IDS Sensor Installation and Configuration

Software Installation, Upgrade, and Recovery

Step 1. Either connect a console cable to the sensor or attach a keyboard and monitor. It is better to use a keyboard and monitor because you will see the entire boot sequence. When using a console cable you cannot change any BIOS settings. You will also need a special console cable. If you do not have this cable you will need to make one.

Step 2. Insert the bootable recovery CD in to the CD-ROM drive of your sensor. You may need to enter setup to change the boot order. Make sure the CD-ROM is selected ahead of the hard disk.

Step 3. Power up the sensor. When prompted, enter either k or s to boot from either the keyboard/monitor or the serial console. For documentation purposes, we chose to use the serial connection because we can log the entire session. You will also be prompted to change the password once the sensor has completed its software installation.

```
SYSLINUX 1.52 2001-02-07  Copyright (C) 1994-2001 H. Peter Anvin


                   Cisco IDS 4.0(1) Upgrade/Recovery CD!


IDS-4220/4230 customers:
Sniffing and Command-and-Control interfaces have been swapped in CIDS 4.0.
Reference the 4.0 software documentation before proceeding.


IDS-4235/4250 customers:
BIOS version "A04" or later is required to run CIDS 4.0 on your appliance.
Reference the 4.0 software documentation before proceeding.


 -  To recover the Cisco IDS 4.0 Application using a local keyboard/monitor,
    type: k <ENTER>.
    (WARNING: ALL DATA ON DISK 1 WILL BE LOST)

 -  To recover the Cisco IDS 4.0 Application using a serial connection,
    type: s <ENTER>, or just press <ENTER>
    (WARNING: ALL DATA ON DISK 1 WILL BE LOST)

boot: s
Loading initrd.img..........
Loading vmlinuz............... ready.
Linux version 2.4.18-3BOOT (bhcompile@stripples.devel.redhat.com) (gcc version
2.96 20000731 (Red Hat Linux 7.3 2.96-110)) #1 T
hu Apr 18 06:53:28 EDT 2002
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
 BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000e8000 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 000000001fff0000 (usable)
 BIOS-e820: 000000001fff0000 - 000000001ffff000 (ACPI data)
 BIOS-e820: 000000001ffff000 - 0000000020000000 (ACPI NVS)
 BIOS-e820: 00000000fec00000 - 00000000fec10000 (reserved)
 BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)
 BIOS-e820: 00000000fff00000 - 0000000100000000 (reserved)
```

```
found SMP MP-table at 000f7300
hm, page 000f7000 reserved twice.
hm, page 000f8000 reserved twice.
hm, page 0009f000 reserved twice.
hm, page 000a0000 reserved twice.
On node 0 totalpages: 131056
zone(0): 4096 pages.
zone(1): 126960 pages.
zone(2): 0 pages.
Intel MultiProcessor Specification v1.1
    Virtual Wire compatibility mode.
OEM ID: INTEL    Product ID: N440BX       APIC at: 0xFEE00000
Processor #1 Pentium(tm) Pro APIC version 17
Processor #0 Pentium(tm) Pro APIC version 17
I/O APIC #2 Version 17 at 0xFEC00000.
Processors: 2
Kernel command line: ks=cdrom:/ks.cfg initrd=initrd.img lang= text devfs=nomount
ramdisk_size=8192 console=ttyS0,9600 BOOT_IMAG
E=vmlinuz
Initializing CPU#0
Detected 598.507 MHz processor.
Console: colour VGA+ 80x25
Calibrating delay loop... 1192.75 BogoMIPS
Memory: 514736k/524224k available (1092k kernel code, 9100k reserved, 327k data,
160k init, 0k highmem)
Dentry cache hash table entries: 65536 (order: 7, 524288 bytes)
Inode cache hash table entries: 32768 (order: 6, 262144 bytes)
Mount-cache hash table entries: 8192 (order: 4, 65536 bytes)
Buffer cache hash table entries: 32768 (order: 5, 131072 bytes)
Page-cache hash table entries: 131072 (order: 7, 524288 bytes)
CPU: L1 I cache: 16K, L1 D cache: 16K
CPU: L2 cache: 512K
CPU serial number disabled.
Intel machine check architecture supported.
Intel machine check reporting enabled on CPU#0.
CPU: Intel Pentium III (Katmai) stepping 03
Enabling fast FPU save and restore... done.
Enabling unmasked SIMD FPU exception support... done.
Checking 'hlt' instruction... OK.
Checking for popad bug... OK.
POSIX conformance testing by UNIFIX
mtrr: v1.40 (20010327) Richard Gooch (rgooch@atnf.csiro.au)
mtrr: detected mtrr type: Intel
