



# Enabling ISG to Interact with External Policy Servers

---

**First Published: March 20, 2006**  
**Last Updated: September 22, 2008**

Intelligent Services Gateway (ISG) is a Cisco IOS software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document describes how to enable ISG to retrieve session policies or accept dynamic updates to session policies from external policy servers.

## 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 ISG Interaction with External Policy Servers](#)” section on page 7.

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

- [Restrictions for ISG Interaction with External Policy Servers](#), page 2
- [Information About ISG Interaction with External Policy Servers](#), page 2
- [How to Enable ISG to Interact with External Policy Servers](#), page 2
- [Configuration Examples for ISG Interaction with External Policy Servers](#), page 6
- [Additional References](#), page 6
- [Feature Information for ISG Interaction with External Policy Servers](#), page 7



---

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

© 2006–2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for ISG Interaction with External Policy Servers

For information about release and platform support, see the [“Feature Information for ISG Interaction with External Policy Servers”](#) section on page 7.

# Restrictions for ISG Interaction with External Policy Servers

The ISG and external policy servers should be in the same virtual routing and forwarding instance (VRF).

# Information About ISG Interaction with External Policy Servers

To configure ISG interaction with external policy servers, you should understand the following concept:

- [Initial and Dynamic Authorization, page 2](#)

## Initial and Dynamic Authorization

ISG works with external devices, referred to as *policy servers*, that store per-subscriber and per-service information. ISG supports two models of interaction between ISG and external policy servers: initial authorization and dynamic authorization.

In the initial authorization model, ISG must retrieve policies from the external policy server at specific points in a session. In this model, the external policy server is typically an authentication, authorization, and accounting (AAA) server that uses RADIUS. ISG is the RADIUS client. Instead of a AAA server, some systems use a RADIUS proxy component that converts to other database protocols such as Lightweight Directory Access Protocol (LDAP).

The dynamic authorization model allows the external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of some algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

# How to Enable ISG to Interact with External Policy Servers

This section contains the following tasks:

- [Configuring the ISG as a AAA Client, page 2](#)
- [Configuring the ISG as a AAA Server, page 4](#)

## Configuring the ISG as a AAA Client

Perform this task to configure AAA method lists and enable ISG to retrieve policies from a AAA server. This task must be performed for both initial and dynamic authorization models.

## Prerequisites

The servers and server groups referenced by the AAA methods must be configured.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication login** {default | list-name} method1 [method2...]
4. **aaa authentication ppp** {default | list-name} method1 [method2...]
5. **aaa authorization** {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [method2...]]
6. **aaa authorization subscriber-service** {default {cache | group | local} | list-name} method1 [method2...]
7. **aaa accounting** {auth-proxy | system | network | exec | connection | commands level} {default | list-name} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] group groupname
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa authentication login</b> {default   list-name} method1 [method2...]  <b>Example:</b> Router(config)# aaa authentication login PPP1 group radius	Specifies one or more AAA authentication methods to be used at login.
Step 4	<b>aaa authentication ppp</b> {default   list-name} method1 [method2...]  <b>Example:</b> Router(config)# aaa authentication ppp default group radius	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	<b>aaa authorization</b> {network   exec   commands level   reverse-access   configuration} {default   list-name} [method1 [method2...]]  <b>Example:</b> Router(config)# aaa authorization network NET1 radius	Specifies one or more AAA authorization methods to be used for restricting subscriber access to a network.

