Configuring ISG Policies for Automatic Subscriber Logon

Last Updated: August 21, 2011

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 module contains information on how to configure ISG to use specified identifiers in place of the username in authorization requests, enabling a user profile to be downloaded from an authentication, authorization, and accounting (AAA) server as soon as packets are received from a subscriber.

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 Table at the end of this document.

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

Prerequisites for ISG Automatic Subscriber Logon

Depending on your AAA implementation, you may need to configure one of the following identifiers in the password field of the user profile: source IP address, MAC address, remote ID, circuit ID. You may also need to configure a global address in the password field.

To use circuit ID and remote ID for authorization for IP sessions, the DSLAM must insert the circuit ID and remote ID in the DHCP Option 82 information.

To use remote ID for authorization of PPPoE sessions, the PPPoE client must provide the remote ID information in the PPPoE Tag ID or line ID.

Restrictions for ISG Automatic Subscriber Logon

The username field in an authorization request has a limit of 253 characters.

Automatic subscriber logon based on traffic class cannot be configured on the Cisco 7600 router.

Information About ISG Automatic Subscriber Logon

Overview of ISG Automatic Subscriber Logon

Service providers commonly implement a policy at the start of IP sessions that redirects all subscriber packets to a logon portal for authentication. Following successful authentication, per-subscriber authorization data is typically returned from a AAA server. For some deployments, usually in subscriber networks that are well protected against spoofing and denial-of-service (DoS) attacks, service providers are willing to forgo authentication and trust subscriber identity. ISG automatic subscriber logon allows service providers to grant certain subscribers access to services without requiring the subscribers to log on.

ISG automatic subscriber logon enables a specified identifier to be used in place of the username in authorization requests. Enabling the AAA server to authorize subscribers on the basis of a specified identifier allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

The event that triggers automatic subscriber logon is session-start. For IP sessions, session-start occurs when a DHCP DISCOVER request is received or when an unrecognized source IP address is detected. For PPPoE sessions, session-start occurs when a client attempts to initiate a session by sending a PPPoE Active Discovery Initiation (PADI) packet.

Supported Identifiers for ISG Automatic Subscriber Logon

For IP sessions, an ISG device can be configured to use the following identifiers in place of the username in authorization requests: IP address, MAC address, circuit ID, remote ID, or a combination of the circuit ID and remote ID.

For PPPoE sessions, an ISG device can be configured to use the remote ID in place of the username in authorization requests.

Authorization Based on Circuit ID and Remote ID

The circuit ID and remote ID fields are part of the DHCP relay agent information option (also referred to as Option 82) and the PPPoE Tag VSA. These fields are inserted into DHCP and PPPoE messages by a DSLAM. An ISG device can be configured to use the circuit ID, remote ID, or a combination of circuit ID and remote ID as the username in authorization requests.

By default, the ISG device will use the circuit ID and remote ID that are provided by the Layer 2 edge access device for authorization. If the **ip dhcp relay information option** command is configured, the ISG device will use the circuit ID and remote ID that are received in a DHCP message.

Accounting Behavior When ISG Automatic Subscriber Logon Is Configured

Accounting Behavior for MAC-Address-Based Authorization

If the MAC address is sent as the username in authorization requests, the MAC address will also be sent as the Calling Station ID in accounting records.

Accounting Behavior for Remote-ID- and Circuit-ID-Based Authorization

For IP sessions that use DHCP Option 82 authorization, accounting messages are sent to the AAA server with the Circuit ID and Remote ID Cisco VSAs. Although you can configure a combination of circuit ID and remote ID as the username for authorization, the attributes are sent individually in accounting records. You can also configure the circuit ID and remote ID to be sent together in accounting records as the NAS Port ID.

For PPPoE sessions, the Remote ID VSA is sent in accounting records, and the remote ID is also sent as the NAS Port ID.

If the **radius-server attribute 31 remote-id** command is configured, the remote ID is sent in accounting records as the Calling Station ID.

How to Configure ISG Policies for Automatic Subscriber Logon

Identifying Traffic for Automatic Logon in a Control Policy Class Map

Perform this task to configure a control policy class map that specifies the traffic to which ISG automatic subscriber logon will apply.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control match-all** *class-map-name*
4. Do one of the following:
   - **match source-ip-address** *ip-address subnet-mask*
   -
   - **match nas-port circuit-id** *name*
   -
   - **match nas-port remote-id** *name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type control match-all** *class-map-name* **Example:** `Router(config)# class-map type control match-all TAL-subscribers`	Creates a control class map, which defines the conditions under which the actions of a control policy map will be executed.

Command or Action	Purpose

Step 4 Do one of the following:
• **match source-ip-address** *ip-address subnet-mask*
•
• **match nas-port circuit-id** *name*
•
• **match nas-port remote-id** *name*
 	
Example:
`Router(config-control-classmap)# match source-ip-address 10.1.1.0 255.255.255.0`
 	
Example:
 	
Example:
`Router(config-control-classmap)# match nas-port circuit-id circuit1`
 	
Example:
 	
Example:
`Router(config-control-classmap)# match nas-port remote-id remote1`
	Creates a condition that will evaluate true if a subscriber's source IP address matches the specified IP address.
	or
	Creates a condition that will evaluate true if a subscriber's circuit ID matches the specified value.
	or
	Creates a condition that will evaluate true if a subscriber's remote ID matches the specified value.

