



RADIUS Servers for AAA

This chapter describes how to configure RADIUS servers for AAA.

- [About RADIUS Servers for AAA, on page 1](#)
- [Guidelines for RADIUS Servers for AAA, on page 18](#)
- [Configure RADIUS Servers for AAA, on page 18](#)
- [Monitoring RADIUS Servers for AAA, on page 25](#)
- [History for RADIUS Servers for AAA, on page 26](#)

About RADIUS Servers for AAA

The Cisco ASA supports the following RFC-compliant RADIUS servers for AAA:

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2, and 5.x
- Cisco Identity Services Engine (ISE)
- RSA RADIUS in RSA Authentication Manager 5.2, 6.1, and 7.x
- Microsoft

Supported Authentication Methods

The ASA supports the following authentication methods with RADIUS servers:

- PAP—For all connection types.
- CHAP and MS-CHAPv1—For L2TP-over-IPsec connections.
- MS-CHAPv2—For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections.
- Authentication Proxy modes—For RADIUS-to-Active-Directory, RADIUS-to-RSA/SDI, RADIUS-to-Token server, and RSA/SDI-to-RADIUS connections,



Note To enable MS-CHAPv2 as the protocol used between the ASA and the RADIUS server for a VPN connection, password management must be enabled in the tunnel group general attributes. Enabling password management generates an MS-CHAPv2 authentication request from the ASA to the RADIUS server. See the description of the **password-management** command for details.

If you use double authentication and enable password management in the tunnel group, then the primary and secondary authentication requests include MS-CHAPv2 request attributes. If a RADIUS server does not support MS-CHAPv2, then you can configure that server to send a non-MS-CHAPv2 authentication request by using the **no mschapv2-capable** command.

User Authorization of VPN Connections

The ASA can use RADIUS servers for user authorization of VPN remote access and firewall cut-through-proxy sessions using dynamic ACLs or ACL names per user. To implement dynamic ACLs, you must configure the RADIUS server to support them. When the user authenticates, the RADIUS server sends a downloadable ACL or ACL name to the ASA. Access to a given service is either permitted or denied by the ACL. The ASA deletes the ACL when the authentication session expires.

In addition to ACLs, the ASA supports many other attributes for authorization and setting of permissions for VPN remote access and firewall cut-through proxy sessions.

Supported Sets of RADIUS Attributes

The ASA supports the following sets of RADIUS attributes:

- Authentication attributes defined in RFC 2138.
- Accounting attributes defined in RFC 2139.
- RADIUS attributes for tunneled protocol support, defined in RFC 2868.
- Cisco IOS Vendor-Specific Attributes (VSAs), identified by RADIUS vendor ID 9.
- Cisco VPN-related VSAs, identified by RADIUS vendor ID 3076.
- Microsoft VSAs, defined in RFC 2548.

Supported RADIUS Authorization Attributes

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. These attributes have vendor ID 3076.

The following table lists the supported RADIUS attributes that can be used for user authorization.



Note RADIUS attribute names do not contain the cVPN3000 prefix. Cisco Secure ACS 4.x supports this new nomenclature, but attribute names in pre-4.0 ACS releases still include the cVPN3000 prefix. The ASAs enforce the RADIUS attributes based on attribute numeric ID, not attribute name.

All attributes listed in the following table are downstream attributes that are sent from the RADIUS server to the ASA except for the following attribute numbers: 146, 150, 151, and 152. These attribute numbers are upstream attributes that are sent from the ASA to the RADIUS server. RADIUS attributes 146 and 150 are sent from the ASA to the RADIUS server for authentication and authorization requests. All four previously listed attributes are sent from the ASA to the RADIUS server for accounting start, interim-update, and stop requests. Upstream RADIUS attributes 146, 150, 151, and 152 were introduced in Version 8.4(3).

