IDS 4.0/AIP−SSM/IPS 5.0 and Later FAQ

Document ID: 50360

Contents

Introduction

This document answers the most Frequently Asked Questions (FAQs) related to Cisco Secure Intrusion Detection System (IDS) 4.0, Advanced Inspection and Prevention Security Services Module (AIP SSM), and 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 through the CLI:

```
sensor#configure terminal
sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/
    IDS−4215−K9−r−1.1−a−4.1−1−S47.tar.pkg
```

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 more information.

Q. What does the "Authentication token manipulation error". error message mean?

A. In order to solve this issue, use default password (cisco) two times and then change the password from the config mode. The IDS requires the default password to be entered twice.

For example:

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re−enter new password: ***
```

Q. How do I remove the IDSM from Switch?

A. The module should be removed only after you disable the power. Complete these steps:

1. From the sensor CLI, issue the **reset powerdown** command.
2. Once the sensor completes shutdown, from the switch CLI, issue either the **no power enable module (module_number)** command for Cisco IOS or the **set module power down (module_number)** command for CatOS.
3. Press the shutdown button on the blade.
4. Physically power down the chassis. When the status light displays a longer green, you can remove the module safely.

IPS 5.0 and Later

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, then it is theoretically possible that if the shun is removed shortly after it is applied, then 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 in order 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: Could not restart the network services. Fatal Error has occurred. Node MUST be rebooted to enable alarming". error message mean?

A. This error means that your default gateway is incorrect or a generic error message that means that either the IP, netmask, or default gateway are 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. Autoupdate fails with the "mainApp[343] Cid/E errSystemError http error response:500". error message. What does this error message mean?

A. This issue might be the auto update feature, which does not work, because it is set to download at an even hour. Try to set the auto update to a random time; even a small offset of eight or night minutes can fix this problem.

In general, the issue is resolved and the `Error: http error response: 500` error message is be seen if you change the retrieval time to a non−hourly boundary.

Note: IPS fails the auto−update of signatures and returns with this error message:

```
AutoUpdate exception: HTTP connection failed [1,110]
name=errSystemError
```

Verify these items in order to resolve this issue:

- Verify if a firewall is preventing the sensor from reaching Cisco.com.
- Verify if routing becomes an issue.
- Verify if NATing is properly configured on the gateway device for the downstream device.
- Verify if the user credentials are correct.
- Change the update start time to odd hours.

Q. What does the "Error: execUpgradeSoftware : AnalysisEngine is currently busy and unable to process this update. Please wait several minutes before attempting update again.". error message mean?

A. In order to resolve this issue, try to reload the sensor or reimage the sensor.

Q. How do I resolve the error message Cid/W Warning − DNS or HTTP proxy is required for global correlation inspection and reputation filtering but no DNS or proxy servers are

defined.Add an HTTP proxy server or DNS server in the 'host' service configuration?

A. Complete these tasks in order to resolve this issue:

- Disable global correlation.
- Add the proxy/dns configuration.

Q. How do I resolve these errors that IPS receives for global correlation health problems: "23Jan2010 15:50:39.831 38.001 collaborationApp[655] rep/E A global correlation update failed: Failed to open a TLS connection to HTTP server at X.X.82.127:443 : TLS connection failed" and "collaborationApp[459] rep/E A global correlation update failed: Failed download of ibrs/1.1/drop/default/1296529950 : URI does not contain a valid ip address"?

A. IPS is unable to get to internet because of a port issue, for example, a firewall in a path that does not have the right ports open for the Internet access or it can be a NAT issue.

For global correlation to function completely, the sensor first contacts through https **update−manifests.ironport.com** in order to authenticate the user and then an HTTP connection to download GC updates. The files that the sensor downloads from the HTTP (updates.ironport.com) are the reputation data that global correlation uses. The https update−manifests.ironport.com should always resolve to the X.X.82.127 address, but the http **updates.ironport.com** IP address can change, which depends on the Internet you access. So you must check the IP address. If URL filtering is enabled, add an exception for the IPS management interface IP in the URL filter, so that IPS can connect to the Internet.

This error occurs when there is corruption in a previous GC update:

