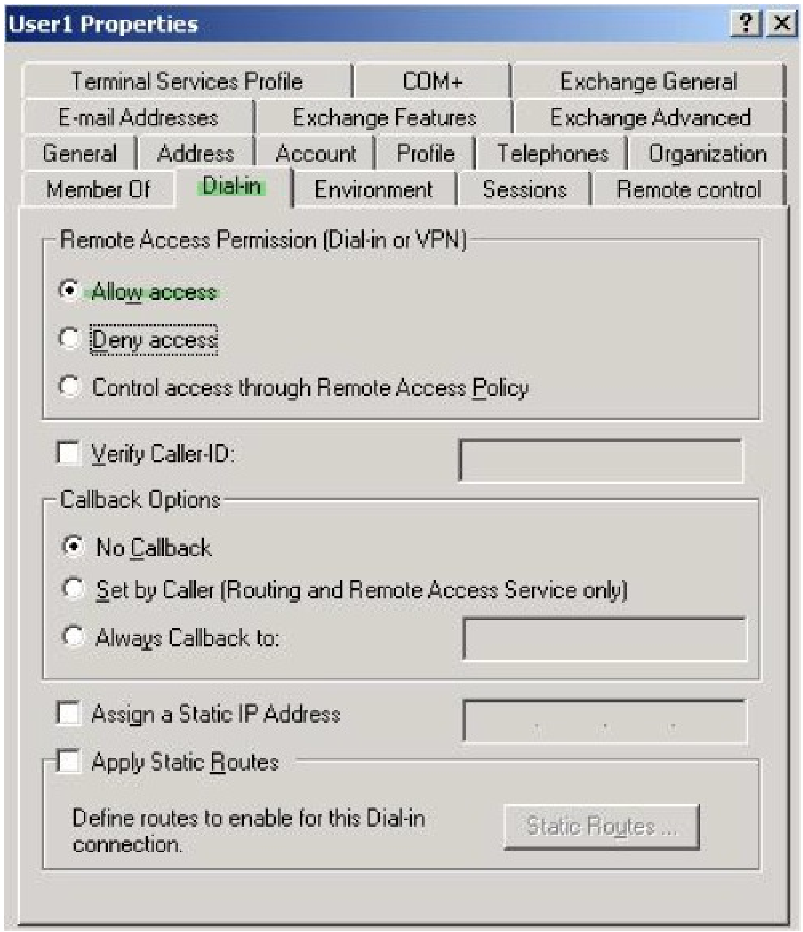
[2] (2) See note 1.

Use this attribute to create an Allow Access (TRUE) or a Deny Access (FALSE) condition for the protocols, and enforce the method for which the user is allowed access.

See Tech Note ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example for another example of enforcing dial-in allow access or deny access.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **Dial-in** tab, and click the Allow Access radio button.



Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Note
If you choose the Control access through the Remote Access Policy option, then a value is not returned from the server, and the permissions that are enforced are based on the internal group policy settings of the ASA.

Step 2 Create an attribute map to allow both an IPsec and AnyConnect Client connection, but deny a clientless SSL connection.

a) Create the map tunneling_protocols:

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

b) Map the AD attribute msNPAllowDialin used by the Allow Access setting to the Cisco attribute Tunneling-Protocols:

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) Add map values:

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

Step 3 Associate the LDAP attribute map to the AAA server.

a) Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) Associates the attribute map tunneling_protocols that you created:

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

Step 4 Verify that the attribute map works as configured.

Try connections using clientless SSL, the user should be informed that an unauthorized connection mechanism was the reason for the failed connection. The IPsec client should connect because IPsec is an allowed tunneling protocol according to the attribute map.

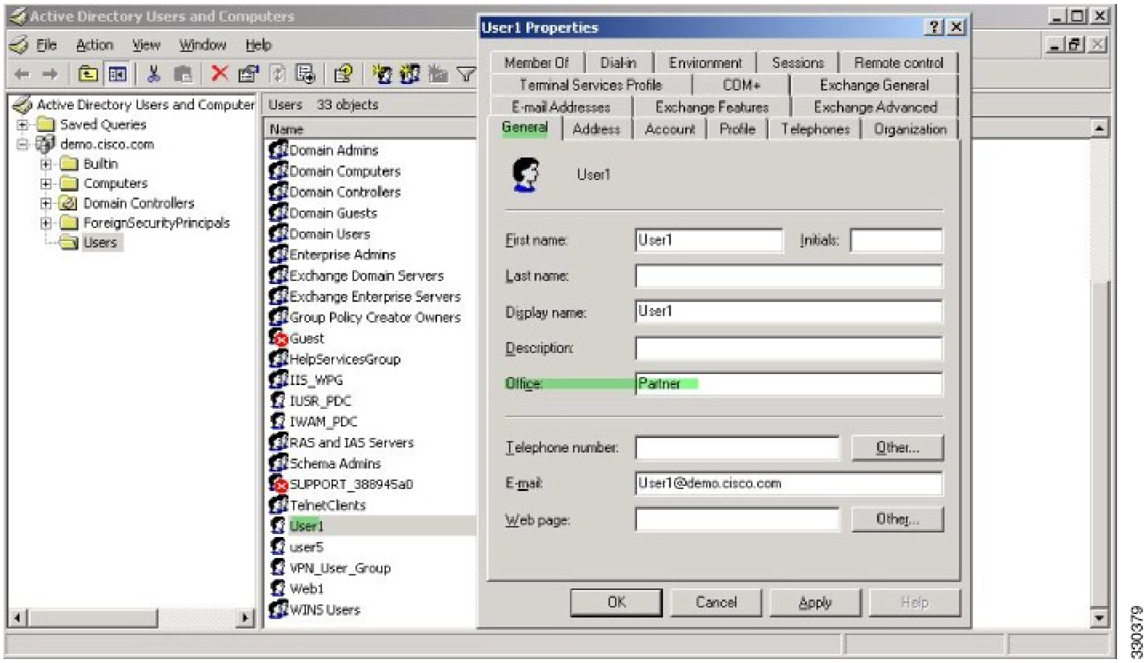
Enforce Logon Hours and Time-of-Day Rules

The following example shows how to configure and enforce the hours that a clientless SSL user (such as a business partner) is allowed to access the network.

On the AD server, use the Office field to enter the name of the partner, which uses the physicalDeliveryOfficeName attribute. Then we create an attribute map on the ASA to map that attribute to the Cisco attribute Access-Hours. During authentication, the ASA retrieves the value of physicalDeliveryOfficeName and maps it to Access-Hours.

Procedure

Step 1 Select the user, right-click **Properties**, and open the **General** tab:



First name: User1

Display name: User1

Office: Partner

E-mail: User1@demo.cisco.com

Step 2 Create an attribute map.

Create the attribute map access_hours and map the AD attribute physicalDeliveryOfficeName used by the Office field to the Cisco attribute Access-Hours.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for host 10.1.1.2 in the AAA server group MS_LDAP and associate the attribute map access_hours that you created.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

Step 4 Configure time ranges for each value allowed on the server.

Configure Partner access hours from 9am to 5pm Monday through Friday:

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```