

Extended ACL Configuration Mode Commands

To create and modify extended access lists on a WAAS device for controlling access to interfaces or applications, use the **ip access-list extended** global configuration command. To disable an extended access list, use the **no** form of this command.

```
ip access-list extended {acl-name | acl-num}
```

```
no ip access-list extended {acl-name | acl-num}
```

| | | |
|--------------------|-----------------|--|
| Syntax Description | extended | Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. The (config-ext-nacl) prompt appears: WAE(config-ext-nacl)# |
| | <i>acl-name</i> | Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter. |
| | <i>acl-num</i> | Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For extended access lists, valid values range from 100 to 199. |

Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Within ACL configuration mode, you can use the editing commands (**list**, **delete**, and **move**) to display the current condition entries, to delete a specific entry, or to change the order in which the entries will be evaluated. To return to global configuration mode, enter the **exit** command at the ACL configuration mode prompt.

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device to drop or to accept for further processing. By default, an access list denies everything because the list is terminated by an implicit **deny any** entry. Therefore, you must include at least one **permit** entry to create a valid access list.

**Note**

ACLs that are defined on a router take precedence over the ACLs that are defined on the WAE. ACLs that are defined on a WAE take precedence over the WAAS application definition policies that are defined on the WAE.

After creating an access list, you can include the access list in an access group using the **access-group** command, which determines how the access list is applied. You can also apply the access list to a specific application using the appropriate command. A reference to an access list that does not exist is the equivalent of a **permit any** condition statement.

To create an extended access list, enter the **ip access-list extended** global configuration command. Identify the new or existing access list with a name up to 30 characters long beginning with a letter, or with a number. If you use a number to identify an extended access list, it must be from 100 to 199

**Note**

You must use a standard access list for providing access to the SNMP server or to the TFTP gateway/server. However, you can use either a standard access list or an extended access list for providing access to the WCCP application.

To allow connections from a specific host, use the **permit host source-ip** option and replace *source-ip* with the IP address of the specific host.

To allow connections from a specific network, use the **permit host source-ip wildcard** option. Replace *source-ip* with a network ID or the IP address of any host on the network that you want to specify. Replace *wildcard* with the dotted decimal notation for a mask that is the reverse of a subnet mask, where a 0 indicates a position that must be matched and a 1 indicates a position that does not matter. For instance, the wildcard 0.0.0.255 causes the last eight bits in the source IP address to be ignored. Therefore, the **permit 192.168.1.0 0.0.0.255** entry allows access from any host on the 192.168.1.0 network.

After you identify the extended access list, the CLI enters the extended ACL configuration mode and all subsequent commands apply to the specified access list.

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)#
```

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it but limit host administrative access using SSH:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

The following example shows how to activate the access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group testextacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
```

```
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group testextacl in
 exit
. . .
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands

- clear arp-cache**
- show ip access-list**
- (config-if) ip access-group**
- (config-ext-nacl) deny**
- (config-ext-nacl) delete**
- (config-ext-nacl) list**
- (config-ext-nacl) move**
- (config-ext-nacl) permit**

(config-ext-nacl) delete

To delete a line from the extended ACL, use the **delete** extended ACL configuration command.

delete *line-num*

| | | |
|--------------------|-----------------|---|
| Syntax Description | <i>line-num</i> | Entry at a specific line number in the access list. |
|--------------------|-----------------|---|

| | |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

| | |
|---------------|---------------------------------|
| Command Modes | extended ACL configuration mode |
|---------------|---------------------------------|

| | |
|--------------|--|
| Device Modes | application-accelerator central-manager |
|--------------|--|

| | |
|----------|---|
| Examples | The following example shows how to delete line 10 from the extended ACL testextacl: |
|----------|---|

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# delete 10
```

| | |
|------------------|--|
| Related Commands | (config-ext-nacl) list (config-ext-nacl) move |
|------------------|--|

(config-ext-nacl) deny

To add a line to an extended access list that specifies the type of packets that you want the WAAS device to drop, use the **deny** extended ACL configuration command. To add a condition to the extended ACL, note that the options depend on the chosen protocol.

