



# RADIUS Profiles and Attributes for SSG

---

**First Published: May 2, 2005**  
**Last Updated: October 2, 2009**



---

Effective with Cisco IOS Release 15.0(1)M, this feature is not available in Cisco IOS software.

---

This module describes RADIUS profiles and their attributes.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for RADIUS Profiles and Attributes for SSG”](#) section on page 57.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for RADIUS Profiles and Attributes for SSG, page 2](#)
- [Information About RADIUS Profiles and Attributes for SSG, page 2](#)
- [Additional References, page 55](#)
- [Feature Information for RADIUS Profiles and Attributes for SSG, page 57](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Prerequisites for RADIUS Profiles and Attributes for SSG

Before you can configure SSG to authenticate subscribers you must first configure SESM and the RADIUS server to support the logon method.

## Information About RADIUS Profiles and Attributes for SSG

This section describes the following concepts:

- [RADIUS Profiles for SSG Support, page 2](#)
- [RADIUS Accounting Records for SSG, page 47](#)

## RADIUS Profiles for SSG Support

This section describes the following concepts:

- [SSG Vendor-Specific Attributes, page 2](#)
- [Subscriber Profiles, page 29](#)
- [Service Profiles, page 32](#)
- [Service Group Profiles, page 40](#)
- [Pseudo-Service Profiles, page 42](#)
- [Examples of SSG RADIUS Profiles, page 44](#)

## SSG Vendor-Specific Attributes

[Table 1](#) lists vendor-specific attributes used by SSG. By sending an Access-Request packet with the vendor-specific attributes shown in the table, SESM can send requests to SSG to log on and log off an account and disconnect and connect services. The vendor ID for all of the Cisco-specific attributes is 9

**Table 1** Vendor-Specific Attributes

AttributeID	VendorID	SubattributeID	SubattributeName	SubattributeDataType
26	9	1	<a href="#">Cisco-AVpair Attributes</a>	String
26	9	250	<a href="#">SSG Account-Info Attributes</a>	String
26	9	251	<a href="#">SSG Service Info Attributes</a>	String
26	9	253	<a href="#">SSG Control Info Attributes</a>	String

The following sections describe the format of each subattribute.



**Note**

All RADIUS attributes are case sensitive.

## Cisco-AVpair Attributes

The Cisco-AVpair attributes are used in user and service profiles to configure ACLs and L2TP

**Table 2** Cisco AV Pair Attributes

Attribute	Description
<a href="#">Downstream Access Control List (outacl)</a>	Specifies either a Cisco IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
<a href="#">Upstream Access Control List</a>	Specifies the secret (the password) used for L2TP tunnel authentication.
<a href="#">Upstream Access Control List (inacl)</a>	Specifies either a Cisco IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.
<a href="#">VPDN IP Address</a>	Specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.
<a href="#">VPDN IP Address</a>	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.

## SSG Account-Info Attributes

The Account-Info attributes are used in user profiles and service group profiles.

User profiles define the password, services, and groups to which the user is subscribed.

Service group profiles contain a list of services and service groups and can be used to create sophisticated directory structures for locating and logging in to services. When a user is subscribed to a service group, the user is automatically subscribed to all services and groups within that service group. A service group profile includes the name of the service group, the password, the service type (outbound), a list of services, and a list of other service groups.

### RADIUS Freeware Format Example

```
Account-Info = "Nservice1.com"
```

### CiscoSecure ACS for UNIX Format Example

```
9,250 = "Nservice1.com"
```

The following account-info attributes set various parameters for the host in SSG.

**Table 3** SSG Account Information Attributes

Subattribute Value	Attribute Function	Description
A	<a href="#">Auto Log On Service</a>	Automatically logs a user into a service when the user logs in to SSG.
D	<a href="#">Default Internet Access</a>	Specifies whether a host is allowed to default Internet access. Not currently used by SSG.
G	<a href="#">Group Name</a>	Used by SESM to display the group name and the list of services in the group.

**Table 3 SSG Account Information Attributes**

Subattribute Value	Attribute Function	Description
M	Messaging IP and Port	Specifies the IP address and port number of the messaging server for a host.
N	Service Name	Specifies the name of the service that a host is subscriber to.
P	Primary Service Name	Tells SSG that this is the Auto-domain service. Not currently used by SSG.
Q	Subscriber QoS Info	Specifies the QoS parameters for the host in both the upstream and downstream directions.
R	TCP Redirection	Specifies the TCP Redirection configuration for the host
S	Subscriber IP	Identifies the host on SSG.
TP	Transparent Pass-through (TP) Info	Specifies the Transparent pass-through (TP) user for Transparent Autologon (TAL).
V	User Cookie	The AAA server sends this attribute to SSG in the user profile.
S	SESM Namespace	Contains subattributes that are used by SESM to form the complete IDs for the host or connections.

**Auto Log On Service**

This attribute specifies the name of the service that the user is automatically logged onto after an Account-Logon. This is configured in the user profile and is present in Access-Accept packets and can appear multiple times.

code: 250, 'A'

len: 3

+-----+

label c |d|e|f|g|

+-----+

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 250 (Subattribute ID for Account-Info)

e = len (length of the vendor specific subattribute)

f = 'A' (account-info code for Auto log on service)

g = <service name[;user;password]>





c = 9 (Cisco vendor ID)  
 d = 250 (Subattribute ID for Account-Info)  
 e = len (length of the vendor specific subattribute)  
 f = 'N' (account-info code for service name)

for account info reply:

g = <name;description;flag>  
 (the flag is 'P', 'X' or 'T' representing the service type)

for service query reply:

g = <[110]name;elapsed time;service username>

for account ping reply:

g = <1;servicename;elapsed-time in seconds;username;downstream packets;upstream packets;downstream bytes;upstream bytes>

### Primary Service Name

This attribute is used in conjunction with auto-domain. It tells SSG that this is the auto-domain service – where the user needs to be authenticated. Currently not used by SSG.

code: 250, 'P'

len: > 6

+--+--+--+--+--+--+--+--+--+....+--++

lalbl c ldlelflg l

+--+--+--+--+--+--+--+--+--+....+--++

a = 26 (RADIUS attr for vendor specific)  
 b = len (length of the RADIUS Vendor specific Attribute)  
 c = 9 (Cisco vendor ID)  
 d = 250 (Subattribute ID for Account-Info)  
 e = len (length of the vendor specific subattribute)  
 f = 'P' (account-info code for Primary Service Name)  
 g = <service-name as a string>

### Subscriber QoS Info

This attribute specifies the QoS parameters for the host in both the upstream and downstream direction. This is configured in the user profile and is present in Access-Accepts and can appear only once.

code: 250, 'Q'

len: > 6

```
+--+--+--+--+--+--+--+--+--+...+--++
```

```
labl c ldlflg l
```

```
+--+--+--+--+--+--+--+--+--+...+--++
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 250 (Subattribute ID for Account-Info)

e = len (length of the vendor specific subattribute)

f = 'Q' (QoS-info code for subscriber IP)

g = <U;cir;normal burst;excess burst;D;cir;normal burst;excess burst>

'U' indicates upstream parameters and 'D' indicates downstream parameters.

### TCP Redirection

This attribute specifies the TCP-redirection configuration for the host. It has three subattributes, one for SMTP redirection, one for initial captivation and one for periodic advertising captivation. This is configured in the user profile and is present in the Access-Accept and each subattribute can appear at most once.

code: 250, 'R'

len: >3

```
+--+--+--+--+--+--+--+--+--+...+--++
```

```
labl c ldlflg l
```

```
+--+--+--+--+--+--+--+--+--+...+--++
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 250 (Subattribute ID for Account-Info)

e = len (length of the vendor specific subattribute)

f = 'R' (account-info code for redirect features... see below)

g = one of the allowable additional features described in the following sections.

SMTP forwarding

g = 'S' indicating user has SMTP forwarding capability

If SMTP forwarding has been enabled on a per-user basis, the presence of this attribute in the user profile allows SMTP forwarding for that host to the server defined on SSG.

#### Initial Captivation

g = 'I<group>;<duration>[;<service>]'

This attribute indicates that the user has Initial Captivation capability, and also indicating captive portal group to use, and duration of the captivation (in seconds). If the optional service field is added then the captivation will only start once the user has activated the named service.

#### Advertisement Captivation

g = 'A<group>;<duration>;<frequency>[;<service>]'

This attribute indicates that the user has Advertisement Captivation capability, and also indicating captive portal group to use, and duration and approximate frequency of the captivation (in seconds). If the optional service field is added then the captivation will only occur when the user has the named service active.

