



# CHAPTER 10

## Configuring Blocking

---

This chapter provides procedures for configuring the sensor to use blocking devices and for configuring the sensor to be a master blocking sensor.

This chapter contains the following sections:

- [Understanding Blocking, page 10-1](#)
- [Blocking Prerequisites, page 10-3](#)
- [Supported Blocking Devices, page 10-3](#)
- [Configuring Blocking Properties, page 10-4](#)
- [Configuring User Profiles, page 10-17](#)
- [Configuring Blocking Devices, page 10-18](#)
- [Configuring the Sensor to be a Master Blocking Sensor, page 10-25](#)
- [Configuring Manual Blocking, page 10-27](#)
- [Obtaining a List of Blocked Hosts and Connections, page 10-28](#)

## Understanding Blocking

Network Access Controller, the blocking application on the sensor, starts and stops blocks on routers, switches, PIX Firewalls, FWSM, and ASA. Network Access Controller blocks the IP address on the devices it is managing. It sends the same block to all the devices it is managing, including any other master blocking sensors. Network Access Controller monitors the time for the block and removes the block after the time has expired.



### Caution

---

If ASA or FWSM is configured in multi-mode, blocking is not supported for the admin context. Blocking is only supported in single mode and in multi-mode customer context.

---

There are three types of blocks:

- **Host block**—Blocks all traffic from a given IP address.
- **Connection block**—Blocks traffic from a given source IP address to a given destination IP address and destination port.




---

**Note** Connection blocks are not supported on firewalls. Firewalls only support host blocks with additional connection information.

---




---

**Note** Multiple connection blocks from the same source IP address to either a different destination IP address or destination port automatically switch the block from a connection block to a host block.

---

- Network block—Blocks all traffic from a given network.




---

**Note** You can initiate host and connection blocks manually or automatically when a signature is triggered. You can only initiate network blocks manually.

---




---

**Note** Do not confuse blocking with the sensor's ability to drop packets. The sensor can drop packets when the following actions are configured for a sensor in inline mode: deny packet inline, deny connection inline, and deny attacker inline.

---

On Cisco routers and Catalyst 6500 series switches, Network Access Controller creates blocks by applying ACLs or VACLs. ACLs and VACLs permit or deny passage of data packets through interface ports or VLANs. Each ACL or VACL contains permit and deny conditions that apply to IP addresses. The PIX Firewall, FWSM, and ASA do not use ACLs or VACLs. The built-in **shun/no shun** command is used.

You need the following information for Network Access Controller to manage a device:

- Login user ID (if the device is configured with AAA)
  - Login password
  - Enable password (not needed if the user has enable privileges)
  - Interfaces to be managed (for example, ethernet0, vlan100)
  - Any existing ACL/VACL information you want applied at the beginning (Pre-Block ACL/VACL) or end (Post-Block ACL/VACL) of the ACL/VACL that will be created
- This does not apply to a PIX Firewall, FWSM, or ASA because they do not use ACLs to block.
- Whether you are using Telnet or SSH to communicate with the device
  - IP addresses (host or range of hosts) you never want blocked
  - How long you want the blocks to last



**Tip**

---

To check the status of Network Access Controller, type **show statistics network-access** at the `sensor#`. The output shows the devices you are managing, any active blocks, and the status for all devices. In the IDM, click **Monitoring > Statistics**, or in the ASDM, click **Monitoring > Features > IPS > Statistics**, to see the status of Network Access Controller.

---

# Blocking Prerequisites

Before you configure blocking, make sure you do the following:

- Analyze your network topology to understand which devices should be blocked by which sensor, and which addresses should never be blocked.



## Caution

Two sensors cannot control blocking on the same device. If this situation is needed, configure one sensor as the master blocking sensor to manage the devices and the other sensors can forward their block requests to the master blocking sensor. For the procedure, see [Configuring the Sensor to be a Master Blocking Sensor, page 10-25](#).

- Gather the usernames, device passwords, enable passwords, and connections types (Telnet or SSH) needed to log in to each device.
- Know the interface names on the devices.
- Know the names of the Pre-Block ACL or VACL and Post-Block ACL or VACL if needed.
- Understand which interfaces should and should not be blocked and in which direction (in or out). You do not want to accidentally shut down an entire network.