For IP, use the following syntax to add a condition:

```
[insert line-num] deny {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] |
  host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

```
no deny {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any}
  {dest-ip [wildcard] | host dest-ip | any}
```

For TCP, use the following syntax to add a condition:

```
[insert line-num] deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

```
no deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

For UDP, use the following syntax to add a condition:

```
[insert line-num] deny udp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

```
no deny udp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

For ICMP, use the following syntax to add a condition:

```
[insert line-num] deny icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] |
  host dest-ip | any} [icmp-type [code] | icmp-msg]
```

```
no deny icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
  [icmp-type [code] | icmp-msg]
```

| Syntax | Description |
|------------------------|--|
| insert line-num | (Optional) Specifies to insert the conditions following the specified line number into the access list. |
| gre | Specifies to match packets using the Generic Routing Encapsulation protocol. |
| icmp | Specifies to match ICMP packets. |
| tcp | Specifies to match packets using the TCP protocol. |
| udp | Specifies to match packets using the UDP protocol. |
| ip | Specifies to match all IP packets. |
| <i>proto-num</i> | IP protocol number. |
| <i>source-ip</i> | Source IP address. The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted-decimal format (for example, 0.0.0.0). |

| | |
|------------------------------|---|
| <i>wildcard</i> | (Optional) Wildcard. The notation is in 4-digit, dotted-decimal format. The bits to match are identified by a digital value of 0; the bits to ignore are identified by a 1. For extended IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for a extended IP ACL, then the <i>wildcard</i> parameter is not allowed. |
| host <i>source-ip</i> | Specifies to match the following IP address. |
| any | Specifies to match any IP address. |
| <i>dest-ip</i> | Specifies destination IP address. The number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format (for example, 0.0.0.0). |
| <i>operator port</i> | (Optional) Operator to use with specified ports, where lt = less than, gt = greater than, eq = equal to, neq = not equal to, and range = an inclusive range. The port value is a number (0–65535) or a keyword; two port numbers are required with the range keyword. See the “Usage Guidelines” section for a listing of the UDP and TCP keywords. |
| established | (Optional) Specifies to match TCP packets with the acknowledgment or reset bits set. |
| <i>icmp-type</i> | (Optional) Match with ICMP message type (0–255). |
| <i>code</i> | (Optional) Code type is 0–255. |
| <i>icmp-msg</i> | (Optional) Match a combination of ICMP message type and code types, as expressed by the keywords shown in the “Usage Guidelines” section. |

Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

extended ACL configuration mode

Device Modes

application-accelerator
central-manager

Usage Guidelines

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device to drop or to accept for further processing. By default, an access list denies everything because the list is terminated by an implicit **deny any** entry. You must include at least one **permit** entry to create a valid access list.

To allow connections from a specific host, use the **permit host source-ip** option and replace *source-ip* with the IP address of the specific host.

To allow connections from a specific network, use the **permit host source-ip wildcard** option. Replace *source-ip* with a network ID or the IP address of any host on the network that you want to specify. Replace *wildcard* with the dotted decimal notation for a mask that is the reverse of a subnet mask, where

a 0 indicates a position that must be matched and a 1 indicates a position that does not matter. For instance, the wildcard 0.0.0.255 causes the last eight bits in the source IP address to be ignored. The **permit 192.168.1.0 0.0.0.255** entry allows access from any host on the 192.168.1.0 network.

For extended IP ACLs, the **wildcard** parameter is required if the **host** keyword is not specified.

Use an extended access list to control connections based on the destination IP address or based on the protocol type. You can combine these conditions with information about the source IP address to create more restrictive conditions.

Table 3-1 lists the UDP keywords that you can use with extended access lists.

Table 3-1 UDP Keywords for Extended Access Lists

| CLI UDP Keyword | Description | UDP Port Number |
|-----------------|--|-----------------|
| bootpc | Bootstrap Protocol (BOOTP) client | 68 |
| bootps | Bootstrap Protocol (BOOTP) server | 67 |
| domain | Domain Name System (DNS) | 53 |
| mms | Microsoft Media Server | 1755 |
| netbios-dgm | NetBIOS datagram service | 138 |
| netbios-ns | NetBIOS name service | 137 |
| netbios-ss | NetBIOS session service | 139 |
| nfs | Network File System service | 2049 |
| ntp | Network Time Protocol | 123 |
| snmp | Simple Network Management Protocol | 161 |
| snmptrap | SNMP traps | 162 |
| tacacs | Terminal Access Controller Access Control System | 49 |
| tftp | Trivial File Transfer Protocol | 69 |
| wccp | Web Cache Communication Protocol | 2048 |

Table 3-2 lists the TCP keywords that you can use with extended access lists.

Table 3-2 TCP Keywords for Extended Access Lists

| CLI TCP Keyword | Description | TCP Port Number |
|-----------------|--|-----------------|
| domain | Domain Name System | 53 |
| exec | Exec (rcp) | 512 |
| ftp | File Transfer Protocol | 21 |
| ftp-data | FTP data connections (used infrequently) | 20 |
| https | Secure HTTP | 443 |
| mms | Microsoft Media Server | 1755 |
| nfs | Network File System service | 2049 |
| ssh | Secure Shell login | 22 |

Table 3-2 TCP Keywords for Extended Access Lists (continued)

| CLI TCP Keyword | Description | TCP Port Number |
|-----------------|--|-----------------|
| tacacs | Terminal Access Controller Access Control System | 49 |
| telnet | Telnet | 23 |
| www | World Wide Web (HTTP) | 80 |

Table 3-3 lists the keywords that you can use to match specific ICMP message types and codes.

Table 3-3 Keywords for ICMP Messages

| | | |
|-----------------------------|---------------------------|---------------------|
| administratively-prohibited | alternate-address | conversion-error |
| dod-host-prohibited | dod-net-prohibited | echo |
| echo-reply | general-parameter-problem | host-isolated |
| host-precedence-unreachable | host-redirect | host-tos-redirect |
| host-tos-unreachable | host-unknown | host-unreachable |
| information-reply | information-request | mask-reply |
| mask-request | mobile-redirect | net-redirect |
| net-tos-redirect | net-tos-unreachable | net-unreachable |
| network-unknown | no-room-for-option | option-missing |
| packet-too-big | parameter-problem | port-unreachable |
| precedence-unreachable | protocol-unreachable | reassembly-timeout |
| redirect | router-advertisement | router-solicitation |
| source-quench | source-route-failed | time-exceeded |
| timestamp-reply | timestamp-request | traceroute |
| ttl-exceeded | unreachable | |

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it but limit host administrative access using SSH:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# deny tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

The following example shows how to activate the access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group extended testextacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
```


