

Upgrading the Intrusion Detection System Module

Document ID: 23080

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Upgrading the IDSM Application Partition

- Step-by-Step Instructions
- Verifying the Application Partition Upgrade

Upgrading the IDSM Service Pack

- Verifying the Service Pack Upgrade

Upgrading the IDSM Signatures

- Verifying the Signature Upgrade

Upgrading the IDSM2

- Upgrading the Maintenance Partition
- Reimaging the Application Partition from the Maintenance Partition
- Minor Image Upgrade
- Upgrading the IDSM2 Service Pack or Signatures

Troubleshoot

Related Information

Introduction

This document explains how to perform a Cisco Intrusion Detection System Module (IDSM) upgrade on an application partition, service pack, and a signature update. For more details on upgrading the IDS Sensor, refer to Catalyst 6000 Intrusion Detection System Module.

Prerequisites

Requirements

Before attempting this configuration, please ensure that you meet the following prerequisites:

- Start with an IDS Sensor that is up and still communicating with the Director until the time of the upgrade.
- You should be able to successfully use ping, passive FTP, and Telnet to get to the Sensor without interference from any sort of firewall or packet-filtering device before the upgrade.
- Make sure you have an FTP server that supports passive mode.

Components Used

The information in this document is based on the software and hardware versions:

- IDSM Sensor Model WS-X6381-IDS running software version 2.5.
- IDS Director running Solaris version 2.6, HP OpenView version x5.01, IDS Director Software version 2.2.3 S9.
- Solaris version 2.8 workstation with passive FTP and Telnet access to the Sensor and the Director.

- Download the files from the Downloads (registered customers only) (IDSk9-sig-3.0-2-S10.bin and nrdirUpdate-S10.bin, are used in this document).

Note: The exact versions used in this document may not be currently available.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

- The IDS Director is named "dir1," and the IP address is 192.168.1.3.
- The IDSM Sensor is named "idsm," and the IP address is 192.168.1.2.
- The host ID matches the last octet of the IP address in the examples.
- The organization ID is defined as "1."
- The FTP server IP address is 10.0.0.1.

For more information on document conventions, see the Cisco Technical Tips Conventions.

Upgrading the IDSM Application Partition

The following steps show you how to upgrade the IDSM from application version 2.5(1)S2 to 3.0(1)S4. Save the IDSM configuration before the upgrade, as the entire IDSM hard disk will be formatted and any configuration will be lost.

Step-by-Step Instructions

Follow the instructions provided below.

1. Session into the IDSM and save the output of the **show configuration** command, as shown in the following example.

```
Console> (enable) session 8
Trying IDS-8...
Connected to IDS-8.
Escape character is '^]'.
login: ciscoids
Password:

show configuration
Using 37584896 out of 267702272 bytes of available memory
!
Using 439668736 out of 4211310592 bytes of available disk space
!
Sensor version is : 2.5(1)S0
!
Sensor application status:
nr.postofficed      running
nr.fileXferd        running
nr.loggerd          running
nr.packetd          running
nr.sapd             running

Configuration last modified Never
Sensor:
IP Address:          192.168.1.2
Netmask:             255.255.255.0
Default Gateway:    192.168.1.1
```

```

Host Name:                idsm
Host ID:                  2
Host Port:                45000
Organization Name:       cisco
Organization ID:         1

Director:
IP Address:               192.168.1.3
Host Name:                dir1
Host ID:                  3
Host Port:                45000
Heart Beat Interval (secs): 5
Organization Name:       cisco
Organization ID:         1
Direct Telnet access to IDSM: disabled

```

2. Download the appropriate files from the Downloads (registered customers only) .

The IDS Sensor and readme files are located under the *Cisco IDS Appliance Sensor 3DES* section. The IDS Director and readme files are located under the *Cisco IDS Director 3DES* section. In this document, the following files are used, however you should use whatever files are most current:

```

IDSMk9-a-3.0-1-S4.readme
IDSMk9-a-3.0-1-S4-1.cab
IDSMk9-a-3.0-1-S4-2.cab
IDSMk9-a-3.0-1-S4-3.cab
IDSMk9-a-3.0-1-S4-4.cab
IDSMk9-a-3.0-1-S4-5.cab
IDSMk9-a-3.0-1-S4.dat

