IDS Device Manager Configuration Tasks

After configuring system information, you are ready to configure signatures, set up blocking, set up automatic signature updates, and restore defaults.

The following sections describe how to configure these options through the Configuration tab:

Configuring Signatures

You can create system variables, create event filters, and tune signatures through the Sensing Engine.

The following sections describe how to configure signatures through the Sensing Engine:

Explaining Signatures

Attacks or other misuses of network resources can be defined as network intrusions. Network intrusions can be detected by sensors that use a signature-based technology. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alarm to IDS Event Viewer. Sensors allow you to modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your sensors.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install IDS Device Manager. When an attack is detected that matches an enabled signature, the sensor generates an alert event (formerly known as an alarm), which is stored in the sensor's event store. The alert events, as well as other events, may be retrieved from the event store by web-based clients. By

default the sensor logs all Informational alarms or higher. If you have added IDS Event Viewer as a destination, the alarm is sent to the IDS Event Viewer database and you can view the alarm in IDS Event Viewer.

Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature. For example, if you edit signature 3050 subsignature 1 and change the severity, the severity change applies to only subsignature 1 and not to 3050 2, 3050 3, and 3050 4.

Built-in signatures are known attack signatures that are included in the sensor software and are enabled by default. You cannot add to or delete from the list of built-in attack signatures. You also cannot rename them. You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called *tuned* signatures.

You can create new signatures, which are called *custom* signatures. Custom signature IDs begin at 20000. You can configure them for any number of things, such as matching of strings on UDP connections, tracking of network floods, and scans. Each signature is created using a signature engine specifically designed for the type of traffic being monitored.

Configuring Alarm Channel System Variables

Alarms are sent to the alarm channel, where they are filtered and aggregated. You cannot select the alarm channel, because there is only one alarm channel in version 4.0.

You can change the value of an alarm channel system variable, but you cannot add variables or delete variables. You also cannot change the name, type, or constraints of a variable.

For all the Sensing Engine panels, you must click the **Save Changes** icon on the Activity bar to apply your new configuration.

You use the system variables when configuring alarm channel event filters. When you want to use the same value within multiple filters, use a variable. When you change the value of a variable, the variables in all the filters are updated. This saves you from having to change the variable repeatedly as you configure alarm filters. See Configuring Alarm Channel Event Filters, page 3-6, for more information.

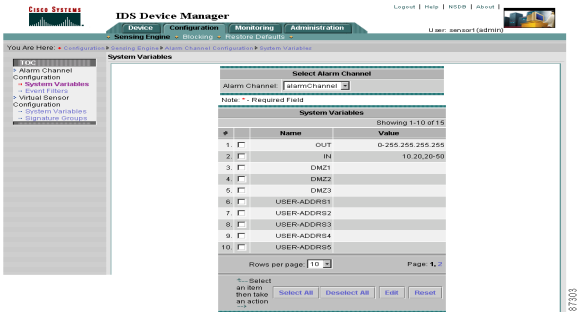
For example, if you had an IP address space that applied to your engineering group and there were no Windows systems in that group, and you were not worried about any Windows-based attacks, you could set up a USER-ADDR1 to be the engineering group's IP address space. You could then use this variable on the Event Filters page to set up the filter to ignore all Windows-based attacks for USER-ADDR1.

To define alarm channel system variables, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Alarm Channel Configuration > System Variables**.

The System Variables page appears.

Figure 3-1 System Variables Page

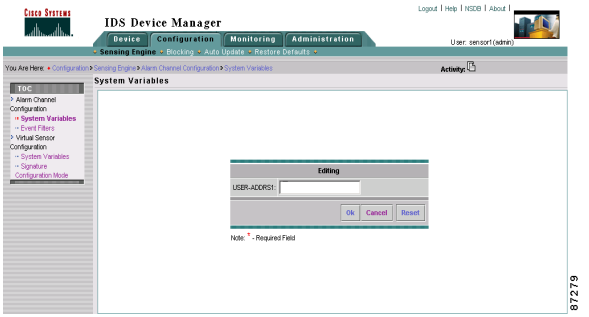


Step 2 Select the check box next to the system variable you want to edit, and then click **Edit**.

The Editing page appears for the variable that you chose.

Note You can edit only one variable at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

Figure 3-2 Editing Page



Step 3 Fill in the following values for the following system variables (according to the one that you are editing):

- OUT

  OUT is defined as anything that is not included in IN. You cannot edit this variable. The default is 0–255.255.255.255.

- IN

  IN is a list of all internal IP address spaces. Enter your internal IP addresses.

- DMZ1, DMZ2, and DMZ3

  You can use DMZ to define any valid IP address. These are named DMZ for you to use with filtering signatures that pertain to firewalls.

- USER-ADDRS1, USER-ADDRS2, USER-ADDRS3, USER-ADDRS4, and USER-ADDRS5

  You can use USER-ADDR to define any valid IP address. You can set up a USER-ADDR variable to apply to any group of IP addresses that you want to use a filter on.

- SIG1, SIG2, SIG3, SIG4, and SIG5

  You can use SIG to define popular signatures that you like to exclude for certain addresses.

Note To reset the form, click **Reset**.

Step 4 Click **Ok**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 5 Click the **Save Changes** icon in the Activity bar to save your system variables.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." In a few minutes, click **Alarm Channel Configuration** > **System Variables** again to see the edited variable in the list.