#### Subscriber IP

This attribute identifies the host on SSG. This is present in all Access-Requests from SESM to SSG and also in all the replies from SSG to SESM. In the normal mode, the IP address is used to identify the host. In the port-bundle host-key mode, a combination of the IP address and the port-bundle is used.

code: 250, 'S'

len: > 6

```
+--+--+--+--+--+--+--+--+--+....+--++
```

```
lalbl c ldlelflg l
```

```
+--+--+--+--+--+--+--+--+--+....+--++
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 250 (Subattribute ID for Account-Info)

e = len (length of the vendor specific subattribute)

f = 'S' (account-info code for subscriber IP)

g = <subscriber's IP in dot notation>[:<port bundle number>]

port bundle number is used in Host-Key mode

#### Transparent Pass-through (TP) Info

This attribute specifies the Transparent Pass-through (TP) user for Transparent Auto-Logon (TAL). This is configured in the user profile and is present in Access-Accepts and can appear only once.

code: 250, 'TP'

len: > 6

```
+--+--+--+--+--+--+--+--+--+...+--++
```

```
labl c ldlflg l
```

```
+--+--+--+--+--+--+--+--+--+...+--++
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 250 (Subattribute ID for Account-Info)

e = len (length of the vendor specific subattribute)

f = 'TP' (Transparent Pass-through for TAL)

### User Cookie

This attribute is used by AAA-server – which is sent transparently by SSG to the aaa-server in all accounting records. AAA-server initially sends this attribute in the user-profile. In a sense, this is similar to class attribute (attribute#25)

code: 250, 'V'

len: > 6

```
+--+--+--+--+--+--+--+--+--+...+--++
```

```
labl c ldlflg l
```

```
+--+--+--+--+--+--+--+--+--+...+--++
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 250 (Subattribute ID for Account-Info)

e = len (length of the vendor specific subattribute)

f = 'V' (account-info code for user cookie)

g = <cookie as string>

### SESM Namespace

This is used by SESM. It has subattributes that are used to form the complete IDs for host or connections. This attribute has the following generic format:

Code: 250, \$

Len: >12

```

+--+--+--+--+--+--+--+--+--+--+....+--+
|a|b| c |d|e|f|g| h | i |
+--+--+--+--+--+--+--+--+--+--+....+--+

```

A = 26 (RADIUS code for vendor-specific Attribute)

B = Len (Length of the RADIUS vendor-specific Attribute)

C = 9 (Cisco's Vendor ID)

D = 250 (Subattribute ID for SSG Account-Info)

E = len (Length of the vendor-specific subattribute)

F = '\$' (Account-Info code for SESM namespace)

G = '...' Sub-code for SESM namespace account-info code

H = value The value of the relevant Complete ID key.

Host Complete ID

The possible values for the host complete ID are described in [Table 4](#) below.



**Note**

The host name, host IP address and host MSISDN will be sent using the standard RADIUS attributes.

**Table 4** Host Complete ID Attributes

Attribute	Sub-Code	Possible Values
Client IP Address	Using the standard RADIUS attribute #8– Framed-IP-Address	The address field is four octets.
Client MAC Address	MA	A string containing the client's MAC Address (in the format "0123.4567.89a0"). This attribute is only present for directly connected clients.
Sub-Interface	SI	A string containing the name of the downlink interface for the client.
VPI/VCI	VP	A string containing the VPI/VCI values. This attribute is only present for PPP or RBE interfaces.
MSISDN	Using the standard RADIUS attribute #31 – Calling-Station-ID	A string field containing the MSISDN of a client. This attribute is only present for RADIUS proxy clients.

.Connection Complete ID

The connection complete ID attribute has the following format:

Code: 250, \$

Len: >12

```
+-----+-----+-----+-----+-----+-----+
```

```
la|bl c |dle|fl|g|h |l|l
```

```
+-----+-----+-----+-----+-----+-----+
```

a = 26 (RADIUS code for vendor-specific Attribute)

b = Len (Length of the RADIUS vendor-specific Attribute)

c = 9 (Cisco's Vendor ID)

d = 250 (Subattribute ID for SSG Account-Info)

e = len (Length of the vendor-specific subattribute)

f = '\$' (Account-Info code for SESM namespace)

g = 'C' (Connection-info sub-code)

h = ' ' sub-code for connection-info (IP/UN/ID)

i = value of the relevant parameter in the format

<servicename>;<value>

The possible values for the connection complete ID are listed in [Table 5](#).

**Table 5 SSG Account Information Attributes**

Attribute	Sub-Code	Possible Values
Connection Username	UN	<servicename>;<username> Username contains the name used during service logon to <servicename>.
Calling ID	ID	<servicename>;<calling-id> The calling-id contains the calling ID used during service logon.
Connection Real IP Address	IP	<servicename>;<real IP> The Real IP address used for NAT in SSG can be assigned by the proxy service AAA server of by the LNS for L2TP services.

**Example:**

For a connection to "service1" with the username "usernam1", calling-id "1234567" and real IP 10.10.0.1, the attribute values would be as follows:

Account-Info 250, "\$CUNservice1;user1"

Account-Info 250, "\$CIDservice1;123456"

Account-Info 250, "\$CIPservice1;10.1.1.1"

## SSG Service Info Attributes

The Service-Info VSAs are used for SSG service specific parameters and are configured in the service profile. These attributes appear in Access-Accept packets for service profile download.

The following Service Info attributes set various parameters for the host in SSG.

**Table 6** SSG Service Info Attributes

Subattribute Value	Attribute Function	Description
A	Authentication Type	Defines the authentication type, PAP or CHAP, for the proxy and tunnel service.
B	MTU for SSG L2TP Service	Specifies the MTU for an L2TP tunnel service.
C	Auto-Domain Service NAT	Specifies whether the Auto-domain service needs to apply NAT.
D	DNS Server Address	Sets the DNS server IP address for the service.
E	Max Connections	Limits the number of connections to a particular service.
F	Attribute Filter	Lists the RADIUS attributes to be filtered from user authentication.
G	Service Next Hop Gateway	Sets the next hop gateway for SSG.
H	Initial URL	Used by SESM to open a page with this URL.
K	TCP-Redirect Server-Group	Specifies TCP-redirect server groups.
L	Accounting Update Interval	Sets the accounting interval for interim accounting for connections to this service.
M	Service Mode	Specifies the mode of access to a service.
N	Service Name for Quota Values	Specifies the name of the service.
O	Service Domain	Specifies the domains that are part of the service.
P	Payment Type	Defines further subattributes relating to prepaid and postpaid services.
Q	Service QoS Info	Sets the upstream and downstream QoS parameters for a connection to the service.
R	Destination Network	Specifies the networks that belong to the service.
S	RADIUS Server	Specifies the RADIUS server to be used for authentication for the service.
T	Service Type	Specifies the type of service.
U	Service User Name	Specifies the username in connection accounting requests.

**Table 6 SSG Service Info Attributes**

Subattribute Value	Attribute Function	Description
V	<a href="#">Service Defined Cookie For Proxy RADIUS</a>	Specifies a cookie string fro a service.
X	<a href="#">Enable Full User Name for Proxy RADIUS</a>	Appends the service name to the username during authentication to the service.

**Authentication Type**

This attribute defines the authentication type – PAP or CHAP - for the proxy and tunnel service.

code: 251, 'A'

len: 4

```

+---+---+---+---+---+---+
|a|b|c|d|e|f|g|
+---+---+---+---+---+---+

```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute>

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'A' (service-info code for PPP Authentication Type)

g = 'P'/C' (PAP or CHAP)

**MTU for SSG L2TP Service**

This attribute specifies the MTU for a L2TP tunnel service. This is configured in the tunnel service profile and can appear almost at once.

code: 251, 'B'

len: > 3

```

+---+---+---+---+---+---+...-+
|a|b|c|d|e|f|g|l|
+---+---+---+---+---+---+...-+

```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute>

c = 9 (Cisco vendor ID)  
 d = 251 (Subattribute ID for Service-Info)  
 e = len (length of the vendor specific subattribute)  
 f = 'B' (service-info code for MTU for SSG l2tp service)  
 g = <non-zero MTU as a string>

#### Auto-Domain Service NAT

This attribute tells if the auto-domain service needs to have NAT applied or not. The auto-domain service provides an ip-address; this attribute dictates whether to use this attribute or to assign an ip-address from local pool and use NAT.

code: 251, 'C'  
 len: = 10

```
+--+--+--+--+--+--+--+--+--+...+
|a|b| c |d|e|f| g | l
+--+--+--+--+--+--+--+--+--+...+
```

a = 26 (RADIUS attr for vendor specific)  
 b = len (length of the RADIUS Vendor specific Attribute)  
 c = 9 (Cisco vendor ID)  
 d = 251 (Subattribute ID for Service-Info)  
 e = len (length of the vendor specific subattribute)  
 f = 'C' (service-info code for auto-domain service NAT)  
 g = [011]

#### DNS Server Address

This attribute sets the DNS server IP address for the service. Two DNS servers, primary and secondary, can be specified using this attribute. This is configured in the service profile and can appear almost at once.

code: 251, 'D'  
 len: > 7

```
+--+--+--+--+--+--+--+--+--+...+
|a|b| c |d|e|f| g | l
+--+--+--+--+--+--+--+--+--+...+
```

a = 26 (RADIUS attr for vendor specific)  
 b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)  
 d = 251 (Subattribute ID for Service-Info)  
 e = len (length of the vendor specific subattribute)  
 f = 'D' (service-info code for service DNS)  
 g = <ip1[;ip2]> (IP of the Primary/Secondary DNS servers in dot notation)

### Max Connections

This value of this attribute limits the number of connections to a particular service.

code: 251, 'E'  
 len: > 9

```
+--+--+--+--+--+--+--+--+...--+
|a|b| c |d|e|f|g| |
+--+--+--+--+--+--+--+--+...--+
```

a = 26 (RADIUS attr for vendor specific)  
 b = len (length of the RADIUS vendor-specific)  
 c = 9 (Cisco vendor ID)  
 d = 253 (subattribute ID for Service-Info)  
 e = len (length of the vendor-specific filter)  
 p = 'E' (service-info code for max connections)  
 g = <number in ascii string format>

### Attribute Filter

This attribute lists the RADIUS attributes that are to be filtered out from user authentication for the service (would apply to both proxy RADIUS service and L2TP tunnel service). Currently only attribute 31 (calling station ID) is supported. The attributes listed here are filtered in Access-Request for proxy service authentication, L2TP tunnel session negotiation and SSG proxy service connection Accounting-Requests sent to the remote AAA (AAA server specified in the proxy service profile). This filter has no effect on host accounting requests, prepaid (re)authorization requests and connection accounting requests to the local AAA server. This attribute can be used when the access provider does not wish to expose the user's calling-ID/MSISDN number to services.

code: 251, 'F'  
 len: > 12