```

3. Place the files in the appropriate directory of the FTP server.

In this example, the files are placed in the root directory. The following is sample output from the FTP client to the FTP server.

```

user@solariswkstn% ftp user@solariswkstn
Connected to solariswkstn.cisco.com.
220 solariswkstn FTP server (SunOS 5.8) ready.
Name (solariswkstn:username): user
331 Password required for user.
Password:
230 User user logged in.
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> pwd

250 CWD command successful.

257 "/" is current directory.
ftp> ls
227 Entering Passive Mode (10,0,0,1,169,229)
150 ASCII data connection for /bin/Ls (10.0.0.1,43494) (0 bytes).
total 110878

-rw-r--r--  1 jlimbo  cisco  10000384 May 11 15:34 IDSMk9-a-3.0-1-S4-1.cab
-rw-r--r--  1 jlimbo  cisco  10000384 May 11 15:22 IDSMk9-a-3.0-1-S4-2.cab
-rw-r--r--  1 jlimbo  cisco  10000384 May 11 15:24 IDSMk9-a-3.0-1-S4-3.cab
-rw-r--r--  1 jlimbo  cisco  10000384 May 11 15:24 IDSMk9-a-3.0-1-S4-4.cab
-rw-r--r--  1 jlimbo  cisco  1126530  May 11 15:23 IDSMk9-a-3.0-1-S4-5.cab
-rw-r--r--  1 jlimbo  cisco    600 May 11 15:20 IDSMk9-a-3.0-1-S4.dat

226 ASCII Transfer complete.
ftp> exit
221 Goodbye.
user@solariswkstn%

```

4. Set the Maintenance partition as the active partition, then console into the IDSM to the maintenance partition (application is the default setting) and set the network configuration parameter of the IDSM.

In the following example, the IDSM is in slot 8 of the Catalyst 6509 chassis.

```
Console> (enable) set boot device hdd:2

Console> (enable) reset 8

This command will reset module 8.
Unsaved configuration on module 8 will be lost
Do you want to continue (y/n) [n]? y
Module 8 shut down in progress, please don't
remove module until shutdown completed.
Console> (enable) Module 8 shutdown completed. Module resetting...

Console> (enable) session 8
Trying IDS-8...
Connected to IDS-8.
Escape character is '^]'.
login: ciscoids
Password:

maintenance#
maintenance# diag
maintenance(diag)#ids-installer
netconfig /configure /ip=192.168.1.2 /subnet=255.255.255.0 /gw=192.168.1.1
STATUS: Network parameters for the config port have been configured!
```

Note: Reset the module for the changes to take effect.

5. Once the IDSM has finished rebooting, session back into the IDSM and install the inactive application partition by issuing the **ids-installer** command, as shown in the following example.

```
Console> (enable) session 8
Trying IDS-8...
Connected to IDS-8.
Escape character is '^]'.
login: ciscoids
Password:

maintenance# diag
maintenance(diag)# ids-installer
system /nw /install /server=10.0.0.1 /user=user /save=yes /dir='/'
 /prefix=IDSMk9-a-3.0-1-S4
Please enter login password: *****

Downloading the image.. File 05 of 05

FTP STATUS: Installation files have been downloaded successfully!

Validating integrity of the image... PASSED!

Formatting drive C:\....
Verifying 4016M
Format completed successfully.

4211310592 bytes total disk space.
4206780416 bytes available on disk.

Volume Serial Number is E893-5968

Extracting the image...

##### ----snip-----
```

```
STATUS: Image has been successfully installed on drive C:\!
```

```
maintenance(diag)# exit
```