The new value appears in the Value column.

Step 6 Repeat Steps 2 though 5 to edit additional system variables.

Configuring Alarm Channel Event Filters

You can configure event filters that are based on source and destination addresses for specified signatures. You can use the alarm channel system variables that you defined on the Alarm Channel System Variables page to group addresses for your filters.

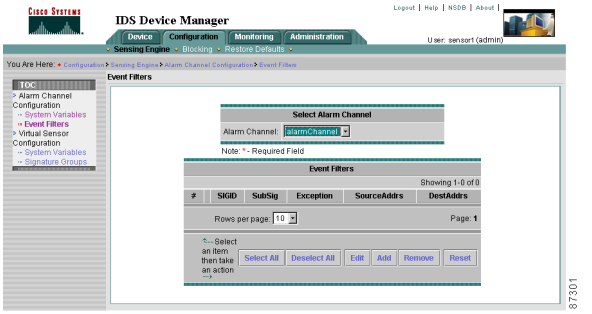
For all the Sensing Engine panels, you must click the **Save Changes** icon on the Activity bar to apply your new configuration.

To configure alarm channel event filters, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters**.

The Event Filters page appears.

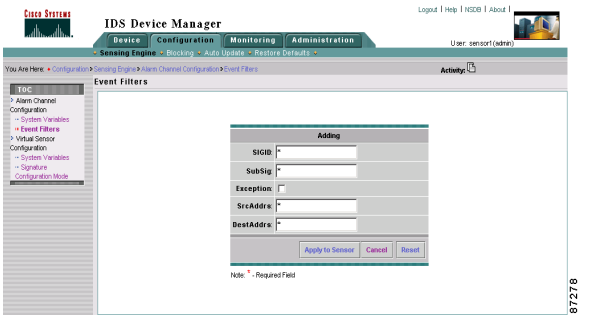
Figure 3-3 Event Filters Page



Step 2 Click **Add** to add an event filter.

The Adding page appears.

Figure 3-4 Adding Page



Step 3 In the SIGID field, enter the signature IDs of the events to which this filter should be applied.

You can use a list (2001, 2004), or a range (2001–2004), an asterisk (*) for all signatures, or one of the SIG variables if you defined them on the Alarm Channel System Variables page.

Step 4 In the SubSig field, enter the subsignature IDs of the events to which this filter should be applied.

Step 5 In the Exception field, enter the exception (Boolean) to the event filter.

Note If the filter describes an exception to an event filter, you can create a "general case" exclusion rather than adding more specific information.

Step 6 In the SrcAddrs field, enter the source addresses of events to which this filter should be applied.

You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page.

Step 7 In the DestAddrs field, enter the destination addresses of events to which this filter should be applied.

You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor**.

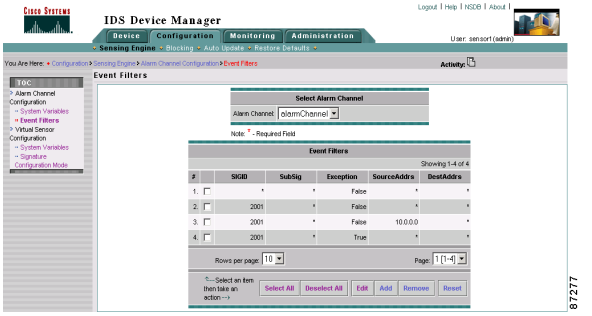
Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 9 Click **Saves Changes** on the Activity bar to save your changes.

Note A message displays "Configuration information is not available at this time. Try again in a few minutes." After a few minutes, click **Event Filters** again to see the filter you added.

The filtered signature appears on the Event Filters page.

Figure 3-5 Added Event Filters Page



Step 10 To remove the filter, select the check box next to the signature and click **Remove**.

Configuring Virtual Sensor System Variables

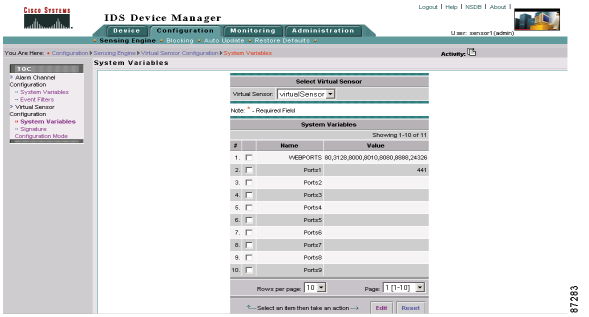
You can change the value of a system variable but you cannot add variables or delete variables. You cannot change the name or type of a variable. You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

To configure the virtual sensor system variables, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Virtual Sensor Configuration > System Variables**.

The System Variables page appears.

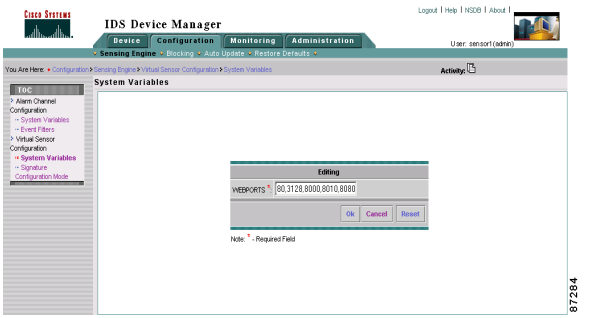
Figure 3-6 System Variables Page



Step 2 Select the system variable that you want to edit and click **Edit**.