Table 1: Supported RADIUS Authorization Attributes

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|-----------------------------|-----|-----------|-------------|------------------------|---|
| Access-Hours | Y | 1 | String | Single | Name of the time range, for example, Business-hours |
| Access-List-Inbound | Y | 86 | String | Single | ACL ID |
| Access-List-Outbound | Y | 87 | String | Single | ACL ID |
| Address-Pools | Y | 217 | String | Single | Name of IP local pool |
| Allow-Non-Extension Mode | Y | 64 | Boolean | Single | 0 = Disabled 1 = Enabled |
| Authentication-Idle-Timeout | Y | 50 | Integer | Single | 1-35791394 minutes |
| Authorization-DN-Field | 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 |
| Authorization-Required | | 66 | Integer | Single | 0 = No 1 = Yes |
| Authorization-Type | Y | 65 | Integer | Single | 0 = None 1 = RADIUS 2 = LDAP |
| Banner1 | Y | 15 | String | Single | Banner string to display for Cisco VPN remote access sessions: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, and Clientless SSL |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|---|-----|-----------|-------------|------------------------|--|
| Banner2 | Y | 36 | String | Single | Banner string to display for Cisco VPN remote access sessions: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, and Clientless SSL. The Banner2 string is concatenated to the Banner1 string , if configured. |
| Cisco-IP-Phone-Bypass | Y | 51 | Integer | Single | 0 = Disabled 1 = Enabled |
| Cisco-LEAP-Bypass | Y | 75 | Integer | Single | 0 = Disabled 1 = Enabled |
| Client Type | Y | 150 | Integer | Single | 1 = Cisco VPN Client (IKEv1) 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN (IKEv2) |
| Client-Type-Version-Limiting | Y | 77 | String | Single | IPsec VPN version number string |
| DHCP-Network-Scope | Y | 61 | String | Single | IP Address |
| Extended-Authentication-Only | Y | 122 | Integer | Single | 0 = Disabled 1 = Enabled |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|---------------------|-----|-----------|-------------|------------------------|--|
| Framed-Interface-Id | Y | 96 | String | Single | Assigned IPv6 interface ID. Combines with Framed-IPv6-Prefix to create a complete assigned IPv6 address. For example: Framed-Interface-Id=1:1:1 combined with Framed-IPv6-Prefix=2001:db8:: gives the assigned IP address 2001:0db8::1:1:1:1. |
| Framed-IPv6-Prefix | Y | 97 | String | Single | Assigned IPv6 prefix and length. Combines with Framed-Interface-Id to create a complete assigned IPv6 address. For example: prefix 2001:0db8::/64 combined with Framed-Interface-Id=1:1:1 gives the IP address 2001:0db8::1:1:1:1. You can use this attribute to assign an IP address without using Framed-Interface-Id, by assigning the full IPv6 address with prefix length /128, for example, Framed-IPv6-Prefix=2001:db8::/128 |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|--|-----|-----------|-------------|------------------------|---|
| Group-Policy | Y | 25 | String | Single | Sets the group policy for the remote access VPN session. For Versions 8.2.x and later, use this attribute instead of IETF-Radius-Class. You can use one of the following formats: <ul style="list-style-type: none"> • <i>group policy name</i> • <i>OU=group policy name</i> • <i>OU=group policy name;</i> |
| IE-Proxy-Bypass-Local | | 83 | Integer | Single | 0 = None 1 = Local |
| IE-Proxy-Exception-List | | 82 | String | Single | New line (\n) separated list of DNS domains |
| IE-Proxy-PAC-URL | Y | 133 | String | Single | PAC address string |
| IE-Proxy-Server | | 80 | String | Single | IP address |
| IE-Proxy-Server-Policy | | 81 | Integer | Single | 1 = No Modify 2 = No Proxy 3 = Auto detect 4 = Use Concentrator Setting |
| IKE-Keep-Alive-Interval | Y | 68 | Integer | Single | 10-300 seconds |
| IKE-Keep-Alive-Retry-Interval | Y | 84 | Integer | Single | 2-10 seconds |
| IKE-Keep-Alive | Y | 41 | Boolean | Single | 0 = Disabled 1 = Enabled |
| Intercept-DHCP-Configure-Mg | Y | 62 | Boolean | Single | 0 = Disabled 1 = Enabled |
| IPsec-Allow-Passwd-Store | Y | 16 | Boolean | Single | 0 = Disabled 1 = Enabled |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|--------------------------------|-----|-----------|-------------|------------------------|---|
| IPsec-Authentication | | 13 | 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 |
| IPsec-Auth-On-Rekey | Y | 42 | Boolean | Single | 0 = Disabled 1 = Enabled |
| IPsec-Backup-Server-List | Y | 60 | String | Single | Server Addresses (space delimited) |
| IPsec-Backup-Servers | Y | 59 | String | Single | 1 = Use Client-Configured list 2 = Disable and clear client list 3 = Use Backup Server list |
| IPsec-Client-Firewall-Name | | 57 | String | Single | Specifies the name of the filter to be pushed to the client as firewall policy |
| IPsec-Client-Firewall-Optional | Y | 58 | Integer | Single | 0 = Required 1 = Optional |