Verifying the Application Partition Upgrade

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Reboot the IDSM back to the application partition and verify that the image has been successfully upgraded, as shown in the following example.

```
Console> (enable) set boot device hdd:1
```

```
Console> (enable) reset 8
```

```
This command will reset module 8.  
Unsaved configuration on module 8 will be lost  
Do you want to continue (y/n) [n]? y  
Module 8 shut down in progress, please  
don't remove module until shutdown completed.  
Console> (enable) Module 8 shutdown completed. Module resetting...
```

```
Console> (enable) session 8
```

```
Trying IDS-8...  
Connected to IDS-8.  
Escape character is '^']'.
```

```
login: ciscoids  
Password:
```

```
idsm# show configuration
```

```
Using 48259072 out of 267702272 bytes of available memory  
!  
Using 504688640 out of 4211310592 bytes of available disk space  
!  
Sensor version is : 3.0(1)S4  
!  
Sensor application status:  
nr.postofficed      running  
nr.fileXferd        running  
nr.loggerd          running  
nr.packetd          running  
nr.sapd             running
```

```
Configuration last modified Wed May 01 01:03:56 2002
```

```
Sensor:  
IP Address:          192.168.1.2  
Netmask:             255.255.255.0  
Default Gateway:    192.168.1.1  
Host Name:           idsm  
Host ID:             2  
Host Port:           45000  
Organization Name:   cisco  
Organization ID:     1
```

```
Director:  
IP Address:          192.168.1.3  
Host Name:           dir1  
Host ID:             3  
Host Port:           45000
```

```
Heart Beat Interval (secs): 5
Organization Name:          cisco
Organization ID:           1
```

Upgrading the IDSM Service Pack

Use the following procedure to update the IDSN service pack.

1. Session into the IDSM by issuing the **session #** command (where # is the module number), and issue the **configure terminal** command, as shown in the following example.

```
idsm#
idsm#configure terminal
```

2. Issue the **apply ftp://<username@server/dir/filename>** command to connect through FTP, and apply the service pack, as shown in the following example.

```
idsm(config)#apply ftp://user@10.0.0.1//IDSMk9-sp-3.0-3-S10.exe
WARNING: Installing Service Pack will temporarily disable IDS.
Continue with IDS Service Pack install?: y
```

```
Enter the FTP user password:  *****
Connecting to site...
```

```
Receiving file.
Installing as 3.0(3)S10
```

```
Installing files from Service Pack 3.0(2)
Installing files from Signature Update 10
```

```
Starting NetRanger Signatures Merging Utility...
Checking file: C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf...
Adding signature: SigOfGeneral 993 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3111 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3112 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3114 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3160 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3162 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3454 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3455 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 4060 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 4101 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 4601 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5158 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5159 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5160 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5161 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5162 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
```

```

Adding signature: SigOfGeneral 5163 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5164 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5165 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5166 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5167 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5168 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5169 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5170 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5171 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5172 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5173 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5174 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5175 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5176 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6197 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6901 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6902 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6903 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6910 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6920 to C:\Program Files\
Cisco Systems\Netranger/etc/packetd.conf.
Installing files from Service Pack 3.0(3)
The Install for IDSM Service Pack file IDSMk9-sp-3.0-3-S10.exe
was successful
2002 May 13 18:29:34 %PAGP-5-PORTFROMSTP:Port 8/1 left bridge port 8/1
2002 May 13 18:29:34 %DTP-5-NONTRUNKPORTON:Port 8/1 has become non-trunk

Systems needs to be restarted. Rebooting...

Module 8 shut down in progress, please don't remove module until
shutdown completed.

idsm(config)# Console> (enable) Module 8 shutdown completed.
Module resetting...

```

Verifying the Service Pack Upgrade

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Session into the IDSM by issuing the **session #** command (where # is the module number), and issue the **show configuration** command, as shown in the following example.

```

idsm#show configuration
Using 46059520 out of 267702272 bytes of available memory

```

```

!
Using 466886656 out of 4211310592 bytes of available disk space
!
Sensor version is : 3.0(3)S10
!
Sensor application status:
nr.postofficed      running
nr.fileXferd        running
nr.loggerd          running
nr.packetd          running
nr.sapd             running
Configuration last modified Fri May 10 23:02:57 2002

```

```

Sensor:
IP Address:          192.168.1.2
Netmask:             255.255.255.0
Default Gateway:    192.168.1.1
Host Name:           idsm
Host ID:             2
Host Port:           45000
Organization Name:   cisco
Organization ID:     1

```

```

Director:
IP Address:          192.168.1.3
Host Name:           dir1
Host ID:             3
Host Port:           45000
Heart Beat Interval (secs): 5
Organization Name:   cisco
Organization ID:     1
Direct Telnet access to IDSM: enabled
Current access list entries:
  [1] 192.168.1.0 0.0.0.255

```

```
idsm#
```

Upgrading the IDSM Signatures

Use the following procedure to upgrade the IDSM signatures.

