

Appendix: FlexVPN RADIUS Attributes

This chapter describes the RADIUS attributes supported by FlexVPN server.

- FlexVPN RADIUS Attributes, on page 1

FlexVPN RADIUS Attributes

The following are the RADIUS attributes categories used by FlexVPN Server:

- Inbound and bidirectional IETF RADIUS attributes
- Outbound Local
- Outbound Remote

Note For inbound attributes sent by the FlexVPN server to RADIUS that are not listed below, the value is set by the AAA system.

Attribute	User-Name
Type	IETF
Format	String
Attribute ID	1
Description	This attribute is sent by the FlexVPN server to Radius and is derived as follows: • AAA based preshared keys—Peer IKEv2 identity • EAP authentication—Peer EAP identity • User or group authorization—Output of the name mangler or the string specified in the IKEv2 profile authorization commands • Accounting—Peer EAP identity or IKEv2 identity This attribute may also be received from Radius in Access-Accept after successful EAP authentication and specifies the authenticated peer EAP identity.

Attribute	User-Password
Type	IETF
Format	String
Attribute ID	2
Description	This attribute is sent by the FlexVPN server to RADIUS and is derived as follows: • AAA based preshared keys—“cisco” • User/group authorization—“cisco”

Attribute	Calling-Station-ID
Type	IETF
Format	String
Attribute ID	31
Description	This attribute is sent by FlexVPN server to RADIUS and is derived as follows: • AAA based pre-shared keys—IKEv2 initiator address • EAP authentication—IKEv2 initiator address • User/group authorization—IKEv2 initiator address

Attribute	Service-Type
Type	IETF
Format	String
Attribute ID	6
Description	This attribute is used by FlexVPN server for EAP authentication and the value of this attribute is set to ‘Login’.

Attribute	EAP-Message
Type	IETF
Format	String
Attribute ID	79
Description	This attribute is used by FlexVPN server for EAP authentication to relay EAP packets between EAP server and the Remote Access Client.

Attribute	Message-Authenticator

Type	IETF
Format	String
Attribute ID	80
Description	This attribute is sent by FlexVPN server for EAP authentication. The value for this attribute is set by AAA subsystem.

Attribute	Framed-Pool
Type	IETF
Format	String
Attribute ID	88
Local config	pool name
Radius config	Framed-Pool=*pool-name*
Description	Specifies the name of IPv4 address pool that is used by FlexVPN server to allocate the IPv4 address to assign to the client. The allocated address is pushed to client via IKEv2 standard config attribute INTERNAL_IP4_ADDRESS.

Attribute	ipsec:group-dhcp-server
Type	Cisco AV Pair
Format	String
Local config	dhcp server {*ipddr* | *host*}
Radius config	cisco-avpair="ipsec: group-dhcp-server=*ipaddr*"
Description	Specifies the IPv4 DHCP server that is used by FlexVPN server to lease IPv4 address to assign to the client. The leased address is pushed to client via IKEv2 standard config attribute INTERNAL_IP4_ADDRESS.

Attribute	ipsec:dhcp-giaddr
Type	Cisco AV Pair
Format	IPaddr
Local config	dhcp giaddr ipaddr
Radius config	cisco-avpair="psec: dhcp-giaddr=*ipaddr*"
Description	Specifies the IPv4 DHCP gateway IP address that is used by FlexVPN server to contact the DCHP server.

Attribute	ipsec:dhcp-timeout

Type	Cisco AV Pair
Format	Integer
Local config	dhcp timeout *seconds*
Radius config	cisco-avpair="ipsec:dhcp-timeout=*seconds*"
Description	Specifies the time to wait for response from IPv4 DHCP server that is used by FlexVPN server to timeout response from the DHCP server.

Attribute	ipsec:ipv6-addr-pool
Type	Cisco AV Pair
Format	String
Local config	ipv6 *pool name*
Radius config	cisco-avpair="ipsec:ipv6-addr-pool=*pool-name*"
Description	Specifies the name of IPv6 address pool used by FlexVPN server to allocate the IPv6 address to assign to the client. The allocated address is pushed to the client via IKEv2 standard config attribute INTERNAL_IP6_ADDRESS.

