



# Configuring SSG to Serve as a RADIUS Proxy

---

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



**Note**

---

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

---

The RADIUS proxy feature is principally an insertion mechanism to allow an SSG device to be introduced to a network with minimum disruption to the existing network access server (NAS) and authentication, authorization, and accounting (AAA) server(s). By acting as a proxy between a NAS using RADIUS authentication (which may or may not be Cisco equipment) and a AAA server, SSG is able to “sniff” the RADIUS flows and transparently create a corresponding SSG session, on successful authentication of the subscriber. This provides an autologon facility with respect to SSG for subscribers that are authenticated by devices that are closer to the network edge. This document describes the types of deployments that use SSG as a RADIUS proxy and how to configure them.

## 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 SSG RADIUS Proxy” section on page 36](#).

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 SSG RADIUS Proxy, page 2](#)
- [Restrictions for SSG RADIUS Proxy, page 2](#)
- [Information About SSG Authentication Using RADIUS Proxy, page 2](#)



---

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

- [How to Configure SSG RADIUS Proxy, page 4](#)
- [Configuration Examples for SSG Authentication of RADIUS Proxy Subscribers, page 29](#)
- [Where to Go Next, page 34](#)
- [Additional References, page 34](#)
- [Feature Information for SSG RADIUS Proxy, page 36](#)

## Prerequisites for SSG RADIUS Proxy

Before you can perform the tasks in this process, you must enable SSG by completing the steps in the task [Enabling SSG](#) in the “Implementing SSG: Initial Tasks” module.

Before you can configure SSG as a RADIUS proxy, you must first configure the RADIUS clients and the RADIUS servers.

## Restrictions for SSG RADIUS Proxy

- Loose coupling of host objects and client device contexts. Not all error conditions can be guaranteed to be cleanly recovered without end-user intervention such as reconnecting.
- Scalability. If the number of contexts supported by a RADIUS-client device exceeds the maximum number of host objects on a single SSG, external load balancing for a two-router solution is required.

## Information About SSG Authentication Using RADIUS Proxy

This section describes the following concepts:

- [SSG Autologon Using RADIUS Proxy, page 2](#)
- [RADIUS Server Redundancy, page 3](#)
- [Broadcast of Host Accounting, page 3](#)
- [RADIUS Client Subnet Definition, page 3](#)
- [Host Route Insertion, page 4](#)
- [Types of Deployments that Use SSG RADIUS Proxy, page 4](#)

## SSG Autologon Using RADIUS Proxy

The RADIUS proxy feature is principally an insertion mechanism to allow an SSG device to be introduced to a network with minimum disruption to the existing NAS and AAA server(s). By acting as a proxy between a client device using RADIUS authentication (which may or may not be Cisco equipment) and a AAA server, SSG is able to “sniff” the RADIUS flows and transparently create a corresponding SSG session, on successful authentication of the subscriber. This provides an “autologon” facility with respect to SSG for subscribers that are authenticated by devices that are closer to the network edge.

When configured as a RADIUS proxy, SSG transparently proxies all RADIUS requests generated by a client device and all RADIUS responses generated by the corresponding AAA server, as described in RFCs 2865, 2866 and 2869.

This RADIUS proxy functionality is largely agnostic to the type of client device, for example, GGSN, PDSN, WLAN AP etc. and supports standard authentication (that is a single Access-Request/Response exchange) using both PAP and CHAP, Access-Challenge packets, and also EAP mechanisms (RFC 2869). Of the various types of EAP authentication in existence (which differ, for example, in the transport mechanism for the session keys), EAP-SIM and EAP-TLS are supported.

Where authentication and accounting requests originate from separate RADIUS client devices, SSG will associate all requests to the appropriate session through the use of certain correlation rules. This may occur for centralized PWLAN deployments, wherein authentication requests originate from the WLAN AP while accounting requests are generated by the AZR. The association of the disparate RADIUS flows to the underlying session is performed automatically where the combination of username (attribute 1) and calling-station-id (attribute 31, if present) is sufficient to make the association reliable. However, in some cases, configuration (that is, the specification of additional attributes for use as correlation keys) is required to coerce the correct association.

Following a successful authentication, authorization data gleaned from the RADIUS response is applied to the corresponding SSG session.

Termination of a session created via RADIUS proxy operation is generally effected by receipt of an Accounting-Stop packet with an appropriate session. Accounting-On/Off from a RADIUS client will result in the termination of all SSG sessions hosted by that client.

## RADIUS Server Redundancy

When SSG acts as a RADIUS Proxy for a client device (GGSN, PDSN, HA etc.), access-requests that are generated by the client device are forwarded to the default RADIUS server, that is the first configured server. If this server fails, SSG provides fail-over to the next configured server (if present).

## Broadcast of Host Accounting

SSG RADIUS Proxy for GPRS networks can provide geographical redundancy by copying host object accounting packets and sending them to multiple RADIUS servers.

## RADIUS Client Subnet Definition

SSG will only proxy RADIUS packets originating from trusted client devices whose addresses have been explicitly configured in SSG. If SSG is acting as a proxy for multiple client devices, each of which resides on the same subnet, then the clients may be configured using a subnet definition rather than discrete IP addresses for each device. This configuration method results in a single client configuration entry for all the client devices, thus all client devices on this subnet must be configured with the same shared secret. Furthermore all these devices must be of the same type. For example CDMA2000 PDSNs and HAs must not share the same subnet configuration, although they may reside on the same subnet.

## Host Route Insertion

By default, SSG inserts a static route to the host for proxy users (if there is no existing route available). For some installations, this may be either unnecessary or even undesirable, so you can disable the host route insertion on a per-client basis.

**Note**

---

The host-route insert command does not apply to Auto-domain users that are not RADIUS-Proxy users. These users always have an IP address before any SSG involvement and so SSG would never be able to insert a static route.

---

When a host object is created, SSG checks to see if the host is reachable (on the correct interface) by an existing route and adds the static route only if it is not, and the insertion of host routes is enabled.

For the case where insertion of host routes is disabled, an "unrouted" timer may also be defined. If configured this timer is started when a host object is created with an unroutable IP address. If this IP address does not become routable (For example, due to a routing protocol update) before the timer expires, then the host object is destroyed.

## Types of Deployments that Use SSG RADIUS Proxy

SSG can be used as a RADIUS Proxy for subscriber authentication in the following types of deployments:

- GPRS networks
- CDMA2000
- 802.1X WLAN

## How to Configure SSG RADIUS Proxy

To configure SSG as a RADIUS proxy, use the tasks below. The first task applies to all RADIUS Proxy deployments and you need to perform this task first. The next three tasks are specific to particular deployments. The last two tasks apply to all RADIUS proxy deployments.

- [Configuring SSG Autologon Using RADIUS Proxy, page 4](#) (required)
- [Configuring SSG RADIUS Proxy for GPRS Networks, page 11](#) (optional)
- [Configuring SSG RADIUS Proxy for CDMA2000 Deployments, page 13](#) (optional)
- [Configuring SSG RADIUS Proxy for 802.1x WLAN Deployments, page 20](#) (optional)
- [Monitoring and Maintaining SSG RADIUS Proxy, page 25](#) (optional)
- [Troubleshooting SSG RADIUS Proxy, page 27](#) (optional)

## Configuring SSG Autologon Using RADIUS Proxy

This feature allows SSG to act as a proxy between a client device using RADIUS authentication and a AAA server and by "sniffing" the RADIUS flows, transparently create a corresponding SSG session, on successful authentication of the subscriber. Perform the following tasks to configure SSG Autologon Using RADIUS Proxy:

- [Enabling SSG Autologon Using RADIUS Proxy, page 5](#) (required)
- [Configuring Session Identification Attributes, page 6](#) (optional)
- [Configuring Timers for RADIUS Proxy, page 7](#)(optional)
- [Configuring Multiple RADIUS Server Support, page 9](#) (optional)

## Enabling SSG Autologon Using RADIUS Proxy

Perform this task to enable SSG Autologon using RADIUS Proxy.