PCI: PCI BIOS revision 2.10 entry at 0xfdaf0, last bus=0
PCI: Using configuration type 1
PCI: Probing PCI hardware
PCI: Using IRQ router PIIX [8086/7110] at 00:12.0
PCI: Cannot allocate resource region 4 of device 00:12.1
Limiting direct PCI/PCI transfers.
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
Starting kswapd
pty: 256 Unix98 ptys configured
Serial driver version 5.05c (2001-07-08) with MANY_PORTS SHARE_IRQ SERIAL_PCI
enabled
ttyS00 at 0x03f8 (irq = 4) is a 16550A
ttyS01 at 0x02f8 (irq = 3) is a 16550A
block: 992 slots per queue, batch=248
Uniform Multi-Platform E-IDE driver Revision: 6.31
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX4: IDE controller on PCI bus 00 dev 91
PIIX4: chipset revision 1
PIIX4: not 100% native mode: will probe irqs later
    ide0: BM-DMA at 0x1000-0x1007, BIOS settings: hda:DMA, hdb:pio
    ide1: BM-DMA at 0x1008-0x100f, BIOS settings: hdc:DMA, hdd:pio
hda: QUANTUM FIREBALL CX6.4A, ATA DISK drive
hdc: TOSHIBA CD-ROM XM-6602B, ATAPI CD/DVD-ROM drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
ide1 at 0x170-0x177,0x376 on irq 15
blk: queue c02c2804, I/O limit 4095Mb (mask 0xffffffff)
```

```
hda: 12594960 sectors (6449 MB) w/418KiB Cache, CHS=784/255/63, UDMA(33)
hdc: ATAPI 40X CD-ROM drive, 128kB Cache
Uniform CD-ROM driver Revision: 3.12
ide-floppy driver 0.99.newide
Partition check:
 hda: hda1 hda2 hda3 hda4 < hda5 hda6 >
Floppy drive(s): fd0 is 1.44M
FDC 0 is a National Semiconductor PC87306
RAMDISK driver initialized: 16 RAM disks of 8192K size 1024 blocksize
loop: loaded (max 8 devices)
ide-floppy driver 0.99.newide
usb.c: registered new driver usbdevfs
usb.c: registered new driver hub
usb-uhci.c: $Revision: 1.275 $ time 06:55:51 Apr 18 2002
usb-uhci.c: High bandwidth mode enabled
PCI: Assigned IRQ 10 for device 00:12.2
PCI: Sharing IRQ 10 with 00:0d.1
usb-uhci.c: USB UHCI at I/O 0x1080, IRQ 10
usb-uhci.c: Detected 2 ports
usb.c: new USB bus registered, assigned bus number 1
hub.c: USB hub found
hub.c: 2 ports detected
usb-uhci.c: v1.275:USB Universal Host Controller Interface driver
usb.c: registered new driver hiddev
usb.c: registered new driver hid
hid-core.c: v1.8.1 Andreas Gal, Vojtech Pavlik <vojtech@suse.cz>
hid-core.c: USB HID support drivers
mice: PS/2 mouse device common for all mice
md: md driver 0.90.0 MAX_MD_DEVS=256, MD_SB_DISKS=27
md: Autodetecting RAID arrays.
md: autorun ...
md: ... autorun DONE.
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP
IP: routing cache hash table of 4096 buckets, 32Kbytes
TCP: Hash tables configured (established 32768 bind 32768)
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
RAMDISK: Compressed image found at block 0
Freeing initrd memory: 511k freed
EXT2-fs warning: checktime reached, running e2fsck is recommended
VFS: Mounted root (ext2 filesystem).
Greetings.
Red Hat install init version 7.2 starting
mounting /proc filesystem... done
mounting /dev/pts (unix98 pty) filesystem... done
Red Hat install init version 7.2 using a serial console
remember, cereal is an important part of a nutritionally balanced breakfast.

checking for NFS root filesystem...no
trying to remount root filesystem read write... done
checking for writeable /tmp... yes
running install...
running /sbin/loader
```

```
Running anaconda - please wait...
Probing for video card:   Cirrus Logic GD5480
Probing for monitor type: Unable to probe
Probing for mouse type:   None - None


sending termination signals...done
sending kill signals...done
disabling swap...
        /tmp/hda5
unmounting filesystems...
        /mnt/runtime done
        disabling /dev/loop0
        /proc/bus/usb done
        /proc done
        /dev/pts done
        /mnt/source done
        /mnt/sysimage/dev/pts done
        /mnt/sysimage/proc/bus/usb done
        /mnt/sysimage/proc done
        /mnt/sysimage/usr/cids/idsRoot/shared done
        /mnt/sysimage/usr/cids/idsRoot/var done
        /mnt/sysimage done
ejecting /tmp/cdrom...
rebooting system
Restarting system.

sensor login: cisco
Password: cisco
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password: cisco
New password: ccie7146
Retype new password: ccie7146
***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.
```

