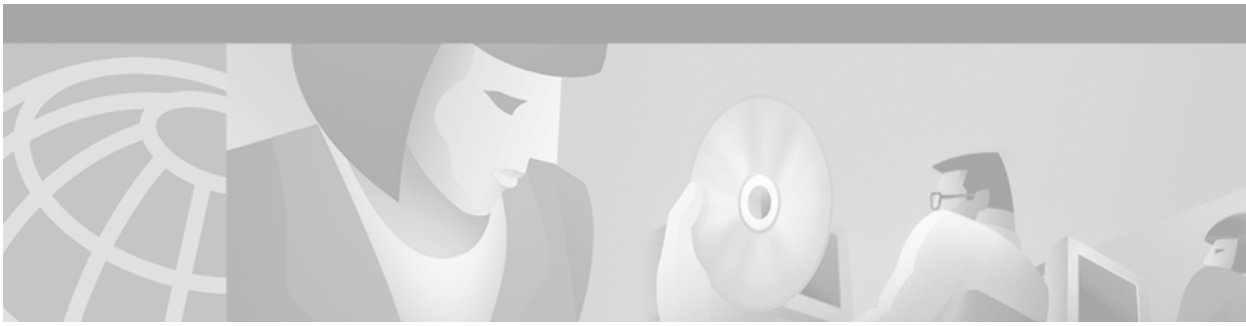

SSG AutoLogon Using Proxy Radius

Feature History

Release	Modification
12.1(3)DC	This feature was introduced on Cisco 6400 series routers.
12.2(4)B	This feature was introduced on the Cisco 7200 series and Cisco 7401ASR routers.

This document describes the SSG AutoLogon Using Proxy Radius feature in Cisco IOS Release 12.2(4)B and contains the following sections:

Feature Overview

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as *x*DSL, cable modems, or wireless to allow simultaneous access to network services.

The SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Access Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside. The SSG also communicates with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of the SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

The user opens an HTML browser and accesses the URL of the SESM or SSD web server application. SESM or SSD forwards user login information to the SSG, which forwards the information to the AAA server.

- If the user is not valid, the AAA server sends an Access-Reject message.
- If the user is valid, the AAA server sends an Access-Accept message with information specific to the user profile about which services the user is authorized to use. The SSG logs the user in, creates a host object in memory, and sends the response to SESM or SSD.

Based on the contents of the Access-Accept response, SESM or SSD presents a dashboard menu of services that the user is authorized to use, and the user selects one or more of the services. The SSG then creates an appropriate connection for the user and starts RADIUS accounting for the connection.

Note that when a non-Point-to-Point Protocol (non-PPP) user, such as in a bridged-networking environment, disconnects from a service without logging off, the connection remains open and the user can reaccess the service without going through the login procedure. This is because no direct connection (PPP) exists between the subscribers and the SSG. To prevent non-PPP users from being logged in to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.

SSG AutoLogon Using Proxy Radius

Before the introduction of the SSG AutoLogon Using Proxy Radius feature, the SSG effectively acted as a RADIUS proxy for the Service Selection Dashboard (SSD). In this mode, when SSD needs to authenticate a user, it forwards an Access-Request to the SSG. The Access-Request uses the IP address and port number configured for RADIUS authentication on the SSG, as well as the configured shared secret between the SSG and the SSD. When SSG receives a request from the SSD to authenticate a user, the SSG uses AAA to construct an Access-Request and send it to the AAA server. When SSG receives the Access-Accept, it processes it and forwards it to the SSD. In this implementation, SSG is far from acting as a generic RADIUS proxy, and standard RADIUS protocol must be extended by the use of Vender Service Attributes (VSAs) to provide a control plane between the SSG and SSD. Before the introduction of the SSG AutoLogon Using Proxy Radius feature, without the VSA in the Access-Request, SSG did not function as a RADIUS proxy.

The SSG AutoLogon Using Proxy Radius feature enables the SSG to act as a RADIUS proxy for non-SSD clients whose Access-Requests do not contain VSAs. Non-SSD Access-Requests must originate from configured, trusted, downstream Network Access Server (NAS) IP addresses which share a RADIUS secret key with the SSG. This shared secret key is a different secret than the one shared between SSG and the SSD. You must configure the IP addresses for each router for which SSG is acting as a RADIUS proxy. Packets received from unrecognized sources are discarded.