(config-ext-nacl) deny

```
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group extended testextacl in
 exit
. . .
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands[\(config-ext-nacl\) delete](#)[\(config-ext-nacl\) list](#)[\(config-ext-nacl\) move](#)[\(config-ext-nacl\) permit](#)

(config-ext-nacl) exit

To terminate extended ACL configuration mode and return to the global configuration mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes all modes

Device Modes application-accelerator
central-manager

Examples The following example shows how to terminate extended ACL configuration mode and return to global configuration mode:

```
WAE(config-ext-nacl)# exit  
WAE(config)#
```

(config-ext-nacl) list

To display a list of specified entries within the extended ACL, use the **list** extended ACL configuration command.

list [*start-line-num* [*end-line-num*]]

| | | |
|--------------------|-----------------------|--|
| Syntax Description | <i>start-line-num</i> | (Optional) Line number from which the list begins. |
| | <i>end-line-num</i> | (Optional) Last line number in the list. |

Defaults No default behavior or values.

Command Modes extended ACL configuration mode

Device Modes application-accelerator
central-manager

Examples The following example shows how to display a list of specified entries within the extended ACL:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# list 25 50
```

Related Commands [\(config-ext-nacl\) delete](#)
[\(config-ext-nacl\) move](#)

(config-ext-nacl) move

To move a line to a new position within the extended ACL, use the **move** extended ACL configuration command.

move *old-line-num new-line-num*

| Syntax | Description |
|---------------------|--|
| <i>old-line-num</i> | Line number of the entry to move. |
| <i>new-line-num</i> | New position of the entry. The existing entry is moved to the following position in the access list. |

Defaults No default behavior or values.