# Supported Blocking Devices

By default, Network Access Controller supports up to 250 devices in any combination. The following devices are supported by Network Access Controller:

- Cisco series routers using Cisco IOS 11.2 or later (ACLs):
  - Cisco 1600 series router
  - Cisco 1700 series router
  - Cisco 2500 series router
  - Cisco 2600 series router
  - Cisco 2800 series router
  - Cisco 3600 series router
  - Cisco 3800 series router
  - Cisco 7200 series router
  - Cisco 7500 series router
- Catalyst 5000 switches with RSM with IOS 11.2(9)P or later (ACLs)
- Catalyst 6500 switches and 7600 routers with IOS 12.1(13)E or later (ACLs)
- Catalyst 6500 switches 7600 routers with Catalyst software version 7.5(1) or later (VACLs)
  - Supervisor Engine 1A with PFC
  - Supervisor Engine 1A with MSFC1
  - Supervisor Engine 1A with MFSC2
  - Supervisor Engine 2 with MSFC2
  - Supervisor Engine 720 with MSFC3




---

**Note** We support VACL blocking on the Supervisor Engine and ACL blocking on the MSFC.

---

- PIX Firewall with version 6.0 or later (**shun** command)
  - 501
  - 506E
  - 515E
  - 525
  - 535
- ASA with version 7.0 or later (**shun** command)
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 or later (**shun** command)

You configure blocking using either ACLs, VACLs, or the **shun** command. All firewall and ASA models support the **shun** command.

## Configuring Blocking Properties

You can change the default blocking properties. It is best to use the default properties, but if you need to change them, use the following procedures:

- [Allowing the Sensor to Block Itself, page 10-4](#)
- [Disabling Blocking, page 10-6](#)
- [Setting Maximum Block Entries, page 10-8](#)
- [Setting the Block Time, page 10-10](#)
- [Enabling ACL Logging, page 10-11](#)
- [Enabling Writing to NVRAM, page 10-12](#)
- [Logging All Blocking Events and Errors, page 10-13](#)
- [Configuring the Maximum Number of Blocking Interfaces, page 10-14](#)
- [Configuring Addresses Never to Block, page 10-15](#)

## Allowing the Sensor to Block Itself

Use the **allow-sensor-block [true | false]** command in the service network-access submode to configure the sensor to block itself.



### Caution

---

We recommend that you do not permit the sensor to block itself, because it may stop communicating with the blocking device. You can configure this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

---

To allow the sensor to block itself, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Enter general submode:

```
sensor(config-net)# general
```

**Step 4** Configure the sensor to block itself:

```
sensor(config-net-gen)# allow-sensor-block true
```

By default, this value is **false**.

**Step 5** Verify the settings:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: true default: false
block-enable: true default: true
block-max-entries: 100 default: 250
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 1)
-----
ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 1)
-----
ip-address: 12.12.0.0/16
-----
block-hosts (min: 0, max: 250, current: 0)
-----
--MORE--
```

**Step 6** Configure the sensor not to block itself:

```
sensor(config-net-gen)# allow-sensor-block false
```

**Step 7** Verify the setting:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false default: false
block-enable: true default: true
block-max-entries: 100 default: 250
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
```

```

-----
-----
never-block-hosts (min: 0, max: 250, current: 1)
-----
    ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 1)
-----
    ip-address: 12.12.0.0/16
-----
block-hosts (min: 0, max: 250, current: 0)
-----
--MORE--

```

**Step 8** Exit network access submode:

```

sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes?[yes]:

```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Disabling Blocking

Use the **block-enable [true | false]** command in the service network access submode to enable or disable blocking on the sensor.

By default, blocking is enabled on the sensor. If Network Access Controller is managing a device and you need to manually configure something on that device, you should disable blocking first. You want to avoid a situation in which both you and Network Access Controller could be making a change at the same time on the same device. This could cause the device and/or Network Access Controller to crash.



### Caution

If you disable blocking for maintenance on the devices, make sure you enable it after the maintenance is complete or the network will be vulnerable to attacks that would otherwise be blocked.

---



### Note

While blocking is disabled, Network Access Controller continues to receive blocks and track the time on active blocks, but will not apply new blocks or remove blocks from the managed devices. After blocking is reenabled, the blocks on the devices are updated.

---

To disable blocking, follow these steps:

---

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```

sensor# configure terminal

```

**Step 3** Enter general submode:

```

sensor(config-net)# general

```

**Step 4** Disable blocking on the sensor:

```
sensor(config-net-gen)# block-enable false
```

By default, this value is **true**.

**Step 5** Verify the settings:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false default: false
block-enable: false default: true
block-max-entries: 100 default: 250
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 1)
-----
ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 1)
-----
ip-address: 12.12.0.0/16
-----
block-hosts (min: 0, max: 250, current: 0)
-----
--MORE--
```

**Step 6** Enable blocking on the sensor:

```
sensor(config-net-gen)# block-enable true
```

**Step 7** Verify that the setting has been returned to the default:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false default: false
block-enable: true default: true
block-max-entries: 100 default: 250
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 1)
-----
ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 1)
-----
ip-address: 12.12.0.0/16
-----
```