```
collaborationApp[459] rep/E A global correlation update
failed: Failed download of ibrs/1.1/drop/default/1296529950 :
URI does not contain a valid ip address
```

This issue can usually be corrected by turning off the GC service and then turning it back on. In IDM, choose **Configuration** > **Policies** > **Global Correlation** > **Inspection/Reputation**, set Global Correlation Inspection (and **Reputation Filtering** if **On**) to **Off**, apply the changes, wait for 10 minutes, turn the features on, and monitor.

Q. The A global correlation update failed: openConnection: Caught IpAddrException badAddrString. Unable to use the Global Correlation HTTP proxy and DNS settings. Verify connection and try again. error message is received in the "Reputation update failure" category. How do I resolve this issue?

A. Verify these items:

- You must have a valid IPS license in order to allow global correlation features to function.
- You must have an HTTP proxy server or a DNS server configured in order to allow global correlation features to function.
- Because global correlation updates occur through the sensor management interface, firewalls must allow tcp 443/80 and udp 53 traffic.
- Make sure your sensor supports the global correlation features. If you do not want this, disable the global collaboration feature from IDM:

    - Go to **Configuration** > **Policies** > **Global Correlation** > **Inspection/Reputation**, and set Global Correlation Inspection (and Reputation Filtering if **On**) to **Off**.

Q. How do I resolve the "A global correlation update failed: openConnection: Caught IpAddrException badAddrString" error that IPS receives for global correlation health problem?

A. If you use global correlation (GC) then make sure that name resolution works, for example, DNS is reachable. Also check if there is a firewall blocked port 53. Otherwise, you can turn off the GC feature if you wish to get rid of this message.

Q. How do I resolve the Exception when initializing the connection to MySQL error message that I receive when I launch IME from the browser?

A. This issue usually occurs when customer attempt to run IME on unsupported operating systems, such as Windows 7.

Q. How do I resolve the " Title: IDM on 88-nsmc-c1 Vendor: Cisco Systems, Inc. Category: Launch File Error JAR resources in JNLP file are not signed by same certificate". or "Error connecting to sensor, Failed to create sensor x.x.x.x:443 exiting idm" error that IDM receives, which happens during the launch of the application?

A. Clear the browser cache in order to resolve this issue.

Q. Is the Asymmetric mode on IPS configurable if you use GUI?

A. In version 6.0, Asymmetric mode on IPS that is configurable using CLI only and not available on GUI. But, in version 6.1 this feature is also available in GUI.

Q. How do I resolve the latency issue with the IPS sensor?

A. In order to resolve this issue, enable the asymmetric mode processing in order to allow the sensor to synchronize state with the flow and maintain inspection for those engines that do not require both directions. Use this configuration:

```
IPS_Sensor#configure terminal
IPS_Sensor(config)#service analysis-engine
IPS_Sensor(config-ana)#virtual-sensor vs0
```

```
IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

The latency issue occurs when the deny action inline and deny packet are enabled for every signature in VS0. Enabling all the signatures will result in latency as IPS inspects every single packet passing through. It is good to enable only the specific signature required as per the network traffic flow in order to resolve the latency issue.

Q. Does AIP−SSM help block Skype?

A. The PIX/ASA is not able to block the skype traffic. Skype has the capacity to negotiate dynamic ports, and to use encrypted traffic. With encrypted traffic, it is virtually impossible to detect it as there are no patterns to look for.

You could eventually use a Cisco IPS (Intrusion Prevention System)/AIP−SSM. It has some signatures that are able to detect a Windows Skype Client that connects to the Skype server to synchronize its version. This is usually done when the client is initiated the connection. When the sensor picks up the initial Skype connection, you can be able to find the person who use the service, and block all connections initiated from their IP address.

Q. Why does the sensing interface `flap` or frequently go to the down state in IPS?

A. During a signature update and reconfigurations, sensorApp stops to process packets as it processes the new signatures in the update. The network driver detects that sensorApp has stopped and pulls any new packets from the buffer. So the network driver does different things, which depends on the configuration and sensor model:

Promiscuous Interface It brings the link down on the interfaces, and brings the link back up once sensorApp starts to monitor again.

