

Atributos RADIUS apoiados no controlador do Wireless LAN

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Atributos RADIUS apoiados no controlador do Wireless LAN](#)

[QoS-nível](#)

[ACL-nome](#)

[Nome da interface](#)

[VLAN-etiqueta](#)

[Atributos de túnel](#)

[Sintaxe para a configuração de atributos WLC em servidores Radius](#)

[Cisco Aireospace VSA no Cisco Access Registrar](#)

[Cisco Aireospace VSA no raio livre separa](#)

[Cisco Aireospace VSA no servidor Radius do Microsoft IAS](#)

[Cisco Aireospace VSA no server do Cisco Secure ACS](#)

[Verificar e solucionar problemas](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento explica a lista de atributos RADIUS apoiados no controlador do Wireless LAN (WLC) que são enviados ao servidor Radius na solicitação de acesso, honrados na aceitação de acesso, e enviados em pedidos da contabilidade. Isto igualmente inclui os atributos específicos de fornecedor.

[Pré-requisitos](#)

[Requisitos](#)

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Métodos da segurança Wireless
- autenticação Raio-baseada

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Atributos RADIUS apoiados no controlador do Wireless LAN

Os atributos RADIUS são usados para definir elementos específicos do Authentication, Authorization, and Accounting (AAA) em um perfil de usuário, que seja armazenado no demônio do RAIO. Esta seção alista os atributos RADIUS apoiados atualmente no controlador do Wireless LAN.

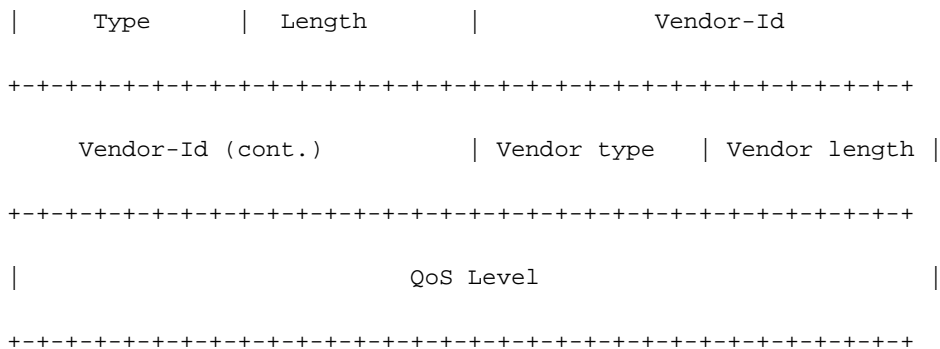
- **Qualidade de Serviço** — Quando atual em um acesso radius aceite, o valor do QoS-nível cancela o valor do QoS especificado no perfil WLAN.
- **ACL** — Quando o atributo do Access Control List (ACL) esta presente no acesso radius aceite, o sistema aplica o ACL-nome à estação do cliente depois que autentica. Isto cancela todos os ACL que forem atribuídos à relação.
- **VLAN** — Quando um nome da interface ou a VLAN-etiqueta VLAN estam presente em um acesso radius aceite, o sistema coloca o cliente em uma relação específica.
- **ID de WLAN** — Quando o atributo do ID de WLAN esta presente no acesso radius aceite, o sistema aplica o ID de WLAN (SSID) à estação do cliente depois que autentica. O ID de WLAN é enviado pelo WLC em todos os exemplos da autenticação exceto o IPsec. Em caso da autenticação da Web, se o WLC recebe um atributo do ID de WLAN na resposta de autenticação do servidor AAA, e dele não combina o ID do WLAN, autenticação é rejeitado. Outros tipos de métodos de segurança não fazem este.
- **Valor DSCP** — Quando atual em um acesso radius aceite, o valor DSCP cancela o valor DSCP especificado no perfil WLAN.
- **802.1p-Tag** — Quando atual em um acesso radius aceite, o valor 802.1p cancela o padrão especificado no perfil WLAN.

Nota: A característica VLAN apoia somente a filtração, o 802.1X, e o Wi-Fi Protected Access (WPA) MAC. A característica VLAN não apoia a autenticação da Web ou o IPsec. O base de dados do filtro do MAC local do sistema operacional foi estendido para incluir o nome da relação. Isto permite que os filtros do MAC local especifiquem que relação o cliente deve ser atribuído. Um servidor Radius separado pode igualmente ser usado, mas o servidor Radius deve ser definido usando os menus Segurança.