```
+--+--+--+--+--+--+--+--+...--+
|a|b| c |d|e|f|g| |
+--+--+--+--+--+--+--+--+...--+
```

a = 26 (RADIUS attr for vendor specific)  
 b = len (length of the RADIUS vendor-specific)  
 c = 9 (Cisco vendor ID)  
 d = 253 (subattribute ID for Service-Info)  
 e = len (length of the vendor-specific filter)  
 p = 'F' (Port filter indication flag)  
 g = <attribute number>

The 'g' parameter contains an ASCII string of the attribute to be filtered. Initially only a value of '31' is allowed to filter out calling station id.

### Service Next Hop Gateway

This attribute sets the next-hop gateway for the SSG service. This attribute is configured in the service profile and can appear almost at once. The string specified in this attribute is used to key off a next-hop table on SSG to find the next-hop gateway IP address. This attribute can appear almost at once. If this attribute is not configured, the service name is used as the key to find the next-hop IP address.

code: 251, 'G'  
 len: > 7

```

++-+-+-+---+---+---+---+---+---+...+
|a|b| c |d|e|f| g | l
++-+-+-+---+---+---+---+---+---+...+

```

a = 26 (RADIUS attr for vendor specific)  
 b = len (length of the RADIUS Vendor specific Attribute)  
 c = 9 (Cisco vendor ID)  
 d = 251 (Subattribute ID for Service-Info)  
 e = len (length of the vendor specific subattribute)  
 f = 'G' (service-info code for service next hop gateway)  
 g = <IP in dot notation or service name>



#### Note

---

Service name will be resolved to IP from the next hop table.

---

### Initial URL

This attribute is used by SESM. When the user logs into the service, SESM opens up a page with this URL.

code: 251, 'H'  
 len: > 7

```

+---+---+---+---+---+---+---+---+---+...-+
|a|b| c |d|e|f| g | |
+---+---+---+---+---+---+---+---+---+...-+

```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS Vendor specific Attribute)  
c = 9 (Cisco vendor ID)  
d = 251 (Subattribute ID for Service-Info)  
e = len (length of the vendor specific subattribute)  
f = 'H' (service-info code for initial-URL)  
g = <uri as a string>

#### TCP-Redirect Server-Group

This attribute specifies service-specific tcp-redirect server-groups. Currently, it is used only for the per-service web-proxy server-group.

```

code: 251, 'K'
len: > 7

```

```

+---+---+---+---+---+---+---+---+---+....-+
|a|b| c |d|e|f|g| h | |
+---+---+---+---+---+---+---+---+---+....-+

```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS Vendor specific Attribute)  
c = 9 (Cisco vendor ID)  
d = 251 (Subattribute ID for Service-Info)  
e = len (length of the vendor specific subattribute)  
f = 'K' (service-info code for tcp-redirect server-group)  
g = 'W' (service-info sub-code for per-service web-proxy server-group)

h = <server-group name as a string>

#### Accounting Update Interval

This attribute sets the accounting interval for interim accounting for connections to this service. This attribute can be present almost at once. If this attribute is not configured in the service profile, the global SSG accounting interval configured in SSG is used.

```

code: 251, 'L'
len: > 7

```

```

+--+--+--+--+--+--+--+--+--+...+
|a|b| c |d|e|f| g |
+--+--+--+--+--+--+--+--+--+...+

```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS Vendor specific Attribute)  
c = 9 (Cisco vendor ID)  
d = 251 (Subattribute ID for Service-Info)  
e = len (length of the vendor specific subattribute)  
f = 'L' (service-info code for accounting update interval)  
g = <seconds as a string>

### Service Mode

This attribute specifies the mode of access to a service. If the mode is sequential, a user cannot access this service if they are already logged on to another service. If the user is logged on to a sequential service, no other service can be accessed. This attribute can appear almost at once. If this attribute is not configured in the service profile, the default mode for the service is concurrent.

```

code: 251, 'M'
len: 4

```

```

+--+--+--+--+--+--+--+--+--+
|a|b| c |d|e|f|g|
+--+--+--+--+--+--+--+--+--+

```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS Vendor specific Attribute)  
c = 9 (Cisco vendor ID)  
d = 251 (Subattribute ID for Service-Info)  
e = len (length of the vendor specific subattribute)  
f = 'M' (service-info code for service mode)  
g = 'S'/'C'/'E' (Sequential, Concurrent or Exclusive)

### Service Name for Quota Values

This attribute specifies the name of the service. This is not configured in the service profile. It is present in Access-Requests from SSG for pre-paid service authorization.

```

code: 251, 'N'
len: 4

```

```

+--+--+--+--+--+--+--+--+--+--+...+--+
|a|b| c |d|e|f| g | |
+--+--+--+--+--+--+--+--+--+--+...+--+

```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS Vendor specific Attribute)  
c = 9 (Cisco vendor ID)  
d = 251 (Subattribute ID for Service-Info)  
e = len (length of the vendor specific subattribute)  
f = 'N' (service-info code for service name)  
g = <service name>

### Service Domain

This attribute specifies the domains that are a part of the service. If a user is connected to this service, all DNS queries to this domain are redirected to the DNS server for this service. This attribute is configured in the service profile and can appear multiple times.

```

code: 251, 'O'
len: > 4

```

```

+--+--+--+--+--+--+--+--+--+--+...+--+
|a|b| c |d|e|f| g | |
+--+--+--+--+--+--+--+--+--+--+...+--+

```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS Vendor specific Attribute)  
c = 9 (Cisco vendor ID)  
d = 251 (Subattribute ID for Service-Info)  
e = len (length of the vendor specific subattribute)  
f = 'O' (service-info code for domain name)  
g = <domain name[;domain name[;...]]> (domain name or names separated by semicolon)

### Payment Type

This attribute is used as a code to define further subattributes relating to prepaid and postpaid services.

```

code: 251, 'P'
len: 3

```

```

+-+--+--+--+--+--+--+--+--+
|a|b| c |d|e|f|g|...|
+-+--+--+--+--+--+--+--+--+

```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'P' (service-info code for payment type)

g='P' or 'Z' (P denotes code for postpaid subattributes, Z denotes code for prepaid subattributes)

#### Postpaid Services - Weekly Tariff Plan

The weekly tariff plan for postpaid services is specified using the following attribute.

code: 251, 'P'

len: > 12

```

+-+--+--+--+--+--+--+--+--+....+
|a|b| c |d|e|f|g|h| i |
+-+--+--+--+--+--+--+--+--+....+

```

a = 26 (RADIUS attr for vendor specific)

b = len(length of the RADIUS vendor-specific)

c = 9 (Cisco vendor ID)

d = 251 (subattribute ID for SSG Service-Info)

e = len (length of the vendor-specific Attribute)

f = 'P' (service-info code for service payment type)

g = 'P' (service-info code for postpaid service)

h = 'W' (service-info code for weekly tariff switch plan specification)

i = <weekly time> Weekly tariff switch time is in hh:mm:ss:d format:

hh = hour of day <0-23>

mm = minutes <0-59>

ss = seconds <0-59>

d = bit-map format for the days of week.

The format of the "d" attribute within the "QW" attribute of a service profile allows the configuration of arbitrary combinations of days where each weekday is represented by one bit. For example:

00000001 = Monday

00000010 = Tuesday

0000100 = Wednesday

00001000 = Thursday

00010000 = Friday

00100000 = Saturday

01000000 = Sunday

Consequently the value "00011111" (= 31 decimal) defines Monday, Tuesday, Wednesday, Thursday and Friday.

Example:

SSG Service-Info = "PPW00:00:00:127" - tariff switch time each day a week at midnight to support daily fee

SSG Service-Info = "PPW20:00:00:31" - tariff switch Monday till Friday at 8:00pm (off peak tariff)

SSG Service-Info = "PPW06:00:00:31" - tariff switch Monday till Friday at 6:00am (on peak tariff)

### Service QoS Info

This attribute sets the upstream and downstream QoS parameters for a connection to the service. This attribute is configured in the service profile and can appear almost at once.

code: 251, 'Q'

len: > 6

```
+--+--+--+--+--+--+--+--+--+...+--++
```

```
lalbl c ldlelfl g l
```

```
+--+--+--+--+--+--+--+--+--+...+--++
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute>

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'Q' (QoS-info code for Service)

g = <U;cir;normal burst;excess burst;D;cir;normal burst;excess burst>

'U' Upstream QoS parameters, 'D' downstream QoS parameters

### Destination Network

This attribute specifies the networks that belong to a service. The network can be either an include network or an exclude network. Users are not allowed to access exclude networks. This is configured in the service profile and should be present at least once.

code: 251, 'R'

len: > 12

```

+--+--+--+--+--+--+--+--+--+...--+
|a|b| c |d|e|f| g | l
+--+--+--+--+--+--+--+--+--+...--+

```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'R' (service-info code for destination network)

g = <ip;mask[;flag]>

(ip and mask are in dot notations, flag can be 'I' for INCLUDED or 'E' for EXCLUDED; flag is default to 'I')



**Note**

Within one RADIUS packet, there may be multiple instances of service-info subattributes for the destination network.

### RADIUS Server

This attribute specifies the RADIUS server to be used for authentication for the service. This is used only for proxy services. Using multiple instances of this attribute can be used to configure multiple servers.

code: 251, 'S'

len: > 7

```

+--+--+--+--+--+--+--+--+--+...--+
|a|b| c |d|e|f| g | l
+--+--+--+--+--+--+--+--+--+...--+

```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'S' (service-info code for RADIUS server)

g = <ip>;<auth port>;<acct port>;<secret>

### Service Type

This attribute specifies the type of the service. A service can be one of 'Proxy', 'Passthrough' or 'Tunnel' type. The default type of a service is 'Passthrough' if this attribute is not set in the service profile.

code: 251, 'T'

len: 4

```
+-----+
|a|b|c|d|e|f|g|
+-----+
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'T' (service-info code for service type)

g = 'X'/'T'/'P' (Proxy, Tunnel or Passthrough)

#### Service User Name

This attribute specifies the username in connection Accounting requests. The Accounting requests to the local AAA server contain the host's username, while the Accounting requests to the remote AAA server for proxy services contain the username that the user used to logon to the service.

code: 251, 'U'

len: 4

```
+-----+
|a|b|c|d|e|f|g|
+-----+
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute)

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'U' (service-info code for service user name)

g = <user name>



#### Note

Note: Currently, only Connection Accounting packet uses this subattribute.

