

Password Recovery Procedure for the Cisco IDS and IPS Sensors and IDS Services Modules (IDSM–1, IDSM–2)

Document ID: 13837

Introduction

Prerequisites

Requirements

Components Used

Conventions

IDS Appliance Version 3

Password Recovery of IDS Appliance that Runs Version 3

Re–image of IDS Appliance that Runs Version 3

IDS Appliance Version 4

Recovery Procedure if Administrator Username/Password is Known

Recovery Procedure if Service Username/Password is Known

Re–image IDS Appliance that Runs Version 4

IPS Appliance Version 5 and Version 6

Reload, Shut Down, Reset, and Recover the AIP–SSM

Reimage the AIP–SSM System Image

IDSM

Re–image IDSM with Switch that Runs Native IOS (Integrated IOS) Code

Re–image IDSM with Switch that Runs Hybrid (CatOS) Code

IDSM–2

Recovery Procedure if Administrator Username/Password is Known

Recovery Procedure if Service Username/Password is Known

Re–image IDSM–2 with Switch that Runs Native IOS (Integrated IOS) Code

Re–image for IDSM–2 with Switch that Runs Hybrid (CatOS) Code

Related Information

Introduction

This document provides procedures on how to recover your Cisco Secure Intrusion Detection System (IDS) (formerly NetRanger) appliance and the modules for all versions.

Prerequisites

Requirements

If an FTP server is needed, it must support passive mode. Recovery CDs can be obtained using the Product Upgrade Tool (registered customers only) .

Components Used

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

- IDS Appliance Versions 3 and 4

- IPS Appliance Versions 5 and 6
- IDS Module (IDSM) Version 3 and IDSM-2 Version 4

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

For more information on document conventions, refer to Cisco Technical Tips Conventions.

IDS Appliance Version 3

Two options are available for the version 3 appliance. You can use the password recovery process or you can do a re-image that uses the Version 3 Recovery CD. Note that all information is lost on a re-image. The password recovery procedure is essentially a Solaris password recovery. Only use this option if you do not have a management station (Cisco Secure Policy Manager (CSPM), VPN/Security Management Solution (VMS), UNIX Director) from which you can copy the configuration.

With IDS Appliance Version 3 and earlier, two usernames exist called 'netrangr' and 'root'. The default password for both is 'attack'.

Password Recovery of IDS Appliance that Runs Version 3

These files are necessary in order to recover your password.

- Solaris Device Configuration Assistant disk (boot disk). You can download the files from the Sun support web site .

Note: If this link does not work, try to go to the top level of the Sun support web site and search for *Device Configuration Assistant Boot Diskette Solaris Driver Downloads* under Drivers. Cisco Systems, Inc. does not maintain the Sun support web site and has no control over where the content is located.

- Solaris for Intel (x86) CD-ROM.
- Console access to the workstation.

Complete these steps in order to recover the password.

1. Insert the boot disk.
2. Insert the CD in the CD-ROM drive.
3. Turn off the workstation, wait ten seconds, and turn it on.

The system boots from the boot disk. After some configuration, the initial Configuration Assistant screen displays.

4. Press **F3** in order to do a partial scan of the system for boot devices.

When the scan is finished, a list of devices displays.

5. Make sure the CD-ROM device appears in the list of devices, and then press **F2** in order to continue.

A screen displays a list of boot devices.

6. Select the **CD-ROM** drive, and then press the space bar.

There is an 'X' next to the CD-ROM device.

7. Press **F2** in order to continue.

The workstation now boots from the CD-ROM.

8. On the screen used to select a type of install, choose **Option 2, Jumpstart**.

The system continues to boot.

9. At the prompt to select a language, choose **Option 0** for English.
10. At the next screen for languages, choose **Option 0** again for English ANSI.

The system continues to boot and the Solaris Installation screen appears.

11. Press and hold the **Control** key and type **C** in order to stop the installation script and allow you access to the prompt.
12. Type **mount -F ufs /dev/dsk/c0t0d0s0 /mnt**.

The '/' partition is now mounted at the '/mnt' mount point. From here you can edit the '/etc/shadow' file and remove the root password.

13. Type **cd /mnt/etc**.
14. Set the shell environment so you can read the data correctly.

- a. Type **TERM=ansi**.
- b. Type **export TERM**.

15. Type **vi shadow**.

You are now in the shadow file and can remove the password. The entry needs to be:

```
root:gNyqp8ohdfxPI:10598:::::::::
```

The ":" is a field separator and the encrypted password is the second field.

16. Delete the second field. For example,

```
root:gNyqp8ohdfxPI:10598:::::::::
```

is changed to

```
root::10598:::::::::
```

This removes the password for the root user.

17. Type **:wq!** in order to write and quit the file.
18. Remove the disk and CD-ROM from the drives.
19. Type **init 6** in order to reboot the system.
20. Type **root** at the login: prompt and then press **Enter**.
21. Press **Enter** at the password prompt.

You are now logged in to the Cisco Secure IDS Sensor.

Re-image of IDS Appliance that Runs Version 3

Complete these steps in order to re-image the IDS Appliance that runs version 3.

Note: Ensure a mouse is not connected to the Sensor before you proceed.

1. Insert the Version 3 Recovery CD into the IDS Appliance and reboot it.

2. Follow the prompts based on your setup until the recovery is successful.
3. Login using the default username/password of 'root/attack'.
4. Run **sysconfig--sensor** in order to reconfigure the appliance.

IDS Appliance Version 4

Recovery Procedure if Administrator Username/Password is Known

If a password for an administrator account is known, this user account can be used in order to reset other user passwords.

For example, two usernames are configured on the IDS Appliance called 'cisco' and 'adminuser'. The password for the user 'cisco' needs to be reset, so 'adminuser' logs in and resets the password.

```
sv8-4-ids4250 login: adminuserPassword:

!--- Output is suppressed.

idsm2-sv-rack#configure terminal
idsm2-sv-rack(config)#no username cisco
idsm2-sv-rack(config)#username cisco priv admin password 123cisco123
idsm2-sv-rack(config)#exit
idsm2-sv-rack#exit

sv8-4-ids4250 login: cisco
Password:

!--- Output is suppressed.

sv8-4-ids4250#
```

Recovery Procedure if Service Username/Password is Known

If a password for the service account is known, this user account can be used in order to reset other user passwords.