QoS-nível

O atributo do QoS-nível indica Qualidade de Serviço em nível para ser aplicado ao tráfego do cliente móvel dentro da tela de switching, assim como sobre o ar. Este exemplo mostra um sumário do formato de atributo do QoS-nível. Os campos são transmitidos da esquerda para a direita.

```
0                 1                 2                 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```



•Type - 26 for Vendor-Specific

•Length - 10

•Vendor-Id - 14179

•Vendor type - 2

•Vendor length - 4

•Value - Three octets:

-3 - Bronze (Background)

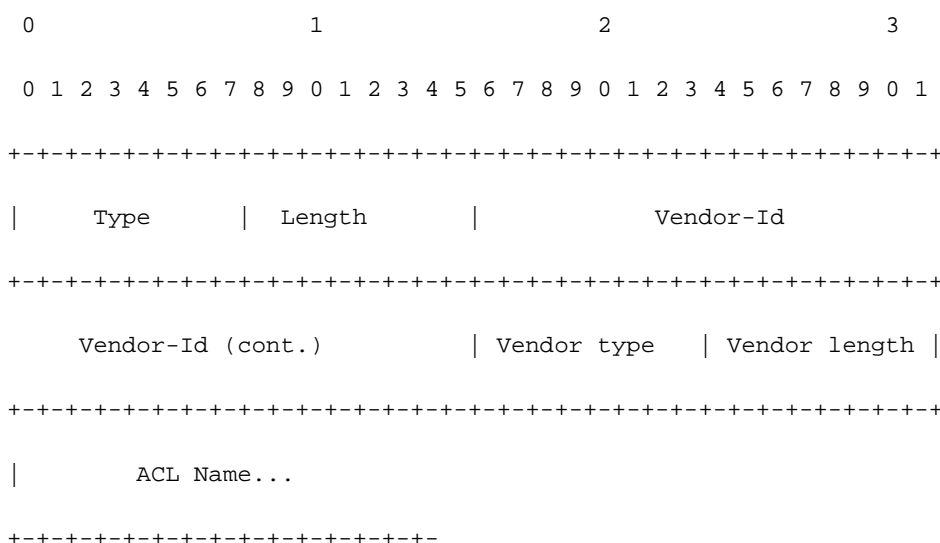
-0 - Silver (Best Effort)

-1 - Gold (Video)

-2 - Platinum (Voice)

ACL-nome

O atributo do ACL-nome indica o nome ACL a ser aplicado ao cliente. Um sumário do formato de atributo do ACL-nome é mostrado aqui. Os campos são transmitidos da esquerda para a direita.



•Type - 26 for Vendor-Specific

•Length - >7

•Vendor-Id - 14179

- Vendor type - 6
- Vendor length - >0
- Value - A string that includes the name of the ACL to use for the client

Nome da interface

O atributo de nome da interface indica que a interface de VLAN um cliente deve ser associada a. Um sumário do formato de atributo do nome da interface é mostrado aqui. Os campos são transmitidos da esquerda para a direita.

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
Type		Length	
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
Vendor-Id (cont.)		Vendor type	Vendor length
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
Interface Name...			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			

- Type - 26 for Vendor-Specific
- Length - >7
- Vendor-Id - 14179
- Vendor type - 5
- Vendor length - >0
- Value - A string that includes the name of the interface the client is to be assigned to.

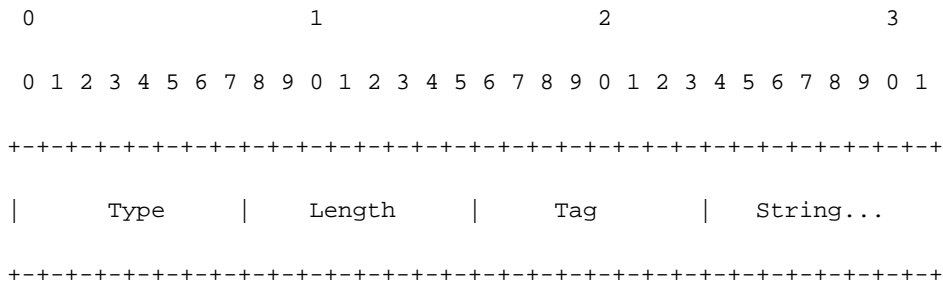
Nota: Este atributo trabalha somente quando a filtração MAC é permitida ou se o 802.1X ou o WPA estão usados como a política de segurança.

VLAN-etiqueta

O atributo da VLAN-etiqueta indica o ID de grupo para uma sessão em túnel particular, e é sabido igualmente como o atributo Túnel-Privado-Grupo-ID.

Este atributo pôde ser incluído no pacote de solicitação de acesso se o iniciador do túnel puder predeterminar o grupo que resulta de uma conexão particular e se está incluído no pacote de aceitação acesso se esta sessão de túnel deve ser tratado como se pertence a um grupo privado particular. Os grupos privados podem ser usados para associar uma sessão em túnel com um grupo particular de usuários. Por exemplo, pode ser usada para facilitar a distribuição dos endereços IP não registrados através de uma interface particular. Deve ser incluída nos pacotes do Contabilidade-pedido que contêm o Acct-Estado-tipo atributos com valores do começo ou da parada e que se referem uma sessão em túnel.

Um sumário do formato de atributo Túnel-Privado-Grupo-ID é mostrado aqui. Os campos são transmitidos da esquerda para a direita.



- Type - 81 for Tunnel-Private-Group-ID.
- Length - > = 3
- Tag - The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag field is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag field is greater than 0x1F, it should be interpreted as the first byte of the following String field.
- String - This field must be present. The group is represented by the String field. There is no restriction on the format of group IDs.

[Atributos de túnel](#)

