



SSG Service Logon Enhancements

This document describes the following Service Selection Gateway (SSG) enhancements:

- Enhancements to SSG service logon, including CHAP authentication for L2TP tunnel and proxy services, and support for the using the Mobile Station ISDN number (MSISDN) during authentication
- Support for additional error codes in the SSG response to the SESM

Feature History for the SSG Enhancements to SSG-SESM Interactions and Service Logon

Release	Modification
12.3(1a)BW	This feature was introduced on the MWAM in Catalyst 6500 series switches and MWAM in Cisco 7600 series routers.
12.3(3)B	This feature was integrated into Cisco IOS Release 12.3(3)B and adds support for the Cisco 7200 series, Cisco 7301, and Cisco 7400 series routers.
12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About the SSG Enhancements to SSG-SESM Interactions and Service Logon, page 2](#)
- [Additional References, page 6](#)
- [Command Reference, page 6](#)



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Information About the SSG Enhancements to SSG-SESM Interactions and Service Logon

This section contains the following concepts:

- [Service Logon Enhancements, page 2](#)
- [SSG Error Codes in Access Responses, page 5](#)
- [SSG Error Codes in Access Responses, page 5](#)

Service Logon Enhancements

When a host wants to log on to a service, SESM sends SSG a service logon request. This request is sent as a RADIUS Access-Request message that includes the SSG Command Code VSA (value 11). The host is identified by the SSG Account-Info VSA for the subscriber IP, which contains the subscriber IP address (or the port-bundle when the port-map feature is enabled). The service is indicated by the service name included in the Command Code VSA.

The following sections describe enhancements to the service logon process:

- [CHAP Authentication for Proxy Services, page 2](#)
- [CHAP Authentication for Tunnel Services, page 2](#)
- [MSISDN for Service Logon, page 3](#)
- [Attribute Filter for Service Logon, page 4](#)
- [Network-Address-Translated IP in Service Logon Response, page 4](#)

CHAP Authentication for Proxy Services

This enhancement provides support for CHAP authentication for service logon requests from the SESM. SSG receives the following CHAP information in the RADIUS Access-Request message for service logon:

- Username in attribute 1
- CHAP ID and Response as CHAP password, attribute 3
- CHAP challenge in either attribute 60 or the request authenticator

These parameters are sent to the authentication, authorization, and accounting (AAA) server in the Access-Request message for user authentication. The service name is added to the username if the service has been configured to use the full username (Service-Info VSA X).

Authentication using CHAP is also supported for autologon to proxy services. If the user authentication is CHAP-based and no username or password is configured for the autologon service, the CHAP information used during account logon is also used for service logon to the proxy service.

CHAP Authentication for Tunnel Services

This enhancement extends CHAP authentication to tunnel services by supporting L2TP Proxy Authentication attribute-value pairs (AVPs). The CHAP authentication information used for service logon is sent to the L2TP Network Server (LNS) in the Incoming-Call-Connected (ICCN) message. [Table 1](#) describes the attributes that provide CHAP authentication information in ICCN messages.

Table 1 CHAP Authentication Information in ICCN Message

Attribute	Value
Proxy Authen Type (attribute 29)	PPP CHAP (value 2)
Proxy Authen Name (attribute 30)	Username received for the service logon request Note If the service is configured to use the full username (Service-Info attribute X), the service name is appended to the username with "@" as a delimiter between them.
Proxy Authen Challenge (attribute 31)	CHAP challenge
Proxy Authen ID (attribute 32)	CHAP ID
Proxy Authen Response (attribute 33)	CHAP response

For detailed information about the attributes listed in [Table 1](#), refer to RFC 2661.

**Note**

The SSG server sends the CHAP challenge and response in the Cisco fixed challenge AVPs. The Cisco AVPs for fixed challenge work with PPP renegotiations between the L2TP Access Concentrator (LAC), such as SSG, and the LNS. But the CHAP parameters sent in proxy authentication AVPs are used only once. Therefore, authentication could fail if renegotiations occur between the LAC and the LNS and the LNS does not support the Cisco fixed challenge AVP.