**Service Defined Cookie For Proxy RADIUS**

This attribute specifies a cookie string for a service. This string is sent in all Access-Requests for authentication for a connection and also in all Accounting-Requests for the connections to this service.

This attribute is configured in the service profile and can be appear almost at once.

code: 251, 'V'

len: >=4

+--+--+--+--+--+--+--+

l|a|b| c |d|e|f|g|

+--+--+--+--+--+--+--+

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute>

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'V' (service-info code for service defined cookie)

g = <service defined cookie>

**Enable Full User Name for Proxy RADIUS**

If this attribute is set for a service, the service name is appended to the username during authentication to the service as 'username@servicename'. This attribute is configured in a service profile and can appear almost at once.

code: 251, 'X'

len: 3

+--+--+--+--+--+--+--+

l|a|b| c |d|e|f|

+--+--+--+--+--+--+--+

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS Vendor specific Attribute>

c = 9 (Cisco vendor ID)

d = 251 (Subattribute ID for Service-Info)

e = len (length of the vendor specific subattribute)

f = 'X' (service-info code for service defined cookie)



code: 253, 'F'  
len: > 12

```
+--+--+--+--+--+--+--+--+...--+--+--+
|a|b|c|d|e|f|g| |h| |
+--+--+--+--+--+--+--+--+...--+--+--+
```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS vendor-specific)  
c = 9 (Cisco vendor ID)  
d = 253 (subattribute ID for Service-Info)  
e = len (length of the vendor-specific filter)  
p = 'F' (Port filter indication flag)  
g = <src ip:src portlist;mask;>  
h = <dst ip:dst portlist;mask;flag;filterID>

**Note**

The portlist can be a list of port numbers delimited by ",". "-" can be used to specify a range. For example, a port list consists of 23, 34, 35, and all the ports that are greater than 3000 can be specified as "23,34-35,3001-". The flag is either 'D' for deny or 'P' for permit.

**Next Hop Gateway Table Entry**

This attribute is used in a next-hop table profile to associate a next-hop key with an IP address. The keys are used in the service profile's Next-hop gateway attribute. This attribute can appear multiple times to create a Next Hop Gateway Table. Each SSG can have a Next Hop Gateway Table defined, and each service can reference entries in this table by using the Service-Info Next Hop Gateway attribute.

code: 253, 'G'  
len: > 12

```
+--+--+--+--+--+--+--+--+...--+--+--+
|a|b|c|d|e|f|g| |
+--+--+--+--+--+--+--+--+...--+--+--+
```

a = 26 (RADIUS attr for vendor specific)  
b = len (length of the RADIUS vendor-specific)  
c = 9 (Cisco vendor ID)  
d = 253 (subattribute ID for Service-Info)  
e = len (length of the vendor-specific filter)  
p = 'G' (Next Hop Gateway Entry Flag)

g = <key;ip> (key can be any string; ip is the corresponding next hop gateway IP in dot notation)

### Input Bytes Count

This attribute is used to indicate the number of input bytes and is used in accounting packets only. For this attribute to be sent in an accounting request by SSG, the **aaa accounting send vsa** command should be enabled on SSG.

code: 253, 'I'

len: > 12

```
+--+--+--+--+--+--+--+--+...
```

```
label c |d|e|f|p| g |
```

```
+--+--+--+--+--+--+--+--+...
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS vendor-specific)

c = 9 (Cisco vendor ID)

d = 253 (subattribute ID for Service-Info)

e = len (length of the vendor-specific filter)

p = 'I' (Input Bytes Count Flag)

g = <HI;LOW> (Formula to calculate exact byte count is HI\*4294967296 + LOW)

### Output Bytes Count

This attribute is used to indicate the number of output bytes and is used in accounting packets only. For this attribute to be sent in an accounting request by SSG, you should enable the **aaa accounting send vsa** command on SSG.

code: 253, 'O'

len: > 12

```
+--+--+--+--+--+--+--+--+...
```

```
label c |d|e|f|p| g |
```

```
+--+--+--+--+--+--+--+--+...
```

a = 26 (RADIUS attr for vendor specific)

b = len (length of the RADIUS vendor-specific)

c = 9 (Cisco vendor ID)

d = 253 (subattribute ID for Service-Info)

e = len (length of the vendor-specific filter)

p = 'O' (Output Bytes Count Flag)

g = <HI;LOW> (Formula to calculate exact byte count is HI\*4294967296 + LOW)



**Note** This attribute is for accounting packets only.

## Subscriber Profiles

RADIUS subscriber profiles contain a password, a list of subscribed services and groups, and access control lists.

Table 8 describes attributes that appear in RADIUS user profiles.

**Table 8** *Subscriber Profile Attributes*

Attribute	Description
<b>Cisco AV Pair Attributes</b>	
<a href="#">Downstream Access Control List</a> (outacl)	Specifies either a Cisco IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
<a href="#">Upstream Access Control List</a> (inacl)	Specifies either a Cisco IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.
<b>Account-Info Attributes</b>	
<a href="#">Auto Service</a>	(Reply attribute) Automatically logs a user in to a service when the user logs in to SSG.
<a href="#">Home URL</a>	(Optional) The URL for the user's preferred Internet home page.
<a href="#">Service Group</a>	(Reply attribute) Subscribes the user to a service group. Multiple instances of this attribute can occur within a single user profile. Use one attribute for each service group to which the user is subscribed.
<a href="#">Service Name</a>	(Reply attribute) Subscribes the user to a service. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service to which the user is subscribed.
<b>Standard Attributes<sup>1</sup></b>	
Framed-IP-Netmask	Indicates the IP net mask to be configured for the user when the user is a router to a network. This attribute value results in the adding of a static route for Framed-IP-Address with the mask specified.
Idle-Timeout	(Reply attribute) Specifies, in seconds, the maximum length of time for which a connection can remain idle.
Password	(Check attribute) Specifies the user's password.
Session-Timeout	(Reply attribute) Specifies, in seconds, the maximum length of the user's session.

1. Standard attributes are described in detail in RFC 2138.

## Downstream Access Control List

The Downstream Access Control List attribute specifies either a Cisco IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.

```
Cisco-AVpair = "ip:outacl[#number]={standard-access-control-list |
extended-access-control-list}"
```

### Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

### Example

```
Cisco-AVpair = "ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



**Note** Multiple instances of the Downstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

## Upstream Access Control List

The Upstream Access Control List attribute specifies either a Cisco IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

```
Cisco-AVpair = "ip:inacl[#number]={standard-access-control-list |
extended-access-control-list}"
```

### Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

### Example

```
Cisco-AVpair = "ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



**Note** Multiple instances of the Upstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

## Auto Service

The Auto Service attribute subscribes the user to a service and automatically logs the user in to the service when the user accesses SESM. A user profile can have more than one Auto Service attribute.

```
Account-Info = "Aservicename[ ;username;password]"
```

**Syntax Description**

<i>servicename</i>	Name of the service.
<i>username</i>	Username used to access the service. Required for proxy services.
<i>password</i>	Password used to access the service. Required for proxy services.

**Example**

```
Account-Info = "Afictiousname.net;jdoe;secret"
```

**Note**

The user must be subscribed to this service.

**Home URL**

The Home URL attribute specifies the URL for the user's preferred Internet home page. This attribute is optional.

```
Account-Info = "Hurl"
```

or

```
Account-Info = "Uurl"
```

**Syntax Description**

<i>url</i>	A fully qualified URL for the user's preferred Internet home page.
------------	--

**Usage**

If the SESM web application is designed to use HTML frames, the Home URL attribute also specifies whether the home page is displayed in a new browser window or in a frame in the current (SESM) window, as follows:

- **Hurl**—URL for the home page displayed in a frame in the SESM browser window.
- **Uurl**—URL for the home page displayed in its own browser window.

**Note**

In a frameless application, both **H** and **U** cause a new browser window to open for the home page. The New World Service Provider (NWSP) application is a frameless application.

**Example**

```
Account-Info = "Uhttp://www.fictiousname.com"
```

**Service Group**

In user profiles, the Service Group attribute subscribes a user to a service group. In service group profiles, this attribute lists the service subgroups that belong to the service group.

```
Account-Info = "Gname"
```

**Syntax Description**

<i>name</i>	Name of the group profile.
-------------	----------------------------

**Example**

```
Account-Info = "GServiceGroup1"
```



**Note** Multiple instances of this attribute can occur within a user or service-group profile. Use one attribute for each service subgroup.

**Service Name**

In user profiles, the Service Name attribute subscribes the user to the specified service. In service-group profiles, this attribute lists services that belong to the service group.

```
Account-Info = "Nname"
```

**Syntax Description**

<i>name</i>	Name of the service profile.
-------------	------------------------------

**RADIUS Freeware Format Example**

```
Account-Info = "Ncisco.com"
```

**CiscoSecure ACS for UNIX Example**

```
9,250="cisco.com"
```



**Note** Multiple instances of this attribute can occur within a user or service profile. Use one attribute for each service.

**Service Profiles**

Service profiles define the services that subscribers can select. Each service that is accessible has a profile that defines the attributes of the service. Service profiles are configured on the RADIUS server or directly on SSG. The RADIUS server or SESM downloads the service profiles to SSG as needed.

Service profiles include the following information: password, service type (outbound), type of service (passthrough or proxy), service access mode (sequential or concurrent), DNS server IP address, networks that exist in the service domain, access control lists, and timeouts. The following sections describe the attributes included in RADIUS service profiles.

**Downstream Access Control List**

Specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.

```
Cisco-AVpair = "ip:outacl [#number]={standard-access-control-list | extended-access-control-list}"
```

**Syntax Description**

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

**Example**

```
Cisco-AVpair = "ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```

**Note**

Multiple instances of the Downstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

**Upstream Access Control List**

Specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

```
Cisco-AVpair = "ip:inacl[#number]={standard-access-control-list |
extended-access-control-list}"
```

**Syntax Description**

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

**Example**

```
Cisco-AVpair = "ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```

**Note**

Multiple instances of the Upstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

**L2TP Tunnel Password**

Specifies the secret (the password) used for the L2TP tunnel authentication.

