



# 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 12](#)
- [Configure RADIUS Servers for AAA, on page 12](#)
- [Test RADIUS Server Authentication and Authorization, on page 18](#)
- [Monitoring RADIUS Servers for AAA, on page 18](#)
- [History for RADIUS Servers for AAA, on page 19](#)

## About RADIUS Servers for AAA

The 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 and 2865.
- Accounting attributes defined in RFC 2139 and 2866.
- RADIUS attributes for tunneled protocol support, defined in RFC 2868 and 6929.
- 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                                                                                                                                   |
| 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-Network-Extension-Mode    | Y   | 64        | Boolean     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                                        |
| Authenticated-User-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, GN, SN, I, GENQ, DNQ, SER, use-entire-na                                                                                             |
| 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 sessions: IPsec IKEv1, Secure Client SSL-TLS/DTLS/IKEv2, and Clientless SSL                                                       |
| Banner2                         | Y   | 36        | String      | Single                  | Banner string to display for Cisco VPN remote sessions: IPsec IKEv1, Secure Client SSL-TLS/DTLS/IKEv2, and Clientless SSL. The string is concatenated to the Banner1 string, if |
| 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 = Secure Client VPN 3 = Clientless SSL VPN 4 = Cut-Thro = L2TP/IPsec SSL VPN 6 = Secure Client II (IKEv2)                                        |

| Attribute Name                    | ASA | Attr. No. | Syntax/Type | Single or Multi- Valued | Description or Value                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------|-----|-----------|-------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client-Type-Version-Limiting      | Y   | 77        | String      | Single                  | IPsec VPN version number string                                                                                                                                                                                                                                                                                                                                                                                                    |
| DHCP-Network-Scope                | Y   | 61        | String      | Single                  | IP Address                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Extended-Authentication-On-Rekey  | Y   | 122       | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                                                                                                                                                                                                                                                                                           |
| Framed-Interface-Id               | Y   | 96        | String      | Single                  | Assigned IPv6 interface ID. Combines with Framed-IPv6-Prefix to create a complete assigned address. For example: Framed-Interface-ID=1:1:1:1 combined with Framed-IPv6-Prefix=2001:0db8::/64 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 address. For example: prefix 2001:0db8::/64 combined with Framed-Interface-Id=1:1:1:1 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, for example, Framed-IPv6-Prefix=2001:0db8::1:1:1:1/64. |
| Group-Policy                      | Y   | 25        | String      | Single                  | Sets the group policy for the remote access VPN. For Versions 8.2.x and later, use this attribute in the IETF-Radius-Class. You can use one of the following formats: <ul style="list-style-type: none"> <li>• <i>group policy name</i></li> <li>• <i>OU=group policy name</i></li> <li>• <i>OU=group policy name;</i></li> </ul>                                                                                                  |
| 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 = Concentrator Setting                                                                                                                                                                                                                                                                                                                                                                |
| IKE-KeepAlive-Confidence-Interval | Y   | 68        | Integer     | Single                  | 10-300 seconds                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IKE-Keepalive-Retry-Interval      | Y   | 84        | Integer     | Single                  | 2-10 seconds                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IKE-Keep-Alives                   | Y   | 41        | Boolean     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                                                                                                                                                                                                                                                                                           |
| Intercept-DHCP-Configure-Msg      | 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) 3 = NT Domain 4 = SDI 5 = Internal 6 = RADIUS Expiry 7 = 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 use backup list 3 = Use Backup Server list                              |
| IPsec-Client-Firewall-Filter-Name         |     | 57        | String      | Single                  | Specifies the name of the filter to be pushed to the client as firewall policy                                         |
| IPsec-Client-Firewall-Filter-Optional     | Y   | 58        | Integer     | Single                  | 0 = Required 1 = Optional                                                                                              |
| IPsec-Default-Domain                      | Y   | 28        | String      | Single                  | Specifies the single default domain name to be pushed to the client (1-255 characters).                                |
| IPsec-IKE-Peer-ID-Check                   | Y   | 40        | Integer     | Single                  | 1 = Required 2 = If supported by peer certificate, 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                                                                                               |
| IPsec-Over-UDP-Port                       | Y   | 35        | Integer     | Single                  | 4001- 49151. The default is 10000.                                                                                     |
| IPsec-Required-Client-Firewall-Capability | Y   | 56        | Integer     | Single                  | 0 = None 1 = Policy defined by remote FW 2 = Are-You-There (AYT) 3 = Policy pushed CPE 4 = Policy pushed 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 be pushed to the client (1-255 characters).                            |
| IPsec-Split-Tunneling-Policy              | Y   | 55        | Integer     | Single                  | 0 = No split tunneling 1 = Split tunneling 2 = Split tunneling is permitted                                            |
| IPsec-Split-Tunnel-List                   | Y   | 27        | String      | Single                  | Specifies the name of the network or ACL to be included in 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                                                                                                              |