Command Modes extended ACL configuration mode

Device Modes application-accelerator
central-manager

Examples The following example shows how to move a line to a new position within the extended ACL:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# move 25 30
```

Related Commands [\(config-ext-nacl\) delete](#)
[\(config-ext-nacl\) list](#)

(config-ext-nacl) permit

To add a line to an extended access list that specifies the type of packets that you want the WAAS device to accept for further processing, use the **permit** extended ACL configuration command. To add a condition to the extended ACL, note that the options depend on the chosen protocol.

For IP, use the following syntax to add a condition:

```
[insert line-num] permit {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] |
  host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

```
no permit {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any}
  {dest-ip [wildcard] | host dest-ip | any}
```

For TCP, use the following syntax to add a condition:

```
[insert line-num] permit tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

```
no permit tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

For UDP, use the following syntax to add a condition:

```
[insert line-num] permit udp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

```
no permit udp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
  {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

For ICMP, use the following syntax to add a condition:

```
[insert line-num] permit icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] |
  host dest-ip | any} [icmp-type [code] | icmp-msg]
```

```
no permit icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip |
  any} [icmp-type [code] | icmp-msg]
```

| Syntax | Description |
|------------------------|--|
| insert line-num | (Optional) Specifies to insert the conditions following the specified line number into the access list. |
| gre | Specifies to match packets using the Generic Routing Encapsulation protocol. |
| icmp | Specifies to match ICMP packets. |
| tcp | Specifies to match packets using the TCP protocol. |
| udp | Specifies to match packets using the UDP protocol. |
| ip | Specifies to match all IP packets. |
| <i>proto-num</i> | IP protocol number. |
| <i>source-ip</i> | Source IP address. The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted-decimal format (for example, 0.0.0.0). |

| | |
|------------------------------|---|
| <i>wildcard</i> | (Optional) Wildcard. The notation is in 4-digit, dotted-decimal format. The bits to match are identified by a digital value of 0; the bits to ignore are identified by a 1. For extended IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for a extended IP ACL, then the <i>wildcard</i> parameter is not allowed. |
| host <i>source-ip</i> | Specifies to match the following IP address. |
| any | Specifies to match any IP address. |
| <i>dest-ip</i> | Specifies destination IP address. The number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format (for example, 0.0.0.0). |
| <i>operator port</i> | (Optional) Operator to use with specified ports, where lt = less than, gt = greater than, eq = equal to, neq = not equal to, and range = an inclusive range. The port value is a number (0–65535) or a keyword; two port numbers are required with the range keyword. See the “Usage Guidelines” section for a listing of the UDP and TCP keywords. |
| established | (Optional) Specifies to match TCP packets with the acknowledgment or reset bits set. |
| <i>icmp-type</i> | (Optional) Match with ICMP message type (0–255). |
| <i>code</i> | (Optional) Code type is 0–255. |
| <i>icmp-msg</i> | (Optional) Match a combination of ICMP message type and code types, as expressed by the keywords shown in the “Usage Guidelines” section. |

Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

extended ACL configuration mode

Device Modes

application-accelerator
central-manager

Usage Guidelines

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device to drop or to accept for further processing. By default, an access list denies everything because the list is terminated by an implicit **deny any** entry. You must include at least one **permit** entry to create a valid access list.

To allow connections from a specific host, use the **permit host source-ip** option and replace *source-ip* with the IP address of the specific host.