The Editing page appears.

Figure 3-7 Editing Page



Step 3 Fill in the value of the system variable that you want to edit:

Note You can edit only one system variable at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

- WEBPORTS

  WEBPORTS has a predefined set of ports where web servers are running, but you can edit the value. This variable affects all signatures that have web ports. The default is 80, 3128, 8000, 8010, 8080, 8888, 24326.

- Ports1, Ports2, Ports3, Ports4

  You can set up a list of ports to apply to particular signatures.

- ADDRS1, ADDRS2, ADDRS3, ADDRS4

  You can set up this variable with a list of addresses to use anywhere you can use IP addresses.

- IPReassembleMaxFrags

  You can define the total number of fragments you want the system to queue. You can define a number between 1000 and 50,000. The default is 10,000.

Note To reset the form, click **Reset**.

Step 4 Click **OK**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 5 Click the **Save Changes** icon on the Activity bar to save your system variables.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." After a few minutes, click **Virtual Sensor Configuration > System Variables** to see the edited variable.

The new value appears in the Value column.

Step 6 Repeat Steps 2 though 5 to edit additional system variables.

Working with Virtual Sensor Signature Configuration Mode

The Signature Configuration Mode page displays a list of top level categories of signature groups for the virtual sensor. You can see all the signatures in the list or you can see signatures that are grouped according to their signature engine type. Certain signatures are enabled by default to provide you immediately with a certain level of security. When you modify a built-in signature, it becomes a tuned signature. You can also create signatures, which are called custom signatures.

You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

You can display all individual signatures at once by clicking **All Signatures**. If you are looking for a particular signature, click **All Signatures**, and use the browser's search option to find the string you are looking for—the signature ID or the signature name.

You can display the signature list within a group by clicking the group name. Each group displays its enable level (the disabled, partially enabled, or enabled icon). You can enable or disable one, some, or all signatures within the group. To select the signature for enabling or disabling, select the signature check box.

You can tune built-in signatures. To tune a signature, select the check box and click **Edit**. Some signatures have subsignatures, which you can edit individually to have more control over the signature. You can create custom signatures, and then delete one, some, or all custom signatures. To create a custom signature, choose the correct signature engine, and then click Add and configure the signature parameters. For more information on signature engines and their parameters, see Appendix A, "Working With Signature Engines."

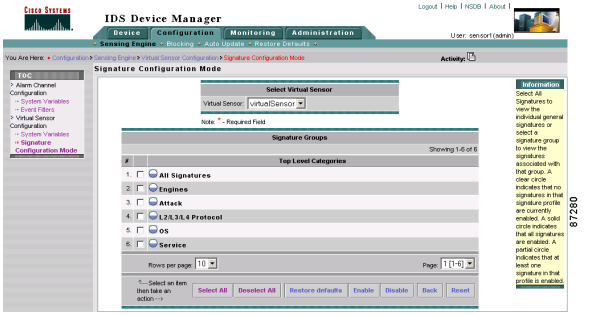
A signature can be in multiple groups. Editing a signature in one group, affects it in all groups. For example, if you enable all general attack signatures in the Attack category, it will enable 7107. If you disable the ATOMIC.ARP signature in the Engine category, 7107 will be disabled. Whichever action is the last one, is the one that is applied.

To configure virtual sensor signature groups, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode**.

The Signature Groups page appears.

Figure 3-8 Signature Groups Page



Step 2 To enable or disable all signatures in a group, select the check box next to the signature group, and then click **Enable** or **Disable**.

Note A clear circle indicates that no signatures in that signature group are enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that group is enabled.

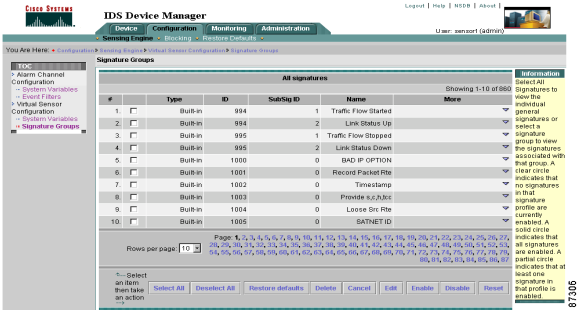
Note Click **Restore Defaults** to return the signature group to its default settings.

Step 3 You can click **All Signatures** to display all the IDS signatures or you can click a signature group name.

The All Signatures page appears.

Note If you select **All** in the Rows per page list box, it can take some time for all signatures to display.

Figure 3-9 All Signatures Page



The All Signatures page contains the following:

- Enabled or Disabled icon
- Signature ID
- Subsignature ID
- Signature name
- Type (built-in, tuned, custom)
- Severity level (Informational, Low, Medium, High)
- Action
- More (lists all the signature parameters; these appear when you edit the signature)

Step 4 Select the check box(es) next to the signatures that you want to perform an action on:

Note You can edit only one signature at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

- To enable or disable the signature(s), click **Enable** or **Disable**.

Caution Signatures can belong to more than one group. Enabling or disabling signatures in one group also affects those signatures that belong to other groups.

- To restore the defaults to a signature(s), click **Restore Defaults**.
- To delete a signature(s), click **Delete**.