### SUMMARY STEPS

1. `ssg radius-proxy`
2. `server-port [auth auth-port] [acct acct-port]`
3. `client-address ip-address [mask] key secret`
4. `forward accounting-start-stop [server-group group-name]`
5. `no host-route insert`
6. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>ssg radius-proxy</code></p> <p><b>Example:</b> Router(config)# ssg radius-proxy</p>	Enables SSG RADIUS Proxy and enters SSG-RADIUS-Proxy mode.
Step 2	<p><code>server-port [auth <i>auth-port</i>] [acct <i>acct-port</i>]</code></p> <p><b>Example:</b> Router(config-radius-proxy)# server-port auth 23 acct 45</p>	<p>Configures the authentication and accounting ports.</p> <ul style="list-style-type: none"> <li>• <b>auth</b>—(Optional) Configures the authentication port.</li> <li>• <i>auth-port</i>—(Optional) Specifies the authentication port number. The default authentication port is 1645. The valid range is 0 to 65535.</li> <li>• <b>acct</b>—(Optional) Configures the accounting port.</li> <li>• <i>acct-port</i>—(Optional) Specifies the accounting port number. The default accounting port is 1646. The valid range is 0 to 65535.</li> </ul>
Step 3	<p><code>client-address <i>ip-address</i> [mask] key <i>secret</i></code></p> <p><b>Example:</b> Router(config-radius-proxy)# client-address 172.16.0.0 key cisco</p>	<p>Configures the client IP address and the shared key secret of a RADIUS client.</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—IP address of a RADIUS client.</li> <li>• <i>mask</i>—Configures the client IP address as a subnet rather than as a discrete NAS IP address</li> <li>• <b>key</b>—Shared secret with the RADIUS client.</li> <li>• <i>secret</i>—Description of the shared secret.</li> </ul>

	Command or Action	Purpose
Step 4	<b>forward accounting-start-stop</b> [ <i>server-group group-name</i> ]  <b>Example:</b> Router(config-radius-proxy)# forward accounting-start-stop	(Optional) Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server. <ul style="list-style-type: none"> <li><b>server-group group-name</b>—Configures SSG to proxy RADIUS accounting packets to a specific server group.</li> </ul>
Step 5	<b>no host-route insert</b>  <b>Example:</b> Router(config-radproxy-client) no host-route insert	(Optional) Disables default host route insertion, on a per-client basis.
Step 6	<b>end</b>  <b>Example:</b> Router(config-radius-proxy)# end	Returns to privileged EXEC mode.

## Configuring Session Identification Attributes

By default, SSG selects the attribute used for session identification based on the type of client device. SSG assigns the 3GPP2-Correlation-ID attribute for PDSNs, Accounting-Session-ID attribute for HAs, and Calling-Station-ID attribute for non-CDMA2000 devices. You can override this automatic selection by using the following commands:

### SUMMARY STEPS

1. **ssg radius-proxy**
2. **client-address** [*ip-address*]
3. **key** [*secret*]
4. **session-identifier** {*auto* | *msid* | *correlation-id* | *accounting-session-id* | *ip* | *username*}
5. **remove vsa** {*3gpp2* | *cisco*}

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>ssg radius-proxy</b>  <b>Example:</b> Router(config)# ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-RADIUS-Proxy mode.
Step 2	<b>client-address</b> <i>ip-address</i>  <b>Example:</b> Router(config-radius-proxy)# client-address 1.2.3.6	Configures the RADIUS-client to proxy requests from the specified IP address to the RADIUS server and enters SSG-RADIUS-Proxy-Client mode.

	Command or Action	Purpose
Step 3	<pre>key <i>secret</i></pre> <p><b>Example:</b>  Router(config-radproxy-client)# key  mypassword</p>	(Optional) Configures the shared secret between SSG and the RADIUS client. The <i>secret</i> attribute describes the shared secret.
Step 4	<pre>session-identifier {auto   msid    correlation-id   accounting-session-id    ip   username}</pre> <p><b>Example:</b>  Router(config-radproxy-client)#  session-identifier auto</p>	(Optional) Overrides SSG's automatic RADIUS client session identification. <ul style="list-style-type: none"> <li>• <b>auto</b>—Automatically determines the session identifier.</li> <li>• <b>msid</b>—Uses the MSID as the client session identifier.</li> <li>• <b>correlation-id</b>—Uses the Correlation-ID as the session identifier.</li> <li>• <b>accounting-session-id</b>—Uses the Accounting-Session-ID as the session identifier.</li> <li>• <b>ip</b>—Specifies the user IP address as the session identifier.</li> <li>• <b>username</b>—Specifies the username as the session identifier.</li> </ul>
Step 5	<pre>remove vsa {3gpp2   cisco}</pre> <p><b>Example:</b>  Router(config-radproxy-client)# remove  vsa 3gpp2</p> <pre>Router(config-radproxy-client)# remove  vsa cisco</pre>	(Optional) Removes a VSA for a RADIUS client. <ul style="list-style-type: none"> <li>• <b>3gpp2</b>—Removes all 3GPP2 VSAs.</li> <li>• <b>cisco</b>—Removes all Cisco VSAs.</li> </ul>

## Configuring Timers for RADIUS Proxy

During the lifetime of an SSG RADIUS Proxy session, SSG expects to receive certain external events which are required for the session to continue. Whilst SSG is waiting for such external events, internal timers are running. If these timers expire, the RADIUS Proxy session is terminated.

Perform this task to configure the SSG RADIUS Proxy timers.

### SUMMARY STEPS

1. **ssg proxy-radius**
2. **server-port** [**auth** *auth-port*][**acct** *acct-port*]
3. **timeouts**
4. **hand-off** *timeout*
5. **idle** *timeout*
6. **session** *timeout*
7. **ip-address** *timeout*
8. **msid** *timeout* **retry** *retries*
9. **unrouted** *timeout*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>ssg proxy-radius</b>  <b>Example:</b> Router(config)# ssg proxy-radius	Enables SSG RADIUS-Proxy and enters SSG-RADIUS-Proxy mode.
Step 2	<b>server-port</b> [ <b>auth</b> <i>auth-port</i> ][ <b>acct</b> <i>acct-port</i> ]  <b>Example:</b> Router(config-radius-proxy)# server-port [auth 1645][acct 1646]	Configures the authentication and accounting ports. <ul style="list-style-type: none"> <li>• <b>auth</b>—(Optional) Configures the authentication port.</li> <li>• <i>auth-port</i>—(Optional) Specifies the authentication port number. The default authentication port is 1645. The valid range is 0 to 65535.</li> <li>• <b>acct</b>—(Optional) Configures the accounting port.</li> <li>• <i>acct-port</i>—(Optional) Specifies the accounting port number. The default accounting port is 1646. The valid range is 0 to 65535.</li> </ul>
Step 3	<b>timeouts</b>  <b>Example:</b> Router(config-radius-proxy)# timeouts	Enters SSG-RADIUS-Proxy-timeouts mode.
Step 4	<b>hand-off</b> <i>timeout</i>  <b>Example:</b> Router(config-radproxy-timer)# hand-off 30	Configures the RADIUS Proxy hand off timeout. Valid range is 1 to 30 seconds.
Step 5	<b>idle</b> <i>timeout</i> [ <b>reset-mode</b> { <b>radius</b>   <b>mixed</b> }]  <b>Example:</b> Router(config-radproxy-timer)# idle 150	Configures a host object timeout value. Valid range is 30 to 65536 seconds. <ul style="list-style-type: none"> <li>• <b>reset-mode</b>—Specifies the type of traffic that resets the idle timer.</li> <li>• <b>radius</b>—Resets the timer exclusively by RADIUS traffic</li> <li>• <b>mixed</b>—Resets the timer by both data traffic and RADIUS traffic.</li> <li>• If the reset mode is not set, by default the idle timer resets on receipt of data traffic.</li> </ul>
Step 6	<b>session</b> <i>timeout</i>  <b>Example:</b> Router(config-radproxy-timer)# session 100	Configures the global session timeout for RADIUS proxy sessions. Valid range is from 30 to 65535. There is no default value.
Step 7	<b>ip-address</b> <i>timeout</i>  <b>Example:</b> Router(config-radproxy-timer)# ip-address 25	Configures an SSG RADIUS Proxy IP address timeout. Valid range is 1 to 30 seconds.

