

ACL Configuration Mode Commands

ACL configuration mode allows you to configure an Access Control List (ACL) on the CSS.

To access ACL mode, use the **acl** command from any configuration mode, except boot, and RMON alarm, event, and history modes. The prompt changes to (config-acl [*index*]). You can use this command from ACL mode to access another ACL. For information about commands available in this mode, refer to the following commands.

Use the **no** form of this command to delete an ACL.

acl *index*
no acl *index*

Syntax Description

index

The number you want to assign to a new ACL or the number for an existing ACL. Enter a number from 1 to 99.

(config-acl) apply

To assign an ACL to an individual circuit, all circuits without ACLs, or DNS queries, use the **apply** command.

```
apply [all|circuit-(circuit_name)|dns]
```

Syntax Description

all	Applies this ACL to all existing circuits without ACLs or reapply the ACL to circuits that currently have the same ACL applied. If a circuit has a different ACL applied, this option bypasses the circuit.
circuit- (<i>circuit_name</i>)	Applies this ACL to an individual circuit.
<i>circuit_name</i>	The name of the circuit. To see a list of existing circuits, enter: <code>apply ?</code>
dns	Adds this ACL to DNS queries.

Usage Guidelines

To add a new clause to an existing and applied ACL, reapply the ACL to the circuit with the **apply circuit** command.

To apply any changes to an existing clause on an existing and applied ACL, you must remove the ACL from the circuit with the **(config-acl) remove** command, and then reapply the ACL to the circuit.

To remove a clause currently in use, you must remove its applied ACL from the circuit, delete the clause, and then reapply the ACL to the circuit.



Note

You cannot apply an ACL that has no clauses.

Related Commands

(config-acl) remove

(config-acl) clause

To enter clauses in a specific ACL to control incoming traffic on a circuit and to control logging on the clause, use the **clause** command. Use the **no** form of this command to delete a clause.

```
clause number [log [enable|disable]][bypass|deny|permit] protocol
    [source_info {source_port}] dest{inaction} [dest_info {dest_port}]
    {sourcegroup name} {prefer service_name}}
no clause number
```

Syntax	Description
log disable	Disables ACL logging.
log enable	Enables ACL logging.
bypass	Sends traffic directly to its destination, bypassing the content rule. The bypass option bypasses traffic only on a content rule, thus does not cause NATing to occur. Do not use the bypass option in an ACL clause with a source group. Since this option does not bypass traffic that does not match a rule, it does not effect NATing on a source group in an ACL clause.
deny	Denies traffic on a circuit.
permit	Permits traffic on a circuit.
<i>number</i>	The number you want to assign to the clause. Enter a number from 1 to 254.
<i>protocol</i>	The protocol for the type of traffic. Enter TCP , UDP , ICMP , IGP , IGMP , OSPF , any for any protocol, or the number associated with the protocol.

source_info

- The source of the traffic. Enter one of the following: **any** for any combination of source IP address and host name information.
- *host_name* for the source host name. Enter a host name in mnemonic host-name format (for example, myhost.mydomain.com).
- *ip_address {mask_ip_address}* for the source IP address and the optional mask IP address. Enter an IP address in dotted decimal notation (for example, 192.168.11.1).
- **nql** *nql* for an existing NQL consisting of a list of IP addresses. Enter the name of the NQL. To see a list of NQLs, enter:

```
show nql
```

source_port

The source port for the traffic. Enter either:

- [**eq**|**lt**|**gt**|**neq**] *number* where:
 - **eq** is equal to the port number.
 - **lt** is less than the port number.
 - **gt** is greater the port number.
 - **neq** is not equal to the port number.
 - *number* is the source port number. Enter a number from 1 to 65535.
- **range** *low high* for a range of port numbers, inclusive. Enter numbers from a range of 1 to 65535. Separate the *low* and *high* number with a space.