Inline Interface or Inline Vlan Pair It depends on the Bypass setting:

- **Bypass Auto** The driver keeps the link up and begins to pass packets through without analysis. It then reverts back to sending the packets through sensorApp once sensorApp starts to monitor again.
- **Bypass Off** The driver brings the link down on the interfaces, which is the same as in promiscuous mode, and brings them back up once sensorApp starts to monitor again.

So, if sensor app does not pull packets from the buffer, which possibly occurs because there is no interface configured to process packets, then the driver can put the interface in a `down` state.

These logs are seen when the sensing interface flaps:

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

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. Does the IDS or Intrusion Prevention System (IPS) sensor support syslog server to send logs?

A. No.

Q. What is the maximum limit of storing events in IPS?

A. The local event of the sensor stores only 30 MB and begins to overwrite itself once the 30 MB limit is reached. This limit is non−configurable.

Q. How do I write a signature to detect foto[a−z]\.zip file in any incoming or outgoing 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 epoc. Use a UNIX epoc 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 nine 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. The "IOException when try to get certificate: java.security.cert.CertificateExpiredException". error message appears. How this can be resolved?

A. In order to solve this error message, login into the AIP−SSM and issue the **tls generate−key** command in privileged EXEC mode as shown in this example:

```
sensor#tls generate-key
```

Note: This resolution of using the command **tls generate−key** also resolves the issue of AIP−SSM not being able to connect to the IME.

Q. The "IOException: Connection refused:connect. IME IME server is not responding. Please check if it is running" error message appears while I add IPS in IME. How can this issue be resolved?

A. In order to solve this error message, choose **Control Panel** > **Admin Tools** > **Services** and restart IME services.

Q. The Could not verify config username/password[IOEXception − connect timed out] error message is received when I add an IPS sensor to the IME. How can this issue be resolved?

A. This indicates broken communication between the IME and the IPS sensor. Make sure that there is no software that blocks the SDEE.

Q. The "Error response from IME server: Unknown error (check log file in installation's log directory)" . error message appears. How can this issue be resolved?

A. In order to solve this error message, verify that correct IP address is used when you add IPS in IME and also check any software firewall that is running on IME computer, which can block the connection.

Q. Can the IDS or Intrusion Prevention System (IPS) sensor send email alerts?

A. The IDS sensor does not have the ability to send email alerts on its own. Security Monitor when used with IDS has the ability to send email notifications when an Event Rule is triggered by the sensor.

Refer to Configure E−mail Notifications for more information on how to configure email notifications with Security Monitor.

Cisco IPS Manager Express (IME) can be configured to send the email notification message (alerts) when Event Rules are triggered by Cisco IPS Sensors. Refer to IPS 6.X and later: Email Notifications using IME Configuration Example for more information.

Q. The `Error: Cannot communicate with mainApp (getVersion). Please contact your system administrator.` error message appears when I try to connect to my sensor. How can this issue be resolved?

A. Reboot the sensor in order to resolve this issue.

Q. The `Warning: WARNING: Insufficient resources available to combine all currently active custom regexes. Some alerts will not fire. Consider retiring signatures until this message no longer occurs.` error message appears signature tuning on my sensor. How can this issue be resolved?

A. Retire the signatures that are not in use in order to resolve this issue and also the number of customer signatures with regexes should be reduced. Also, it is not recommended to use ***** and + metacharacters in regexes.

Q. Why do latency issues occur on Cisco Intrusion Prevention System (IPS) sensors? How can this issue be resolved?

A. The latency issue can occur due to the assymetric routing. Try to disable the signature 1330 in order to resolve this issue.

Q. Is it possible to disable SSHv1 and leave only the SSHv2 enabled on the Cisco Intrusion Prevention System (IPS) sensors?

A. Right now it is not possible to disable SSHv1 and leave only SSHv2 enabled. Both SSHv1 and SSHv2 are enabled together and cannot be disabled individually.

Q. The `error: An error occurred at the sensor during the update, sensor message = The update requires 115000 KB in /usr/cids/idsRoot/var, there are only 110443 KB available.` message appears when I upgrade the sensor to version 4.1(5). How can this issue be resolved?