	Command or Action	Purpose
Step 8	<b>msid timeout retry retries</b>  <b>Example:</b> Router(config-radproxy-timer)# msid 4 retry 9	Configures the SSG RADIUS Proxy mobile station ID (MSID) timeout. Valid range is 1 to 5 seconds. <ul style="list-style-type: none"> <li><i>timeout</i>—Timeout value, in seconds. Valid range is 1 to 5 seconds. The default is 1 second.</li> <li><b>retry retries</b>—Specifies the maximum number of times the MSID timer is restarted before SSG assumes it is not going to receive an MSID from the PDSN. Valid range is 1 to 20 retries. The default is 10 retries.</li> </ul>
Step 9	<b>unrouted timeout</b>  <b>Example:</b> Router(config-radproxy-timer)# unrouted 600	Configures the RADIUS proxy unroutable IP address timeout. Valid range is from 1 to 43200 seconds. <ul style="list-style-type: none"> <li>This timer may be used when insertion of host routes is disabled. If the IP address does not become routable before the timer expires, the host object is destroyed.</li> </ul>

## Configuring Multiple RADIUS Server Support

Perform this task to configure geographical redundancy for accounting records by allowing copies of host object accounting packets to be sent to multiple RADIUS servers. Note this is distinct from RADIUS server failover—the requirement here is that clones of accounting packets are always forwarded to each of the configured servers, not just when the primary server fails. To configure the support for multiple RADIUS servers, use the following commands:

### SUMMARY STEPS

1. **aaa group server radius** *group-name*
2. **server** *ip-address* [**auth** *auth-port*] [**acct** *acct-port*]
3. Repeat [Step 2](#) to configure additional RADIUS servers.
4. **exit**
5. **aaa group server radius** *group-name*
6. **server** *ip-address* [**auth** *auth-port*] [**acct** *acct-port*]
7. Repeat [Step 6](#) to configure additional RADIUS servers.
8. **exit**
9. **aaa accounting network** *ssg\_broadcast\_accounting start-stop broadcast group group-name 1 group group-name 2*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>aaa group server radius <i>group-name</i></pre> <p><b>Example:</b> Router(config)# aaa group server radius myservergroup1</p>	<p>Groups RADIUS server hosts into distinct lists and distinct methods.</p> <ul style="list-style-type: none"> <li><i>group-name</i>—Character string used to name the group of servers.</li> </ul>
Step 2	<pre>server <i>ip-address</i> [<b>auth</b> <i>auth-port</i>] [<b>acct</b> <i>acct-port</i>]</pre> <p><b>Example:</b> Router(config-sg-radius)# server 1.2.3.4 [auth 1645][acct 1646]</p>	<p>Configures the IP address of the RADIUS server for the group server.</p> <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of the RADIUS server host.</li> <li><b>auth</b> <i>auth-port</i>—(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The [<i>auth-port</i>] argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.</li> <li><b>acct</b> <i>acct-port</i>—(Optional) Specifies the UDP destination port for accounting requests. The [<i>acct-port</i>] argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.</li> </ul>
Step 3	Repeat <a href="#">Step 2</a> to configure additional RADIUS servers.	
Step 4	<pre>exit</pre> <p><b>Example:</b> Router(config-sg-radius)# exit</p>	Exits server group RADIUS configuration mode.
Step 5	<pre>aaa group server radius <i>group-name</i></pre> <p><b>Example:</b> Router(config)# aaa group server radius myservergroup2</p>	Configures the second, redundant RADIUS server.
Step 6	<pre>server <i>ip-address</i> [<b>auth</b> <i>auth-port</i>] [<b>acct</b> <i>acct-port</i>]</pre> <p><b>Example:</b> Router(config-sg-radius)# server 1.2.3.5 [auth 1645][acct 1646]</p>	Configures the IP address of the second RADIUS server for the group server.
Step 7	Repeat <a href="#">Step 6</a> to configure additional RADIUS servers.	

	Command or Action	Purpose
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(config-sg-radius)# exit</p>	Exits server group RADIUS configuration mode.
Step 9	<pre>aaa accounting network ssg_broadcast_accounting start-stop broadcast group group-name group group-name</pre> <p><b>Example:</b> Router(config)# aaa accounting network ssg_broadcast_accounting start-stop broadcast group myservergroup1 group myservergroup2</p>	<p>Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.</p> <ul style="list-style-type: none"> <li>• <b>ssg_broadcast_accounting</b>—Configures the broadcast group.</li> <li>• <b>start-stop</b>—Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.</li> <li>• <b>broadcast</b>—Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.</li> <li>• <b>group group-name</b>—Uses a subset of RADIUS servers for accounting as defined by the <b>server group group-name</b> command.</li> </ul>

## Configuring SSG RADIUS Proxy for GPRS Networks

The General Packet Radio System (GPRS) is a service that provides packet radio access for mobile Global System for Mobile Communications (GSM) and time-division multiple access (TDMA) users. By configuring SSG as a RADIUS proxy to the GGSN, SSG can provide service selection to and direct traffic of mobile wireless subscribers.

Before you configure SSG RADIUS proxy support for GPRS networks, you should understand the following concepts:

- [Prerequisites, page 11](#)
- [Overview of SSG RADIUS Proxy in GPRS Networks, page 12](#)
- [IP Addresses Assignment in GPRS Networks that Use SSG RADIUS Proxy, page 12](#)
- [Support For Overlapped Host IP Addresses, page 12](#)
- [Forwarding of Accounting Packets, page 13](#)
- [Session Identification by IP address, page 13](#)
- [Per-PDP Accounting in GPRS Networks that Use SSG RADIUS Proxy, page 13](#)

### Prerequisites

Before you configure RADIUS Proxy in GPRS networks, you must complete the steps in [Enabling SSG Autologon Using RADIUS Proxy, page 5](#).

## Overview of SSG RADIUS Proxy in GPRS Networks

The General Packet Radio System (GPRS) is a service that provides packet radio access for Global System for Mobile Communications (GSM) and time-division multiple access (TDMA) users.

The SSG RADIUS Proxy for GPRS feature allows an SSG device to be inserted between a GGSN and a NAP AAA server and act as a proxy for the authentication and accounting RADIUS flows. By monitoring these flows SSG can transparently create a corresponding SSG session, on successful authentication of the subscriber, and thus provide the user with access to the full range of SSG features.

## IP Addresses Assignment in GPRS Networks that Use SSG RADIUS Proxy

You can assign an IP address to the host object in any of the following ways; these are in order of precedence (but not necessarily preference):

1. Use the IP specified in the Access-Request. In this case, the GGSN has assigned the IP address and merely signals to the SSG the IP address that was allocated. SSG accepts this IP address (unless it is replaced by an AAA assigned IP address as explained below) and the Access-Accept packet replies with the same IP address.
2. Use the IP specified in the Access-Accept from the AAA. This is the case where the AAA server is being used to manage IP addresses.
3. For Auto-domain cases, use the IP address returned from the service domain. For the case where an IP address has not been assigned via the Access-Request or Access-Accept, the IP address from a tunnel or proxy service may be used.
4. If an IP address has not been acquired by any other method, assign one from an ip local pool configured for this purpose.
5. If an IP address was not assigned during the authentication phase, and no suitable local IP pools were available for IP assignment then use the IP address in the Accounting-Start from the client device. This is the case where the client device is using DHCP to allocate IP addresses.

If SSG receives an IP address in an AR from the GGSN, SSG proxies it to the AAA server. If the AAA server returns a different address in the AA, SSG assigns it to the host object, and returns it to the GGSN in the proxied AA. This in accordance with the RADIUS specification whereby IP addresses in ARs are treated by the server as hints and do not have to be honored.

For the case of auto-domain tunnel or proxy services, if there is already an IP address, SSG assigns this address to the host object and performs NAT towards this service.

If there is no existing route to the assigned IP address, static routes are added to the SSG's routing table with RADIUS-client as next-hop. This default behavior may be overridden by configuration (see ....) if, for example, routing protocols are in effect on the network and the static route addition is unnecessary.

## Support For Overlapped Host IP Addresses

Overlapped host IP addresses are supported for hosts connected to SSG on different point-to-point (other than RBE) downlink interfaces.

## Forwarding of Accounting Packets

While SSG is acting as a RADIUS Proxy for the GGSN it also receives all the Accounting packets. The Accounting Stop packet is used as an indication of session termination. By default, only Accounting-On/Off packets are forwarded to the real AAA server: Accounting-/Start/Stop/Update packets are not forwarded and SSG generates the responses locally. A CLI is provided to override this default behavior and allows transparent proxying of all accounting packets.

SSG will always proxy Accounting-On (or Accounting-Off) packets received from client GGSNs. These are used to signal that the client GGSN has just rebooted (or is about to be rebooted). When SSG receives the packets, SSG destroys all host objects associated with the specified client GGSN before forwarding the packet. Note that SSG uses the NAS-IP-Address in the Accounting-On/Off packets to determine the affected GGSN. This allows scenarios where multiple tunnel interfaces exist between the GGSN and SSG. In these scenarios, although there are multiple RADIUS clients configured at SSG, only a single Accounting-On/Off packet is generated by the GGSN. As part of normal SSG functionality, SSG sends Accounting-Start/Update/Stop records for both the active host objects and for any services they are connected to.

## Session Identification by IP address

The default session identification is the MSID. To override this default and specify the subscriber's IP address as the session identifier, use the **session-identifier** command.

## Per-PDP Accounting in GPRS Networks that Use SSG RADIUS Proxy

The Cisco GGSN (and presumably other GGSNs) supports per-PDP accounting rather than per-user accounting. In this mode Accounting-Start/Stop packets are generated for each PDP context activated by a subscriber, rather than a single pair representing the lifetime of the entire subscriber session. These multiple Accounting-Start/Stop pairs share the same Framed-IP-Address attribute (that is, the IP address of the user) and are distinguished by unique Accounting-Session-ID attributes.

SSG monitors the number of separate contexts associated with an IP address by monitoring the number of (different) Accounting-Starts received. When the number of contexts drops to zero or SSG receives an Accounting-Stop with a 3GPP-Session-Stop-Indicator, SSG terminates the session.

