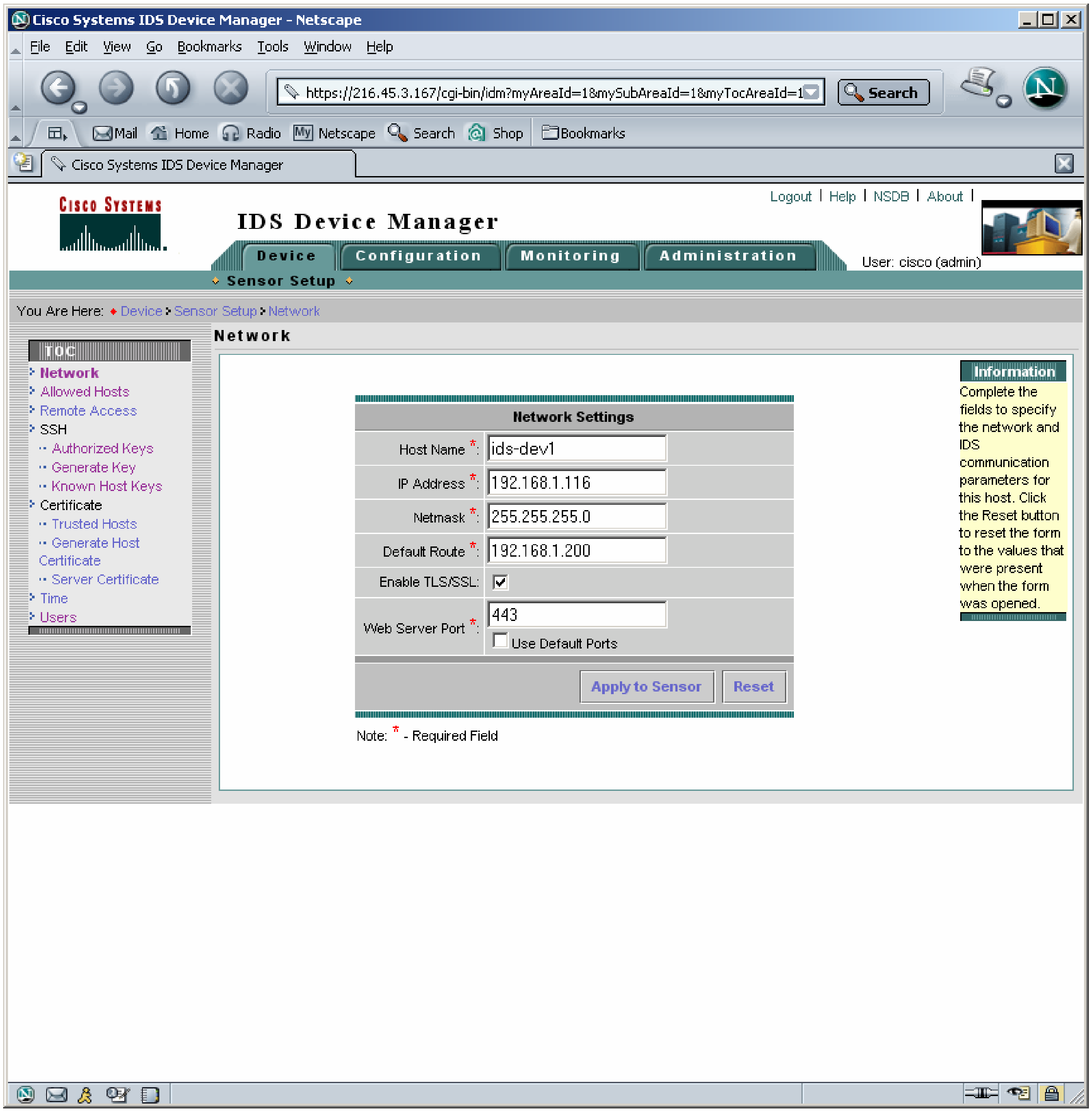
1. Configure the sensor's IP address using the VPN and IDS Visio. Configure the sensor to allow HTTPS access to the ACS/CA server. You may also use your home/work network. This server also runs IEV.
2. Configure the clock to use the current time. Set the time to Pacific Standard Time and allow for the sensor to automatically change the clock for daylight savings time. Clear all old events to make sure your logs are not timestamped improperly.
3. Configure the sensor to get NTP from R13.
4. Create an account that can tune signatures but cannot change the sensor's IP addresses or allowed hosts.
5. Create an account that can view configuration and events, but cannot make any configuration changes.
6. Create an account that can be used for specific troubleshooting purposes. This account cannot be allowed to logon to IDM.
7. Connect to IDM using HTTPS on port 8043.
8. Configure RSA authentication for SSH. Only allow clients that know the key to connect using SSH.
9. Tune the sensor so that you will see if the sensor is having performance problems. Specifically, if packets are being dropped.
10. Tune the sensor so that no alarms will be generated from hosts on the 66.124.87.40 network. This network includes hosts from .41 - .45.
11. You are getting several "WWW Solaris AnswerBook 2 attack" false positives from 66.124.87.41-45 network. Disable this signature from this specific network.
12. Increase the Active Perl PerlIS.dll Buffer Overflow to high priority.
13. Create a custom signature that detects when the text string "testattack" is typed in a Telnet session.
14. Configure the router at 192.168.1.254 to shun this connection or host.
15. Configure the sensor to update its signatures automatically. The ACS/CA server also runs FTP and has the latest signatures.

Question 1.



https://216.45.3.167/cgi-bin/idm?myAreaId=1&mySubAreaId=1&myTocAreaId=1

IDS Device Manager

User: cisco (admin)

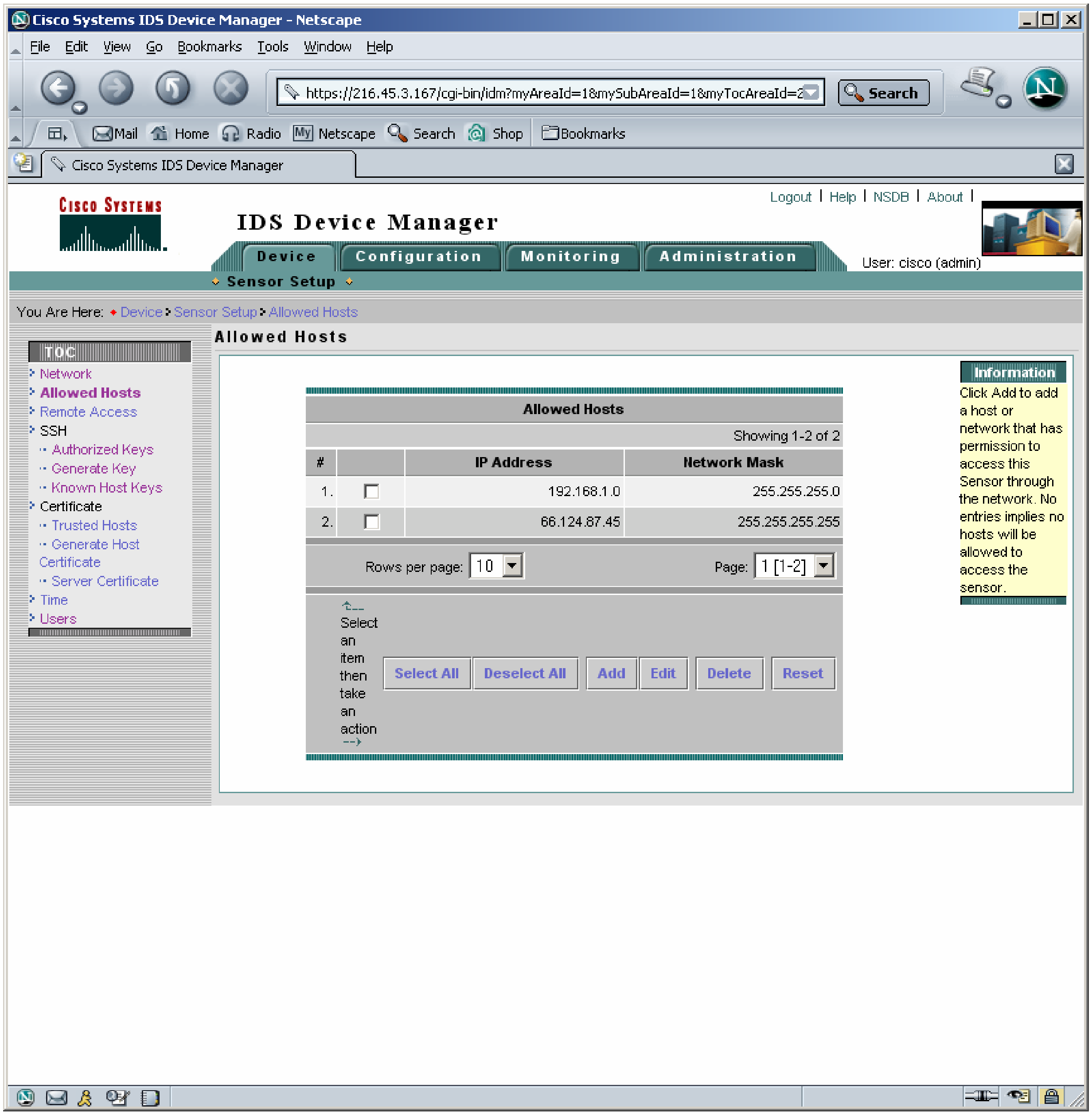
You Are Here: Device > Sensor Setup > Network

Network

Network Settings	
Host Name *:	ids-dev1
IP Address *:	192.168.1.116
Netmask *:	255.255.255.0
Default Route *:	192.168.1.200
Enable TLS/SSL:	☑
Web Server Port *:	443 □ Use Default Ports

Note: * - Required Field

Complete the fields to specify the network and IDS communication parameters for this host. Click the Reset button to reset the form to the values that were present when the form was opened.



https://216.45.3.167/cgi-bin/idm?myAreaId=1&mySubAreaId=1&myTocAreaId=2

IDS Device Manager

User: cisco (admin)

You Are Here: Device > Sensor Setup > Allowed Hosts

Allowed Hosts

Allowed Hosts

Showing 1-2 of 2

#		IP Address	Network Mask
1.	□	192.168.1.0	255.255.255.0
2.	□	66.124.87.45	255.255.255.255

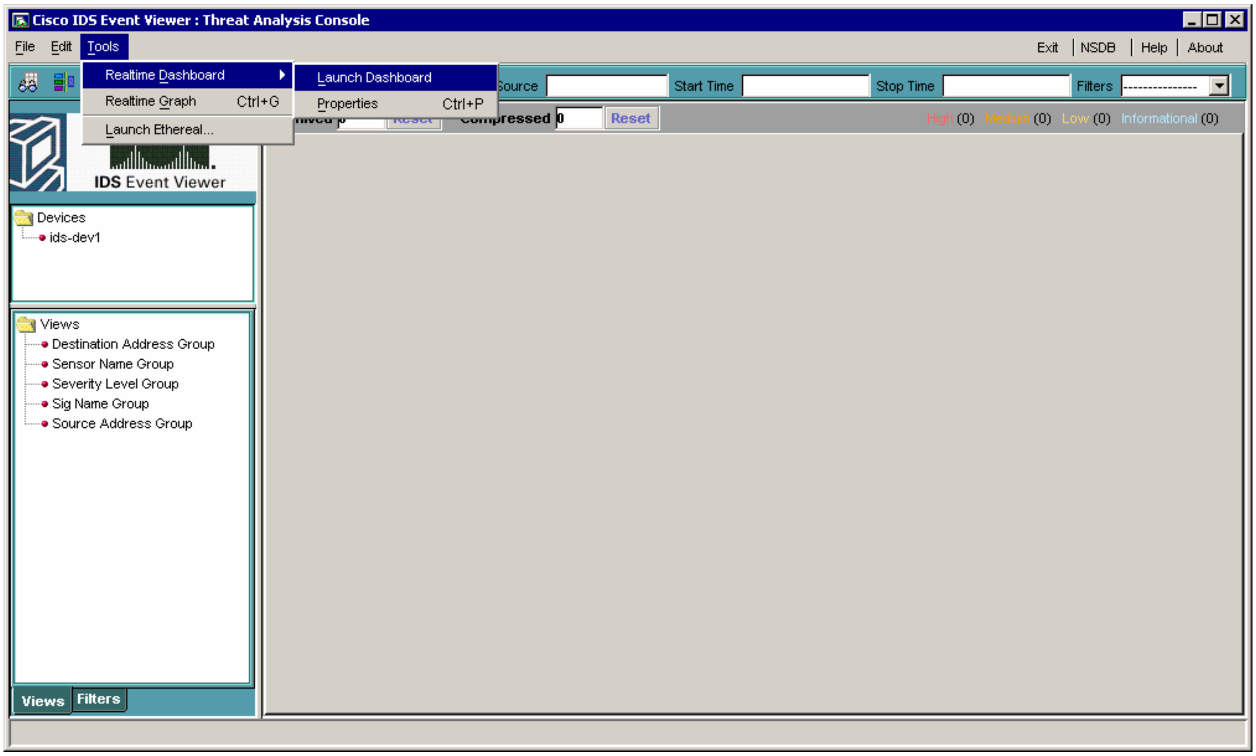
Rows per page: 10

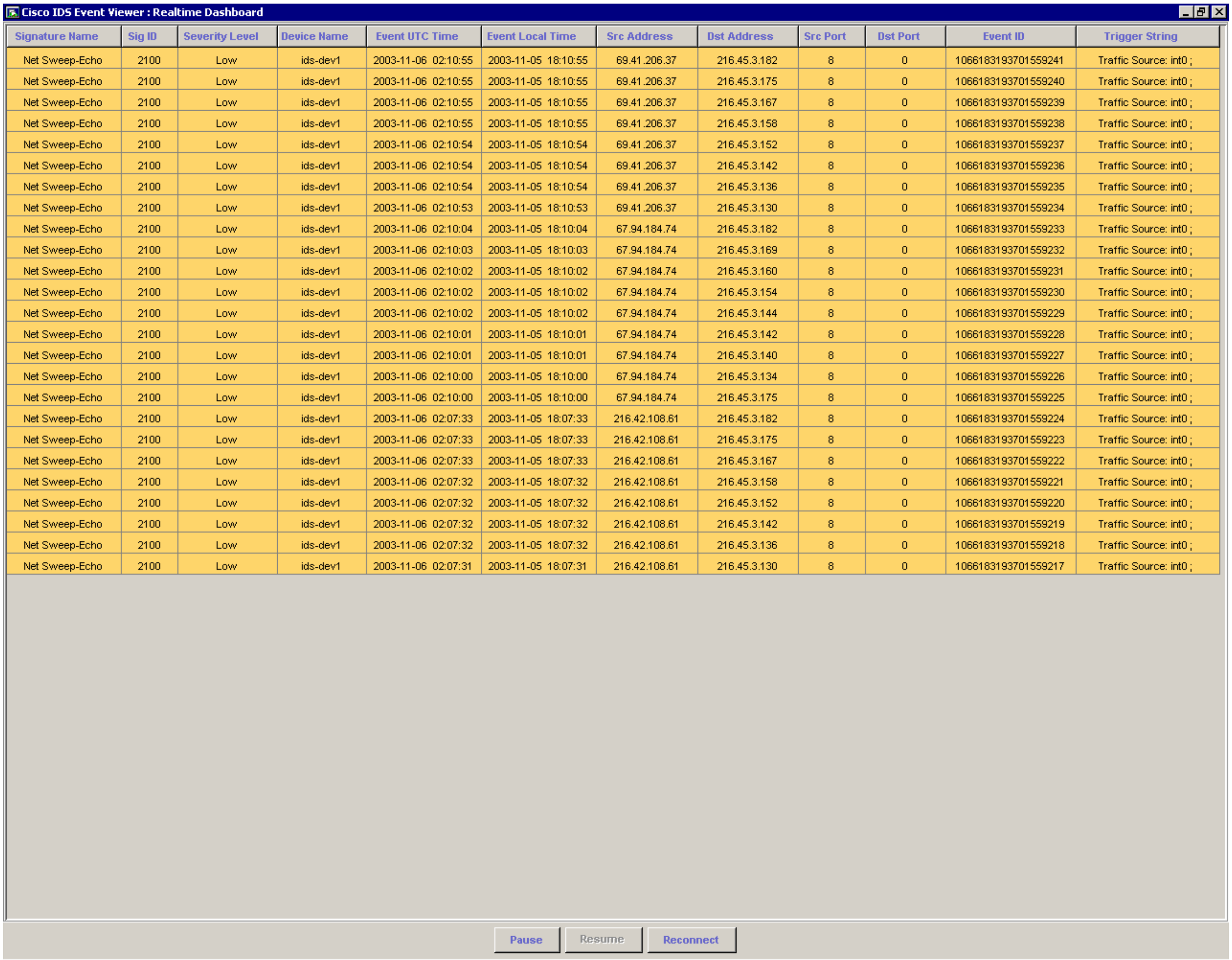
Page: 1 [1-2]

Select an item then take an action -->

Information

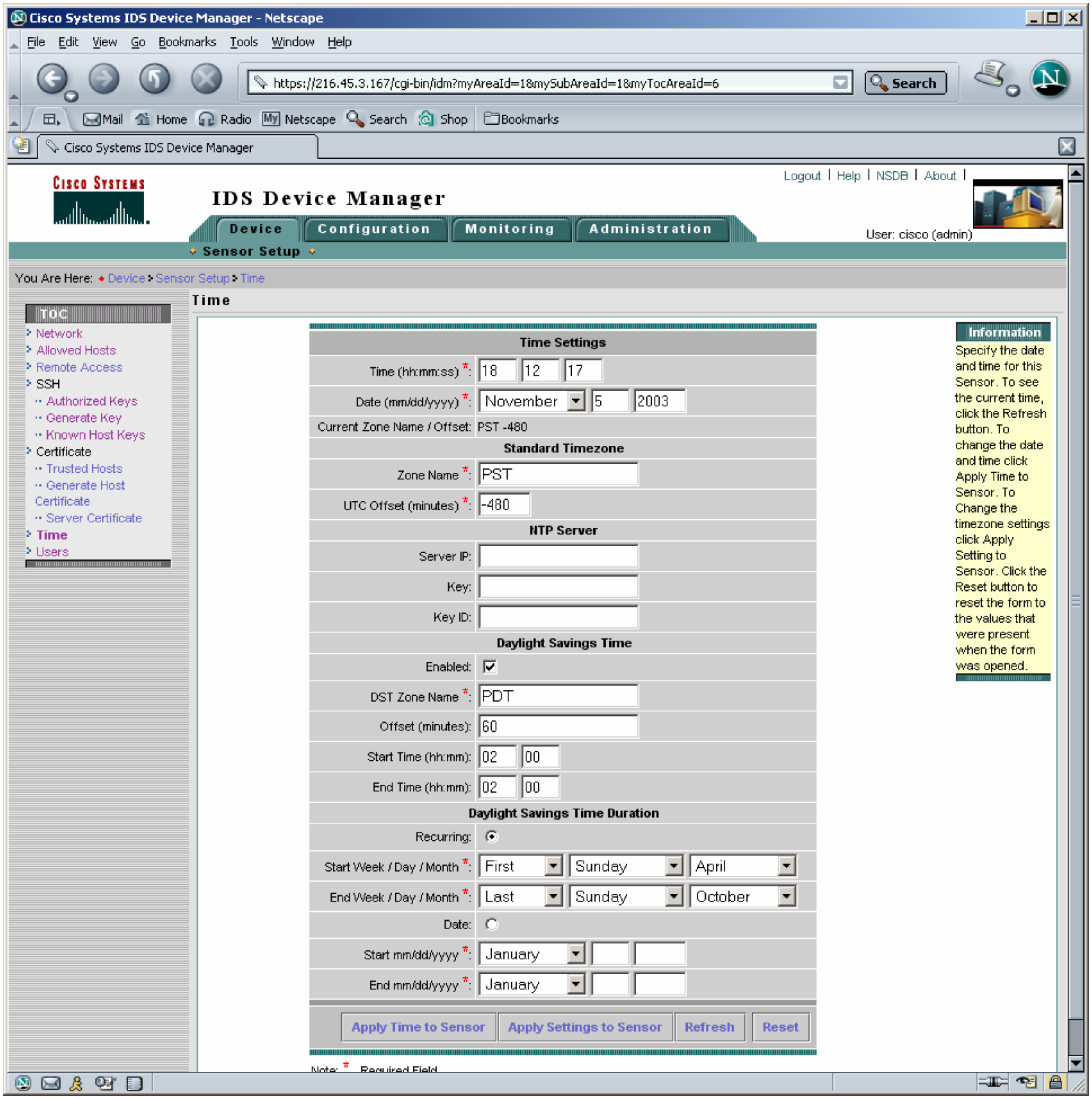
Click Add to add a host or network that has permission to access this Sensor through the network. No entries implies no hosts will be allowed to access the sensor.




Cisco IDS Event Viewer : Realtime Dashboard

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst Address	Src Port	Dst Port	Event ID	Trigger String
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:55	2003-11-05 18:10:55	69.41.206.37	216.45.3.182	8	0	1066183193701559241	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:55	2003-11-05 18:10:55	69.41.206.37	216.45.3.175	8	0	1066183193701559240	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:55	2003-11-05 18:10:55	69.41.206.37	216.45.3.167	8	0	1066183193701559239	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:55	2003-11-05 18:10:55	69.41.206.37	216.45.3.158	8	0	1066183193701559238	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:54	2003-11-05 18:10:54	69.41.206.37	216.45.3.152	8	0	1066183193701559237	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:54	2003-11-05 18:10:54	69.41.206.37	216.45.3.142	8	0	1066183193701559236	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:54	2003-11-05 18:10:54	69.41.206.37	216.45.3.136	8	0	1066183193701559235	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:53	2003-11-05 18:10:53	69.41.206.37	216.45.3.130	8	0	1066183193701559234	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:04	2003-11-05 18:10:04	67.94.184.74	216.45.3.182	8	0	1066183193701559233	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:03	2003-11-05 18:10:03	67.94.184.74	216.45.3.169	8	0	1066183193701559232	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:02	2003-11-05 18:10:02	67.94.184.74	216.45.3.160	8	0	1066183193701559231	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:02	2003-11-05 18:10:02	67.94.184.74	216.45.3.154	8	0	1066183193701559230	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:02	2003-11-05 18:10:02	67.94.184.74	216.45.3.144	8	0	1066183193701559229	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:01	2003-11-05 18:10:01	67.94.184.74	216.45.3.142	8	0	1066183193701559228	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:01	2003-11-05 18:10:01	67.94.184.74	216.45.3.140	8	0	1066183193701559227	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:00	2003-11-05 18:10:00	67.94.184.74	216.45.3.134	8	0	1066183193701559226	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:10:00	2003-11-05 18:10:00	67.94.184.74	216.45.3.175	8	0	1066183193701559225	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:33	2003-11-05 18:07:33	216.42.108.61	216.45.3.182	8	0	1066183193701559224	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:33	2003-11-05 18:07:33	216.42.108.61	216.45.3.175	8	0	1066183193701559223	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:33	2003-11-05 18:07:33	216.42.108.61	216.45.3.167	8	0	1066183193701559222	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:32	2003-11-05 18:07:32	216.42.108.61	216.45.3.158	8	0	1066183193701559221	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:32	2003-11-05 18:07:32	216.42.108.61	216.45.3.152	8	0	1066183193701559220	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:32	2003-11-05 18:07:32	216.42.108.61	216.45.3.142	8	0	1066183193701559219	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:32	2003-11-05 18:07:32	216.42.108.61	216.45.3.136	8	0	1066183193701559218	Traffic Source: int0 ;
Net Sweep-Echo	2100	Low	ids-dev1	2003-11-06 02:07:31	2003-11-05 18:07:31	216.42.108.61	216.45.3.130	8	0	1066183193701559217	Traffic Source: int0 ;

Question 2.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167/cgi-bin/idm?myAreaId=1&mySubAreaId=1&myTocAreaId=6
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager
Device Configuration Monitoring Administration
Sensor Setup
User: cisco (admin)
You Are Here: Device > Sensor Setup > Time
TOC
Network
Allowed Hosts
Remote Access
SSH
Authorized Keys
Generate Key
Known Host Keys
Certificate
Trusted Hosts
Generate Host Certificate
Server Certificate
Time
Users
Apply Time to Sensor
Apply Settings to Sensor
Refresh
Reset

Time

Time Settings

Time (hh:mm:ss) *:	18 : 12 : 17
Date (mm/dd/yyyy) *:	November / 5 / 2003
Current Zone Name / Offset:	PST -480

Standard Timezone

Zone Name *:	PST
UTC Offset (minutes) *:	-480

NTP Server

Server IP:	
Key:	
Key ID:	

Daylight Savings Time

Enabled:	☑
DST Zone Name *:	PDT
Offset (minutes):	60
Start Time (hh:mm):	02 : 00
End Time (hh:mm):	02 : 00

Daylight Savings Time Duration

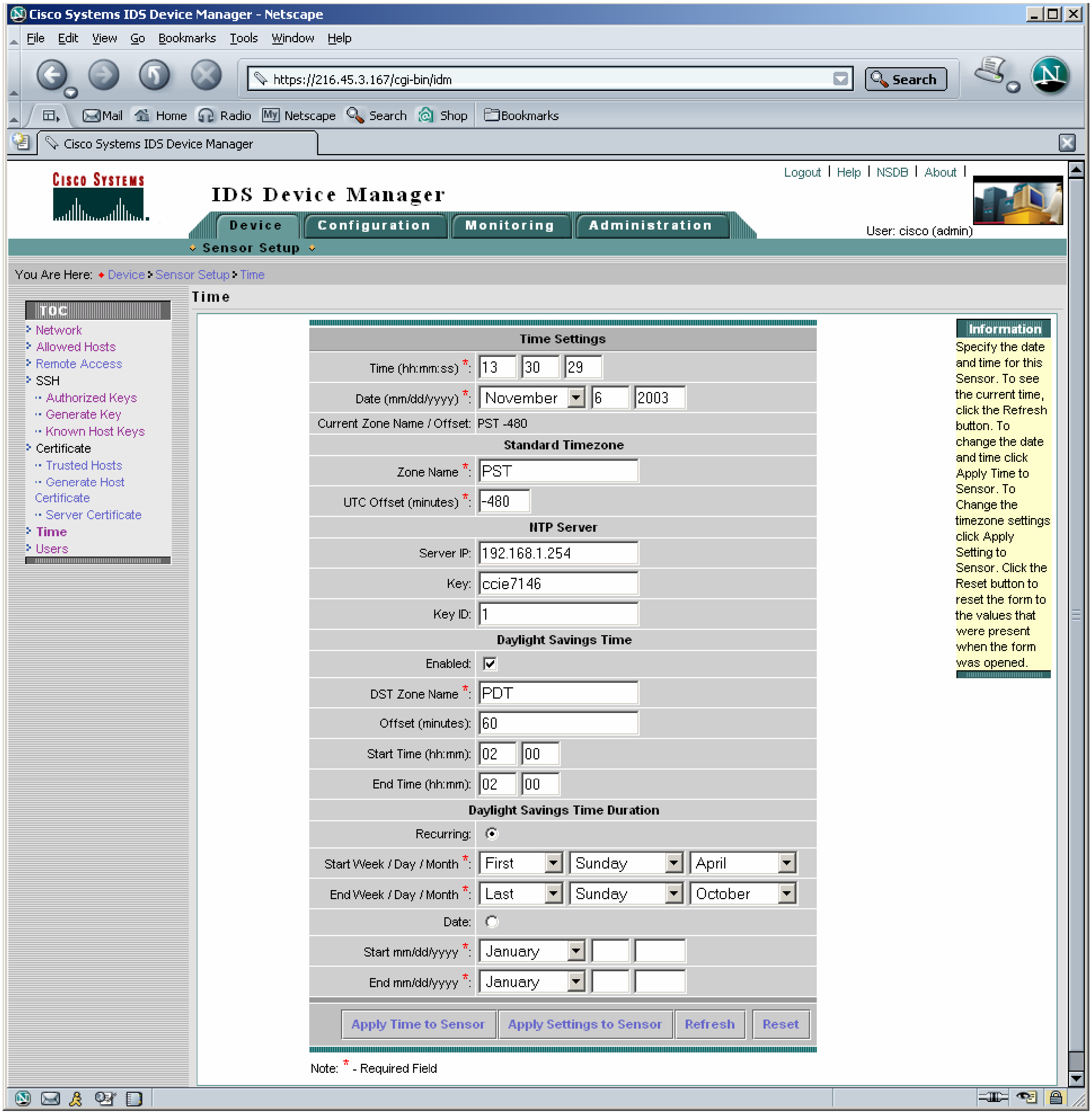
Recurring:	●
Start Week / Day / Month *:	First / Sunday / April
End Week / Day / Month *:	Last / Sunday / October
Date:	○
Start mm/dd/yyyy *:	January
End mm/dd/yyyy *:	January

Note: * Required Field

Information

Specify the date and time for this Sensor. To see the current time, click the Refresh button. To change the date and time click Apply Time to Sensor. To Change the timezone settings click Apply Setting to Sensor. Click the Reset button to reset the form to the values that were present when the form was opened.