For example, three usernames are configured on the IDS Appliance named 'cisco', 'adminuser', and 'serviceuser'. The password for the user 'cisco' needs to be reset, so 'serviceuser' logs in and resets the password.

```
sv8-4-ids4250 login: tacPassword:

!--- Output is suppressed.

bash-2.05a$ su root
Password:
[root@sv8-4-ids4250 serviceuser]#passwd cisco
Changing password for user cisco.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@sv8-4-ids4250 serviceuser]#exit
exit
bash-2.05a$ exit
logout

sv8-4-ids4250 login: cisco
Password:
```

!--- Output is suppressed.

sv8-4-ids4250#

Note: The root password is the same as the password of the service account.

Re-image IDS Appliance that Runs Version 4

Complete these steps in order to re-image the IDS appliance.

Note: Ensure a mouse is not connected to the Sensor before you proceed.

1. Insert the Version 4 Recovery CD into the IDS Appliance and reboot it.
2. Follow the prompts based on your setup until the recovery is successful.
3. Login using the default username/password which is 'cisco/cisco'.
4. Run **setup** in order to reconfigure the appliance.

IPS Appliance Version 5 and Version 6

Reload, Shut Down, Reset, and Recover the AIP-SSM

Use these commands to reload, shut down, reset, recover the password, and recover the Advanced Inspection and Prevention Security Services Module (AIP-SSM) directly from the Adaptive Security Appliance:

Note: You can enter the **hw-module** commands from privileged EXEC mode or from global configuration mode. You can enter the commands in single routed mode and single transparent mode. For adaptive security devices that operate in multi-mode (routed or transparent multi-mode) you can only execute the **hw-module** commands from the system context (not from administrator or user contexts).

- **hw-module module slot_number reload** This command reloads the software on the AIP-SSM without doing a hardware reset. It is effective only when the AIP-SSM is in the Up state.
- **hw-module module slot_number shutdown** This command shuts down the software on the AIP-SSM. It is effective only when the AIP-SSM is in the Up state.
- **hw-module module slot_number reset** This command performs a hardware reset of the AIP-SSM. It is applicable when the card is in the Up/Down/Unresponsive/Recover states.
- **hw-module module slot_number password-reset** This command recovers a password on a Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM) or the AIP-SSM without having to re-image the device.

Note: This command starts support from IPS 6.0 (ASA 7.2 version) and is used to restore the Cisco CLI account password to the default **cisco**.

- **hw-module module slot_number recover [boot | stop | configure]** The **recover** command displays a set of interactive options for setting or changing the recovery parameters. You can change the parameter or keep the existing setting when you press **Enter**.

For the procedure you use to recover the AIP-SSM, see Installing the AIP-SSM System Image.

- ◆ **hw-module module slot_number recover boot** This command initiates recovery of the AIP-SSM. It is applicable only when AIP-SSM is in the Up state.
- ◆ **hw-module module slot_number recover stop** This command stops recovery of the AIP-SSM. It is applicable only when the AIP-SSM is in the Recover state.

Note: If AIP-SSM recovery needs to be stopped, you must issue the **hw-module module 1 recover stop** command within 30 to 45 seconds after you start the AIP-SSM recovery. If you wait any longer, it can lead to unexpected consequences. For example, the AIP-SSM might come up in the Unresponsive state.

- ◆ **hw-module module 1 recover configure** Use this command to configure parameters for module recovery. The essential parameters are the IP address and recovery image TFTP URL location.

Example:

```
aip-ssm#hardware-module module 1 recover configure
Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-1.img]:
Port IP Address [10.89.149.226]:
VLAN ID [0]:
Gateway IP Address [10.89.149.254]:
```

Reimage the AIP-SSM System Image

Complete these steps in order to install the AIP-SSM system image:

1. Log in to the ASA.
2. Enter enable mode:

```
asa>enable
```

3. Configure the recovery settings for the AIP-SSM:

```
asa#hw-module module 1 recover configure
```

Note: If you make an error in the recovery configuration, use the **hw-module module 1 recover stop** command to stop the system reimaging and then you can correct the configuration.

4. Specify the TFTP URL for the system image:

```
Image URL [tftp://0.0.0.0/]:
```

Example:

```
Image URL [tftp://0.0.0.0/]:
tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
```

5. Specify the command and control interface of the AIP-SSM:

```
Port IP Address [0.0.0.0]:
```

Example:

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

6. Leave the VLAN ID at 0.

```
VLAN ID [0]:
```

7. Specify the default gateway of the AIP-SSM:

```
Gateway IP Address [0.0.0.0] :
```

Example:

```
Gateway IP Address [0.0.0.0]:10.89.149.254
```

8. Execute the recovery:

```
asa#hw-module module 1 recover boot
```

9. Periodically check the recovery until it is complete:

Note: The status reads `guest@localhost.localdomain#` during recovery and reads `guest@localhost.localdomain#` when reimaging is complete.

```
asa#show module 1
Mod Card Type                               Model                               Serial No.
-----
  0 ASA 5540 Adaptive Security Appliance   ASA5540                             P2B00000019
  1 ASA 5500 Series Security Services Module-20 ASA-SSM-20                          P1D000004F4
Mod MAC Address Range                       Hw Version   Fw Version   Sw Version
-----
  0 000b.fcf8.7b1c to 000b.fcf8.7b20 0.2          1.0(7)2     7.0(0)82
  1 000b.fcf8.011e to 000b.fcf8.011e 0.1          1.0(7)2     5.0(0.22)S129.0
Mod Status
-----
  0 Up Sys
  1 Up
asa#
```

Note: In order to debug any errors that might happen in the recovery process, use the **debug module-boot** command to enable debugging of the system reimaging process.