## Configuring SSG RADIUS Proxy for CDMA2000 Deployments

This section describes how to configure SSG RADIUS Proxy for CDMA2000 deployments. Before you configure SSG RADIUS proxy for CDMA2000 deployments, you should understand the following concepts:

- [Prerequisites, page 14](#)
- [Restrictions, page 14](#)
- [CDMA, page 15](#)
- [SSG RADIUS Proxy for CDMA2000 Overview, page 15](#)
- [SSG RADIUS Proxy for CDMA2000 for Simple IP, page 16](#)
- [SSG RADIUS Proxy for CDMA2000 for Mobile IP, page 17](#)
- [Dynamic Home Agent Assignment, page 17](#)
- [Benefits of SSG RADIUS Proxy for CDMA2000, page 18](#)

This section contains the following tasks:

- [Configuring Home Agent IP Addresses, page 18](#)
- [Verifying SSG RADIUS Proxy for CDMA2000, page 19](#)

## Prerequisites

### PDSN

- All RADIUS packets (including Access-Request packets for the Cisco variant of Module Subscriber Identity (MSID) based access) generated by the PDSN must contain the 3GPP2-Correlation-ID VSA.
- Access-Request packets for the Cisco variant of MSID-based access generated by the PDSN must contain the 3GPP2-Correlation-ID Vendor Specific Attribute (VSA).
- Accounting-Start packets generated by the PDSN must contain the 3GPP2-IP-Technology VSA.

### HA

- No RADIUS packets generated by the HA can contain the 3GPP2-Correlation-ID VSA.




---

**Note** The following HA prerequisites are not standard HA behavior and must be configured.

---

- The HA must issue Access-Requests for all Mobile IP sessions.
- The HA must issue Accounting-Start packets and Accounting-Stop packets for all Mobile IP sessions.
- The HA must provide the Acct-Session-ID attribute in all RADIUS packets it generates. This enables the system to differentiate between multiple sessions with the same Network Access Identifier (NAI).

### Miscellaneous

- RADIUS Access-Accept packets sent by the RADIUS server must contain the 3GPP2-IP-Technology VSA.

## Restrictions

SSG RADIUS Proxy for CDMA2000 requires non standard extensions to the Home Agent behavior. See [Prerequisites, page 14](#) for more information.

In Auto-domain mode, SSG bypasses user authentication at the Network Attached Storage (NAS) Authentication, Authorization and Accounting (AAA) server. SSG instead downloads a generic profile for the specified Auto-domain. This profile may be a service profile for simple Auto-domain or a virtual user profile in extended mode Auto-domain. When SSG is acting as a RADIUS Proxy in a CDMA2000 network, the profile returned in an Access-Accept from the AAA server must contain the 3GPP2-IP-Technology VSA to indicate to SSG whether this call setup is for a Simple IP call or for a Mobile IP call. Even if a network supports only one type of user (either all Simple IP users or all Mobile IP users), the Access-Accept packets received from the AAA must contain the 3GPP2-IP-Technology VSA. In networks that support only one type of user, the Auto-domain profiles can be formatted to contain the correct attribute. In networks that support both Mobile IP and Simple IP users simultaneously, the Access-Accept packets must contain the correct attribute for the type of user. The AAA server must be able to modify the contents of the generic Auto-domain profile so that it contains

the correct VSA. SSG must receive a real rather than a cached response from the AAA server for each user logon. SSG Service Profile Caching must be disabled when SSG Auto-domain is enabled and SSG is acting as a RADIUS Proxy in a CDMA2000 network that supports both Simple IP and Mobile IP users.

## CDMA

Code Division Multiple Access (CDMA) is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

For more information about CDMA, see the “CDMA Overview” knowledge byte on the Mobile Wireless Knowledge Bytes web page.

CDMA2000 Radio Transmission Technology (RTT) is a wideband, spread-spectrum radio interface that uses CDMA technology to satisfy the needs of third generation (3G) wireless communication systems. CDMA2000 is backward compatible with CDMA.

For more information about CDMA2000, refer to the “CDMA2000 Overview” knowledge byte on the Mobile Wireless Knowledge Bytes web page.

## SSG RADIUS Proxy for CDMA2000 Overview

The SSG RADIUS Proxy for CDMA2000 feature allows you to extend the functionality of the existing SSG RADIUS Proxy so that it may be used in CDMA2000 networks.

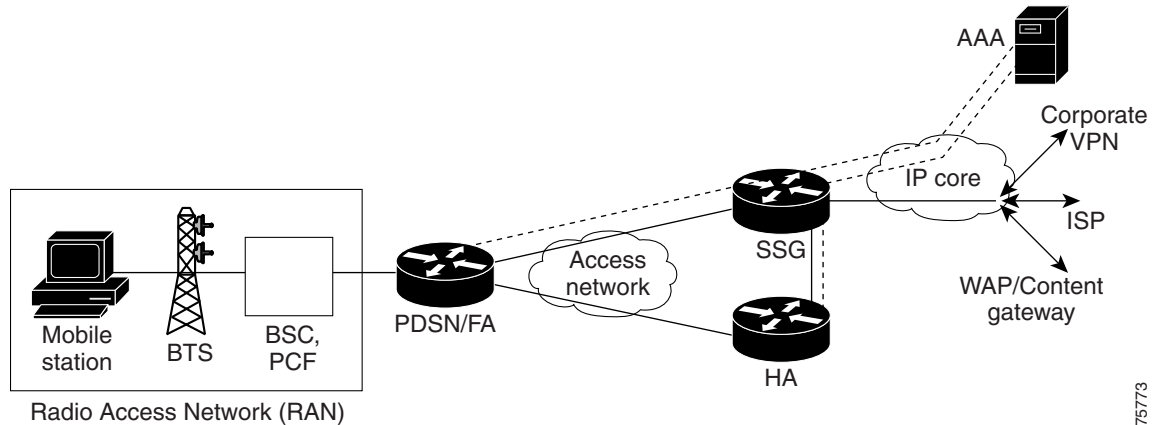
Code Division Multiple Access (CDMA) is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

When used in a CDMA2000 network, the Service Selection Gateway (SSG) provides RADIUS Proxy services to the Packet Data Serving Node (PDSN) and the Home Agent (HA) for both Simple IP and Mobile IP authentication. SSG also provides service selection management and policy-based traffic direction for subscribers.

SSG RADIUS Proxy for CDMA2000, used with Cisco Subscriber Edge Services Manager (SESM), provides users with on-demand services and service providers with service management and subscriber management.

SSG RADIUS Proxy for CDMA2000 supports time- and volume-based usage accounting for Simple IP and Mobile IP sessions. Prepaid and postpaid services are supported. Host accounting records can be sent to multiple network elements, including Content Service Gateways (CSGs), Content Optimization Engines (COEs), and Wireless Application Protocol (WAP) gateways.

Figure 1 CDMA Network



75773

Key to [Figure 1](#)

Item	Description
BTS	Base Transceiver Station
BSC	Base Station Controller
PCF	Packet Control Function
PDSN/FA	Packet Data Serving Node / Foreign Agent
VPN	Virtual Private Network

## SSG RADIUS Proxy for CDMA2000 for Simple IP

When used in a CDMA2000 environment, SSG acts as a RADIUS Proxy to the Packet Data Serving Node (PDSN) and to the Home Agent for Simple IP authentication. SSG sets up a host object for the following three access modes:

- PAP/CHAP authentication. In this mode, Password Authentication Protocol/ Challenge Handshake Authentication Protocol (PAP/CHAP) is performed during PPP setup and the NAI is received from a mobile node (MN).
- MSID-based access. In this mode, the MN does not negotiate CHAP or PAP and no Network Access Identifier (NAI) is received by the PDSN. The PDSN does not perform additional authentication. PDSN constructs an NAI based on the MSID and generates accounting records. Because a user password is not available from the MN, a globally configured password is used as the service password.
- MSID-based access Cisco variant. In this mode, a Cisco PDSN supports MSID-based access by using a realm retrieved from the RADIUS server. This realm is retrieved during an extra authentication phase with the RADIUS server.

SSG operating in a CDMA2000 network correlates Accounting-Start and Accounting-Stop requests. A PDSN may send out many Accounting-Start and Accounting-Stop requests during a session. These Accounting-Start and Accounting-Stop requests can be generated by PDSN hand off, Packet Control Function (PCF) hand off, interim accounting, and time-of-date accounting. SSG terminates a session

only when it receives an Accounting-Stop request with the 3GPP2-Session-Continue VSA set to FALSE or when a subsequent Accounting-Start request is not received within a configured timeout. PPP renegotiation during a PDSN hand off is treated as a new session.