A. This error message occurs due to insufficient memory in the sensor.

Complete these tasks in order to resolve this issue:

1. Log into service account and become root
2. Remove the following directories as shown below:

```
# rm −rf /usr/cids/idsRoot/var/updates/files/S69
# rm −rf /usr/cids/idsRoot/var/updates/files/common
# rm /usr/cids/idsRoot/var/virtualSensor/*
# rm /usr/cids/idsRoot/var/.tmp/*
```

3. Now try to upgrade the sensor. Refer to Cisco bug ID CSCsb81288 (registered customers only) for more information.

Q. I get the `mainApp[396] cplane/E Error − accept() call returned −1` error message in the log on ASA. How can this error be resolved?

A. The `mainApp[396] cplane/E Error − accept() call returned −1` error message indicates that Web server cannot read the file, and accept() program failed, which yields file descriptors when TLS connections exist. But this file is not needed for normal behavior. It is harmless.

Q. How do I resolve the `tls/W errTransport WebSession::sessionTask TLS connection exception: handshake incomplete` error message?

A. This error message indicates that the certificate is no longer valid on the module. Complete these steps in order to resolve the issue:

1. Regenerate the certificate from the CLI:
    a. Log in to the sensor command line.
    b. Issue the **tls generate** command, and press **enter**. Note the fingerprints that are displayed.
2. Pull the new certificate in to IME:
    a. Open the IME and locate the sensor name in the list on the Home page.
    b. Right−click the sensor, and click **Edit**.
    c. When you reach the Edit Device screen, click **OK**. Bypass any warning about not being able to retrieve the sensor time.
    d. You will be prompted with the new security certificate (the one that you just generated). Check to make sure the fingerprints match, and click **Yes**.
    e. After several seconds, the sensor should show "Connected" in the Event Status again.

Q. When I attempt to log in to IPS, I receive this error message: `errSystemError−ct−sensorAPP.450 not responding, clientpipe failed`. How can I resolve this error?

A. In order to resolve this error, use the **reset** command in order to reboot the IPS.

Q. The time on AIP−SSM differs from the time on the Cisco Adaptive Security Appliance (ASA). How can this issue be resolved?

A. In order to resolve this issue, use the NTP server to synchronize the time on the Cisco Adaptive Security Appliance(ASA) and AIP−SSM.

Refer to Configuring NTP on IPS sensors for more information.

Q. How can I apply multiple virtual sensors on AIP−SSM?

A. Virtual sensors on AIP−SSM cannot be applied per interface because the AIP−SSM has only one interface. When you create multiple virtual sensors, you must assign this interface to only one virtual sensor. You do not need to designate an interface for the other virtual sensors.

After you create virtual sensors, you must map them to a security context on the Adaptive Security Appliance (ASA) using the **allocate−ips** command. You can map many security contexts to many virtual sensors. Refer to the *Assigning Virtual Sensors to Adaptive Security Appliance Contexts* section of Configuring AIP−SSM for more information.

Q. What is the maximum number of virtual sensors supported by AIP−SSM?

A. A maximum number of four virtual sensors can be supported.

Q. If I use SSH or IDM in order to login to IPS then is it possible to configure the IPS 4240/IDSM/IDSM2 in order to validate administrative users against a RADIUS/TACACS+ server?

A. It is not possible with a TACACS+ server but RADIUS is supported from the IPS 7.0.(4)E4 release. Refer to the *New and Changed Information* and *Restrictions and Limitations* sections of the Release Notes for Cisco Intrusion Prevention System 7.0(4)E4 for more information. Also, refer to IPS 7.X: User Login Authentication using ACS 5.X as Radius Server Configuration Example for a sample configuration.

Q. What is the impact of expired license on IPS funcationality?

A. The only impact an expired license has on the sensor is that it halts the signature updates.

Q. Do the IPS signature updates have an impact on the services or network connectivity?

A. No. The IPS signature updates do not have an impact on the services or the network connectivity.

Q. What is the exact URL I need to enter for the IPS module to update automatically with the latest signatures?

A. The link required to allow the IPS module to update automatically with the latest signature is: https://198.133.219.25/cgi−bin/front.x/ida/locator/locator.pl.