Quando alguns dos outros atributos RADIUS (QoS-nível, ACL-nome, nome da interface, ou VLAN-etiqueta) são retornados, os atributos de túnel do [RFC 2868](#) devem igualmente ser retornados.

[O RFC 2868](#) define os atributos de túnel do RAIO usados para a authentication e autorização, e o [RFC 2867](#) define os atributos de túnel usados explicando. [Onde o autenticador do IEEE 802.1X apoia o Tunelamento, um túnel obrigatório pode estabelecer-se para o suplicante em consequência da autenticação.](#)

Em particular, pôde ser desejável permitir que uma porta seja colocada em um VLAN particular, definido no IEEE 802.1Q, com base no resultado da autenticação. Isto pode ser usado, por exemplo, para permitir que um host wireless permaneça no mesmo VLAN que move dentro de uma rede do campus.

O servidor Radius indica tipicamente o VLAN desejado incluindo atributos de túnel dentro da aceitação de acesso. Contudo, o autenticador do IEEE 802.1X pôde igualmente fornecer uma sugestão a respeito do VLAN a ser atribuído ao suplicante incluindo atributos de túnel dentro da solicitação de acesso.

Estes atributos de túnel são usados para a atribuição de VLAN:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

O VLANID é 12-bits, é um valor entre 1 e 4094, e é inclusivo. Desde que o Túnel-Privado-Grupo-ID é do tipo corda como definido no [RFC 2868](#), para o uso com IEEE 802.1X, o valor de número

inteiro VLANID é codificado como uma corda.

Quando os atributos de túnel são enviados, é necessário preencher o campo da etiqueta. Isto é notado no [RFC 2868](#), a seção 3.1:

- O campo da etiqueta é um octeto de comprimento e é pretendido fornecer meios de agrupar os atributos no mesmo pacote que referem o mesmo túnel. Os valores válidos para este campo são 0x01 com 0x1F (inclusivo). Se o campo Tag não for utilizado, ele deve ser zero (0x00).
- Para o uso com Túnel-Cliente-valor-limite, Túnel-Server-valor-limite, atributos Túnel-Privado-Grupo-ID, Túnel-Atribuição-ID, Túnel-Cliente-AUTH-ID ou Túnel-Server-AUTH-ID (mas não Tipo de túnel, Túnel-Media-tipo, Túnel-senha, ou Túnel-preferência), um campo da etiqueta de maior do que 0x1F é interpretado como o primeiro octeto do campo seguinte da corda. Para informações detalhadas sobre do formato refira a seção 3.1 do [RFC 2868](#).
- A menos que os tipos de túnel alternativos forem fornecidos, (por exemplo, para os autenticadores do IEEE 802.1X que puderam apoiar o Tunelamento mas não os VLAN), é somente necessário que os atributos de túnel especifique um único túnel. Em consequência, onde se deseja somente especificar o VLANID, o campo da etiqueta deve ser ajustado a zero (0x00) em todos os atributos de túnel. Onde os tipos de túnel alternativos são fornecidos, você deve escolher valores da etiqueta entre 0x01 e 0x1F.

[Sintaxe para a configuração de atributos WLC em servidores Radius](#)

[Cisco Airespace VSA no Cisco Access Registrar](#)

O Registrar de Acesso CNS Cisco é um server Raio-complacente, da política de acesso projetado apoiar a entrega do seletor, um ISDN, e uns serviços novos que incluem o DSL, o cabo com Telco-Return, o Sem fio e a Voz sobre o IP. Para informações detalhadas sobre do Cisco Access Registrar refira a [página de suporte do Cisco Access Registrar](#).

Esta é a sintaxe que precisa de ser usada no Cisco Access Registrar para definir os atributos WLC.

- **Define atributos RADIUS de Airespace:**