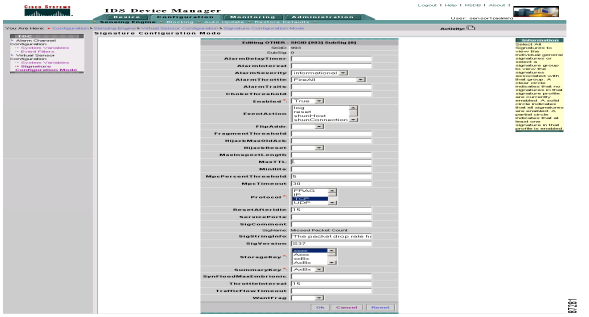
Note You cannot delete built-in or tuned signatures, only custom signatures.

- To edit the signature(s), click **Edit**.

The Editing page appears.

This is where you tune built-in signatures. You can see the definition of each parameter by passing your mouse over the parameter. Some parameters are required (red asterisk), others have menu lists you can choose from, for others you must add text. For a detailed description of signature engines and parameters, see Appendix A, “Working With Signature Engines.”

Figure 3-10 Editing Page



Step 5 Click **Ok** to save the changes you made to the built-in signature.

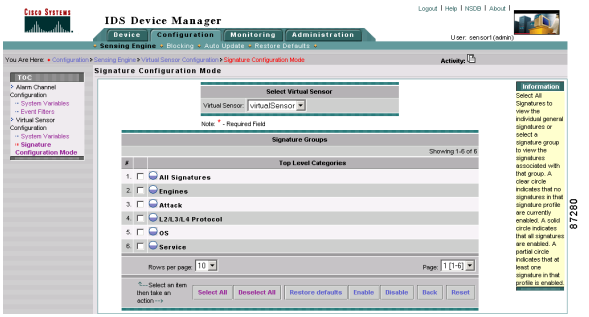
The Type has changed from Built-in to Tuned on the All Signatures page.

Note Use the **Back** button at the bottom of the page as you tune or create multiple signatures.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

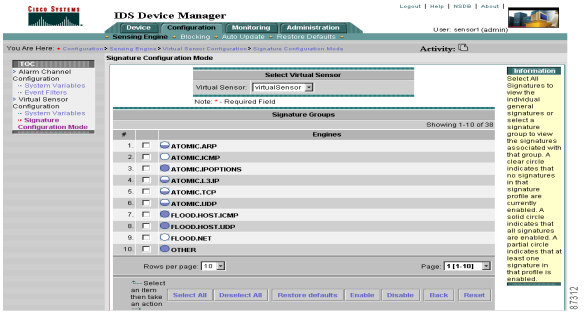
Step 6 To create a custom signature, click the Engines category on the Signature Groups page.

Figure 3-11 Signature Groups Page



The Engines page appears.

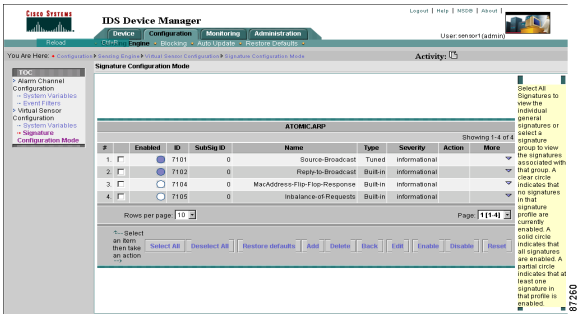
Figure 3-12 Engines Page



Step 7 Click the engine you want to use to create a custom signature, for example, **ATOMIC.ARP**.

The ATOMIC.ARP page appears.

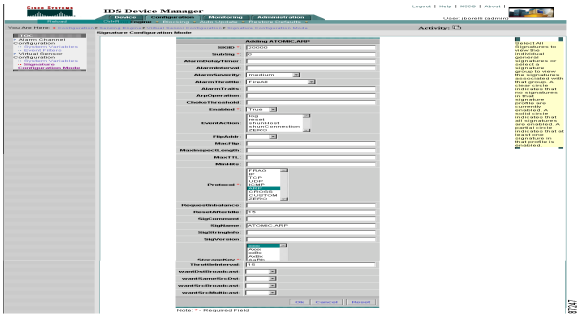
Figure 3-13 ATOMIC.ARP Page



Step 8 Click **Add**.

The Adding page appears.

Figure 3-14 Adding ATOMIC.ARP Page

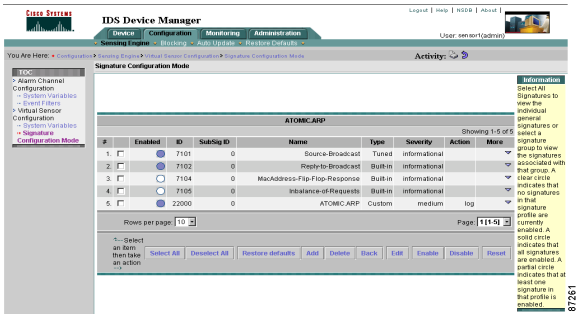


Step 9 Fill in the parameters that you want, and then click **OK**.

Note For a detailed description of signature engines and parameters, see Appendix A, "Working With Signature Engines."

A note tells you that to add the signature you must click **Save Changes** on the Activity bar (see Step 10). The ATOMIC.ARP page appears with the custom signature in the list.