Question 3.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
IDS Device Manager
Device Configuration Monitoring Administration
User: cisco (admin)
Sensor Setup
TOC
Network
Allowed Hosts
Remote Access
SSH
Authorized Keys
Generate Key
Known Host Keys
Certificate
Trusted Hosts
Generate Host Certificate
Server Certificate
Time
Users
Information

You Are Here: Device > Sensor Setup > Time

Time

Time Settings

Time (hh:mm:ss) *:	13 30 29
Date (mm/dd/yyyy) *:	November 6 2003
Current Zone Name / Offset:	PST -480

Standard Timezone

Zone Name *:	PST
UTC Offset (minutes) *:	-480

NTP Server

Server IP:	192.168.1.254
Key:	ccie7146
Key ID:	1

Daylight Savings Time

Enabled:	☑
DST Zone Name *:	PDT
Offset (minutes):	60
Start Time (hh:mm):	02 00
End Time (hh:mm):	02 00

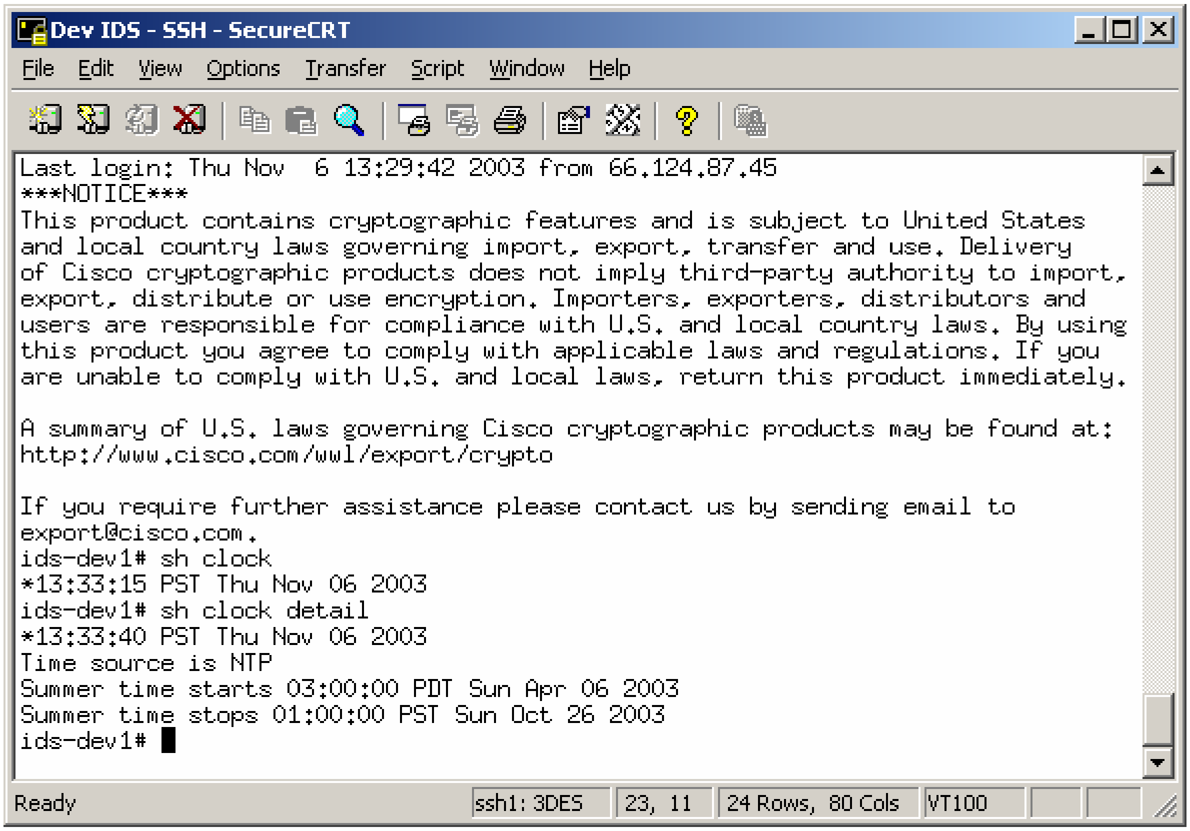
Daylight Savings Time Duration

Recurring:	●
Start Week / Day / Month *:	First Sunday April
End Week / Day / Month *:	Last Sunday October
Date:	○
Start mm/dd/yyyy *:	January
End mm/dd/yyyy *:	January

Apply Time to Sensor | Apply Settings to Sensor | Refresh | Reset

Note: * - Required Field

Specify the date and time for this Sensor. To see the current time, click the Refresh button. To change the date and time click Apply Time to Sensor. To Change the timezone settings click Apply Setting to Sensor. Click the Reset button to reset the form to the values that were present when the form was opened.


Dev IDS - SSH - SecureCRT
File Edit View Options Transfer Script Window Help
Ready
ssh1: 3DES
23, 11
24 Rows, 80 Cols
VT100

```
Last login: Thu Nov  6 13:29:42 2003 from 66.124.87.45
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto

If you require further assistance please contact us by sending email to
export@cisco.com.
ids-dev1# sh clock
*13:33:15 PST Thu Nov 06 2003
ids-dev1# sh clock detail
*13:33:40 PST Thu Nov 06 2003
Time source is NTP
Summer time starts 03:00:00 PDT Sun Apr 06 2003
Summer time stops 01:00:00 PST Sun Oct 26 2003
ids-dev1#
```

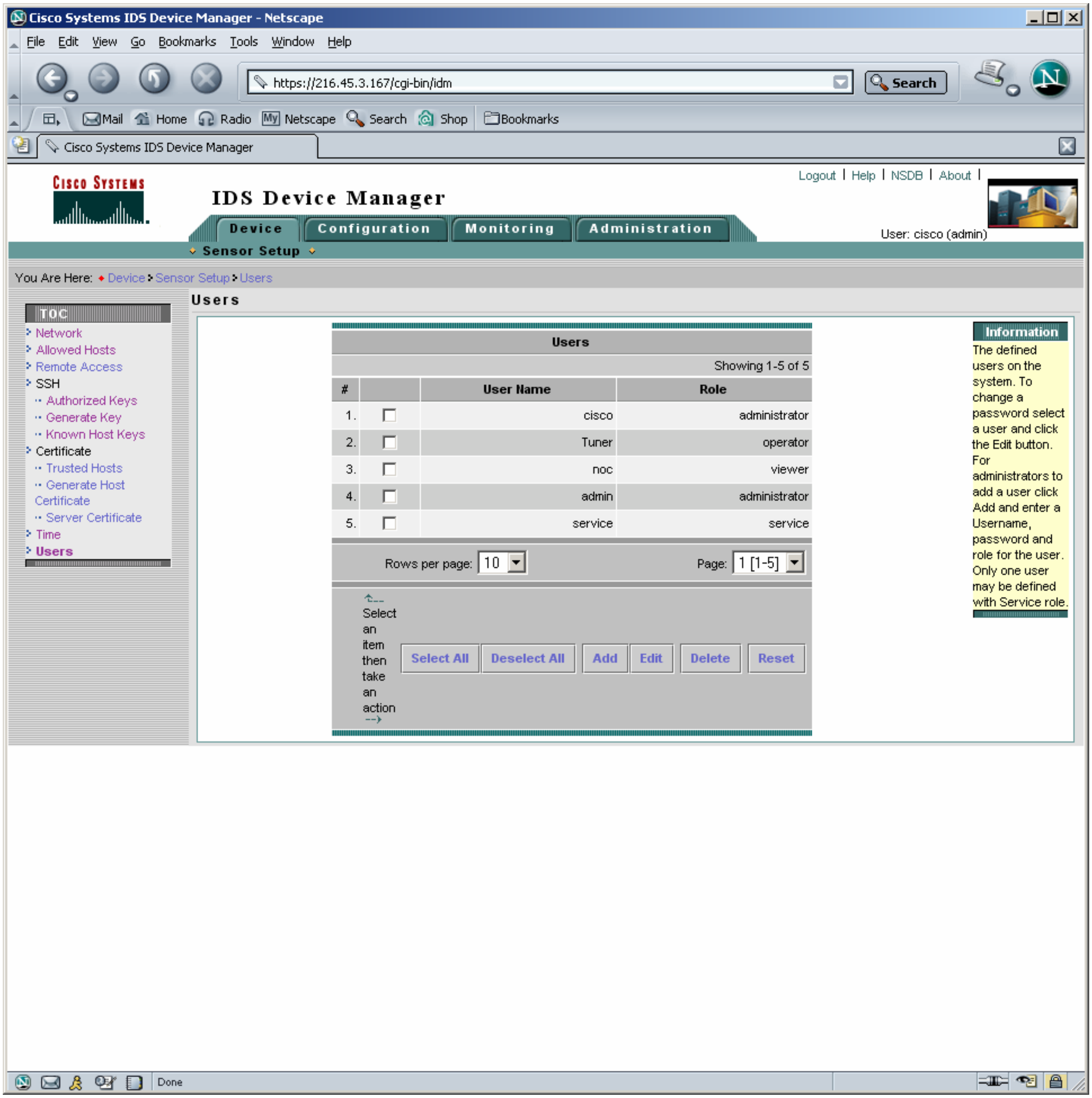
```
ntp-router#wr t
Building configuration...

Current configuration : 1015 bytes
!
! Last configuration change at 21:31:35 UTC Thu Nov 6 2003 by cisco
! NVRAM config last updated at 05:08:49 UTC Fri Nov 7 2003 by cisco
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ntp-router
!
logging rate-limit console 10 except errors
enable secret 5 $1$eWAB$qqlJ.fxjhEGReTX0d50bW.
!
username cisco password 0 cisco
ip subnet-zero
no ip finger
!
no ip dhcp-client network-discovery
!
!
!
!
interface Ethernet0
 ip address 192.168.1.254 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
ip kerberos source-interface any
ip classless
ip http server
```

```
        !
        !
        !
        line con 0
         transport input none
        line aux 0
        line vty 0 4
         exec-timeout 120 0
         password cisco
         login local
        line vty 5 15
         exec-timeout 120 0
         password cisco
         login local
        !
        ntp authentication-key 1 md5 030758020358701818 7
        ntp authenticate
        ntp master
        end

        ntp-router#sh clock
        21:31:48.951 UTC Thu Nov 6 2003
ntp-router#
```

Question 4 – 6


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
Device Configuration Monitoring Administration
Sensor Setup
TOC
Network
Allowed Hosts
Remote Access
SSH
Authorized Keys
Generate Key
Known Host Keys
Certificate
Trusted Hosts
Generate Host Certificate
Server Certificate
Time
Users
Select All Deselect All Add Edit Delete Reset
Done

IDS Device Manager

User: cisco (admin)

You Are Here: Device > Sensor Setup > Users

Users

Users

Showing 1-5 of 5

#		User Name	Role
1.	□	cisco	administrator
2.	□	Tuner	operator
3.	□	noc	viewer
4.	□	admin	administrator
5.	□	service	service

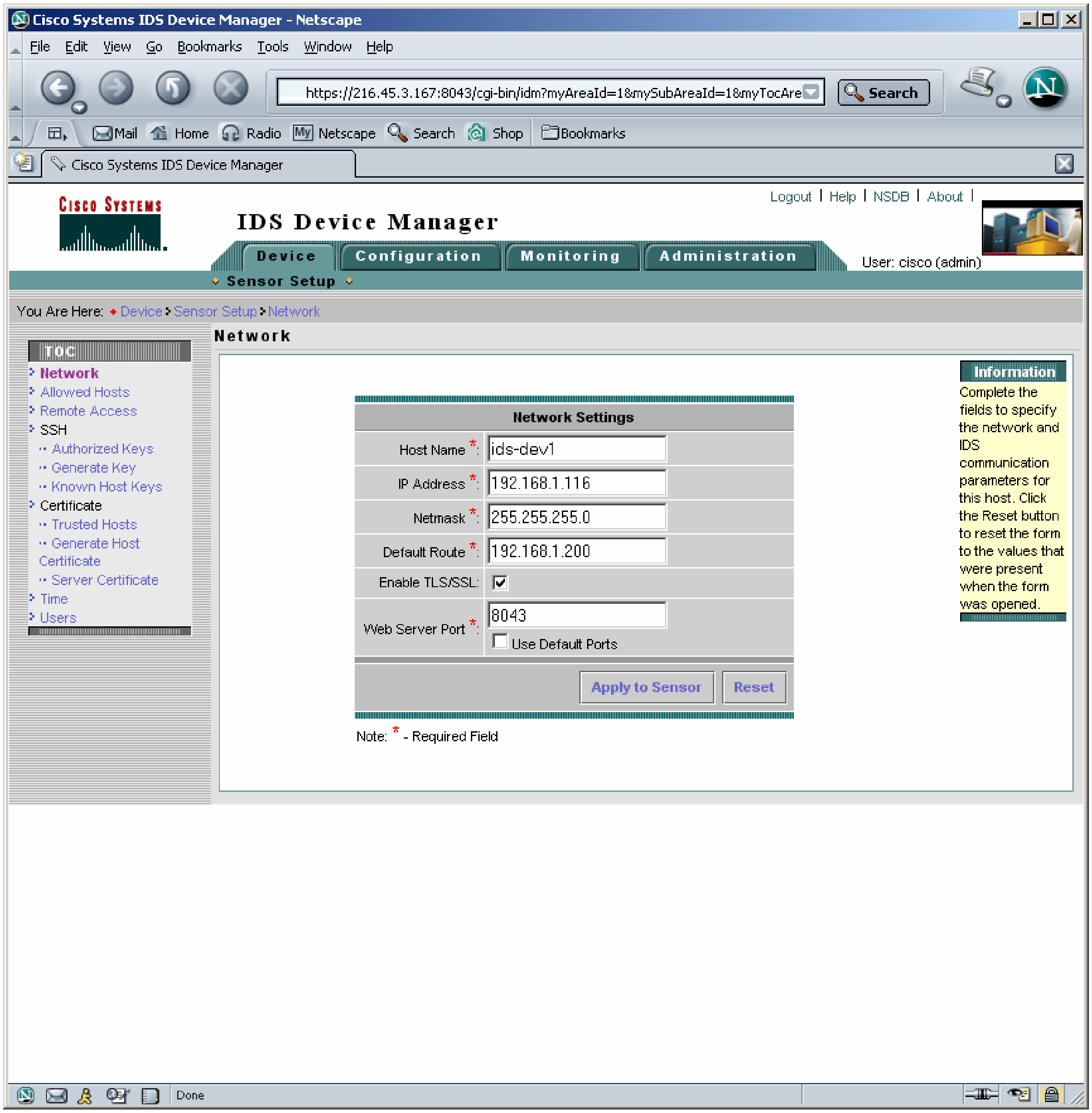
Rows per page: 10 Page: 1 [1-5]

Select an item then take an action

Information

The defined users on the system. To change a password select a user and click the Edit button. For administrators to add a user click Add and enter a Username, password and role for the user. Only one user may be defined with Service role.

Question 7.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167:8043/cgi-bin/idm?myAreaId=1&mySubAreaId=1&myTocAre
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
IDS Device Manager
Logout | Help | NSDB | About |
Device Configuration Monitoring Administration
User: cisco (admin)
Sensor Setup
You Are Here: Device > Sensor Setup > Network
TOC
Network
Allowed Hosts
Remote Access
SSH
Authorized Keys
Generate Key
Known Host Keys
Certificate
Trusted Hosts
Generate Host Certificate
Server Certificate
Time
Users
Information
Done

Network

Network Settings

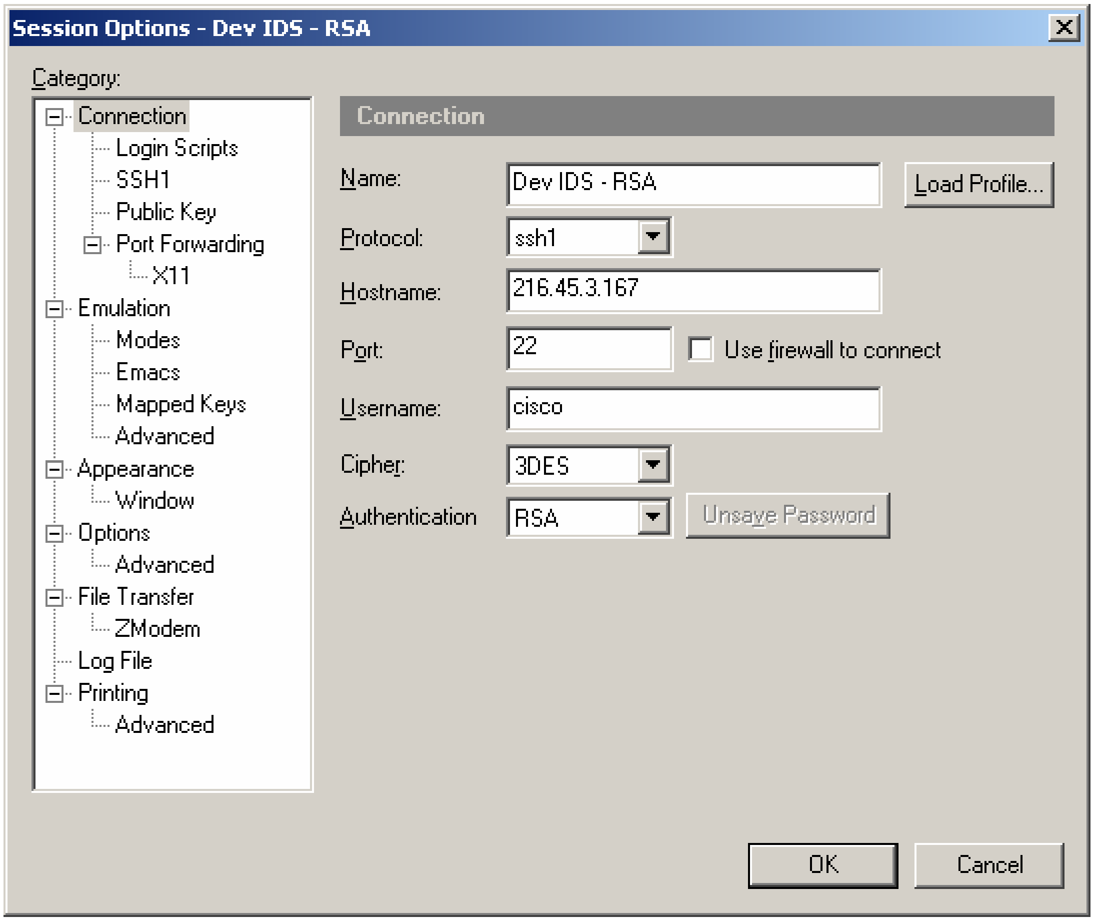
Host Name *:	ids-dev1
IP Address *:	192.168.1.116
Netmask *:	255.255.255.0
Default Route *:	192.168.1.200
Enable TLS/SSL:	☑
Web Server Port *:	8043 □ Use Default Ports

Apply to Sensor | Reset

Note: * - Required Field

Complete the fields to specify the network and IDS communication parameters for this host. Click the Reset button to reset the form to the values that were present when the form was opened.

Question 8.