| IPsec-Default-Domain | Y | 28 | String | Single | Specifies the single default domain name to send to the client (1-255 characters). |
| IPsec-IKE-Peer-ID-Check | Y | 40 | Integer | Single | 1 = Required 2 = If supported by peer certificate 3 = Do not check |
| IPsec-IP-Compression | Y | 39 | Integer | Single | 0 = Disabled 1 = Enabled |
| IPsec-Mode-Config | Y | 31 | Boolean | Single | 0 = Disabled 1 = Enabled |
| IPsec-Over-UDP | Y | 34 | Boolean | Single | 0 = Disabled 1 = Enabled |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|------------------------------|-----|-----------|-------------|------------------------|---|
| IPsec-Over-UDP-Port | Y | 35 | Integer | Single | 4001- 49151. The default is 10000. |
| IPsec-Remote-Filter-Apply | Y | 56 | 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 | | 12 | String | Single | Name of the security association |
| IPsec-Split-DNS-Names | Y | 29 | String | Single | Specifies the list of secondary domain names to send to the client (1-255 characters). |
| IPsec-Split-Tunneling-Policy | Y | 55 | Integer | Single | 0 = No split tunneling 1 = Split tunneling 2 = Local LAN permitted |
| IPsec-Split-Tunnel-List | Y | 27 | String | Single | Specifies the name of the network or ACL that describes the split tunnel inclusion list. |
| IPsec-Tunnel-Type | Y | 30 | Integer | Single | 1 = LAN-to-LAN 2 = Remote access |
| IPsec-User-Group-Lock | | 33 | Boolean | Single | 0 = Disabled 1 = Enabled |
| IPv6-Address-Pools | Y | 218 | String | Single | Name of IP local pool-IPv6 |
| IPv6-VPN-Filter | Y | 219 | String | Single | ACL value |
| L2TP-Encryption | | 21 | Integer | Single | Bitmap: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Enc/Stateless-Req |
| L2TP-MPPC-Compression | | 38 | Integer | Single | 0 = Disabled 1 = Enabled |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|---------------------------|-----|-----------|-------------|------------------------|--|
| Member-Of | Y | 145 | String | Single | Comma-delimited string, for example: Engineering, Sales An administrative attribute that can be used in dynamic access policies. It does not set a group policy. |
| MS-Client-Subnet-Mask | Y | 63 | Boolean | Single | An IP address |
| NAC-Default-ACL | | 92 | String | | ACL |
| NAC-Enable | | 89 | Integer | Single | 0 = No 1 = Yes |
| NAC-Revalidation-Timer | | 91 | Integer | Single | 300-86400 seconds |
| NAC-Settings | Y | 141 | String | Single | Name of the NAC policy |
| NAC-Status-Query-Timer | | 90 | Integer | Single | 30-1800 seconds |
| Perf-Forward-Secur-Enable | Y | 88 | Boolean | Single | 0 = No 1 = Yes |
| PPTP-Encryption | | 20 | Integer | Single | Bitmap: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Required 15 = 40/128-Encr/Stateless-Req |
| PPTP-MPPC-Compression | | 37 | Integer | Single | 0 = Disabled 1 = Enabled |
| Primary-DNS | Y | 5 | String | Single | An IP address |
| Primary-WINS | Y | 7 | String | Single | An IP address |
| Privilege-Level | Y | 220 | Integer | Single | An integer between 0 and 15. |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|---------------------------------------|-----|-----------|-------------|------------------------|--|
| Required-Client-Firewall-Vendor-Code | Y | 45 | 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) |
| Required-Client-Firewall-Description | Y | 47 | String | Single | String |
| Required-Client-Firewall-Product-Code | Y | 46 | 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 |
| Required-Individual-User-Auth | Y | 49 | Integer | Single | 0 = Disabled 1 = Enabled |
| Require-HW-Client-Auth | Y | 48 | Boolean | Single | 0 = Disabled 1 = Enabled |
| Secondary-DNS | Y | 6 | String | Single | An IP address |
| Secondary-WINS | Y | 8 | String | Single | An IP address |
| SEP-Card-Assignment | | 9 | Integer | Single | Not used |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|--------------------------|-----|-----------|-------------|------------------------|--|
| Session Subtype | Y | 152 | Integer | Single | 0 = None 1 = Clientless 2 = Client 3 = Client Only Session Subtype applies only when the Session Type (151) attribute has the following values: 1, 2, 3, and 4. |
| Session Type | Y | 151 | Integer | Single | 0 = None 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN (IKEv2) 3 = Clientless SSL VPN 4 = Clientless Email Proxy 5 = Cisco VPN Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN Load Balancing |
| Simultaneous-Logins | Y | 2 | Integer | Single | 0-2147483647 |
| Smart-Tunnel | Y | 136 | String | Single | Name of a Smart Tunnel |
| Smart-Tunnel-Auto | Y | 138 | Integer | Single | 0 = Disabled 1 = Enabled 2 = AutoStart |
| Smart-Tunnel-Auto-Signon | Y | 139 | String | Single | Name of a Smart Tunnel Auto Signon list appended by the domain name |
| Strip-Realm | Y | 135 | Boolean | Single | 0 = Disabled 1 = Enabled |
| SVC-Ask | Y | 131 | String | Single | 0 = Disabled 1 = Enabled 3 = Enable default service 5 = Enable default clientless (2 and 4 not used) |