```

-----
block-hosts (min: 0, max: 250, current: 0)
-----
--MORE--

```

**Step 8** Exit network access submode:

```

sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:[yes]:

```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Setting Maximum Block Entries

Use the **block-max-entries** command in the service network access submode to configure the maximum block entries.

You can set how many blocks are to be maintained simultaneously (1 to 65535). The default value is 250.



### Caution

We do not recommend setting the maximum block entries higher than 250. Some devices have problems with larger numbers of ACL or shun entries. Refer to the documentation for each device to determine its limits before increasing this number.

---



### Note

The number of blocks will not exceed the maximum block entries. If the maximum is reached, new blocks will not occur until existing blocks time out and are removed.

---

To change the maximum number of block entries, follow these steps:

---

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```

sensor# configure terminal
sensor(config)# service network-access

```

**Step 3** Enter general submode:

```

sensor(config-net)# general

```

**Step 4** Change the maximum number of block entries:

```

sensor(config-net-gen)# block-max-entries 100

```

**Step 5** Verify the setting:

```

sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false default: false
block-enable: true <defaulted>
block-max-entries: 100 default: 250

```

```

max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 1)
-----
    ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 1)
-----
    ip-address: 12.12.0.0/16
-----
block-hosts (min: 0, max: 250, current: 0)
-----
--MORE--

```

**Step 6** To return to the default value of 250 blocks:

```
sensor(config-net-gen)# default block-max-entries
```

**Step 7** Verify the setting:

```

sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false default: false
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 1)
-----
    ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 1)
-----
    ip-address: 12.12.0.0/16
-----
block-hosts (min: 0, max: 250, current: 0)
-----
--MORE--

```

**Step 8** Exit network access submode:

```

sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:[yes]:

```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

## Setting the Block Time

Use the **global-block-timeout** command in the service event action rules submode to change the amount of time an automatic block lasts. The default is 30 minutes.


**Note**

If you change the default block time, you are changing a signature parameter, which affects all signatures.


**Note**

The time for manual blocks is set when you request the block.

To change the default block time, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter event action rules submode:

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
```

**Step 3** Enter general submode:

```
sensor(config-rul)# general
```

**Step 4** Configure the block time:

```
sensor(config-rul-gen)# global-block-timeout 60
```

The value is the time duration of the block event in minutes (0 to 10000000).

**Step 5** Verify the setting:

```
sensor(config-rul-gen)# show settings
general
-----
global-overrides-status: Enabled <defaulted>
global-filters-status: Enabled <defaulted>
global-summarization-status: Enabled <defaulted>
global-metaevent-status: Enabled <defaulted>
global-deny-timeout: 3600 <defaulted>
global-block-timeout: 60 default: 30
max-denied-attackers: 10000 <defaulted>
-----
sensor(config-rul-gen)#
```

**Step 6** Exit event action rules submode:

```
sensor(config-rul-gen)# exit
sensor(config-rul)# exit
Apply Changes:[yes]:
```

**Step 7** Press **Enter** to apply the changes or type **no** to discard them.


**Note**

There is a time delay while the signatures are updated.

## Enabling ACL Logging

Use the **enable-acl-logging [true | false]** command in the service network access submode to enable ACL logging, which causes Network Access Controller to append the log parameter to block entries in the ACL or VACL. This causes the device to generate syslog events when packets are filtered. Enable ACL logging only applies to routers and switches. The default is disabled.

To enable ACL logging, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Enter general submode:

```
sensor(config-net)# general
```

**Step 4** Enable ACL logging:

```
sensor(config-net-gen)# enable-acl-logging true
```

**Step 5** Verify that ACL logging is enabled:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: true default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
```

**Step 6** To disable ACL logging, use the **false** keyword:

```
sensor(config-net-gen)# enable-acl-logging false
```

**Step 7** Verify that ACL logging is disabled:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
```

**Step 8** Exit network access mode:

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:[yes]:
```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Enabling Writing to NVRAM

Use the **enable-nvram-write [true | false]** command to configure the sensor to have the router write to NVRAM when the Network Access Controller first connects. If **enable-nvram-write** is enabled, NVRAM is written each time the ACLs are updated. The default is disabled.

Enabling NVRAM writing ensures that all changes for blocking are written to NVRAM. If the router is rebooted, the correct blocks will still be active. If NVRAM writing is disabled, a short time without blocking occurs after a router reboot. And not enabling NVRAM writing increases the life of the NVRAM and decreases the time for new blocks to be configured.