MSISDN for Service Logon

This enhancement supports using the MSISDN for proxy and L2TP tunnel service authentication. The MSISDN for service logon can be different from the one used for account logon. This MSISDN is sent as Calling Station ID (attribute 31) in the connection RADIUS messages for proxy services to the remote AAA server. The MSISDN in the service logon request can determine the MSISDN used during service authentication.

[Table 2](#) lists the attributes used for service logon with and without the MSISDN.

Table 2 Service Logon Comparison (With and Without MSISDN)

Service Logon	Connection Authentication ¹	Connection Accounting to Local AAA	Connection Accounting to Remote AAA ²	Prepaid (Re)authorization	Prepaid Accounting
Without MSISDN	Host Calling ID	Host Calling ID	Host Calling ID	Host Calling ID	Host Calling ID
With MSISDN ³	Connection Calling ID	Host Calling ID	Connection Calling ID	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.

Attribute Filter for Service Logon

Some services require the MSISDN to be hidden from the service provider. To support this capability, an attribute filter can be added 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 only attribute 31 (Calling Station ID) can be filtered.

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

Table 3 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 4 lists the attributes used for service logon with and without the MSISDN and with MSISDN filter set to F31.

Table 4 Service Logon Comparison (With MSISDN, Without MSISDN, and With MSISDN Filter)

Service Logon	Connection Authentication ¹	Connection Accounting to Local AAA	Connection Accounting to Remote AAA ²	Prepaid (Re)authorization	Prepaid Accounting
Without MSISDN	Host Calling ID	Host Calling ID	Host Calling ID	Host Calling ID	Host Calling ID
With MSISDN ³	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.

The **show ssg connection** command can be used to display the attributes that are being filtered.

Network-Address-Translated IP in Service Logon Response

External SSG clients sometimes require the real IP address of a connection on which Network Address Translation (NAT) has occurred. To provide this capability, this enhancement allows SSG to send the real IP address of translated connections in the service logon response to the SESM. The real IP address is

obtained from the Access Response message for service authentication from the remote AAA server for proxy services or is assigned by the LNS for tunnel services. The real IP address is sent in an SSG Account-Info VSA.

This feature is available for both translated proxy connections and L2TP tunnel service connections.

The real IP address is also returned in response to service status queries for translated connections in an SSG Account-Info VSA.

SSG Error Codes in Access Responses

SSG provides the **account logoff** command to force the deletion of a host. The host is identified by the subscriber IP address (or the port-bundle when the port-map feature is enabled).

This enhancement provides the result of the account logoff in the response. If the host exists, an Access-Accept is sent. If the host does not exist, the SSG sends an Access Reject message with the error code 2.

SSG also supports the **service logoff** command for SESM for a connection where the host is indicated by the host IP address (or port-bundle when the port-map feature is enabled) and the service is indicated by the service name. If the connection exists, an Access Accept message is sent. If the host is not connected to the service, an Access Reject message returns with the error code 56.

Table 5 lists the attributes for the SSG error codes sent to the SESM.

Table 5 SSG Error Code VSA Descriptions

Attribute ID	Vendor ID	Subattribute ID	Attribute Name	Subattribute Data
26	9	252	Command-code	16;2;<host-username> when host is not logged on
26	9	252	Command-code	16;56<host IP[:port bundle]>;<service-name> when host is not connected to service

For more information on RADIUS SSG VSAs, refer to “Vendor Specific Attributes” document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/3_0/concepts/vsa.htm

Additional References

The following sections provide references related to the SSG Enhancements to SSG-SESM Interactions and Service Logon.

Related Documents

Related Topic	Document Title
SSG commands	<i>Cisco IOS Wide-Area Networking Command Reference</i> , Release 12.3 T
SSG configuration tasks	“Broadband Access” section in the <i>Cisco IOS Wide-Area Networking Configuration Guide</i> , Release 12.3 SSG Features in Cisco IOS Release 12.3(4)T
SESM	<i>Cisco Subscriber Edge Services Manager</i> <i>Cisco Service Selection Dashboard</i>
RADIUS commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T
RADIUS configuration tasks	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature. Support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands.