10. Session to the AIP-SSM and initialize the AIP-SSM with the **setup** command.

ISDM

There is no method you can use to perform a password recovery on the ISDM while the configuration is retained.

Note: This procedure requires the use of the maintenance partition. If the maintenance partition password has been changed and you are unable to log in, the ISDM needs to be replaced. In this case, contact Cisco Technical Support for assistance.

Re-image ISDM with Switch that Runs Native IOS (Integrated IOS) Code

Complete these steps in order to re-image the ISDM with a switch that runs Native IOS (Integrated IOS) code.

1. Boot the ISDM to the Maintenance Partition using the switch command **hw-module module x reset hdd:2** where *x* stands for the slot number.

```
SV9-1#show module 6
Mod Ports Card Type                               Model                               Serial No.
-----
  6    2  Intrusion Detection System             WS-X6381-IDS                       SAD063000CE
Mod MAC addresses                               Hw   Fw           Sw           Status
-----
  6  0002.7e39.2b20 to 0002.7e39.2b21 1.2  4B4LZ0XA     3.0(1)S4     Ok
SV9-1#hw-module module 6 reset hdd:2
Device BOOT variable for reset =
Warning: Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 6
```

!--- Output suppressed.

2. Check that the IDSM comes online using the switch command **show module x** .

Make sure that the IDSM Software version has 2 located at the beginning that indicates that the maintenance partition software currently runs on the IDSM and that the status is OK.

```
SV9-1#show module 6
Mod Ports Card Type Model Serial No.
-----
6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE
Mod MAC addresses Hw Fw Sw Status
-----
6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 2.5(0) Ok
```

3. Connect to the IDSM maintenance partition using the switch command **session slot x processor 1**.

Use the username/password of **ciscoids/attack**.

```
SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: ciscoidsPassword:
maintenance#
```

4. Install the cached image in order to re-image the IDSM Application Partition.

Issue the diagnostics command **ids-installer system /cache /show** in order to verify that the cached image exists.

```
maintenance#diag
maintenance(diag)#ids-installer system /cache /show
Details of the cached image:
Package Name : IDSMk9-a-3.0-1-S4
Release Info : 3.0-1-S4
Total CAB Files in the package : 5
CAB Files present : 5
CAB Files missing : 0
List of CAB Files missing
-----
maintenance(diag)#
```

If no cached image exists or the version cached is not the one you want to install, proceed to step 5.

In order to re-image the ISDM using the cached image, use the diagnostics command **ids-installer system /cache /install**.

```
maintenance(diag)#ids-installer system /cache /install
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 E41E-3608
Extracting the image...
```

!--- Output is suppressed.

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

Once the re-image has completed, proceed to step 12.

5. Make sure that the IDSM has IP connectivity. Issue the command **ping ip_address** .

```
maintenance#diag
maintenance(diag)#ping 10.66.84.1
Pinging 10.66.84.1 with 32 bytes of data:
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
```

6. If the IDSM has IP connectivity, proceed to step 11. If you do not have IP connectivity, proceed with steps 7 through 9.
7. Make sure that the Command and Control Interface is configured properly on the switch. Issue the command **show run interface Gigx/2**.

```
SV9-1#show run interface Gig6/2
Building configuration...
Current configuration : 115 bytes
!
interface GigabitEthernet6/2
 no ip address switchport
 switchport access vlan 210
 switchport mode access
end
SV9-1#
```

8. Make sure that the communication parameters are configured properly on the IDSM Maintenance Partition. Issue the diagnostics command **ids-installer netconfig /view**.

```
maintenance#diag
maintenance(diag)#ids-installer netconfig /view
IP Configuration for Control Port:
IP Address       : 10.66.84.124
Subnet Mask      : 255.255.255.128
Default Gateway  : 10.66.84.1
Domain Name Server : 1.1.1.1
Domain Name      : cisco
Host Name        : idsm-sv-rack
```

9. If none of the parameters are set, or if some of them need to be changed, use the diagnostics command **ids-installer netconfig /configure parameters** .

```
maintenance(diag)#ids-installer netconfig /configure /
ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 /
dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack
STATUS: Network parameters for the config port have been configured
!
NOTE: Reset the module for the changes to take effect!
```

10. Check IP connectivity again after you have reset the IDSM for the changes to take effect. If IP connectivity is still an issue, troubleshoot as per a normal IP connectivity problem, then proceed with step 11.
11. Re-image the IDSM Application Partition. Download the image using the diagnostic command **ids-installer system /nw /install /server=ip_address /user=account /save={yes/no} /dir=ftp_path /prefix=file_prefix** where:

- ◆ *ip_address* is the IP address of the FTP server.
- ◆ *account* is the user or account name to be used when logging into the FTP server.
- ◆ *save* determines whether to save a copy of the downloaded image as the cached copy. If yes,

any cached image that exists is overwritten. If no, the downloaded image is installed on the inactive partition but a cached copy is not saved.

- ◆ *ftp_path* specifies the directory on the FTP server where the image files are located.
- ◆ *file_prefix* is the file name of the .dat file in the downloaded image. The downloaded image consists of one file with the .dat extension and several files with the .cab extension. The file_prefix value needs to be the name of the DAT file, up to but not including the .dat suffix.

```
maintenance#diag
maintenance(diag)#ids-installer system /nw /install /server=10.66.64.10
/user=cisco /save=yes /dir='/tftpboot/georgia' /
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 2407-F686
Extracting the image...
```

!--- Output is suppressed.

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

12. Boot the IDSM to the Application Partition using the switch command **hw-module module x reset hdd:1**.

```
SV9-1#hw-module module 6 reset hdd:1
Device BOOT variable for reset =
Warning: Device list is not verified.

Proceed with reload of module? [confirm]
```

!--- Output is suppressed.