Connection

Name: Dev IDS - RSA

Protocol: ssh1

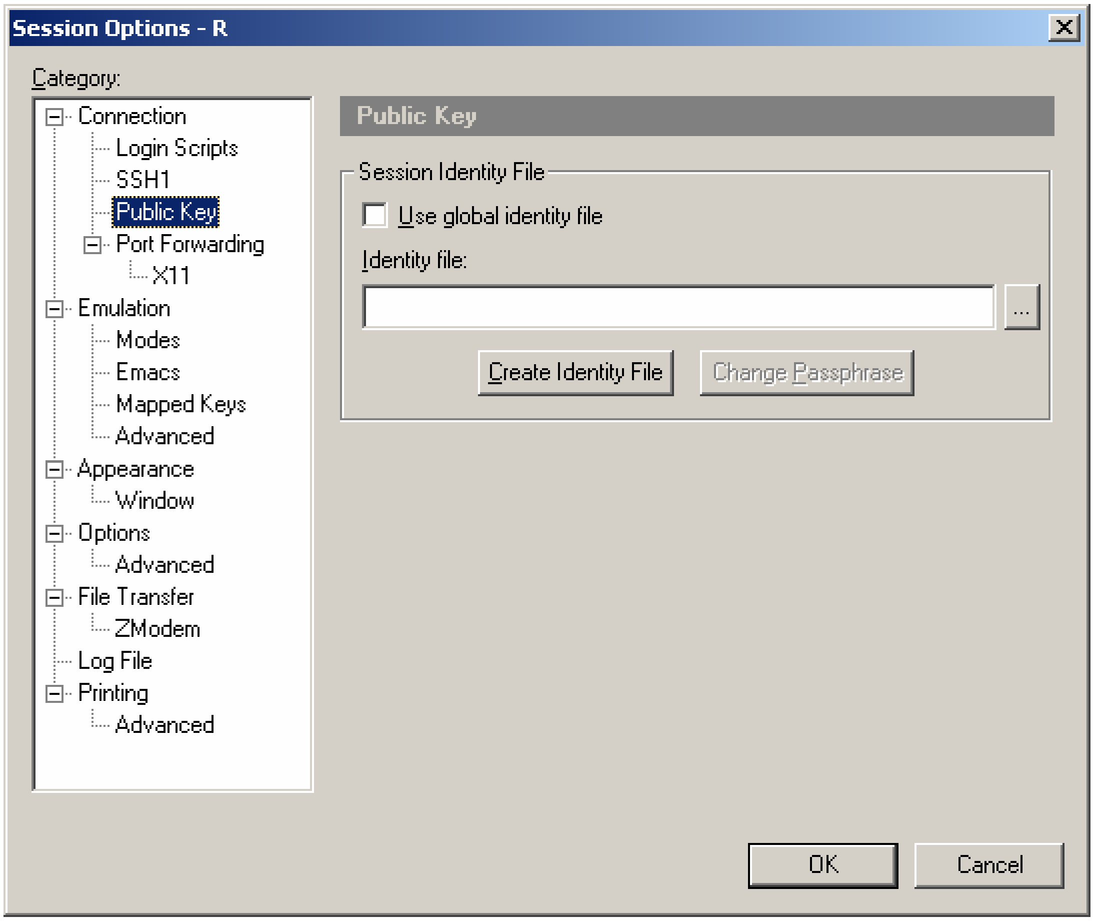
Hostname: 216.45.3.167

Port: 22 ☐ Use firewall to connect

Username: cisco

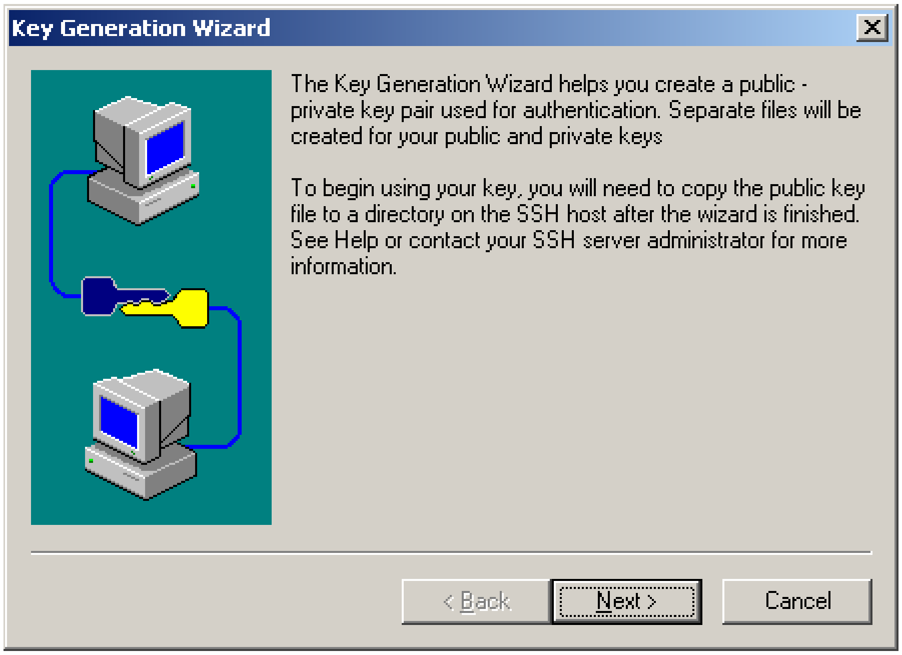
Cipher: 3DES

Authentication RSA



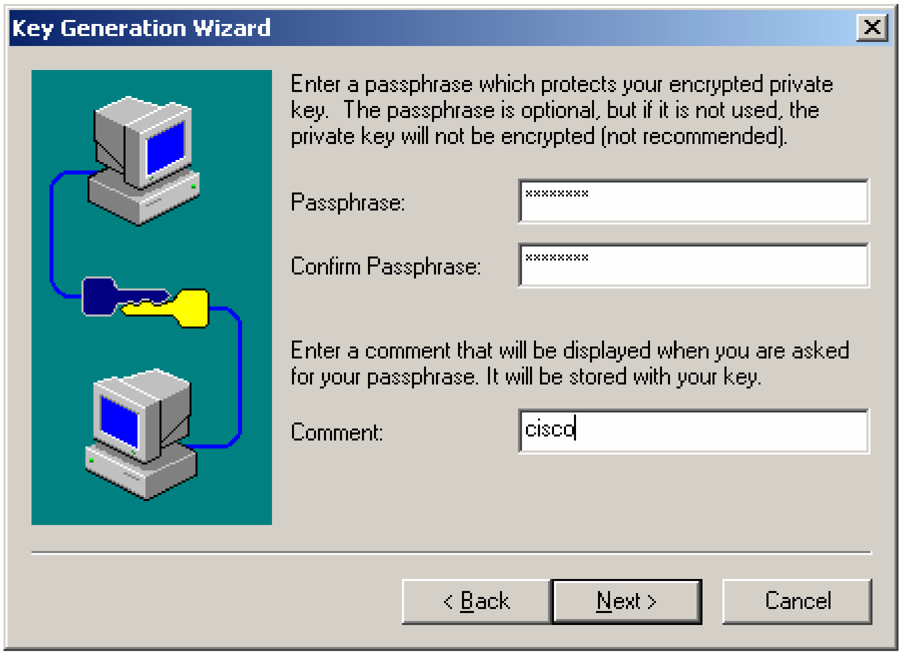
□ Use global identity file

Identity file:



The Key Generation Wizard helps you create a public - private key pair used for authentication. Separate files will be created for your public and private keys

To begin using your key, you will need to copy the public key file to a directory on the SSH host after the wizard is finished. See Help or contact your SSH server administrator for more information.



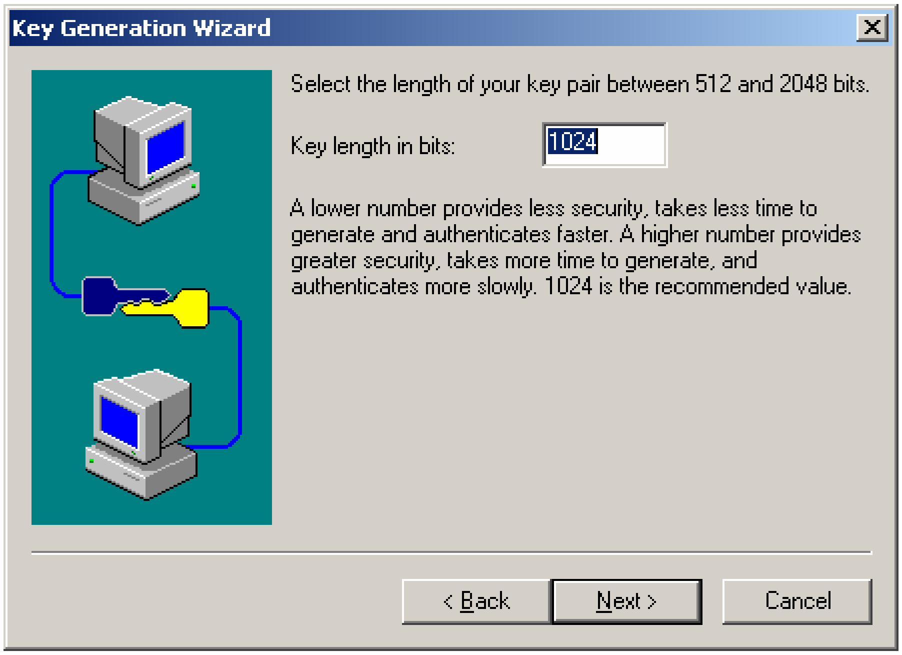
Enter a passphrase which protects your encrypted private key. The passphrase is optional, but if it is not used, the private key will not be encrypted (not recommended).

Passphrase: *********

Confirm Passphrase: *********

Enter a comment that will be displayed when you are asked for your passphrase. It will be stored with your key.

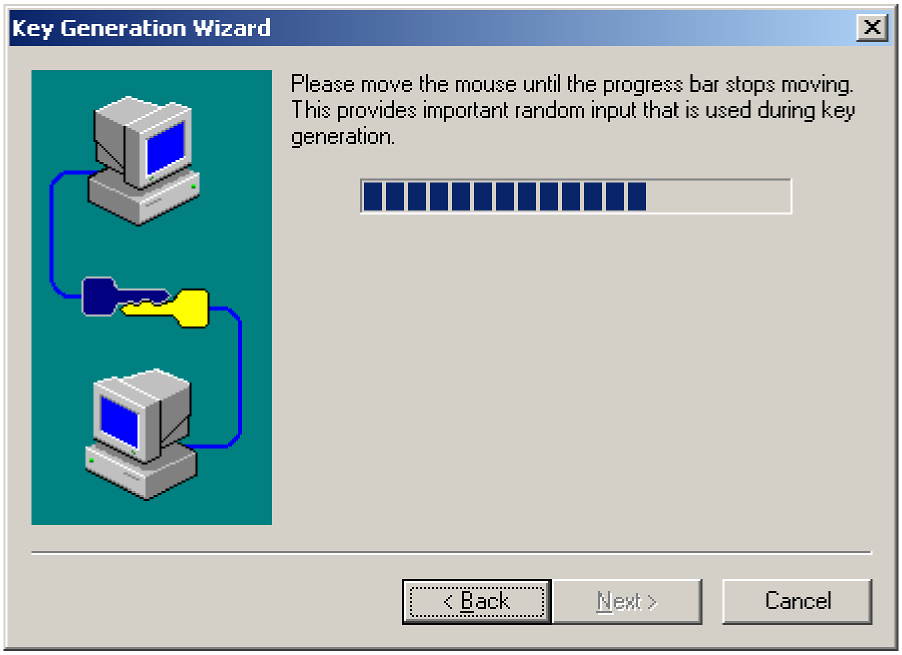
Comment: cisco



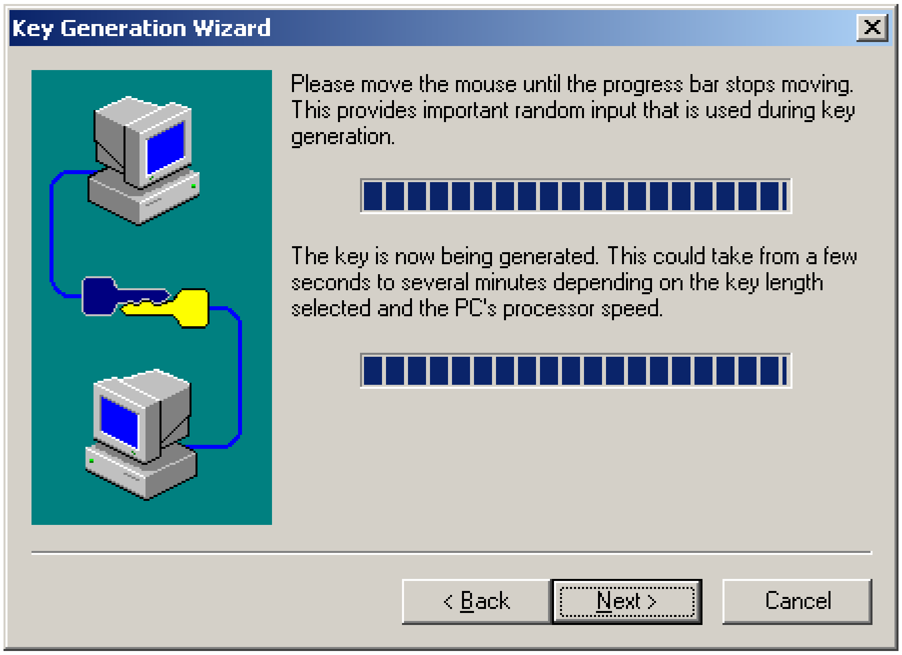
Select the length of your key pair between 512 and 2048 bits.

Key length in bits: 1024

A lower number provides less security, takes less time to generate and authenticates faster. A higher number provides greater security, takes more time to generate, and authenticates more slowly. 1024 is the recommended value.

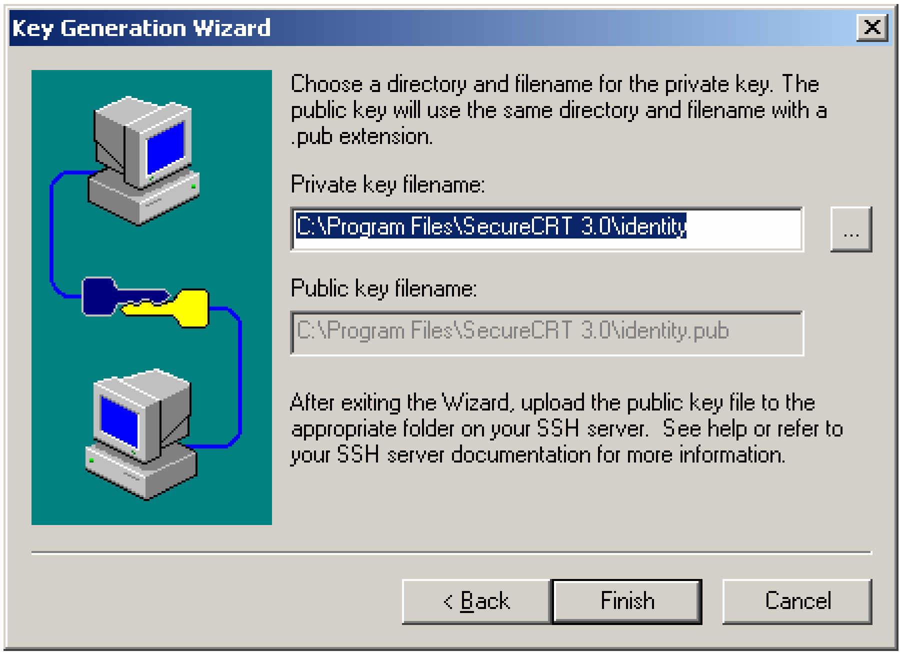


Please move the mouse until the progress bar stops moving. This provides important random input that is used during key generation.



Please move the mouse until the progress bar stops moving. This provides important random input that is used during key generation.

The key is now being generated. This could take from a few seconds to several minutes depending on the key length selected and the PC's processor speed.

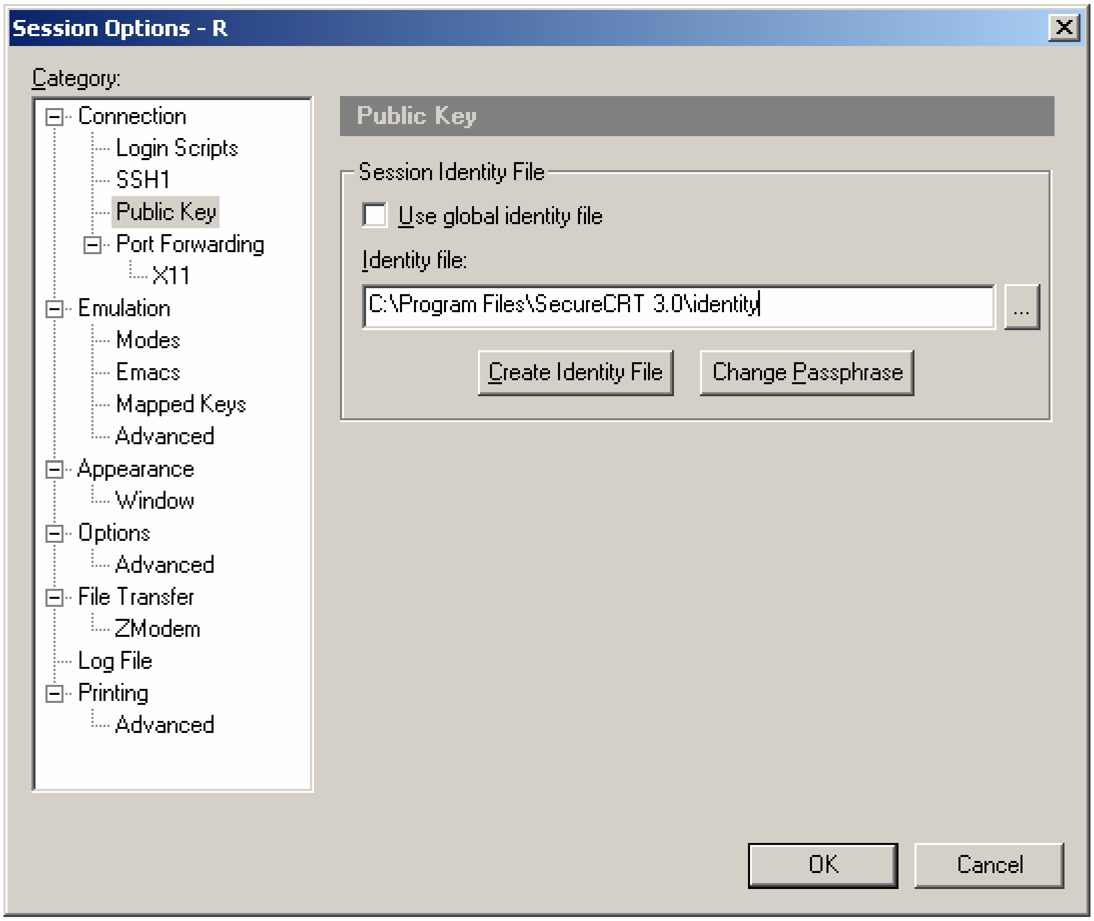


Choose a directory and filename for the private key. The public key will use the same directory and filename with a .pub extension.

Private key filename: C:\Program Files\SecureCRT 3.0\identity

Public key filename: C:\Program Files\SecureCRT 3.0\identity.pub

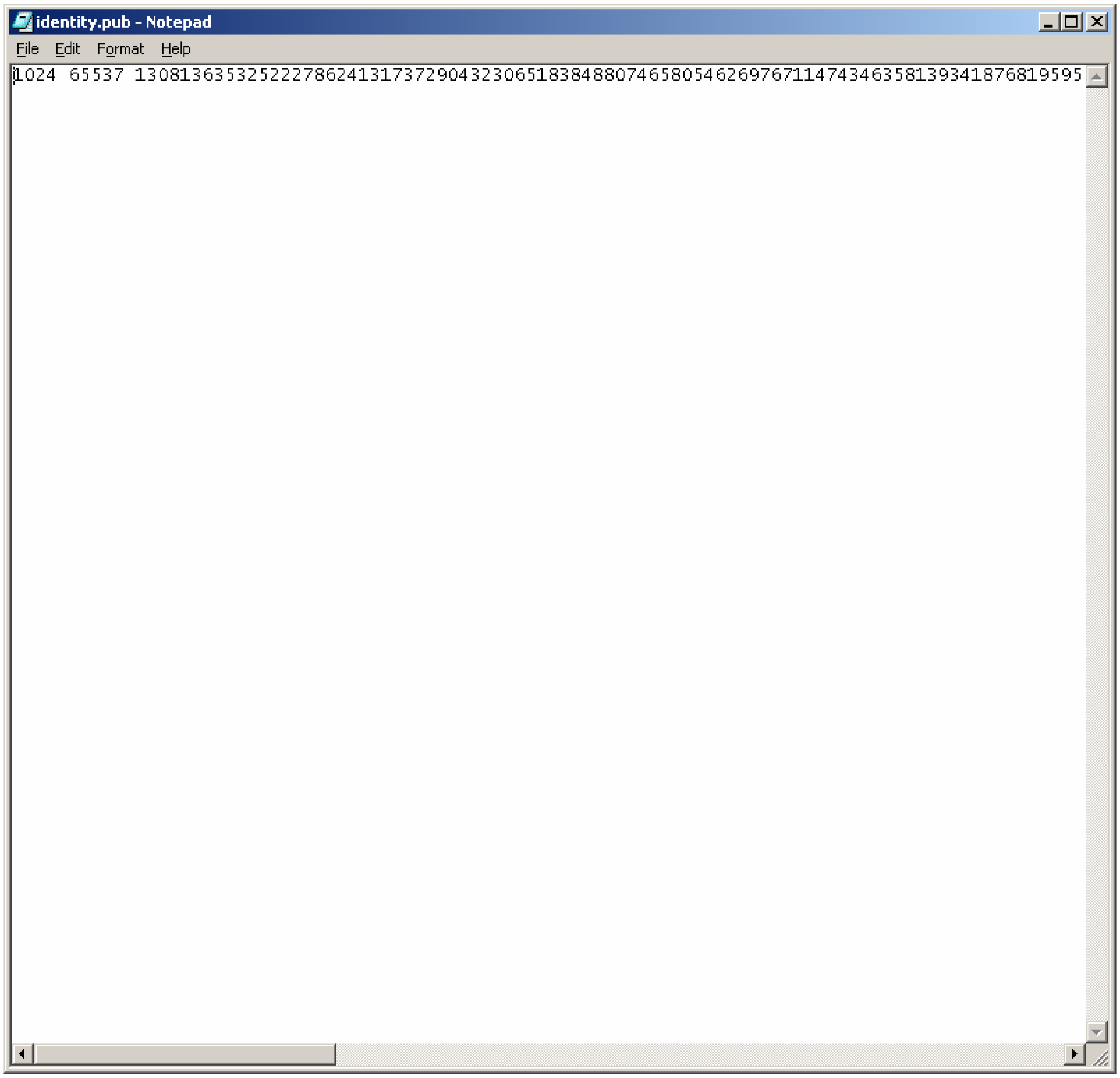
After exiting the Wizard, upload the public key file to the appropriate folder on your SSH server. See help or refer to your SSH server documentation for more information.



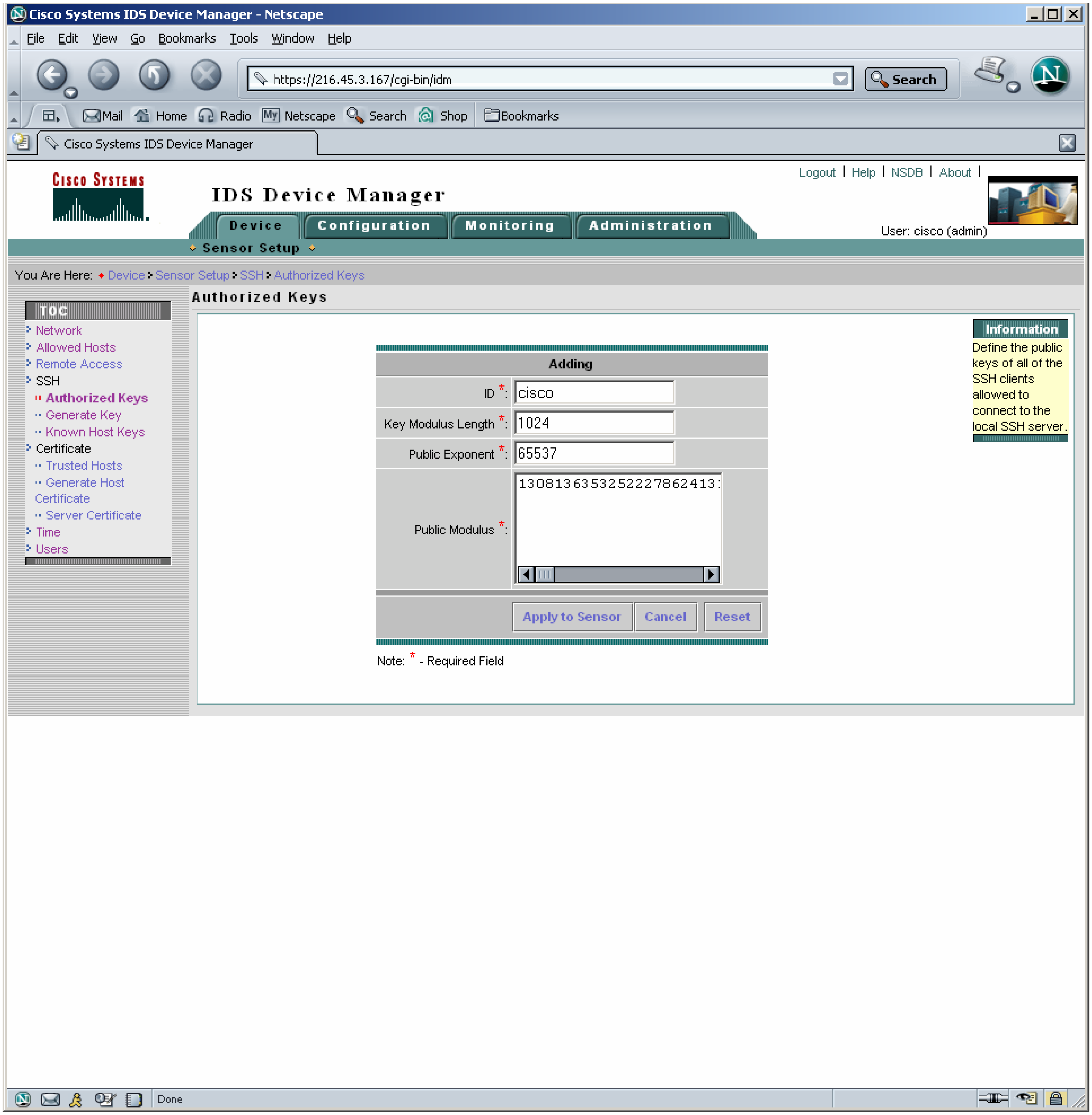
□ Use global identity file

Identity file: C:\Program Files\SecureCRT 3.0\identity

C:\Program Files\SecureCRT 3.0



```
1024 65537 1308136353252227862413173729043230651838488074658054626976711474346358139341876819595
```



https://216.45.3.167/cgi-bin/idm

IDS Device Manager

User: cisco (admin)

You Are Here: Device > Sensor Setup > SSH > Authorized Keys

Authorized Keys

Adding

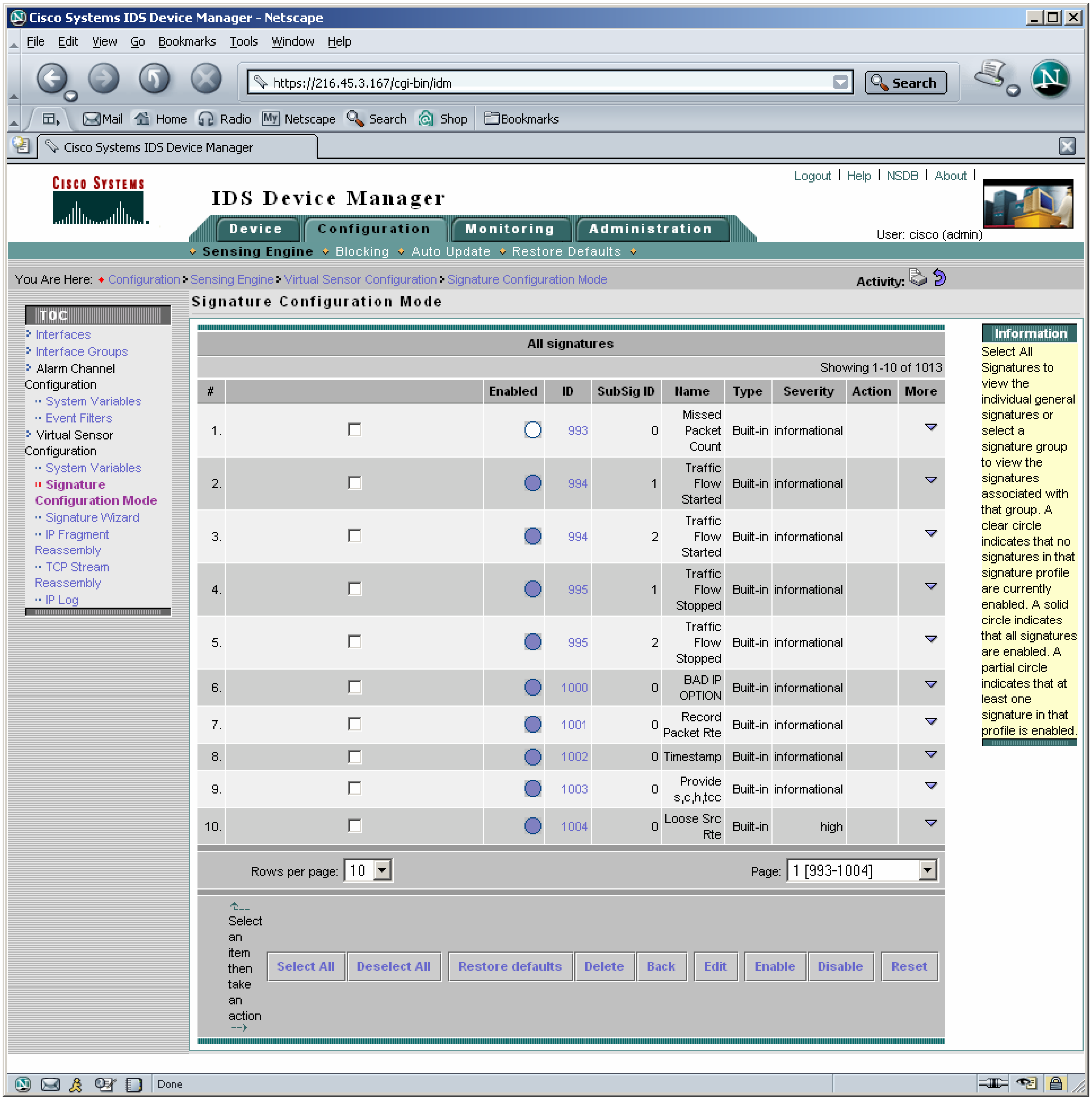
ID *:	cisco
Key Modulus Length *:	1024
Public Exponent *:	65537
Public Modulus *:	1308136353252227862413

Note: * - Required Field

Information

Define the public keys of all of the SSH clients allowed to connect to the local SSH server.