Attribute	ipsec:route-set=prefix
Type	Cisco AV Pair
Format	String
Local config	N/A
Radius config	cisco-avpair="ipsec:route-set=prefix *prefix*/*length*"
Example	ipsec:route-set=prefix 192.168.1.0/24
Description	Specifies a subnet protected by FlexVPN server. This is pushed to the client via IKEv2 standard configuration attribute INTERNAL_IP4_SUBNET. **Note** This AV pair was introduced in Cisco IOS Release 15.2(2)T.

Attribute	ipsec:route-set=interface
Type	Cisco AV Pair
Format	String
Local config	route set interface
Radius config	cisco-avpair="ipsec:route-set=interface"

Description	This attribute is used locally and enables sending of VPN interface IP address to the peer via IKEv2 standard config attribute INTERNAL_IP4_SUBNET. This allows running routing protocols such as BGP over VPN. **Note** In Cisco IOS Release 15.2(2)T, this AV pair replaced the “ipsec:route-set-interface” AV pair.

Attribute	ipsec:route-accept
Type	Cisco AV Pair
Format	String
Local config	route accept any [tag *tag-id*] [distance *distance*]
Radius config	cisco-avpair=“ipsec:route-accept=any [tag:*tag*] [distance:*distance*]”
Example	ipsec:route-accept=any tag=100
Description	This attribute is used locally and specifies the filter for the subnets received from the peer via IKEv2 standard config attribute INTERNAL_IP4_SUBNET. The attribute also specifies the tag and distance for the routes added by IKEv2 for the filtered subnets. **Note** In Cisco IOS Release 15.2(2)T, the AV pair “ipsec:route-accept=any” replaced “ipsec:route-accept=accept acl:any” and the AV pair “ipsec:route-accept=none” replaced “ipsec:route-accept=deny”.

Attribute	ipsec:ipsec-flow-limit
Type	Cisco AV Pair
Format	Integer
Local config	ipsec flow-limit *limit*
Radius config	cisco-avpair=“ipsec:ipsec-flow-limit=*limit*”
Description	This attribute is used by FlexVPN server and specifies the maximum number of IPsec SAs that an IPSec dVTI session can have. There is no limit by default. This parameter is similar to the **crypto ipsec profile** and **set security-policy limit** commands.

Attribute	ip:interface-config
Type	Cisco AV Pair
Format	String
Local config	aaa attribute list *list* attribute type interface-config *string*
Radius config	cisco-avpair=“ip:interface-config=interface cmd string”

Example	ip:interface-config=ip vrf forwarding red
Description	This attribute is used locally and specifies an interface configuration mode command string that is applied on the virtual access interface for the session. For local configuration, the IKEv2 authorization policy points to an AAA attribute list that must have interface-config attribute.

Attribute	Tunnel-Type
Type	IETF
Format	Integer
Attribute ID	64
Radius config	Tunnel-Type=type
Description	This attribute specifies the tunnel type (ESP, AH, GRE, etc.) and is received when FlexVPN server fetches preshared key for the session from RADIUS server.

Attribute	Tunnel-Medium-Type
Type	IETF
Format	Integer
Attribute ID	65,
Radius config	Tunnel-Medium-Type=type
Description	This attribute specifies the tunnel transport type (IPv4, IPv6, etc.) and is received when FlexVPN server fetches preshared key for the session from the RADIUS server.

Attribute	Tunnel-Password
Type	IETF
Format	String
Attribute ID	69
Radius config	Tunnel-Password=string
Description	This attribute specifies the symmetric preshared key and is received when FlexVPN server fetches preshared key for the session from RADIUS server.

Attribute	ipsec:ikev2-password-local
Type	Cisco AV Pair
Format	String
Radius config	cisco-avpair="ipsec:ikev2-password-local=*string*"

Description	This attribute specifies the local preshared key and is received when FlexVPN server fetches preshared key for the session from RADIUS server.

Attribute	ipsec:ikev2-password-remote
Type	Cisco AV Pair
Format	String
Radius config	cisco-avpair="ipsec:ikev2-password-remote=*string*"
Description	This attribute specifies the remote preshared key and is received when FlexVPN server fetches preshared key for the session from RADIUS server.