Also ensure that the switch is configured to boot up the IDSM into the application partition. In order to check this, use the command **show bootvar device module x**.

```
SV9-1#show bootvar device module 6
[mod:6 ]:
SV9-1#
```

In order to configure the boot device variable for the IDSM, use the switch configuration command **boot device module x hdd:1**.

```
SV9-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SV9-1(config)#boot device module 6 hdd:1
Device BOOT variable = hdd:1
Warning: Device list is not verified.
SV9-1(config)#endSV9-1#show bootvar device module 6
[mod:6 ]: hdd:1
SV9-1#
```

13. Check that the IDSM comes online using the switch command **show module x**.

Make sure that the IDSM software version is an application partition version, for example 3.0(1)S4, and that the status is OK.

```
SV9-1#show module 6
Mod Ports Card Type Model Serial No.
-----
6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE
Mod MAC addresses Hw Fw Sw Status
-----
6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok
```

14. Connect to the IDSM now that it has booted up into the application partition and configure it so it can communicate to the director. Use the command **setup**.

Once communication with the director has been established, configuration can be downloaded to the IDSM.

Use the username/password of **ciscoids/attack** in order to log in.

```
SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: ciscoids
Password:#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:
Configuration last modified Never
Sensor:
IP Address: 10.0.0.1
Netmask: 255.0.0.0
Default Gateway:Host Name: Not Set
Host ID: Not Set
Host Port: 45000
Organization Name: Not Set
Organization ID: Not Set
Director:
IP Address: Not Set
Host Name: Not Set
Host ID: Not Set
Host Port: 45000
Heart Beat Interval (secs): 5
Organization Name: Not Set
Organization ID: Not Set
Direct Telnet access to IDSM: disabled
Continue with configuration dialog? [yes]:
Enter virtual terminal password[:
Enter sensor IP address[10.0.0.1]: 10.66.84.124
Enter sensor netmask [255.0.0.0]: 255.255.255.128
Enter sensor default gateway []: 10.66.84.1
Enter sensor host name []: idsm-sv-rack
Enter sensor host id []: 124
Enter sensor host post office port [45000]:
Enter sensor organization name []: cisco
Enter sensor organization id []: 100
Enter director IP address[: 10.66.79.249
Enter director host name []: vms1
Enter director host id []: 249
Enter director host post office port [45000]:
Enter director heart beat interval [5]:
```

```

Enter director organization name []: cisco
Enter director organization id []: 100
Enable direct Telnet access to IDSM? [no]:
The following configuration was entered:
Configuration last modified Never
Sensor:IP Address:          10.66.84.124
Netmask:                   255.255.255.128
Default Gateway:           10.66.84.1
Host Name:                 idsm-sv-rack
Host ID:                   124
Host Port:                 45000
Organization Name:        cisco
Organization ID:          100
Director:
IP Address:               10.66.79.249
Host Name:                vms1
Host ID:                  249
Host Port:                45000
Heart Beat Interval (secs): 5
Organization Name:        cisco
Organization ID:          100
Direct Telnet access to IDSM: disabled
WARNING: Applying this configuration will cause all
configuration files
to be initialized and the card to be rebooted.
Apply this configuration?: yes
Configuration Saved. Resetting...

```

!--- Output is suppressed.

Re-image IDSM with Switch that Runs Hybrid (CatOS) Code

Complete these steps in order to re-image IDSM with a switch that runs hybrid (CatOS) code.

Note: All information is lost on the application partition. There is no method you can use to perform a password recovery on the IDSM while you retain the configuration.

Note: This procedure requires the use of the maintenance partition. If the maintenance partition password has been changed and you are unable to log in, the IDSM needs to be replaced. In this case, contact Cisco Technical Support for assistance.

1. Boot the IDSM to the Maintenance Partition with the switch command **reset x hdd:2**.

```

ltd9-9> (enable) show module 4
Mod Slot Ports Module-Type          Model          Sub Status
-----
4   4   2   Intrusion Detection Syste WS-X6381-IDS   no  ok
Mod Module-Name          Serial-Num
-----
4                          SAD063000CE
Mod MAC-Address(es)      Hw      Fw      Sw
-----
4  00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2      4B4LZ0XA  3.0(5)S23
ltd9-9> (enable)reset 4 hdd:2
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
Module 4 shut down in progress, please don't remove module
until shutdown completed.

```

!--- Output is suppressed.

2. Check that the IDSM comes online with the switch command **show module x**.

Make sure that the IDSM software version has 2 located at the beginning that indicates that the maintenance partition software currently runs on the IDSM and that the status is OK.

```
ltd9-9> (enable) show module 4
Mod Slot Ports Module-Type Model Sub Status
-----
4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok
Mod Module-Name Serial-Num
-----
4 SAD
063000CEMod MAC-Address(es) Hw Fw Sw
-----
4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 2.5(0)
```

3. Connect to the IDSM now that it has booted up into the maintenance partition with the switch command **session x**.

Use the username/password of **ciscoids/attack**.

```
ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:
maintenance#
```

4. Install the cached image in order to re-image the IDSM Application Partition.

Verify that the cached image exists with the use of the diagnostics command **ids-installer system /cache /show**.

```
maintenance#diag
maintenance(diag)#ids-installer system /cache /show
Details of the cached image:
Package Name : IDSMk9-a-3.0-1-S4
Release Info : 3.0-1-S4
Total CAB Files in the package : 5
CAB Files present : 5
CAB Files missing : 0
List of CAB Files missing
-----
maintenance(diag)#
```

If no cached image exists, or the version cached is not the one you want to install, proceed to step 5.

In order to re-image the ISDM that uses the cached image, use the diagnostics command **ids-installer system /cache /install**.

```
maintenance(diag)#ids-installer system /cache /install
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 E41E-3608
Extracting the image...
```

!--- Output is suppressed.

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

Once the reimage has completed, proceed to step 12.