In SSG RADIUS Proxy for CDMA2000 for Simple IP, the end-user IP address may be assigned statically by the PDSN, RADIUS server, or SSG. The end-user IP address can also be assigned directly from the Auto-domain service.

Network Address Translation (NAT) is automatically performed when necessary. NAT is generally necessary when IP address assignment is performed by any mechanism other than directly from the Auto-domain service (which may be a VPN). You can also configure SSG to always use NAT.

If the user profile contains Cisco attribute-value (AV) pairs of Virtual Private Dialup Network (VPDN) attributes, SSG initiates Layer 2 Tunneling Protocol (L2TP) VPN.

## SSG RADIUS Proxy for CDMA2000 for Mobile IP

For Mobile IP, SSG functions as the RADIUS Proxy for both PDSN and the HA. SSG proxies PPP PAP or CHAP and Mobile Node (MN)/Foreign Agent (FA) CHAP authentication. SSG RADIUS Proxy for CDMA2000 for Mobile IP can assign IP addresses statically by the PDSN, RADIUS server, or SSG. The end user IP address can also be assigned directly from the Auto-domain service.

Home Agent-Mobile Node (HA-MN) authentication and reverse tunneling must be enabled so that SSG can create host objects for Mobile IP sessions based on proxied RADIUS packets received from the HA.

The Home Agent must generate RADIUS accounting packets so that SSG can discover the user IP address and detect the termination of the session. Multiple Mobile IP sessions with the same NAI are supported. RADIUS packets must contain the Accounting-Session-ID attribute to be associated with the correct user session. SSG correlates RADIUS packets from the PDSN in order to obtain MSID information for a host object of a Mobile IP session.

SSG can set up a host object either with or without PAP/CHAP performed during the original PPP session.

SSG initiates L2TP VPN according to the SSG tunnel service VSAs in the user's profile. If the user profile contains Cisco AV pairs of VPDN, SSG sets up the L2TP tunnel per these VPDN attributes. SSG removes these AV pairs when sending the Access-Accept packet back to the PDSN.

Either the HA or the RADIUS server can assign the user's IP address.

## Dynamic Home Agent Assignment

Dynamic HA assignment based on a mobile user's location is supported.

The SSG RADIUS Proxy for CDMA2000 feature provides three options for dynamic HA assignment:

- The RADIUS server selects the local HA or any HA that is configured for session requests. For foreign-user call requests, the AAA server assigns the HA.
- SSG modifies the fixed HA address received from the RADIUS server to a local HA address. This method can be implemented without making any changes to the RADIUS server configuration. SSG does not modify the HA address for a foreign user. The foreign-user call request is registered with the HA address assigned by the AAA server.
- The PDSN implements dynamic HA assignment based on detection of the PDSN hand off.

## Benefits of SSG RADIUS Proxy for CDMA2000

SSG RADIUS Proxy for CDMA2000 provides the following features and capabilities:

- Centralized L2TP VPN tunnel management for Simple IP and for Mobile IP
- Centralized management for user service access and user-specific routing
  - Automatic logon of a user to SSG when the user establishes a PPP session with the PDSN or a Mobile IP flow with the HA
  - Automatic logon of the user to a service based on the domain name, structured username (user@domain), and Mobile Station ID (MSID). This eliminates the need for a service provider to have to make changes to existing AAA servers for VPDN service.
- Dynamic HA assignment
- Multiservice networking, including simultaneous services and sequential services, without the user having to log off and log back in
- Packet filtering. SSG uses Cisco IOS access control lists (ACLs) to prevent users, services, and pass through traffic from accessing specific IP addresses and ports.
- Per-service and per-destination accounting and billing
- Prepaid for CDMA2000 services
- SSG TCP Redirect for Services to captive portals for unauthenticated users

## Configuring Home Agent IP Addresses

SSG supports dynamic assignment of the Home Agent IP address using these commands. The HA IP address will only be dynamically assigned for sessions from a domain configured using these commands, where the domain is derived from the structured username of the session. The actual HA IP address assigned may be configured globally (that is, the same for all recognized domains) or on a per-domain basis. To configure Home Agent domain names and Home Agent IP addresses, use the following commands:

### SUMMARY STEPS

1. **ssg proxy-radius**
2. **home-agent address** [*ip-address*]
3. **home-agent domain** [*domain-name*] **address** [*ip-address*]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>ssg proxy-radius</b>  <b>Example:</b> Router(config)# ssg proxy-radius	Enables SSG RADIUS Proxy and enters SSG-RADIUS-Proxy mode.

	Command or Action	Purpose
Step 2	<b>home-agent address</b> [ <i>ip-address</i> ]  <b>Example:</b> Router(config-radius-proxy)# home-agent address 1.2.3.7	Configures an IP address for a Home Agent in a CDMA2000 network.
Step 3	<b>home-agent domain</b> <i>domain-name</i> [ <b>address</b> <i>ip-address</i> ]  <b>Example:</b> Router(config-radius-proxy)# home-agent domain mydomain.com address 1.2.3.8	Configures a domain for a Home Agent in a CDMA2000 network. Optionally configures an IP address for the domain.

## Verifying SSG RADIUS Proxy for CDMA2000

Perform this task to verify SSG RADIUS Proxy for CDMA2000.

### SUMMARY STEPS

1. **show ssg host** [*ip-address*]

### DETAILED STEPS

#### Step 1 **show ssg host** [*ip-address*]

Use the **show ssg host** command to display information about a host object including client device type. The following example shows host object information for Simple IP:

```
Router# show ssg host 10.0.0.0

----- HostObject Content -----
Activated: TRUE
Interface:
User Name: user1
Host IP: 10.0.0.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.3
  Device: PDSN (Simple IP)
  NASIP : 10.0.48.3
  SessID: 12345678
  APN   :
  MSID  : 5551000
  Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2002
User last activity at: *05:59:52.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
```

```
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
Subscribed Service Groups: NONE
```

The following example shows host object information for Mobile IP:

```
Router# show ssg host 10.0.0.101
```

```
----- HostObject Content -----
Activated: TRUE
Interface:
User Name: user1
Host IP: 10.0.0.101
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.4
    Device: HA
    NASIP : 10.0.48.4
    SessID: 44444445
    APN   :
    MSID  : 5551001
    Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *06:01:02.000 UTC Fri May 3 2002
User last activity at: *06:01:09.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
Subscribed Service Groups: NONE
```

## Configuring SSG RADIUS Proxy for 802.1x WLAN Deployments

In 802.1x WLAN deployments, SSG acts as a RADIUS Proxy during Extensible Authentication Protocol (EAP) authentication between a WLAN AP and the corresponding AAA server. Using SSG as a RADIUS Proxy in 802.1x deployments enables WLAN users to access SSG functionality after they have connected to the AP.

Before you configure SSG RADIUS Proxy for 802.1x WLAN deployments, you should understand the following concepts:

- [Prerequisites, page 21](#)
- [EAP Implementations Supported by SSG, page 21](#)
- [SSG EAP Environment, page 21](#)
- [EAP Transparency, page 22](#)
- [Prevention of IP Address Reuse, page 23](#)
- [User Reconnect After Logoff, page 23](#)

Perform the following task to configure SSG RADIUS Proxy for 802.1x WLAN deployments:

- [Configuring SSG RADIUS Proxy for 802.1x Deployments, page 23](#)

## Prerequisites

The SSG EAP Transparency feature operates in the environment described in the “[SSG EAP Environment](#)” section on page 21. Before you can use this feature, you must set up each of the components of the environment, as specified in other Cisco documents.

The SSG EAP Transparency feature has the following requirements:

- You must set up the SSG RADIUS Proxy feature on the router that has SSG. It enables the SSG to be aware of EAP authentication and process the user’s SSG service information sent in the Access-Accept packet. You also must configure the access point (AP) and AZR as the RADIUS Proxy client.
- The AP must use SSG as the authentication, authorization, and accounting (AAA) server for EAP authentication.
- The AZR must use the Domain Host Configuration Protocol (DHCP) accounting feature and the Address Resolution Protocol (ARP) log feature.
- SESM must be in RADIUS mode.

## EAP Implementations Supported by SSG

SSG supports the following EAP implementations, which are designed to support 802.1x requirements for public wireless LANs (PWLANS) and Ethernet LANs:

- EAP-Subscriber Identity Module (SIM)
- EAP-Transport Layer Security (TLS)
- Microsoft Protected Extensible Authentication Protocol (PEAP)
- Any other EAP mechanisms that use Microsoft Point-to-Point Encryption (MPPE) to share Wired Equivalent Privacy (WEP) keys

**Note**

---

SSG does not terminate native EAP messages. SSG supports EAP transparency by looking at the RADIUS packets generated by APs or switches.