Attribute	Framed-IP-Address
Type	IETF
Format	IPaddr
Attribute ID	8
Radius config	Framed-IP-Address=*ipaddr*
Description	Specifies IPv4 address assigned to the client. This is pushed to the client via IKEv2 standard configuration attribute INTERNAL_IP4_ADDRESS.

Attribute	Framed-IP-Netmask
Type	IETF
Format	IPaddr
Attribute ID	9
Local config	netmask *mask*
Radius config	Framed-IP-Netmask=*mask*
Description	Specifies the subnet mask of the IPv4 address assigned to the client. This is pushed to client via IKEv2 standard configuration attribute INTERNAL_IP4_NETMASK.

Attribute	ipsec:dns-servers
Type	Cisco AV Pair
Format	String
Local config	dns *primary* [*secondary*]
Radius config	cisco-avpair="ipsec:dns-servers=*primary secondary*"
Description	Specifies the primary and secondary IPv4 DNS servers for the client. This is pushed to the client via IKEv2 standard config attribute INTERNAL_IP4_DNS.

Attribute	ipsec:wins-servers
Type	Cisco AV Pair
Format	String
Local config	wins *primary* [*secondary*]
Radius config	cisco-avpair="ipsec:wins-servers=*primary secondary*"
Description	Specifies the primary and secondary IPv4 WINS servers for the client. This is pushed to the client via IKEv2 standard configuration attribute INTERNAL_IP4_NBNS.

Attribute	ipsec:route-set=access-list
Type	Cisco AV Pair
Format	String
Local config	route set access-list {*acl-name* | *acl-number*}
Radius config	cisco-avpair="ipsec:route-set=access-list {*acl-name* | *acl-number*}"
Description	Specifies the IPv4 subnets protected by FlexVPN server. This is pushed to the client via IKEv2 standard configuration attribute INTERNAL_IP4_SUBNET. **Note** In Cisco IOS Release 15.2(2)T, this AV pair replaced the "ipsec:inacl" AV pair.

Attribute	ipsec:addrv6
Type	Cisco AV Pair
Format	String
Radius config	cisco-avpair="ipsec:addrv6=*ipv6-addr*"
Description	Specifies the IPv6 address assigned to the client. This is pushed to client via IKEv2 standard configuration attribute INTERNAL_IP6_ADDRESS in the first 16 bytes.

Attribute	ipsec:prefix-len
Type	Cisco AV Pair
Format	Integer
Local config	N/A
Radius config	cisco-avpair="ipsec:prefix-len=*value*"
Example	ipsec:prefix-len=24

Description	Specifies the prefix length of the IPv6 address assigned to the client. This is pushed to client via IKEv2 standard configuration attribute INTERNAL_IP6_ADDRESS in the last (17^{th}) byte.

Attribute	ipsec:ipv6-dns-servers-addr
Type	Cisco AV Pair
Format	String
Local config	ipv6 dns *primary* [*secondary*]
Radius config	cisco-avpair="ipsec: ipv6-dns-servers-addr=ipaddr1 *ipaddr2"
Description	Specifies the primary and secondary IPv6 DNS servers for the client. This is pushed to the client via IKEv2 standard configuration attribute INTERNAL_IP6_DNS.

Attribute	ipsec:route-set=access-list ipv6
Type	Cisco AV Pair
Format	String
Local config	route set access-list ipv6 acl-name
Radius config	cisco-avpair="ipsec:route-set=access-list ipv6 *acl-name*"
Description	Specifies IPv6 subnets protected by the FlexVPN server. This is pushed to the client via IKEv2 standard configuration attribute INTERNAL_IP6_SUBNET. **Note** In Cisco IOS Release 15.2(2)T, this AV pair replaced the " ipsec:ipv6-subnet-acl" AV pair.

Attribute	ipsec:banner
Type	Cisco AV Pair
Format	String
Local config	banner *text*
Radius config	cisco-avpair="ipsec:banner=*text*"
Description	Specifies the banner text. This is pushed to the client via Cisco Unity attribute MODECFG_BANNER.