5. Make sure that the IDSM has IP connectivity with the use of the command **ping ip_address** .

```
maintenance#diag
maintenance(diag)#ping 10.66.84.1
Pinging 10.66.84.1 with 32 bytes of data:
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
```

6. If the IDSM has IP connectivity, proceed to step 11. If you do not have IP connectivity, proceed with steps 7 through 9.
7. Make sure that the Command and Control Interface is configured properly on the switch with the use of the command **show port status x/2**.

```
ltd9-9> (enable)show port status 4/2
Port Name Status Vlan Duplex Speed Type
-----
4/2 connected 1 full 1000 Intrusion De
```

8. Make sure that the communication parameters are configured properly on the IDSM Maintenance Partition with the use of the the diagnostics command **ids-installer netconfig /view**.

```
maintenance#diag
maintenance(diag)#ids-installer netconfig /view
IP Configuration for Control Port:
IP Address : 10.66.84.124
Subnet Mask : 255.255.255.128
Default Gateway : 10.66.84.1
Domain Name Server : 1.1.1.1
Domain Name : cisco
Host Name : idsm-sv-rack
```

9. If none of the parameters are set, or if some of them need to be changed, use the diagnostics command **ids-installer netconfig /configure parameters** .

```
maintenance(diag)# ids-installer netconfig /configure /
ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 /
dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack
```

10. Check IP Connectivity again after you have reset the IDSM for the changes to take effect.

If IP connectivity is still an issue, troubleshoot as per a normal IP connectivity problem, then proceed with step 11.

11. Re-image the IDSM Application Partition. Download the image with the use of the diagnostic command **ids-installer system /nw /install /server=ip_address /user=account /save={yes/no} /dir=ftp_path /prefix=file_prefix** where:

- ◆ *ip_address* is the IP address of the FTP server.
- ◆ *account* is the user or account name to be used when logging into the FTP server.
- ◆ *save* determines whether to save a copy of the downloaded image as the cached copy. If yes, any existing cached image is overwritten. If no, the downloaded image is installed on the inactive partition but a cached copy is not saved.
- ◆ *ftp_path* specifies the directory on the FTP server where the image files are located.

- ◆ *file_prefix* is the file name of the .dat file in the downloaded image. The downloaded image consists of one file with the .dat extension and several files with the .cab extension. The file_prefix value should be the name of the DAT file, up to but not including the .dat suffix.

```

maintenance#diag
maintenance(diag)#ids-installer system /nw /install /server=10.66.64.10
/user=cisco /save=yes /dir='/tftpboot/georgia'
/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 2407-F686
Extracting the image...

```

!--- Output is suppressed.

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

12. Boot the IDSM to the Application Partition with the use of the switch command **reset x hdd:1**.

```

ltd9-9> (enable)reset 4 hdd:1
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y

```

!--- Output is suppressed.

Also make sure that the switch is configured in order to boot up the IDSM into the application partition. IUse the command **show boot device x** in order to check this.

```

ltd9-9> (enable)show boot device 4
Device BOOT variable =

```

In order to configure the boot device variable for the IDSM, use the switch configuration command **set boot device hdd:1 x** .

```

ltd9-9> (enable)set boot device hdd:1 4
Device BOOT variable = hdd:1
Warning: Device list is not verified but still set in the boot string.
ltd9-9> (enable)show boot device 4
Device BOOT variable = hdd:1

```

13. Check that the IDSM comes online with the use of the switch command **show module x** .

Make sure that the IDSM software version is an application partition version, for example, *3.0(1)S4*, and that the status is OK.

```

ltd9-9> (enable)show module 4
Mod Slot Ports Module-Type Model Sub Status
-----
4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok
Mod Module-Name Serial-Num
-----
4 SAD063000CE
Mod MAC-Address(es) Hw Fw Sw
-----

```

14. Connect to the IDSM now that it has booted up into the application partition and configure it so it can communicate to the director. Use the command **setup**.

Login with the username/password of **ciscoids/attack**.

```

ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:#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:
Configuration last modified Never
Sensor:
IP Address:                10.0.0.1
Netmask:                   255.0.0.0
Default Gateway:
Host Name:                 Not Set
Host ID:                   Not Set
Host Port:                 45000
Organization Name:        Not Set
Organization ID:          Not Set
Director:
IP Address:                Not Set
Host Name:                 Not Set
Host ID:                   Not Set
Host Port:                 45000
Heart Beat Interval (secs): 5
Organization Name:        Not Set
Organization ID:          Not Set
Direct Telnet access to IDSM: disabled
Continue with configuration dialog? [yes]:
Enter virtual terminal password[]:
Enter sensor IP address[10.0.0.1]: 10.66.84.124
Enter sensor netmask [255.0.0.0]: 255.255.255.128
Enter sensor default gateway []: 10.66.84.1
Enter sensor host name []: idsm-sv-rack
Enter sensor host id []: 124
Enter sensor host post office port [45000]:
Enter sensor organization name []: cisco
Enter sensor organization id []: 100
Enter director IP address[]: 10.66.79.249
Enter director host name []: vms1
Enter director host id []: 249
Enter director host post office port [45000]:
Enter director heart beat interval [5]:
Enter director organization name []: cisco
Enter director organization id []: 100
Enable direct Telnet access to IDSM? [no]:
The following configuration was entered:
Configuration last modified Never
Sensor:
IP Address:                10.66.84.124
Netmask:                   255.255.255.128
Default Gateway:          10.66.84.1
Host Name:                 idsm-sv-rack
Host ID:                   124
Host Port:                 45000

```

```

Organization Name:      cisco
Organization ID:        100
Director:IP Address:   10.66.79.249
Host Name:              vms1
Host ID:                249
Host Port:              45000
Heart Beat Interval (secs): 5
Organization Name:      cisco
Organization ID:        100
Direct Telnet access to IDSM: disabled
WARNING: Applying this configuration will cause all
configuration files to be initialized and the
card to be rebooted.
Apply this configuration?: yes
Configuration Saved.
Resetting...

```

!--- Output is suppressed.

ISDM-2

Recovery Procedure if Administrator Username/Password is Known

If a password for an administrator account is known, this user account can be used in order to reset other user passwords.