Question 9.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
Cisco Systems
Device Configuration Monitoring Administration
Sensing Engine • Blocking • Auto Update • Restore Defaults
Activity:
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Select All
Deselect All
Restore defaults
Delete
Back
Edit
Enable
Disable
Reset
Done

https://216.45.3.167/cgi-bin/idm

IDS Device Manager

User: cisco (admin)

You Are Here: Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode

Signature Configuration Mode

All signatures

Showing 1-10 of 1013

#		Enabled	ID	SubSig ID	Name	Type	Severity	Action	More
1.	□	○	993	0	Missed Packet Count	Built-in	informational		▽
2.	□	●	994	1	Traffic Flow Started	Built-in	informational		▽
3.	□	●	994	2	Traffic Flow Started	Built-in	informational		▽
4.	□	●	995	1	Traffic Flow Stopped	Built-in	informational		▽
5.	□	●	995	2	Traffic Flow Stopped	Built-in	informational		▽
6.	□	●	1000	0	BAD IP OPTION	Built-in	informational		▽
7.	□	●	1001	0	Record Packet Rte	Built-in	informational		▽
8.	□	●	1002	0	Timestamp	Built-in	informational		▽
9.	□	●	1003	0	Provide s,c,h,tcc	Built-in	informational		▽
10.	□	●	1004	0	Loose Src Rte	Built-in	high		▽

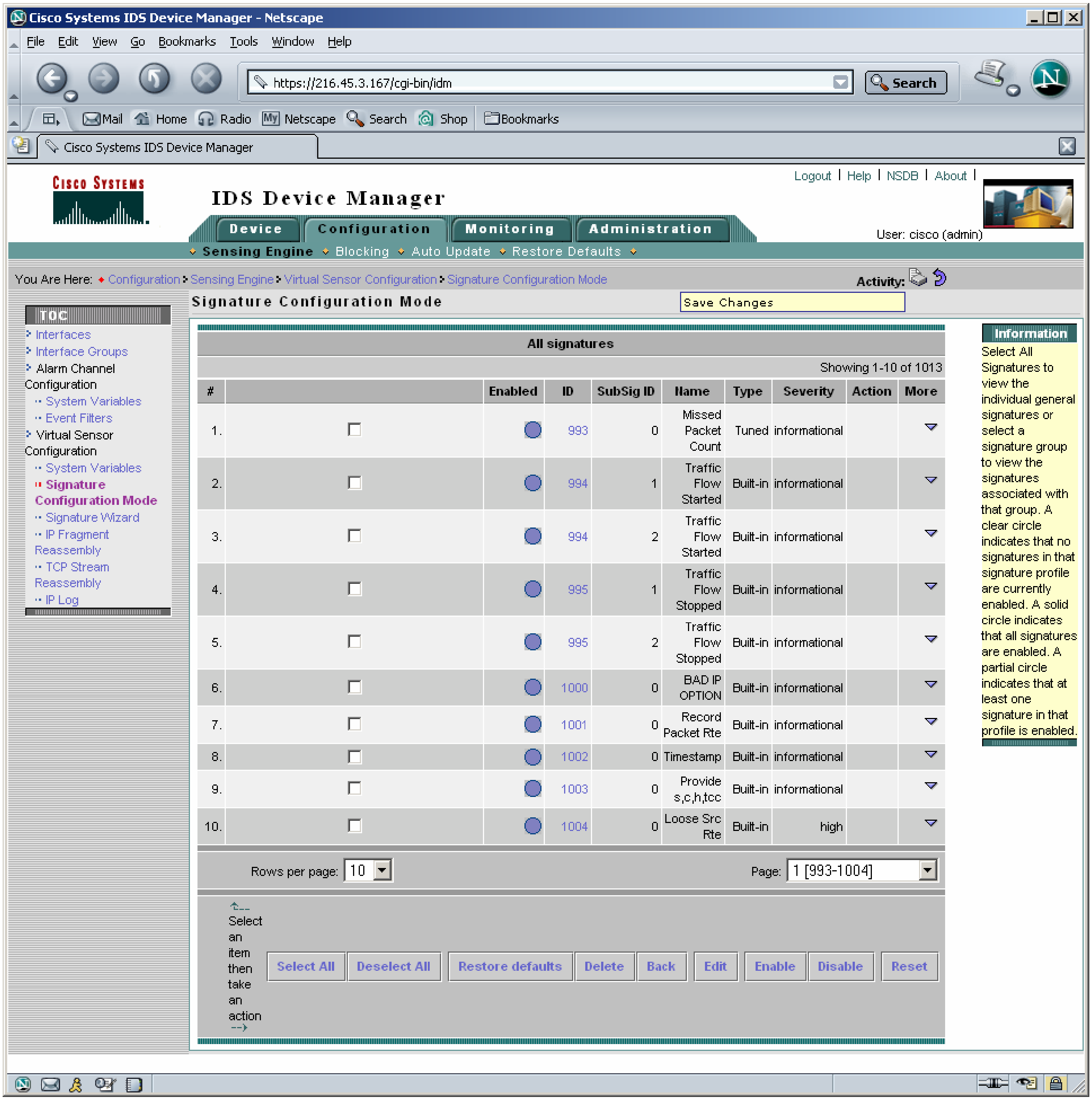
Rows per page: 10

Page: 1 [993-1004]

Select an item then take an action

Information

Select All Signatures to view the individual general signatures or select a signature group to view the signatures associated with that group. A clear circle indicates that no signatures in that signature profile are currently enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that profile is enabled.



Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
CISCO SYSTEMS
IDS Device Manager
Device Configuration Monitoring Administration
User: cisco (admin)
Sensing Engine Blocking Auto Update Restore Defaults

You Are Here: Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode

Activity:

Signature Configuration Mode

Save Changes

TOC

- Interfaces
- Interface Groups
- Alarm Channel Configuration
  - System Variables
  - Event Filters
- Virtual Sensor Configuration
  - System Variables
  - **Signature Configuration Mode**
  - Signature Wizard
  - IP Fragment Reassembly
  - TCP Stream Reassembly
  - IP Log

All signatures

Showing 1-10 of 1013

#		Enabled	ID	SubSig ID	Name	Type	Severity	Action	More
1.	□	●	993	0	Missed Packet Count	Tuned	informational		▽
2.	□	●	994	1	Traffic Flow Started	Built-in	informational		▽
3.	□	●	994	2	Traffic Flow Started	Built-in	informational		▽
4.	□	●	995	1	Traffic Flow Stopped	Built-in	informational		▽
5.	□	●	995	2	Traffic Flow Stopped	Built-in	informational		▽
6.	□	●	1000	0	BAD IP OPTION	Built-in	informational		▽
7.	□	●	1001	0	Record Packet Rte	Built-in	informational		▽
8.	□	●	1002	0	Timestamp	Built-in	informational		▽
9.	□	●	1003	0	Provide s,c,h,tcc	Built-in	informational		▽
10.	□	●	1004	0	Loose Src Rte	Built-in	high		▽

Rows per page: 10

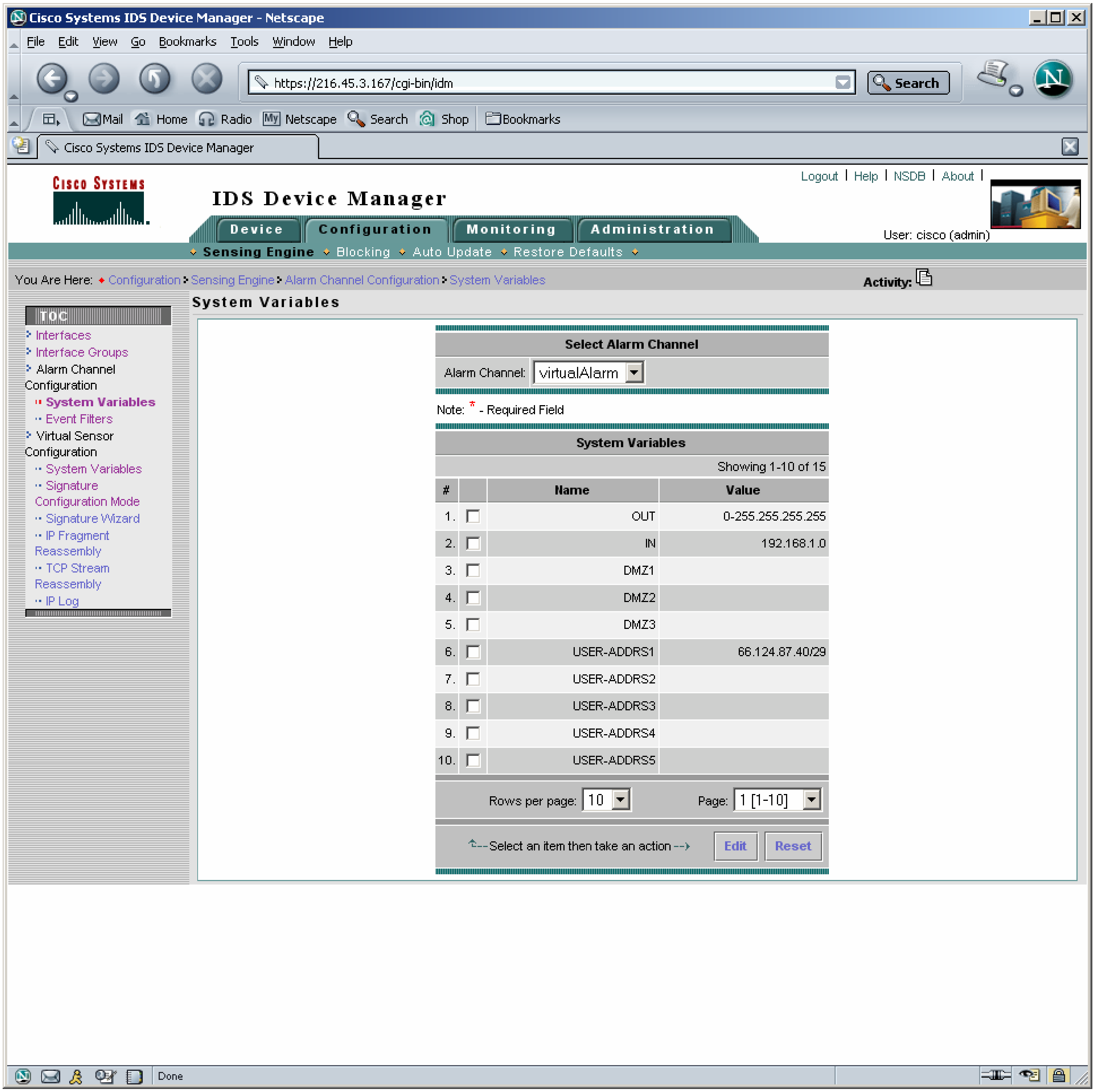
Page: 1 [993-1004]

Select an item then take an action -->

Information

Select All Signatures to view the individual general signatures or select a signature group to view the signatures associated with that group. A clear circle indicates that no signatures in that signature profile are currently enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that profile is enabled.

Question 10


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
Device
Configuration
Monitoring
Administration
Sensing Engine
Blocking
Auto Update
Restore Defaults
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Edit
Reset
Done

IDS Device Manager

User: cisco (admin)

You Are Here: Configuration > Sensing Engine > Alarm Channel Configuration > System Variables

Activity:

System Variables

Select Alarm Channel

Alarm Channel: virtualAlarm

Note: * - Required Field

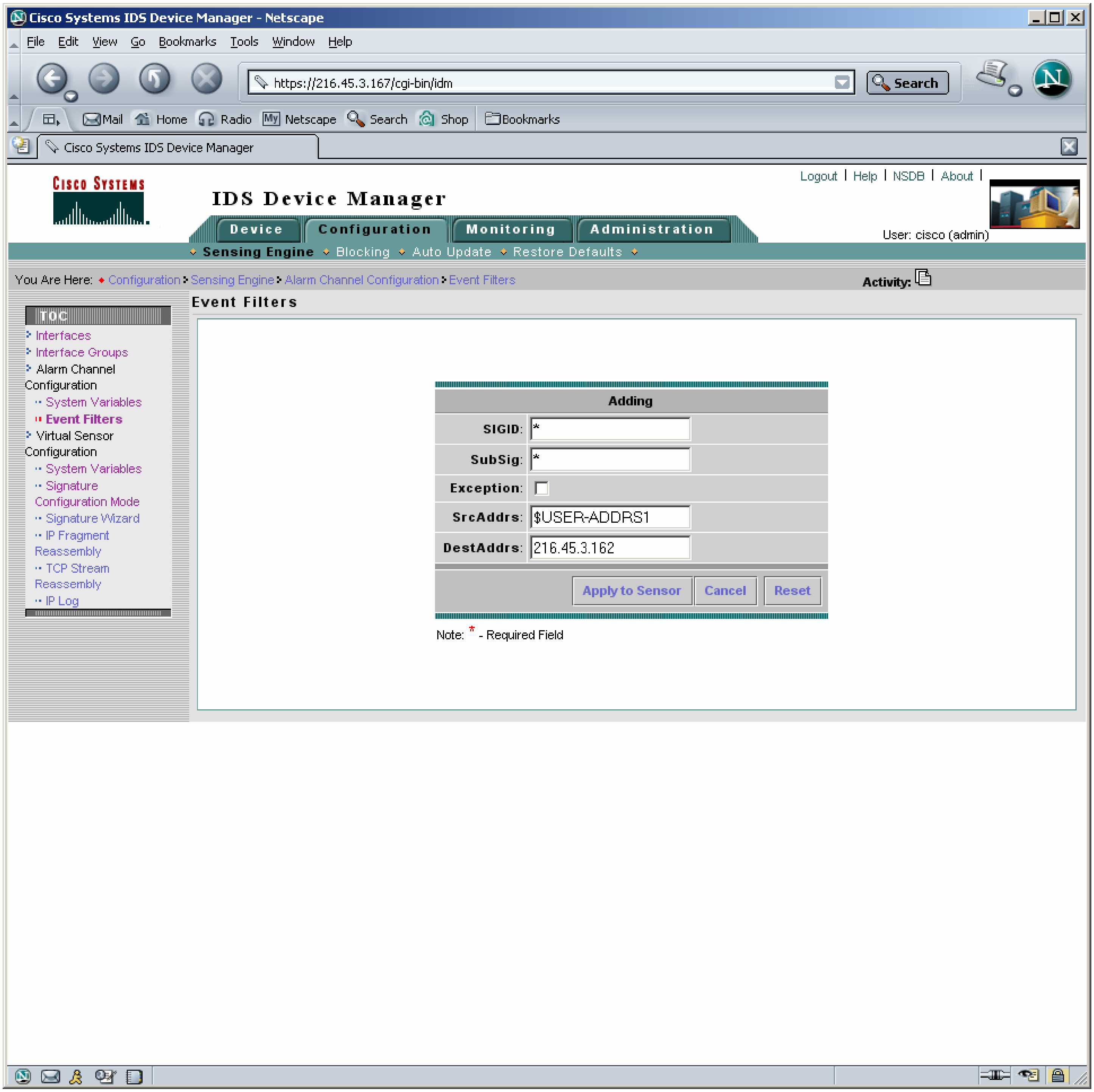
System Variables

Showing 1-10 of 15

#		Name	Value
1.	□	OUT	0-255.255.255.255
2.	□	IN	192.168.1.0
3.	□	DMZ1	
4.	□	DMZ2	
5.	□	DMZ3	
6.	□	USER-ADDRS1	66.124.87.40/29
7.	□	USER-ADDRS2	
8.	□	USER-ADDRS3	
9.	□	USER-ADDRS4	
10.	□	USER-ADDRS5	

Rows per page: 10 Page: 1 [1-10]

Select an item then take an action -->


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.167/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
IDS Device Manager
Logout | Help | NSDB | About |
Device Configuration Monitoring Administration
User: cisco (admin)
Sensing Engine Blocking Auto Update Restore Defaults
You Are Here: Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters
Activity:
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Apply to Sensor
Cancel
Reset

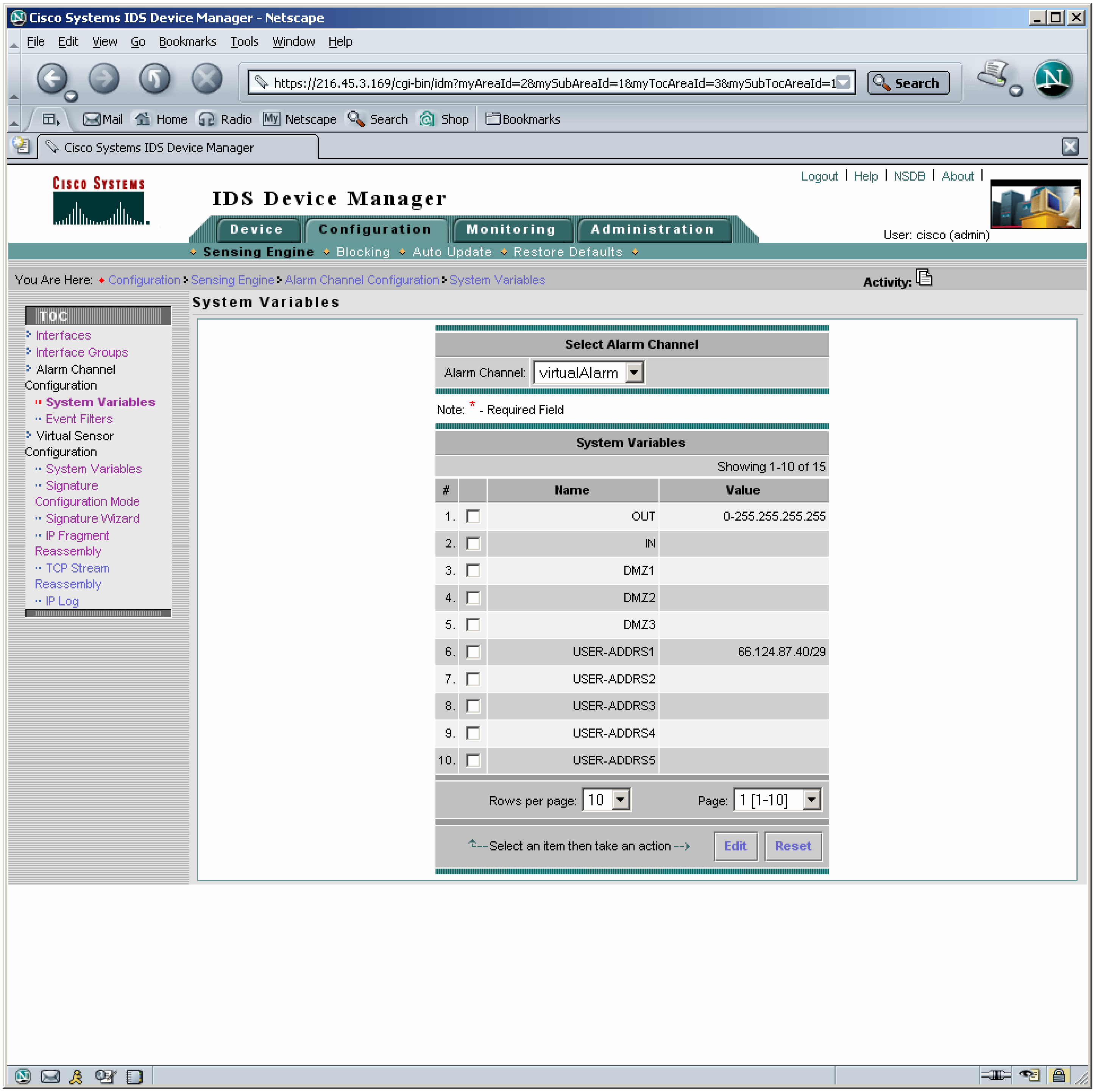
Event Filters

Adding

SIGID:	*
SubSig:	*
Exception:	□
SrcAddrs:	$USER-ADDRS1
DestAddrs:	216.45.3.162

Note: * - Required Field

Question 11


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
Device
Configuration
Monitoring
Administration
Sensing Engine
Blocking
Auto Update
Restore Defaults
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Activity:
Edit
Reset

https://216.45.3.169/cgi-bin/idm?myAreaId=2&mySubAreaId=1&myTocAreaId=3&mySubTocAreaId=1

IDS Device Manager

User: cisco (admin)

You Are Here: Configuration > Sensing Engine > Alarm Channel Configuration > System Variables

System Variables

Select Alarm Channel

Alarm Channel: virtualAlarm

Note: * - Required Field

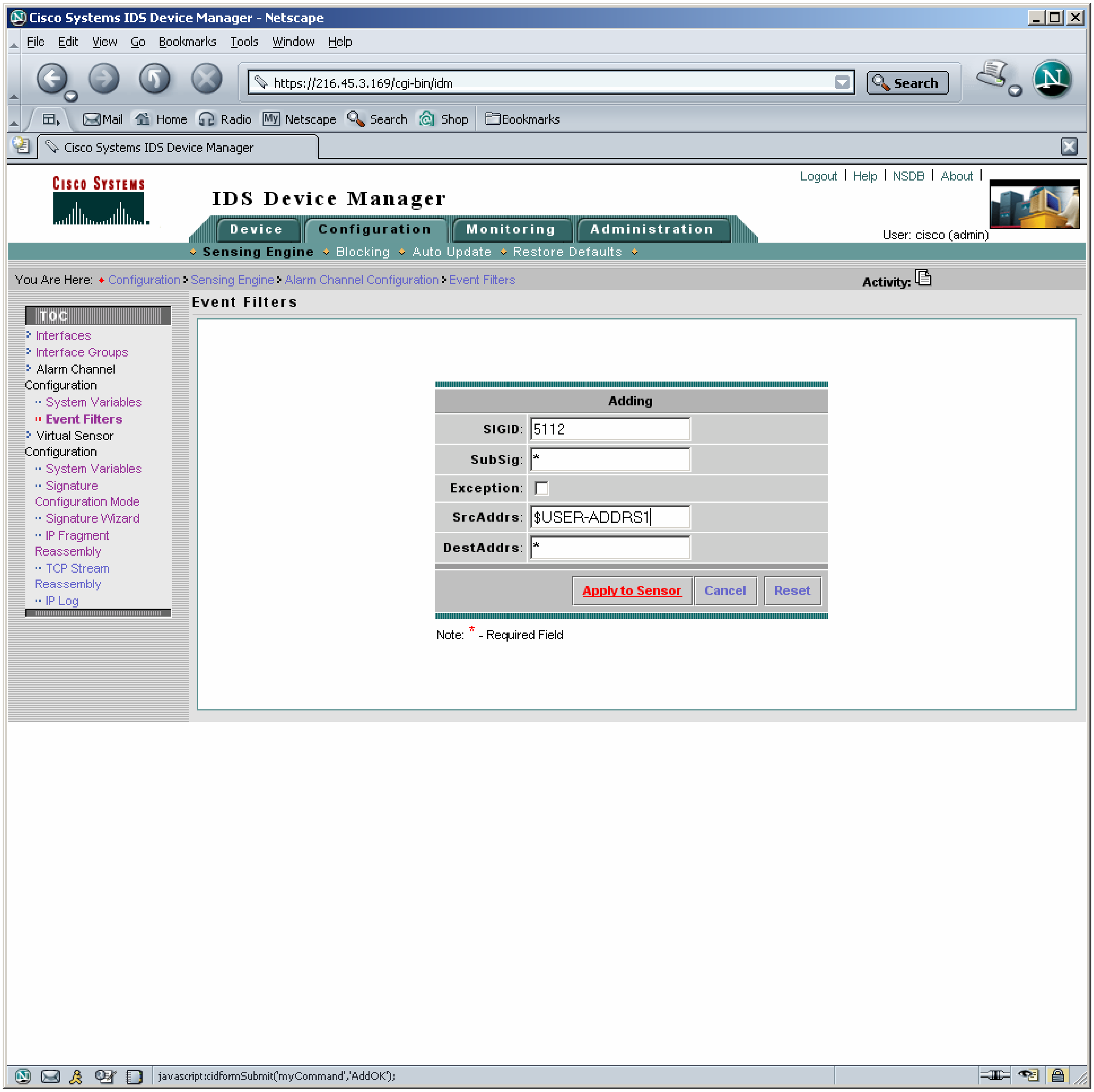
System Variables

Showing 1-10 of 15

#		Name	Value
1.	□	OUT	0-255.255.255.255
2.	□	IN	
3.	□	DMZ1	
4.	□	DMZ2	
5.	□	DMZ3	
6.	□	USER-ADDRS1	66.124.87.40/29
7.	□	USER-ADDRS2	
8.	□	USER-ADDRS3	
9.	□	USER-ADDRS4	
10.	□	USER-ADDRS5	