---

## SSG EAP Environment

EAP authentication is an enhancement to Global System for Mobile communications (GSM) authentication and operates over the IEEE 802.1x standard. The Cisco implementation of EAP transparency for PWLANs operates in conjunction with the following components:

- Wireless LAN (WLAN) Access Point (AP)— A Network Access Server (NAS) to which wireless device users connect to this to reach the network. APs have radio channels on the user side and IP infrastructure on the network side.
- Access Zone Router (AZR)—A router that represents a “hotspot,” or access zone, and serves multiple clients in a populated area, such as an airport or coffee shop. Multiple Access Points are served by one AZR. The AZR is also the DHCP server for clients. The AZR is generally a lower-end Cisco router such as a Cisco 1700 or Cisco 2600-XM series routers.
- Cisco Service Selection Gateway (SSG)—A Cisco IOS feature that implements Layer 3 service selection through selective routing of IP packets to destination networks on a per-subscriber basis. When configured as a RADIUS Proxy between a WLAN AP and the corresponding AAA server, SSG enables users to access SSG functionality after they connect to the AP.

- Subscriber Edge Services Manager (SESM)—An extensible set of applications for providing support for on-demand value-added services and access control at the network edge. Together with SSG, SESM provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM web application and portal using a standard Internet browser. In RADIUS mode, SESM obtains subscriber and service information from a RADIUS server. (SESM in RADIUS mode is similar to the Cisco Service Selection Dashboard (SSD), which was replaced by SESM.)
- Authentication, authorization, and accounting (AAA) server—This server validates the claimed identity of a user device, grants access rights to a user or group, records who performed a certain action, and tracks user connections and certain activities, such as service and network resource usage. An AAA database is managed and accessed by a RADIUS security server.
- RADIUS server—An access server that uses the AAA protocol. It is a system of distributed security that secures remote access to networks and network services against unauthorized access. The server runs on a central computer, typically at the customer's site, and the clients reside in the dialup access servers and can be distributed throughout the network.
- Signaling System 7 (SS7) network—A system that stores information that is required for setting up and managing telephone calls on the public switched telephone network (PSTN). The information is stored on a network separate from the network on which the call was made. The AAA server communicates with a Cisco IP Transfer Point (ITP), which acts as a gateway between the IP and SS7 networks. Using Mobile Application Part (MAP) messages, the system gets user service profiles from the subscriber's Home Location Register (HLR). In addition, the system includes an authentication center (AuC), which provides authentication and encryption parameters to verify each user's identity and ensure call confidentiality.

On the client side, the EAP protocol is implemented in the EAP supplicant. The supplicant code is linked into the EAP framework provided by the operating system; currently, supplicants exist for Microsoft Windows XP and Windows 2000. The EAP framework handles EAP protocol messages and communications between the supplicant and the AAA server; it also installs any encryption keys provided to the supplicant in the client's WLAN radio card.

On the network side, the EAP authenticator code resides on the service provider's AAA server. Besides handling the server side of the EAP protocol, this code is also responsible for communicating with the service provider's AuC. In a Cisco implementation of EAP, the AAA server communicates with a Cisco IP transfer point (ITP). The Cisco ITP translates messages from the AAA server into standard GSM protocol messages, which are then sent to the AuC.

## EAP Transparency

The SSG EAP Transparency feature allows SSG on a Cisco router to act as a RADIUS Proxy during EAP authentication. SSG creates the host after successful EAP authentication, so the user does not have to log on through the web portal. Instead, the user is automatically logged in.

The AP does the authentication for the client. SSG looks like a AAA server, which proxies relevant packets to the real AAA server. To create a host automatically, SSG has to know that the authentication was successful. By proxying messages, it obtains this information. The IP address is not assigned until authentication is complete, so SSG creates an inactive host and uses the MAC address as an identifier. To get the IP address, it waits for a DHCP Accounting Start from the AZR, so the AZR must be configured as an SSG RADIUS Proxy client.

## Prevention of IP Address Reuse

When the AZR reboots, it sends Accounting On/Off packets. SSG receives these packets and, even though EAP users may be connected, it moves hosts to the inactive state and starts an inactive-period timer. During the DHCP renewal, the AZR performs an ARP lock and sends an Accounting Start packet to SSG. After receiving an Accounting Start packet, SSG activates the corresponding hosts using the MAC address as the identity. If the inactive-period timer expires, SSG removes all of the inactive hosts.

This functionality prevents the use of previously valid IP addresses after an AZR reboot. It closes a security hole that could allow an illegal user to hijack the session of a valid user through the IP address, and at the same time it removes the inconvenience of reauthentication for the user. In order to prevent the reuse of IP addresses, clients must be configured with a short DHCP lease interval. If users are not configured with a short lease interval, they will have to reauthenticate whenever the AZR reboots.

## User Reconnect After Logoff

EAP users do not have a username and password as other types of SSG users do. If they access SESM, log off, and try to reconnect to the service later, SESM presents them with a logon page, which they cannot use. To allow EAP users to reconnect without being asked to log on again, enable the user reconnect functionality with the `ssg wlan reconnect` command.

The following steps describe the SSG EAP transparency user reconnect process:

1. The user connects to SSG via an EAP mechanism, and SSG creates the host (as explained in the “EAP Transparency” section).
2. The user accesses SESM. SESM queries SSG about the user, and SSG provides SESM with the user profile information. SESM displays the service logon page for the user to select services.
3. When the EAP user logs off SESM, SSG does not remove the host (as it does for other types of users), but rather inactivates the host.
4. The user attempts to access SESM again to use a service. SESM queries SSG. SSG activates the host and enables autologon services.

SSG deletes an active or inactive host when it receives an Accounting Stop packet from the AZR.

The SSG EAP transparency user reconnect functionality can be enabled or disabled using the command-line interface, as described in the “SUMMARY STEPS” section on page 23.



### Note

If user reconnect is enabled and a user refreshes or reloads the SESM page after an account logoff, SESM sends a query to SSG, which causes SSG to activate the host. It is recommended that users be made aware of this behavior so they do not accidentally activate the host.

## Configuring SSG RADIUS Proxy for 802.1x Deployments

Perform this task to configure SSG as a RADIUS proxy in a 802.1x WLAN deployment.

### SUMMARY STEPS

1. `ssg radius-proxy`
2. `client-address IP-address`
3. `key secret`
4. `session-identifier { auto | msid | correlation-id | accounting-session-id }`

5. **timeouts**
6. **idle timeout**  
or  
**ip-address timeout**
7. **exit**
8. **exit**
9. Repeat Steps 5 to 9 to configure the AZR as a RADIUS client.
10. **ssg wlan reconnect**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>ssg radius-proxy</b>  <b>Example:</b> Router(config)# ssg radius-proxy	Enables SSG RADIUS Proxy and SSG-RADIUS-Proxy configuration mode.
Step 2	<b>client-address</b> <i>IP-address</i>  <b>Example:</b> Router(config-radius-proxy)# client-address 123.123.123.123	Configures the RADIUS client IP address. <ul style="list-style-type: none"> <li>Use this command to configure the AP as a RADIUS client to proxy requests from the specified IP address to the RADIUS server.</li> </ul>
Step 3	<b>key</b> <i>secret</i>  <b>Example:</b> Router(config-radproxy-client)# key cisco	Configures the shared secret. <ul style="list-style-type: none"> <li>Use the <i>secret</i> argument to configure each client IP with a unique shared secret. This shared secret should be the same one that is configured on the RADIUS client.</li> </ul>
Step 4	<b>session-identifier</b> { <b>auto</b>   <b>msid</b>   <b>correlation-id</b>   <b>accounting-session-id</b> }  <b>Example:</b> Router(config-radproxy-client)# session-identifier auto	(Optional) Overrides SSG automatic RADIUS client session identification. Keywords are as follows: <ul style="list-style-type: none"> <li><b>auto</b>—Automatically determines the session identifier.</li> <li><b>msid</b>—Uses the MSID as the client session identifier.</li> <li><b>correlation-id</b>—Uses the Correlation-ID as the session identifier.</li> <li><b>accounting-session-id</b>—Uses the Accounting-Session-ID as a session identifier.</li> </ul>
Step 5	<b>timeouts</b>  <b>Example:</b> Router(config-radproxy-client)# timeouts	(Optional) Enters SSG-RADIUS-Proxy-Timeouts mode.