When the SSG receives a valid Access-Request, it forwards it to the RADIUS server. The SSG performs a full, transparent proxy of the Access-Request to the RADIUS server, faithfully reproducing the attributes provided originally by the RADIUS client. If the Access-Request is successful, the AAA server responds with an Access-Accept and an SSG host object is created.

RADIUS Authentication and Authorization

A RADIUS client can be configured to use a RADIUS AAA server for user authentication. In a Cisco RADIUS client, the RADIUS server can be configured as a global AAA server for General Packet Radio System (GPRS) or individual servers per Access Point Name (APN). The RADIUS client sends an Access-Request to the AAA server to authenticate a user. The Access-Request contains attributes depending on whether the router is using CHAP or PAP.

Table 1 Access-Request Attributes

Attribute Number	Attribute Name	Description	Notes
1	User-Name	Mobile Subscriber user name	May be anonymous (for example, for users using WAP[1]).
2/3	PAP/CHAP password	Password Authentication Protocol (PAP)/Challenge Handshake Authentication (CHAP) Protocol password	May be anonymous (for example, for users using WAP).
4	Network Access Server (NAS) IP address	RADIUS client IP address	
6	Service-Type	Framed-user	
7	FramedProtocol	PPP	
8	Framed IP address	User IP address	
30	Called-Station-Id	APN	
31	Calling-Station-Id	MSISDN	
60	CHAP-challenge	CHAP challenge	Only for CHAP mode
61	NAS-Port-Type	Async (Value-0)	

1. Wireless Application Protocol

After a successful authentication, the RADIUS AAA server responds to the Access-Request by sending an Access-Accept containing a RADIUS attribute.

Table 2 RADIUS Attributes

Attribute Number	RADIUS Attribute
6	Service-Type
7	Framed-Protocol
8	Framed-IP-address

Table 2 RADIUS Attributes (continued)

Attribute Number	RADIUS Attribute
9	Framed-IP-Netmask
12	Framed-MTU

The attributes listed in Table 2 are not the only attributes that can be sent. The RADIUS attributes are part of the user database held on the RADIUS AAA server and can be modified or extended as required. You can configure the AAA server to select a user profile based on Called-Station-ID (Access Point Name [APN]) or Calling-Station-ID (MSISDN header field type for wireless clients using the Wireless Application Protocol [WAP]).

If the AAA is configured to select profiles based on Called-Station-ID, all users connecting to the same APN are given the same profile even though they have different assigned IP addresses.

The supplied username does not have to be unique for WAP users on the RADIUS client. These users are granted anonymous access and all have the same user name and password.

AAA authorization involves extracting all of the parameters needed to create the Packet Data Protocol (PDP) context. The authorization extracts the Framed-IP-Address and the Framed-IP-Netmask.

SSG Vendor-Specific Attributes

The SSG uses vendor-specific RADIUS attributes. If using the SSG with Cisco User Control Point (UCP) software, specify settings that allow processing of the SSG attributes while configuring the CiscoSecure Access Control Server (ACS) component. If using another AAA server, you must customize that server RADIUS dictionary to incorporate the SSG vendor-specific attributes.

Table 3 lists vendor-specific attributes used by the SSG to support the proxy RADIUS enhancements. The vendor ID for all of the Cisco-specific attributes is 9.

Table 3 VSAs Related to NRP-SSG Support of the Proxy RADIUS Server

AttrID	Vendor ID	SubAttrID	SubAttrName	SubAttrDataType
26	9	250	Account-Info	String
26	9	251	Service-Info	String
26	9	253	Control-Info	String

Benefits

The SSG AutoLogon Using Proxy Radius provides the following benefits:

- Provides multi-service features of SSG for mobile users by using SSG as a radius proxy to a radius-client.

Restrictions

The SSG AutoLogon Using Proxy Radius feature has the following restrictions:

- Restricted support of Dynamic Host Configuration Protocol (DHCP)—DHCP for IP address assignment must be done prior to RADIUS negotiation.
- Loose coupling of host objects and PDP contexts—Not all error conditions can be guaranteed to be cleanly recovered without end-user intervention such as reconnecting.
- Scalability—If the number of PDP contexts supported by a radius-client exceeds the maximum number of host objects on a single SSG, external load balancing for a two-router solution is required.