| Attribute Name                        | ASA | Attr. No. | Syntax/Type | Single or Multi- Valued | Description or Value                                                                                                                                                        |
|---------------------------------------|-----|-----------|-------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2TP-Encryption                       |     | 21        | Integer     | Single                  | Bitmap: 1 = Encryption required 2 = 40 bits 4 = 8 = Stateless-Req 15= 40/128-Encr/Stateless-Re                                                                              |
| L2TP-MPPC-Compression                 |     | 38        | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                                    |
| Member-Of                             | Y   | 145       | String      | Single                  | Comma-delimited string, for example:<br><br>Engineering, Sales<br><br>An administrative attribute that can be used in d<br>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                                                                                                                                                             |
| Perfect-Forward-Secrecy-Enable        | Y   | 88        | Boolean     | Single                  | 0 = No 1 = Yes                                                                                                                                                              |
| PPTP-Encryption                       |     | 20        | Integer     | Single                  | Bitmap: 1 = Encryption required 2 = 40 bits 4 = 8 = Stateless-Required 15= 40/128-Encr/Stateless-Re                                                                         |
| 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.                                                                                                                                                |
| Required-Client- Firewall-Vendor-Code | Y   | 45        | Integer     | Single                  | 1 = Cisco Systems (with Cisco Integrated Client<br>Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco<br>(with Cisco Intrusion Prevention Security Agent                         |
| Required-Client-Firewall-Description  | Y   | 47        | String      | Single                  | String                                                                                                                                                                      |

| Attribute Name                        | ASA | Attr. No. | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|-----|-----------|-------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Required-Client-Firewall-Product-Code | Y   | 46        | Integer     | Single                 | Cisco Systems Products:<br>1 = Cisco Intrusion Prevention Security Agent<br>Integrated Client (CIC)<br>Zone Labs Products: 1 = Zone Alarm 2 = Zone Labs Integrity<br>3 = Zone Labs Integrity<br>NetworkICE Product: 1 = BlackIce Defender<br>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                                                                                                                                                                                                                                                                                                                         |
| Session Subtype                       | Y   | 152       | Integer     | Single                 | 0 = None 1 = Clientless 2 = Client 3 = Clientless<br>Session Subtype applies only when the Session (151) attribute has the following values: 1, 2                                                                                                                                                                                |
| Session Type                          | Y   | 151       | Integer     | Single                 | 0 = None 1 = Secure Client SSL VPN 2 = Secure Client IPSec VPN (IKEv2) 3 = Clientless SSL VPN 4 = Clientless Email Proxy 5 = Cisco VPN Client 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = 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-Enable       | Y   | 139       | String      | Single                 | Name of a Smart Tunnel Auto Signon list applied to 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 clientless (2 and 4 not used)                                                                                                                                                                                                                                                        |
| 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                                                                                                                                                                                                                                                                                                          |

| Attribute Name                     | ASA | Attr. No. | Syntax/Type | Single or Multi- Valued | Description or Value                                                                                                                                        |
|------------------------------------|-----|-----------|-------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 = L2TPv3 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 = mutually exclusive. 0 - 11, 16 - 27, 32 - 43, 48 - 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                                                                                                                            |
| WebVPN-Apply-ACL                   | Y   | 102       | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                    |
| WebVPN-Auto-HTTP-Signon            | Y   | 124       | String      | Single                  | Reserved                                                                                                                                                    |
| WebVPN-Citrix-Metaframe-Enable     | Y   | 101       | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                    |
| WebVPN-Content-Filter-Parameters   | Y   | 69        | Integer     | Single                  | 1 = Java ActiveX 2 = Java Script 4 = Image 8 = 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-Server-Browsing-Enable | Y   | 96        | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                    |
| WebVPN-File-Server-Entry-Enable    | Y   | 95        | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                    |