1. Session into the IDSM by issuing the **session #** command (where # is the module number), and issue the **configure terminal** command, as shown in the following example.

```
idsm#
idsm#configure terminal
```

2. Issue the **apply ftp://<username@server/dir/filename>** command to connect through FTP, and apply the IDSM signatures, as shown in the following example:

```
idsm(config)#apply ftp://user@10.0.0.1//IDSMk9-sig-3.0-3-S13.exe
WARNING: Installing Signature Update will temporarily disable IDS.
Continue with IDS Signature Update install?:
% Please answer 'yes' or 'no'.
Continue with IDS Signature Update install?: yes
Enter the FTP user password: *****
Connecting to site...
```

```
Receiving file.
WARNING!!! Installation of this IDSM Signature Update will
now prevent uninstalling of the current IDSM Service Pack 3.0(3).
WARNING!!! To uninstall IDSM Service Pack 3.0(3) you will need
to first uninstall this IDSM Signature Update.
```

Starting NetRanger Signatures Merging Utility...
Checking file: C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf...
Adding signature: SigOfGeneral 1107 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3116 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3117 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3118 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3119 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3120 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3163 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3403 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3456 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3501 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3651 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 4507 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5178 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5179 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5180 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5181 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5182 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5183 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5184 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5188 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5191 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5194 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5195 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5196 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5197 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5199 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5200 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.

The Install for IDSM Signature Update file IDSMk9-sig-3.0-3-S13.exe was successful

Systems needs to be restarted. Rebooting...

Module 8 shut down in progress, please don't remove module until shutdown completed.

```
idsm(config)# Console> (enable) Module 8 shutdown completed. Module resetting...  
2002 May 13 18:58:08 %SYS-3-SUP_OSBOOTSTATUS:Starting IDSM Diagnostics  
2002 May 13 18:58:50 %SYS-3-SUP_OSBOOTSTATUS:IDSM diagnostics
```

```

        completed successfully.
2002 May 13 18:58:56 %SYS-5-MOD_OK:Module 8 is online
2002 May 13 18:58:56 %PAGP-5-PORTFROMSTP:Port 8/1 left bridge port 8/1
2002 May 13 18:58:56 %DTP-5-TRUNKPORTON:Port 8/1 has become dot1q trunk
2002 May 13 18:58:56 %PAGP-5-PORTTOSTP:Port 8/2 joined bridge port 8/2
2002 May 13 18:58:57 %SYS-3-MOD_PORTINTFINSYNC:Port Interface in sync for
        Module 8
2002 May 13 18:58:57 %PAGP-5-PORTTOSTP:Port 8/1 joined bridge port 8/1

Console> (enable)
Console> (enable) session 8
Trying IDS-8...
Connected to IDS-8.
Escape character is '^]'.

login: ciscoids
Password:

```

Verifying the Signature Upgrade

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Session into the IDSM by issuing the **session #** command (where # is the module number), and issue the **show configuration** command, as shown in the following example.

```

idsm#show configuration
Using 46014464 out of 267702272 bytes of available memory
!
Using 470089728 out of 4211310592 bytes of available disk space
!
Sensor version is : 3.0(3)S13
!
Sensor application status:
nr.postofficed      running
nr.fileXferd        running
nr.loggerd          running
nr.packetd          running
nr.sapd             running
Configuration last modified Fri May 10 23:02:57 2002

Sensor:
IP Address:          192.168.1.2
Netmask:             255.255.255.0
Default Gateway:    192.168.1.1
Host Name:           idsm
Host ID:             2
Host Port:          45000
Organization Name:   cisco
Organization ID:     1

Director:
IP Address:          192.168.1.3
Host Name:          dirl
Host ID:            3
Host Port:          45000
Heart Beat Interval (secs): 5
Organization Name:   cisco
Organization ID:     1
Direct Telnet access to IDSM: enabled
Current access list entries:
  [1] 192.168.1.0 0.0.0.255

idsm#

```

Upgrading the IDSM2

The following sections provide information on upgrading the IDSM2.

