



---

## A

### AAA

LDAP [6-1](#)

Microsoft Active Directory [6-1](#)

server group [6-5](#)

SSO [8-1](#)

tunnel group [6-12](#)

Access Control Server, add to group [9-3](#)

Access Control Server group [9-2](#)

access hours, VPN [2-24](#)

Accounting Mode, NAC [9-2](#)

ACL filter, internal group policy [2-12](#)

ACL Netmask Convert, NAC [9-5](#)

### ASA 5505

#### client

authentication [12-14](#)

device pass-through [12-10](#)

group policy attributes pushed to [12-15](#)

mode [12-5](#)

remote management [12-11](#)

TCP [12-12](#)

tunneling [12-1](#)

Xauth [12-8](#)

server (headend) [12-1, 12-4](#)

### attribute, LDAP

Cisco [6-4](#)

map [6-2](#)

name [6-4](#)

value [6-4](#)

attribute-value pairs (AVP) [2-2](#)

### authentication

ASA 5505 as Easy VPN client [12-14](#)

bypass and ASA 5505 [12-10](#)

certificate [1-4](#)

individual user [2-44](#)

Authentication Server Group, NAC [9-7](#)

Auto Signon, group-policy [2-61](#)

---

## B

banner, configuring [2-33](#)

base DN [6-9](#)

bypass authentication [12-10](#)

---

## C

certificate authority. *See* trustpoint for certificates

### certificate enrollment

authenticating to the CA [1-4](#)

generating key pairs [1-2](#)

summary of steps [1-1](#)

trustpoint configuration [1-3](#)

certificate filtering, Easy VPN client, ASA 5505 [12-13](#)

certificate management in ASDM [1-5](#)

Cisco attribute name [6-4](#)

Cisco client parameters, internal group policy [2-36](#)

### Citrix

access method [7-15](#)

configuring [7-1](#)

enabling [7-10](#)

trustpoint [7-2, 7-7](#)

- client
  - VPN 3002 hardware, forcing client update [4-1](#)
  - Windows client update notification [4-1](#)
- client access rules [2-29](#)
- client authentication, secure unit authentication [2-43](#)
- Client Configuration tab attributes, internal group policy [2-31](#)
- client firewall policy [2-40](#)
- clientless authentication, enable [9-12](#)
- client mode [12-5](#)
- client parameters
  - Cisco [2-36](#)
  - general [2-32](#)
  - Microsoft [2-38](#)
- clients for load balancing [11-2](#)
- client update
  - client types supported [4-2](#)
  - function list [4-1](#)
  - performing [4-1](#)
- common name [7-4, 7-5](#)
- Common Password, NAC [9-5](#)
- compression
  - HTTP [2-58](#)
  - IP [2-29](#)
  - SVC [2-60](#)
- Content Filtering tab, WebVPN tab [2-51](#)
- default, group policy
  - DefaultL2Lgroup [2-1](#)
  - DefaultRAGroup [2-1](#)
  - DefaultWebVPNgroup [2-1](#)
  - DfltGrpPolicy [2-3](#)
  - domain name for tunneled packets [2-34](#)
  - group policy [2-3](#)
  - group policy (DfltGrpPolicy) [2-1](#)
- Default ACL, NAC [9-9](#)
- Deny Message attribute, configuring [2-58](#)
- Depletion, NAC Reactivation Mode [9-3](#)
- destination and source networks, internal group policy [2-16](#)
- Detect Automatically, NAC ACL Netmask Convert [9-5](#)
- device pass-through, ASA 5505 as Easy VPN client [12-10](#)
- DfltGrpPolicy [2-1](#)
- DHCP scope, internal group policy [2-27](#)
- DHCP server and DDNS update settings [5-4](#)
- digital certificate filtering, Easy VPN client, ASA 5505 [12-13](#)
- DN field [6-10](#)
- DNS records and DDNS update [5-1](#)
- DNS servers
  - as IPSec backup servers [2-37](#)
  - internal group policy [2-27](#)
- DPD (dead peer detection) [2-61](#)
- dynamic DNS. *See* DDNS

---

## D

- DDNS update
  - DHCP server settings [5-4](#)
  - example, DHCP server updates both RRs [5-2](#)
  - interface [5-3](#)
  - interval between updates [5-2](#)
  - method of update [5-2](#)
  - resource records [5-1](#)
  - scenarios possible [5-1](#)
- Dead Peer Detection (DPD), internal group policy [2-61](#)
- Dead Time, NAC [9-3](#)

