

Walk-By User Support in ISG

The Walk-By User Support in ISG feature enables the Cisco Intelligent Services Gateway (ISG) to handle unauthenticated sessions from neighboring devices that do not intend to use the ISG service. These sessions, called walk-by sessions or lite sessions, may be triggered by various initiators.

With the implementation of this feature, unauthenticated users are assigned lite sessions based on the default session. These lite sessions optimize resource usage because they enable the walk-by user to use only session start services mentioned in the default policy configured for the default session.

This module describes how to create and apply a default policy for default sessions to enable the Walk-By User Support in ISG feature.

- Prerequisites for Walk-By User Support for PWLANs in ISG, on page 1
- Restrictions for Walk-By User Support for PWLANs in ISG, on page 1
- Information About Walk-By User Support for PWLANs in ISG, on page 2
- How to Configure Walk-By User Support for PWLANs in ISG, on page 3
- Configuration Examples for Walk-By User Support for PWLANs in ISG, on page 7
- Additional References, on page 8
- Feature Information for Walk-By User Support for PWLANs in ISG, on page 8

Prerequisites for Walk-By User Support for PWLANs in ISG

Your implementation of the Cisco software image must support authentication, authorization, and accounting (AAA) and Intelligent Services Gateway (ISG).

Restrictions for Walk-By User Support for PWLANs in ISG

- IPv6 sessions are not supported.
- Only Layer 4 Redirect (L4R), Port-Bundle Host Key (PBHK), and service virtual routing and forwarding (VRF) features are supported. The L4R feature for walk-by session supports only 16 translation entries.
- Lite sessions do not support prepaid, accounting, quality of service (QoS), timers, or RADIUS-timeout features.

Information About Walk-By User Support for PWLANs in ISG

Default Sessions

A default session is a template session that is used as a reference by lite sessions created for walk-by subscribers on a given interface. When an edge device connects to an open service set ID (SSID) in a public wireless LAN (PWLAN) environment a lite session is created on the Intelligent Services Gateway (ISG). Each lite session applies the session start services defined in the default policy configured for the default session. Only one default session can be configured on each device interface. The default policy defines the default session start services and features to be used as a template for the lite session.

Lite Sessions or Walk-By Sessions

In most public wireless LAN (PWLAN) setups, a high percentage of Intelligent Services Gateway (ISG) sessions are unauthenticated sessions from wireless devices that do not use the PWLAN service. These sessions are called walk-by sessions or lite sessions, and users that use these sessions are called walk-by users. Walk-by sessions consume a significant amount of CPU, memory and other physical resources of the ISG router. This resource utilization may lead to an increase in the number of ISG devices that are required for a given PWLAN deployment.

A lite session inherits the session start services applied for the default session. Lite sessions are created on ISG to support walk-by users and optimize resource usage. Each lite session is associated with an individual timer that specifies the duration for which the session can utilize PWLAN services while remaining unauthenticated. If these lite sessions remain unauthenticated even after the timer expires, these sessions are deleted from ISG.

Lite sessions are also created when dedicated sessions fail authentication.

Dedicated Sessions

A dedicated or regular session is a full-fledged Intelligent Services Gateway (ISG) subscriber session. All subscriber sessions that are authenticated cause the creation of dedicated sessions on ISG. The policy manager of ISG decides whether to create a complete session context (a dedicated session) or a minimal session context (a lite session).



Note ISG provides high availability support for converted (lite to dedicated) unclassified and DHCPv4 sessions.

Supported Triggers

Walk-by sessions can be created through any of the following session initiators:

- Packet trigger: Here the session creation is triggered by a subscriber's IP packet having an unclassified IP address or MAC address.
- RADIUS proxy: This trigger is commonly used in PWLAN deployments where ISG acts as a RADIUS proxy. Here, the session creation is triggered by the subscriber's RADIUS packets.

- DHCP: This trigger is another SIP used in a few PWLAN deployments. Here, the session creation is triggered by the subscriber's DHCP control packets.
- EoGRE walkby: When ISG is configured for EoGRE, DHCP control packets and unclassified MAC packets on the EoGRE interface trigger session creation on ISG.

Session Limit

The total number of sessions supported on ISG is 128,000. Currently, ISG can support 128,000 lite sessions and 64,000 converted sessions. ISG can also now support 64,000 tunnel endpoints.