- [show ssg connection](#)
- [show ssg service](#)

show ssg connection

To display the connections of a given Service Selection Gateway (SSG) host and a service name, use the **show ssg connection** command in privileged EXEC mode.

```
show ssg connection ip-address service-name [interface]
```

Syntax Description		
<i>ip-address</i>		IP address of an active Service Selection Gateway (SSG) connection. This is always a subscribed host.
<i>service-name</i>		Name of an active SSG connection.
<i>interface</i>		(Optional) IP address through which the host is connected.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(2)B	The <i>interface</i> argument was added for the SSG Host Key feature.
	12.2(4)B	This command was modified to display information about SSG prepaid billing.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(13)T	The modifications from Release 12.2(4)B were integrated into Cisco IOS Release 12.2(13)T.
	12.3(1a)BW	This command was modified to display the MSISDN (Calling Station ID) used for service logon.
	12.3(3)B	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(7)T.

Examples

Prepaid Service Based on Volume: Example

The following example displays the SSG connection for a prepaid service that uses a volume-based quota:

```
Router# show ssg connection 19.1.1.19 InstMsg
```

```
-----ConnectionObject Content -----
```

```
User Name:
Owner Host:19.1.1.19
Associated Service:InstMsg
Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2001
User last activity at:*00:25:59.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
```

```

        Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled

```

Prepaid Service Based on Time: Example

The following example displays the SSG connection for a prepaid service that uses a time-based quota:

```
Router# show ssg connection 19.1.1.22 Prepaid-internet
```

```

-----ConnectionObject Content -----
User Name:Host
Owner Host:19.1.1.22
Associated Service:Prepaid-internet
Connection State:0 (UP)
Connection Started since:*00:34:06.000 UTC Tue Oct 23 2001
User last activity at:*00:34:07.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'TIME', Quota Value = 100
Session policing disabled

```

Autologin Service: Example

The following example shows the service connection for the autologin service to host 10.3.6.1:

```
Router# show ssg connection 10.3.6.1 autologin
```

```

----- ConnectionObject Content -----
User Name:autologin
Owner Host:10.3.6.1
Associated Service:autologin
Connection State:0 (UP)
Connection Started since:
*20:41:26.000 UTC Fri Jul 27 2001
User last activity at:*20:41:26.000 UTC Fri Jul 27 2001
Connection Traffic Statistics:
    Input Bytes = 0 (HI = 0), Input packets = 0
    Output Bytes = 0 (HI = 0), Output packets = 0

```

MSISDN: Example

The following sample output for the **show ssg connection** command shows the MSISDN that is used for service logon:

```
Router# show ssg connection 10.0.1.1 proxy2
```

```

-----ConnectionObject Content -----
User Name: dev-user2
Owner Host: 10.0.1.1
Associated Service: proxy2
Calling station id: 12345
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2003
User last activity at: *17:44:59.000 GMT Sun Jul 6 2003
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
Session policing disabled

```

[Table 6](#) describes the significant fields shown in the displays.

Table 6 *show ssg connection Field Descriptions*

Field	Description
User Name	Subscriber name supplied at authentication.
Owner Host	IP address of the subscribed host.
Associated Service	Service name of the connected service.
Calling station id	MSISDN used for service logon.
Connection State	State of activation (active or inactive).
Connection Started since	Time of host connection to the associated service.
User last activity at	Time of last data packet sent over this connection.
Input Bytes	Number of bytes received on this connection.
Input packets	Number of packets received on this connection.
Output Bytes	Number of bytes sent on this connection.
Output packets	Number of packets sent on this connection.
Quota Type	Form in which the quota value is expressed (time or volume).
Quota Value	Value of the quota (in bytes for volume or seconds for time).

Related Commands

Command	Description
clear ssg connection	Removes the connections of a given host and a service name.

show ssg service

To display the information for a Service Selection Gateway (SSG) service, use the **show ssg service** command in privileged EXEC mode.

```
show ssg service [service-name [begin expression | exclude expression | include expression]]
```

Syntax Description

<i>service-name</i>	(Optional) Name of an active Service Selection Gateway (SSG) service.
begin	(Optional) Begin with the line that contains <i>expression</i> .
<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain <i>expression</i> .
include	(Optional) Include lines that contain <i>expression</i> .