---

## E

- EAPoUDP Port [9-12](#)
- EAPoUDP Retries [9-12](#)
- Easy VPN
  - client
    - authentication [12-14](#)
    - enabling and disabling [12-4](#)
    - group policy attributes pushed to [12-15](#)
    - mode [12-5](#)
    - remote management [12-11](#)

- tunnels [12-11](#)
- Xauth [12-8](#)
- server (headend) [12-1, 12-4](#)
- Easy VPN client
  - ASA 5505
    - device pass-through [12-10](#)
    - TCP [12-12](#)
    - tunneling [12-1](#)
- Enable, NAC exemption [9-9](#)
- Enable Clientless Authentication [9-12](#)
- Enable NAC [9-8](#)
- enrolling for certificate
  - authenticating to the CA [1-4](#)
  - generating key pairs [1-2](#)
  - summary of steps [1-1](#)
  - trustpoint configuration [1-3](#)
- enrolling for identity certificate [1-5](#)
- exemptions from posture validation [9-9](#)
- external group policy
  - adding [2-6](#)
  - configuring [2-6](#)
  - editing [2-9](#)

---

## F

- Fallback Trustpoint [7-7](#)
- Filter, NAC exemption [9-9](#)
- firewall policy, client [2-40](#)
- FQDN [7-4, 7-5](#)
- Functions tab, WebVPN Tab [2-49](#)

---

## G

- general client parameters, configuring [2-32](#)
- group policy
  - configuring [2-5](#)
  - default [2-3](#)
  - definition [2-1, 2-2](#)

- Easy VPN client, attributes pushed to ASA 5505 [12-15](#)
- external, adding [2-6](#)
- external, configuring [2-6](#)
- external, editing [2-9](#)
- internal, adding or editing [2-10](#)
- internal, configuring [2-9](#)
- internal, general attributes [2-11](#)
- WebVPN [2-48](#)

---

## H

- Hardware Client tab attributes, internal group policy [2-42](#)
- Hold Timer [9-11](#)
- home page
  - applying customizations [2-52](#)
  - redirecting to Citrix server [7-15](#)
- HTTP compression, enabling or disabling [2-58](#)
- HTTP Form protocol
  - form data, gathering
    - action URI [8-11](#)
    - authentication cookie [8-11](#)
    - hidden parameters [8-11](#)
    - HTTP header analyzer [8-10](#)
    - password parameter [8-10](#)
    - POST request [8-10](#)
    - username parameter [8-10](#)
- HTTPS [8-15](#)
- overview [8-9](#)
- SSO, configuring [8-13](#)
- tunnel group, assigning to [8-16](#)
- HTTP redirection for login, Easy VPN client on the ASA 5505 [12-14](#)
- HTTPS and SSO
  - HTTP Form protocol [8-15](#)
  - SiteMinder [8-4](#)

**I**

- identity certificate, enrolling [1-5](#)
- idle timeout, hardware client users [2-44](#)
- idle timeout, user [2-27](#)
- IKE pre-shared key, Easy VPN client on the ASA 5505 [12-7](#)
- individual user authentication, ASA 5505 [12-14](#)
- individual user authentication, hardware client [2-44](#)
- interface, DDNS update [5-3](#)
- Interface Name, NAC [9-4](#)
- internal group policy
  - adding or editing [2-10](#)
  - configuring [2-9](#)
  - General tab attributes [2-11](#)
  - Hardware Client tab attributes [2-42](#)
  - IPSec tab attributes [2-28](#)
  - maximum connect time [2-26](#)
  - Other WebVPN tab [2-55](#)
  - WebVPN tab attributes [2-48](#)
- IP address requirements for load balancing [11-2](#)
- IP compression [2-29](#)
- IP phone
  - bypass, hardware client [2-45](#)
  - bypass and ASA 5505 [12-10](#)
- IPSec
  - backup servers [2-37](#)
  - over NAT [2-37](#)
  - over UDP [2-37](#)
- IPSec tab attributes, internal group policy [2-28](#)

**K**

- Keepalive Ignore attribute, configuring [2-58](#)
- keepalive interval, internal group policy [2-60](#)
- Keep Installer on Client System [2-60](#)
- Kerberos and LDAP. *See* LDAP SASL Kerberos
- key pairs, generating [1-2](#)
- key renegotiation settings, internal group policy [2-61](#)