Related Features and Technologies

- Cisco Subscriber Edge Services Manager
- HTTP Redirect-Login in Cisco IOS Release 12.1(5)DC on 6400 series routers. See the "Service Selection Gateway" chapter of the *Cisco 6400 Feature Guide* for Releases 12.1(5)DB and 12.1(5)DC for more information.
- Dynamic Subscriber Bandwidth Selection
- Hierarchical Policing in SSG
- PPPoA/PPPoE Autosense for ATM PVCs
- SSG Accounting Update Interval Per Service
- SSG Autologoff and MAC Address in Accounting Records
- SSG Host Key Port Bundle
- SSG Open Garden
- SSG Prepaid
- SSG TCP Redirect for Services

Related Documents

- *APN Manager Application Programming Guide*
- *Cisco 6400 Software Configuration Guide and Command Reference*
- *Cisco Subscriber Edge Services Documentation*
- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- *Configuring RADIUS*
- *Service Selection Gateway*
- *SSG AutoDomain*
- *SSG Autologoff*
- *Service Selection Gateway Hierarchical Policing*
- *SSG Open Garden*
- *SSG Port-Bundle Host Key*

- *SSG Prepaid*
- *SSG TCP Redirect for Services*

Supported Platforms

- Cisco 6400 series
- Cisco 7200 series
- Cisco 7401ASR router

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- You must enable Cisco Express Forwarding (CEF) on the router before SSG functionality can be enabled. If CEF is not enabled and you attempt to configure SSG, the following error message is displayed:

```
SSG: Please enable ip cef first
```

Note You can disable CEF at the individual interface level without affecting SSG.

- SSG must be enabled before SSG AutoLogon Using Proxy Radius can be configured.

Configuration Tasks

See the following sections for configuration tasks for this feature. Each feature in the list is identified as either required or optional:

- Configuring SSG AutoLogon Using Proxy Radius (required)

Configuring SSG AutoLogon Using Proxy Radius

To configure the SSG AutoLogon Using Proxy Radius feature, follow the steps in the table below beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip cef`	Enables CEF.
Step 2	`Router(config)# ssg enable`	Enables SSG.
Step 3	`Router(config)# ssg radius-proxy`	Enables SSG RADIUS proxy and enters SSG-Radius-Proxy mode.
Step 4	`Router(config-radius-proxy)# server-port [auth auth-port][acct acct-port]`	Configures the authentication and accounting ports. • **auth**—(Optional) Configures the authentication port. • *auth-port*—(Optional) Specifies the authentication port number. The default authentication port is 1645. The valid range is 0 to 65535. • **acct**—(Optional) Configures the accounting port. • *acct-port*—(Optional) Specifies the accounting port number. The default accounting port is 1646. The valid range is 0 to 65535.
Step 5	`Router(config-radius-proxy)# client-address ip-address key secret`	Configures the client IP address and the shared key secret of a RADIUS client. • *ip-address*—IP address of a RADIUS client. • **key**—Shared secret with the RADIUS client. • *secret*—Description of the shared secret.
Step 6	`Router(config-radius-proxy)# address-pool start-ip end-ip [domain domain-name]`	(Optional) Configures the local IP pools used by SSG. • *start-ip*—First IP address of the local IP address pool. • *end-ip*—End IP address of the local IP address pool. • **domain**—(Optional) Configures the IP address pool for a specific domain. • *domain-name*—(Optional) Assigns a name to the domain.
Step 7	`Router(config-radius-proxy)# idle-timeout timeout`	(Optional) Configures the global host object inactivity timeout. • *timeout*—Timeout value in seconds. Valid range is 30 to 65536.
Step 8	`Router(config-radius-proxy)# forward accounting-start-stop`	(Optional) Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.

	Command	Purpose
Step 9	`Router(config-radius-proxy)# exit`	Exits SSG-Radius-Proxy mode.
Step 10	`Router(config)# exit`	Exits global configuration mode.
Step 11	`Router# clear ssg radius-proxy client-address` *ip address*	(Optional) Clears all hosts connected to a specific RADIUS client. • *ip-address*—IP address of the RADIUS client to clear.
Step 12	`Router# clear ssg radius-proxy nas-address` *ip address*	(Optional) Clears all hosts connected to a specific NAS client. • *ip-address*—IP address of the NAS client to clear.