Rows per page: 10 Page: 1 [1-10]

Select an item then take an action


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
CISCO SYSTEMS
IDS Device Manager
Device
Configuration
Monitoring
Administration
User: cisco (admin)
Sensing Engine
Blocking
Auto Update
Restore Defaults
You Are Here: Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters
Activity:
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Apply to Sensor
Cancel
Reset

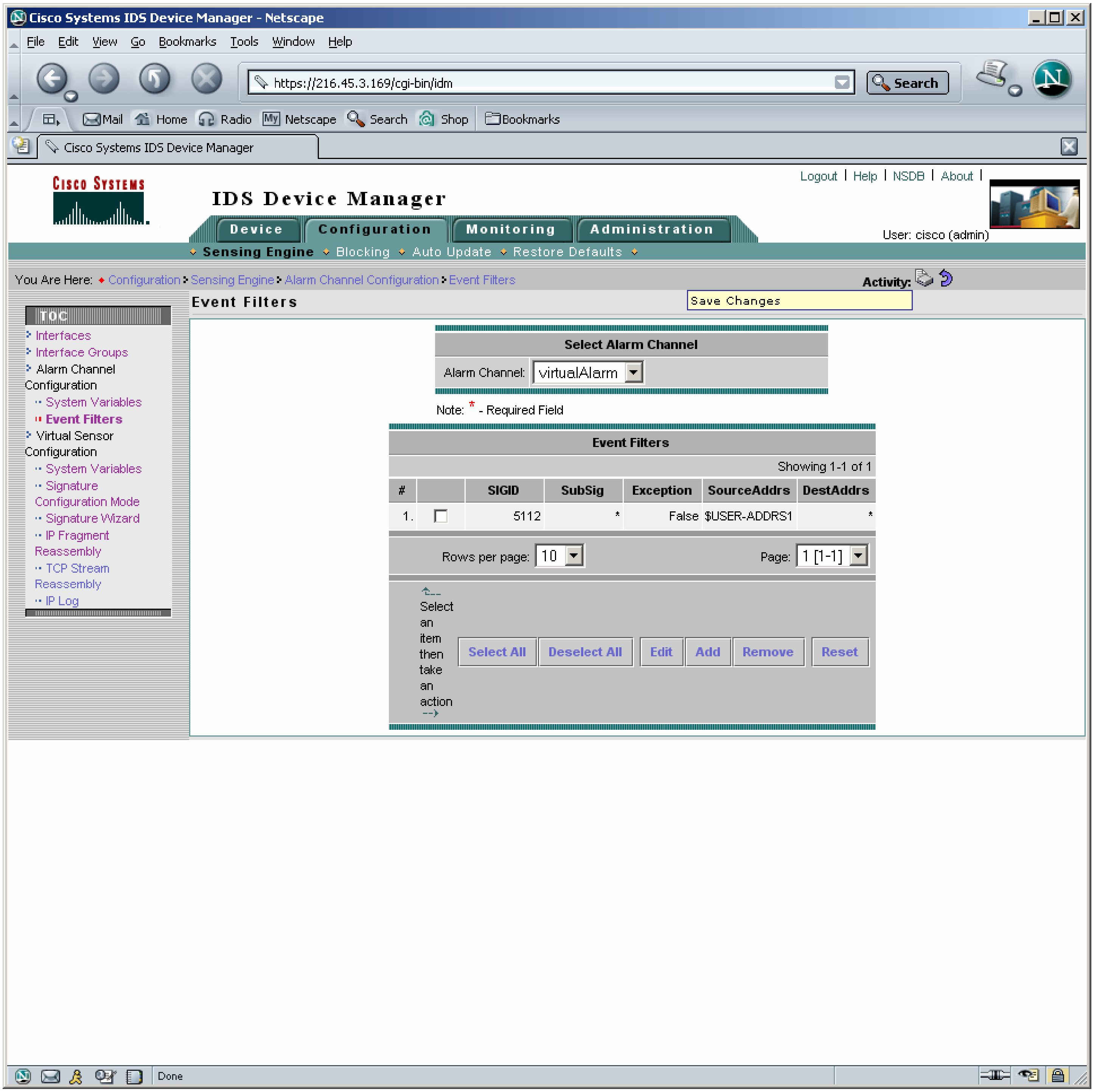
Event Filters

Adding

SIGID:	5112
SubSig:	*
Exception:	□
SrcAddrs:	$USER-ADDRS1
DestAddrs:	*

Note: * - Required Field

javascript:cidformSubmit('myCommand','AddOK');


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
IDS Device Manager
Logout | Help | NSDB | About |
User: cisco (admin)
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
You Are Here: Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters
Activity:
Save Changes
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Select an item then take an action
Select All Deselect All Edit Add Remove Reset
Done

Event Filters

Select Alarm Channel

Alarm Channel: virtualAlarm

Note: * - Required Field

Event Filters

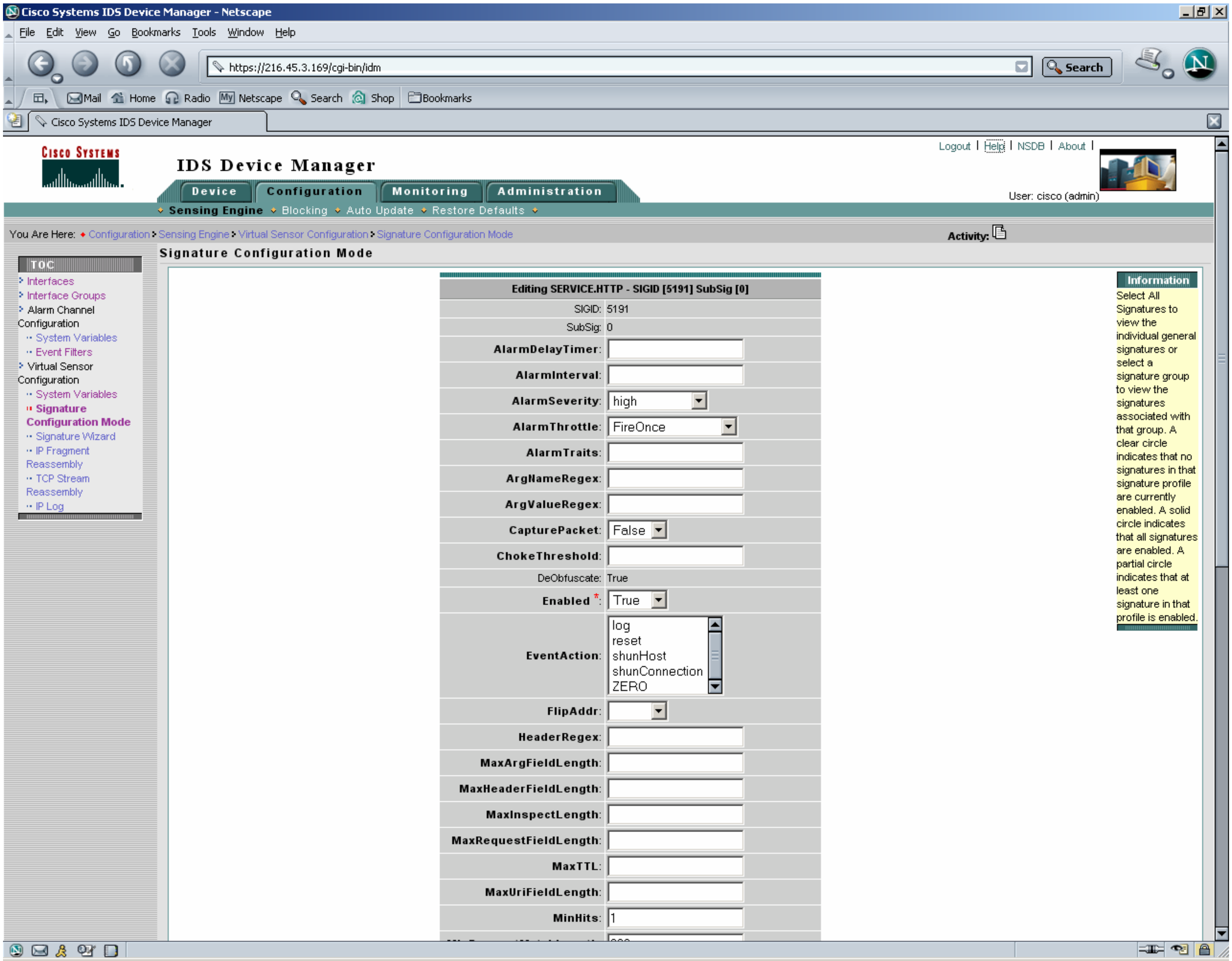
Showing 1-1 of 1

#		SIGID	SubSig	Exception	SourceAddrs	DestAddrs
1.	□	5112	*	False	$USER-ADDRS1	*

Rows per page: 10

Page: 1 [1-1]

Question 12


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
User: cisco (admin)
You Are Here: Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode
Activity:
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Information

Signature Configuration Mode

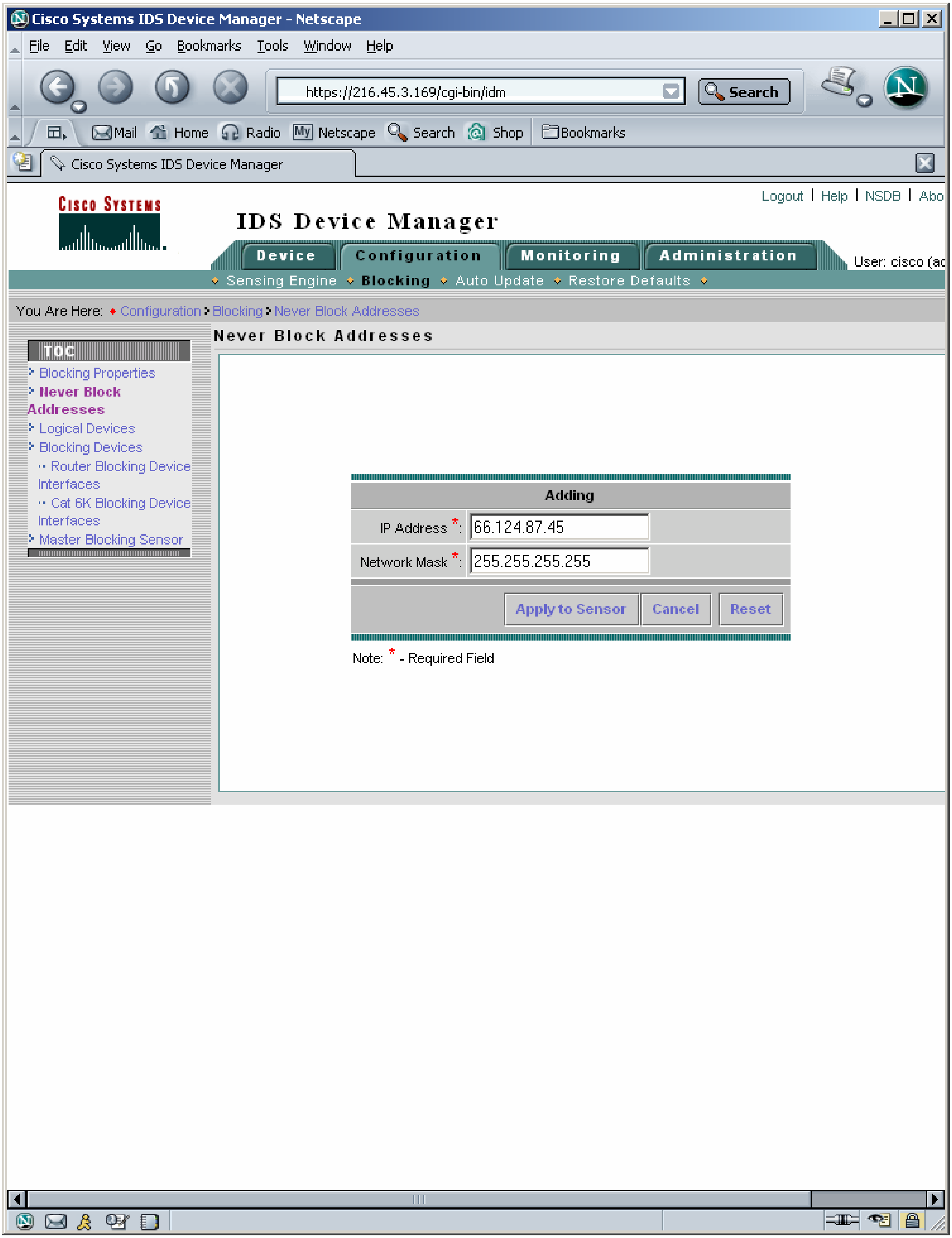
Editing SERVICE.HTTP - SIGID [5191] SubSig [0]

SIGID:	5191
SubSig:	0
AlarmDelayTimer:	
AlarmInterval:	
AlarmSeverity:	high
AlarmThrottle:	FireOnce
AlarmTraits:	
ArgNameRegex:	
ArgValueRegex:	
CapturePacket:	False
ChokeThreshold:	
DeObfuscate:	True
Enabled *:	True
EventAction:	log reset shunHost shunConnection ZERO
FlipAddr:	
HeaderRegex:	
MaxArgFieldLength:	
MaxHeaderFieldLength:	
MaxInspectLength:	
MaxRequestFieldLength:	
MaxTTL:	
MaxUriFieldLength:	
MinHits:	1

Select All Signatures to view the individual general signatures or select a signature group to view the signatures associated with that group. A clear circle indicates that no signatures in that signature profile are currently enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that profile is enabled.

Question 13

Question 14


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | Abo
IDS Device Manager
Device Configuration Monitoring Administration
User: cisco (ad
Sensing Engine Blocking Auto Update Restore Defaults
You Are Here: Configuration > Blocking > Never Block Addresses
TOC
Blocking Properties
Never Block Addresses
Logical Devices
Blocking Devices
Router Blocking Device Interfaces
Cat 6K Blocking Device Interfaces
Master Blocking Sensor

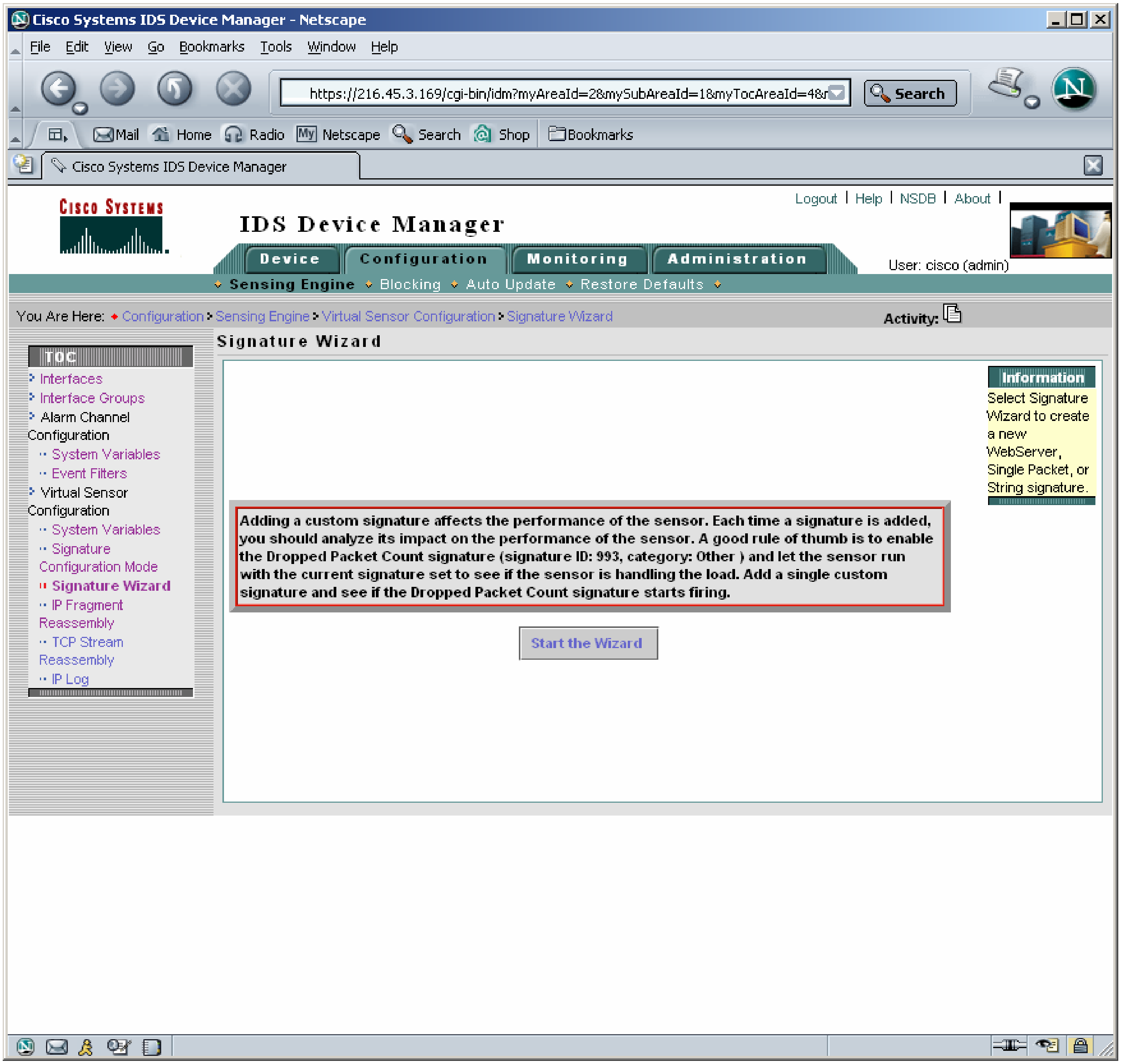
Never Block Addresses

Adding

IP Address *:	66.124.87.45
Network Mask *:	255.255.255.255

Apply to Sensor
Cancel
Reset

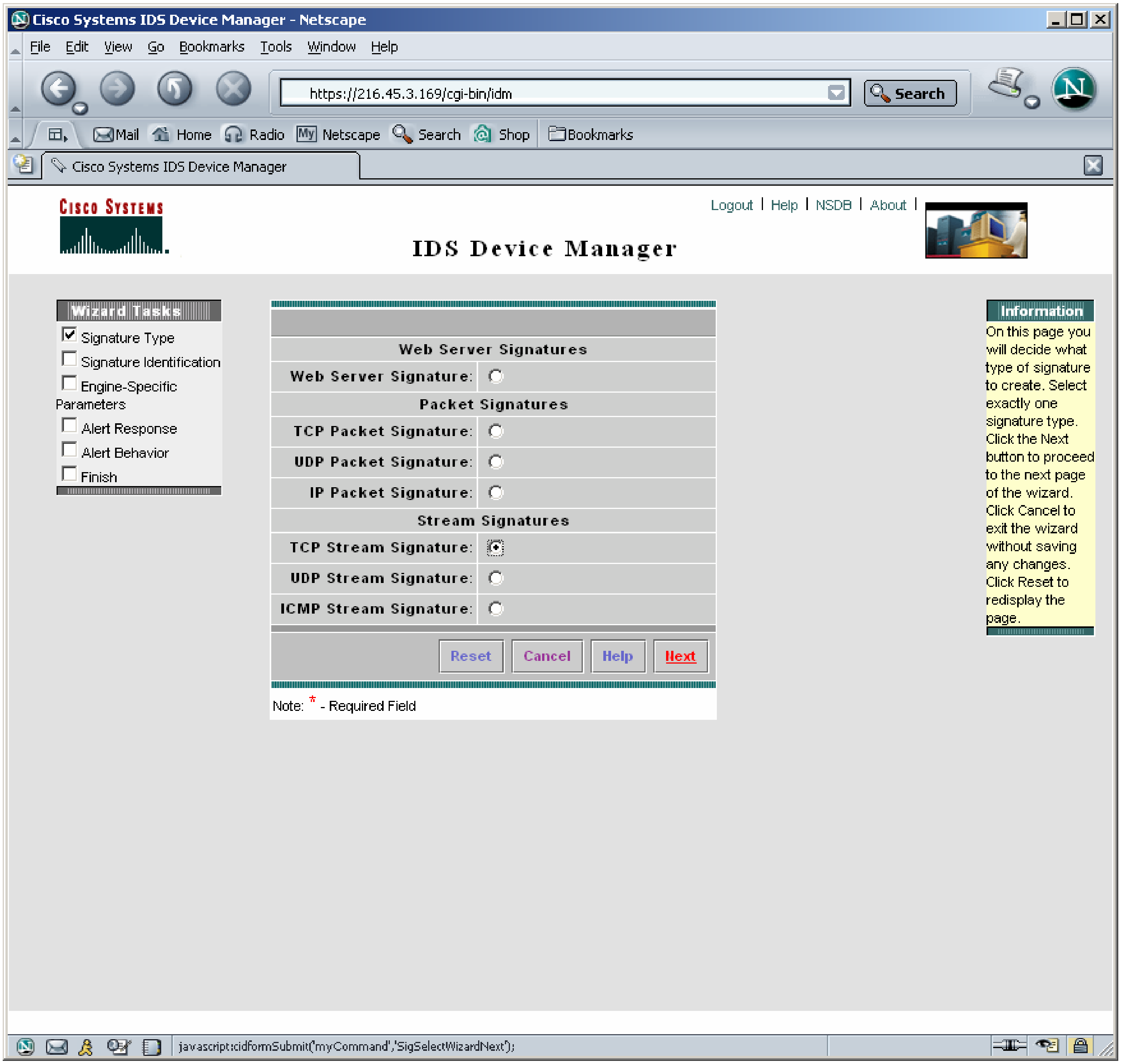
Note: * - Required Field


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm?myAreaId=2&mySubAreaId=1&myTocAreaId=4&r
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager
Device Configuration Monitoring Administration
User: cisco (admin)
Sensing Engine Blocking Auto Update Restore Defaults
You Are Here: Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Wizard
Activity:
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Information
Start the Wizard

Signature Wizard

Select Signature Wizard to create a new WebServer, Single Packet, or String signature.