Initial Setup

The initial setup is fairly simple. The purpose is mainly to change the IP address so that you can manage the Sensor using a web browser.

Step 1. Type setup from the sensor prompt.

Step 2. Enter in the appropriate information when prompted. Enter yes to reboot.

```
sensor# setup
```

```
    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
networkParams
hostname sensor
ipAddress 10.1.9.201
netmask 255.255.255.0
defaultGateway 10.1.9.1
telnetOption disabled
exit
exit
!
service webServer
general
ports 443
exit
exit

Current time: Tue Sep 30 13:28:46 2003

Setup Configuration last modified: Tue Sep 30 13:26:01 2003


Continue with configuration dialog?[yes]: yes
Enter host name[sensor]: nli-sensor
Enter IP address[10.1.9.201]: 192.168.1.250
Enter netmask[255.255.255.0]: 255.255.255.0
Enter default gateway[10.1.9.1]: 192.168.1.1
Enter telnet-server status[disabled]: disabled
Enter web-server port[443]: 443

The following configuration was entered.

service host
networkParams
hostname nli-sensor
ipAddress 192.168.1.250
netmask 255.255.255.0
defaultGateway 192.168.1.1
telnetOption disabled
exit
exit
!
service webServer
general
ports 443
exit
exit

Use this configuration?[yes]: yes
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: yes

Broadcast message from root (Tue Sep 30 13:31:15 2003):

A system reboot has been requested.  The reboot may not start for 90 seconds.
sensor#
Broadcast message from root (Tue Sep 30 13:31:17 2003):

The system is going down for reboot NOW!
```

Basic Configuration

Once you have run setup, you can now connect to the sensor using a web browser or continue to use the CLI.

Step 1. From configure terminal, type service host. Then type show settings to see your current settings.

```
nli-sensor# conf t
nli-sensor(config)# service host
nli-sensor(config-Host)# show settings
   networkParams
   -----------------------------------------------
      ipAddress: 192.168.1.250
      netmask: 255.255.255.0 default: 255.255.255.0
      defaultGateway: 192.168.1.1
      hostname: nli-sensor
      telnetOption: enabled default: disabled
      accessList (min: 0, max: 512, current: 1)
      -----------------------------------------------
         ipAddress: 10.0.0.0
         netmask: 255.0.0.0 default: 255.255.255.255
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   optionalAutoUpgrade
   -----------------------------------------------
   -----------------------------------------------
   timeParams
   -----------------------------------------------
      offset: 0 minutes <defaulted>
      standardTimeZoneName: UTC <defaulted>
      summerTimeParams
      -----------------------------------------------
      -----------------------------------------------
      ntpServers (min: 0, max: 1, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
```

Step 2. Configure your network parameters. Specifically, you should remove the default ACL and replace it with one that will work with your network. This ACL limits the management control of the Sensor. If you do not change this setting and the source of your management workstation is not on a 10.0.0.0 network then you will not be able to Telnet, SSH, or HTTPS to the sensor.

```
nli-sensor(config-Host)# networkParams
nli-sensor(config-Host-net)# no accesslist ipaddress 10.0.0.0 netmask 255.0.0.0
nli-sensor(config-Host-net)# accesslist ipaddress 192.168.1.0 netmask
255.255.255.0
nli-sensor(config-Host-net)# exit
```