**L**

- L2TP over IPSec [10-1](#)
  - address assignment [10-4](#)
  - as a tunneling protocol [10-7](#)
  - configuring L2TP over IPSec [10-3](#)
  - L2TP overview [10-1](#)
  - modes [10-2](#)
  - multiple clients behind NAT [10-12](#)
  - PPP authentication protocols [10-9](#)
  - transport mode [10-3](#)
- LDAP
  - attribute
    - Cisco attribute name [6-4](#)
    - map [6-2](#)
    - Map Name tab [6-4](#)
    - Map Value tab [6-4](#)
    - naming attributes [6-10](#)
  - base DN [6-9](#)
  - DN field [6-10](#)
  - over SSL [6-9](#)
  - SASL
    - Kerberos [6-10](#)
    - MD5 [6-10](#)
  - search scope [6-10](#)
  - server
    - AAA server [6-8](#)
    - AAA server groups [6-6](#)
    - detect type automatically [6-9](#)
    - Microsoft Active Directory [6-9](#)
    - other type [6-9](#)
    - reactivation mode [6-7](#)
    - server group [6-5](#)
    - server port [6-9](#)
    - server type [6-9](#)
    - Sun Microsystems Directory Server [6-9](#)
  - transaction flow overview [6-2](#)
  - tunnel group [6-12](#)

**LEAP**

- bypass, hardware client [2-45](#)
- protocol [2-46](#)

Lightweight Extensible Authentication Protocol. *See* LEAP

**load balancing**

- and 3DES/AES licensing [11-2](#)
- and VRRP [11-2](#)
- clients supported [11-2](#)
- configurations [11-3](#)
- configuring [11-4](#)
- mixed clusters [11-4](#)
- security appliance models [11-2](#)
- virtual cluster [11-2](#)
- VPN session limits [11-6](#)

LOCAL group [9-7](#)

logging level [2-23](#)

---

**M**

MAC addresses, ASA 5505 device pass-through [12-11](#)

managing certificates in ASDM [1-5](#)

**map attribute**

- name [6-4](#)
- value [6-4](#)

Max Failed Attempts, NAC [9-3](#)

maximum connect time, internal group policy [2-26](#)

maximum sessions, IPsec VPN [11-7](#)

MD5 and LDAP. *See* LDAP SASL MD5

Microsoft Active Directory, for AAA [6-1](#)

Microsoft client parameters, configuring [2-38](#)

mixed cluster configuration and WebVPN connections [11-4](#)

MTU size, Easy VPN client, ASA 5505 [12-13](#)

---

**N**

NAC [9-1](#)

NAC tab (Network Admission Control) [2-46](#)

naming attributes, LDAP [6-10](#)

NAT, IPsec over NAT [2-37](#)

Network Admission Control. *See* NAC

**network extension mode**

- hardware client [2-46](#)
- specifying on the ASA 5505 [12-5](#)

---

**O**

operating system, NAC exemption [9-9](#)

Other tab arguments, WebVPN group policy tab [2-55](#)

---

**P**

Password, clientless authentication [9-12](#)

password, common [9-5](#)

password storage, internal group policy [2-36](#)

PAT, Easy VPN client mode [12-6](#)

perfect forward secrecy (pfs) [2-29](#)

platforms for load balancing. *See* load balancing, security appliance models

Port Address Translation. *See* PAT

port forwarding, enabling [2-54](#)

port forwarding list, adding or editing [2-54](#)

Port Forwarding WebVPN tab [2-54](#)

posture validation [9-1](#)

Posture Validation Exception List [9-9](#)

pre-shared key, Easy VPN client on the ASA 5505 [12-7](#)

printers [12-10](#)

Protocol, NAC [9-2](#)

protocol and service groups, managing [2-17](#)

protocol attribute, internal group policy [2-17](#)

---

**R**

RADIUS, NAC [9-2](#)

Reactivation Mode, NAC [9-3](#)

reactivation of failed LDAP servers [6-7](#)

reauthentication on IKE rekey [2-28](#)

remote management, ASA 5505 [12-11](#)

resource records [5-1](#)

Retransmission Timer [9-11](#)

Retry Interval, NAC [9-4](#)

Revalidation Timer [9-8](#)

## S

SASL

Kerberos [6-10](#)

MD5 [6-10](#)

SCEP, obtaining certificates with [1-4](#)

secure SSO messaging. *See* HTTPS and SSO

secure unit authentication

with the ASA 5505 [12-14](#)

secure unit authentication, requiring [2-43](#)

security appliance

load balancing and models [11-2](#)

Server Accounting Port, NAC [9-4](#)

Server Authentication Port, NAC [9-4](#)

server certificate filtering, Easy VPN client, ASA 5505 [12-13](#)