Adding a custom signature affects the performance of the sensor. Each time a signature is added, you should analyze its impact on the performance of the sensor. A good rule of thumb is to enable the Dropped Packet Count signature (signature ID: 993, category: Other) and let the sensor run with the current signature set to see if the sensor is handling the load. Add a single custom signature and see if the Dropped Packet Count signature starts firing.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |

IDS Device Manager

Wizard Tasks

☑ Signature Type
□ Signature Identification
□ Engine-Specific Parameters
□ Alert Response
□ Alert Behavior
□ Finish

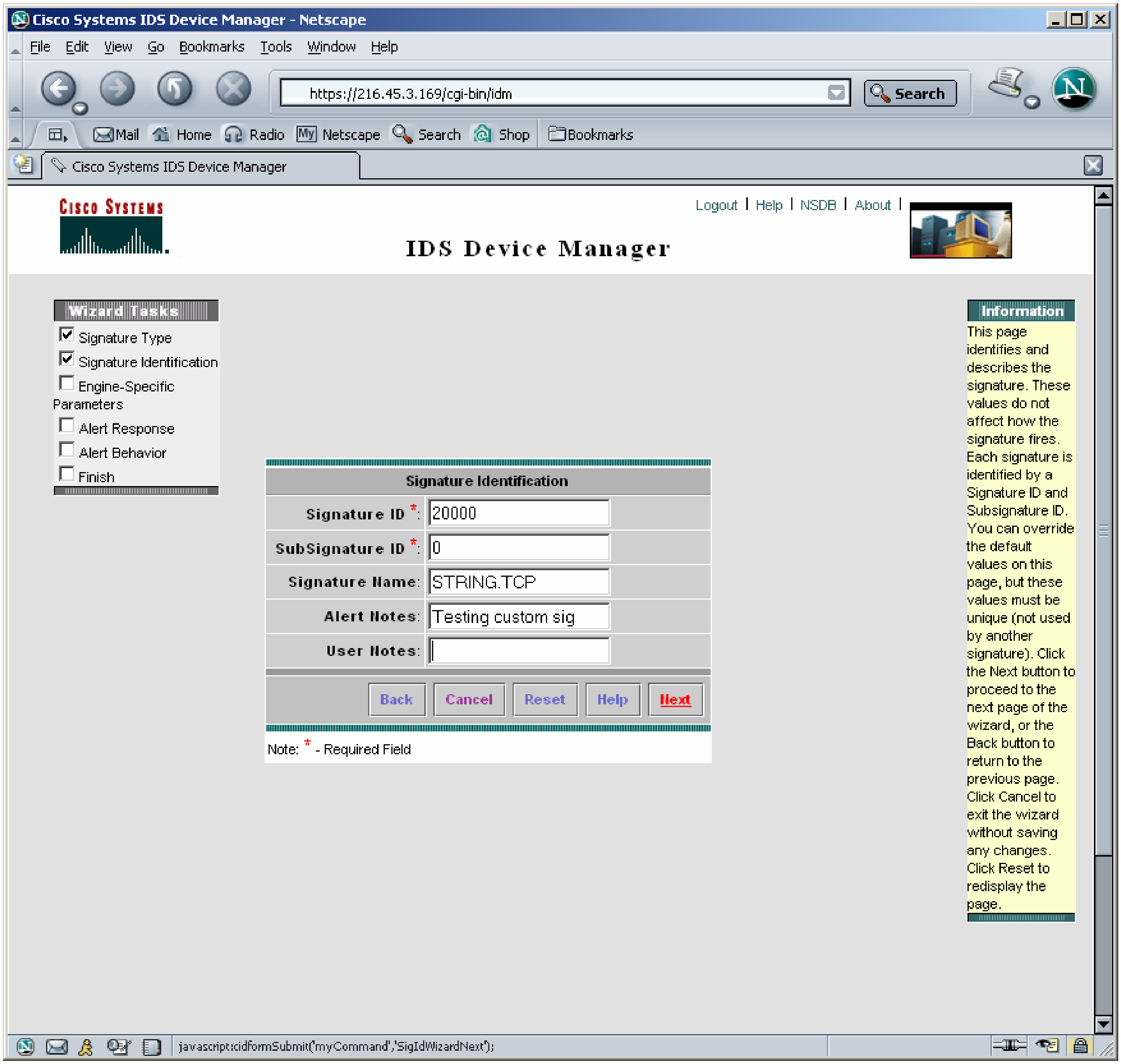
Web Server Signatures	
Web Server Signature:	○
Packet Signatures	
TCP Packet Signature:	○
UDP Packet Signature:	○
IP Packet Signature:	○
Stream Signatures	
TCP Stream Signature:	●
UDP Stream Signature:	○
ICMP Stream Signature:	○

Note: * - Required Field

Information

On this page you will decide what type of signature to create. Select exactly one signature type. Click the Next button to proceed to the next page of the wizard. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the page.

javascript:cidformSubmit('myCommand','SigSelectWizardNext');


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
javascript:cidformSubmit('myCommand','SigIdWizardNext');

IDS Device Manager

Wizard Tasks

- ☑ Signature Type
- ☑ Signature Identification
- □ Engine-Specific Parameters
- □ Alert Response
- □ Alert Behavior
- □ Finish

Signature Identification

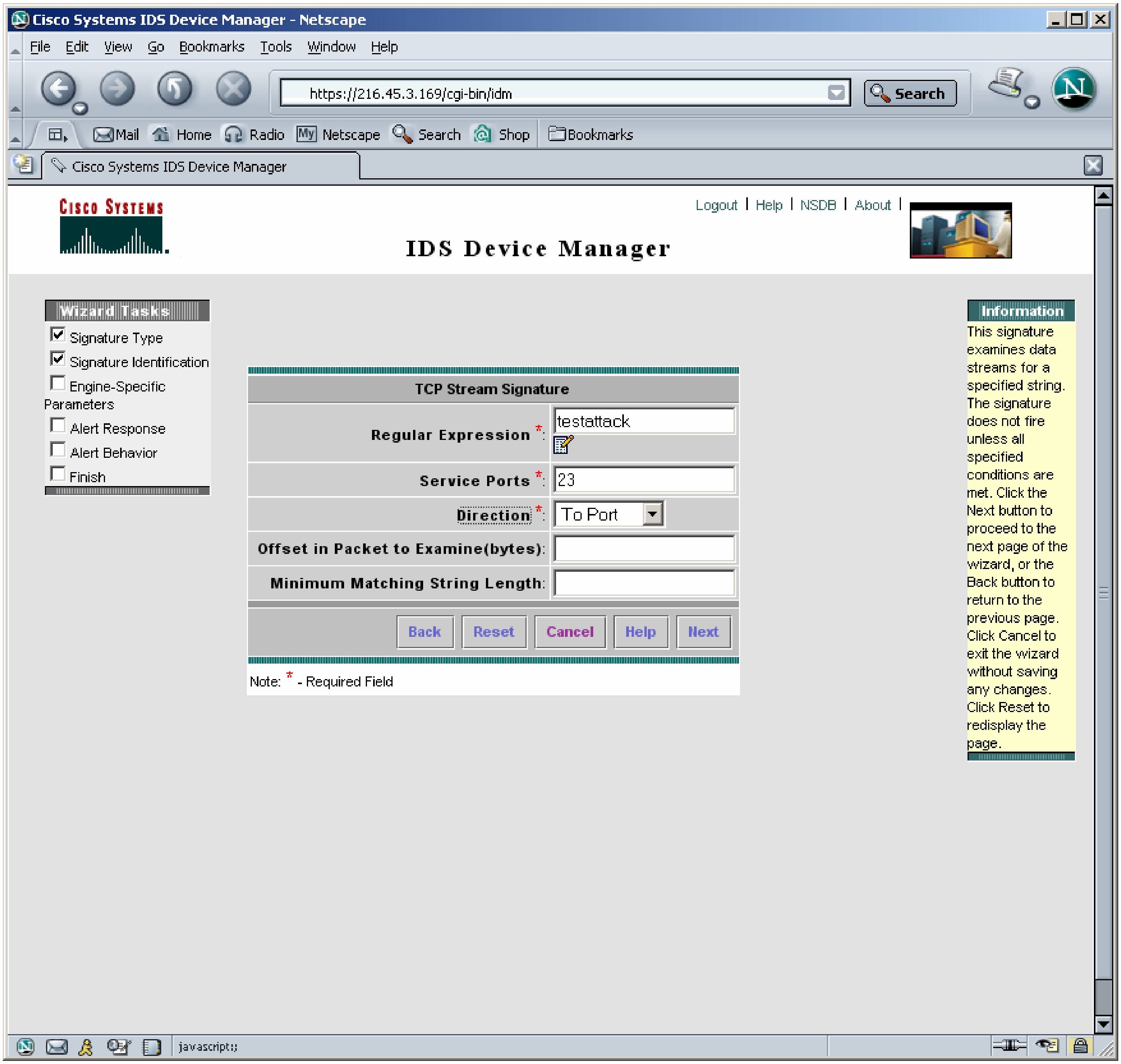
Signature ID *:	20000
SubSignature ID *:	0
Signature Name:	STRING.TCP
Alert Notes:	Testing custom sig
User Notes:	

Back Cancel Reset Help Next

Note: * - Required Field

Information

This page identifies and describes the signature. These values do not affect how the signature fires. Each signature is identified by a Signature ID and Subsignature ID. You can override the default values on this page, but these values must be unique (not used by another signature). Click the Next button to proceed to the next page of the wizard, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the page.



IDS Device Manager

Wizard Tasks

- ☑ Signature Type
- ☑ Signature Identification
- □ Engine-Specific Parameters
- □ Alert Response
- □ Alert Behavior
- □ Finish

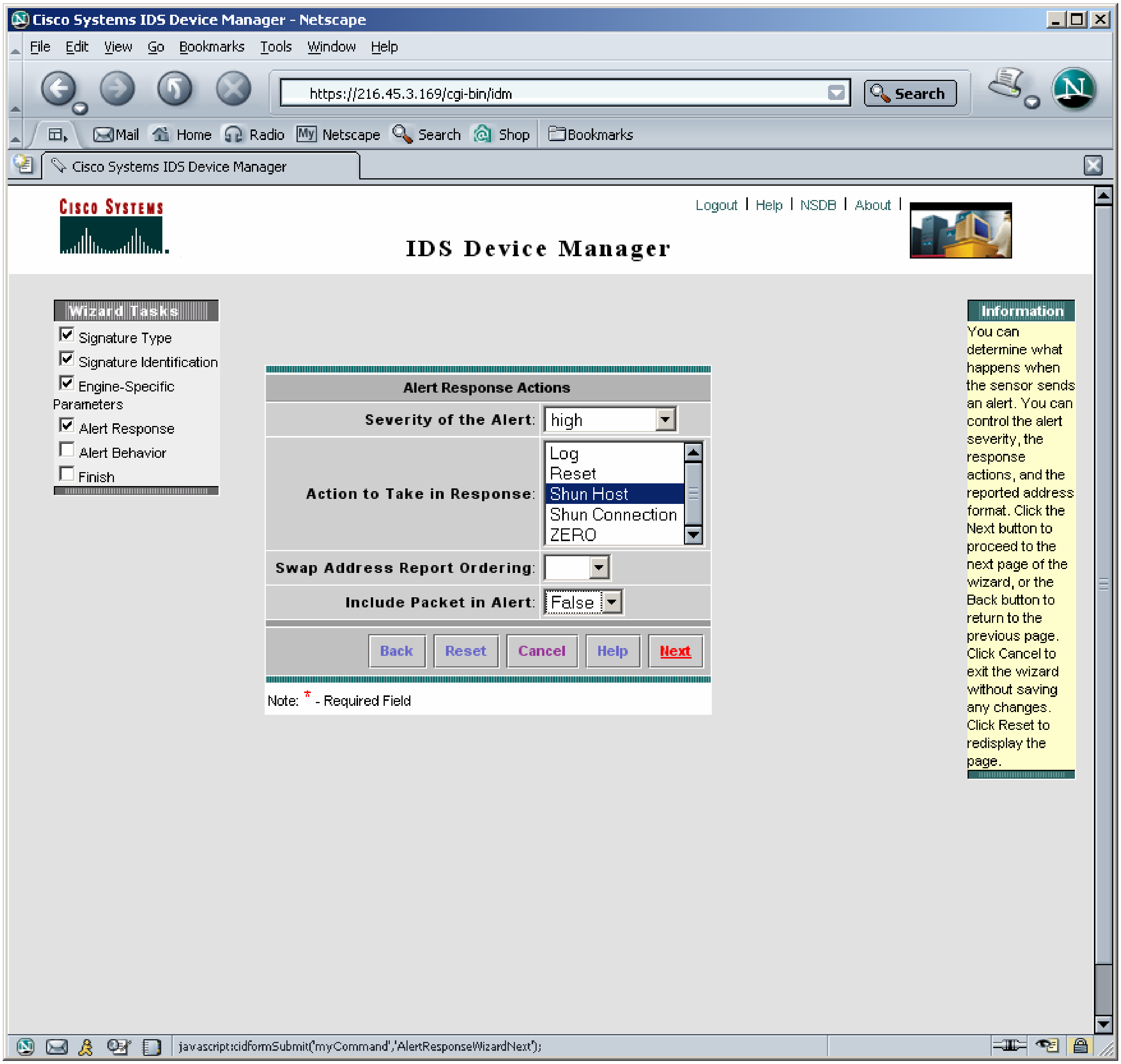
TCP Stream Signature

Regular Expression *:	testattack
Service Ports *:	23
Direction *:	To Port
Offset in Packet to Examine(bytes):	
Minimum Matching String Length:	

Note: * - Required Field

Information

This signature examines data streams for a specified string. The signature does not fire unless all specified conditions are met. Click the Next button to proceed to the next page of the wizard, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the page.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager
Wizard Tasks

☑ Signature Type
☑ Signature Identification
☑ Engine-Specific Parameters
☑ Alert Response
☐ Alert Behavior
☐ Finish

Alert Response Actions

Severity of the Alert:	high
Action to Take in Response:	Log Reset Shun Host Shun Connection ZERO
Swap Address Report Ordering:	
Include Packet in Alert:	False

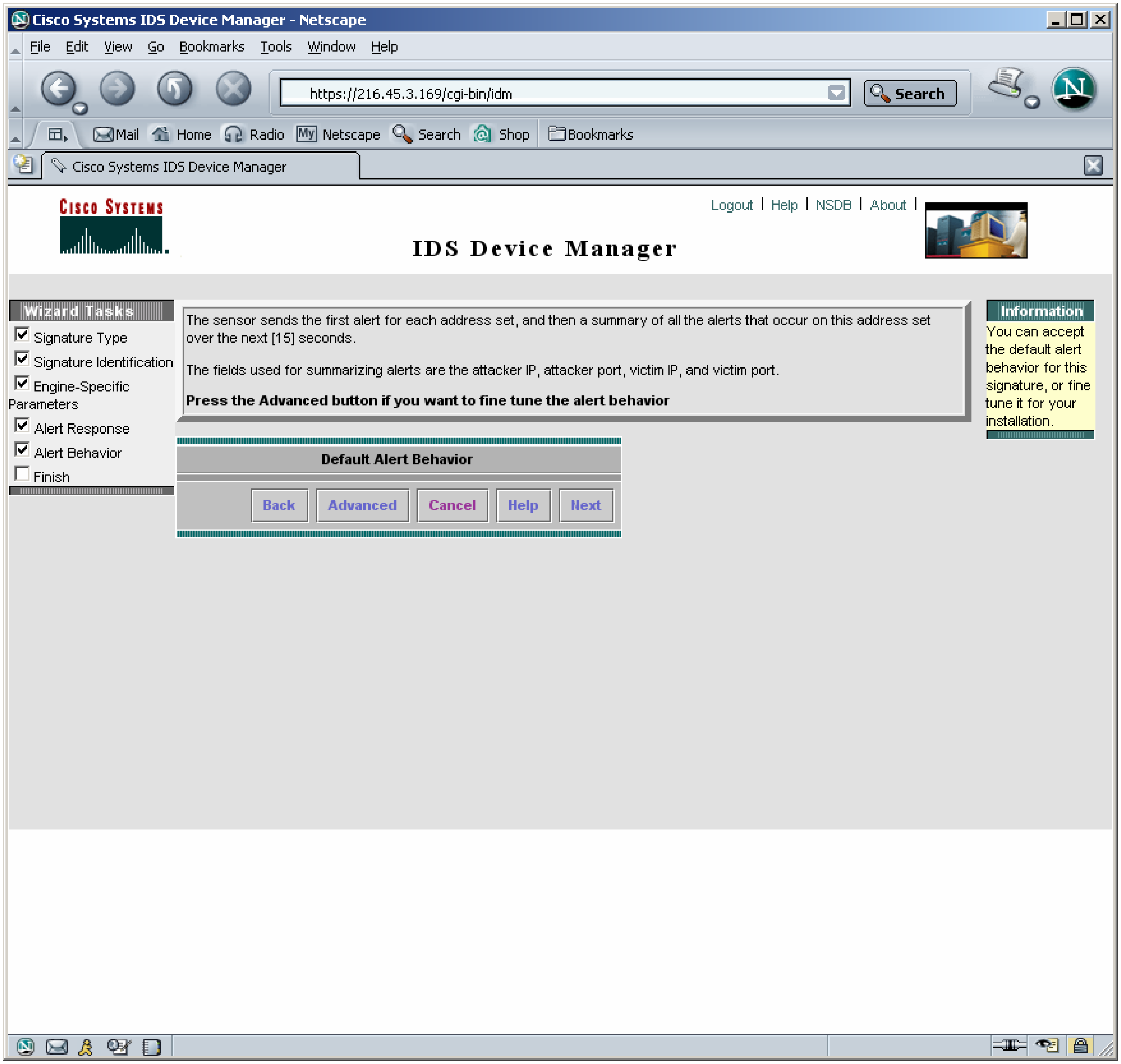
Back Reset Cancel Help Next

Note: * - Required Field

Information

You can determine what happens when the sensor sends an alert. You can control the alert severity, the response actions, and the reported address format. Click the Next button to proceed to the next page of the wizard, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the page.

javascript:cidformSubmit('myCommand','AlertResponseWizardNext');



Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager

Wizard Tasks

☑ Signature Type
☑ Signature Identification
☑ Engine-Specific Parameters
☑ Alert Response
☑ Alert Behavior
☐ Finish

The sensor sends the first alert for each address set, and then a summary of all the alerts that occur on this address set over the next [15] seconds.

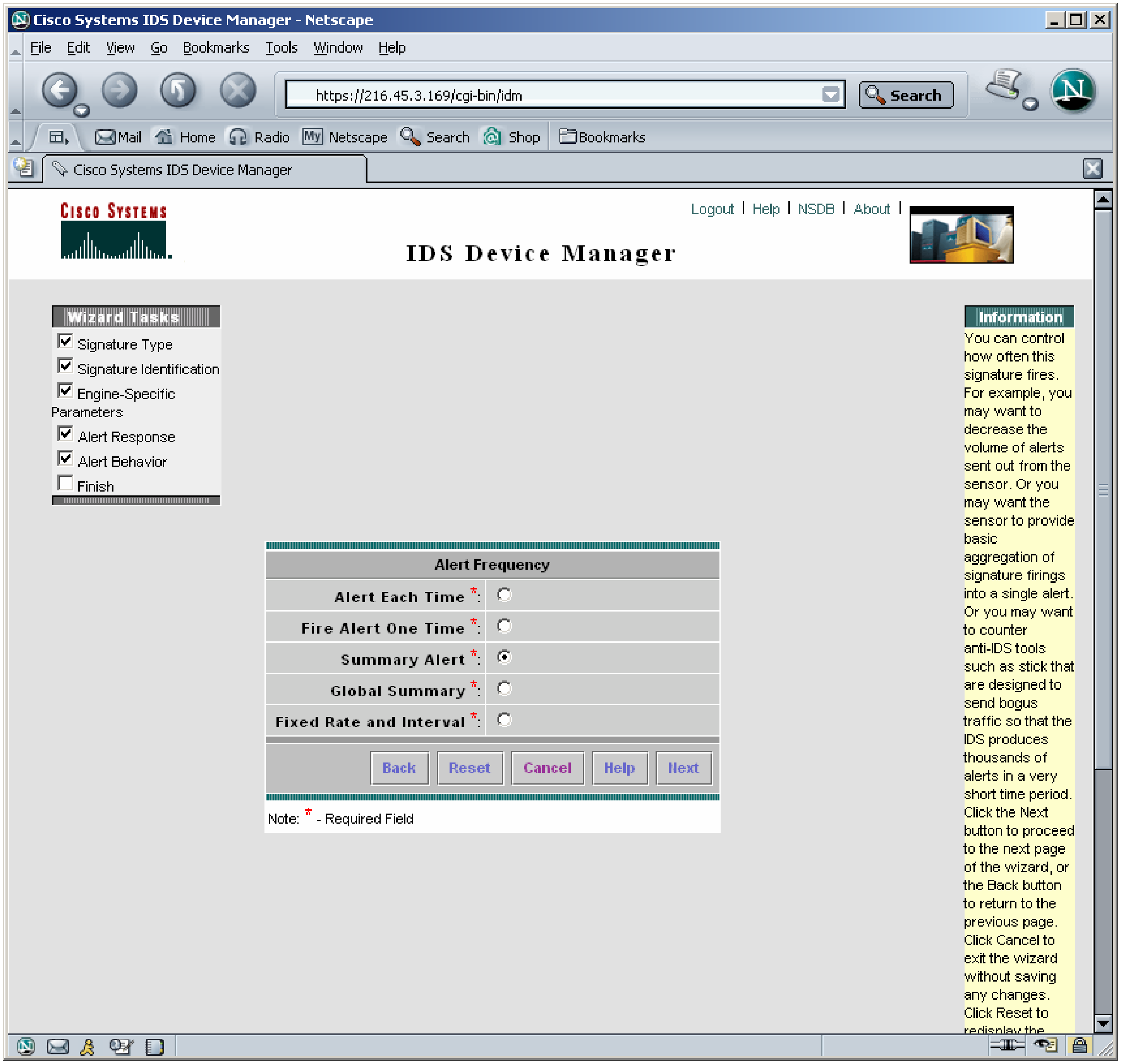
The fields used for summarizing alerts are the attacker IP, attacker port, victim IP, and victim port.

Press the Advanced button if you want to fine tune the alert behavior

Default Alert Behavior

Information

You can accept the default alert behavior for this signature, or fine tune it for your installation.



Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |

IDS Device Manager

Wizard Tasks

- ☑ Signature Type
- ☑ Signature Identification
- ☑ Engine-Specific Parameters
- ☑ Alert Response
- ☑ Alert Behavior
- □ Finish

Alert Frequency

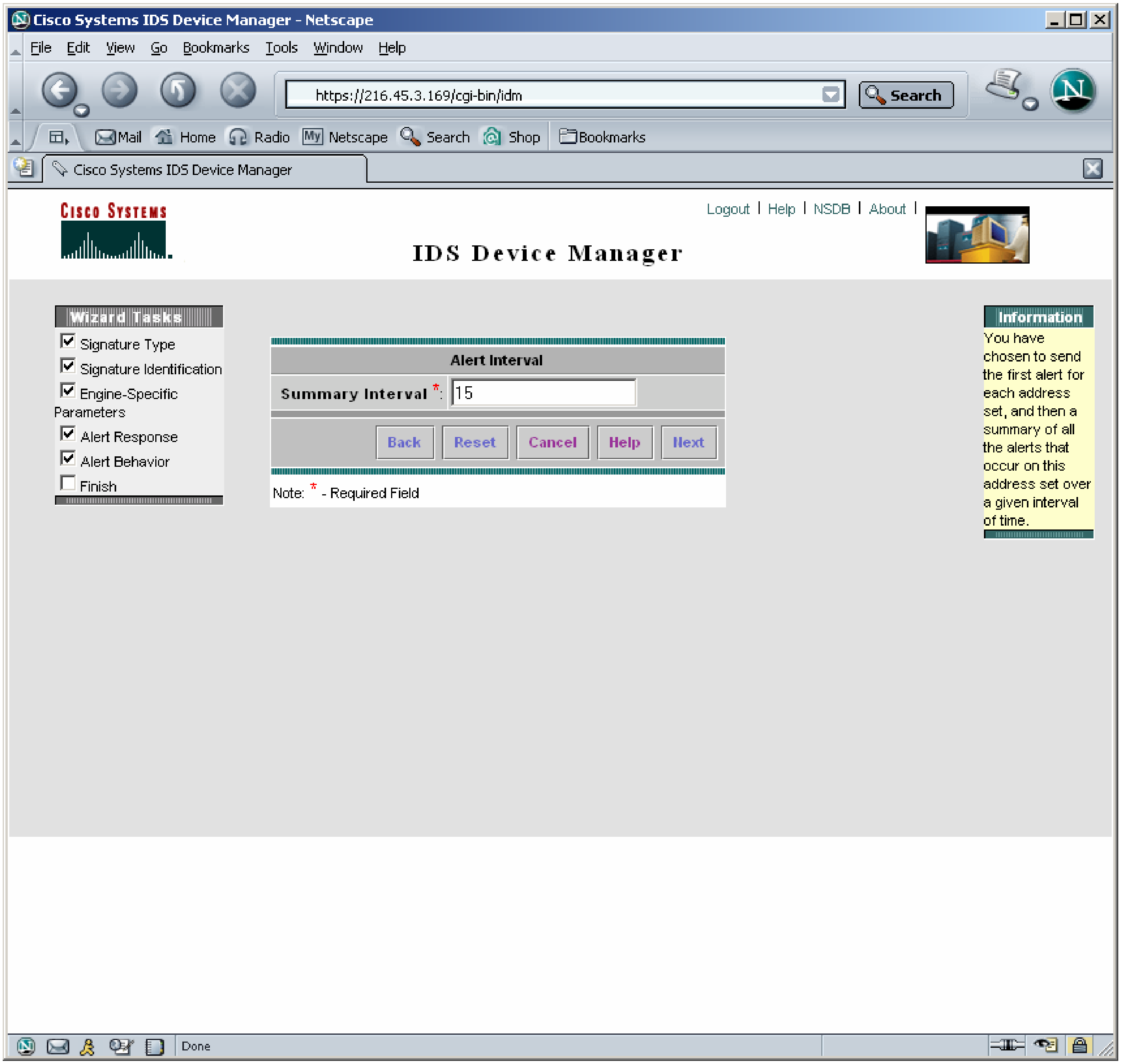
Alert Each Time *:	○
Fire Alert One Time *:	○
Summary Alert *:	●
Global Summary *:	○
Fixed Rate and Interval *:	○

Back
Reset
Cancel
Help
Next

Note: * - Required Field

Information

You can control how often this signature fires. For example, you may want to decrease the volume of alerts sent out from the sensor. Or you may want the sensor to provide basic aggregation of signature firings into a single alert. Or you may want to counter anti-IDS tools such as stick that are designed to send bogus traffic so that the IDS produces thousands of alerts in a very short time period. Click the Next button to proceed to the next page of the wizard, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
Done

URL: https://216.45.3.169/cgi-bin/idm

IDS Device Manager

Wizard Tasks

- ☑ Signature Type
- ☑ Signature Identification
- ☑ Engine-Specific Parameters
- ☑ Alert Response
- ☑ Alert Behavior
- □ Finish

Alert Interval

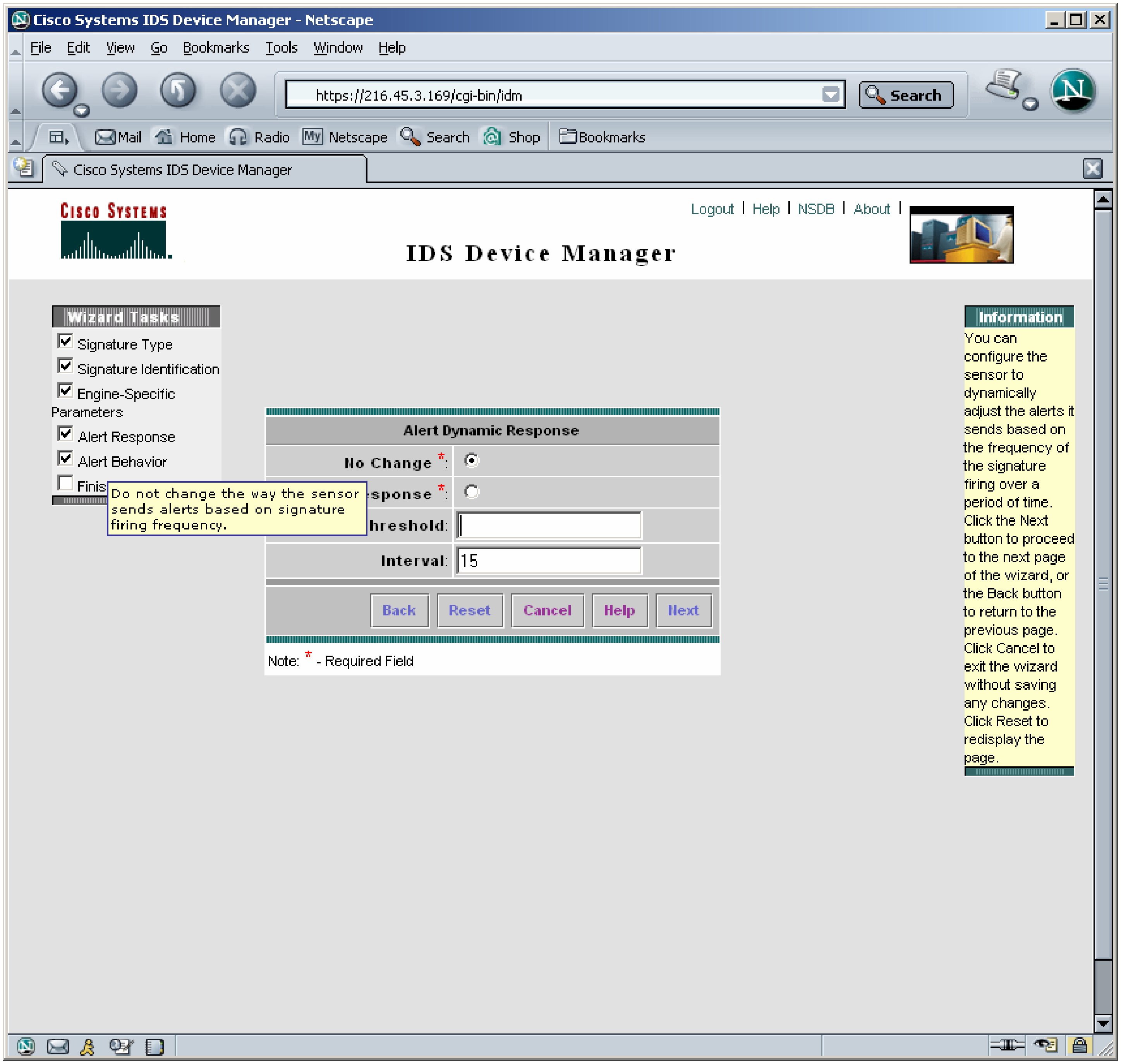
Summary Interval *: 15

Back | Reset | Cancel | Help | Next

Note: * - Required Field

Information

You have chosen to send the first alert for each address set, and then a summary of all the alerts that occur on this address set over a given interval of time.



Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |

IDS Device Manager

Wizard Tasks

☑ Signature Type

☑ Signature Identification

☑ Engine-Specific Parameters

☑ Alert Response

☑ Alert Behavior

☐ Finis

Do not change the way the sensor sends alerts based on signature firing frequency.

Alert Dynamic Response

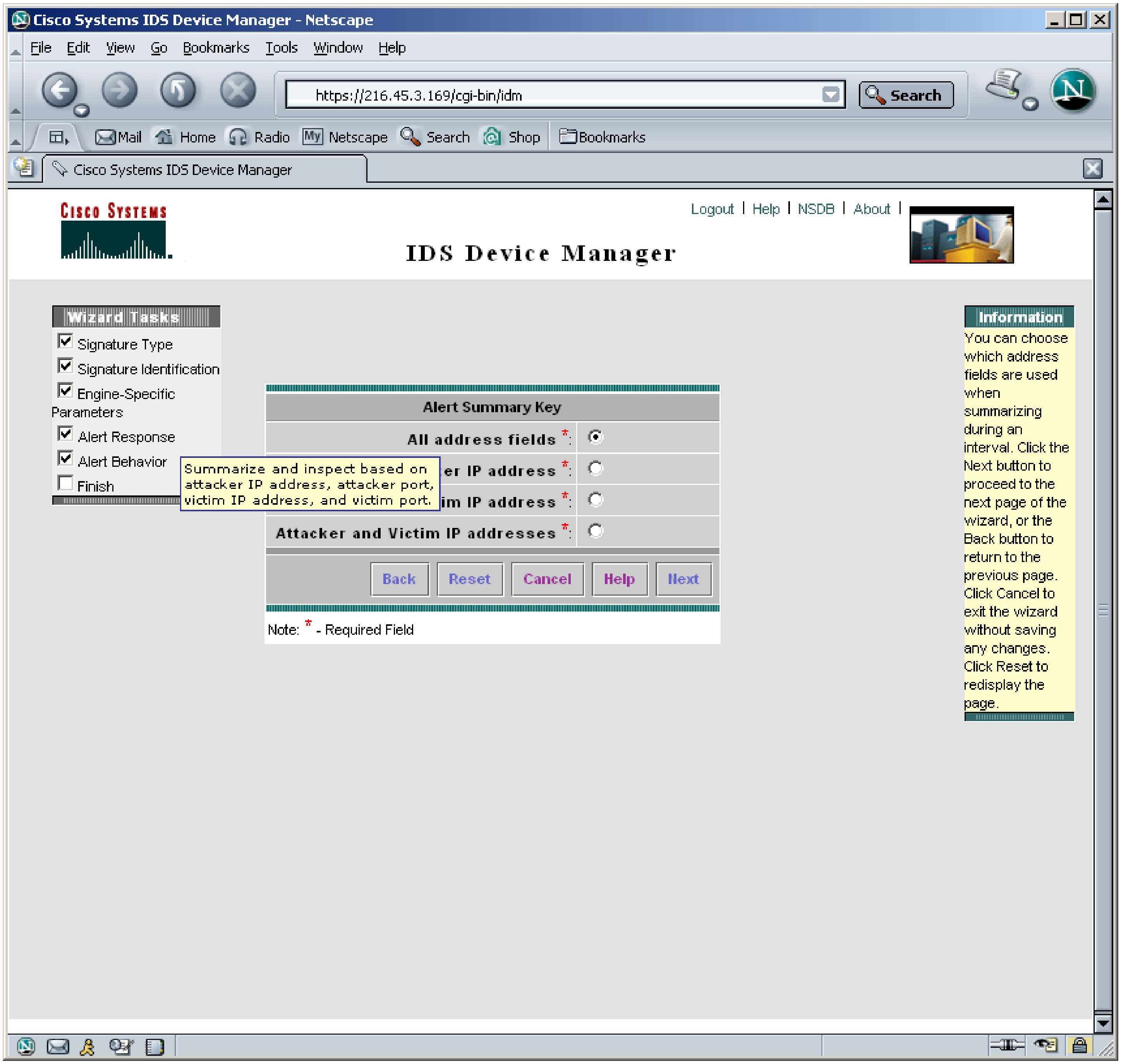
No Change *:	●
sponse *:	○
hreshold:	
Interval:	15

Back Reset Cancel Help Next

Note: * - Required Field

Information

You can configure the sensor to dynamically adjust the alerts it sends based on the frequency of the signature firing over a period of time. Click the Next button to proceed to the next page of the wizard, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the page.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |

IDS Device Manager

Wizard Tasks

☑ Signature Type
☑ Signature Identification
☑ Engine-Specific Parameters
☑ Alert Response
☑ Alert Behavior
□ Finish

Alert Summary Key	
All address fields *:	●
er IP address *:	○
im IP address *:	○
Attacker and Victim IP addresses *:	○

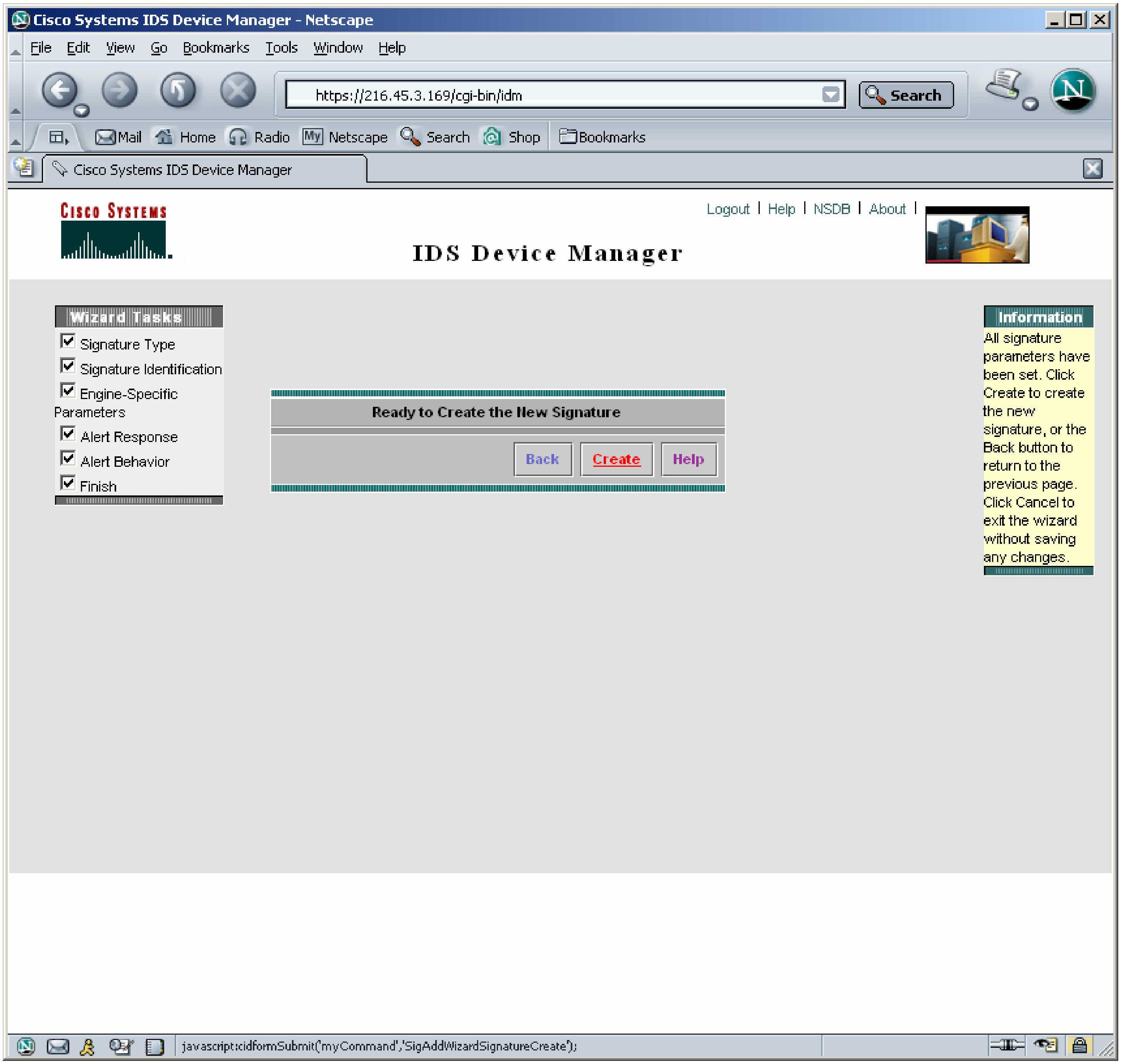
Summarize and inspect based on attacker IP address, attacker port, victim IP address, and victim port.

Back Reset Cancel Help Next

Note: * - Required Field

Information

You can choose which address fields are used when summarizing during an interval. Click the Next button to proceed to the next page of the wizard, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes. Click Reset to redisplay the page.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager
Wizard Tasks

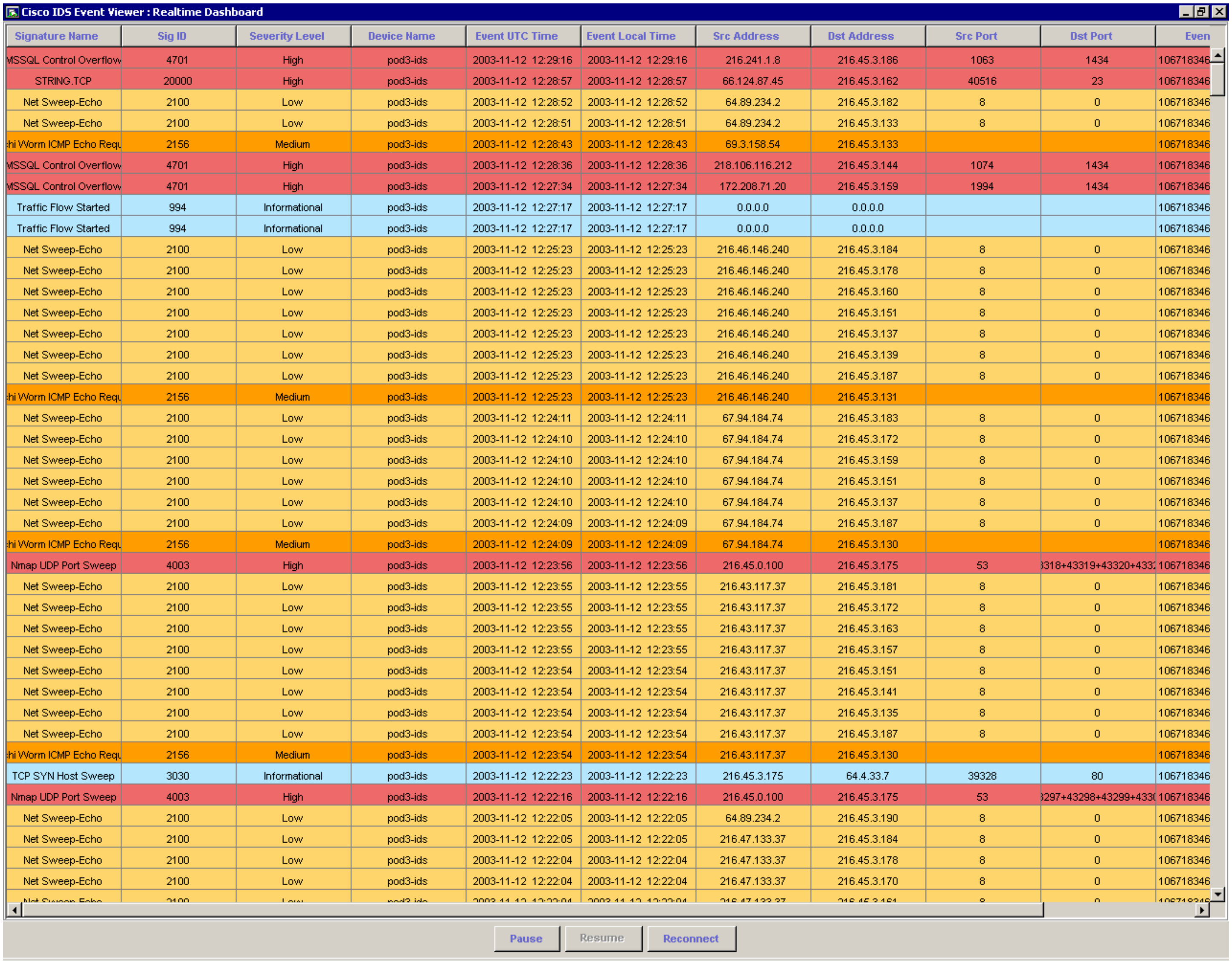
☑ Signature Type
☑ Signature Identification
☑ Engine-Specific Parameters
☑ Alert Response
☑ Alert Behavior
☑ Finish

Ready to Create the New Signature

Information

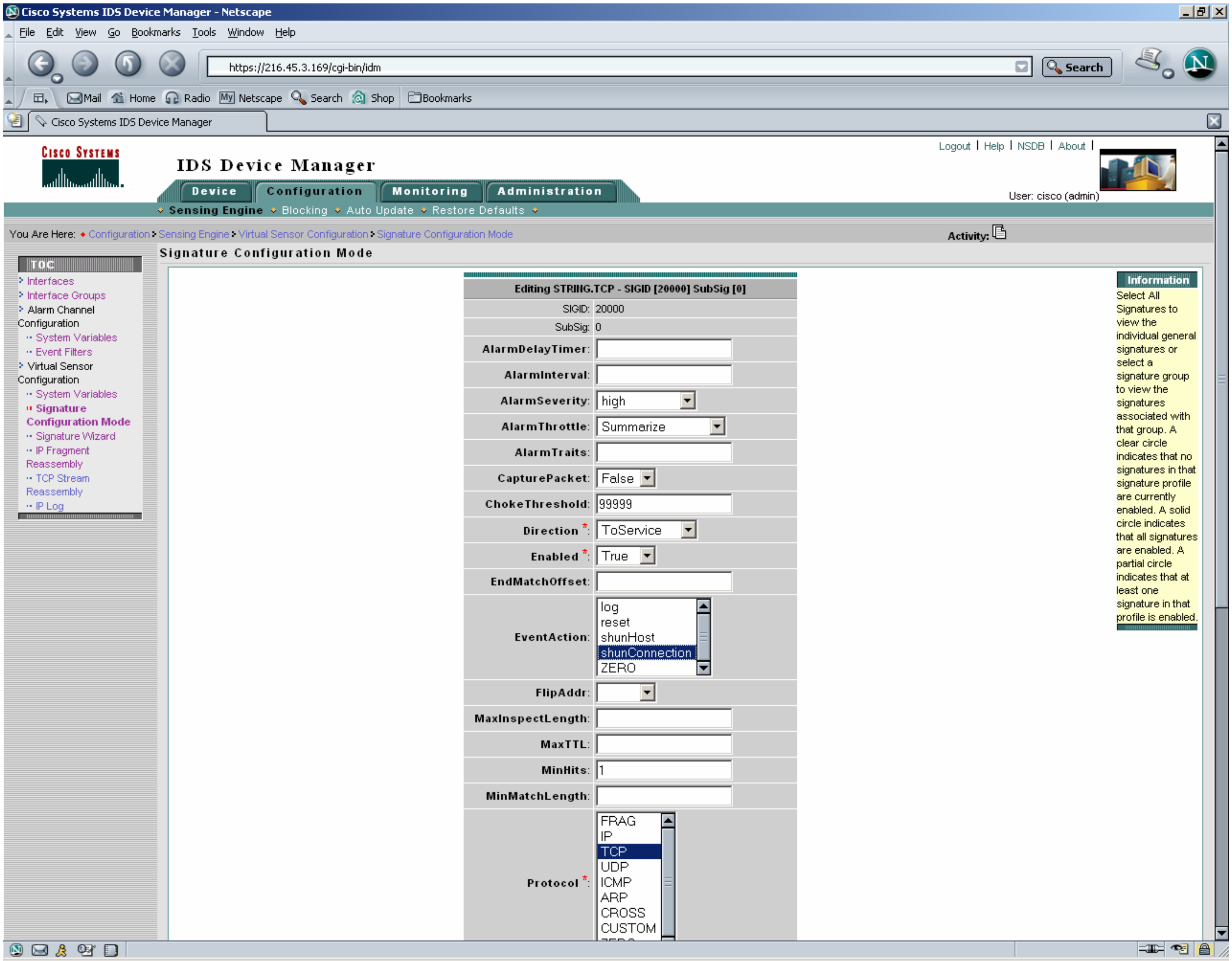
All signature parameters have been set. Click Create to create the new signature, or the Back button to return to the previous page. Click Cancel to exit the wizard without saving any changes.

javascript:cidformSubmit('myCommand','SigAddWizardSignatureCreate');



Cisco IDS Event Viewer : Realtime Dashboard

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst Address	Src Port	Dst Port	Even
MSSQL Control Overflow	4701	High	pod3-ids	2003-11-12 12:29:16	2003-11-12 12:29:16	216.241.1.8	216.45.3.186	1063	1434	106718346
STRING.TCP	20000	High	pod3-ids	2003-11-12 12:28:57	2003-11-12 12:28:57	66.124.87.45	216.45.3.162	40516	23	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:28:52	2003-11-12 12:28:52	64.89.234.2	216.45.3.182	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:28:51	2003-11-12 12:28:51	64.89.234.2	216.45.3.133	8	0	106718346
hi Worm ICMP Echo Requ	2156	Medium	pod3-ids	2003-11-12 12:28:43	2003-11-12 12:28:43	69.3.158.54	216.45.3.133			106718346
MSSQL Control Overflow	4701	High	pod3-ids	2003-11-12 12:28:36	2003-11-12 12:28:36	218.106.116.212	216.45.3.144	1074	1434	106718346
MSSQL Control Overflow	4701	High	pod3-ids	2003-11-12 12:27:34	2003-11-12 12:27:34	172.208.71.20	216.45.3.159	1994	1434	106718346
Traffic Flow Started	994	Informational	pod3-ids	2003-11-12 12:27:17	2003-11-12 12:27:17	0.0.0.0	0.0.0.0			106718346
Traffic Flow Started	994	Informational	pod3-ids	2003-11-12 12:27:17	2003-11-12 12:27:17	0.0.0.0	0.0.0.0			106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.184	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.178	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.160	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.151	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.137	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.139	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.187	8	0	106718346
hi Worm ICMP Echo Requ	2156	Medium	pod3-ids	2003-11-12 12:25:23	2003-11-12 12:25:23	216.46.146.240	216.45.3.131			106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:24:11	2003-11-12 12:24:11	67.94.184.74	216.45.3.183	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:24:10	2003-11-12 12:24:10	67.94.184.74	216.45.3.172	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:24:10	2003-11-12 12:24:10	67.94.184.74	216.45.3.159	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:24:10	2003-11-12 12:24:10	67.94.184.74	216.45.3.151	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:24:10	2003-11-12 12:24:10	67.94.184.74	216.45.3.137	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:24:09	2003-11-12 12:24:09	67.94.184.74	216.45.3.187	8	0	106718346
hi Worm ICMP Echo Requ	2156	Medium	pod3-ids	2003-11-12 12:24:09	2003-11-12 12:24:09	67.94.184.74	216.45.3.130			106718346
Nmap UDP Port Sweep	4003	High	pod3-ids	2003-11-12 12:23:56	2003-11-12 12:23:56	216.45.0.100	216.45.3.175	53	3318+43319+43320+4333	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:55	2003-11-12 12:23:55	216.43.117.37	216.45.3.181	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:55	2003-11-12 12:23:55	216.43.117.37	216.45.3.172	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:55	2003-11-12 12:23:55	216.43.117.37	216.45.3.163	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:55	2003-11-12 12:23:55	216.43.117.37	216.45.3.157	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:54	2003-11-12 12:23:54	216.43.117.37	216.45.3.151	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:54	2003-11-12 12:23:54	216.43.117.37	216.45.3.141	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:54	2003-11-12 12:23:54	216.43.117.37	216.45.3.135	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:23:54	2003-11-12 12:23:54	216.43.117.37	216.45.3.187	8	0	106718346
hi Worm ICMP Echo Requ	2156	Medium	pod3-ids	2003-11-12 12:23:54	2003-11-12 12:23:54	216.43.117.37	216.45.3.130			106718346
TCP SYN Host Sweep	3030	Informational	pod3-ids	2003-11-12 12:22:23	2003-11-12 12:22:23	216.45.3.175	64.4.33.7	39328	80	106718346
Nmap UDP Port Sweep	4003	High	pod3-ids	2003-11-12 12:22:16	2003-11-12 12:22:16	216.45.0.100	216.45.3.175	53	3297+43298+43299+433(	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:22:05	2003-11-12 12:22:05	64.89.234.2	216.45.3.190	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:22:05	2003-11-12 12:22:05	216.47.133.37	216.45.3.184	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:22:04	2003-11-12 12:22:04	216.47.133.37	216.45.3.178	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:22:04	2003-11-12 12:22:04	216.47.133.37	216.45.3.170	8	0	106718346
Net Sweep-Echo	2100	Low	pod3-ids	2003-11-12 12:22:04	2003-11-12 12:22:04	216.47.133.37	216.45.3.161	8	0	106718346


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
User: cisco (admin)
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
Activity:
TOC
Interfaces
Interface Groups
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Signature Wizard
IP Fragment Reassembly
TCP Stream Reassembly
IP Log
Information

IDS Device Manager

You Are Here: Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode

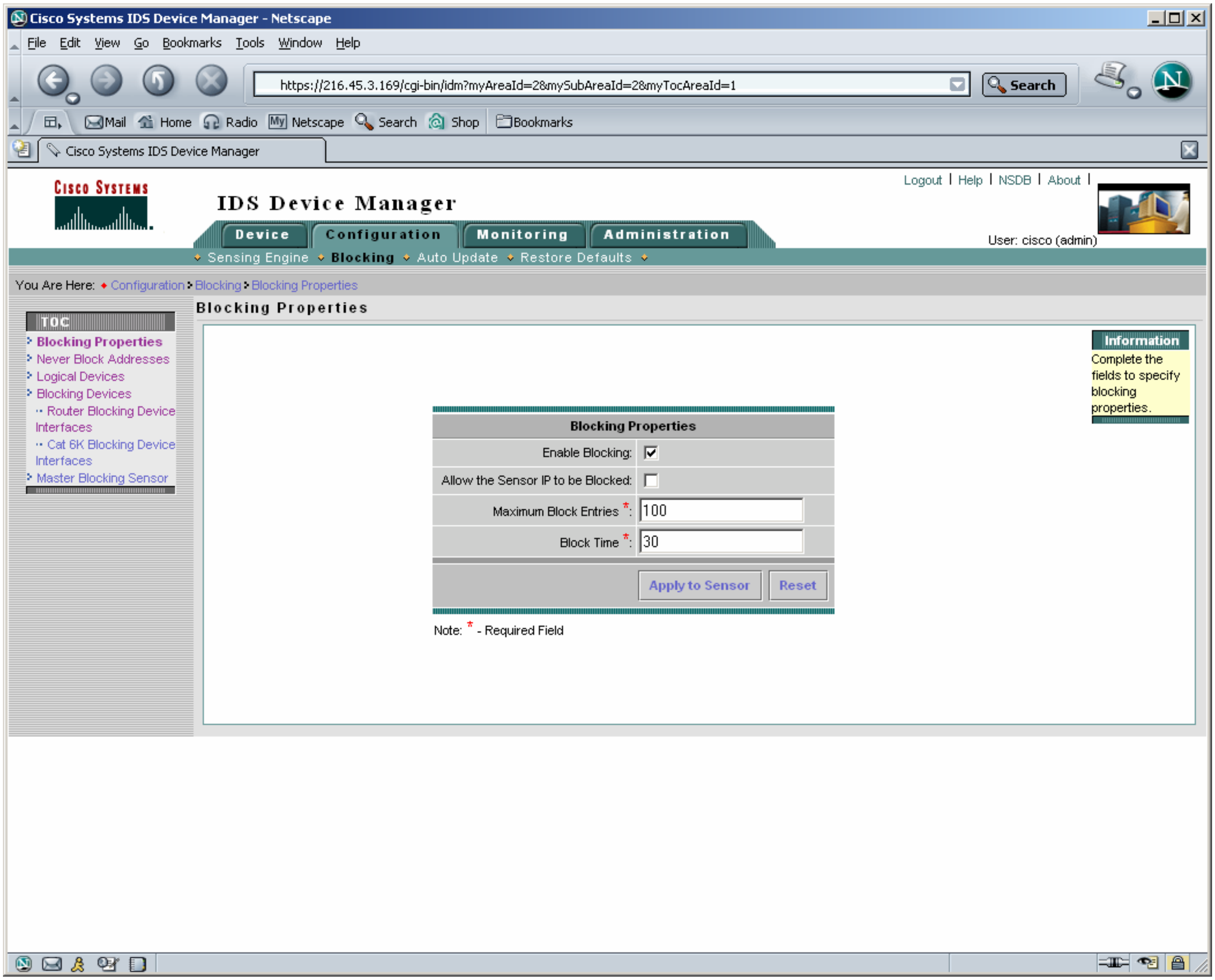
Signature Configuration Mode

Editing STRING.TCP - SIGID [20000] SubSig [0]

SIGID: 20000
SubSig: 0
AlarmDelayTimer:
AlarmInterval:
AlarmSeverity: high
AlarmThrottle: Summarize
AlarmTraits:
CapturePacket: False
ChokeThreshold: 99999
Direction *: ToService
Enabled *: True
EndMatchOffset:
EventAction: log, reset, shunHost, shunConnection (selected), ZERO
FlipAddr:
MaxInspectLength:
MaxTTL:
MinHits: 1
MinMatchLength:
Protocol *: FRAG, IP, TCP (selected), UDP, ICMP, ARP, CROSS, CUSTOM, ZERO

Select All Signatures to view the individual general signatures or select a signature group to view the signatures associated with that group. A clear circle indicates that no signatures in that signature profile are currently enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that profile is enabled.