To enable writing to NVRAM, follow these steps:

---

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Enter general submode:

```
sensor(config-net)# general
```

**Step 4** Enable writing to NVRAM:

```
sensor(config-net-gen)# enable-nvram-write true
```

**Step 5** Verify that writing to NVRAM is enabled:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: true default: false
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
```

**Step 6** Disable writing to NVRAM:

```
sensor(config-net-gen)# enable-nvram-write false
```

**Step 7** Verify that writing to NVRAM is disabled:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false default: false
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
```

**Step 8** Exit network access submode:

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:[yes]:
```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Logging All Blocking Events and Errors

Use the **log-all-block-events-and-errors [true | false]** command in the service network access submode to configure the sensor to log events that follow blocks from start to finish. For example, when a block is added to or removed from a device, an event is logged. You may not want all of these events and errors to be logged. Disabling **log-all-block-events-and-errors** suppresses the new events and errors. The default is enabled.

To disable blocking event and error logging, follow these steps:

---

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access mode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Enter general submode:

```
sensor(config-net)# general
```

**Step 4** Disable blocking event and error logging:

```
sensor(config-net-gen)# log-all-block-events-and-errors false
```

**Step 5** Verify that logging is disabled:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: false default: true
enable-nvram-write: false default: false
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
```

```

block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----

```

**Step 6** Enable blocking event and error logging:

```
sensor(config-net-gen)# log-all-block-events-and-errors true
```

**Step 7** Verify that logging is enabled:

```

sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true default: true
enable-nvram-write: false default: false
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----

```

**Step 8** Exit network access mode:

```

sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes?[yes]:

```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Configuring the Maximum Number of Blocking Interfaces

Use the **max-interfaces** command to configure the maximum number of interfaces for performing blocks. For example, a PIX Firewall counts as one interface. A router with one interface counts as one, but a router with two interfaces counts as two. You can configure up to 250 Catalyst 6K switches, 250 routers, and 250 firewalls.

The **max-interfaces** command configures the limit of the sum total of all interfaces and devices. In addition to configuring the limit on the sum total of interfaces and devices, there is a fixed limit on the number of blocking interfaces you can configure per device. Use the **show settings** command in network access mode to view the specific maximum limits per device.

To configure the maximum number of blocking interfaces, follow these steps:

---

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access mode:

```

sensor# configure terminal
sensor(config)# service network-access

```

**Step 3** Enter general submode:

```
sensor(config-net)# general
```

**Step 4** Configure the maximum number of interfaces:

```
sensor(config-net-gen)# max-interfaces 50
```

**Step 5** Verify the number of maximum interfaces:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true default: true
enable-nvram-write: false default: false
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 50 default: 250
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
```

**Step 6** Return the setting to the default of 250:

```
sensor(config-net-gen)# default max-interfaces
```

**Step 7** Verify the default setting:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true default: true
enable-nvram-write: false default: false
enable-acl-logging: false default: false
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
```

**Step 8** Exit network access mode:

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:[yes]:
```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Configuring Addresses Never to Block

Use the **never-block-hosts** and the **never-block-networks** commands in the service network access submode to configure hosts and network that should never be blocked.

The following options apply:

- *ip\_address*—IP address of the device that should never be blocked.
- *ip\_address/netmask*— IP address of the network that should never be blocked. The format for is A.B.C.D./nn.

You must tune your sensor to identify hosts and networks that should never be blocked, not even manually, because you may have a trusted network device whose normal, expected behavior appears to be an attack. Such a device should never be blocked, and trusted, internal networks should never be blocked.

You can specify a single host or an entire network.

To set up addresses never to be blocked by blocking devices, follow these steps:

---

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Enter general submode:

```
sensor(config-net)# general
```

**Step 4** Define the address that should never be blocked:

- For a single host:

```
sensor(config-net-gen)# never-block-hosts 10.16.0.0
```

- For an entire network:

```
sensor(config-net-gen)# never-block-networks 10.0.0.0/8
```

**Step 5** Verify the settings:

```
sensor(config-net-gen)# show settings
general
-----
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false default: false
block-enable: true default: true
block-max-entries: 100 default: 250
max-interfaces: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 2)
-----
ip-address: 10.16.0.0
-----
ip-address: 11.11.11.11
-----
never-block-networks (min: 0, max: 250, current: 2)
-----
ip-address: 10.0.0.0/8
-----
ip-address: 12.12.0.0/16
--MORE--
```

**Step 6** Exit network access submode:

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes?[yes]:
```

**Step 7** Press **Enter** to apply the changes or type **no** to discard them.

---

# Configuring User Profiles

Use the **user-profiles** *profile\_name* command in the service network access submode to set up user profiles for the other devices that the sensor will manage. The user profiles contain userid, password, and enable password information. For example, routers that all share the same passwords and usernames can be under one user profile.