Verifying the SSG AutoLogon Using Proxy Radius Configuration

To verify the SSG AutoLogon Using Proxy Radius Configuration, follow the steps below:

Step 1 To verify that SSG AutoLogon Using Proxy Radius has been enabled, enter the **show running-config** command:

```
Router# show running-config
.
.
.
!
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.1.2.2 key secret1
 client-address 10.2.25.90 key secret2
 client-address 10.0.0.1 key secret3
 client-address 10.23.3.2 key secret4
 idle-timeout 30
 forward accounting-start-stop
 address-pool 10.1.1.1 10.1.40.250
 address-pool 10.1.5.1 10.1.5.30 domain ssg.com
!
```

Step 2 If you configured an IP address pool, enter the **show ssg radius-proxy address-pool** command in Privileged EXEC mode to view the IP address pool:

```
Router# show ssg radius-proxy address-pool

Global Pool:  Free Addresses= 10234   Inuse Addresses= 0
```

Step 3 To view the IP address pool for a particular domain, enter the **show ssg radius-proxy address-pool domain** *domain-name* command in Privileged EXEC mode. In the example below, the domain name is "ssg.com":

```
Router# show ssg radius-proxy address-pool domain ssg.com

Domain Pool(ssg.com):  Free Addresses= 20   Inuse Addresses= 10
```

Troubleshooting Tips

To troubleshoot communication between the RADIUS server and the router, use the **debug radius** command.

To display RADIUS requests from RADIUS clients, use the **debut ssg ctrl-packets** command.

```
Router# debug ssg ctrl-packets

Access-request:
3d05h:SSG-CTL-PAK:Received Packet:
                sIP=5.5.5.2 sPort=1645 dIP=5.5.5.1 dPort=1645
3d05h:RADIUS:id= 91, code= Access-Request, len= 93
3d05h:RADIUS: authenticator B8 5D 3D 06 E3 2B A2 F3 - 68 E6 C5 E0 F3
1C 60 C7
3d05h:RADIUS: User-Name           [1]   10  "user"
3d05h:RADIUS: User-Password       [2]   18  *
3d05h:RADIUS: Called-Station-Id   [30]  9   "ssg.com"
3d05h:RADIUS: Calling-Station-Id  [31]  6   "1234"
3d05h:RADIUS: Framed-Protocol     [7]   6   GPRS_PDP_CONTEXT
[7]
3d05h:RADIUS: NAS-Port-Type       [61]  6   Virtual
[5]
3d05h:RADIUS: NAS-Port            [5]   6   0
3d05h:RADIUS: Service-Type        [6]   6   Framed
[2]
3d05h:RADIUS: NAS-IP-Address      [4]   6   10.1.1.102

Access-Accept:
3d05h:RADIUS:id= 91, code= Access-Accept, len= 38
3d05h:RADIUS: authenticator 62 57 FE F6 96 65 C1 79 - 18 D7 12 56 EA
28 62 73
3d05h:RADIUS: Service-Type        [6]   6   Framed
[2]
3d05h:RADIUS: Idle-Timeout        [28]  6   2000
3d05h:RADIUS: Framed-IP-Address   [8]   6   10.1.5.10

Accounting-Request(start) to SSG:
3d05h:SSG-CTL-EVN:Received cmd (4) from proxy-client (5.5.5.2:1646)
3d05h:SSG-CTL-PAK:Received Accounting Packet:
                sIP=5.5.5.2 sPort=1646 dIP=5.5.5.1 dPort=1646
3d05h:RADIUS:id= 128, code= Accounting-Request, len= 109
3d05h:RADIUS: authenticator 42 42 D8 7D EC 18 20 42 - 61 B1 03 A2 29
F8 26 56
3d05h:RADIUS: User-Name           [1]   10  "user"
3d05h:RADIUS: Acct-Status-Type    [40]  6   Start
[1]
3d05h:RADIUS: Acct-Session-Id     [44]  10  "00001F5D"
3d05h:RADIUS: Framed-Protocol     [7]   6   GPRS_PDP_CONTEXT
[7]
3d05h:RADIUS: Called-Station-Id   [30]  9   "ssg.com"
3d05h:RADIUS: Calling-Station-Id  [31]  6   "1234"
3d05h:RADIUS: Framed-IP-Address   [8]   6   10.1.5.10
3d05h:RADIUS: Authentic           [45]  6   RADIUS
[1]
3d05h:RADIUS: NAS-Port-Type       [61]  6   Virtual
[5]
3d05h:RADIUS: NAS-Port            [5]   6   0
3d05h:RADIUS: Service-Type        [6]   6   Framed
[2]
3d05h:RADIUS: NAS-IP-Address      [4]   6   10.1.1.102
3d05h:RADIUS: Delay-Time          [41]  6   0
```

```
Accounting-Response sent by SSG:
3d05h:SSG-CTL-PAK:Sent accounting response packet:
                sIP=?? sPort=56708 dIP=5.5.5.2 dPort=1646
3d05h:RADIUS:id= 128, code= Accounting-response, len= 20
3d05h:RADIUS: authenticator F6 9A 88 38 6C 9D 77 FE - 68 A2 7F 90 9F
DF 15 99
```