	Command or Action	Purpose
Step 6	<p><code>idle timeout</code></p> <p>or</p> <p><code>ip-address timeout</code></p> <p><b>Example:</b> Router(config-radproxy-timer)# <code>idle 30</code></p>	<p>(Optional) Specifies a timeout value. Use one of two commands:</p> <ul style="list-style-type: none"> <li>The first command configures a host object timeout value. The valid range is from 30 to 65536 seconds.</li> <li>The second command configures an SSG RADIUS Proxy IP address timeout. The valid range is from 1 to 180 seconds.</li> </ul>
Step 7	<p><code>exit</code></p> <p><b>Example:</b> Router(config-radproxy-timer)# <code>exit</code></p>	Exits to SSG-RADIUS-Proxy-Client configuration mode.
Step 8	<p><code>exit</code></p> <p><b>Example:</b> Router(config-radproxy-client)# <code>exit</code></p>	Exits to SSG-RADIUS-Proxy configuration mode.
Step 9	Repeat Steps 5 to 9 to configure the AZR as a RADIUS client.	
Step 10	<p><code>ssg wlan reconnect</code></p> <p><b>Example:</b> Router(config)# <code>ssg wlan reconnect</code></p>	Enables EAP users to reconnect after logging off or having idle time out occur.

## Monitoring and Maintaining SSG RADIUS Proxy

Perform this task to monitor and maintain SSG Autologon for RADIUS Proxy users.

### SUMMARY STEPS

1. `clear ssg radius-proxy client-address ip address`
2. `clear ssg radius-proxy nas-address ip address`
3. `show ssg auto-domain exclude-profile`
4. `show ssg binding`
5. `show ssg connection ip-address service-name`
6. `show ssg direction`
7. `show ssg host [ip-address] [count] [username]`
8. `show ssg next-hop`
9. `show ssg radius-proxy address-pool address-pool`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>clear ssg radius-proxy client-address ip address</pre> <p><b>Example:</b> Router# clear ssg radius-proxy client-address 172.16.0.0 </p>	(Optional) Clears all hosts connected to a specific RADIUS client. <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of the RADIUS client to clear.</li> </ul>
Step 2	<pre>clear ssg radius-proxy nas-address ip address</pre> <p><b>Example:</b> Router# clear ssg radius-proxy nas-address 172.16.0.0 </p>	(Optional) Clears all hosts connected to a specific NAS client. <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of the NAS client to clear.</li> </ul>
Step 3	<pre>show ssg auto-domain exclude-profile</pre> <p><b>Example:</b> Router# show ssg auto-domain exclude-profile </p>	Displays the contents of an Auto-domain exclusion profile downloaded from the AAA server. Only Auto-domain exclude entries entered via CLI are displayed.
Step 4	<pre>show ssg binding</pre> <p><b>Example:</b> Router# show ssg binding </p>	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
Step 5	<pre>show ssg connection ip-address service-name</pre> <p><b>Example:</b> Router# show ssg connection 19.1.1.19 InstMsg </p>	Displays the connections of a given host and service name. <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of an active SSG connection. This is always a subscribed host.</li> <li><i>service-name</i>—The name of an active SSG connection.</li> </ul>
Step 6	<pre>show ssg direction</pre> <p><b>Example:</b> Router# show ssg direction </p>	Displays the direction of all interfaces for which a direction has been specified.
Step 7	<pre>show ssg host [ip-address] [count] [username]</pre> <p><b>Example:</b> Router# show ssg host 10.3.1.1 </p>	Displays the information about a subscriber and the current connections of the subscriber. <ul style="list-style-type: none"> <li><i>ip-address</i>—(Optional) IP address of the host.</li> <li><b>count</b>—(Optional) Displays the host object count, including inactive hosts.</li> <li><b>username</b>—(Optional) Displays the usernames logged into the active hosts.</li> </ul>

	Command or Action	Purpose
Step 8	<code>show ssg next-hop</code>	Displays the next-hop table.
	<b>Example:</b> Router# <code>show ssg next-hop</code>	
Step 9	<code>show ssg radius-proxy address-pool address-pool</code> [ <code>domain domain-name</code> ] [ <code>free</code>   <code>inuse</code> ]	Displays IP address pool usage for a specific domain for an entire router.
	<b>Example:</b> Router# <code>show ssg radius-proxy address-pool domain</code> <code>ssg.com free</code>	

## Troubleshooting SSG RADIUS Proxy

Perform this task to troubleshoot SSG authentication of RADIUS proxy subscribers.

### SUMMARY STEPS

1. `debug ssg ctrl-packets`
2. `debug ssg port-map events`
3. `debug ssg port-map packets`

### DETAILED STEPS

Step 1	<code>debug ssg ctrl packets</code>	Displays packet contents handled by control modules.
	<b>Example:</b> Router# <code>debug ssg ctrl packets</code>	
Step 2	<code>debug ssg port-map events</code>	Displays port mapping event messages.
	<b>Example:</b> Router# <code>debug ssg port-map events</code>	
Step 3	<code>debug ssg port-map packets</code>	Displays port mapping packet contents.
	<b>Example:</b> Router# <code>debug ssg port-map packets</code>	

## Examples

The following output is generated by using the `debug ssg ctrl-packets` command when a RADIUS proxy subscriber logs out of a service:

```
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.

# Configuration Examples for SSG Authentication of RADIUS Proxy Subscribers

This section contains the following examples:

- [SSG Autologon Using RADIUS Proxy: Examples, page 29](#)
- [SSG RADIUS Proxy for CDMA2000: Examples, page 30](#)
- [SSG RADIUS Proxy for 802.1x WLAN Deployments: Example, page 33](#)

## SSG Autologon Using RADIUS Proxy: Examples

This section contains the following examples:

- [Enabling SSG Autologon Using RADIUS Proxy: Example, page 29](#)
- [Configuring Session Identification Attributes: Examples, page 29](#)
- [Configuring Timers for RADIUS Proxy: Examples, page 30](#)

### Enabling SSG Autologon Using RADIUS Proxy: Example

In the following example, SSG is configured as a RADIUS Proxy. Port 1500 is configured as the authentication port, and port 1499 is configured as the accounting port. A client with the IP address 192.0.2.0 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 192.2.2.0 and an end IP address 192.6.2.0. 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 192.7.2.0 and from the NAS at IP address 192.8.2.0 are deactivated and destroyed.

```
ssg enable
!
ssg radius-proxy
server-port auth 1500 acct 1499
client-address 192.0.2.0 key secret1
address-pool 192.2.0. 192.6.2.0 domain cisco
idle-timeout 60
!
forward accounting-start-stop
exit
```

### Configuring Session Identification Attributes: Examples

The following example shows how to configure SSG to identify the specified client session based on MSID:

```
ssg enable
ssg proxy-radius
client-address 192.0.2.0
key cisco
session-identifier msid
```

The following example shows how to configure SSG to identify the specified client session based on the 3GPP2-Correlation-ID attribute:

```

ssg enable
ssg proxy-radius
  client-address 192.0.2.0
  key cisco
  session-identifier correlation-id

```

The following example shows how to configure SSG to identify the specified client session based on the Accounting-Session-ID attribute:

```

ssg enable
ssg proxy-radius
  client-address 192.0.2.0
  key cisco
  session-identifier accounting-session-id

```

## Configuring Timers for RADIUS Proxy: Examples

The following example shows how to enable SSG RADIUS Proxy and to configure a hand off timeout of 25 seconds:

```

ssg enable
ssg proxy-radius
  server-port auth 1812 acct 1813
  hand-off 25

```

The following example shows how to enable SSG RADIUS Proxy and to configure an idle timeout of 60 seconds:

```

ssg enable
ssg proxy-radius
  server-port auth 1812 acct 1813
  idle 60

```

The following example shows how to enable SSG RADIUS Proxy and to configure an IP address timeout of 10 seconds:

```

ssg enable
ssg proxy-radius
  server-port auth 1812 acct 1813
  ip-address 60

```

The following example shows how to enable SSG RADIUS Proxy and to configure an MSID timeout of 3 seconds:

```

ssg enable
ssg proxy-radius
  server-port auth 1812 acct 1813
  msid 3 retry 3

```

## SSG RADIUS Proxy for CDMA2000: Examples

- [Configuring Multiple RADIUS Server Support: Example, page 31](#)
- [Configuring Timers for RADIUS Proxy: Examples, page 30](#)
- [Configuring Multiple RADIUS Server Support: Example, page 31](#)
- [Configuring Home Agent IP Addresses: Example, page 31](#)
- [Removing VSA Types: Examples, page 31](#)
- [SSG RADIUS Proxy for CDMA2000 - Complete Configuration: Example, page 31](#)

## Configuring Multiple RADIUS Server Support: Example

The following example shows how to configure multiple RADIUS servers in a CDMA2000 network. Configuring multiple RADIUS servers provides geographical redundancy by sending copies of host object accounting packets to multiple RADIUS servers.

```
aaa group server radius billing
  server 10.0.0.1 auth-port 1812 acct-port 1813
  end
!
aaa server group server radius hotstandby
  server 10.0.0.2 auth-port 1813 acct-port 1813
  end
!
aaa accounting network ssg_broadcast_accounting start-stop broadcast group billing group
hotstandby
```

## Configuring Home Agent IP Addresses: Example

The following example shows how to configure a Home Agent with IP address 172.16.0.0 and with a domain name of "hadomain1".