Step 5 **end** **Example:** `Router(config-control-classmap)# end`	(Optional) Returns to privileged EXEC mode.

Configuring an ISG Control Policy for Automatic Subscriber Logon

Perform this task to configure an ISG control policy that initiates subscriber authorization and inserts a specified identifier into the username field of the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Creates or modifies a control policy map, which is used to define a control policy.
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Specifies a control class, which defines the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the task "Identifying Traffic for Automatic Logon in a Control Policy Class Map".

	Command or Action	Purpose
Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address`	Inserts the specified identifier into the username field of authorization requests.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- What to Do Next, page 7

What to Do Next

You must apply the control policy to a context by using the **service-policy type control** command. For information about applying control policies, see the module "Configuring ISG Control Policies".

You may want to configure policies to determine what should happen for autologon subscribers whose IP address or MAC address authorization fails; for example, you may want to redirect the subscriber to the policy server for authentication.

Enabling the Remote-ID to Be Sent as the Calling-Station-ID

Perform this task to enable the ISG device to send the remote ID in the Calling-Station-ID (attribute 31) field of accounting records and access requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 31 remote-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 31 remote-id** **Example:** `Router#(config) radius-server attribute 31 remote-id`	Enables the ISG device to send the remote ID in the Calling Station ID (attribute 31) field of accounting records and access requests.

Verifying ISG Automatic Subscriber Logon

Perform this task to determine whether or not automatic subscriber logon was successful.

SUMMARY STEPS

1. **enable**
2. **show subscriber session**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Step 2 **show subscriber session**
Use the **show subscriber session** command to display information about ISG subscriber sessions. If the output shows that a session was brought up in the state “authen”, automatic subscriber authorization was successful. If automatic subscriber authorization was not successful, the session will still be brought up, but in the state “unauthen”.

The following sample output shows information for a session for which automatic subscriber authorization was successful:

Example:

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 1
------------------------------------------------
```

```
Unique Session ID: 3
Identifier: aabb.cc01.3000
```

SIP subscriber access type(s): IP

Example:

```
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:24, Last Changed: 00:00:21

Policy information:
  Authentication status: authen
  Rules, actions and conditions executed:
    subscriber rule-map DEFAULT
      condition always event session-start
        1 authorize identifier mac-address

Session inbound features:
 Feature: IP Idle Timeout
  Timeout value is 600
  Idle time is 00:00:21
Configuration sources associated with this session:
```

Interface: Ethernet0/0, Active Time = 00:00:24

Configuration Examples for ISG Automatic Subscriber Logon

Automatic Subscriber Logon Based on IP Address Example

In the following example, if the client is from the 1.1.1.0 subnet, the ISG sends an authorization request to the list “TAL_LIST” with the subscriber’s source IP address as the username. If the authorization request is successful, any automatic-activation services specified in the returned user profile are activated for the session, and the execution of rules within the control policy stops. If the authorization is not successful, the rule execution proceeds, and the subscriber is redirected to the policy server to log in. If the subscriber does not log in within five minutes, the session is disconnected.

ISG Configuration

```
interface Ethernet0/0
 service-policy type control RULEA
aaa authorization network TAL_LIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any
class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100
policy-map type service redirectprofile
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080
class-map type control match-all CONDA
 match source-ip-address 10.1.1.0 255.255.255.0
!
class-map type control match-all CONDF
```

```
 match timer TIMERB
 match authen-status unauthenticated
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 service-policy type service aaa list LOCAL name redirectprofile
  3 set-timer TIMERB 5 minutes
!
 class type control CONDF event timed-policy-expiry
  1 service disconnect
```

User Profile Configuration

```
1.1.1.1 Password = "cisco"
 Service-Type = Outbound,
 Cisco:Account-Info = "AAuto-Internet;proxy-user;cisco"
```

Service Profile Configuration

```
Auto-Internet Password = "cisco"
 Cisco:Service-Info = "IAuto-Internet",
 Cisco-Avpair = "traffic-class=input access-group 100"
proxy-user Password = "cisco"
```

Idle-Timeout = 5

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Automatic Subscriber Logon

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 Feature Information for ISG Automatic Subscriber Logon

Feature Name	Releases	Feature Configuration Information
ISG: Session: Authentication (MAC, IP)	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG automatic subscriber logon enables an IP address or MAC address to be used in place of the username in authorization requests. This functionality allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers. This module provides information about this feature. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.
ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support	12.2(28)SB 12.2(33)SRC 15.0(1)S	This feature enhances ISG automatic subscriber logon by providing support for authorization on the basis of the circuit-id and remote-id. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.