To display control path events or errors for the host and service logon, use the **debug ssg ctrl-events**, **debug ssg ctrl-errors**, and **debug ssg errors** commands.

Monitoring and Maintaining SSG AutoLogon Using Proxy Radius

To monitor and maintain SSG AutoLogon Using Proxy Radius, use the commands in the table below.

Command	Purpose
Router# **debug ssg port-map events**	Displays port mapping event messages.
Router# **debug ssg port-map packets**	Displays port mapping packet contents.
Router# **show ssg auto-domain exclude-profile**	Displays the contents of an Autodomain exclusion profile downloaded from the AAA server. Only Autodomain exclude entries entered via CLI are displayed.
Router# **show ssg binding**	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
Router# **show ssg connection** *ip-address service-name*	Displays the connections of a given host and service name. • *ip-address*—IP address of an active SSG connection. This is always a subscribed host. • *service-name*—The name of an active SSG connection.
Router# **show ssg direction**	Displays the direction of all interfaces for which a direction has been specified.
Router# **show ssg host** [*ip-address*] [**count**] [**username**]	Displays the information about a subscriber and the current connections of the subscriber. • *ip-address*—(Optional) IP address of the host. • **count**—(Optional) Displays the host object count, including inactive hosts. • **username**—(Optional) Displays the usernames logged into the active hosts.
Router# **show ssg next-hop**	Displays the next-hop table.
Router# **show ssg pending-command**	Displays current pending commands.
Router# **show ssg radius-proxy address-pool** [**domain** *domain-name*] [**free** | **inuse**]	Displays IP address pool usage for a specific domain for an entire router.

Configuration Examples

This section provides the following example:

- SSG AutoLogon Using Proxy Radius Configuration Example

SSG AutoLogon Using Proxy Radius Configuration Example

In the following example SSG AutoLogon Using Proxy Radius is enabled. Port 1500 is configured as the authentication port, and port 1499 is configured as the accounting port. A client with the IP address 172.16.0.0 is configured and assigned a shared key secret called "secret1". An IP address pool is configured for the domain called "cisco" with a start IP address 172.18.0.0 and an end IP address 172.22.0.0. An idle timeout of 60 seconds is configured. Accounting start-stop is enabled and accounting start/stop/update packets from all RADIUS clients are proxied to the AAA server. All host objects received from the RADIUS client at IP address 172.23.0.0 and from the NAS at IP address 172.24.0.0 are deactivated and destroyed.

```
 ssg enable
 ssg radius-proxy
  server-port auth 1500 acct 1499
  client-address 172.16.0.0 key secret1
  address-pool 172.18.0.0 172.22.0.0 domain cisco
  idle-timeout 60
  forward accounting-start-stop
  exit
 exit
clear ssg radius-proxy client-address 172.23.0.0
clear ssg radius-proxy nas-address 172.24.0.0
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications. Additional SSG commands can be found in the *SSG Commands for the Cisco 6400 NRP* document.

- **address-pool**
- **clear ssg radius-proxy client-address**
- **clear ssg radius-proxy nas-address**
- **client-address**
- **forward accounting-start-stop**
- **idle-timeout**
- **server-port**
- **show ssg radius-proxy address-pool**
- **ssg radius-proxy**

address-pool

To define local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client, use the **address-pool** command in SSG-Radius-Proxy mode. To remove a local IP pool, use the **no** form of this command.

address-pool *start-ip end-ip* [**domain** *domain-name*]

no address-pool *start-ip end-ip* [**domain** *domain-name*]

Syntax Description

start-ip	First IP address of the local IP address pool.
end-ip	End IP address of the local IP address pool.
domain	(Optional) IP address pool for a specific domain.
domain-name	(Optional) Name of the domain.

Defaults

SSG does not assign IP addresses from a local IP pool.

Command Modes

SSG-radius-proxy

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to configure SSG to assign an IP address from a local pool to a user for which SSG is acting as a RADIUS client. SSG assigns an IP address from a local pool only when one has not been assigned by one of the following methods:

- Assigned in the Access-Accept from the AAA server
- Assigned in the Access-Request received from the client
- Assigned from an Autodomain service (tunnel or proxy) that does not have the **auto-domain nat user-address** configuration enabled

Note You must have SSG Autodomain configured for an IP address to be assigned from an Autodomain tunnel. See *SSG AutoDomain* for more information about configuring SSG Autodomain.

You can use this command to define a global local IP address pool or an IP address pool for a specific domain by using the **domain** keyword. You cannot create pools with more than 20000 addresses.

Note Using IP address pools within SSG is completely standalone and unrelated to IOS IP local pools.

Examples

The following example shows how to configure a local IP address pool for SSG:

```
address-pool 172.16.16.0 172.16.20.0
```

The following example shows how to configure a local IP address pool for the domain named “cisco”.

```
address-pool 172.21.21.0 172.21.25.0 domain cisco
```

Related Commands

Command	Description
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
client-address	Configures the RADIUS proxy IP address and shared secret.
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.
idle-timeout	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

clear ssg radius-proxy client-address

To clear all hosts connected to a specific RADIUS client, use the **clear ssg radius-proxy client-address** command in privileged EXEC mode.

client ssg radius-proxy client-address *ip-address*

Syntax Description

ip-address	IP address of a RADIUS client.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to clear all hosts connected to a specific RADIUS client. This command deactivates and destroys all host objects associated with the specified RADIUS client.

Examples

The following example shows how to clear all hosts connected to the RADIUS client with the IP address 172.16.0.0:

```
clear ssg radius-proxy client-address 172.16.0.0
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
client-address	Configures the RADIUS proxy IP address and shared secret.
idle-timeout	Configures a host object timeout value.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

clear ssg radius-proxy nas-address

To clear all hosts connected to a specific Network Access Server (NAS), use the **clear ssg radius-proxy nas-address** command in privileged EXEC mode.

client ssg radius-proxy nas-address *ip-address*

Syntax Description

ip-address	IP address of a RADIUS client.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to clear all hosts connected to a specific NAS. This command deactivates and destroys all host objects associated with the specified NAS client.

Note SSG does not currently notify radius-clients when a host object is removed from the SSG.

Examples

The following example shows how to clear all hosts connected to the NAS with IP address 172.16.0.0:

```
clear ssg radius-proxy nas-address 172.16.0.0
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
client-address	Configures the RADIUS proxy IP address and shared secret.
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.
idle-timeout	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.

ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

client-address

To configure the RADIUS client IP address and shared secret, use the **client-address** command in SSG-Radius-Proxy mode. To disable the RADIUS proxy IP address and shared secret, use the **no** form of this command.

client-address *ip-address* **key** *secret*

no client-address *ip-address* **key** *secret*

Syntax Description

ip-address	IP address of a RADIUS client.
key	Shared secret between the SSG and the RADIUS-client.
secret	Description of the shared secret.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to configure the radius-client to proxy requests from the specified IP address to the RADIUS server. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one configured on the RADIUS client.

Examples

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret “cisco” to the client:

```
client-address 172.16.0.0 key cisco
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS client to the AAA server.
idle-timeout	Configures a host object timeout value.

Command	Description
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

forward accounting-start-stop

To proxy accounting start/stop/update packets generated by any RADIUS clients to the AAA server, use the **forward accounting-start-stop** command in SSG-Radius-Proxy mode. To stop accounting start/stop/update packet forwarding, use the **no** form of this command.

forward accounting-start-stop

no forward accounting-start-stop

Syntax Description

This command has no arguments or keywords.

Defaults

Forward accounting-start-stop is disabled by default and accounting start/stop/update packets generated by RADIUS clients are not proxied to the AAA server.

Command Modes

SSG-radius-proxy

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to proxy accounting start/stop/update packets generated by all RADIUS clients to the AAA server. Disabling this command reduces RADIUS packet traffic and processing for deployments where the billing server is not using these packets for billing purposes.

Note The **forward accounting-start-stop** command does not affect Accounting on/off packets, that are forwarded regardless of this command.