Upgrading the Maintenance Partition

To upgrade the Maintenance Partition from 1.3.1 to 1.3.2, boot the IDSM2 blade in the Application Partition by issuing the following commands at the switch.

```
reset <mod> hdd:1
```

```
Console> (enable) reset 5 hdd:1
```

```
idsm-2#show version
```

```
Application Partition:
```

```
Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S41
```

```
OS Version 2.4.18-5-phoenix
```

```
Platform: WS-SVC-IDS2-XL
```

```
Sensor up-time is 43 min.
```

```
Using 748920832 out of 1979682816 bytes of available memory (37% usage)
```

```
Using 997M out of 17G bytes of available disk space (6% usage)
```

```
MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
```

```
CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600
```

```
Upgrade History:
```

```
No upgrades installed
```

```
Maintenance Partition Version 1.3(1)
```

```
idsm-2(config)#upgrade ftp://user@10.1.1.1/mp.1-3-2.bin.gz
```

```
Password: *****
```

```
Warning: Executing this command will re-image the maintenance partition. The system may be rebooted to complete the upgrade.
```

```
Continue with upgrade? : yes
```

Once the re-image is complete and the system has rebooted, a **show version** will allow you to confirm that the upgrade was successful.

```
idsm-2#show version
```

```
Application Partition:
```

```
Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S41
```

```
OS Version 2.4.18-5-phoenix
```

```
Platform: WS-SVC-IDS2-XL
```

Using 762945536 out of 1979682816 bytes of available memory (38% usage)
Using 1007M out of 17G bytes of available disk space (7% usage)

```
MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600
```

Upgrade History:

No upgrades installed

Maintenance Partition Version 1.3(2)

Reimaging the Application Partition from the Maintenance Partition



Caution: After re-imaging the IDS module, you must initialize the IDS module using the **setup** command. This process removes all sensor configuration and reimages the application partition. This process should be used only if the Application Partition is corrupt or inaccessible. If the Application Partition is accessible, to avoid losing current configuration, use the Minor Image Upgrade to upgrade from the Application Partition itself.

1. Boot into the Maintenance Partition by issuing the following commands on the switch.

```
reset <mod> cf:1

Console> (enable)reset 5 cf:1
This command will reset module 5.
Unsaved configuration on module 5 will be lost
Do you want to continue (y/n) [n]? y
SendShutDownMsg: shut down module 5 no response, reset module...
Module 5 experienced problems during shutdown.
It may take several minutes to come online.

Console> (enable) 2003 Sep 02 14:01:55 %SYS-3-SUP_OSBOOTSTATUS:MP
OS Boot Status: f
inished booting
Console> (enable)
Console> (enable) sess 5
Trying IDS-5...
Connected to IDS-5.
Escape character is '^]'.

Cisco Maintenance image
```

2. Log into the IDS module by entering the following username and password.

```
login: guest
Password: cisco

Maintenance image version: 1.3(2)

guest@localhost.localdomain#ip address 172.16.171.22 255.255.255.192
guest@localhost.localdomain#ip gateway 172.16.171.1
```

3. Enter configuration terminal mode using the **configure terminal** command.
4. Perform the reimage using the **upgrade ftp://<user>@<ftp server IP>/<directory path>/<image**

file> command.

You will be prompted to enter the FTP server password (if required). You will also be prompted to proceed with the installation. Enter **y** to continue.

```
guest@localhost.localdomain#upgrade ftp://user@10.1.1.1/
WS-SVC-IDS2-K9-a-4.1-1-S47.bin.gz
ftp://user@10.1.1.1//home/user/WS-SVC-IDS2-K9-a-4.1-1-S47.bin.gz (unknown size)
/tmp/upgrade.gz [-] 65259K
66825226 bytes transferred in 13.38 sec (4878.70k/sec)

Upgrade file ftp://user@10.1.1.1//home/user/WS-SVC-IDS2-K9-a-4.1-1-S47.bin.gz
is downloaded.
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|N]: y

Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@localhost.localdomain#exit
logout
```

5. Reboot the IDS module to the application partition by entering the **reset <module number> hdd:1** command.

```
Console> (enable)reset 5 hdd:1
This command will reset module 5.
Unsaved configuration on module 5 will be lost
Do you want to continue (y/n) [n]? y
Module 5 shut down in progress, please don't remove module
until shutdown completed.
Console> (enable) Module 5 shutdown completed. Module resetting...
```