For example, two usernames are configured on the IDSM-2 named 'cisco' and 'adminuser'. The password for the user 'cisco' needs to be reset, so 'adminuser' logs in and resets the password.

```

SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: adminuser
Password:

```

!--- Output is suppressed.

```

idsm2-sv-rack#configure terminal
idsm2-sv-rack(config)#no username cisco
idsm2-sv-rack(config)#username cisco priv admin password 123cisco123
idsm2-sv-rack(config)#exit
idsm2-sv-rack#exit

```

```

[Connection to 127.0.0.61 closed by foreign host]
SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: cisco
Password:

```

!--- Output is suppressed.

```

idsm2-sv-rack#

```

Recovery Procedure if Service Username/Password is Known

If a password for the service account is known, this user account can be used in order to reset other user passwords.

For example, three usernames are configured on the IDSM-2 named 'cisco', 'adminuser', and 'serviceuser'. The password for the user 'cisco' needs to be reset, so 'serviceuser' logs in and resets the password.

```
SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: serviceuser
Password:
```

!--- Output is suppressed.

```
bash-2.05a$ su root
Password:
[root@idsm2-sv-rack serviceuser]#passwd cisco
Changing password for user cisco.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@idsm2-sv-rack serviceuser]# exit
exit
bash-2.05a$ exit
logout
```

```
[Connection to 127.0.0.61 closed by foreign host]
SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: cisco
Password:
```

!--- Output is suppressed.

```
idsm2-sv-rack#
```

Note: The root password is the same as the service account's password.

Re-image IDSM-2 with Switch that Runs Native IOS (Integrated IOS) Code

Complete these steps in order to re-image IDSM-2 with a switch that runs Native IOS (Integrated IOS) code.

Note: All information is lost on the application partition. There is no method you can use in order to perform a password recovery on the IDSM-2 while the configuration is retained.

1. Boot the IDSM-2 to the Maintenance Partition with the use of the switch command **hw-module module x reset cf:1** where *x* stands for the slot number and *cf* stands for 'compact flash'.

Note: If a problem is encountered using *cf:1*, try to use *hdd:2* as an alternative.

```
SV9-1#show module 6
```

```

Mod Ports Card Type                               Model                               Serial No.
-----
 6      8 Intrusion Detection System              WS-SVC-IDS2M2                      SAD0645010J
Mod MAC addresses                               Hw   Fw   Sw   Status
-----
 6  0030.f271.e3fd to 0030.f271.e404  0.102 7.2(1) 4.1(1)S47  Ok
Mod Sub-Module                               Model   Serial   Hw   Status
-----
 6 IDS 2 accelerator board              WS-SVC-IDSUPG  0347FDB6B8  2.0  Ok
Mod Online Diag Status
-----
 6 Pass
SV9-1#hw-module module 6 reset cf:1
Device BOOT variable for reset =
Warning: Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 6

!--- Output is suppressed.

```

2. Check that the IDSM-2 comes online with the use of the switch command **show module x**.

Make sure that the IDSM-2 software version has 'm' located at the end and that the status is OK.

```

SV9-1#show module 6
Mod Ports Card Type                               Model                               Serial No.
-----
 6      8 Intrusion Detection System (MP)        WS-SVC-IDS2M2                      SAD0645010J
Mod MAC addresses                               Hw   Fw   Sw   Status
-----
 6  0030.f271.e3fd to 0030.f271.e404  0.102 7.2(1) 1.3(2)m  Ok
Mod Sub-Module                               Model   Serial   Hw   Status
-----
 6 IDS 2 accelerator board              WS-SVC-IDSUPG  0347FDB6B8  2.0  Ok
Mod Online Diag Status
-----
 6 Pass

```

3. Connect to the IDSM-2 now that it has booted up into the maintenance partition. Use the switch command **session slot xprocessor 1**.

Use the username/password of **guest/cisco**.

```

SV9-1#session slot 6 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
Cisco Maintenance image
login: guest
Password:
Maintenance image version: 1.3(2)
guest@idsm2-sv-rack.localdomain#

```

4. Make sure that the IDSM-2 has IP connectivity. Use the command **ping ip_address**.

```

guest@idsm2-sv-rack.localdomain#ping 10.66.79.193
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193
PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data.
64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=2.188 msec
64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.014 msec
64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=991 usec
64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.011 msec
64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.019 msec

```

```

--- 10.66.79.193 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.991/1.244/2.188/0.473 ms
guest@idsm2-sv-rack.localdomain#

```

5. If the IDSM-2 has IP connectivity, proceed to step 14.
6. Make sure that the Command and Control Interface is configured properly on the switch. Use the command **show run | inc intrusion-detection**.

```

SV9-1#show run | inc intrusion-detection
intrusion-detection module 6 management-port access-vlan 210

```

7. Make sure that the communication parameters are configured properly on the IDSM-2 Maintenance Partition. Use the command **show ip**.

```

guest@idsm2-sv-rack.local
domain#show ip
IP address      : 10.66.79.210
Subnet Mask     : 255.255.255.224
IP Broadcast    : 10.66.79.223
DNS Name       : idsm2-sv-rack.localdomain
Default Gateway : 10.66.79.193Nameserver(s)   :

```

8. If none of the parameters are set, or if some of them need to be changed, clear them all. Use the command **clear ip**.

```

guest@idsm2-sv-rack.localdomain#clear ip
guest@localhost.localdomain#show ip
IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name       : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)  :

```

9. Configure the IP address and mask information on the IDSM-2 Maintenance Partition. Use the command **ip address ip_address netmask**.

```

guest@localhost.localdomain#ip address 10.66.79.210 255.255.255.224

```

10. Configure the default gateway on the IDSM-2 Maintenance Partition. Use the command **ip gateway gateway-address**.

```

guest@localhost.localdomain#ip gateway 10.66.79.193

```

11. Configure the hostname on the IDSM-2 Maintenance Partition. Use the command **ip host hostname**.

Although this is not necessary, it does help to identify the device since this also sets the prompt.

```

guest@localhost.localdomain#ip host idsm2-sv-rack
guest@idsm2-sv-rack.localdomain#

```

12. You might possibly need to configure your broadcast address explicitly. Use the command **ip broadcast broadcast-address**.

The default setting usually suffices.

```

guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223

```

13. Check the IP Connectivity again. If IP connectivity is still an issue, troubleshoot as per a normal IP connectivity problem and proceed with step 14.