Supported RADIUS Authorization Attributes

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|--------------------------|-----|-----------|-------------|------------------------|--|
| SVC-Ask-Timeout | Y | 132 | Integer | Single | 5-120 seconds |
| SVC-DPD-Interval-Client | Y | 108 | Integer | Single | 0 = Off 5-3600 seconds |
| SVC-DPD-Interval-Gateway | Y | 109 | Integer | Single | 0 = Off) 5-3600 seconds |
| SVC-DTLS | Y | 123 | Integer | Single | 0 = False 1 = True |
| SVC-Keepalive | Y | 107 | Integer | Single | 0 = Off 15-600 seconds |
| SVC-Modules | Y | 127 | String | Single | String (name of a module) |
| SVC-MTU | Y | 125 | Integer | Single | MTU value 256-1406 in bytes |
| SVC-Profiles | Y | 128 | String | Single | String (name of a profile) |
| SVC-Rekey-Time | Y | 110 | Integer | Single | 0 = Disabled 1-10080 minutes |
| Tunnel Group Name | Y | 146 | String | Single | 1-253 characters |
| Tunnel-Group-Lock | Y | 85 | String | Single | Name of the tunnel group or "none" |
| Tunneling-Protocols | Y | 11 | 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 | | 17 | Boolean | Single | 0 = Disabled 1 = Enabled |
| VLAN | Y | 140 | Integer | Single | 0-4094 |
| WebVPN-Access-List | Y | 73 | String | Single | Access-List name |
| WebVPN ACL | Y | 73 | String | Single | Name of a WebVPN ACL on the device |
| WebVPN-ActiveX-Relay | Y | 137 | Integer | Single | 0 = Disabled Otherwise = Enabled |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|--------------------------------|-----|-----------|-------------|------------------------|--|
| WebVPN-Apply-ACL | Y | 102 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Auto-HTTPS-Group | Y | 124 | String | Single | Reserved |
| WebVPN-Client-Frame-Enable | Y | 101 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Content-Filter-Params | Y | 69 | Integer | Single | 1 = Java ActiveX 2 = Java Script 4 = Image 8 = Cookies in images |
| WebVPN-Customization | Y | 113 | String | Single | Name of the customization |
| WebVPN-Default-Homepage | Y | 76 | String | Single | A URL such as http://example-example.com |
| WebVPN-Deny-Message | Y | 116 | String | Single | Valid string (up to 500 characters) |
| WebVPN-Download-Max-Size | Y | 157 | Integer | Single | 0x7fffffff |
| WebVPN-File-Access-Enable | Y | 94 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-File-Save-Dialog-Enable | Y | 96 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-File-Save-Entry-Enable | Y | 95 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Group-HTTP-Proxy-Exempt | Y | 78 | String | Single | Comma-separated DNS/IP with an optional wildcard (*) (for example *.cisco.com, 192.168.1.*, wwwin.cisco.com) |
| WebVPN-Hidden-Shares | Y | 126 | Integer | Single | 0 = None 1 = Visible |
| WebVPN-Image-Page-Size-Enable | Y | 228 | Boolean | Single | Enabled if clientless home page is to be rendered through Smart Tunnel. |
| WebVPN-HTML-Filter | Y | 69 | Bitmap | Single | 1 = Java ActiveX 2 = Scripts 4 = Image 8 = Cookies |