Figure 3-15 ATOMIC.ARP Page with Custom Signature



Step 10 Click the **Save Changes** icon on the Activity bar to save your changes.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." Click **Virtual Sensor Configuration** > **Signature Configuration Mode** to return to the Signature Configuration Mode page. Click **All Signatures** or the relevant signature group to see the tuned signature in the list.

The built-in signature that you edited now shows Tuned in the Type column.

Identifying Traffic Oversubscription

Signature 993 alarms tell you if the sensor is dropping packets and the percentage dropped to help you tune the traffic level you are sending to the sensor. For example, if the alarms show that there is zero or a very small percentage of dropped packets, the sensor is able to monitor the quantity of traffic being sent.

If you are seeing 993 alarms with a higher percentage of dropped packets, your sensor is oversubscribed. When a sensor gets oversubscribed, it can have difficulty in detecting alarms in TCP streams in a nonlinear fashion. The percentage of streams that are affected by the dropped packets is not easy to predict. If you find that you are operating your sensor in an environment where it is oversaturated and you need to continue operating it in that environment, we recommend disabling the TCP3WayHandshake and setting TCPReassemblyMode to loose so that best security is ensured.

Signature 993, which is part of the signature engine OTHER, has the following configuration parameters:

- MpcInterval in seconds 5 <= MpcInterval <= 2500 (default = 30).

  MpcInterval is the interval between alarms.

- MpcPercentThreshold in percent 0 <= MpcPercentThreshold <= 100 (default = 0).

  MpcPercentThreshold is the percentage of missed packets that must be exceeded to trigger an alarm. A value of 100 percent disables this threshold.

- MpcAbsThreshold in packets 0 <= MpcAbsThreshold <= 65535 (default = 0).

  MpcAbsThreshold is the absolute number of missed packets that must be exceeded to trigger an alarm. A value of 65535 disables this threshold.

If either the MpcPercentThreshold or the MpcAbsThreshold is exceeded, the alarm is triggered.

Note If signature 993 is firing with 100 percent packet loss, the sensor is not generating alarms and there is a problem. Make sure that you have the most recent version of the sensor. If you have the most recent version, contact TAC to report the problem.

See OTHER Engine, page A-30, for more information on the OTHER signature engine.

Configuring Blocking

You can configure a sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6500 family switch, or by generating shun rules on a PIX Firewall.

The following sections describe how to set up blocking:

Configuring Blocking Properties

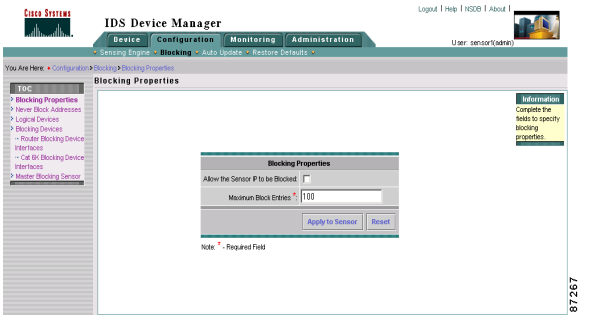
You set up global blocking properties for the Network Access Controller (NAC) on this page. NAC is responsible for controlling blocking actions on managed devices.

To configure blocking on the sensor, follow these steps:

Step 1 Select **Configuration > Blocking Properties**.

The Blocking Properties page appears.

Figure 3-16 Blocking Properties Page



Step 2 Do not select the Allow the Sensor IP to be Blocked check box unless necessary.

Caution We suggest that you do not allow the sensor to block itself, because it will stop communicating with the managed device. You can select 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.

Step 3 In the Maximum Block Entries field, enter how many blocks are to be maintained simultaneously (0 to 250).

Note We do not recommend or support setting the maximum block entries higher than 250.

The default value is 100.

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.

Note To reset the form, click **Reset**.

Step 4 Click **Apply to Sensor** to save your changes.

Configuring Addresses Never To Block

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. But such a device should never be blocked, and trusted, internal networks should never be blocked. Properly tuning signatures reduces the number of false positives and helps ensure proper network operations. Tuning and filtering signatures prevents alarms from being generated. If an alarm is not generated, the associated block does not occur.

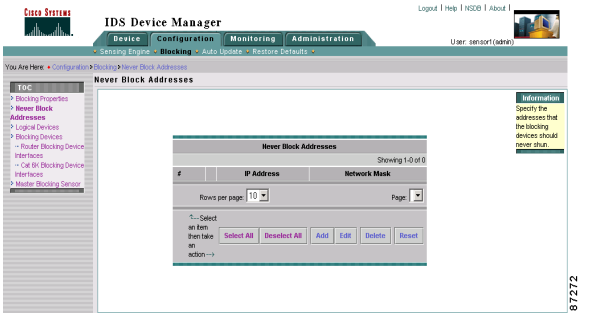
If you specify a netmask, this is the netmask of the network that should never be blocked. If no netmask is specified, only the IP address you specify will never be blocked.

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

Step 1 Select **Configuration > Never Block Addresses**.

The Never Block Addresses page appears.