```
Description = str:[0]
Name = str:[0]Airespace
Type = str:[0]SUB_ATTRIBUTES
VendorID = int32:[0]14179
VendorTypeSize = str:[0]8-bit
```
- **Define o ID de WLAN para o usuário:**

```
Description = str:[0]
Max = int32:[0]4294967295
Min = int32:[0]0
Name = str:[0]Airespace-WLAN-Id
SubAttribute = int32:[0]1
Type = str:[0]UINT32
```
- **Define o nível de QoS para um usuário:**

```
Description = str:[0]
Max = int32:[0]3
Min = int32:[0]0
Name = str:[0]Airespace-QoS-Level
SubAttribute = int32:[0]2
Type = str:[0]ENUM
0 = str:[0]Silver
```

- ```

1 = str:[0]Gold
2 = str:[0]Platinum
3 = str:[0]Bronze

```
- **Define o valor DSCP dos pacotes de um usuário:**

```

Description = str:[0]
Max = int32:[0]4294967295
Min = int32:[0]0
Name = str:[0]Airespace-DSCP
SubAttribute = int32:[0]3
Type = str:[0]UINT32

```
  - **Define a etiqueta 802.1p:**

```

Description = str:[0]
Max = int32:[0]4294967295
Min = int32:[0]0
Name = str:[0]Airespace-802.1P-Tag
SubAttribute = int32:[0]4
Type = str:[0]UINT32

```
  - **Define a relação a que o usuário é traçado:**

```

Description = str:[0]
Max = int32:[0]253
Min = int32:[0]0
Name = str:[0]Airespace-Interface-Name
SubAttribute = int32:[0]5
Type = str:[0]STRING

```
  - **Define o ACL que é aplicado:**

```

Description = str:[0]
Max = int32:[0]253
Min = int32:[0]0
Name = str:[0]Airespace-ACL-Name
SubAttribute = int32:[0]6
Type = str:[0]STRING

```

## [Cisco Airespace VSA no raio livre separa](#)

O arquivo de dicionário de Airespace para o servidor Radius livre está disponível no diretório de instalação sob a **parte do** nome de diretório. O nome de arquivo é dictionary.airespace.

**Nota:** O arquivo de dicionário pôde ser diferente para versões anterior. Os exemplos dados neste documento são da versão de RADIUS livre 1.1.6.

```

-*- text -*-
#
#As found on the net.
#
#$Id: dictionary.airespace,v 1.3.2.1 2005/11/30 22:17:19 aland Exp $
#
VENDORAirespace14179

BEGIN-VENDORAirespace
ATTRIBUTEAirespace-Wlan-Idlinteger
ATTRIBUTEAirespace-QOS-Level2integer
ATTRIBUTEAirespace-DSCP3integer
ATTRIBUTEAirespace-8021p-Tag4integer
ATTRIBUTEAirespace-Interface-Name5string
ATTRIBUTEAirespace-ACL-Name6string

VALUEAirespace-QOS-LevelBronze3
VALUEAirespace-QOS-LevelSilver0
VALUEAirespace-QOS-LevelGold1
VALUEAirespace-QOS-LevelPlatinum2

END-VENDOR Airespace

```

O dicionário específico do vendedor para o Produtos de Airespace é incluído no arquivo de

dicionário disponível sob o mesmo diretório. O nome de arquivo é dicionário.