Server Group, NAC [9-2, 9-4](#)

Server Name or IP Address, NAC [9-4](#)

server port [6-9](#)

servers and URL lists, WebVPN Other tab [2-56](#)

Server Secret Key, NAC [9-5](#)

server type [6-9](#)

service groups, managing, internal group policy [2-17](#)

session failover and virtual cluster [11-2](#)

shared secret, NAC [9-5](#)

Simple Authentication and Security Layer. *See* SASL

Simple Certificate Enrollment Protocol. *See* SCEP

simultaneous logins [2-26](#)

single sign-on. *See* SSO

SiteMinder

Cisco authentication scheme, adding [8-9](#)

group policies [8-4](#)

HTTPS [8-4](#)

SSO, configuring [8-2](#)

user assignment [8-7](#)

source and destination networks, internal group policy [2-16](#)

source and destination port service, internal group policy [2-19](#)

split tunneling

attributes [2-35](#)

domain list [2-34](#)

network list, internal group policy [2-35](#)

policy, internal group policy [2-35](#)

SSL [7-7](#)

SSL LDAP communications. *See* LDAP over SSL

SSL VPN Client

benefits [3-1](#)

configuring

address assignment [3-6](#)

features [3-11](#)

tunnel group [3-9](#)

tunneling protocol [3-11](#)

WebVPN on interface [3-5](#)

enabling [3-2](#)

installation [3-2](#)

loading images [3-2](#)

ordering images [3-4](#)

view sessions [3-14](#)

SSL VPN Client tab attributes, internal group policy [2-59](#)

SSO

for WebVPN users [8-1](#)

HTTP Form protocol, using [8-9](#)

SiteMinder, using [8-2](#)

SSO server, adding, internal group policy [2-57](#)

Status Query Timer [9-8](#)

SVC compression [2-60](#)

**T**

TCP, ASA 5505 as Easy VPN client [12-12](#)  
 TCP Port Forwarding JAVA applet and digital certificate [2-51](#)  
 Timed, NAC Reactivation Mode [9-3](#)  
 timeout, idle, hardware client users [2-44](#)  
 Timeout, NAC [9-4](#)  
 timeout, user idle [2-27](#)  
 time range  
   applying [2-24](#)  
   browse [2-23](#)  
   defining [2-25](#)  
   viewing [2-25](#)  
 trustpoint  
   certificates, creating for [1-3](#)  
   Citrix  
     adding [7-2](#)  
     applying to interfaces [7-7](#)  
     CA authentication [7-5](#)  
     certificate enrollment [7-6](#)  
     Fallback Trustpoint [7-7](#)  
 tunnel, ASA 5505 as Easy VPN client [12-1](#)  
 tunnel group  
   default [2-1](#)  
   definition [2-1](#)  
   for LDAP authentication [6-12](#)  
   locking [2-29](#)  
 tunneling attributes, configuring [2-34](#)  
 tunneling protocol, internal group policy [2-11](#)

**U**

UDP, IPSec over UDP [2-37](#)  
 update method for DDNS [5-2](#)  
 updating clients. *See* client update  
 URL Enable entry [7-12, 7-14](#)  
 Use LOCAL if Server Group fails [9-7](#)  
 user, definition [2-1](#)

user authentication, hardware client, requiring [2-44](#)  
 user home page, applying customizations [2-52](#)  
 user idle timeout, internal group policy [2-27](#)  
 username  
   management tunnels [12-11](#)  
   Xauth for Easy VPN client [12-8](#)  
 Username, clientless authentication [9-12](#)

**V**

virtual cluster [11-2](#)  
   IP address [11-1](#)  
   master [11-1](#)  
   secondary devices [11-1](#)  
   session failover [11-2](#)  
 VPN  
   access hours [2-24](#)  
   hardware clients [2-42](#)  
   session limits and load balancing [11-6](#)

**W**

Web Type ACL, managing [2-57](#)  
 WebVPN  
   enabling [7-8](#)  
   SSO [8-1](#)  
   users, access to Citrix server [7-15](#)  
 WebVPN application access, enabling [2-54](#)  
 WebVPN group policy attributes [2-48](#)  
 WebVPN tab attributes [2-48](#)  
 Wildcard, NAC ACL Netmask Convert [9-5](#)  
 WINS servers  
   as IPSec backup servers [2-37](#)  
   internal group policy [2-27](#)

---

**X**

Xauth, Easy VPN client [12-8](#)

xlate [2-14](#)