Supported RADIUS Authorization Attributes

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|--------------------------------------|-----|-----------|-------------|------------------------|--|
| WebVPN-HTTP-Compression | Y | 120 | Integer | Single | 0 = Off 1 = Deflate Compression |
| WebVPN-HTTP-Proxy-Paths | Y | 74 | String | Single | Comma-separated DNS/IP:port, with http= or https= prefix (for example http=10.10.10.10:80, https=11.11.11.11:443) |
| WebVPN-Idle-Timeout-Alert | Y | 148 | Integer | Single | 0-30. 0 = Disabled. |
| WebVPN-Keepalive-Ignore | Y | 121 | Integer | Single | 0-900 |
| WebVPN-Macro-Substitution | Y | 223 | String | Single | Unbounded. |
| WebVPN-Macro-Substitution | Y | 224 | String | Single | Unbounded. |
| WebVPN-Port-Forwarding-Enable | Y | 97 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Port-Forwarding-Exchange-File | Y | 98 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Port-Forwarding-HTTP-Proxy | Y | 99 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Port-Forwarding-List | Y | 72 | String | Single | Port forwarding list name |
| WebVPN-Port-Forwarding-Name | Y | 79 | String | Single | String name (example, "Corporate-Apps"). This text replaces the default string, "Application Access," on the clientless portal home page. |
| WebVPN-Post-Max-Size | Y | 159 | Integer | Single | 0x7ffffff |
| WebVPN-Session-Timeout-Alert | Y | 149 | Integer | Single | 0-30. 0 = Disabled. |
| WebVPN-Smart-Card-Removal-Disconnect | Y | 225 | Boolean | Single | 0 = Disabled 1 = Enabled |
| WebVPN-Smart-Tunnel | Y | 136 | String | Single | Name of a Smart Tunnel |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|---|-----|-----------|-------------|------------------------|--|
| WebVPN-SmartTunnel-AutoSignOn | Y | 139 | String | Single | Name of a Smart Tunnel auto sign-on list appended by the domain name |
| WebVPN-SmartTunnel-AutoStart | Y | 138 | Integer | Single | 0 = Disabled 1 = Enabled 2 = Auto Start |
| WebVPN-SmartTunnel-Exclude | Y | 227 | String | Single | One of “e networkname,” “i networkname,” or “a,” where networkname is the name of a Smart Tunnel network list, e indicates the tunnel excluded, i indicates the tunnel specified, and a indicates all tunnels. |
| WebVPN-SSL-VPN-Client-Enabled | Y | 103 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-SSL-VPN-Client-Keep-Installation | Y | 105 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-SSL-VPN-Client-Require | Y | 104 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-SSO-Server-Name | Y | 114 | String | Single | Valid string |
| WebVPN-Storage-Key | Y | 162 | String | Single | |
| WebVPN-Storage-Objects | Y | 161 | String | Single | |
| WebVPN-SVC-Keep-Interval | Y | 107 | Integer | Single | 15-600 seconds, 0=Off |
| WebVPN-SVC-Idle-Timeout | Y | 108 | Integer | Single | 5-3600 seconds, 0=Off |
| WebVPN-SVC-DILS-Enabled | Y | 123 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-SVC-DILS-MTU | Y | 125 | Integer | Single | MTU value is from 256-1406 bytes. |
| WebVPN-SVC-Idle-Timeout | Y | 109 | Integer | Single | 5-3600 seconds, 0=Off |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|----------------------------|-----|-----------|-------------|------------------------|----------------------------------|
| WebVPN-SVC-Rekey-Time | Y | 110 | Integer | Single | 4-10080 minutes, 0=Off |
| WebVPN-SVC-Rekey-Methd | Y | 111 | Integer | Single | 0 (Off), 1 (SSL), 2 (New Tunnel) |
| WebVPN-SVC-Compression | Y | 112 | Integer | Single | 0 (Off), 1 (Deflate Compression) |
| WebVPN-UNIX-Group-ID (GID) | Y | 222 | Integer | Single | Valid UNIX group IDs |
| WebVPN-UNIX-User-ID (UIDs) | Y | 221 | Integer | Single | Valid UNIX user IDs |
| WebVPN-Upload-Max-Size | Y | 158 | Integer | Single | 0x7fffffff |
| WebVPN-URL-Entry-Enable | Y | 93 | Integer | Single | 0 = Disabled 1 = Enabled |
| WebVPN-URL-List | Y | 71 | String | Single | URL list name |
| WebVPN-User-Storage | Y | 160 | String | Single | |
| WebVPN-VDI | Y | 163 | String | Single | List of settings |

Supported IETF RADIUS Authorization Attributes

The following table lists the supported IETF RADIUS attributes.