How to Configure Walk-By User Support for PWLANs in ISG

Creating and Enabling a Default Policy for a Default Session

Perform this task to create and enable a default policy for a default session on an interface. Each interface can have only one default policy.

A default session is set up to optimize the creation of Intelligent Services Gateway (ISG) sessions for walk-by users. The default session serves as a template that is used by lite sessions for walk-by users. The default policy contains session start services only to which all lite sessions refer. A default policy has the following two functions:

- Identify users who qualify for lite session optimization.
- Identify services or features that need to be applied on default sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **service local**
5. **ip portbundle**
6. **exit**
7. **class-map type traffic match-any** *class-map-name*
8. **match access-group** {**input** | **output**} {*access-list-number* | **name** *access-list-name*}
9. **exit**
10. **policy-map type service** *policy-map-name*
11. [*priority*] **class type traffic** {*class-map-name* | **default** {**in-out** | **input** | **output**}}
12. **redirect to group** {*server-group-name* | **ip** *server-ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]]
13. **exit**
14. **exit**
15. **policy-map type control** *policy-map-name*
16. **class type control** {*control-class-name* | **always**} [**event session-start**]
17. *action-number* **service-policy type service name** *policy-map-name*

18. *action-number* **service-policy type service name** *policy-map-name*
19. *action-number* **set-timer** *name-of-timer minutes*
20. **exit**
21. **exit**
22. **interface** *type number*
23. **service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]}
24. **service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]}
25. **end**
26. **show running-config interface** *type number*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service PBHK`	Configures a service policy map, and enters service policy-map configuration mode.
Step 4	**service local** **Example:** `Device(config-service-policymap)# service local`	Specifies the local termination service in the ISG service policy map.
Step 5	**ip portbundle** **Example:** `Device(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key (PBHK) feature for the service.
Step 6	**exit** **Example:** `Device(config-service-policymap)# exit`	Returns to global configuration mode.
Step 7	**class-map type traffic match-any** *class-map-name* **Example:** `Device(config)# class-map type traffic match-any ALLTRAFFIC`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class, and enters traffic class-map configuration mode.

	Command or Action	Purpose
Step 8	**match access-group** {**input** | **output**} {*access-list-number* | **name** *access-list-name*} **Example:** `Device(config-traffic-classmap)# match access-group input 100`	Configures the match criteria for an ISG traffic class map on the basis of the specified access control list (ACL).
Step 9	**exit** **Example:** `Device(config-traffic-classmap)# exit`	Exits traffic class-map configuration mode.
Step 10	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service L4R`	Configures another service policy map, and enters service policy-map configuration mode.
Step 11	[*priority*] **class type traffic** {*class-map-name* | **default** {**in-out** | **input** | **output**}} **Example:** `Device(config-service-policymap)# class type traffic ALLTRAFFIC`	Associates a previously configured ISG traffic class map with a service policy map, and enters service policy-map traffic class configuration mode.
Step 12	**redirect to group** {*server-group-name* | **ip** *server-ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]] **Example:** `Device(config-service-policymap-class-traffic)# redirect to group PORTAL`	Redirects ISG Layer 4 traffic to a specified server or server group.
Step 13	**exit** **Example:** `Device(config-service-policymap-class-traffic)# exit`	Returns to service policy-map configuration mode.
Step 14	**exit** **Example:** `Device(config-service-policymap)# exit`	Returns to global configuration mode.
Step 15	**policy-map type control** *policy-map-name* **Example:** `Device(config)# policy-map type control DefRULE`	Creates or modifies a default control policy map, which is used to define a control policy, and enters control policy-map configuration mode.
Step 16	**class type control** {*control-class-name* | **always**} [**event session-start**] **Example:** `Device(config-control-policymap)# class type control always event session-start`	Specifies a control class for which actions are configured and enters control policy-map class configuration mode.