Defaults

If no service name is provided, the command displays information for all services.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: <ul style="list-style-type: none"> • Service-Defined Cookie • Full Username Attribute
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(1a)BW	This command was modified to display the attribute filter that is set in the service profile.
12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B. The output for this command was modified to display information about default DNS redirection.
12.3(7)T	The modifications in Release 12.3(3)B were integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command to display connection information for a service.

Examples**L2TP Tunnel Service: Example**

The following example shows the information for the L2TP tunnel service called “tunnel1”. The attribute filter that is set in the service profile can be seen in the output.

```
Router# show ssg service tunnel1

----- ServiceInfo Content -----
Uplink IDB: gw: 0.0.0.0
Name: tunnel1
Type: TUNNEL
Mode: CONCURRENT
Service Session Timeout: 0 seconds
Service Idle Timeout: 0 seconds
Service refresh timeleft: 99 minutes
No Authorization Required
Authentication Type: CHAP
Attribute Filter: 31
Session policing disabled
Reference Count: 1

DNS Server(s):
No Radius server group created. No remote Radius servers.

TunnelId: ssg1
TunnelPassword: cisco
HomeGateway Addresses: 172.0.0.1
ConnectionCount 1
Full User Name not used

Domain List: Included Network Segments:
              0.0.0.0/0.0.0.0

Active Connections:
      1 : RealIP=172.0.1.1, Subscriber=10.0.1.1

----- End of ServiceInfo Content -----
```

Proxy Service: Example

The following example shows information for the proxy service called “serv1-proxy”:

```
Router# show ssg service serv1-proxy

----- ServiceInfo Content -----
Uplink IDB:
Name:serv1-proxy
Type:PROXY
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Class Attr:NONE
Authentication Type:CHAP
Reference Count:1

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5

Radius Server:IP=10.13.1.2, authPort=1645, acctPort=1646, secret=my-secret

Included Network Segments:
              10.13.0.0/255.255.0.0
```

```
Excluded Network Segments:
Full User Name Used
Service Defined Cookie exist
```

```
Domain List:service1.com;
```

```
Active Connections:
    1 :Virtual=255.255.255.255, Subscriber=10.20.10.2
```

```
----- End of ServiceInfo Content -----
```

Table 7 describes the significant fields shown in the display.

Table 7 show ssg service Field Descriptions

Field	Description
Uplink IDB	Interface through which the service is reachable.
Name	Service name.
Type	Type of service.
Mode	One of the following values: Concurrent—user can log into this service and other services simultaneously. Sequential—user cannot log into this service simultaneously with other services.
Service Session Timeout	Period of time after which the session (SSG connection) will be terminated.
Service Idle Timeout	If the session (SSG connection) is idle for this many seconds, the session will be terminated.
Service refresh timeleft	Amount of time after which SSG will refresh the service profile.
Authentication Type	Type of authentication that will be used for proxy or tunnel services. Values are PAP and CHAP.
Attribute Filter	RADIUS attribute that is being filtered out from user authentication.
Next Hop Gateway Key	Defines the next-hop binding. Services can be bound to the next hop using next-hop gateways. The key to next-hop-gateway mapping is present in the next-hop profile.
DNS Server(s)	DNS server used for this service.
TunnelId	ID for tunneling services.
TunnelPassword	Password for tunneling services.
HomeGateway Addresses	IP address of the LNS.

Table 7 *show ssg service Field Descriptions (continued)*

Field	Description
Radius Server: IP authPort acctPort secret	Information about the RADIUS server where proxy users are authenticated for service connectivity.
Included Network Segments	IP address subnets that form the service network.
Excluded Network Segments	IP address subnets that are excluded from the service network.
Full User Name Used	Indicates that the RADIUS authentication and accounting requests use the full username (user@service).
Service Defined Cookie exist	Indicates that user-defined information is included in RADIUS authentication and accounting requests.
Domain List	List of domain names that belong to the service and can be resolved by the DNS server specified for this service.
Active Connections Virtual Subscriber	Lists the host IP address for active connections. The subscriber IP address is the IP address of the host. In cases where there is a service-defined NAT, the virtual IP address is not zero and is the IP address given by the service.

Related Commands

Command	Description
clear ssg service	Removes a service.
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
ssg bind service	Specifies the interface for a service.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.