```
Cisco-AVpair = "vpdn:tunnel-password=secret"
```

**Syntax Description**

<i>secret</i>	Secret (password) for L2TP tunnel authentication.
---------------	---

**RADIUS Freeware Format Example**

```
Cisco-AVpair = "vpdn:l2tp-tunnel-password=cisco"
```

**CiscoSecure ACS for UNIX Example**

```
9,1 = "vpdn:l2tp-tunnel-password=cisco"
```

**VPDN IP Address**

Specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.

```
Cisco-AVpair =
"vpdn:ip-addresses=address1[<delimiter>address2] [<delimiter>address3]..."
```

**Syntax Description**

<i>address</i>		IP address of the home gateway.
<i>&lt;delimiter&gt;</i>	, (comma)	Selects load sharing among IP addresses.
	(space)	Selects load sharing among IP addresses.
	/ (slash)	Groups IP addresses on the left side of the slash in higher priority than those on the right side of the slash.

In the following example, the LAC sends the first PPP session through a tunnel to 10.1.1.1, the second PPP session to 10.2.2.2, and the third to 10.3.3.3. The fourth PPP session is sent through the tunnel to 10.1.1.1, and so forth. If the LAC fails to establish a tunnel with any of the IP addresses in the first group, then it attempts to connect to those in the second group (10.4.4.4 and 10.5.5.5).

**RADIUS Freeware Format Example**

```
Cisco-AVpair = "vpdn:ip-addresses=10.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

**CiscoSecure ACS for UNIX Example**

```
9,1 = "vpdn:ip-addresses=10.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

**VPDN Tunnel ID**

Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.

```
Cisco-AVpair = "vpdn:tunnel-id=name"
```

**Syntax Description**

<i>name</i>	Tunnel name.
-------------	--------------

**RADIUS Freeware Format Example**

```
Cisco-AVpair = "vpdn:tunnel-id=My-Tunnel"
```

**CiscoSecure ACS for UNIX Example**

```
9,1 = "vpdn:tunnel-id=My-Tunnel"
```

**L2TP Hello Interval**

Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.

```
Cisco-AVpair = "vpdn:l2tp-hello-interval=interval"
```

**Syntax Description**

<i>interval</i>	Interval at which hello keepalive packets are sent, in seconds.
-----------------	---

**RADIUS Freeware Format Example**

```
Cisco-AVpair = "vpdn:l2tp-hello-interval=2"
```

**CiscoSecure ACS for UNIX Example**

```
9,1 = "vpdn:l2tp-hello-interval=2"
```

## attribute filter

Some services require the MSISDN to be hidden from the service provider. To support this capability, you can add an attribute filter to the service profile. You can specify the attributes to be filtered from authentication and accounting records sent to the remote AAA server.

The SSG Service-Info VSA lists the RADIUS attributes to filter from user authentication for the service; this capability applies to both proxy RADIUS service and L2TP tunnel service. At present you can only filter attribute 31 (Calling Station ID).

The Calling Station ID is filtered only from connection authentication for proxy and L2TP tunnel services and for connection accounting records sent to the remote AAA server.

Table 9 shows the format of the Service-Info VSA needed to enable attribute filtering.

**Table 9 SSG Service-Info VSA Descriptions**

Attribute ID	Vendor ID	Subattribute ID	Attribute Name	Subattribute Data
26	9	250	Service-Info	The value F is the filter indication flag and should be set as F31.

Table 10 lists the attributes used for service logon with and without the MSISDN and with MSISDN filter set to F31.

**Table 10 Service Logon Comparison (With MSISDN, Without MSISDN, and With MSISDN Filter)**

Service Logon	Connection Authentication <sup>1</sup>	Connection Accounting to Local AAA	Connection Accounting to Remote AAA <sup>2</sup>	Prepaid (Re)authorization	Prepaid Accounting
Without MSISDN	Host Calling ID	Host Calling ID	Host Calling ID	Host Calling ID	Host Calling ID
With MSISDN <sup>3</sup>	Connection Calling ID	Host Calling ID	Connection Calling ID	Host Calling ID	Host Calling ID
With MSISDN filter set to F31	Calling ID not sent	Host Calling ID	Calling ID not sent	Host Calling ID	Host Calling ID

1. Calling Station ID in RADIUS (attribute 31) in authentication for proxy services or calling number AVP (22) for L2TP tunnel services.
2. Only for proxy services.
3. Service profile is not set to filter MSISDN.

You can use the **show ssg connection** command to display the attributes that are being filtered.

## DNS Server Address

(Optional) Specifies the primary and/or secondary DNS servers for this service.

If two servers are specified, SSG can send DNS requests to the primary DNS server until performance is diminished or it fails (failover).

```
Service-Info = "Dip_address_1[;ip_address_2]"
```

**Syntax Description**

<i>ip_address_1</i>	IP address of the primary DNS server.
<i>ip_address_2</i>	(Optional) IP address of the secondary DNS server used for fault tolerance.

**Example**

```
Service-Info = "D192.168.1.2;192.168.1.3"
```

**Domain Name**

(Optional) Specifies domain names that get DNS resolution from the DNS servers specified by the DNS server address.

```
Service-Info = "Oname1[;name2]...[;nameX]"
```

**Syntax Description**

<i>name1</i>	Domain name that gets DNS resolution from this server.
<i>name2...X</i>	(Optional) Additional domain names that get DNS resolution from this server.

**Usage**

Use the DNS Resolution attribute to specify domain names that get DNS resolution from this DNS server.

**Example**

```
Service-Info = "Ocisco.com;cisco-sales.com"
```

**Note**

Multiple instances of the Domain Name attribute can occur within a single service profile.

**Full Username**

Indicates that RADIUS authentication and accounting requests use the full username (user@service). This attribute is supported by SSG with SSD or SESM in RADIUS mode.

```
Service-Info = "X"
```

The size of the full username is limited to the smaller of the following values:

- 246 bytes (10 bytes less than the standard RADIUS protocol limitation)
- 10 bytes less than the maximum size of the RADIUS attribute supported by your proxy

**RADIUS Freeware Format Example**

```
Service-Info = "X"
```

**CiscoSecure ACS for UNIX Example**

```
9,251 = "X"
```

**MTU Size**

Specifies the PPP MTU size of SSG as a LAC. By default, the PPP MTU size is 1500 bytes.

```
Service-Info = "Bsize"
```

**Note**

SESM in LDAP mode does not support the use of this attribute.

**Syntax Description**

<i>size</i>	MTU size in bytes
-------------	-------------------

**RADIUS Freeware Format Example**

```
9,251 = "B1500"
```

**CiscoSecure ACS for UNIX Example**

```
9,1 = "B1500"
```

**RADIUS Server**

(Required for proxy services.) Specifies the remote RADIUS servers that SSG uses to authenticate, authorize, and perform accounting for a service logon for a proxy service type. This attribute is only used in proxy service profiles and is required.

You can configure each remote RADIUS server with timeout and retransmission parameters. SSG will perform failover among the servers.

**Service-Info =**

```
"SRadius-server-address;auth-port;acct-port;secret-key[;retrans;timeout;deadtime]"
```

**Syntax Description**

<i>RADIUS-server-address</i>	IP address of the RADIUS server.
<i>auth-port</i>	UDP port number for authentication and authorization requests.
<i>acct-port</i>	UDP port number for accounting requests.
<i>secret-key</i>	Secret key shared with RADIUS clients.
<i>retrans</i>	Number of retransmissions. Default is 3.
<i>timeout</i>	Time, in seconds, before retransmission. Default is 5.
<i>deadtime</i>	Time, in minutes, during which SSG does not try to perform authentication or accounting with a AAA server that was detected as down. Default is 10.

**Example**

```
Service-Info = "S192.168.1.1;1645;1646;cisco"
```

**Service Authentication Type**

Specifies whether SSG uses the CHAP or PAP protocol to authenticate users for proxy services.

**Service-Info = "Aauthen-type"**

**Syntax Description**

<i>authen-type</i>	C—CHAP Authentication. P—PAP Authentication.
--------------------	---

**Example**

```
Service-Info = "AC"
```

**Service-Defined Cookie**

Enables you to include user-defined information in RADIUS authentication and accounting requests. This attribute is supported by SSG with SSD or SESM in RADIUS mode.

```
Service-Info = "Vstring"
```

**Syntax Description**

<i>string</i>	Information that you choose to include in the RADIUS authentication and accounting requests.  The size of the user-defined <i>string</i> is limited to the smaller of the following values: <ul style="list-style-type: none"> <li>• 246 bytes (10 bytes less than the standard RADIUS protocol limitation)</li> <li>• 10 bytes less than the maximum size of the RADIUS attribute supported by your proxy</li> </ul>
---------------	---

**RADIUS Freeware Format Example**

```
Service-Info = "VserviceIDandAAA-ID"
```

**CiscoSecure ACS for UNIX Example**

```
9,251 = "VserviceIDandAAA-ID"
```

**Note**

SSG does not parse or interpret the value of the Service-Defined Cookie. You must configure the proxy RADIUS server to interpret this attribute.

**Note**

SSG supports only one Service-Defined Cookie per RADIUS service profile.

**Service Description**

(Optional) Describes the service.

```
Service-Info = "Idescription"
```

**Syntax Description**

<i>description</i>	Description of the service.
--------------------	-----------------------------

**Example**

```
Service-Info = "ICompany Intranet Access"
```

**Service Mode**

(Optional) Defines whether the user is able to log on to this service while simultaneously connected to other services (concurrent mode) or whether the user cannot access any other services while using this service (sequential mode). The default is concurrent mode.