If you do not designate a source port, this clause allows traffic from any port number.

dest_info

The destination information for the traffic. Enter one of the following:

- **any** for any combination of destination information.
- **content** *owner_name/rule_name* for an owner's content rule. Separate the owner and rule name with a / character. To see a list of owners and content rules, enter:

```
content ?
```

- *host_name* for the destination host name. Enter a host name in mnemonic host-name format (for example, myhost.mydomain.com).
- *ip_address {mask_ip_address}* for the destination IP address and the optional mask IP address. Enter an IP address in dotted decimal notation (for example, 192.168.11.1).
- **nql** *nql* for an existing NQL consisting of host IP addresses. Enter the name of the NQL. To see a list of NQLs, enter:

```
show nql
```

<i>dest_port</i>	<p>The destination port. Enter one of the following:</p> <ul style="list-style-type: none"> • [eq lt gt neq] <i>number</i> where: <ul style="list-style-type: none"> eq is equal to the port number. lt is less than the port number. gt is greater the port number. neq is not equal to the port number. <p><i>number</i> is the destination port number. Enter a number from 1 to 65535.</p> • range <i>low high</i> for a range of port numbers, inclusive. Enter numbers from a range of 1 to 65535. Separate the <i>low</i> and <i>high</i> number with a space. • <i>destport-enum</i> where you enter one of the following ports: ftp-data, ftp, telnet, smtp, domain, gopher, http, pop, nntp, ntp, bgp, ldap, https <p>If you do not designate a destination port, this clause allows traffic to any port number.</p>
sourcegroup <i>name</i>	<p>Define a source group based on matching this ACL clause. Enter the group name. To see a list of source groups, enter:</p> <pre style="margin-left: 40px;">show group ?</pre>
prefer <i>service_name</i>	<p>Define a preferred service based on matching this ACL clause. Enter the service name. To see a list of services, enter:</p> <pre style="margin-left: 40px;">show service summary</pre> <p>You can define two preferred services. Separate each service with a comma (,).</p>

Usage Guidelines

When implementing an ACL, the number assigned to each clause is very important. The CSS looks at the ACL starting from clause 1 and sequentially progresses through the rest of the clauses. Assign the lowest clause numbers to clauses with the most specific matches. Then, assign higher clause numbers to clauses with less specific matches.

You do not need to enter the clauses sequentially. The CSS automatically inserts the clause in the appropriate order in the ACL. When you can enter clauses 10 and 24, and then clause 15, the CSS inserts the clauses in the right sequence.

**Note**

To add a new clause to an existing and applied ACL, reapply the ACL to the circuit with the **apply circuit** command.

To apply any changes to an existing clause on an existing and applied ACL, you must remove the ACL from the circuit with the **(config-acl) remove** command, and then reapply the ACL to the circuit.

To remove a clause currently in use, you must remove its applied ACL from the circuit, delete the clause, and then reapply the ACL to the circuit.

If you did not enable global ACL logging, the **enable** option does not work. To enable global ACL logging, use the **(config) logging subsystem acl level debug-7** command.

Related Commands

show acl
show running-config acl
(config-acl) apply

(config-acl) no

To negate a command or set it to its default in ACL mode, use the **no** command. Not all commands have a **no** form. For information on general **no** commands you can use in this mode, refer to the general **no** command.

Syntax Description		
	no acl <i>number</i>	Deletes an ACL
	no clause <i>number</i>	Deletes a clause
	no rmon-event <i>index</i>	Deletes an RMON event
	no rmon-history <i>index</i>	Deletes an RMON history

(config-acl) remove

To remove the ACL from an individual circuit, all circuits, or DNS queries, use the **remove** command.

```
remove [all|circuit-(circuit_name)|dns]
```

Syntax Description		
	all	Remove this ACL from all circuits.
	circuit- (<i>circuit_name</i>)	Remove this ACL from the circuit.
	<i>circuit_name</i>	The name of the circuit for the ACL. To get a list of circuits, enter: <code>remove ?</code>
	dns	Remove this ACL from DNS queries.

Related Commands (config-acl) apply

(config-acl) zero counts

To set the content and DNS hit counters in the **show acl** command screen to zero for this ACL, use the **zero counts** command.

zero counts

Related Commands **show acl**