**Note** If the username or password is not needed to log in to the device, do not set a value for it.



**Note** You **MUST** create a user profile before configuring the blocking device.

To set up user profiles, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access mode:

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

**Step 3** Create the user profile name:

```
sensor(config-net)# user-profiles PROFILE1
```

**Step 4** Type the username for that user profile:

```
sensor(config-net-use)# username username
```

**Step 5** Specify the password for the user:

```
sensor(config-net-use)# password
Enter password[]: *****
Re-enter password *****
```

**Step 6** Specify the enable password for the user:

```
sensor(config-net-use)# enable-password
Enter enable-password[]: *****
Re-enter enable-password *****
```

**Step 7** Verify the settings:

```
sensor(config-net-use)# show settings
profile-name: PROFILE1
-----
enable-password: <hidden>
password: <hidden>
username: jsmith default:
-----
sensor(config-net-use)#
```

**Step 8** Exit network access submode:

```
sensor(config-net-use)# exit
sensor(config-net)# exit
Apply Changes:[yes]:
```

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Configuring Blocking Devices

This section describes how to configure devices that the sensor uses to block. It contains the following topics:

- [How the Sensor Manages Devices, page 10-18](#)
- [Configuring the Sensor to Manage Cisco Routers, page 10-19](#)
- [Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 10-21](#)
- [Configuring the Sensor to Manage Cisco Firewalls, page 10-24](#)

## How the Sensor Manages Devices

Network Access Controller uses ACLs on Cisco routers and switches to manage those devices. These ACLs are built as follows:

1. A **permit** line with the sensor's IP address or, if specified, the NAT address of the sensor



**Note** If you permit the sensor to be blocked, this line does not appear in the ACL.

---

2. Pre-Block ACL (if specified)

This ACL must already exist on the device.



**Note** Network Access Controller reads the lines in the ACL and copies these lines to the beginning of the ACL.

---

3. Any active blocks

4. Either:

- Post-Block ACL (if specified)

This ACL must already exist on the device.



**Note** Network Access Controller reads the lines in the ACL and copies these lines to the end of the ACL.

---

**Note**

Make sure the last line in the ACL is **permit ip any any** if you want all unmatched packets to be permitted.

- **permit ip any any** (not used if a Post-Block ACL is specified)

Network Access Controller uses two ACLs to manage devices. Only one is active at any one time. It uses the offline ACL name to build the new ACL, then applies it to the interface. Network Access Controller then reverses the process on the next cycle.

**Note**

The ACLs that NAC creates are not removed from the managed device after you configure NAC to no longer manage that device. You must remove the ACLs manually on any device that NAC formerly managed.

If you need to modify the Pre-Block or Post-Block ACL, do the following:

1. Disable blocking on the sensor.
2. Make the changes to the device's configuration.
3. Reenable blocking on the sensor.

When blocking is reenabled, the sensor reads the new device configuration. For the procedure, see [Disabling Blocking, page 10-6](#).

**Caution**

A single sensor can manage multiple devices, but you cannot use multiple sensors to control a single device. In this case, use a master blocking sensor. For the procedure, see [Configuring the Sensor to be a Master Blocking Sensor, page 10-25](#).

## Configuring the Sensor to Manage Cisco Routers

This section describes how to configure the sensor to manage Cisco routers. It contains the following topics:

- [Routers and ACLs, page 10-19](#)
- [Configuring the Sensor to Manage Cisco Routers, page 10-20](#)

### Routers and ACLs

You create and save Pre-Block and Post-Block ACLs in your router configuration. These ACLs must be extended IP ACLs, either named or numbered. See your router documentation for more information on creating ACLs.

Enter the names of these ACLs that are already configured on your router in the Pre-Block ACL and Post-Block ACL fields.

The Pre-Block ACL is mainly used for permitting what you do not want the sensor to ever block. When a packet is checked against the ACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block ACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the ACL. The Pre-Block ACL can override the deny lines resulting from the blocks.

The Post-Block ACL is best used for additional blocking or permitting that you want to occur on the same interface or direction. If you have an existing ACL on the interface or direction that the sensor will manage, that existing ACL can be used as a Post-Block ACL. If you do not have a Post-Block ACL, the sensor inserts a **permit ip any any** at the end of the new ACL.

When the sensor starts up, it reads the contents of the two ACLs. It creates a third ACL with the following entries:

- A **permit** line for the sensor's IP address
- Copies of all configuration lines of the Pre-Block ACL
- A **deny** line for each address being blocked by the sensor
- Copies of all configuration lines of the Post-Block ACL

The sensor applies the new ACL to the interface and direction that you designate.

**Note**

When the new ACL is applied to an interface or direction of the router, it removes the application of any other ACL to that interface or direction.