```
Service-Info = "Mmode"
```

**Syntax Description**

<i>mode</i>	S—Sequential mode. C—Concurrent mode. This is the default.
-------------	---

**Example**

```
Service-Info = "MS"
```

**Service Next-Hop Gateway**

(Optional) Specifies the next-hop key for this service. Each SSG uses its own next-hop gateway table to associate this key with an actual IP address.

```
Service-Info = "Gkey"
```

**Syntax Description**

<i>key</i>	Name of the next hop.
------------	-----------------------

**Example**

```
Service-Info = "GnextHop1"
```

**Service Route**

Specifies networks available to the user for this service.

```
Service-Info = "Rip_address;mask"
```

**Syntax Description**

<i>ip_address</i>	IP address.
<i>mask</i>	Subnet mask.

**Usage**

Use the Service Route attribute to specify networks that exist for a service.

**Note**

An Internet service is typically specified as "**R0.0.0.0;0.0.0.0**" in the service profile.

**Example**

```
Service-Info = "R192.168.1.128;255.255.255.192"
```

**Note**

There can be multiple instances of the Service Route attribute within a single service profile.

**Service URL**

(Optional) Specifies the URL that is displayed in the SESM HTTP address field when the service opens.

```
Service-Info = "Hurl"
```

or

```
Service-Info = "Uurl"
```

If the SESM web application is designed to use HTML frames, this attribute also specifies whether the service is displayed in a new browser window or in a frame in the current (SESM) window, as follows:

- **Hurl**—URL for a service displayed in a frame in the SESM browser window.
- **Url**—URL for a service displayed in its own browser window.

**Note**

In a frameless application, both **H** and **U** cause a new browser window to open for the service. The NWSP application is a frameless application.

**Example**

```
Service-Info = "Uhttp://www.fictitiousname.com"
```

**Type of Service**

(Optional) Indicates whether the service is proxy, tunnel, or passthrough.

```
Service-Info = "Ttype"
```

**Syntax Description**

<i>type</i>	P—Pass-through. Indicates that the user's packets are forwarded through the SSG. This is the default.
	T—Tunnel. Indicates that this is a tunneled service.
	X—Proxy. Indicates that the SSG performs proxy service.

**RADIUS Freeware Format Example**

```
Service-Info = "TT"
```

**CiscoSecure ACS for UNIX Example**

```
9,251 = "TT"
```

**Service Group Profiles**

Service group profiles contain a list of services and service groups and can be used to create directory structures for locating and logging in to services. When a user is subscribed to a service group, the user is automatically subscribed to all services and groups within that service group. A service-group profile includes the password and the service type (outbound) as check attributes and a list of services and a list of service groups as reply attributes.

[Table 11](#) describes attributes that can be used in SSG service-group profiles.

**Table 11** *Service-Group Profile Attributes*

Attribute	Description
<b>Account-Info Attributes</b>	
<a href="#">Group Description</a>	Provides a description of the service group.
<a href="#">Service Group</a>	(Reply attribute) Lists services that belong to the service group. Multiple instances of this attribute can occur within a single user profile. Use one attribute for each service.

**Table 11** *Service-Group Profile Attributes*

Attribute	Description
<a href="#">Service Name</a>	Lists the service subgroups that belong to the service group. When configured, the service-group and service-name attributes can define an organized directory structure for accessing services.  There can be multiple instances of this attribute within a service-group profile. Use one attribute for each service subgroup that belongs to this service group.
<b>Standard Attributes<sup>1</sup></b>	
Password	(Check attribute) Specifies the password.
Service-Type	(Check attribute) Specifies the level of service. Must be "outbound."

1. Standard attributes are described in detail in RFC 2138.

## Group Description

Describes the service group to SESM. If this attribute is omitted, the service group profile name is used.

**Account-Info** = "*Idescription*"

### Syntax Description

<i>description</i>	Description of the service group.
--------------------	-----------------------------------

### Example

**Account-Info** = "ICompany Intranet Access"

## Service Group

In user profiles, the Service Group attribute subscribes a user to a service group. In service group profiles, this attribute lists the service subgroups that belong to the service group.

**Account-Info** = "*Gname*"

### Syntax Description

<i>name</i>	Name of the group profile.
-------------	----------------------------

### Example

**Account-Info** = "GServiceGroup1"



**Note** Multiple instances of the Service Group attribute can occur within a user or service-group profile. Use one attribute for each service subgroup.

## Service Name

In user profiles, the Service Name attribute subscribes the user to the specified service. In service-group profiles, this attribute lists services that belong to the service group.

**Account-Info** = "*Nname*"

**Syntax Description**

<i>name</i>	Name of the service profile.
-------------	------------------------------

**Example**

```
Account-Info = "Ncisco.com"
```



**Note** Multiple instances of the Service Name attribute can occur within a user or service profile. Use one attribute for each service.

**Pseudo-Service Profiles**

Pseudo-service profiles are used to define variable-length tables or lists of information in the form of services. There are currently two types of pseudo-service profiles: Transparent Pass-Through Filter and Next-Hop Gateway. The following sections describe both profiles.

**Transparent Pass-Through Filter Pseudo-Service Profile**

Transparent pass-through is designed to allow unauthenticated traffic (users or network devices that have not logged in to the SSG through SESM) to be routed through normal Cisco IOS processing.

Table 12 lists the Cisco AVPair attributes that appear within transparent pass-through filter pseudo-service profiles. The Cisco-AVpair attributes are used to configure ACLs.

**Table 12** *Transparent Pass-Through Filter Pseudo-Service Profile Attributes*

Attribute	Description
<a href="#">Downstream Access Control List (outacl)</a>	Specifies either a Cisco IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
<a href="#">Upstream Access Control List (inacl)</a>	Specifies either a Cisco IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

**Downstream Access Control List**

The Downstream Access Control List attribute specifies either a Cisco IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.

```
cisco-AVpair = "ip:outacl[#number]={standard-access-control-list | extended-access-control-list}"
```

**Syntax Description**

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

**Example**

```
Cisco-AVpair = "ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



**Note** Multiple instances of the Downstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

### Upstream Access Control List

This attribute specifies either a Cisco IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

```
Cisco-AVpair = "ip:inacl[#number]={standard-access-control-list |
extended-access-control-list}"
```

### Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

### Example

```
Cisco-AVpair = "ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



**Note** Multiple instances of the Upstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

The Transparent Pass-Through Filter pseudo-service profile allows or denies access to IP addresses and ports accessed through the transparent pass-through feature.

To define what traffic can pass through, SSG downloads the Transparent Pass-Through Filter pseudo-service profile. This profile contains a list of ACL attributes. Each item contains an IP address or range of IP addresses and a list of port numbers and specifies whether traffic is allowed or denied.

To create a filter for transparent pass-through, create a profile that contains ACL attributes that define what can and cannot be accessed.

You can also create ACLs locally.

## Next-Hop Gateway Pseudo-Service Profile

Because multiple SSGs might access services from different networks, each service profile can specify a next-hop key, which is any string identifier, rather than an actual IP address. For each SSG to determine the IP address of the next hop, each SSG downloads its own next-hop gateway table, which associates keys with IP addresses. [Table 13](#) describes the attribute that can be used in Next-Hop Gateway pseudo-service profiles.

**Table 13** Next-Hop Gateway Pseudo-Service Profile Attributes

Attribute	Usage
<a href="#">Next-Hop Gateway Table Entry</a>	Associates next-hop gateway keys with IP addresses.

### Next-Hop Gateway Table Entry

Because multiple SSGs might access services from different networks, each service profile specifies a next-hop key rather than an actual IP address. For each SSG to determine the IP address of the next hop, each SSG downloads its own next-hop gateway table, which associates keys with IP addresses.

**Note**

The Next-Hop Gateway Table Entry attribute is used only in Next-Hop Gateway pseudo-service profiles and should not appear in service profiles or user profiles.

```
Control-Info = "key;ip_address"
```

### Syntax Description

<i>key</i>	Service name or key specified in the Next-Hop Gateway service profile.
<i>ip_address</i>	IP address of the next hop for this service.

### Usage

Use this attribute to create a next-hop gateway table for the selected SSG.

To define the IP address of the next hop for each service, SSG downloads a special service profile that associates the next-hop gateway key for each service with an IP address.

To create a next-hop gateway table, create a service profile and give it any name. Use this attribute to associate service keys with their IP addresses. When you have finished, repeat this process for each SSG.

### Example

```
Control-Info = "GNHT_for_SSG_1;192.168.1.128"
```

To create a next-hop gateway table, create a profile and give it any name. Use the Next-Hop Gateway Entry attribute to associate service keys with their IP addresses. When you have finished, repeat this process for each SSG if the next-hop IP addresses are different.

## Examples of SSG RADIUS Profiles

### Subscriber Profile: Examples

The following is an example of a user profile. The profile is formatted for use with a freeware RADIUS server:

```
bert Password = "ernie"
Session-Timeout = 21600,
Account-Info = "GServiceGroup1",
Account-Info = "Nservice1.com",
Account-Info = "Ngamers.net"
```

The following is the same profile as above, formatted for CiscoSecure ACS for UNIX:

```
user = bert {
radius = SSG {
check_items = {
2 = "ernie"
}
reply_attributes = {
27 = 21600
9,250 = "GServiceGroup1"
9,250 = "Nservice1.com"
9,250 = "Ngamers.net"
```

## Service Profile: Examples

### Service Profile Formatted for use with a Freeware RADIUS Server: Example

The following is a service profile formatted for use with a freeware RADIUS server:

```

servicel.com Password = "cisco", Service-Type = outbound,
Idle-Timeout = 1800,
Service-Info = "R192.168.1.128;255.255.255.192",
Service-Info = "R192.168.2.0;255.255.255.192",
Service-Info = "R192.168.3.0;255.255.255.0",
Service-Info = "Gservicel",
Service-Info = "D192.168.2.81",
Service-Info = "MC",
Service-Info = "TP",
Service-Info = "ICompany Intranet Access",
Service-Info = "Oservicel.com"

```

### Service Profile Formatted for use with a Freeware RADIUS Server Formatted for CiscoSecure ACS for UNIX: Example

The following is the same profile as above, formatted for CiscoSecure ACS for UNIX:

```

user = servicel.com {
radius = SSG {
check_items = {
2 = "cisco"
6 = 5
}
reply_attributes = {
28 = 1800
9,251 = "R192.168.1.128;255.255.255.192"
9,251 = "R192.168.2.0;255.255.255.192"
9,251 = "R192.168.3.0;255.255.255.0"
9,251 = "Gservicel"
9,251 = "D192.168.2.81"
9,251 = "MC"
9,251 = "TP"
9,251 = "ICompany Intranet Access"
9,251 = "Oservicel.com"
}
}

```

### RADIUS ProxyService Profile: Example

The following is an example of a proxy RADIUS service profile. This profile contains the Service-Defined Cookie attribute and a Full Username attribute.