Examples

The following example show how to proxy accounting packets generated by all RADIUS clients to the AAA server:

```
forward accounting-start-stop
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
client-address	Configures the RADIUS proxy IP address and shared secret.

Command	Description
idle-timeout	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

idle-timeout

To configure a host object timeout value, use the **idle-timeout** command in SSG-Radius-Proxy mode. To disable the timeout value, use the **no** form of this command.

idle-timeout *timeout*

no idle-timeout *timeout*

Syntax Description

timeout	Timeout value in seconds. Valid range is 30 to 65536.

Defaults

No timeout value is configured.

Command Modes

SSG-radius-proxy

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to configure a timeout value for a host object. Configuring this command prevents dangling host objects on the SSG. If a RADIUS client reloads and does not indicate its fault condition to the SSG, the SSG retains the host objects, that are no longer valid. This command removes all host objects from a RADIUS-client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.

Note Timeout values configured in the user-profile that appear in the Access-Accept take precedence over any timeout value configured by the **idle-timeout** command.

Examples

The following example shows how to configure a timeout value of 60 seconds:

```
idle-timeout 60
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
client-address	Configures the RADIUS proxy IP address and shared secret.

Command	Description
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

server-port

To configure the ports on which SSG listens for RADIUS-requests from configured RADIUS clients, use the **server-port** command in SSG-Radius-Proxy configuration mode. To stop SSG from listening for RADIUS requests from configured RADIUS clients on a port, use the **no** form of this command.

server-port [**auth** *auth-port*] [**acct** *acct-port*]

no server-port [**auth** *auth-port*] [**acct** *acct-port*]

Syntax Description

auth	(Optional) RADIUS authentication port.
auth-port	(Optional) Port number to be used for RADIUS authentication. The default is 1645.
acct	(Optional) RADIUS accounting port.
acct-port	(Optional) Port number to be used for RADIUS accounting. The default is 1646.

Defaults

Port 1645 is the default RADIUS authentication port. Port 1646 is the default RADIUS accounting port.

Command Modes

SSG-radius-proxy

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to configure the authentication and accounting ports for the SSG RADIUS Proxy feature. Ports configured with this command are global parameters that apply to all proxy clients in the SSG.

Examples

The following example shows how to configure port 23 as the RADIUS authentication port and port 45 as the RADIUS accounting port:

```
server-port auth-port 23 acct-port 45
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).

Command	Description
client-address	Configures the RADIUS proxy IP address and shared secret.
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.
idle-timeout	Configures a host object timeout value.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

show ssg radius-proxy address-pool

To display the pool of IP addresses configured for a router or for a specific domain, use the **show ssg radius-proxy address-pool** command in privileged EXEC mode.

show ssg radius-proxy address-pool [**domain** *domain-name*] [**free** | **inuse**]

Syntax Description

domain	(Optional) IP addresses configured for a specific domain.
domain-name	(Optional) Name of the domain to display.
free	(Optional) IP addresses currently available in the free pool.
inuse	(Optional) IP addresses currently in use.

Defaults

If no domain name is provided, the command displays information for all IP addresses configured in an address-pool.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to display the IP address pools configured for a router or for a specific domain. You can also display which IP addresses are available or are in use.

Examples

The following example shows how to display information for IP addresses in the IP address pool:

```
Router# show ssg radius-proxy address-pool

Global Pool:  Free Addresses= 10234   Inuse Addresses= 0
```

The following example shows how to display information about the IP addresses in the IP address pool in the domain called “ssg.com”:

```
Router# show ssg radius-proxy address-pool domain ssg.com

Domain Pool(ssg.com):  Free Addresses= 20   Inuse Addresses= 10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called “ssg.com” that are currently in use:

```
Router# show ssg radius-proxy address-pool domain cisco inuse

Inuse Addresses in Domain Pool(ssg.com):10
19.1.5.1
19.1.5.2
19.1.5.3
19.1.5.4
```

```
19.1.5.5
19.1.5.6
19.1.5.7
19.1.5.8
19.1.5.9
19.1.5.10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called “ssg.com” that are currently available:

```
Router# show ssg radius-proxy address-pool domain ssg.com free

Free Addresses in Domain Pool(ssg.com):20
19.1.5.11
19.1.5.12
19.1.5.13
19.1.5.14
19.1.5.15
19.1.5.16
19.1.5.17
19.1.5.18
19.1.5.19
19.1.5.20
19.1.5.21
19.1.5.22
19.1.5.23
19.1.5.24
19.1.5.25
19.1.5.26
19.1.5.27
19.1.5.28
19.1.5.29
19.1.5.30
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
clear ssg service	Removes a service.
client-address	Configures the RADIUS proxy IP address and shared secret.
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.
idle-timeout	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
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.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

ssg radius-proxy

To enable SSG RADIUS Proxy, use the **ssg radius-proxy** command in global configuration mode. To prevent further connection of proxy users, use the **no** form of this command. The **no ssg radius-proxy** command does not log off already logged in RADIUS client hosts.

ssg radius-proxy

no ssg radius-proxy

Syntax Description

This command has no keywords or arguments.