6. When the IDS module has rebooted, check the software version.

Note: This can also be used for verification purposes.

```
Console> (enable)
Console> (enable)sess 5
Trying IDS-5...
Connected to IDS-5.
Escape character is '^]'.

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

```
sensor#  
sensor#show version  
Application Partition:
```

```
Cisco Systems Intrusion Detection Sensor, Version 4.1(1)S47
```

```
OS Version 2.4.18-5-phoenix  
Platform: WS-SVC-IDSM2-BUN  
Sensor up-time is 4 min.  
Using 701689856 out of 1979682816 bytes of available memory (35% usage)  
Using 527M out of 17G bytes of available disk space (4% usage)
```

```
MainApp 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
AnalysisEngine 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
Authentication 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
Logger 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
NetworkAccess 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
TransactionSource 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
WebServer 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running  
CLI 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500
```

```
Upgrade History:
```

```
No upgrades installed
```

```
Maintenance Partition Version 1.3(2)
```

7. Log in to the application partition CLI and initialize the IDS module, using the **setup** command.

Minor Image Upgrade

This update can be used in situations where the application partition is still accessible, but only part of this application is broken. As compared to using the full image to reimage the Application Partition, the minor image retains the sensor configurations.

To install the minor update, follow these steps:

1. Log into the CLI using an account with administrator privileges.
2. Enter configuration mode by issuing the **configure terminal** command.
3. Type the **upgrade [URL]/<filename>** command to upgrade the sensor.

[URL] is the uniform resource locator pointing to where the signature update package is located. For example, to retrieve the update via FTP, enter the following:

```
upgrade ftp://<username>@<ip-address>//<directory>/<filename>
```

The available transport methods are SCP, FTP, HTTP, or HTTPS.

4. Enter the appropriate password when prompted.
5. To complete the upgrade, type **yes** when prompted.

Upgrading the IDSM2 Service Pack or Signatures

Use the following procedure to upgrade the ISDM2 service sack or signatures.

1. To upgrade the sensor with a service pack or a signature, boot up in the Application Partition.

```
sensor24#show version
Application Partition:
Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S41
OS Version 2.4.18-5-phoenix
Platform: WS-SVC-IDS2-XL
Sensor up-time is 16:45.
Using 377667584 out of 1979682816 bytes of available memory (19% usage)
Using 765M out of 17G bytes of available disk space (5% usage)

MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 NotRunning
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600

Upgrade History:
No upgrades installed
Maintenance Partition Version 1.3(2)
```

2. Log into the IDS module CLI.
3. Enter configure terminal mode using the **configure terminal** command.
4. Enter the **upgrade ftp://<user>@<ftp server IP>/<directory path>/<service pack file>** command to install the service pack and when prompted, type **y** to confirm the installation.

The module reboots when installation is complete.

```
sensor24#configure terminal
sensor24(config)#upgrade ftp://user@10.1.1.1/IDS-K9-min-4.1-1-S47.rpm.pkg
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 (Sat Sep 20 17:59:09 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.

Console> Module 5 shut down in progress, please don't remove module
until shutdown completed.
Console> Module 5 shutdown completed. Module resetting...
```

5. After the module has rebooted, enter the switch CLI and check the version.

Note: This can also be used for verification purposes.

```
sensor24#show version
Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.1(1)S47
OS Version 2.4.18-5-phoenix
Platform: WS-SVC-IDSM2-BUN
Sensor up-time is 6 min.
Using 401248256 out of 1979682816 bytes of available memory (20% usage)
Using 872M out of 17G bytes of available disk space (6% usage)

MainApp 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
```

AnalysisEngine 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
Authentication 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
Logger 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
NetworkAccess 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
TransactionSource 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
WebServer 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
CLI 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500

Upgrade History:

* IDS-maj-4.0-1-S41 12:41:04 UTC Tue Apr 29 2003

IDS-K9-min-4.1-1-S47.rpm.pkg 17:59:06 UTC Sat Sep 20 2003

Maintenance Partition Version 1.3(2)

sensor24#

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco Secure Intrusion Detection Support Page](#)
 - [Documentation for Cisco Secure Intrusion Detection System](#)
 - [Subscribe to Cisco IDS Active Update Notifications](#)
 - [Documentation for Netranger](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 23080