## Configuring the Sensor to Manage Cisco Routers

To configure a sensor to manage Cisco routers, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Set the IP address for the router controlled by Network Access Controller:

```
sensor(config-net)# router-devices ip_address
```

**Step 4** Type the logical device name that you created in [Configuring User Profiles, page 10-17](#).

```
sensor(config-net-rou)# profile-name user_profile_name
```

Network Access Controller accepts anything you type. It does not check to see if the user profile exists.

**Step 5** Designate the method used to access the sensor:

```
sensor(config-net-rou)# communication [telnet | ssh-des | sh-3des]
```

If unspecified, SSH 3DES is used.

**Note**

If you are using DES or 3DES, you must use the command **ssh host-key ip\_address** to accept the key or Network Access Controller cannot connect to the device.

**Step 6** Specify the sensor's NAT address:

```
sensor(config-net-rou)# nat-address nat_address
```

**Note**

This changes the IP address in the first line of the ACL from the sensor's address to the NAT address. This is not a NAT address configured on the device being managed. It is the address the sensor is translated to by an intermediate device, one that is between the sensor and the device being managed.

**Step 7** Set the interface name and direction:

```
sensor(config-net-rou)# block-interfaces interface_name [in | out]
```

**Caution**

The name of the interface must either be the complete name of the interface or an abbreviation that the router recognizes with the **interface** command.

**Step 8** (Optional) Add the pre-ACL name:

```
sensor(config-net-rou-blo)# pre-acl-name pre_acl_name
```

**Step 9** (Optional) Add the post-ACL name:

```
sensor(config-net-rou-blo)# post-acl-name post_acl_name
```

**Step 10** Exit network access submode:

```
sensor(config-net-rou-blo)# exit
sensor(config-net-rou)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:[yes]:
```

**Step 11** Press **Enter** to apply the changes or type **no** to discard them.

## Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers

This section describes how to configure the sensor to manage Cisco switches. It contains the following topics:

- [Switches and VACLs, page 10-21](#)
- [Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 10-22](#)

### Switches and VACLs

You can configure Network Access Controller to block using VACLs on the switch itself when running Cisco Catalyst software, or to block using router ACLs on the MSFC or on the switch itself when running Cisco IOS software. This section describes blocking using VACLs. For blocking using the router ACLS see [Configuring the Sensor to Manage Cisco Routers, page 10-19](#).

You must configure the blocking interfaces on the Catalyst 6500 series switch and specify the VLAN of traffic you want blocked.

You create and save Pre-Block and Post-Block VACLs in your switch configuration. These VACLs must be extended IP VACLs, either named or numbered. See your switch documentation for more information on creating VACLs.

Enter the names of these VACLs that are already configured on your switch in the Pre-Block VACL and Post-Block VACL fields.

The Pre-Block VACL is used mainly for permitting what you do not want the sensor to ever block. When a packet is checked against the VACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block VACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the VACL. The Pre-Block VACL can override the deny lines resulting from the blocks.

The Post-Block VACL is best used for additional blocking or permitting that you want to occur on the same VLAN. If you have an existing VACL on the VLAN that the sensor will manage, the existing VACL can be used as a Post-Block VACL. If you do not have a Post-Block VACL, the sensor inserts a **permit ip any any** at the end of the new VACL.

**Note**


---

The IDS-2 inserts a **permit ip any any capture** at the end of the new VACL.

---

When the sensor starts up, it reads the contents of the two VACLs. It creates a third VACL with the following entries:

- A **permit** line for the sensor's IP address
- Copies of all configuration lines of the Pre-Block VACL
- A **deny** line for each address being blocked by the sensor
- Copies of all configuration lines of the Post-Block VACL

The sensor applies the new VACL to the VLAN that you designate

**Note**


---

When the new VACL is applied to a VLAN of the switch, it removes the application of any other VACL to that VLAN.

---

## Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers

To configure the sensor to manage Catalyst 6500 series switches and Cisco 7600 series routers, follow these steps:

- 
- Step 1** Log in to the CLI using an account with administrator privileges.
- Step 2** Enter network access submode:
- ```
sensor# configure terminal
```
- Step 3** Set the IP address for the router controlled by Network Access Controller:
- ```
sensor(config-net)# cat6k-devices ip_address
```

**Step 4** Type the user profile name that you created in [Configuring User Profiles, page 10-17](#).

```
sensor(config-net-cat)# profile-name user_profile_name
```



**Note** Network Access Controller accepts anything you type. It does not check to see if the logical device exists.

**Step 5** Designate the method used to access the sensor:

```
sensor(config-net-cat)# communication [telnet | ssh-des/ | sh-3des]
```

If unspecified, SSH 3DES is used.



**Note** If you are using DES or 3DES, you must use the command **ssh host-key ip\_address** to accept the key or Network Access Controller cannot connect to the device. For the procedure, see [Adding Hosts to the Known Hosts List, page 4-31](#).