To allow connections from a specific network, use the **permit host source-ip wildcard** option. Replace *source-ip* with a network ID or the IP address of any host on the network that you want to specify. Replace *wildcard* with the dotted decimal notation for a mask that is the reverse of a subnet mask, where

a 0 indicates a position that must be matched and a 1 indicates a position that does not matter. For instance, the wildcard 0.0.0.255 causes the last eight bits in the source IP address to be ignored. The **permit 192.168.1.0 0.0.0.255** entry allows access from any host on the 192.168.1.0 network.

For extended IP ACLs, the **wildcard** parameter is required if the **host** keyword is not specified.

Use an extended access list to control connections based on the destination IP address or based on the protocol type. You can combine these conditions with information about the source IP address to create more restrictive condition.

Table 3-4 lists the UDP keywords that you can use with extended access lists.

Table 3-4 UDP Keywords for Extended Access Lists

| CLI UDP Keyword | Description | UDP Port Number |
|-----------------|--|-----------------|
| bootpc | Bootstrap Protocol (BOOTP) client | 68 |
| bootps | Bootstrap Protocol (BOOTP) server | 67 |
| domain | Domain Name System (DNS) | 53 |
| mms | Microsoft Media Server | 1755 |
| netbios-dgm | NetBIOS datagram service | 138 |
| netbios-ns | NetBIOS name service | 137 |
| netbios-ss | NetBIOS session service | 139 |
| nfs | Network File System service | 2049 |
| ntp | Network Time Protocol | 123 |
| snmp | Simple Network Management Protocol | 161 |
| snmptrap | SNMP traps | 162 |
| tacacs | Terminal Access Controller Access Control System | 49 |
| tftp | Trivial File Transfer Protocol | 69 |
| wccp | Web Cache Communication Protocol | 2048 |

Table 3-5 lists the TCP keywords that you can use with extended access lists.

Table 3-5 TCP Keywords for Extended Access Lists

| CLI TCP Keyword | Description | TCP Port Number |
|-----------------|--|-----------------|
| domain | Domain Name System | 53 |
| exec | Exec (rcp) | 512 |
| ftp | File Transfer Protocol | 21 |
| ftp-data | FTP data connections (used infrequently) | 20 |
| https | Secure HTTP | 443 |
| mms | Microsoft Media Server | 1755 |
| nfs | Network File System service | 2049 |
| ssh | Secure Shell login | 22 |

Table 3-5 TCP Keywords for Extended Access Lists (continued)

| CLI TCP Keyword | Description | TCP Port Number |
|-----------------|--|-----------------|
| tacacs | Terminal Access Controller Access Control System | 49 |
| telnet | Telnet | 23 |
| www | World Wide Web (HTTP) | 80 |

Table 3-6 lists the keywords that you can use to match specific ICMP message types and codes.

Table 3-6 Keywords for ICMP Messages

| | | |
|-----------------------------|---------------------------|---------------------|
| administratively-prohibited | alternate-address | conversion-error |
| dod-host-prohibited | dod-net-prohibited | echo |
| echo-reply | general-parameter-problem | host-isolated |
| host-precedence-unreachable | host-redirect | host-tos-redirect |
| host-tos-unreachable | host-unknown | host-unreachable |
| information-reply | information-request | mask-reply |
| mask-request | mobile-redirect | net-redirect |
| net-tos-redirect | net-tos-unreachable | net-unreachable |
| network-unknown | no-room-for-option | option-missing |
| packet-too-big | parameter-problem | port-unreachable |
| precedence-unreachable | protocol-unreachable | reassembly-timeout |
| redirect | router-advertisement | router-solicitation |
| source-quench | source-route-failed | time-exceeded |
| timestamp-reply | timestamp-request | traceroute |
| ttl-exceeded | unreachable | |

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it but limit host administrative access using SSH:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

The following example shows how to activate the access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
```


(config-ext-nacl) permit

```
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group testextacl in
 exit
. . .
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands[\(config-ext-nacl\) delete](#)[\(config-ext-nacl\) deny](#)[\(config-ext-nacl\) list](#)[\(config-ext-nacl\) move](#)