```
ssg enable
ssg proxy-radius
  home-agent address 192.0.2.0
  home-agent domain hadomain1
```

## Removing VSA Types: Examples

The following example shows how to remove all Cisco VSAs from a RADIUS response sent to a RADIUS client:

```
ssg enable
ssg proxy-radius
  client-address 192.0.2.0
  remove vsa cisco
```

The following example shows how to remove all 3GPP2 VSAs from a RADIUS response sent to a RADIUS client:

```
ssg enable
ssg proxy-radius
  client-address 192.0.2.0
  remove vsa 3gpp2
```

## SSG RADIUS Proxy for CDMA2000 - Complete Configuration: Example

The following example shows the complete configuration of SSG as a RADIUS proxy in a CDMA2000 network:

```
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
!
aaa new-model
!
```

```

aaa group server radius OPERATIONS
  server 10.10.50.181 auth-port 1645 acct-port 1646
!
aaa group server radius RASCUSTOMER
  server 10.10.50.180 auth-port 1645 acct-port 1646
!
aaa authentication login vty line
aaa authentication ppp default local group radius
aaa authorization exec vty none
aaa authorization network default local group radius none
aaa authorization network ssg_aaa_author_internal_list none
aaa accounting update periodic 1
aaa accounting network ssg_broadcast_accounting start-stop broadcast group OPERATIONS
group RASCUSTOMER
aaa nas port extended
aaa session-id common
enable password password1
!
username cisco password 0 cisco
redundancy
  main-cpu
  auto-sync standard
  no secondary console enable
!
ip subnet-zero
ip cef
no ip domain-lookup
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
vpdn enable
vpdn search-order domain
!
vpdn-group 1
  accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 1000
  pppoe limit per-vc 1000
!
vpdn-group 3
  request-dialin
  protocol l2tp
  domain tunsvc
  domain banking
  local name dial-tunnel
!
!
!
ssg enable
ssg default-network 10.0.48.0 255.255.255.0
ssg service-password servicecisco
ssg radius-helper auth-port 1812 acct-port 1813
ssg radius-helper key cisco
ssg maxservice 12
ssg accounting interval 300000
ssg bind service vidconf ATM0/0/0.159
ssg bind service banking ATM0/0/0.156
ssg bind service internet-red ATM0/0/0.152
ssg bind service games ATM0/0/0.155
ssg bind service corporate ATM0/0/0.154
ssg bind service shop ATM0/0/0.158
ssg bind service distlearn ATM0/0/0.157
ssg bind service internet-green ATM0/0/0.153
ssg bind service iptv ATM0/0/0.160

```

```

ssg bind service internet-blue ATM0/0/0.151
ssg bind direction downlink Ethernet0/0/0
ssg bind direction downlink FastEthernet0/0/0
!
ssg radius-proxy
  server-port auth 1645 acct 1646
  client-address 10.0.48.3
  key cisco
!
  client-address 10.0.48.4
  key cisco
!
  timeouts
  idle 60000
!
  address-pool 77.77.77.77 77.77.77.88 domain msid3.access
  address-pool 88.88.88.88 88.88.88.99 domain corporate3
  address-pool 99.99.99.99 99.99.99.111 domain nat-test
  address-pool 66.66.66.66 66.66.66.77 domain corporate
  home-agent address 4.3.2.1
!
ssg auto-domain
  exclude apn corporate
  exclude apn corporate3
!
local-profile local1
  attribute 26 9 251 "D192.1.1.1"
.
.
.
radius-server host 10.0.48.3 auth-port 1812 acct-port 1813 key troy
radius-server host 10.10.50.181 auth-port 1645 acct-port 1646
radius-server host 10.10.50.180 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute nas-port format d
radius-server key troy
radius-server vsa send accounting
radius-server vsa send authentication
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password cisco
  login authentication vty
!

```

## SSG RADIUS Proxy for 802.1x WLAN Deployments: Example

The following example shows the configuration of SSG as a RADIUS proxy in a 802.1x WLAN deployment.

```

.
.
.
radius-server host 9.2.36.253 auth-port 1645 acct-port 1646 key cisco

```

```

ssg enable

ssg radius-proxy
server-port auth 1645 acct 1646
client-address 1.1.1.1
key cisco
session-identifier auto
!
client-address 1.1.1.1
key cisco
!
timeouts
ip-address 60
!

ssg wlan reconnect

```

## Where to Go Next

To configure other methods of subscriber authentication, refer to the following modules:

- [Configuring SSG to Authenticate Subscribers Automatically in the Service Domain](#)
- [Configuring SSG Support for Subnet-Based Authentication](#)
- [Configuring SSG for MAC-Address-Based Authentication](#)
- [Configuring SSG to Authenticate PPP Subscribers](#)
- [Configuring SSG to Authenticate Web Logon Subscribers](#)
- [Configuring SSG to Authenticate Subscribers with Transparent Autologon](#)

To configure SSG to authenticate RADIUS Proxy subscribers, refer to [Configuring SSG to Serve as a RADIUS Proxy](#)

## Additional References

The following sections provide references related to configuring SSG to authenticate RADIUS Proxy subscribers.

## Related Documents

Related Topic	Document Title
Cisco IOS voice, video and fax commands	<a href="#">Cisco IOS Voice, Video, and Fax Command Reference</a>
Cisco IOS voice, video and fax configuration	<a href="#">Cisco IOS Voice, Video, and Fax Configuration Guide</a>
Configuring SESM	<a href="#">Cisco Subscriber Edge Services Manager documentation</a>
RADIUS commands	<a href="#">Cisco IOS Security Command Reference</a>
RADIUS configuration tasks	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i>
SSG commands	<a href="#">Cisco IOS Service Selection Gateway Command Reference</a>

Related Topic	Document Title
DHCP accounting	<i>DHCP Accounting</i> feature
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>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Feature Information for SSG RADIUS Proxy

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, 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](#).

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. 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.



### Note

Table 1 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 1** Feature Information for Configuring SSG to Serve as a RADIUS Proxy

Feature Name	Releases	Feature Configuration Information
SSG AAA Server Group for Proxy RADIUS	12.3(3)B 12.3(1a)BW 12.3(4)T 12.4	This feature allows you to configure multiple AAA servers. You can configure each remote RADIUS server with timeout and retransmission parameters. SSG will perform failover among the servers in the predefined group.  The following section provides information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Configuring Multiple RADIUS Server Support, page 9</a></li> </ul>
SSG Autologon Using Proxy RADIUS	12.2(4)B 12.2(13)T 12.4	The SSG Autologon Using Proxy RADIUS feature enables SSG to act as a RADIUS proxy for non-SSD clients whose Access-Requests do not contain VSAs.  The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">SSG Autologon Using RADIUS Proxy, page 2</a></li> <li>• <a href="#">Types of Deployments that Use SSG RADIUS Proxy, page 4</a></li> <li>• <a href="#">Configuring SSG Autologon Using RADIUS Proxy, page 4</a></li> <li>• <a href="#">Monitoring and Maintaining SSG RADIUS Proxy, page 25</a></li> <li>• <a href="#">Troubleshooting SSG RADIUS Proxy, page 27</a></li> </ul>

**Table 1** Feature Information for Configuring SSG to Serve as a RADIUS Proxy

Feature Name	Releases	Feature Configuration Information
SSG EAP Transparency	12.2T 12.3(4)T	<p>In 802.1x WLAN deployments, SSG acts as a RADIUS Proxy during Extensible Authentication Protocol (EAP) authentication between a WLAN AP and the corresponding AAA server. Using SSG as a RADIUS Proxy in 802.1x deployments enables WLAN users to access SSG functionality after they have connected to the AP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring SSG RADIUS Proxy for 802.1x WLAN Deployments, page 20</a></li> <li>• <a href="#">EAP Implementations Supported by SSG, page 21</a></li> <li>• <a href="#">SSG EAP Environment, page 21</a></li> <li>• <a href="#">EAP Transparency, page 22</a></li> <li>• <a href="#">Prevention of IP Address Reuse, page 23</a></li> <li>• <a href="#">User Reconnect After Logoff, page 23</a></li> <li>• <a href="#">SSG Autologon Using RADIUS Proxy: Examples, page 29</a></li> <li>• <a href="#">SSG RADIUS Proxy for 802.1x WLAN Deployments: Example, page 33</a></li> </ul>
SSG Proxy for CDMA2000	12.2(15)B 12.2T 12.3(4)T	<p>This feature enables service selection in CDMA2000 networks through enhancements to the SSG RADIUS Proxy functionality.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring SSG RADIUS Proxy for CDMA2000 Deployments, page 13</a></li> <li>• <a href="#">Configuring Home Agent IP Addresses: Example, page 31</a></li> </ul>
Configuring SSG to Serve as a RADIUS Proxy	15.0(1)M	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.