	Command or Action	Purpose
Step 17	*action-number* **service-policy type service name** *policy-map-name* **Example:** `Device(config-control-policymap-class-control)# 10 service-policy type service name PBHK`	Activates the specified ISG service.
Step 18	*action-number* **service-policy type service name** *policy-map-name* **Example:** `Device(config-control-policymap-class-control)# 20 service-policy type service name L4R`	(Optional) Activates another specified ISG service.
Step 19	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Device(config-control-policymap-class-control)# 30 set-timer UNAUTH 1`	Starts a named policy timer. • Expiration of the timer initiates the timed-policy-expiry event.
Step 20	**exit** **Example:** `Device(config-control-policymap-class-control)# exit`	Returns to control policy-map configuration mode.
Step 21	**exit** **Example:** `Device(config-control-policymap)# exit`	Returns to global configuration mode.
Step 22	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/4`	Specifies an interface and enters interface configuration mode.
Step 23	**service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]} **Example:** `Device(config-if)# service-policy type control default DefRULE`	Applies a default control policy on the interface.
Step 24	**service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]} **Example:** `Device(config-if)# service-policy type control RegRULE`	Applies a regular control policy on the interface.
Step 25	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 26	**show running-config interface** *type number* **Example:** `Device# show running-config interface GigabitEthernet 0/0/4`	(Optional) Displays the running configuration for a specific interface.

Configuration Examples for Walk-By User Support for PWLANs in ISG

Example: Creating and Enabling a Default Policy for a Default Session

The following example shows how to create and enable a default policy named DefRULE on the Gigabit Ethernet interface:

```
Device> enable
Device# configure terminal
Device(config)# policy-map type service PBHK
Device(config-service-policymap)# service local
Device(config-service-policymap)# ip portbundle
Device(config-service-policymap)# exit
Device(config)# class-map type traffic match-any ALLTRAFFIC
Device(config-traffic-classmap)# match access-group input 100
Device(config-traffic-classmap)# exit
Device(config)# policy-map type service L4R
Device(config-service-policymap)# class type traffic ALLTRAFFIC
Device(config-service-policymap-class-traffic)# redirect to group PORTAL
Device(config-service-policymap-class-traffic)# exit
Device(config-service-policymap)# exit
Device(config)# policy-map type control DefRULE
Device(config-control-policymap)# class type control always event session-start
Device(config-control-policymap-class-control)# 10 service-policy type service name PBHK
Device(config-control-policymap-class-control)# 20 service-policy type service name L4R
Device(config-control-policymap-class-control)# 30 set-timer UNAUTH 1
Device(config-control-policymap-class-control)# exit
Device(config-control-policymap)# exit
Device(config)# interface GigabitEthernet 0/0/4
Device(config-if)# service-policy type control default DefRULE
Device(config-if)# service-policy type control RegRULE
Device(config-if)# end
```

The following sample output from the **show running-config interface** command displays the policies configured on the Gigabit Ethernet interface. The default policy configured for default sessions on the Gigabit Ethernet interface is DefRULE, and the regular policy configured for dedicated sessions on the Gigabit Ethernet interface is RegRULE.

```
Device# show running-config interface GigabitEthernet 0/0/4

Building configuration...

Current configuration : 318 bytes
!
interface GigabitEthernet0/0/4
ip address 192.0.2.1 255.255.255.0
```

```
negotiation auto
service-policy type control default DefRULE
service-policy type control RegRULE
ip subscriber routed
  initiator unclassified ip-address
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Walk-By User Support for PWLANs in ISG

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 Walk-By User Support for PWLANs in ISG

Feature Name	Releases	Feature Information
Walk-By User Support for PWLANs in ISG	Cisco IOS XE Release 3.7S	The Walk-By User Support for PWLANs in ISG feature enables the Intelligent Services Gateway (ISG) that is configured as a RADIUS proxy to handle unauthenticated sessions from wireless devices that do not use the public wireless LAN (PWLAN) service. These sessions are called walk-by sessions. With the implementation of this feature, unauthenticated users are assigned lite sessions based on the default session. These lite sessions optimize resource usage because they enable the walk-by user to use only session start services mentioned in the default policy configured for the default session. The following commands were introduced or modified: **clear subscriber lite-session**, **clear subscriber session**, **debug subscriber lite-session errors**, **debug subscriber lite-session events**, **service-policy type control**, **show subscriber default-session**, and **show subscriber statistics**.
Walkby session support on EoGRE interface	Cisco IOS XE Release 3.13.1S	This feature enables the Intelligent Services Gateway (ISG) to support walk-by sessions over EoGRE interfaces
HA support for converted (lite to dedicated) sessions	Cisco IOS XE Release 3.13.1S	This feature enables the Intelligent Services Gateway (ISG) to support high availability for converted (lite to dedicated) sessions.