Defaults

SSG RADIUS Proxy is not enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to enable SSG RADIUS Proxy. This command also enables SSG-Radius-Proxy configuration mode. You must enable SSG with the **ssg enable** command before you can enter the **ssg radius-proxy** command. If you do not enter the **ssg radius-proxy** command, SSG continues to proxy RADIUS packets contain SSG Vendor Service Attributes (VSAs) received from the Service Selection Dashboard (SSD), but does not act as a generic RADIUS proxy.

If you configure the **no ssg radius-proxy** command, no further connections of proxy users are allowed but hosts from already configured RADIUS clients remain connected. If you subsequently configure the **ssg radius-proxy** command, the previous radius proxy configuration is restored.

Examples

The following example enables SSG RADIUS Proxy:

```
ssg enable
ssg radius-proxy
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific Network Access Server (NAS).
client-address	Configures the RADIUS proxy IP address and shared secret.

Command	Description
forward accounting-start-stop	Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.
idle-timeout	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg radius-proxy address-pool	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.

Glossary

AAA—Authentication, authorization, and accounting (pronounced “triple a”).

APN—Access Point Name. Identifies a PDN that is configured on and accessible from a GGSN in a GPRS network.

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

GGSN—Gateway GPRS Support Node. A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks.

GPRS—General Packet Radio System. Service defined and standardized by the European Telecommunication Standards Institute (ETSI). GPRS is an IP packet-based data service for Global System for Mobile Communications (GSM) networks.

GSM—global system for mobile communication. A second generation (2G) mobile wireless networking standard defined by ETSI, GSM is deployed widely throughout the world. GSM uses TDMA technology and operates in the 900-MHz radio band.

L2TP—Layer 2 Tunneling Protocol. Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines features of two existing tunneling protocols: Cisco Layer 2 Forwarding (L2F) and Microsoft Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs.

MSISDN—The header field type for Wireless Application Protocol (WAP).

NAS—Network Access Server. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).

NAT—Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as *Network Address Translator.*

PDN—Public/Private/Packet Data Network. Represents a public or private packet-based network, such as an IP or X.25 network.

PDP—Packet Data Protocol. Network protocol used by external packet data networks that communicate with a GPRS network. IP is an example of a PDP supported by GPRS. Refers to a set of information (such as a charging ID) that describes a mobile wireless service call or session, which is used by mobile stations and GGSNs in a GPRS network to identify the session.

PTA-MD—PPP Termination and Aggregation Multi-Domain. The Aggregation part of the acronym indicates that after the PPP sessions are terminated, the traffic is aggregated. For an ISP, the aggregated traffic either remains in the ISP network or routes to the Internet. For a wholesale provider, the aggregated IP traffic is forwarded to different destinations or domains depending on the service selected; thus the term PTA-Multi-Domain.

RADIUS—Remote Access Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

SESM—Cisco Subscriber Edge Services Manager. Successor product of the SSD. Cisco SESM is part of a Cisco solution that allows subscribers of DSL, cable, wireless, and dial-up to simultaneously access multiple services provided by different Internet service providers, application service providers, and Corporate Access Servers.

Cisco SESM allows a service provider to create a customized web application that provides a network portal for individual subscribers. Through the Cisco SESM's web-based network portals, subscribers can have simultaneous access to the Internet, corporate intranets, gaming, and other entertainment-based services. After logging on and being authenticated to the system, subscribers access their own personalized services by pointing and clicking.

SSD—Service Selection Dashboard. A specialized web server that allows users to log in to and disconnect from multiple passthrough and proxy services through a standard web browser.

SSG—Service Selection Gateway. SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services.

TDMA—Time Division Multiplex Access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel; that is, the channels take turns to use the link. Some kind of periodic synchronizing signal or distinguishing identifier usually is required so that the receiver can tell which channel is which.

VPDN—Virtual Private Dialup Network. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.