Step 3. This is an optional step, but it is always recommended to configure proper time on security devices and use NTP whenever possible.

```
nli-sensor(config-Host)# timeparams
nli-sensor(config-Host-tim)# ?
default                  Set the value back to the system default setting
exit                     Exit timeParams configuration submode
no                       Remove an entry or selection setting
ntpServers               NTP server definition, if no NTP server defined the
                          system clock will be used
```

```
offset                    num of minutes added to UTC to get local time
show                      Display system settings and/or history information
standardTimeZoneName      descriptive name for standard time
summerTimeParams          summertime parameters

nli-sensor(config-Host-tim)# standardtimezone PST
nli-sensor(config-Host-tim)# offset –480


nli-sensor(config-Host-tim)# summertimeparams
nli-sensor(config-Host-tim-sum)# active-selection recurringparams
nli-sensor(config-Host-tim-sum)# recurringparams
nli-sensor(config-Host-tim-sum-rec)# summertimezonename PDT


nli-sensor(config-Host-tim-sum-rec)# exit
nli-sensor(config-Host-tim-sum)# exit
nli-sensor(config-Host-tim)# exit
nli-sensor(config-Host)# exit
Apply Changes:?[yes]: yes
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is rebooted. Please
use the reset command to complete the configuration.
nli-sensor(config)# exit


nli-sensor# clock set 12:29:00 Sept 29 2003
```

Step 4. Generate your SSH and SSL key. It is recommended that you write down these values to verify you are connecting to the proper host. For lab purposes, this step is probably not necessary.

```
nli-sensor# tls generate-key
MD5 fingerprint is 38:0D:66:FE:32:40:45:2C:6E:DA:C5:02:5C:F1:5A:1D
SHA1 fingerprint is 52:53:00:1C:55:9D:65:09:2B:B0:C1:7C:16:50:24:0A:B7:24:92:89


nli-sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? : yes

Broadcast message from root (Mon Sep 29 05:29:19 2003):

A system reboot has been requested.  The reboot may not start for 90 seconds.
Request Suceeded.
nli-sensor#
Broadcast message from root (Mon Sep 29 05:29:22 2003):

The system is going down for reboot NOW!
```

Upgrading the Software

Step 1. Download the package software or, if your sensor's management interface has internet connectivity, you can download the software directly from Cisco's site. You must have a CCO account with download privileges.

Step 2. Type config t. Then type upgrade <path> where <path> is the location and filename of the upgrade package. Type this all on one line.

```
nli-sensor# conf t
nli-sensor(config)# upgrade
http://ftp.cisco.com/cisco/crypto/3DES/ciscosecure/ids/4.x/IDS-K9-min-4.1-1-
S47.rpm.pkg
User: jkaberna
```

```
Server's IP Address: 198.133.219.27
Port[80]:
Password: *****
Warning: Executing this command will apply a minor version upgrade to the
application partition. The system may be rebooted to complete the upgrade.
Continue with upgrade? : yes

Broadcast message from root (Mon Sep 29 05:37:33 2003):

Applying update IDS-K9-min-4.1-1-S47.
    Shutting down all CIDS processes. All connections will be terminated.
    The system will be rebooted upon completion of the update.

nli-sensor login: cisco
Password:
Last login: Mon Sep 29 05:35:10 on ttyS0
***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.

nli-sensor login:
```

Upgrading Signatures

Step 1. Download the signature software or, if your sensor's management interface has internet connectivity, you can download the software directly from Cisco's site. You must have a CCO account with download privileges.

Step 2. Type config t. Then type upgrade <path> where <path> is the location and filename of the signature. Type this all on one line.

```
nli-sensor# conf t
nli-sensor(config)# upgrade
http://ftp.cisco.com/cisco/crypto/3DES/ciscosecure/ids/4.x/IDS-sig-4.1-1-
S54.rpm.pkg
User: jkaberna
Server's IP Address: 198.133.219.27
Port[80]:
Password: *****
Warning: Executing this command will apply a signature update to the application
partition.
Continue with upgrade? : yes

Broadcast message from root (Mon Sep 29 05:52:09 2003):

Applying update IDS-sig-4.1-1-S54. This may take several minutes.
            Please do not reboot the sensor during this update.


Broadcast message from root (Mon Sep 29 06:01:56 2003):

Update complete.
            sensorApp is restarting
            This may take several minutes.
nli-sensor(config)#
```

*****This document is being provided as a pre-release for those customers that have bought the CCIE Security Lab Guide.   This material is currently being updated and when it is complete a new version of the Lab Guide will be printed. If you have any comments or questions about this document please email john@netcginc.com**