Table 2: Supported IETF RADIUS Attributes

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|-------------------|-----|-----------|-------------|------------------------|---|
| IETF-Radius-Class | Y | 25 | | Single | <p>For Versions 8.2.x and later, we recommend that you use the Group-Policy attribute (VSA 3076, #25):</p> <ul style="list-style-type: none"> • <i>group policy name</i> • <i>OU=group policy name</i> • <i>OU=group policy name</i> |

| Attribute Name | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value |
|-------------------------------|-----|-----------|-------------|------------------------|---|
| IETF-Radius-Filter-Id | Y | 11 | String | Single | ACL name that is defined on the ASA, which applies only to full tunnel IPsec and SSL VPN clients. |
| IETF-Radius-Framed-IP-Address | Y | n/a | String | Single | An IP address |
| IETF-Radius-Framed-IP-Netmask | Y | n/a | String | Single | An IP address mask |
| IETF-Radius-Idle-Timeout | Y | 28 | Integer | Single | Seconds |
| IETF-Radius-Service-Type | Y | 6 | Integer | Single | Seconds. Possible Service Type values: <ul style="list-style-type: none"> • Administrative-User is allowed access to the configure prompt. • NAS-Port-User is allowed access to the exec prompt. • remote-access-User is allowed network access |
| IETF-Radius-Session-Timeout | Y | 27 | Integer | Single | Seconds |

RADIUS Accounting Disconnect Reason Codes

These codes are returned if the ASA encounters a disconnect when sending packets:

Disconnect Reason Code

ACCT_DISC_USER_REQ = 1

ACCT_DISC_LOST_CARRIER = 2

ACCT_DISC_LOST_SERVICE = 3

ACCT_DISC_IDLE_TIMEOUT = 4

ACCT_DISC_SESS_TIMEOUT = 5

ACCT_DISC_ADMIN_RESET = 6

Disconnect Reason Code

ACCT_DISC_ADMIN_REBOOT = 7

ACCT_DISC_PORT_ERROR = 8

ACCT_DISC_NAS_ERROR = 9

ACCT_DISC_NAS_REQUEST = 10

ACCT_DISC_NAS_REBOOT = 11

ACCT_DISC_PORT_UNNEEDED = 12

ACCT_DISC_PORT_PREEMPTED = 13

ACCT_DISC_PORT_SUSPENDED = 14

ACCT_DISC_SERV_UNAVAIL = 15

ACCT_DISC_CALLBACK = 16

ACCT_DISC_USER_ERROR = 17

ACCT_DISC_HOST_REQUEST = 18

ACCT_DISC_ADMIN_SHUTDOWN = 19

ACCT_DISC_SA_EXPIRED = 21

ACCT_DISC_MAX_REASONS = 22

Guidelines for RADIUS Servers for AAA

This section describes the guidelines and limitations that you should check before configuring RADIUS servers for AAA.

- You can have up to 200 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 8 servers in multiple mode.

Configure RADIUS Servers for AAA

This section describes how to configure RADIUS servers for AAA.

Procedure

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

- If you are using Cisco ACS: the server already has these attributes integrated. You can skip this step.
- For RADIUS servers from other vendors (for example, Microsoft Internet Authentication Service): you must manually define each ASA attribute. To define an attribute, use the attribute name or number, type, value, and vendor code (3076).

Step 2 [Configure RADIUS Server Groups, on page 19.](#)

Step 3 [Add a RADIUS Server to a Group, on page 22.](#)

Configure RADIUS Server Groups

If you want to use an external RADIUS server for authentication, authorization, or accounting, you must first create at least one RADIUS server group per AAA protocol and add one or more servers to each group.