**Step 6** Specify the sensor's NAT address:

```
sensor(config-net-cat)# nat-address nat_address
```



**Note** This changes the IP address in the first line of the ACL from the sensor's address to the NAT address. This is not a NAT address configured on the device being managed. It is the address the sensor is translated to by an intermediate device, one that is between the sensor and the device being managed.

**Step 7** Specify the VLAN number:

```
sensor(config-net-cat)# block-vlans vlan_number
```

**Step 8** (Optional) Add the pre-VACL name:

```
sensor(config-net-cat-blo)# pre-vacl-name pre_vacl_name
```

**Step 9** (Optional) Add the post-VACL name:

```
sensor(config-net-cat-blo)# post-vacl-name post_vacl_name
```

**Step 10** Exit network access submode:

```
sensor(config-net-cat-blo)# exit
sensor(config-net-cat)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:[yes]:
```

**Step 11** Press **Enter** to apply the changes or type **no** to discard them.

## Configuring the Sensor to Manage Cisco Firewalls

To configure the sensor to manage Cisco firewalls, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access submode:

```
sensor# configure terminal
sensor(config)# service network-access
```

**Step 3** Set the IP address for the firewall controlled by Network Access Controller:

```
sensor(config-net)# firewall-devices ip_address
```

**Step 4** Type the user profile name that you created in [Configuring User Profiles, page 10-17](#).

```
sensor(config-net-fir)# profile-name user_profile_name
```

Network Access Controller accepts anything you type. It does not check to see if the logical device exists.

**Step 5** Designate the method used to access the sensor:

```
sensor(config-net-fir)# communication [telnet | ssh-des | sh-3des]
```

If unspecified, SSH 3DES is used.



**Note** If you are using DES or 3DES, you must use the command `ssh host-key ip_address` to accept the key or Network Access Controller cannot connect to the device. For the procedure, see [Adding Hosts to the Known Hosts List, page 4-31](#).

**Step 6** Specify the sensor's NAT address:

```
sensor(config-net-fir)# nat-address nat_address
```



**Note** This changes the IP address in the first line of the ACL from the sensor's address to the NAT address. This is not a NAT address configured on the device being managed. It is the address the sensor is translated to by an intermediate device, one that is between the sensor and the device being managed.

**Step 7** Exit network access submode:

```
sensor(config-net-fir)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

**Step 8** Press **Enter** to apply the changes or type **no** to discard them.

# Configuring the Sensor to be a Master Blocking Sensor

Multiple sensors (blocking forwarding sensors) can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The master blocking sensor is the Network Access Controller running on a sensor that controls blocking on one or more devices on behalf of one or more other sensors. The Network Access Controller on a master blocking sensor controls blocking on devices at the request of the Network Access Controllers running on other sensors.

On the blocking forwarding sensor, identify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its access list.

If the master blocking sensor requires TLS for web connections, you must configure the Network Access Controller of the blocking forwarding sensor to accept the X.509 certificate of the master blocking sensor remote host. Sensors by default have TLS enabled, but you can change this option.



## Note

Typically the master blocking sensor is configured to manage the network devices. Blocking forwarding sensors are not normally configured to manage other network devices, although doing so is permissible.



## Caution

Only one sensor should control all blocking interfaces on a device.

Use the **master-blocking-sensors** *mbs\_ip\_address* command in the service network access submode to configure a master blocking sensor.

The following options apply:

- *mbs\_ip\_address*—IP address of sensor for forward block requests.
- **password**—Account password of sensor for forward block requests.
- **port**—Port of sensor for forward block requests.
- **tls [true | false]**—Set to true if the remote sensor requires TLS, otherwise set to false.
- **username**—Account name of sensor for forward block requests.

To configure the Network Access Controller on a sensor to forward blocks to a master blocking sensor, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges on both the master blocking sensor and the blocking forwarding sensor.

**Step 2** Enter configuration mode on both sensors:

```
sensor# configure terminal
```

**Step 3** Configure TLS if necessary:

- a. On the master blocking sensor, check to see if it requires TLS and what port number is used:

```
sensor(config)# service web-server
sensor(config-web)# show settings
  enable-tls: true <defaulted>
  port: 443 <defaulted>
  server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)#
```

If *enable-tls* is true, go to Step b.

- b. On the blocking forwarding sensor, configure it to accept the X.509 certificate of the master blocking sensor:

```
sensor(config-web)# exit
sensor(config)# tls trusted-host ip-address mbs_ip_address port port_number
```

Example:

```
sensor(config)# tls trusted-host ip-address 10.0.0.0 port 8080
Certificate MD5 fingerprint is
F4:4A:14:BA:84:F4:51:D0:A4:E2:15:38:7E:77:96:D8Certificate SHA1 fingerprint is
84:09:B6:85:C5:43:60:5B:37:1E:6D:31:6A:30:5F:7E:4D:4D:E8:B2
Would you like to add this to the trusted certificate table for this host?[yes]:
```




---

**Note** You are prompted to accept the certificate based on the certificate's fingerprint. Sensors provide only self-signed certificates (instead of certificates signed by a recognized certificate authority). You can verify the master blocking sensor host sensor's certificate by logging in to the host sensor and typing the **show tls fingerprint** command to see that the host certificate's fingerprints match.

---

**Step 4** Type **yes** to accept the certificate from the master blocking sensor.

**Step 5** Enter network access mode:

```
sensor(config)# service network-access
```

**Step 6** Enter general submode:

```
sensor(config-net)# general
```

**Step 7** Add a master blocking sensor entry:

```
sensor(config-net-gen)# master-blocking-sensors mbs_ip_address
```

**Step 8** Specify the username for an administrative account on the master blocking sensor host:

```
sensor(config-net-gen-mas)# username username
```

**Step 9** Specify the password for the user:

```
sensor(config-net-gen-mas)# password
Enter password []: *****
Re-enter mbs-password []: *****
sensor(config-net-gen-mas)#
```

**Step 10** Specify the port number for the host's HTTP communications.

```
sensor(config-net-gen-mas)# port port_number
```

The default is 80/443 if not specified.

**Step 11** Set the status of whether or not the host uses TLS/SSL:

```
sensor(config-net-gen-mas)# tls [true | false]
sensor(config-net-gen-mas)
```




---

**Note** If you set the value to true, you need to use the command **tls trusted-host ip-address mbs\_ip\_address**.

---

**Step 12** Exit network access submode:

```
sensor(config-net-gen-mas)# exit
sensor(config-net-gen)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:[yes]:
```

**Step 13** Press **Enter** to apply the changes or type **no** to discard them.

**Step 14** On the master blocking sensor, add the block forwarding sensor's IP address to the access list. For the procedure, see [Changing the Access List, page 4-5](#).

## Configuring Manual Blocking

Use the **block-hosts** and **block-networks** commands in the service network access submode to manually block a host or a network. You must have blocking configured before you can set up manual blocks. You can also view a list of hosts and networks that are being blocked.



### Note

Manual blocks in the CLI are actually changes to the configuration, so they are permanent. You cannot do a timed manual block. You cannot use the IPS manager to delete blocks created by the CLI. Manual blocks have to be removed in the CLI.



### Caution

We recommend that you use manual blocking on a very limited basis, if at all.

To manually block a host or a network, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Enter network access mode:

```
sensor# configuration terminal
sensor(config)# service network-access
```

**Step 3** Enter general mode:

```
sensor (config-net)# general
```

**Step 4** Start the manual block:

a. For a host IP address:

```
sensor(config-net-gen)# block-hosts ip_address
```

b. For a network IP address:

```
sensor(config-net-gen)# block-networks ip_address/netmask
```

The format for *ip\_address/netmask* is A.B.C.D/nn.

Example:

```
sensor (config-net-gen)# block-networks 10.0.0.0/8
```



**Note** You must end the manual block in the CLI or it is permanent.

**Step 5** To end the manual block:

```
sensor (config-net-gen)# no block-hosts ip_address
```

**Step 6** Exit network access submode:

```
sensor (config-net-gen)# exit
sensor (config-net)# exit
sensor (config)# exit
sensor#
```

## Obtaining a List of Blocked Hosts and Connections

Use the **show statistics** command to obtain a list of blocked hosts and blocked connections.

To obtain a list of blocked hosts and connections, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Check the statistics for Network Access Controller:

```
sensor# show statistics network-access
Current Configuration
  LogAllBlockEventsAndSensors = true
  EnableNvramWrite = false
  EnableAclLogging = false
  AllowSensorBlock = false
  BlockMaxEntries = 250
  MaxDeviceInterfaces = 250
  NetDevice
    Type = Cisco
    IP = 10.1.1.1
    NATAddr = 0.0.0.0
    Communications = telnet
  BlockInterface
    InterfaceName = fa0/0
    InterfaceDirection = in
State
  BlockEnable = true
  NetDevice
    IP = 10.1.1.1
    AclSupport = uses Named ACLs
    Version = 12.2
    State = Active
```

```
BlockedAddr
Host
  IP = 192.168.1.1
  Vlan =
  ActualIp =
  BlockMinutes = 80
  MinutesRemaining = 76
```

The `Host` entry indicates which hosts are being blocked and how long the blocks are.

---