```
-*- text -*-
#
Version $Id: dictionary,v 1.93.2.5.2.10 2007/04/08 14:42:06 aland Exp $
#
#DO NOT EDIT THE FILES IN THIS DIRECTORY
#
#
#Use the main dictionary file (usually /etc/raddb/dictionary)
#for local system attributes and $INCLUDEs.
#
#
#This file contains dictionary translations for parsing
#requests and generating responses. All transactions are
#composed of Attribute/Value Pairs. The value of each attribute
#is specified as one of 4 data types. Valid data types are:
#
#text - printable, generally UTF-8 encoded (subset of 'string')
#string - 0-253 octets
#ipaddr - 4 octets in network byte order
#integer - 32 bit value in big endian order (high byte first)
#date - 32 bit value in big endian order - seconds since
00:00:00 GMT, Jan. 1, 1970
#ifid - 8 octets in network byte order
#ipv6addr - 16 octets in network byte order
#ipv6prefix - 18 octets in network byte order
#
#FreeRADIUS includes extended data types which are not defined
#in the RFC's. These data types are:
#
#abinary - Ascend's binary filter format.
#octets - raw octets, printed and input as hex strings.
e.g.: 0x123456789abcdef
#
#
#Enumerated values are stored in the user file with dictionary
#VALUE translations for easy administration.
#
#Example:
#
#ATTRIBUTE VALUE
#-----
#Framed-Protocol = PPP
#7= 1(integer encoding)
#
#
#Include compatibility dictionary for older users file. Move
#this directive to the end of this file if you want to see the
#old names in the logfiles, INSTEAD OF the new names.
#
$INCLUDE dictionary.compat
#
#Include the RFC dictionaries next.
#
#For a complete list of the standard attributes and values,
#see:
#http://www.iana.org/assignments/radius-types
#
$INCLUDE dictionary.rfc2865
```



```

$INCLUDE dictionary.rfc2866
$INCLUDE dictionary.rfc2867
$INCLUDE dictionary.rfc2868
$INCLUDE dictionary.rfc2869
$INCLUDE dictionary.rfc3162
$INCLUDE dictionary.rfc3576
$INCLUDE dictionary.rfc3580
$INCLUDE dictionary.rfc4372
$INCLUDE dictionary.rfc4675
$INCLUDE dictionary.rfc4679