Procedure

Step 1 Create the RADIUS AAA server group.

aaa-server *group_name* **protocol radius**

Example:

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group) #
```

When you enter the **aaa-server protocol** command, you enter aaa-server group configuration mode.

Step 2 (Optional.) Specify the maximum number of failed AAA transactions with a RADIUS server in the group before trying the next server.

max-failed-attempts *number*

The range is from 1 and 5. The default is 3.

If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, or their responses are invalid, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the **reactivation-mode** command in the next step.

If you do not have a fallback method, the ASA continues to retry the servers in the group.

Example:

```
ciscoasa(config-aaa-server-group) # max-failed-attempts 2
```

Step 3 (Optional.) Specify the method (reactivation policy) by which failed servers in a group are reactivated.

reactivation-mode {**depletion** [*deadtime minutes*] | **timed**}

Where:

- **depletion** [**deadtime** *minutes*] reactivates failed servers only after all of the servers in the group are inactive. This is the default reactivation mode. You can specify the amount of time, between 0 and 1440 minutes, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes.
- **timed** reactivates failed servers after 30 seconds of down time.

Example:

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

Step 4 (Optional.) Send accounting messages to all servers in the group.

accounting-mode simultaneous

To restore the default of sending messages only to the active server, enter the **accounting-mode single** command.

Example:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Step 5 (Optional.) Enable the periodic generation of RADIUS interim-accounting-update messages.

interim-accounting-update [**periodic** [*hours*]]

ISE maintains a directory of active sessions based on the accounting records that it receives from NAS devices like the ASA. However, if ISE does not receive any indication that the session is still active (accounting message or posture transactions) for a period of 5 days, it will remove the session record from its database. To ensure that long-lived VPN connections are not removed, configure the group to send periodic interim-accounting-update messages to ISE for all active sessions.

- **periodic** [*hours*] enables the periodic generation and transmission of accounting records for every VPN session that is configured to send accounting records to the server group in question. You can optionally include the interval, in hours, for sending these updates. The default is 24 hours, the range is 1 to 120.
- (No parameters.) If you use this command without the **periodic** keyword, the ASA sends interim-accounting-update messages only when a VPN tunnel connection is added to a clientless VPN session. When this happens the accounting update is generated in order to inform the RADIUS server of the newly assigned IP address.

Example:

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

Step 6 (Optional.) Enable the RADIUS Dynamic Authorization (ISE Change of Authorization, CoA) services for the AAA server group.

dynamic-authorization [**port** *number*]

Specifying a port is optional. The default is 1700, the range is 1024 to 65535.

When you use the server group in a VPN tunnel, the RADIUS server group will be registered for CoA notification and the ASA will listen to the port for the CoA policy updates from ISE. Enable dynamic authorization only if you are using this server group in a remote access VPN in conjunction with ISE.

Example:

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

- Step 7** (Optional.) If you do not want to use ISE for authentication, enable authorize-only mode for the RADIUS server group. (Enable authorize-only mode only if you are using this server group in a remote access VPN in conjunction with ISE.)

authorize-only

This indicates that when this server group is used for authorization, the RADIUS Access Request message will be built as an “Authorize Only” request as opposed to the configured password methods defined for the AAA server. If you do configure a common password using **radius-common-pw** command for the RADIUS server, it will be ignored.

For example, you would use authorize-only mode if you want to use certificates for authentication rather than this server group. You would still use this server group for authorization and accounting in the VPN tunnel.

Example:

```
ciscoasa(config-aaa-server-group)# authorize-only
```

- Step 8** (Optional.) Merge a downloadable ACL with the ACL received in the Cisco AV pair from a RADIUS packet.

merge-dacl {before-avpair | after-avpair}**Example:**

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

This option applies only to VPN connections. For VPN users, ACLs can be in the form of Cisco AV pair ACLs, downloadable ACLs, and an ACL that is configured on the ASA. This option determines whether or not the downloadable ACL and the AV pair ACL are merged, and does not apply to any ACLs configured on the ASA.

The default setting is **no merge dacl**, which specifies that downloadable ACLs will not be merged with Cisco AV pair ACLs. If both an AV pair and a downloadable ACL are received, the AV pair has priority and is used.

The **before-avpair** option specifies that the downloadable ACL entries should be placed before the Cisco AV pair entries.

The **after-avpair** option specifies that the downloadable ACL entries should be placed after the Cisco AV pair entries.

Examples

The following example shows how to add one RADIUS group with a single server:

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
```

```
ciscoasa(config-aaa-server-host)# exit
```

The following example shows how to configure an ISE server group for dynamic authorization (CoA) updates and hourly periodic accounting. Included is the tunnel group configuration that configures password authentication with ISE.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. Include the authorize-only command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Add a RADIUS Server to a Group

To add a RADIUS server to a group, perform the following steps:

Procedure

Step 1

Identify the RADIUS server and the AAA server group to which it belongs.

```
aaa-server server_group [(interface_name)] host server_ip
```

Example:

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

If you do not specify an (*interface_name*), then the ASA uses the **inside** interface by default.