| Attribute Name                                     | ASA | Attr. No. | Syntax/Type | Single or Multi- Valued | Description or Value                                                                                                              |
|----------------------------------------------------|-----|-----------|-------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List | Y   | 78        | String      | Single                  | Comma-separated DNS/IP with an optional v (for example *.cisco.com, 192.168.1.*, wwwin                                            |
| WebVPN-Hidden-Shares                               | Y   | 126       | Integer     | Single                  | 0 = None 1 = Visible                                                                                                              |
| WebVPN-Home-Page-Use-Smart-Tunnel                  | Y   | 228       | Boolean     | Single                  | Enabled if clientless home page is to be rende Smart Tunnel.                                                                      |
| WebVPN-HTML-Filter                                 | Y   | 69        | Bitmap      | Single                  | 1 = Java ActiveX 2 = Scripts 4 = Image 8 =                                                                                        |
| WebVPN-HTTP-Compression                            | Y   | 120       | Integer     | Single                  | 0 = Off 1 = Deflate Compression                                                                                                   |
| WebVPN-HTTP-Proxy-IP-Address                       | Y   | 74        | String      | Single                  | Comma-separated DNS/IP:port, with http= c prefix (for example http=10.10.10.10:80, https=11.11.11.11:443)                         |
| WebVPN-Idle-Timeout-Alert-Interval                 | 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-Proxy-Enable       | 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”).<br>This text replaces the default string, “Applicati on the clientless portal home page. |
| WebVPN-Post-Max-Size                               | Y   | 159       | Integer     | Single                  | 0x7fffffff                                                                                                                        |
| WebVPN-Session-Timeout-Alert-Interval              | 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                                                                                                            |
| WebVPN-Smart-Tunnel-Auto-Sign-On                   | Y   | 139       | String      | Single                  | Name of a Smart Tunnel auto sign-on list ap the domain name                                                                       |
| WebVPN-Smart-Tunnel-Auto-Start                     | Y   | 138       | Integer     | Single                  | 0 = Disabled 1 = Enabled 2 = Auto Start                                                                                           |

| Attribute Name                           | ASA | Attr. No. | Syntax/Type | Single or Multi- Valued | Description or Value                                                                                                                                                                               |
|------------------------------------------|-----|-----------|-------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WebVPN-Smart-Tunnel-Tunnel-Policy        | Y   | 227       | String      | Single                  | One of “e networkname,” “i networkname,” or “a networkname” is the name of a Smart Tunnel network. e indicates the tunnel excluded, i indicates the tunnel specified, and a indicates all tunnels. |
| WebVPN-SSL-VPN-Client-Enable             | 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-Required           | 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-Keepalive-Frequency           | Y   | 107       | Integer     | Single                  | 15-600 seconds, 0=Off                                                                                                                                                                              |
| WebVPN-SVC-Client-DPD-Frequency          | Y   | 108       | Integer     | Single                  | 5-3600 seconds, 0=Off                                                                                                                                                                              |
| WebVPN-SVC-DTLS-Enable                   | Y   | 123       | Integer     | Single                  | 0 = Disabled 1 = Enabled                                                                                                                                                                           |
| WebVPN-SVC-DTLS-MTU                      | Y   | 125       | Integer     | Single                  | MTU value is from 256-1406 bytes.                                                                                                                                                                  |
| WebVPN-SVC-Gateway-DPD-Frequency         | Y   | 109       | Integer     | Single                  | 5-3600 seconds, 0=Off                                                                                                                                                                              |
| WebVPN-SVC-Rekey-Time                    | Y   | 110       | Integer     | Single                  | 4-10080 minutes, 0=Off                                                                                                                                                                             |
| WebVPN-SVC-Rekey-Method                  | 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                 | For Versions 8.2.x and later, we recommend that you use the Group-Policy attribute (VSA 3076, #25): <ul style="list-style-type: none"> <li>• <i>group policy name</i></li> <li>• <i>OU=group policy name</i></li> <li>• <i>OU=group policy name</i></li> </ul>                        |
| 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"> <li>• .Administrative—User is allowed access to the configure prompt.</li> <li>• .NAS-Prompt—User is allowed access to the exec prompt.</li> <li>• .remote-access—User is allowed network access</li> </ul> |
| 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

ACCT\_DISC\_ADMIN\_REBOOT = 7

**Disconnect Reason Code**

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.
- The maximum length of the RADIUS payload is 4096 bytes.