14. Re-image the IDSM-2 Application Partition. Use the command **upgrade ftp-url --install**.

```

guest@idsm2-sv-rack.localdomain#upgrade ftp://cisco@10.66.64.10//
tftpboot/WS-SVC-IDS2-K9-a-4.1-1-S47.bin.gz --install
Downloading the image. This may take several minutes...

```

```

Password for cisco@10.66.64.10:
500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood.
ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz
  (unknown size)/tmp/upgrade.gz          [|] 65259K
66825226 bytes transferred in 71.40 sec (913.99k/sec)
Upgrade file ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz is
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.

```

15. Boot the IDSM-2 to the Application Partition. Use the switch command **hw-module module x reset hdd:1**.

```

SV9-1#hw-module module 6 reset hdd:1
Device BOOT variable for reset =
Warning: Device list is not verified.

Proceed with reload of module? [confirm]y
% reset issued for module 6

```

!--- Output is suppressed.

Alternatively, you can use the **reset** command on the IDSM-2 as long as the boot device variable is set correctly.

In order to check the boot device variable setting for the IDSM-2, use the switch command **show bootvar device module x**.

```

SV9-1#show bootvar device module 6
[mod:6 ]:
SV9-1#

```

In order to configure the boot device variable for the IDSM-2, use the switch configuration command **boot device module x hdd:1**.

```

SV9-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SV9-1(config)#boot device module 6 hdd:1
Device BOOT variable = hdd:1
Warning: Device list is not verified.
SV9-1(config)#exitSV9-1#show bootvar device module 6
[mod:6 ]: hdd:1

```

In order to reset the IDSM-2 via the Maintenance Partition CLI, use the command **reset**.

```

guest@idsm2-sv-rack.localdomain#reset

```

!--- Output is suppressed.

16. Check that the IDSM-2 comes online. Use the switch command **show module x**.

Make sure that the IDSM-2 software version is an application partition version, for example 4.1(1)S47 and that the status is OK.

```
SV9-1#show module 6
Mod Ports Card Type                               Model                               Serial No.
-----
   6    8  Intrusion Detection System             WS-SVC-IDSM2                       SAD0645010J
Mod MAC addresses                               Hw  Fw                               Sw                               Status
-----
   6  0030.f271.e3fd to 0030.f271.e404  0.102 7.2(1)                       4.1(1)S47                       Ok
Mod Sub-Module                               Model                               Serial                               Hw                               Status
-----
   6 IDS 2 accelerator board             WS-SVC-IDSUPG  0347FDB6B8                       2.0                               Ok
Mod Online Diag Status
-----
   6 Pass
```

17. Connect to the IDSM-2 now that it has booted up into the application partition. Use the switch command **session slot x processor 1**.

Use the username/password of **cisco/cisco**.

```
SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
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:
```

!--- Output is suppressed.

18. Configure the IDSM-2. Use the command **setup**.

```
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:networkParams
ipAddress 10.1.9.201
netmask 255.255.255.0
defaultGateway 10.1.9.1
hostname sensor
telnet
Option disabled
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
Current time: Sat Sep 20 23:34:53 2003
```

```

Setup Configuration last modified: Sat Sep 20 23:32:38 2003
Continue with configuration dialog?[yes]:
Enter host name[sensor]: idsm2-sv-rack
Enter IP address[10.1.9.201]: 10.66.79.210
Enter netmask[255.255.255.0]: 255.255.255.224
Enter default gateway[10.1.9.1]: 10.66.79.193
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]:
Modify system clock settings?[no]:
The following configuration was entered.
networkParams
ipAddress 10.66.79.210
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname idsm2-sv-rack
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.Enter your selection
[2]:Configuration Saved.
sensor#

```

Re-image for ISDM-2 with Switch that Runs Hybrid (CatOS) Code

Complete these steps in order to re-image the ISDM-2 with a switch that runs hybrid (CatOS) code.

1. Boot the ISDM-2 into the Maintenance Partition. Use the switch command **reset x hdd:2**.

Note: If a problem is encountered using hdd:2, try to use cf:1 as an alternative.

```

SV9-1> (enable)show module 6
Mod Slot Ports Module-Type Model Sub Status
-----
6 6 8 Intrusion Detection Syste WS-SVC-IDS2M2 yes ok
Mod Module-Name Serial-Num
-----
6 SAD0645010J
Mod MAC-Address(es) Hw Fw Sw
-----
6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47
Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw
-----
6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0
SV9-1> (enable)reset 6 hdd:2
This command will reset module 6.
Unsaved configuration on module 6 will be lost
Do you want to continue (y/n) [n]? y
Module 6 shut down in progress, please don't remove module
until shutdown completed.

```

!--- Output is suppressed.

2. Check that the IDSM-2 comes online. Use the switch command **show module x** .

Make sure that the IDSM-2 software version has 'm' located at the end that indicates that the maintenance partition software currently runs and that the status is OK.

```
SV9-1> (enable)show module 6
Mod Slot Ports Module-Type Model Sub Status
-----
6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
Mod Module-Name Serial-Num
-----
6 SAD0645010J
Mod MAC-Address(es) Hw Fw Sw
-----
6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 1.3(2)m
Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw
-----
6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0
```

3. Connect to the IDSM-2 now that it has booted up into the maintenance partition. Use the switch command **session x** .