Question 15


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
Logout | Help | NSDB | About |
IDS Device Manager
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
TOC
Blocking Properties
Never Block Addresses
Logical Devices
Blocking Devices
Router Blocking Device Interfaces
Cat 6K Blocking Device Interfaces
Master Blocking Sensor
Apply to Sensor
Reset

https://216.45.3.169/cgi-bin/idm?myAreaId=2&mySubAreaId=2&myTocAreaId=1

User: cisco (admin)

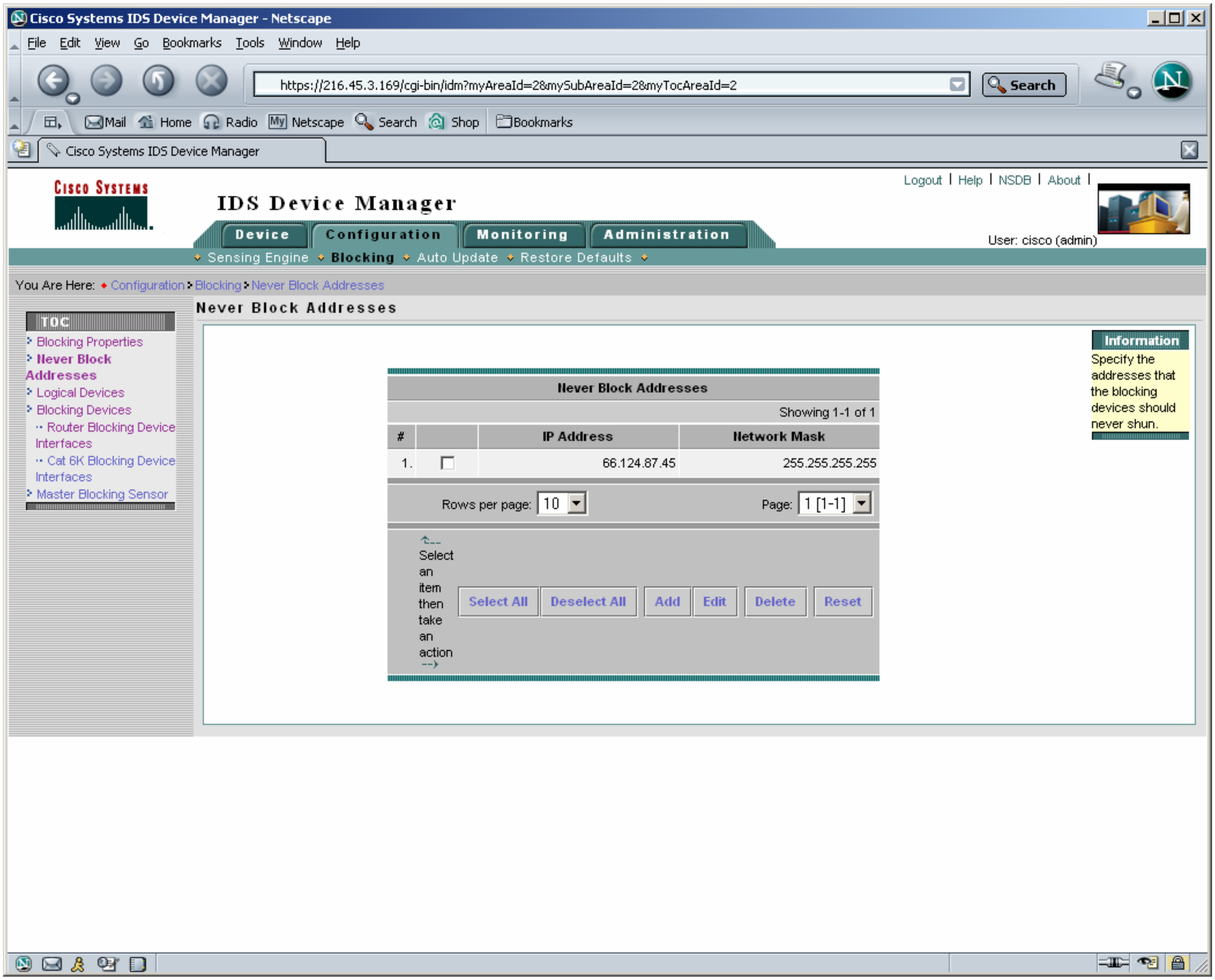
You Are Here: Configuration > Blocking > Blocking Properties

Blocking Properties

Information
Complete the fields to specify blocking properties.

Blocking Properties	
Enable Blocking:	☑
Allow the Sensor IP to be Blocked:	□
Maximum Block Entries *:	100
Block Time *:	30

Note: * - Required Field


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm?myAreaId=2&mySubAreaId=2&myTocAreaId=2
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
IDS Device Manager
Logout | Help | NSDB | About |
User: cisco (admin)
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
You Are Here: Configuration > Blocking > Never Block Addresses
TOC
Blocking Properties
Never Block Addresses
Logical Devices
Blocking Devices
Router Blocking Device Interfaces
Cat 6K Blocking Device Interfaces
Master Blocking Sensor
Information
Rows per page: 10
Page: 1 [1-1]
Select an item then take an action
Select All
Deselect All
Add
Edit
Delete
Reset

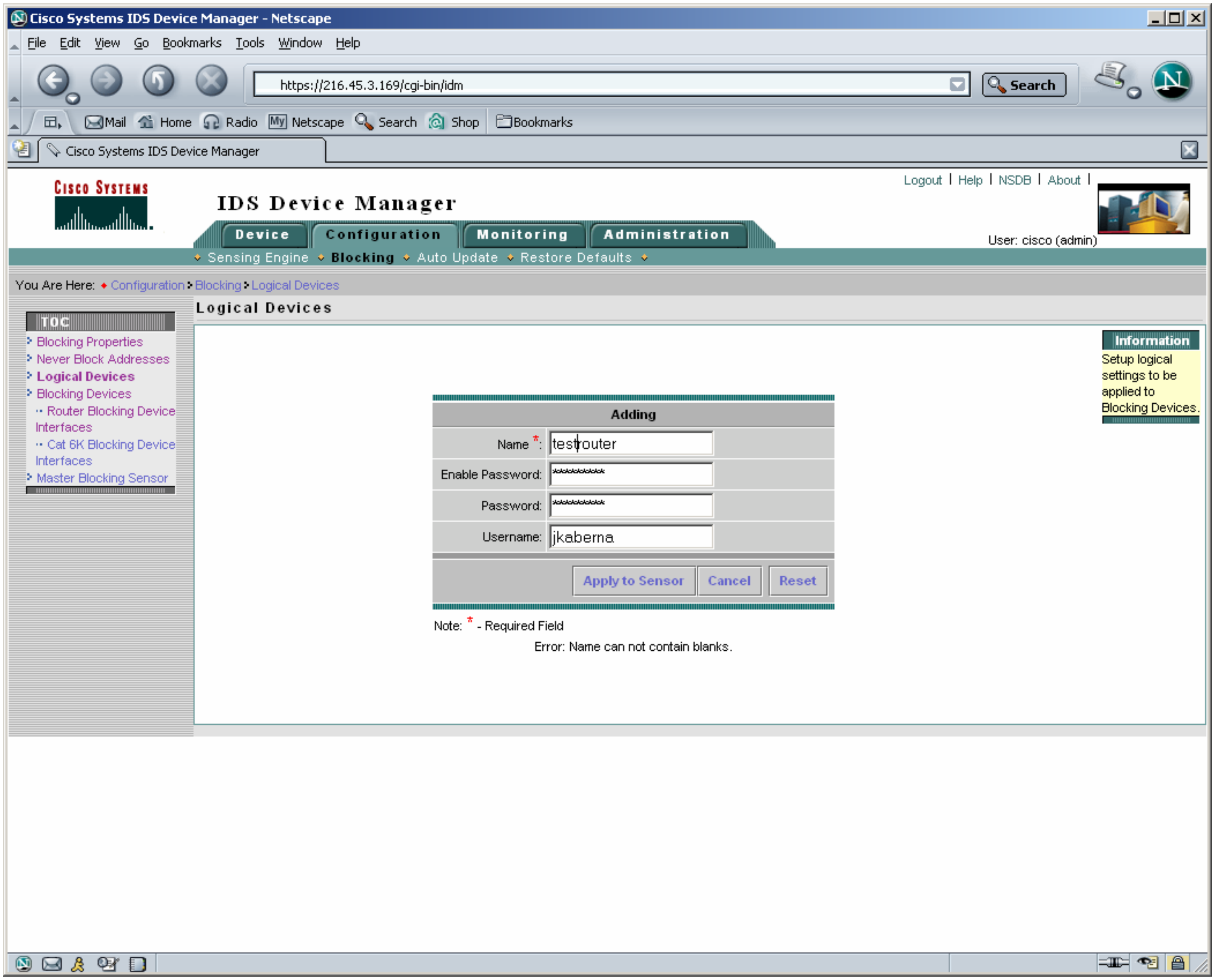
Never Block Addresses

Specify the addresses that the blocking devices should never shun.

Never Block Addresses

Showing 1-1 of 1

#		IP Address	Network Mask
1.	□	66.124.87.45	255.255.255.255


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
IDS Device Manager
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
User: cisco (admin)
You Are Here: Configuration > Blocking > Logical Devices
TOC
Blocking Properties
Never Block Addresses
Logical Devices
Blocking Devices
Router Blocking Device Interfaces
Cat 6K Blocking Device Interfaces
Master Blocking Sensor
Information
Apply to Sensor
Cancel
Reset

Logical Devices

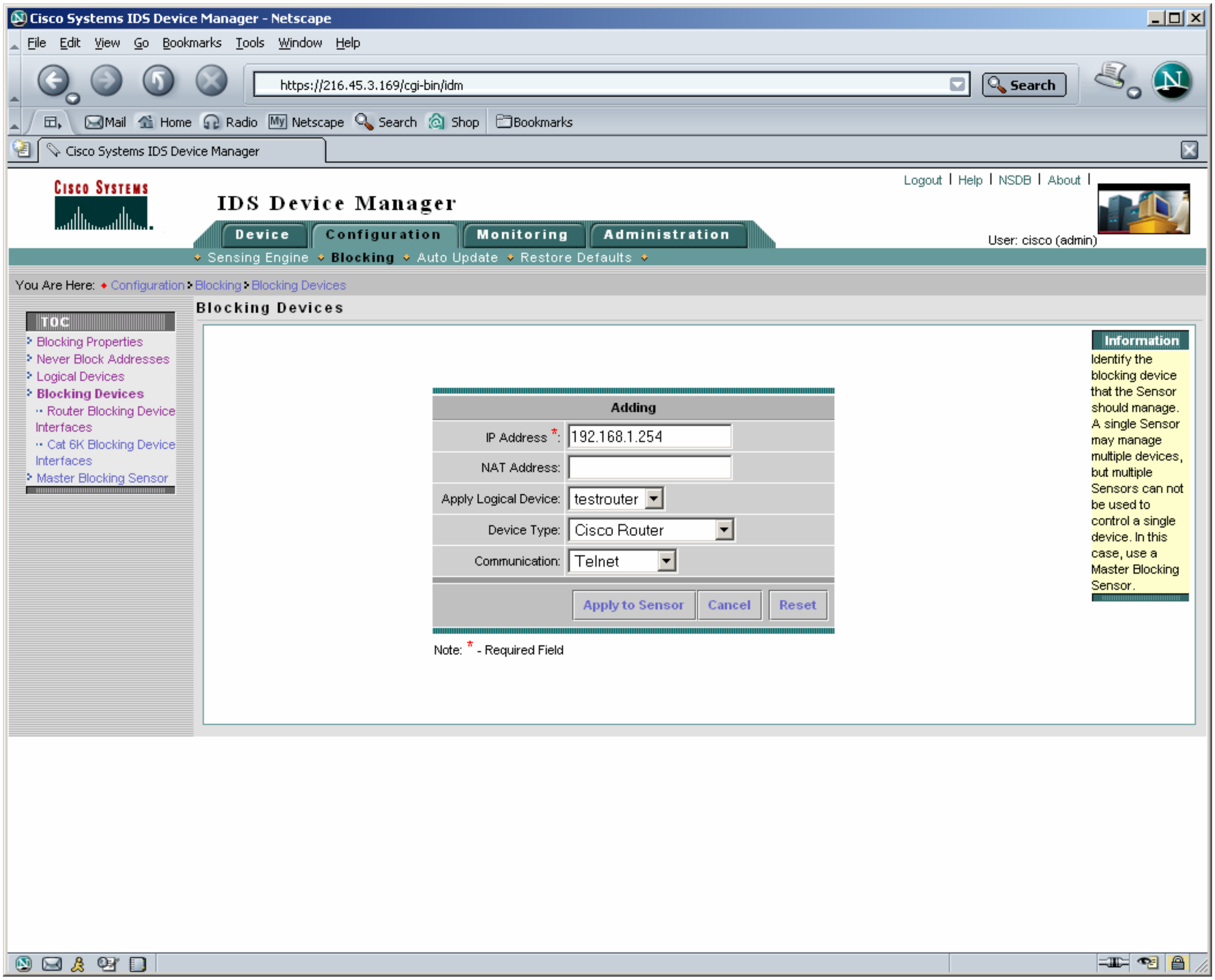
Setup logical settings to be applied to Blocking Devices.

Adding

Name *:	testrouter
Enable Password:	**********
Password:	**********
Username:	jkaberna

Note: * - Required Field

Error: Name can not contain blanks.



Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Cisco Systems
IDS Device Manager
Logout | Help | NSDB | About |
User: cisco (admin)
Device Configuration Monitoring Administration
Sensing Engine Blocking Auto Update Restore Defaults
You Are Here: Configuration > Blocking > Blocking Devices
TOC
Blocking Properties
Never Block Addresses
Logical Devices
Blocking Devices
Router Blocking Device Interfaces
Cat 6K Blocking Device Interfaces
Master Blocking Sensor
Apply to Sensor
Cancel
Reset

Blocking Devices

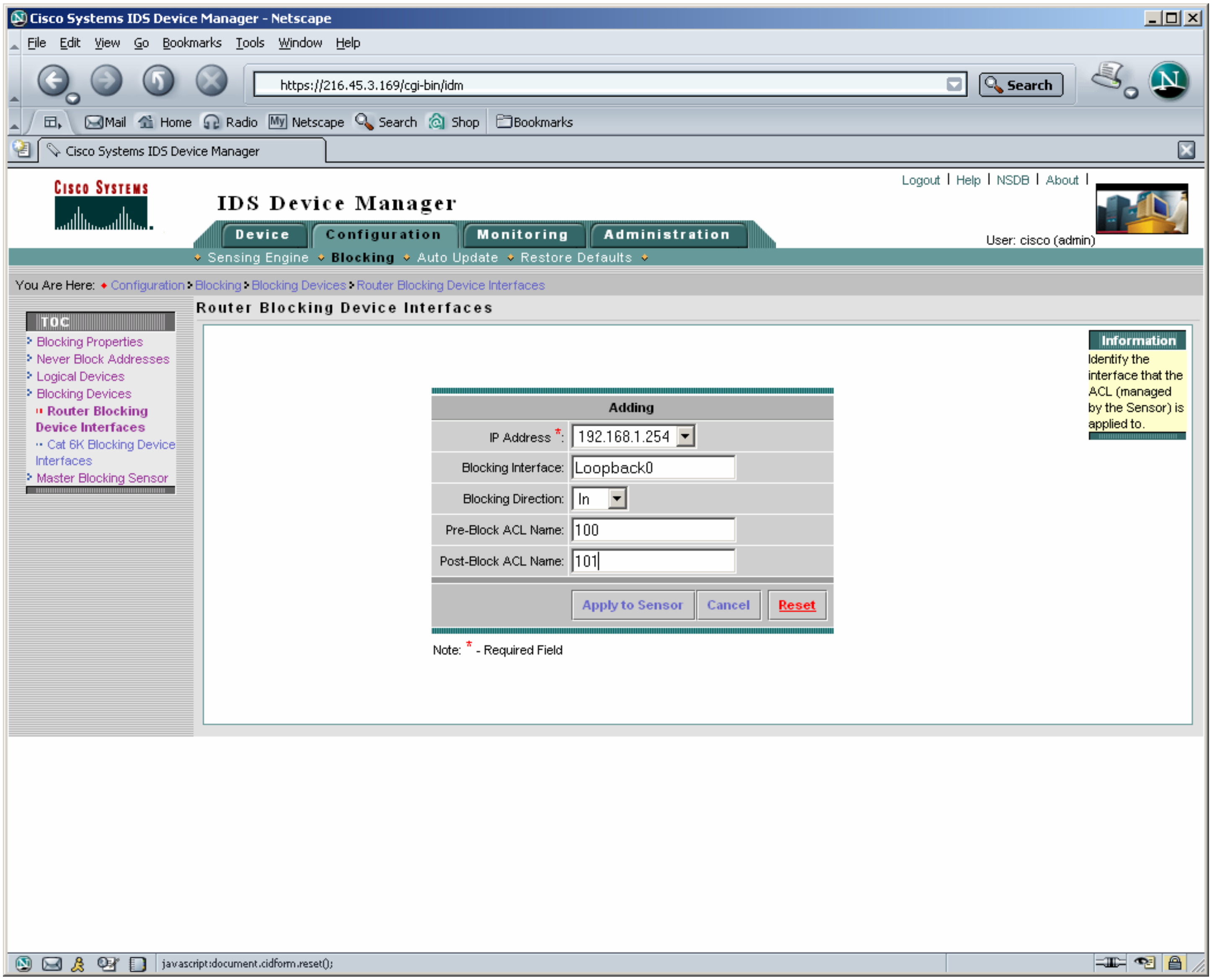
Adding

IP Address *:	192.168.1.254
NAT Address:	
Apply Logical Device:	testrouter
Device Type:	Cisco Router
Communication:	Telnet

Note: * - Required Field

Information

Identify the blocking device that the Sensor should manage. A single Sensor may manage multiple devices, but multiple Sensors can not be used to control a single device. In this case, use a Master Blocking Sensor.


Cisco Systems IDS Device Manager - Netscape
File Edit View Go Bookmarks Tools Window Help
https://216.45.3.169/cgi-bin/idm
Search
Mail Home Radio Netscape Search Shop Bookmarks
Cisco Systems IDS Device Manager
Logout | Help | NSDB | About |
Cisco Systems
IDS Device Manager
Device
Configuration
Monitoring
Administration
User: cisco (admin)
Sensing Engine
Blocking
Auto Update
Restore Defaults
TOC
Blocking Properties
Never Block Addresses
Logical Devices
Blocking Devices
Router Blocking Device Interfaces
Cat 6K Blocking Device Interfaces
Master Blocking Sensor
Apply to Sensor
Cancel
Reset
javascript:document.cidform.reset();

You Are Here: Configuration > Blocking > Blocking Devices > Router Blocking Device Interfaces

Router Blocking Device Interfaces

Adding

IP Address *:	192.168.1.254
Blocking Interface:	Loopback0
Blocking Direction:	In
Pre-Block ACL Name:	100
Post-Block ACL Name:	101

Note: * - Required Field

Information

Identify the interface that the ACL (managed by the Sensor) is applied to.

```
ntp-router#wr t
Building configuration...

5d04h: %SYS-5-CONFIG_I: Configured from console by jkaberna on vty0 (192.168.1.10)
Current configuration : 1121 bytes
!
! Last configuration change at 00:56:52 UTC Wed Nov 12 2003 by jkaberna
! NVRAM config last updated at 05:08:49 UTC Fri Nov 7 2003 by jkaberna
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ntp-router
!
logging rate-limit console 10 except errors
enable secret 5 $1$eWAB$qqlJ.fxjhEGReTX0d50bW.
!
username jkaberna password 0 xxxx
ip subnet-zero
no ip finger
!
no ip dhcp-client network-discovery
!
!
!
!
```

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 100 in
!
interface Ethernet0
 ip address 192.168.1.254 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
ip kerberos source-interface any
ip classless
ip http server
!
access-list 100 permit ip host 66.124.87.43 any
access-list 100 permit ip any any
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 120 0
 password xxxx
 login local
line vty 5 15
 exec-timeout 120 0
 password xxxx
 login local
!
ntp authentication-key 1 md5 030758020358701818 7
ntp authenticate
ntp master
end

ntp-router#sh user
    Line       User       Host(s)              Idle       Location
*  2 vty 0     jkaberna   idle                 00:00:00 192.168.1.10
   3 vty 1     jkaberna   idle                 00:00:36 192.168.1.102

  Interface      User        Mode                     Idle     Peer Address

ntp-router#sh access-l
Extended IP access list 100
    permit ip host 66.124.87.43 any
```

<Telnet attack initiated>

```
5d05h: %SYS-5-CONFIG_I: Configured from console by jkaberna on vty1 (192.168.1.102)r

ntp-router#sh access-l
Extended IP access list 100
    permit ip host 66.124.87.43 any
    permit ip any any
Extended IP access list IDS_Loopback0_in_0
    permit ip host 192.168.1.102 any
    deny ip host 66.124.87.45 any
    permit ip any any

ntp-router#wr t
Building configuration...

Current configuration : 1326 bytes
!
! Last configuration change at 01:13:09 UTC Wed Nov 12 2003 by jkaberna
! NVRAM config last updated at 01:13:10 UTC Wed Nov 12 2003 by jkaberna
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname ntp-router
!
logging rate-limit console 10 except errors
enable secret 5 $1$eWAB$qqlJ.fxjhEGReTX0d50bW.
!
username jkaberna password 0 xxxx
ip subnet-zero
no ip finger
!
no ip dhcp-client network-discovery
!
!
!
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 ip access-group IDS_Loopback0_in_0 in
!
interface Ethernet0
 ip address 192.168.1.254 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
ip kerberos source-interface any
ip classless
ip http server
!
!
ip access-list extended IDS_Loopback0_in_0
 permit ip host 192.168.1.102 any
 deny   ip host 66.124.87.45 any
 permit ip any any
access-list 100 permit ip host 66.124.87.43 any
access-list 100 permit ip any any
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 120 0
 password xxxx
 login local
line vty 5 15
 exec-timeout 120 0
 password xxxx
 login local
!
ntp authentication-key 1 md5 030758020358701818 7
ntp authenticate
ntp master
end

ntp-router#
```