



ACS Trigger Condition Configuration Mode Commands

The ACS Trigger Condition Configuration Mode is used to configure Active Charging Service (ACS) trigger conditions.

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-trig-condn) #
```



Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- [any-match](#), on page 1
- [content-type](#), on page 2
- [committed-data-rate](#), on page 3
- [delay](#), on page 4
- [end](#), on page 5
- [exit](#), on page 6
- [flow-length](#), on page 6
- [local-policy-rule](#), on page 6
- [multi-line-or](#), on page 8
- [rule-name](#), on page 8
- [tdf-app-id](#), on page 9
- [tethered-flow](#), on page 10

any-match

This command will be applied to analyze all flows created after event activation.

Product

ACS

Privilege	Security Administrator, Administrator
Command Modes	Exec > ACS Configuration > ACS Trigger Condition Configuration active-charging service <i>service_name</i> > trigger-condition <i>trigger_condn_name</i> Entering the above command sequence results in the following prompt: <pre>[local]host_name(config-acs-trig-condn) #</pre>
Syntax Description	[no] any-match <i>operator condition</i> no If previously configured, deletes the specified configuration. operator Specifies how to match. <i>operator</i> must be one of the following: <ul style="list-style-type: none"> • !=: Does not equal • =: Equals condition Specifies the condition to match. <i>condition</i> must be one of the following: <ul style="list-style-type: none"> • FALSE • TRUE
Usage Guidelines	Use this command to analyze all flows created after event activation.
	Example The following command defines any-match rule to analyze all flows: any-match = TRUE

content-type

This command specifies the content-type.

Product	ACS
Privilege	Security Administrator, Administrator
Command Modes	Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

Syntax Description

content-type *operator condition*

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- =: Equals
- !contains: does not contain
- !ends-with: does not end with
- !starts-with: does not start with
- case-sensitive: strings are matched in case sensitive manner
- contains: contains
- ends-with: ends with
- starts-with: starts with

condition

Specifies the condition to match.

condition must be one of the following:

- FALSE
- TRUE

Usage Guidelines

Use this command to analyze all flows created after event activation.

Example

The following command defines content-type to be matched:

```
content-type = TRUE
```

committed-data-rate

This command configures the committed data rate of the current negotiated value.

Product

ACS

Privilege	Security Administrator, Administrator
Command Modes	Exec > ACS Configuration > ACS Trigger Condition Configuration active-charging service <i>service_name</i> > trigger-condition <i>trigger_condn_name</i> Entering the above command sequence results in the following prompt: <pre>[local]host_name(config-acs-trig-condn)#</pre>
Syntax Description	<pre>[no] committed-data-rate { lower_threshold <value_in_percentage> upper_threshold <value_in_percentage> }</pre> <p>no Disables the committed data rate of the current negotiated value.</p> <p>committed-data-rate Specifies the committed data rate of the current negotiated value.</p> <p>lower_threshold Configures threshold as a percentage of the current negotiated value.</p> <p>upper_threshold Configures threshold as a percentage of the current negotiated value.</p> <p>value_in_percentage Specifies the percentage of initial configured committed-data-rate value. This is an integer value of 0 through 100.</p>
Usage Guidelines	<p>Use the committed-data-rate command to configure the upper-threshold or lower-threshold of the committed data rate of the current negotiated value.</p> <p>For more information on this feature, see the <i>ECS Administration Guide</i>.</p> <p>Example</p> <p>The following command defines the upper-threshold of committed-data-rate value:</p> <pre>committed-data-rate upper-threshold 80</pre>

delay

This command allows you to specify the delay for the configured time in seconds.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

Syntax Description

delay = *delay_time*
no delay

no

Use the **no delay** command to checkpoint all eligible rules immediately without any delay.

delay_time

Specifies the delay time in seconds and must be an integer from 1 through 600.

Default: 0 (immediate checkpointing)

Usage Guidelines

Use this command to specify the delay after which the flows can be checkpointed. This CLI command is introduced in support of the Flow Recovery feature. If the "delay" CLI command is not configured under trigger-condition, any flow for the rule will be checkpointed immediately on flow creation.

When configured in conjunction with the flow-recovery trigger, the flows for the rule(s) will be checkpointed as per session level and call level limit after the delay timer is expired.

**Important**

Flow Recovery is a licensed Cisco feature requiring a separate feature license. Contact your Cisco account representative for more information.

For more information on this feature, see the *ECS Administration Guide*.

Example

The following command specifies a delay of **40** seconds after which the flows can be checkpointed:

```
delay = 40
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.

flow-length

This command specifies the flow length condition for a TCP flow.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

Syntax Description

flow-length threshold exceed
no delay

no

Disables flow recovery for a trigger-action.

threshold

Specifies the threshold value configured in the trigger-action configuration.

exceed


Invokes the exceed condition when the flow length is exceeded.