Use the username/password of **guest/cisco**.

```
SV9-1> (enable)session 6
Trying IDS-6...
Connected to IDS-6.
Escape character is '^]'.
Cisco Maintenance image
login: guest
Password:
Maintenance image version: 1.3(2)
guest@idsm2-sv-rack.localdomain#
```

4. Make sure that the IDSM-2 has IP connectivity. Use the command **ping ip_address** .

```
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193
PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data.
64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=1.035 msec
64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.041 msec
64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=1.066 msec
64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.074 msec
64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.026 msec
--- 10.66.79.193 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 1.026/1.048/1.074/0.034 ms
```

5. If the IDSM-2 has IP connectivity, proceed to step 14.
6. Make sure that the Command and Control Interface is configured properly on the switch. Use the command **show port status x/2**.

```
SV9-1> (enable)show port status 6/2
Port Name Status Vlan Duplex Speed Type
-----
6/2 connected 210 full 1000 Intrusion De
```

7. Make sure that the communication parameters are configured properly on the IDSM-2 Maintenance Partition. Use the command **show ip**.

```
guest@idsm2-sv-rack.localdomain#show ip
IP address : 10.66.79.210
Subnet Mask : 255.255.255.224
```

```
IP Broadcast      : 10.255.255.255
DNS Name          : idsm2-sv-rack.localdomain
Default Gateway  : 10.66.79.193
Nameserver(s)    :
```

8. If none of the parameters are set or if some of them need to be changed, clear them all with the use of the command **clear ip**.

```
guest@idsm2-sv-rack.localdomain#clear ip
guest@localhost.localdomain#show ip
IP address       : 0.0.0.0
Subnet Mask      : 0.0.0.0
IP Broadcast     : 0.0.0.0
DNS Name         : localhost.localdomain
Default Gateway  : 0.0.0.0
```

9. Configure the IP address and mask information on the IDSM-2 Maintenance Partition. Use the command **ip address ip_address netmask**.

```
guest@localhost.localdomain#ip address 10.66.79.210 255.255.255.224
guest@localhost.localdomain#
```

10. Configure the default gateway on the IDSM-2 Maintenance Partition. Use the command **ip gateway gateway-address**.

```
guest@localhost.localdomain#ip gateway 10.66.79.193
guest@localhost.localdomain#
```

11. Configure the hostname on the IDSM-2 Maintenance Partition. Use the command **ip host hostname**.

Although this is not necessary, it helps to identify the device since this also sets the prompt.

```
guest@localhost.localdomain#ip host idsm2-sv-rack
guest@idsm2-sv-rack.localdomain#
```

12. You might possibly need to configure your broadcast address explicitly. Use the command **ip broadcast broadcast-address**.

The default setting usually suffices.

```
guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223
```

13. Check IP Connectivity again. If IP connectivity is still an issue, troubleshoot as per a normal IP connectivity problem then proceed with step 14.

14. Re-image the IDSM-2 Application Partition. Use the command **upgrade ftp-url --install**.

```
guest@idsm2-sv-rack.localdomain#upgrade ftp://cisco@10.66.64.10//
tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz --install
Downloading the image. This may take several minutes...
Password for cisco@10.66.64.10:500
'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not
understood.ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.
gz (unknown size)/tmp/upgrade.gz          [||] 65259K
66825226 bytes transferred in 71.37 sec (914.35k/sec)
Upgrade file ftp://cisco@10.66.64.10//tftpboot/
WS-SVC-IDSM2-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.

15. Boot the IDSM-2 to the Application Partition. Use the switch command **reset x hdd:1**.

```
SV9-1> (enable)reset 6 hdd:1
This command will reset module 6.
Unsaved configuration on module 6 will be lost
Do you want to continue (y/n) [n]? y
Module 6 shut down in progress, please don't remove module
until shutdown completed.
```

!--- Output is suppressed.

Alternatively, you can use the **reset** command on the IDSM-2 as long as the the boot device variable is set correctly.

In order to check the boot device variable setting for the IDSM-2, use the switch command **show boot device x** .

```
SV9-1> (enable)show boot device 6
Device BOOT variable = (null) (Default boot partition is hdd:1)
Memory-test set to PARTIAL
```

In order to configure the boot device variable for the IDSM-2, use the switch configuration command **set boot device hdd:1 x** .

```
SV9-1> (enable)set boot device hdd:1 6
Device BOOT variable = hdd:1
Memory-test set to PARTIAL
Warning: Device list is not verified but still set in
the boot string.
SV9-1> (enable) show boot device 6
Device BOOT variable = hdd:1
Memory-test set to PARTIAL
```

In order to reset the IDSM-2 via the Maintenance Partition CLI, use the command **reset**.

```
guest@idsm2-sv-rack.localdomain#reset
```

!--- Output is suppressed.

16. Check that the IDSM-2 comes online. Use the switch command **show module x** .

Make sure that the IDSM-2 software version is an application partition version, for example *4.1(1)S47*, and that the status is OK.

```
SV9-1> (enable)show module 6
Mod Slot Ports Module-Type Model Sub Status
-----
6 6 8 Intrusion Detection Syste WS-SVC-IDS2M2 yes ok
Mod Module-Name Serial-Num
-----
6 SAD0645010J
Mod MAC-Address(es) Hw Fw Sw
-----
6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47
Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw
-----
6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0
```

17. Connect to the IDSM-2 now that it has booted up into the application partition. Use the switch command **session x**.

Use the username/password of **cisco/cisco**.

```
SV9-1> (enable)session 6
Trying IDS-6...
Connected to IDS-6.
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:
```

!--- Output is suppressed.

18. Configure the IDSM-2 with the use of the command **setup**.

```
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:
networkParams
ipAddress 10.1.9.201
netmask 255.255.255.0
defaultGateway 10.1.9.1
hostname sensor
telnetOption disabled
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
Current time: Sat Sep 20 21:39:29 2003
Setup Configuration last modified: Sat Sep 20 21:36:30 2003
Continue with configuration dialog?[yes]:
Enter host name[sensor]: idsm2-sv-rack
Enter IP address[10.1.9.201]: 10.66.79.210
Enter netmask[255.255.255.0]: 255.255.255.224
Enter default gateway[10.1.9.1]: 10.66.79.193
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]:
Modify system clock settings?[no]:
The following configuration was entered.
networkParams
ipAddress 10.66.79.210
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname idsm2-sv-rack
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
```

```
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
Enter your selection[2]:
Configuration Saved.
sensor#
```

Related Information

- **Cisco IDS Sensor Software**
 - **Cisco IDS UNIX Director**
 - **Catalyst 6500 Series Intrusion Detection System (IDSM-1) Services Module**
 - **Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module**
 - **Requests for Comments (RFCs)**
 - **Technical Support – Cisco Systems**
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 19, 2007

Document ID: 13837
