

Standard ACL Configuration Mode Commands

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

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

Syntax Description

standard	Enables standard ACL configuration mode. The CLI enters the standard ACL configuration mode in which all subsequent commands apply to the current standard access list. The (config-std-nacl) prompt appears: WAE(config-std-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 standard access lists, the valid range is 1 to 99.

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

Use access lists to control access to specific applications or interfaces on a WAAS device. An access control list consists of one or more condition entries that specify the kind of packets that the WAAS device will drop or accept for further processing. The WAAS device applies each entry in the order in which it occurs in the access list, which by default is the order in which you configured the entry.

The following list contains examples of how IP ACLs can be used in environments that use WAAS devices:

- A WAAS device resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- A WAAS device is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet, SSH, and WAAS GUI access to the IT source subnets.

- An application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access, primarily for security reasons. With an outside interface, many types of security attacks are possible.) The WAE's outside address is Internet global, and its inside address is private. The inside interface has an IP ACL to limit Telnet, SSH, and WAAS GUI access to the device.
- A WAAS device using WCCP is positioned between a firewall and an Internet router or a subnet off the Internet router. Both the WAAS device and the router must have IP ACLs.

**Note**

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

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 **exit** 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.

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 a standard access list, enter the **ip access-list standard** 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 a standard access list, it must be between 1 and 99.

**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.

You typically use a standard access list to allow connections from a host with a specific IP address or from hosts on a specific network. 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 standard access list, the CLI enters the standard ACL configuration mode and all subsequent commands apply to the specified access list.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# exit
```

Examples

The following example creates a standard access list on the WAAS device that permits any packets from source IP address 192.168.1.0 for further processing.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# permit 192.168.1.0 any
WAE(config-std-nacl)# exit
```

The following commands activate the access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl 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 teststdacl in
 exit
...
ip access-list standard teststdacl
 permit 192.168.1.0 any
 exit
...

```

Related Commands

clear
show ip access-list
(config-if) ip access-group
(config-std-nacl) deny
(config-std-nacl) delete
(config-std-nacl) list
(config-std-nacl) move
(config-std-nacl) permit

(config-std-nacl) delete

To delete a line from the standard IP ACL, use the **delete** command.

delete *line-num*

Syntax Description	delete	Deletes the specified entry.
	<i>line-num</i>	Identifies the entry at a specific line number in the access list.

Command Modes Standard ACL configuration mode

Device Modes application-accelerator
central-manager

Examples The following example deletes line 10 from the standard IP ACL teststdacl.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# delete 10
```

Related Commands

- [\(config-std-nacl\) deny](#)
- [\(config-std-nacl\) delete](#)
- [\(config-std-nacl\) list](#)
- [\(config-std-nacl\) move](#)
- [\(config-std-nacl\) permit](#)

(config-std-nacl) deny

To add a line to a standard access-list that specifies the type of packets that you want the WAAS device to drop, use the **deny** command.

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

To negate a standard IP ACL, use the following syntax.

```
no deny {source-ip [wildcard] | host source-ip | any}
```

Syntax Description		
insert	(Optional) Inserts the conditions following the specified line number into the access list.	
<i>line-num</i>	Identifies the entry at a specific line number in the access list.	
deny	Causes packets that match the specified conditions to be dropped.	
<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) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1.	
	Note For standard IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for a standard IP ACL, then the <i>wildcard</i> parameter is not allowed.	
host	Matches the following IP address.	
any	Matches any IP address.	

Defaults

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

Command Modes

Standard 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. Therefore, you must include at least one **permit** entry to create a valid access list.

You typically use a standard access list to allow connections from a host with a specific IP address or from hosts on a specific network. 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.

Examples

The following example creates standard access-list that denies any packets from source IP address 192.168.1.0 for processing.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# deny 192.168.1.0 any
WAE(config-std-nacl)# exit
```

The following commands activate the standard access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl 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 teststdacl in
 exit
. . .
ip access-list standard example
 deny 192.168.1.0 any
 exit
. . .
```

Related Commands

- [\(config-std-nacl\) delete](#)
- [\(config-std-nacl\) list](#)
- [\(config-std-nacl\) move](#)
- [\(config-std-nacl\) permit](#)

(config-std-nacl) exit

To terminate standard 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 terminates standard ACL configuration mode and returns to global configuration mode:

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

(config-std-nacl) list

To display a list of specified entries within the standard IP ACL, use the **list** command.

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

Syntax Description	list	Lists the specified entries (or all entries when none are specified).
	<i>start-line-num</i>	Line number from which the list begins.
	<i>end-line-num</i>	(Optional) Last line number in the list.

Command Modes Standard ACL configuration mode

Device Modes application-accelerator
central-manager

Examples The following example displays a list of specified entries within the standard IP ACL.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# list 25 50
```

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

(config-std-nacl) move

To move a line to a new position within the standard IP ACL, use the **move** command.

```
move old-line-num new-line-num
```

Syntax Description	move	Moves the specified entry in the access list to a new position in the list.
	<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.

Command Modes Standard ACL configuration mode

Device Modes application-accelerator
central-manager

Examples The following example moves a line to a new position within the standard IP ACL.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# move 25 30
```

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

(config-std-nacl) permit

To add a line to a standard access-list that specifies the type of packets that you want the WAAS device to accept for further processing, use the **permit** command.

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

To negate a standard IP ACL, use the following syntax.

```
no permit {source-ip [wildcard] | host source-ip | any}
```

Syntax Description		
insert	(Optional) Inserts the conditions following the specified line number into the access list.	
<i>line-num</i>	Identifies the entry at a specific line number in the access list.	
permit	Causes packets that match the specified conditions to be accepted for further processing.	
<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) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1.	
	Note For standard IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for a standard IP ACL, then the <i>wildcard</i> parameter is not allowed.	
host	Matches the following IP address.	
any	Matches any IP address.	

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

Command Modes Standard 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. Therefore, you must include at least one **permit** entry to create a valid access list.

You typically use a standard access list to allow connections from a host with a specific IP address or from hosts on a specific network. 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.

Examples

The following example creates standard access-list that permits any packets from source IP address 192.168.1.0 for further processing.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# permit 192.168.1.0 any
WAE(config-std-nacl)# exit
```

The following commands activate the standard access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl 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 teststdacl in
 exit
...
ip access-list standard example
 permit 192.168.1.0 any
 exit
...

```

Related Commands

[\(config-std-nacl\) delete](#)
[\(config-std-nacl\) deny](#)
[\(config-std-nacl\) list](#)
[\(config-std-nacl\) move](#)

■ (config-std-nacl) permit