Usage Guidelines

Use this command to specify the trigger condition **exceed** for a given threshold value.

local-policy-rule

This command allows you to specify the local-policy rule within ECS for enabling trigger condition.

Product	GGSN P-GW
Privilege	Security Administrator, Administrator
Command Modes	Exec > ACS Configuration > ACS Trigger Condition Configuration active-charging service <i>service_name</i> > trigger-condition <i>trigger_condn_name</i> Entering the above command sequence results in the following prompt: <pre>[local]host_name(config-acs-trig-condn)#</pre>
Syntax Description	[no] local-policy-rule = local_policy_rule no If previously configured, deletes the specified configuration. local-policy-rule This keyword allows operators to suppress the throttling when the subscriber is in a particular LAC or TAC location and hits the specified local-policy rule. The local-policy-rule contains either a list, range, or index of LAC and/or TAC entries. local_policy_rule Specifies the local-policy rule name. <i>local_policy_rule</i> must be an existing local-policy rule within the service scheme expressed as an alphanumeric string of 1 through 63 characters.
Usage Guidelines	Use this command to specify the local-policy rule within ECS for enabling trigger condition. This CLI command is introduced in support of the Location based QoS Override feature. To enable this feature for the subscriber, both local-policy and service-scheme framework must be configured. For redundancy support, the corresponding ICSR configuration must also be present. The service-scheme framework helps in overriding feature behavior specific to a subscriber or a set of subscribers. The user can update the policies specific to subscribers based on pre-configured events. For more information on the service-scheme framework, see the <i>ECS Administration Guide</i> .
 Important	This feature requires the license to configure local-policy. For more information on the licensing requirements, contact Cisco account representative. Local-policy provides ECS, the list of rules to activate and the list of rules to delete. In case, the rule to be activated is already installed, ECS ignores this rule. Similarly if the rule to be deleted was not installed, ECS ignores this rule as well. The trigger action will be applied only to a subset of traffic that matches the criteria defined under trigger condition. For more information on this feature, see the <i>ECS Administration Guide</i> .
Example	The following command defines the local-policy rule as zone1.

```
local-policy-rule = zone1
```

multi-line-or

This command allows to check if the OR operator must be applied to all lines in a trigger-condition.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

Syntax Description

[**no**] **multi-line-or** **all-lines**

no

If previously configured, deletes the specified configuration.

Usage Guidelines

Use this command to check if the OR operator must be applied to all lines in a trigger-condition.

rule-name

This command allows you to define a particular rule/GoR for flow checkpoint.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

Syntax Description

[**no**] **rule-name** *operator rule_name*

no

Use the **no rule-name** command to remove the particular rule from the list of eligible rules for flow checkpoint. For wildcard-based rule definition, this command must contain the rule name in the same format.

operator

Specifies how to match.

operator must be one of the following:

- =: Equals
- !=: Not Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

These operators cannot be used with dynamic rule names. For dynamic rules, the entire rule name must be mentioned with the "=" operator.

rule_name

Specifies the rule name and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to define the a particular rule/GoR for flow checkpoint. This CLI command is introduced in support of the Flow Recovery feature. To have more rules eligible for flow checkpoint, a user can configure multiple trigger condition(s) associated with the same trigger-action. In any defined trigger-condition, a user can configure upto a maximum of 15 entries.

When configured in conjunction with flow-recovery trigger, the flows for the rule(s) will be checkpointed as per session level and call level limit after the delay timer is expired.



Important

Flow Recovery is a licensed Cisco feature requiring a separate feature license. Contact your Cisco account representative for more information.

For more information on this feature, see the *ECS Administration Guide*.

Example

The following command defines a rule to match the **rule01** rule name for flow checkpoint:

```
rule-name = rule01
```

tdf-app-id

This command specifies the content-type.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

```
active-charging service service_name > trigger-condition trigger_condn_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn) #
```

Syntax Description

tdf-app-id*operator condition*

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- =: Equals
- !contains: does not contain
- !ends-with: does not end with
- !starts-with: does not start with
- case-sensitive: strings are matched in case sensitive manner
- contains: contains
- ends-with: ends with
- starts-with: starts with

condition

Specifies the condition to match.

condition must be one of the following:

- FALSE
- TRUE

Usage Guidelines

Use this command to analyze all flows created after event activation.

Example

The following command defines tdf-app-id value to be matched:

```
tdf-app-id = TRUE
```

tethered-flow

This command configures the tethered traffic flow.

Product

ACS
P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service *service_name* > **trigger-condition** *trigger_condn_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

Syntax Description

[no] **tethered-flow**

no

Disables the tethered traffic flow.

tethered-flow

Specifies the tethered traffic.

Usage Guidelines

Use this command to configure the tethered traffic.

For more information on this feature, see the *P-GW Administration Guide*.

tethered-flow