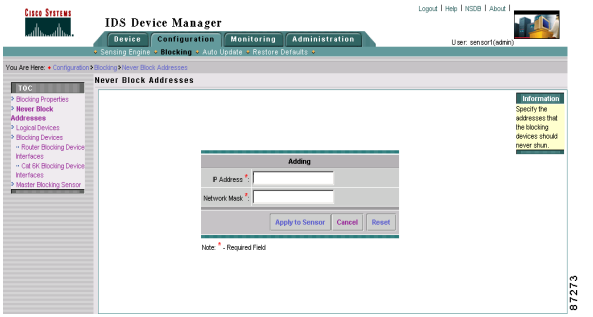
Figure 3-17 Never Block Addresses Page



Step 2 Click **Add** to add addresses that should never be blocked.

The Adding page appears.

Figure 3-18 Adding Page



Step 3 In the IP Address field, enter the IP address of the host that should never be blocked.

Step 4 In the Network Mask field, enter the network mask of the network that should never be blocked.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save your changes.

Setting Up Logical Devices

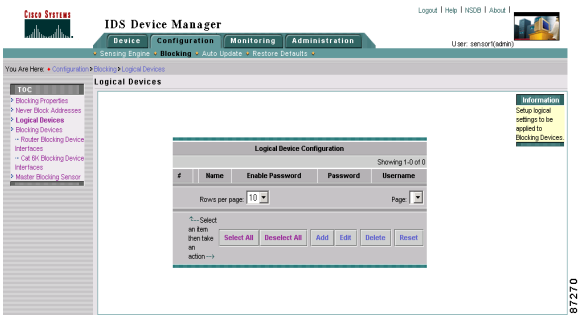
You can add logical devices that the senor will manage. For example, routers that all share the same passwords and usernames can be under one logical device name.

To set up logical devices, follow these steps:

Step 1 Select **Configuration > Logical Devices**.

The Logical Devices Configuration page appears.

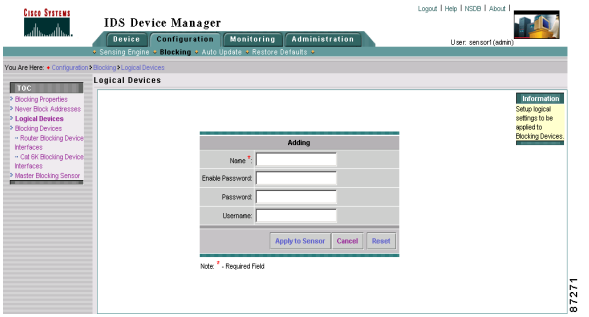
Figure 3-19 Logical Device Configuration Page



Step 2 Click **Add** to add the logical devices that the sensor will manage.

The Adding page appears.

Figure 3-20 Adding Page



Step 3 In the Name field, enter the name of the logical device.

Step 4 In the Enable Password field, enter the enable password for the logical device (1 to 16 characters).

Note If there is no enable password, enter **none**.

Step 5 In the Password field, enter the Telnet or SSH password for the logical device (1 to 16 characters).

Note If there is no password, enter **none**.

Step 6 In the Username field, enter the username for the logical device.

Note If there is no username, enter **none**.

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

Configuring Blocking Devices

You can configure your sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6500 switch, or by generating shun rules on a PIX Firewall. The router, switch, or firewall is called a blocking device.

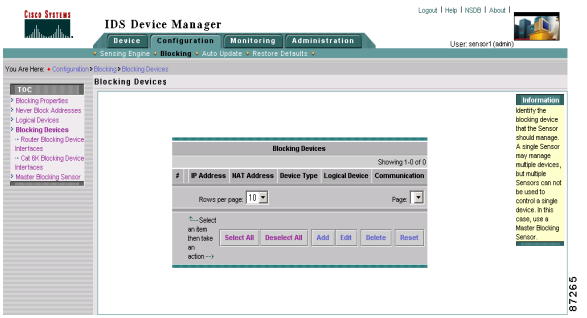
To configure blocking devices, follow these steps:

Step 1 Select **Configuration > Blocking Devices**.

The Blocking Devices page appears.

Caution A single sensor can manage multiple devices, but multiple sensors cannot be used to control a single device. In this case, use a master blocking sensor. See Configuring a Master Blocking Sensor, page 3-31, for more information.

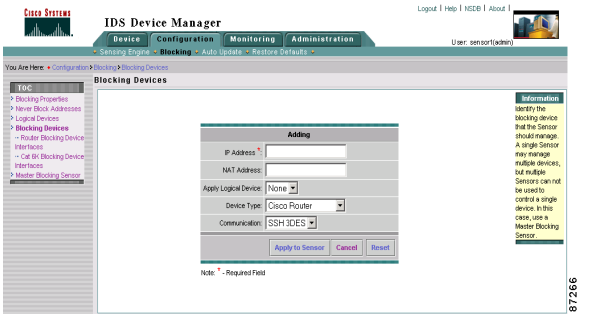
Figure 3-21 Blocking Devices Page



Step 2 Click **Add** to add a blocking device.

The Adding page appears.

Figure 3-22 Adding Page



Step 3 In the IP Address field, enter the IP address of the blocking device.

Step 4 In the NAT Address field, enter the NAT address of the blocking sensor.

Step 5 Select an option from the Apply Logical Device list box.

Note The same logical device can be used for multiple blocking devices. If you do not have logical devices set up, the only option is None.