```

user = serv1-proxy{
profile_id = 98
profile_cycle = 42
member = Single_Logon
radius=6510-SSG-v1.1a {
check_items= {
2=alex
}
reply_attributes= {
9,251="Oservicel.com"
9,251="R10.13.0.0;255.255.0.0"
9,251="TX"
9,251="D10.13.1.5"
9,251="S10.13.1.2;1645;1646;my-secret"
9,251="Gmy-key"
9,251="X"
9,251="Vproxy-service_at_X.X.X.X"
}
}

```

```
}

```

## Service Group Profile: Examples

### Service Group Profile Formatted for use with a Freeware RADIUS Server: Example

The following is an example of a service group profile. The profile is formatted for use with a freeware RADIUS server:

```
ServiceGroup1 Password = "cisco", Service-Type = outbound,
Account-Info = "Nservice1.com",
Account-Info = "Ngamers.net",
Account-Info = "GServiceGroup3",
Account-Info = "GServiceGroup4",
Account-Info = "IStandard User Services"
```

### Service Group Profile Formatted for use with a Freeware RADIUS Server Formatted for CiscoSecure ACS for UNIX: Example

The following is the same service-group profile, formatted for CiscoSecure ACS for UNIX:

```
user = ServiceGroup1 {
radius = SSG {
check_items = {
2 = "cisco"
6 = 5

reply_attributes = {
9,250 = "Nservice1.com"
9,250 = "Ngamers.net"
9,250 = "GServiceGroup3"
9,250 = "GServiceGroup4"
9,250 = "IStandard User Services"
}
}
```

## Pseudo-Service Profile: Examples

### Transparent Pass-Through Filter Pseudo-Service Profile: Example

The following is an example of the Transparent Pass-Through Filter pseudo-service profile. The profile is formatted for use with a freeware RADIUS server:

```
ssg-filter Password = "cisco", Service-Type = outbound,
Cisco-AVpair="ip:inacl#3=deny tcp 192.168.1.0 0.0.0.255 any eq 21",
Cisco-AVpair="ip:inacl#7=permit ip any any"
```

The following is the same profile as above, formatted for CiscoSecure ACS for UNIX:

```
user = ssg-filter {
radius = SSG {
check_items = {
2 = "cisco"
6 = 5

reply_attributes = {
9,1 = "ip:inacl#3=deny tcp 192.168.1.0 0.0.0.255 any eq 21",
9,1 = "ip:inacl#7=permit ip any any"
}
}
}
```

### Next-Hop Gateway Pseudo-Service Profile Example

The following is an example of the Next-Hop Gateway pseudo-service profile. The profile is formatted for use with a freeware RADIUS server:

```
nht1          Password = "cisco", Service-Type = outbound,
Account-Info = "Gservice3;192.168.103.3",
Account-Info = "Gservice2;192.168.103.2",
Account-Info = "Gservice1;192.168.103.1",
Account-Info = "GLabservices;192.168.4.2",
Account-Info = "GWorldwide_Gaming;192.168.4.2"
```

The following is the same Next-Hop Gateway pseudo-service profile, formatted for CiscoSecure ACS for UNIX:

```
user = nht1{
radius= SSG {
check_items= {
2=cisco
6=5
}
reply_attributes= {
9,253="Gservice3;192.168.103.3"
9,253="Gservice2;192.168.103.2"
9,253="Gservice1;192.168.103.1"
9,253="GLabservices;192.168.4.2"
9,253="GWorldwide_Gaming;192.168.4.2"
}
}
```

## RADIUS Accounting Records for SSG

This section describes the following concepts:

- [Account Logon, page 47](#)
- [Account Logoff, page 48](#)
- [Connection Start, page 49](#)
- [Connection Stop, page 50](#)
- [Attributes Used in Accounting Records, page 52](#)



#### Note

---

This section applies if you are using SSG with SSD or SESM in RADIUS or LDAP mode.

---

This section describes events that generate RADIUS accounting records and the attributes associated with the accounting records sent from SSG to the accounting server.

### Account Logon

When a user logs in, SSG sends a RADIUS accounting request on behalf of the user to the accounting server. The following example shows the information contained in the RADIUS accounting-request record:

```
Acct-Status-Type = Start
NAS-IP-Address = ip_address
User-Name = "username"
Acct-Session-Id = "session_id"
```

```
Framed-IP-Address = user_ip
Proxy-State = "n"
```

Table 14 describes the attributes shown in the display.

**Table 14 Account Logon Accounting Record Attributes**

Attribute	Description
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).
NAS-IP-Address	IP address of SSG.
User-Name	Name used to log on to the service provider network.
Acct-Session-Id	Session number.
Framed-IP-Address	IP address of the user's system.
Proxy-State	Accounting record queuing information (has no effect on account billing).

## Account Logoff

When a user logs out, the SSG sends a RADIUS accounting request on behalf of the user to the accounting server. The following example shows the information contained in the RADIUS accounting-request record:

```
Acct-Status-Type = Stop
NAS-IP-Address = ip_address
User-Name = "username"
Acct-Session-Time = time
Acct-Terminate-Cause = cause
Acct-Session-Id = "session_id"
Framed-IP-Address = user_ip
Proxy-State = "n"
```

Table 15 describes the attributes shown in the display.

**Table 15 Account Logoff Accounting Record Attributes**

Attribute	Description
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).
NAS-IP-Address	IP address of SSG.
User-Name	Name used to log on to the service provider network.
Acct-Session-Time	Length of session, in seconds.
Acct-Terminate-Cause	Cause of account termination: <ul style="list-style-type: none"> <li>• User-Request</li> <li>• Session-Timeout</li> <li>• Idle-Timeout</li> <li>• Lost-Carrier</li> </ul>
Acct-Session-Id	Session number.

**Table 15** Account Logoff Accounting Record Attributes (continued)

Attribute	Description
Framed-IP-Address	IP address of the user's system.
Proxy-State	Accounting record queuing information (has no effect on account billing).

## Connection Start

When a user accesses a service, SSG sends a RADIUS Accounting-Request to the accounting server. The following example shows the information contained in the RADIUS Accounting-Request record:

```
NAS-IP-Address = 172.16.6.1
NAS-Port = 0
NAS-Port-Type = Virtual
User-Name = "username"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "00000010"
Framed-Protocol = PPP
Service-Info = "Nisp-name.com"
Service-Info = "Username"
Service-Info = "TP"
Acct-Delay-Time = 0
```

Table 16 describes the attributes shown in the display.

**Table 16** Connection Start Accounting Record Attributes

Attribute	Description
NAS-IP-Address	IP address of SSG.
NAS-Port	Physical port number of the network access server that is authenticating the user.
NAS-Port-Type	Type of physical port that the network access server is using to authenticate the user.
User-Name	Name used to log on to the service provider network.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS, the network access server itself, or another remote authentication protocol.
Service-Type	Indicates the type of service requested or the type of service to be provided. PPP and SLIP connections use the service type "Framed".
Acct-Session-Id	Session number.
Framed-Protocol	Indicates the framing to be used for framed access.
Service-Info	"Nname". Name of the service profile.
Service-Info	"Uname". Username used to authenticate the user with the remote RADIUS server. This attribute is used for proxy services.

**Table 16** Connection Start Accounting Record Attributes (continued)

Attribute	Description
Service-Info	<p>“Type”. Indicates whether the connection is proxy, tunnel, or pass-through.</p> <ul style="list-style-type: none"> <li>• P—Pass-through (usually the Internet)</li> <li>• T—Tunnel</li> <li>• X—Proxy</li> </ul>
Acct-Delay-Time	Indicates for how many seconds the client has been trying to send a particular record.

## Connection Stop

When a user terminates a service, SSG sends a RADIUS Accounting-Request to the accounting server. The following example shows the information contained in the RADIUS Accounting-Request record:

```

NAS-IP-Address = 192.168.2.48
NAS-Port = 0
NAS-Port-Type = Virtual
User-Name = "zeus"
Acct-Status-Type = Stop
Service-Type = Framed-User
Acct-Session-Id = "00000002"
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 84
Acct-Input-Octets = 0
Acct-Output-Octets = 649
Acct-Input-Packets = 0
Acct-Output-Packets = 17
Framed-Protocol = PPP
Framed-IP-Address = 201.168.101.10
Control-Info = "I0;0"
Control-Info = "O0;649"
Service-Info = "Ninternet"
Service-Info = "Uzeus"
Service-Info = "TP"
Acct-Delay-Time = 0

```

Table 17 describes the attributes shown in the display.

**Table 17** Connection Stop Accounting Record Attributes

Attribute	Description
NAS-IP-Address	IP address of SSG.
NAS-Port	Physical port number of the network access server that is authenticating the user.
NAS-Port-Type	Type of physical port that the network access server is using to authenticate the user.
User-Name	Name used to log on to the service provider network.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).

**Table 17** *Connection Stop Accounting Record Attributes (continued)*

<b>Attribute</b>	<b>Description</b>
Service-Type	Indicates the type of service requested or the type of service to be provided. PPP and SLIP connections use the service type “Framed”.
Acct-Session-Id	Session number.
Acct-Terminate-Cause	Cause of service termination: <ul style="list-style-type: none"> <li>• User-Request</li> <li>• Lost-Carrier</li> <li>• Lost-Service</li> <li>• Session-Timeout</li> <li>• Idle-Timeout</li> </ul>
Acct-Session-Time	Indicates for how long, in seconds, the user has been receiving service.
Acct-Input-Octets	Number of octets that have been received from the port over the course of providing a service.
Acct-Output-Octets	Number of octets that have been sent to the port in the course of delivering a service.
Acct-Input-Packets	Number of octets that have been received from the port over the course of providing a service to a framed user.
Acct-Output-Packets	Number of octets that have been sent to the port in the course of delivering a service to a framed user.
Framed-Protocol	Indicates the framing to be used for framed access.
Framed-IP-Address	IP address of the user’s system.
Control-Info	“ <i>Irollover;value</i> ”. Number of times the 32-bit integer rolls over and the value of the integer when it overflows for inbound data.
Control-Info	“ <i>Orollover;value</i> ”. Number of times the 32-bit integer rolls over and the value of the integer when it overflows for outbound data.
Service-Info	“ <i>Nname</i> ”. Name of the service profile.
Service-Info	“ <i>Uname</i> ”. Username used to authenticate the user with the remote RADIUS server. This attribute is used for proxy services.
Service-Info	“ <i>Ttype</i> ”. Indicates whether the connection is proxy, tunnel, or pass-through. <ul style="list-style-type: none"> <li>• P—Pass-through (usually the Internet)</li> <li>• T—Tunnel</li> <li>• X—Proxy</li> </ul>
Acct-Delay-Time	Indicates for how many seconds the client has been trying to send a particular record.

## Attributes Used in Accounting Records

The following attributes are used for accounting purposes only. They do not appear in profiles.

### Service User

The Service User attribute provides the username used by the SESM user to log on to the service and presented for authentication with the home gateway.

**Service-Info** = "Uusername"

#### Syntax Description

<i>username</i>	The name provided by the user for authentication.
-----------------	---

#### Example

Service-Info = "Ujoe@cisco.com"



#### Note

The Service User attribute is used only for accounting purposes and does not appear in profiles.

### Service Name

The Service Name attribute defines the name of the service.

**Service-Info** = "Nname"

#### Syntax Description

<i>name</i>	Name of the service profile or service that belongs to a service group.
-------------	---

#### Example

Service-Info = "Nservice1.com"



#### Note

The Service Name attribute is used only for accounting purposes and does not appear in profiles.

### Octets Output

Current RADIUS standards support the counting of up to only 32 bits of information with the ACCT-Output-Octets attribute. Standards such as ADSL have much higher throughput.

In order for the accounting server to keep track of and bill for usage, SSG uses the Octets Output attribute.

The Octets Output attribute keeps track of how many times the 32-bit integer rolls over and the value of the integer when it overflows for outbound data.

**Control-Info** = "Orollover;value"

#### Syntax Description

<i>rollover</i>	Number of times the 32-bit integer rolls over to 0.
<i>value</i>	Value in the 32-bit integer when the stop record is generated and the service or user is logged out.

**Usage**

Use the Octets Output attribute to keep accurate track of and bill for usage. To calculate the actual number of bytes of data represented by the Octets Output values, use the following formula:

$$\text{rollover} * 2^{32} + \text{value}$$

**Example**

In the following example, *rollover* is 2 and *value* is 153 ( $2 * 2^{32} + 153 = 8589934745$ ):

```
Control-Info = "02;153"
```

**Note**

The Octets Output attribute is used only for accounting purposes and does not appear in profiles.

**Octets Input**

Current RADIUS standards support the counting of up to only 32 bits of information with the ACCT-Input-Octets attribute. Standards such as ADSL have much higher throughput.

In order for the accounting server to keep track of and bill for usage, SSG uses the Octets Input attribute.

The Octets Input attribute keeps track of how many times the 32-bit integer rolls over and the value of the integer when it overflows for inbound data.

```
Control-Info = "Irollover;value"
```

**Syntax Description**

<i>rollover</i>	Number of times the 32-bit integer rolls over to 0.
<i>value</i>	Value in the 32-bit integer when the stop record is generated and the service or user is logged out.

**Usage**

Use the Octets Input attribute to keep accurate track of and bill for usage. To calculate the actual number of bytes of data represented by the Octets Input values, use the following formula:

$$\text{rollover} * 2^{32} + \text{value}$$

**Example**

In the following example, *rollover* is 3 and *value* is 151 ( $3 * 2^{32} + 151 = 12884902039$ ):

```
Control-Info = "I3;151"
```

**Note**

The Octets Input attribute is used only for accounting purposes and does not appear in profiles.

**Class Attribute**

The class attribute is an arbitrary value that the network access server includes in all accounting packets for this user if supplied by the RADIUS server.

**Full Username RADIUS**

The Full Username RADIUS attribute allows SSG to include the user's full username and domain (user@service) in the RADIUS authentication and accounting requests.

**Restrictions for SSG Full Username RADIUS Attribute**

The size of the full username is limited to the smaller of the following values:

- 246 bytes (10 bytes less than the standard RADIUS protocol limitation)
- 10 bytes less than the maximum size of the RADIUS attribute supported by your proxy

**Configuration Examples for SSG Full Username RADIUS Attribute**

RADIUS Freeware Format: Example

```
Service-Info = "X"
```

CiscoSecure ACS for UNIX: Example

```
9,251 = "X"
```

**Acct-Session Id**

A unique accounting identifier that makes it easy to match start and stop records in a log file.

Acct-session ID numbers restart at 1 each time the router is power cycled or the software is reloaded.

**3GPP VSAs in Accounting Records**

When a RADIUS client (GGSN) sends the 3GPP attributes (IMSI, ChargingID and SGSN address) in sending Access Request Packet, SSG caches these attributes in this host's proxy logon attributes. When accounting records (start/interim/stop) are sent for this user (host/service accounting records) these 3GPP attributes will be sent.

**Format of these attributes:**

3GPP Vendor Id = 10415

```
Octets8  7  6  5  4  3  2  1
```

1 Type = 26

2 Length =  $n$

3 Vendor id octet 1

4 Vendor id octet 2

5 Vendor id octet 3

6 Vendor id octet 4

7- $n$  String

where  $n \geq 7$

These attributes must also be included, if available, in authorization requests (that is for pre-paid authorization) and remote authentication requests (authentication of the user at a remote AAA sever for proxy service).

**NAS-Port in Authentications**

When a user accesses a service, SSG sends a RADIUS Accounting-Request to the accounting server. The RADIUS Accounting-Request record contains attributes to define the Network Access Server. The NAS-Port attributes are described in [Table 18](#).

**Table 18**      **NAS-Port Accounting Record Attributes**

Attribute	Description
NAS-Port	<p>Physical port number of the network access server that is authenticating the user. The NAS-Port value (32 bits) consists of one or two 16-bit values (depending on the setting of the <b>radius-server extended-portnames</b> command. Each 16-bit number should be viewed as a 5-digit decimal integer for interpretation as follows:</p> <ul style="list-style-type: none"> <li>• For asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is <b>00ttt</b> where <i>ttt</i> is the line number or async interface unit number.</li> <li>• For ordinary synchronous network interface, the value is <b>10xxx</b>.</li> <li>• For channels on a primary rate ISDN interface, the value is <b>2ppcc</b>.</li> <li>• For channels on a basic rate ISDN interface, the value is <b>3bb0c</b>.</li> <li>• For other types of interfaces, the value is <b>6nnss</b>.</li> </ul>
NAS-Port-Type	<p>Type of physical port that the network access server is using to authenticate the user. Physical ports are indicated by a numeric value as follows:</p> <p>0: Asynchronous  1: Synchronous  2: ISDN-Synchronous  3: ISDN-Asynchronous (V.120)  4: ISDN-Asynchronous (V.110)  5: Virtual</p>

## Additional References

The following sections provide references related to RADIUS Profiles and Attributes for SSG.

## Related Documents

Related Topic	Document Title
SSG commands	<i>Cisco IOS Service Selection Gateway Command Reference</i>
SESM	<i>Cisco Subscriber Edge Services Manager</i> documentation
RADIUS commands	<i>Cisco IOS Security Command Reference</i>

Related Topic	Document Title
RADIUS configuration tasks	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Configuring L2TP	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Technologies Configuration Guide</i></li> <li>• <i>Cisco IOS Dial Technologies Command Reference</i></li> </ul>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for RADIUS Profiles and Attributes for SSG

Table 19 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.0(3)DC or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the [Service Selection Gateway Features Roadmap](#).

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 19 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 19** Feature Information for RADIUS Profiles and Attributes for SSG

Feature Name	Releases	Feature Configuration Information
RADIUS Profiles and Attributes for SSG	12.0(3)DC 12.2(4)B 12.2(11)T 12.2(13)T 12.3(4)T 12.3(7)T 12.3(14)T 12.4 15.0(1)M	SSG uses RADIUS Profiles and attributes for the authentication, authorization, and accounting of subscribers.  The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">RADIUS Profiles for SSG Support, page 2</a></li> <li>• <a href="#">SSG Vendor-Specific Attributes, page 2</a></li> <li>• <a href="#">Subscriber Profiles, page 29</a></li> <li>• <a href="#">Service Profiles, page 32</a></li> <li>• <a href="#">Service Group Profiles, page 40</a></li> <li>• <a href="#">Pseudo-Service Profiles, page 42</a></li> <li>• <a href="#">Examples of SSG RADIUS Profiles, page 44</a></li> <li>• <a href="#">RADIUS Accounting Records for SSG, page 47</a></li> <li>• <a href="#">Attributes Used in Accounting Records, page 52</a></li> </ul> This feature was removed in Cisco IOS Release 15.0(1)M.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.