	Command or Action	Purpose
Step 6	<pre>aaa authorization subscriber-service {default {cache   group   local}   list-name} method1 [method2...]</pre> <p><b>Example:</b> Router(config)# aaa authorization subscriber-service default local group radius </p>	<p>Specifies one or more AAA authorization methods for ISG to use in providing a service.</p> <p>The <b>default</b> keyword used with either the <b>cache</b>, <b>group</b> or <b>local</b> keywords select the default cached-group, server-group or local database respectively for the authorization method.</p>
Step 7	<pre>aaa accounting {auth-proxy   system   network   exec   connection   commands level} {default   list-name} [vrf vrf-name] {start-stop   stop-only   none} [broadcast] group groupname</pre> <p><b>Example:</b> Router(config)# aaa accounting network default start-stop group radius </p>	<p>Enables AAA accounting of requested services for billing or security purposes.</p>
Step 8	<pre>end</pre> <p><b>Example:</b> Router(config)# end </p>	<p>Exits global configuration mode.</p>

## Configuring the ISG as a AAA Server

Dynamic authorization allows a policy server to dynamically send policies to ISG. Perform this task to configure the ISG as a AAA server and enable dynamic authorization.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client {name | ip-address} [key [0 | 7] word] [vrf vrf-id]**
5. **port port-number**
6. **server-key [0 | 7] word**
7. **auth-type {all | any | session-key}**
8. **ignore {server-key | session-key}**
9. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa server radius dynamic-author</b>  <b>Example:</b> Router(config)# aaa server radius dynamic-author	Configures the ISG as a AAA server.
Step 4	<b>client {name   ip-address} [key [0   7] word] [vrf vrf-id]</b>  <b>Example:</b> Router(config-locsvr-da-radius)#	Specifies a client with which ISG will be communicating.
Step 5	<b>port port-number</b>  <b>Example:</b> Router(config-locsvr-da-radius)# port 1600	Specifies the RADIUS server port. <ul style="list-style-type: none"><li>Default is 1700.</li></ul>
Step 6	<b>server-key [0   7] word</b>  <b>Example:</b> Router(config-locsvr-da-radius)# server-key cisco	Specifies the encryption key shared with the RADIUS client.
Step 7	<b>auth-type {all   any   session-key}</b>  <b>Example:</b> Router(config-locsvr-da-radius)# auth-type all	Specifies the attributes to be used for session authorization.
Step 8	<b>ignore {server-key   session-key}</b>  <b>Example:</b> Router(config-locsvr-da-radius)# ignore session-key	Configures ISG to ignore the shared encryption key or attribute 151.
Step 9	<b>end</b>  <b>Example:</b> Router(config)# end	Exits global configuration mode.

# Configuration Examples for ISG Interaction with External Policy Servers

This section contains the following example:

- [ISG Interaction with External Policy Servers: Example, page 6](#)

## ISG Interaction with External Policy Servers: Example

The following example configures ISG to interact with external policy servers:

```
!
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
!
aaa server radius dynamic-author
 client 10.76.86.90 key cisco
 client 172.19.192.25 vrf VRF1 key cisco
 client 172.19.192.25 vrf VRF2 key cisco
 client 172.19.192.25 key cisco
 message-authenticator ignore
```

## Additional References

The following sections provide references related to ISG interaction with external policy servers.

## Related Documents

Related Topic	Document Title
ISG commands	<a href="#">Cisco IOS Intelligent Services Gateway Command Reference</a>
AAA configuration tasks	Part 1, “Authentication, Authorization, and Accounting (AAA),” <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
AAA commands	Part 1, “Authentication, Authorization, and Accounting (AAA),” <i>Cisco IOS Security Command Reference</i> , Release 12.2

## Standards

Standard	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
None	—

## Technical Assistance

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

# Feature Information for ISG Interaction with External Policy Servers

[Table 1](#) lists the release history for this feature.

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

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



### Note

[Table 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 ISG Interaction with External Policy Servers

Feature Name	Releases	Feature Information
ISG: Policy Control: Policy Server: CoA	12.2(28)SB 12.2(33)SRC 12.4(20)T	<p>This feature provides ISG support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Initial and Dynamic Authorization, page 2</a></li> <li>• <a href="#">How to Enable ISG to Interact with External Policy Servers, page 2</a></li> </ul> <p>In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.</p> <p>In Cisco IOS Release 12.4(20)T, this feature was integrated into the T train.</p>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0903R)

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.