## 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 13.](#)
- Step 3**     [Add a RADIUS Server to a Group, on page 15.](#)
- Step 4**     (Optional) [Add an Authentication Prompt, on page 17.](#)

## 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**     Choose **Configuration > Device Management > Users/AAA > AAA Server Groups**.
- Step 2**     Click **Add** in the **AAA Server Groups** area.
- The **Add AAA Server Group** dialog box appears.
- Step 3**     Enter a name for the group in the **AAA Server Group** field.
- Step 4**     Choose the RADIUS server type from the **Protocol** drop-down list.
- Step 5**     Select the **Accounting Mode**.
- **Simultaneous**—Send accounting data to all servers in the group.
  - **Single**—Send accounting data to only one server.
- Step 6**     Configure the method (**Reactivation Mode**) by which failed servers in a group are reactivated.
- **Depletion, Dead Time**—Reactivate failed servers only after all of the servers in the group are inactive. This is the default reactivation mode. 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. Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses. The default is 10 minutes.
  - **Timed**—Reactivate failed servers after 30 seconds of down time.
- Step 7**     In **Max Failed Attempts**, specify the maximum number of failed AAA transactions with a RADIUS server in the group before trying the next server.
- The range is from 1 and 5. The default is 3.
- If you configure 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 (if you use the default reactivation mode and dead time), 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 change the **Dead Time**.

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

**Step 8** (Optional.) Enable the periodic generation of RADIUS interim-accounting-update messages by selecting the desired options.

These options are relevant only if you are using this server group for Secure Client or clientless SSL VPN.

- **Enable interim accounting update**—If you use this command without selecting the **Update Interval** option, 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.
- **Update Interval**—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 change the interval, in hours, for sending these updates. The default is 24 hours, the range is 1 to 120.

**Note**

For server groups containing ISE servers, select both options. 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.

**Step 9** (Optional.) If this group contains AD Agents or Cisco Directory Agent (CDA) servers only, select **Enable Active Directory Agent Mode**.

CDA or AD Agents are used in identity firewall, and are not full-featured RADIUS servers. If you select this option, you can use this group for identity firewall purposes only.

**Step 10** (Optional) If you are using this server group for ISE Policy Enforcement in remote access VPN, configure the following options:

- **Enable dynamic authorization**—Enable the RADIUS Dynamic Authorization (ISE Change of Authorization, CoA) services for the AAA server group. 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.
- **Dynamic Authorization Port**—If you enable dynamic authorization, you can specify the listening port for RADIUS CoA requests. The default is 1700. The valid range is 1024 to 65535.
- **Use authorization only mode**—If you do not want to use ISE for authentication, enable authorize-only mode for the RADIUS server group. 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 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.

- Step 11** (Optional.) Configure the **VPN3K Compatibility Option** to specify whether or not a downloadable ACL received from a RADIUS packet should be merged with a Cisco AV pair ACL.
- 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.
- **Do not merge** —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. This is the default option.
  - **Place the downloadable ACL after Cisco AV-pair ACL**
  - **Place the downloadable ACL before Cisco AV-pair ACL**
- Step 12** Click **OK**.
- The **Add AAA Server Group** dialog box closes, and the new server group is added to the **AAA Server Groups** table.
- Step 13** Click **Apply** to save the changes to the running configuration.
- 

## Add a RADIUS Server to a Group

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

### Procedure

- 
- Step 1** Choose **Configuration > Device Management > Users/AAA > AAA Server Groups**, and in the **AAA Server Groups** area, click the server group to which you want to add a server.
- Step 2** Click **Add** in the **Servers in the Selected Group** area (lower pane).
- The **Add AAA Server Group** dialog box appears for the server group.
- Step 3** Choose the interface name on which the authentication server resides.
- Step 4** Add either a server name or IP address for the server that you are adding to the group.
- Step 5** Specify the timeout value for connection attempts to the server.
- 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 retry interval) until the timeout is reached. If the number of consecutive failed transactions reaches the maximum-failed-attempts limit specified in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.
- Step 6** Select **Require message authenticator from RADIUS Server** to specify that the Message-Authenticator attribute must be present in RADIUS requests and responses.
- The Message-Authenticator attribute is used to protect against Blast-RADIUS attacks. If you have upgraded your RADIUS server so it supports the message authenticator, you can enable this option to help protect against these attacks. When enabled, all requests and responses must have the message authenticator, or authentication will fail.