Step 2 Specify how the ASA treats netmasks received in a downloadable ACL from a RADIUS server.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

Example:

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

The **auto-detect** keyword specifies that the ASA should attempt to determine the type of netmask expression used. If the ASA detects a wildcard netmask expression, it converts it to a standard netmask expression.

The **standard** keyword specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.

The **wildcard** keyword specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions and converts them all to standard netmask expressions when the ACLs are downloaded.

Step 3 Specify a common password to be used for all users who are accessing a RADIUS authorization server through the ASA.

radius-common-pw *string*

Example:

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

The *string* argument is a case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with the RADIUS server.

Step 4 Enable MS-CHAPv2 authentication requests to the RADIUS server.

mschapv2-capable

Example:

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

Step 5 Specify the timeout value for connection attempts to the server.

timeout *seconds*

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the interval defined on the **retry-interval** command) until the timeout is reached. If the number of consecutive failed transactions reaches the limit specified on the **max-failed-attempts** command in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Example:

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Step 6 Configure the amount of time between retry attempts for a particular AAA server designated in a previous command.

retry-interval *seconds*

Example:

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

The *seconds* argument specifies the retry interval (1-10 seconds) for the request. This is the time that the ASA waits before retrying a connection request.

Note For the RADIUS protocol, if the server responds with an ICMP Port Unreachable message, the *retry-interval* setting is ignored and the AAA server is immediately moved to the failed state. If this is the only server in the AAA group, it is reactivated and another request is sent to it. This is the intended behavior.

Step 7 Send accounting messages to all servers in the group.

accounting-mode simultaneous

Example:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Enter the **accounting-mode single** command to restore the default of sending messages only to the active server.

Step 8 Specify the authentication port as port number 1645, or the server port to be used for authentication of users.

authentication-port *port*

Example:

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

Step 9 Specify the accounting port as port number 1646, or the server port to be used for accounting for this host.

accounting-port *port*

Example:

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

Step 10 Specify the server secret value used to authenticate the RADIUS server to the ASA. The server secret that you configure should match the one configured on the RADIUS server. If you do not know the server secret value, ask the RADIUS server administrator. The maximum length is 64 characters.

key

Example:

```
ciscoasa(config-aaa-host)# key myexamplekey1
```


The server secret that you configure should match the one configured on the RADIUS server. If you do not know the server secret value, ask the RADIUS server administrator. The maximum length is 64 characters.

Example

The following example shows how to add a RADIUS server to an existing RADIUS server group:

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexamplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Monitoring RADIUS Servers for AAA

See the following commands for monitoring the status of RADIUS servers for AAA:

- **show aaa-server**

This command shows the configured RADIUS server statistics. You can use the **clear aaa-server statistics** command to reset the counters to zero.

- **show running-config aaa-server**

This command shows the RADIUS server running configuration.

History for RADIUS Servers for AAA

Table 3: History for RADIUS Servers for AAA

| Feature Name | Platform Releases | Description |
|---|-------------------|---|
| RADIUS Servers for AAA | 7.0(1) | <p>Describes how to configure RADIUS servers for AAA.</p> <p>We introduced the following commands:</p> <p>aaa-server protocol, max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, show aaa-server, show running-config aaa-server, clear aaa-server statistics, authentication-port, accounting-port, retry-interval, acl-netmask-convert, clear configure aaa-server, merge-dacl, radius-common-pw, key.</p> |
| Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA | 8.4(3) | <p>Four New VSAs—Tunnel Group Name (146) and Client Type (150) are sent in RADIUS access request packets from the ASA. Session Type (151) and Session Subtype (152) are sent in RADIUS accounting request packets from the ASA. All four attributes are sent for all accounting request packet types: Start, Interim-Update, and Stop. The RADIUS server (for example, ACS and ISE) can then enforce authorization and policy attributes or use them for accounting and billing purposes.</p> |
| Increased limits for AAA server groups and servers per group. | 9.13(1) | <p>You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4).</p> <p>In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged.</p> <p>We modified the following commands to accept these new limits: aaa-server, aaa-server host.</p> |