Attribute	ipsec:default-domain
Type	Cisco AV Pair
Format	String
Local config	def-domain *name*

Radius config	cisco-avpair="ipsec:default-domain=*name*"
Description	Specifies the default domain. This is pushed to the client via Cisco Unity attribute MODECFG_DEFDOMAIN.

Attribute	ipsec:split-dns
Type	Cisco AV Pair
Format	String
Local config	split-dns name
Radius config	cisco-avpair="ipsec:split-dns=name"
Description	Specifies the split DNS name. This is pushed to the client via Cisco Unity attribute MODECFG_SPLITDNS_NAME. You can configure up to 10 split DNS names.

Attribute	ipsec:ipsec-backup-gateway
Type	Cisco AV Pair
Format	String
Local config	backup-gateway *name*
Radius config	cisco-avpair="ipsec:ipsec-backup-gateway=*name*"
Description	Specifies the backup gateway. This is pushed to the client via Cisco Unity attribute MODECFG_BACKUPSERVERS. You can configure up to 10 backup gateways.

Attribute	ipsec:pfs
Type	Cisco AV Pair
Format	Integer
Local config	pfs
Radius config	cisco-avpair="ipsec:pfs=*value*"
Description	Specifies IPsec PFS (Perfect Forward Secrecy) enable/disable. This is pushed to the client via Cisco Unity attribute MODECFG_PFS. The value must be 0 to disable and 1 to enable.

Attribute	ipsec:include-local-lan
Type	Cisco AV Pair
Format	Integer
Local config	include-local-lan
Radius config	cisco-avpair="ipsec:include-local-lan=*value*"

Description	Enables or disables include local LAN. This is pushed to the client via Cisco Unity attribute MODECFG_INCLUDE_LOCAL_LAN. The value must be 0 to disable and 1 to enable.

Attribute	ipsec:smartcard-removal-disconnect
Type	Cisco AV Pair
Format	Integer
Local config	smartcard-removal-disconnect
Radius config	cisco-avpair="ipsec:smartcard-removal-disconnect =*value*"
Description	Enables or disables smartcard removal disconnect. This is pushed to the client via Cisco Unity attribute MODECFG_SMARTCARD_REMOVAL_DISCONNECT. The value must be 0 to disable and 1 to enable.

Attribute	ipsec:configuration-url
Type	Cisco AV Pair
Format	String
Local config	configuration url *url*
Radius config	cisco-avpair="ipsec:configuration-url=*url*"
Description	Specifies the URL for configuration download. This is pushed to the client via Cisco FlexVPN attribute MODECFG_CONFIG_URL.

Attribute	ipsec:configuration-version
Type	Cisco AV Pair
Format	Integer
Local config	configuration version *version*
Radius config	cisco-avpair="ipsec:configuration-version=*version*"
Description	Specifies the version of the configuration to download. This is pushed to the client via Cisco FlexVPN attribute MODECFG_CONFIG_VERSION.

Attribute	Route-set remote
Type	Cisco AV Pair
Format	String
Local config	route set remote {ipv4 ip-address mask | ipv6 ip-address/mask}
Radius config	cisco-avpair="ipsec:route-set=remote {ipv4 network subnet_mask | ipv6 network/subnet_mask}"

Description	Specifies a subnet protected by FlexVPN server. This is pushed to the client through IKEv2 standard configuration attribute INTERNAL_IP4_SUBNET. While route-set prefix is working with a subnet mask represented in decimal fashion [e.g. /24], route-set remote requires the standard subnet mask representation. [e.g. 255.255.255.0] **Note** This AV pair was introduced in Cisco IOS Release 3.10.0S

Attribute	Route-set local
Type	Cisco AV Pair
Format	String
Local config	route set local {ipv4 ip-address mask | ipv6 ip-address/mask}
Radius config	cisco-avpair="ipsec:route-set=local {ipv4 network subnet_mask | ipv6 network/subnet_mask}”
Description	This attribute is useful in an extranet scenario where you do not necessary trust the routing information that you receive from the remote device. In other words, remote routes can be denied and route addition can be locally controlled by using this AV pair. **Note** This AV pair was introduced in Cisco IOS Release 3.10.0S.