#
#Include vendor dictionaries after the standard ones.
#
$INCLUDE dictionary.3com
$INCLUDE dictionary.3gpp
$INCLUDE dictionary.3gpp2
$INCLUDE dictionary.acc
$INCLUDE dictionary.airespace $INCLUDE dictionary.alcatel $INCLUDE dictionary.alteon $INCLUDE
dictionary.alvarion $INCLUDE dictionary.aruba $INCLUDE dictionary.ascend $INCLUDE dictionary.asn
$INCLUDE dictionary.bay $INCLUDE dictionary.bintec $INCLUDE dictionary.cablelabs $INCLUDE
dictionary.cabletron $INCLUDE dictionary.cisco # # The Cisco VPN300 dictionary is the same as
the altiga one. # You shouldn't use both at the same time. # # $INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000 $INCLUDE dictionary.cisco.bbsm # # And finally the server
internal attributes. # $INCLUDE dictionary.freeradius.internal # # Miscellaneous attributes
defined in weird places that # don't really belong anywhere else... # ATTRIBUTE Originating-
Line-Info 94 string # As defined in draft-sterman-aaa-sip-00.txt ATTRIBUTE Digest-Response 206
string ATTRIBUTE Digest-Attributes 207 octets # # # Integer Translations # VALUE Service-Type
Voice 12 VALUE Service-Type Fax 13 VALUE Service-Type Modem-Relay 14 VALUE Service-Type IAPP-
Register 15 VALUE Service-Type IAPP-AP-Check 16 VALUE Framed-Protocol GPRS-PDP-Context 7 VALUE
NAS-Port-Type Wireless-CDMA2000 22 VALUE NAS-Port-Type Wireless-UMTS 23 VALUE NAS-Port-Type
Wireless-1X-EV 24 VALUE NAS-Port-Type IAPP 25 VALUE Framed-Protocol PPTP 9

```

## [Cisco Airespace VSA no servidor Radius do Microsoft IAS](#)

Para obter informações sobre de como configurar um server do Internet Authentication Service de Microsoft (MS IAS) para apoiar os atributos do específico do vendedor de Cisco Airespace (VSA) leia [Cisco Airespace VSA no exemplo da configuração de servidor RADIUS MS IAS](#)

## [Cisco Airespace VSA no server do Cisco Secure ACS](#)

A solution engine da liberação 4.0 do Serviço de controle de acesso Cisco Secure, apoia muitos atributos do Remote Access Dial-In User Service (RAIO) que incluem atributos de Cisco Airespace.

O ACS não pode oferecer o apoio parcial do IETF. Daqui, quando você adiciona um dispositivo de Cisco Airespace (na configuração de rede), permite automaticamente todos os atributos IETF. Esta tabela dá os atributos de Cisco Airespace apoiados por Cisco ACS.

Os dispositivos de Cisco Airespace apoiam alguns atributos IETF para trabalhos em rede da identidade do 802.1x:

- Tipo de túnel (64)
- Túnel-Media-tipo (65)
- Túnel-Privado-Grupo-identificação (81)

A fim configurar um atributo específico a ser enviado para um usuário, você deve assegurar aquele:

- Na seção de configuração de rede, você deve configurar a entrada do cliente de AAA que corresponde ao dispositivo de acesso que concede o acesso de rede ao usuário para usar uma variedade de RAIOS que apoia o atributo que você quer enviado ao cliente de AAA.
- Na seção de configuração da interface, você deve permitir o atributo de modo que apareça em páginas do perfil do usuário ou do grupo de usuário. Você pode permitir os atributos na página que correspondem à variedade do RAIOS que apoia o atributo. Por exemplo, o atributo do Sessão-intervalo do RADIUS IETF (27) aparece na página do RAIOS (IETF). **Nota:** À revelia, os atributos RADIUS não são permitidos por usuário (não aparecem na página da configuração da interface). Antes que você possa permitir atributos em uma base do usuário per., você deve permitir a opção dos atributos do usuário per. TACACS+/RADIUS na página avançada das opções na seção de configuração da interface. Após ter permitido atributos por usuário, uma coluna do usuário aparece como desabilitado na página da configuração da interface para esse atributo.
- No perfil que você se usa para controlar autorizações para o usuário — no usuário ou no grupo edite páginas ou a página componente compartilhada da autorização RADIUS — você deve permitir o atributo. Quando você permite este atributo, faz com que o ACS envie o atributo ao cliente de AAA na mensagem da aceitação de acesso. Nas opções que são associadas com o atributo, você pode determinar o valor do atributo que é enviado ao cliente de AAA.

Refira a seção dos [atributos RADIUS do Guia do Usuário para a solution engine 4.0 do Cisco Secure ACS](#) para mais informação.

## Verificar e solucionar problemas

Quando o usuário conecta ao WLAN com um usuário - a identificação e a senha, o WLC passam as credenciais ao servidor Radius que autentica o usuário contra as circunstâncias e o perfil de usuário configurados. Se a autenticação de usuário é bem sucedida, o servidor Radius retorna um RAIOS aceita o pedido que igualmente contém os atributos RADIUS configurados para esse usuário. Neste exemplo, a política de QoS do usuário é retornada.

Você pode emitir o **comando debug aaa all enable** a fim ver a sequência de evento que ocorre durante a autenticação. Aqui está o exemplo de saída:

```
(Cisco Controller) >debug aaa all enable Wed Apr 18 18:14:24 2007: User admin authenticated Wed
Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile
28:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c Wed Apr 18
18:14:24 2007: structureSize.....70 Wed Apr 18 18:14:24 2007:
resultCode.....0 Wed Apr 18 18:14:24 2007:
protocolUsed.....0x00000008 Wed Apr 18 18:14:24 2007:
proxyState..... 28:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007: Packet
contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type..... 0x00000006
(6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02] Airespace / WLAN-Identifier.... 0x00000000 (0)
(4 bytes) Wed Apr 18 18:14:24 2007: User admin authenticated Wed Apr 18 18:14:24 2007:
29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile 29:1f:00:00:00:00 Wed Apr 18
18:14:24 2007: AuthorizationResponse: 0xbadff97c Wed Apr 18 18:14:24 2007:
structureSize.....70 Wed Apr 18 18:14:24 2007:
resultCode.....0 Wed Apr 18 18:14:24 2007:
protocolUsed.....0x00000008 Wed Apr 18 18:14:24 2007:
proxyState..... 29:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007:
Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type.....
0x00000006 (6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02] Airespace / WLAN-Identifier....
0x00000000 (0) (4 bytes) Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-
VLAN10 Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc Wed Apr 18 18:15:08 2007:
```

