

# Intrusion Detection System 4.0/Intrusion Prevention System (IPS) 5.0 and Later FAQ

Document ID: 50360

---

## Questions

**Introduction**

**IDS 4.0**

**IPS 5.0 and Later**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document answers the most Frequently Asked Questions (FAQs) related to Cisco Secure Intrusion Detection System (IDS) 4.0, Cisco Intrusion Prevention System (IPS) 5.0 and later.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## IDS 4.0

**Q. I have installed IDS MC and SecMon over a new server, and now I want to import all configurations (user, device, and so forth) from the old server to the new one. How do I do this?**

**A.** The easiest way to perform this is to bring up your new VMS server, and then discover the Sensors with this new box.

**Note:** When you add the Sensor, do not add it manually. Check the **discover settings** box.

Once the Sensor is discovered, import it into SecMon. All the configurations are saved on the Sensor. The signature settings, filters, and so forth should come across after you build your new server. Make sure you update IDS MC to the latest signatures.

**Q. IDS-4215 receives the `idsPackageMgr: invalid argument error` message while it attempts to upgrade the IDS recovery partition. What do I need to do to resolve this issue?**

**A.** This is a manufacturing issue. Some customers received IDS-4215s with a bad base image (4.0). Complete these steps.

1. Download the recovery partition image ( registered customers only) .
2. Apply the recovery partition image upgrade via the CLI:

```
sensor#configure terminal
sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/IDS-4215-K9-r-1.1-a-4.1-
```

3. Once the recovery partition image is applied, the 4215 is restored to a normal running 4.1(1) 4215 base.

```
sensor(config)#recover application-partition
```

**Q. IDS-4215 receives the `idsPackageMgr: invalid argument error` message while it attempts to upgrade the IDS recovery partition. What do I need to do to resolve this issue?**

A. This is a manufacturing issue. Some customers received IDS-4215s with a bad base image (4.0). Complete these steps.

1. Download the recovery partition image ( registered customers only) .
2. Apply the recovery partition image upgrade via the CLI:

```
sensor#configure terminal
sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/IDS-4215-K9-r-1.1-a-4.1-
```

3. Once the recovery partition image is applied, the 4215 is restored to a normal running 4.1(1) 4215 base.

```
sensor(config)#recover application-partition
```

**Q. When I upgrade from a 2-digit to 3-digit sig level packages, such as S100 or later (for example, 4.1(4)S99 to 4.1(4)S100), the auto-update functionality fails. How do I fix this?**

**Note:** Cisco VMS and CLI customers do not experience this issue.

The cause of the problem is the sorting logic that is used when the filename is parsed. It is an alphanumeric sort when it should be numeric. The workaround is to use CLI (or VMS) to upgrade to 3-digit sig level packages, such as S100 or later. Once this is completed, the auto-update begins to function again. Refer to Cisco bug ID CSCef07999 ( registered customers only) for additional information.

## IPS 5.0 and Later

**Q. If I use SSH or IDM to Login IPS, is it possible to configure the IPS 4240 to validate administrative users against a RADIUS server?**

A. No, RADIUS is not supported for sensor login authentication.

**Q. Can IPS/IDS send email alerts to users?**

A. No, it is not supported.

**Q. I have shunning configured but I am confused about how to configure blocking on the signatures. What is the difference between block host and block connection?**

A. *Block host* blocks all packets from that source address. *Block connection* only blocks the one connection based on source and destination IP/port. The PIX works in a slightly different

manner. For automatic shuns, the Sensor sends the source IP, destination IP, source port, and destination port. The PIX blocks all packets that originate from that IP address. The additional information is used by the PIX to remove that one connection from its connection tables. If the connection has not been removed from the connection table, it is theoretically possible that, if the shun is removed shortly after it is applied, the original connection might not have timed out yet. This allows the attacker to continue the attack on the original connection. The removal of the connection from the table ensures that the original connection cannot be used to continue the attack after the shun is removed. The Sensor cannot shun a single connection on the PIX because the PIX does not support the use of the **shun** command to shun a single connection. The PIX **shun** command always shuns the source address regardless of whether or not the additional connection information is provided.

**Q. What does the error "Error: Could not restart the network services. Fatal Error has occurred. Node MUST be rebooted to enable alarming." mean?**

A. This error means that your default gateway is incorrect, or it is a generic error message that means that the IP, netmask, or default gateway is incorrect. The **Fatal** part of the message means that, after the first failure, the previous configuration was applied and also failed. The Sensor issues **ifconfig** and **route** commands and one or both of them fails.

**Q. Does the IDS or Intrusion Prevention System (IPS) sensor maintain a password history?**

A. No, the sensor does not maintain a password history. Passwords are not viewable at any time.

**Q. How do I write a signature to detect foto[a-z]\.zip file in any inbound or outbound email?**

A. Use the **STRING.TCP** in order to write a signature that detects the attachment. Look for something similar to this:

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["] [Ff][Oo]
               [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

**Q. How do you configure the FTP client timeout?**

A. Issue these commands:

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

## Q. How do you convert the Start time and End time in the iplog-status to a readable format?

A. This output is a decimal representation of the current time since UNIX epoch. Use a UNIX epoch calculator such as the one located at the UNIX Date/Time Calculator site. Enter the first 10 digits because this calculator is granular to only seconds, and the IDS stores nanoseconds. This means the last 9 digits are stripped off. From the Start time in this output, 1084798479 = Mon May 17 12:54:39 2004 (GMT) is what you receive.

From the CLI, enter **iplog-status** in order to receive this output:

```
"
Log ID:                138343946
IP Address:            xxx.xxx.xxx.xxx
Group:                 0
Status:                completed
Start Time:         1084798479512524000
End Time:          1084798510136582000
Bytes Captured:        2833
Packets Captured:     14
"
```

## Q. You receive this error message: Error: Cannot communicate with mainApp (getVersion). Please contact your system administrator. How is this resolved?

A. The resolution for this issue is to reboot the sensor.

## Q. Are there any issues when IOS Intrusion Prevention System (IPS) and NM-CIDS monitoring are used together?

A. This is not allowed. On a router, either NM-CIDS or IOS-based IPS monitoring needs to be configured. Their use on the same router is mutually exclusive.

## Q. You might receive these error messages:

- `errorMessage: IpLogProcessor::addIpLog: Ran out of file descriptors name=errWarn`
- `errorMessage: IpLog 1701858066 terminated early due to lack of file handles. name=ErrLimitExceeded`

How is this resolved?

A. These messages are indicative of IP LOGGING being enabled, which in turn hogged up all the system resources. Cisco recommends to disable IP LOGGING as it should only be used for troubleshooting or investigative purposes.

## Q. I receive this error when logging into CLI and trying to upgrade IPS sensors: Error: execUpgradeSoftware : This update may only be installed on a sensor with and engine version of 2" This is the engine 2 update. How is this resolved?

A. This usually means that the file used for upgrade does not have the same engine version as the image currently on the sensor.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

---

## Related Information

- [Cisco Secure Intrusion Prevention System Support Page](#)
- [Documentation for Cisco Secure Intrusion Detection System](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

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

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Apr 10, 2008

Document ID: 50360

---