- Step 7** Specify how you want the ASA to handle netmasks received in downloadable ACLs. Choose from the following options:
- **Detect automatically**—The ASA attempts to determine the type of netmask expression used. If the ASA detects a wildcard netmask expression, the ASA converts it to a standard netmask expression.
- Note**  
Because some wildcard expressions are difficult to detect clearly, this setting may misinterpret a wildcard netmask expression as a standard netmask expression.
- **Standard**—The ASA assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.
  - **Wildcard**—The ASA assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions, and it converts them all to standard netmask expressions when the ACLs are downloaded.
- Step 8** Specify a case-sensitive password that is common among users who access this RADIUS authorization server through this ASA. Be sure to provide this information to your RADIUS server administrator.
- Note**  
For an authentication RADIUS server (rather than authorization), do not configure a common password.  
If you leave this field blank, the username is the password for accessing this RADIUS authorization server.  
Never use a RADIUS authorization server for authentication. Common passwords or usernames as passwords are less secure than assigning unique user passwords.  
Although the password is required by the RADIUS protocol and the RADIUS server, users do not need to know it.
- Step 9** 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 unchecking this check box.
- Step 10** Specify the length of time, from 1 to 10 seconds, that the ASA waits between attempts to contact the server.
- 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 11** Click **Simultaneous** or **Single**.
- In Single mode, the ASA sends accounting data to only one server.  
In Simultaneous mode, the ASA sends accounting data to all servers in the group.
- Step 12** Specify the server port to be used for accounting of users. The default port is 1646.
- Step 13** Specify the server port to be used for authentication of users. The default port is 1645.
- Step 14** Specify the shared secret key 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, ask the RADIUS server administrator. The maximum field length is 64 characters.
- Step 15** Click **OK**.



The **Add AAA Server Group** dialog box closes, and the AAA server is added to the AAA server group.

**Step 16** In the **AAA Server Groups** pane, click **Apply** to save the changes to the running configuration.

## Add an Authentication Prompt

You can specify the AAA challenge text for HTTP, FTP, and Telnet access through the ASA when requiring user authentication from RADIUS servers. This text is primarily for cosmetic purposes and appears above the username and password prompts that users see when they log in. If you do not specify an authentication prompt, users see the following when authenticating with a RADIUS server:

| Connection Type | Default Prompt      |
|-----------------|---------------------|
| FTP             | FTP authentication  |
| HTTP            | HTTP authentication |
| Telnet          | None                |

To add an authentication prompt, perform the following steps:

### Procedure

**Step 1** Choose **Configuration > Device Management > Users/AAA > Authentication Prompt**.

**Step 2** Enter text in the **Prompt** field to add as a message to appear above the username and password prompts that users see when they log in.

The following table shows the allowed character limits for authentication prompts:

| Application                 | Character Limit |
|-----------------------------|-----------------|
| Microsoft Internet Explorer | 37              |
| Telnet                      | 235             |
| FTP                         | 235             |

**Step 3** Add messages in the **User accepted message** and **User rejected message** fields.

If the user authentication occurs from Telnet, you can use the **User accepted message** and **User rejected message** options to display different status prompts to indicate that the authentication attempt is either accepted or rejected by the RADIUS server.

If the RADIUS server authenticates the user, the ASA displays the **User accepted message** text, if specified, to the user; otherwise, the ASA displays the **User rejected message** text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The **User accepted message** and **User rejected message** text are not displayed.

**Step 4** Click **Apply** to save the changes to the running configuration.

# Test RADIUS Server Authentication and Authorization

To determine whether the ASA can contact a RADIUS server and authenticate or authorize a user, perform the following steps:

## Procedure

---

**Step 1** Choose **Configuration > Device Management > Users/AAA > AAA Server Groups**.

**Step 2** Click the server group in which the server resides in the **AAA Server Groups** table.

**Step 3** Click the server that you want to test in the **Servers in the Selected Group** table.

**Step 4** Click **Test**.

The **Test AAA Server** dialog box appears for the selected server.

**Step 5** Click the type of test that you want to perform—**Authentication** or **Authorization**.

**Step 6** Enter a username.

**Step 7** Enter the password for the username if you are testing authentication.

**Step 8** Click **OK**.

The ASA sends an authentication or authorization test message to the server. If the test fails, an error message appears.

---

## Monitoring RADIUS Servers for AAA

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

- **Monitoring > Properties > AAA Servers**

This pane shows the RADIUS server running configuration.

- **Tools > Command Line Interface**

This pane allows you to issue various non-interactive commands and view results.

# 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 screens:</p> <p>Configuration &gt; Device Management &gt; Users/AAA &gt; AAA Server Groups Configuration &gt; Device Management &gt; Users/AAA &gt; Authentication Prompt.</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 AAA screens to accept these new limits.</p>          |
| Support for the RADIUS Message-Authenticator attribute.                                                         | 9.23(1)           | <p>The Message-Authenticator attribute is used to protect against Blast-RADIUS attacks. If you have upgraded your RADIUS server so it supports the message authenticator, you can enable this option to help protect against these attacks. When enabled, all requests and responses must have the message authenticator, or authentication will fail.</p> <p>We added the <b>Require message authenticator from RADIUS Server</b> option to the Add/Edit RADIUS Server dialog box.</p>       |