```

Callback.....0x8250c40 Wed Apr 18 18:15:08 2007:
protocolType.....0x00000001 Wed Apr 18 18:15:08 2007:
proxyState..... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007:
Packet contains 8 AVPs (not shown) Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful
transmission of Authentication Packet (id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-
96:ac Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00 00 00 00 00 00 00 00 00
...h..... Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73 65 72 2d 56 4c 41
4e 31User-VLAN1 Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a ba 57 38 11
bc 9a 5d 59 0...2W.*.W8...Y Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 01 04
06 ac 10 01 1e 20 ..#..... Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00
00 37 63 01 06 00 00 00 .WLC2...7c.... Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e
30 2e 30 2e 31 1e 0d 31 37 32 ...20.0.0.1..172 Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e
31 2e 33 30 .16.1.30 Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc e4 ea 41 3e 28
7e cc bc ...F?....A>(~.. Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00 37 63 02
06 00 00 00 03 ..a.....7c..... Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20 37
d0 03 e6 00 00 01 377.....7 Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01
c7 7a 8b 35 20 31 80 00 00z.5.1... Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 00
1b Wed Apr 18 18:15:08 2007: ****Enter processIncomingMessages: response code=2 Wed Apr
18 18:15:08 2007: ****Enter processRadiusResponse: response code=2 Wed Apr 18 18:15:08 2007:
00:40:96:ac:e6:57 Access-Accept received from RADIUS server 172.16.1.1 for mobile
00:40:96:ac:e6:57 receiveId = 0 Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520 Wed
Apr 18 18:15:08 2007: structureSize.....114 Wed Apr 18 18:15:08 2007:
resultCode.....0 Wed Apr 18 18:15:08 2007:
protocolUsed.....0x00000001 Wed Apr 18 18:15:08 2007:
proxyState..... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007: Packet
contains 3 AVPs: Wed Apr 18 18:15:08 2007: AVP[01] Airespace / QOS-Level..... 0x00000003 (3)
(4 bytes) Wed Apr 18 18:15:08 2007: AVP[02] Service-Type..... 0x00000001 (1) (4
bytes) Wed Apr 18 18:15:08 2007: AVP[03] Class..... DATA (30 bytes) Wed Apr 18
18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Wed Apr
18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48,
valid bits: 0x3 qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAVgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: ' Wed Apr 18
18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc Wed Apr 18 18:15:12 2007: Packet
contains 13 AVPs: Wed Apr 18 18:15:12 2007: AVP[01] User-Name..... User-
VLAN10 (11 bytes) Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port.....
0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[03] Nas-Ip-Address.....
0xac10011e (-1408237282) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[04] NAS-
Identifier..... 0x574c4332 (1464615730) (4 bytes) Wed Apr 18 18:15:12 2007:
AVP[05] Airespace / WLAN-Identifier..... 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007:
AVP[06] Acct-Session-Id..... 4626602c/00:40:96:ac:e6:57/16 (29 bytes) Wed Apr 18
18:15:12 2007: AVP[07] Acct-Authentic..... 0x00000001 (1) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[08] Tunnel-Type..... 0x0000000d (13) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[09] Tunnel-Medium-Type..... 0x00000006 (6) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[10] Tunnel-Group-Id..... 0x3230 (12848) (2 bytes) Wed Apr 18
18:15:12 2007: AVP[11] Acct-Status-Type..... 0x00000001 (1) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[12] Calling-Station-Id..... 20.0.0.1 (8 bytes) Wed Apr 18 18:15:12
2007: AVP[13] Called-Station-Id..... 172.16.1.30 (11 bytes)

```

Este usuário mostra que o usuário está autenticado. Então, os valores da ultrapassagem AAA são retornados com o RAIIO aceita a mensagem. Neste caso, você vê que o atributo de QoS está retornado junto com o RAIIO aceita a mensagem. Conseqüentemente, o usuário é dado a política de QoS do bronze que cancela o valor do QoS do padrão ajustado para esse SSID.

## [Informações Relacionadas](#)

- [Cisco Airespace VSA no exemplo da configuração de servidor RADIUS MS IAS](#)
- [Guia de configuração do Cisco Wireless LAN Controller, versão 4.1](#)
- [Página de Suporte Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)