Step 6 In the Device Type field, enter the type of device that will do the blocking:

- Cisco Router
- Catalyst 6000 VACL
- PIX Firewall

Step 7 In the Enable SSH field, select the type of secure communications you want to enable between the sensor and the blocking device:

- SSH 3DES
- SSH DES
- Telnet

Note Before you can use SSH 3DES or SSH DES, you have to use the **ssh host-key** *ipaddress* to obtain the public key in the correct format so that you can add the host to the known hosts list. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0* for the procedure.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Configuring Router Blocking Device Interfaces

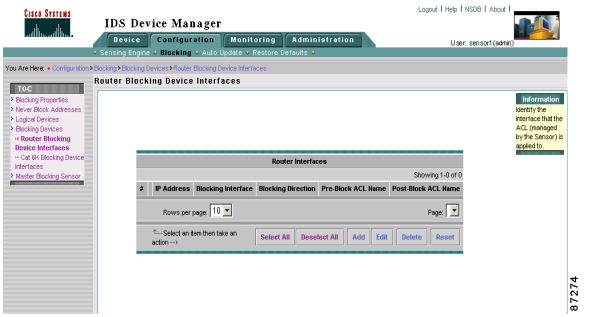
You must configure the blocking interfaces on the router and specify the direction of traffic you want blocked.

To configure the blocking interfaces on a router, follow these steps:

Step 1 Select **Configuration > Router Blocking Device Interfaces**.

The Router Blocking Device Interfaces page appears.

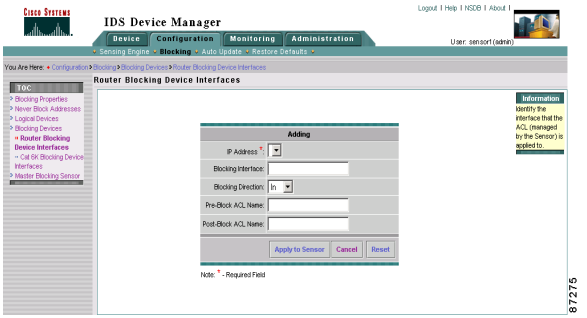
Figure 3-23 Router Blocking Device Interfaces Page



Step 2 Click **Add** to configure the blocking interfaces on the router.

The Adding page appears.

Figure 3-24 Adding Panel



Step 3 In the IP Address field, enter the IP address of the router that will be used to block.

Step 4 In the Blocking Interface field, enter the interface on the router that will be used for blocking (1 to 32 characters).

Step 5 From the Blocking Direction list box, select the direction of the traffic through the interface that should be blocked (In, Out).

Step 6 In the Pre-Block ACL Name field, enter the name of the Pre-Block ACL (1 to 64 characters).

Step 7 In the Post-Block ACL Name field, enter the name of the Post-Block ACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Configuring Catalyst 6K Blocking Device Interfaces

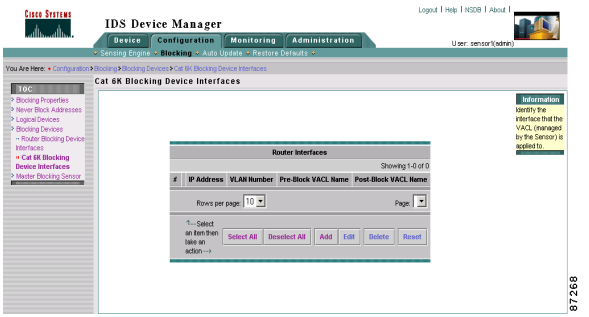
You must configure the blocking interfaces on the Catalyst switch and specify which VLAN you want blocked.

To configure the blocking interfaces on a Catalyst switch, follow these steps:

Step 1 Select **Configuration > CAT 6K Blocking Device Interfaces**.

The CAT 6K Blocking Device Interfaces page appears.

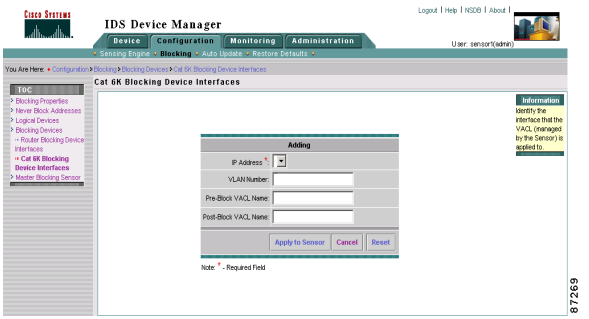
Figure 3-25 CAT 6K Blocking Device Interfaces Page



Step 2 Click **Add** to configure the blocking interfaces on the router.

The Adding page appears.

Figure 3-26 Adding Page



Step 3 In the IP Address field, enter the IP address of the Catalyst switch that will be used to block.

Step 4 In the VLAN field, enter the VLAN number that the sensor will configure for blocking.

Step 5 In the Pre-Block VACL Name field, enter the name of the Pre-Block VACL (1 to 64 characters).

Step 6 In the Post-Block VACL Name field, enter the name of the Post-Block VACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

Configuring a Master Blocking Sensor

Multiple sensors can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The sensor that is sending its block requests to the master blocking sensor is referred to as a "blocking forwarding sensor." On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

Note Only the master blocking sensor is configured to manage the network devices. The blocking forwarding sensor should not be configured to manage network devices.

See Setting Up a Blocking Forwarding Sensors, page 3-33, for the procedure to configure the blocking forwarding sensor.

To configure blocking forwarding sensors to a master blocking sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts**.

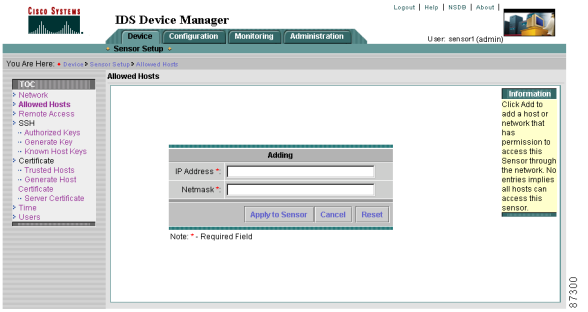
The Allowed Hosts page appears.

Figure 3-27 Allowed Hosts Page

Step 2 Click **Add** to add a sensor as a blocking forwarding sensor.

The Adding page appears.

Figure 3-28 Adding Page



Step 3 In the IP Addressfield, enter the IP address of the blocking forwarding sensor.

Step 4 If you are using SSH, the port number is the same port number that the master blocking sensor is using for IDM connections.

Note For example, if you are connecting using https, it is port 443 by default.

Step 5 In the User Name field, enter your IDS Device Manager administrator username.

Step 6 In the Password field, enter your IDS Device Manager administrator password.

Step 7 If you select Use SSH, you have to use the **tls trusted-host ip-address** *ipaddress* command.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Note Repeat this procedure for each sensor you want to identify as a blocking forwarding sensor.

Setting Up a Blocking Forwarding Sensors

The blocking forwarding sensor sends block requests to the master blocking sensor. On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor.

See Configuring a Master Blocking Sensor, page 3-31, for more information on how to set up a master blocking sensor.

To set up a blocking forwarding sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts**.

The Allowed Hosts page appears.

Figure 3-29 Allowed Hosts Page

Step 2 Click **Add** to add a sensor as a master blocking sensor.

The Adding page appears.

Figure 3-30 Adding Page

Step 3 In the IP Address field, enter the IP address of the master blocking sensor.

Step 4 In the Netmask field, enter the netmask of the master blocking sensor.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save your changes.

The master blocking sensor is added to both the Allowed Hosts page and to the Master Blocking Sensor page.

Configuring Automatic Updates

You can configure automatic service pack and signature updates, so that when service pack and signature updates are loaded on a central FTP or SCP server, they will be downloaded and applied to your sensor. The timeout default is 5 minutes.

Note The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server.

See Supported FTP Servers, page 3-37, for a list of supported servers.

To configure automatic updates, follow these steps:

Step 1 Select **Configuration** > **Auto Update**.

The Auto Update page appears.

Figure 3-31 Auto Update Page

Step 2 Select the Enable Auto Update check box to enable automatic updates.

Step 3 In the IP Address field, enter the IP address of the server to poll for updates.

Step 4 In the Directory field, enter the path to the directory on the server where the updates are located (1 to 128 characters).

Step 5 In the Username field, enter the username to use when logging in to the server (1 to 16 characters).

Step 6 In the Password field, enter the username password on the server (1 to 16 characters).

Step 7 In the File Copy Protocol list box, select either **SCP** or **FTP**.

Step 8 For hourly updates, select **Hourly**, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start (hh:mm:ss).

b. In the Frequency field, enter the hour interval at which you want every update to occur (1 to 8760).

For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates.

Step 9 For calendar updates, select **Calendar**, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start (hh:mm:ss).

b. In the Day field, select the day(s) you want to download updates.

Note To reset the form, click **Reset**.

Step 10 Click **Apply to Sensor** to save your changes.

Supported FTP Servers

The following FTP servers are supported for service pack and signature updates:

- Sambar FTP Server Version 5.0 (win32).
- Web-mail Microsoft FTP Service Version 5.0 (win32).
- Serv-U FTP-Server v2.5h for WinSock (win32).
- Solaris 2.8.
- HP-UX (HP-UX qdir-5 B.10.20 A 9000/715).
- Windows 2000 (Microsoft ftp server version 5.0).
- Windows NT 4.0 (Microsoft ftp server version 3.0).

Note The sensor cannot download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

Restoring Default Settings

You can restore the default configuration to your sensor.

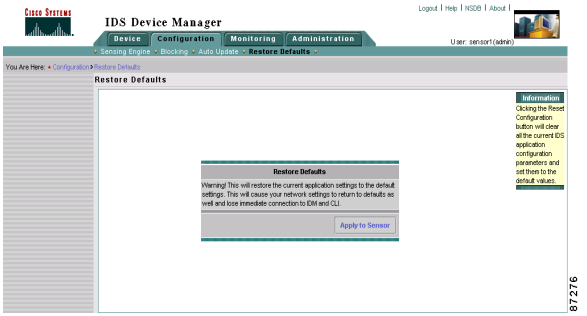
Warning **Clicking Apply to Sensor removes the current application settings and restores the default settings. Your network settings also return to the defaults and you immediately lose connection to IDS Device Manager and the CLI.**

To restore the default configuration, follow these steps:

Step 1 Select **Device > Configuration > Restore Defaults**.

The Restore Defaults page appears.

Figure 3-32 Restore Defaults Page



Step 2 Click **Apply to Sensor** to restore the default configuration.

The IP address, netmask, default gateway, allowed hosts, password, and time will not be reset. Manual and automatic blocks also remain in effect.