You must use your Cisco user ID and password to complete the update of the IPS module.

Note: In the 6.x train of code, automatic updates from Cisco.com are not supported. You must manually download the signature files and apply them to the sensor. There is an auto−update function in the 6.x code; however, this is possible only from a local file server in which the signature files must be manually downloaded as well.

Q. Does the IPS sensor vulnerable to the X11 port forwarding session hijack vulnerability ?

A. No. It is not vulnerable for these reasons:

- The sensor does not have X11 libraries. Therefore there are no sessions to hijack.
- X11 port forwarding is not enabled in the SSH configuration.
- IPv6 is not compiled into the sensor kernel. This is required in order to exploit the vulnerability.

Q. Why does the AIP−SSM not show any logs when the ASA shows plenty of warning and attack logs?

A. This happens because when the ASA blocks something, it is not passed to the IPS for duplicate inspection. Therefore, you cannot see duplicate logs on the ASA and IPS.

Q. After a user deploys the S518 signature set, the "invalidValue:Editng string−xl−tcp sig XXXX has NO effect in this version" error message occurs. Why?

A. This is the complete error message:

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=−240 timeZone=GMT−05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string−xl−tcp
sig 21619 has NO effect
```

This issue comes up because the string−xl−tcp or string−tcp−xl engine is not supported on the hardware. For more details, refer to the IPS Engine E4 Release Notes.

Q. When I automatically update signatures on an ASA−SSM−10 with the auto update feature, I receive this error message: No installable auto update package found on server status=true. How can I resolve this issue?

A. This output shows the complete error message:

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi−bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

This error has been generated and the signatures do not automatically update because the Signature definition updates after S479 require the E4 engine. In order to resolve this, you need to manually upgrade the Sensor to 7.0(2)E4.

Note: The Sensor is not able to automatically upgrade itself to E4 because it requires 7.0(2) and a reboot of the Sensor.

Q. The auto update feauture on the IPS 5.0 for NIDS module is not working. How can I resolve this issue?

A. This output shows the complete error message:

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

This issue occurs because of an improper directory listing style with the FTP server. In order to resolve this, switch to UNIX−style directory listings from the existing MS−DOS style directory listings.

In order to modify the directory listing settings, select **Start** > **Program Files** > **Administrative Tools** in order to open the Internet Services Manager. Then go to the Home Directory tab and change the directory listing style from MS−DOS to UNIX.

Q. IPS−4255 receives the SensorApp fails in TcpRootNode::expireNow() error message during an upgrade. How do I resolve this issue?

A. This issue is due to the failure of the analysis engine and is addressed in Cisco bug ID CSCtb39179 (registered customers only) . Upgrade the sensor to version 7.0(4)E4 in order to fix this issue.

Q. When I attempt to perform a license update after I purchanse a new license the device reports this error: "Failed to update license on sensor." "errExpiredLicense−The new license expire date is older than current license expire date." How can I resolve this issue?

A. This issue occurs when the license file received is invalid. To obtain a valid license file, log in to Cisco.com as a registered user, and download the appropriate license file. Once you obtain the valid license file, install it on your sensor.

If you install the new license file and you still receive an error, there might be an issue with the existing invalid license file. In order to resolve this issue, complete these steps to delete the existing invalid license file:

1. Log in to the service account by typing your service account user name.

   If you do not have a service account, open the IPS command line, enter configuration mode, and enter this command

   username *name* **privilege service password** *password*

```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```

2. Once you log in to your service account, enter the **su** command in order to go to root (using the same password as the service account).
3. Delete the files in the /usr/cids/idsRoot/shared/ directory.

   Note: Do not delete the host.conf file.

   a. Enter the **cd /usr/cids/idsRoot/shared/** command in order to go to the shared directory.
   b. Enter the **ls** command in order to view the files in the directory.
   c. Enter the **rm** *file_name* command in order to remove the files.

      Note: Do not delete the host.conf file.
4. Enter the **/etc/init.d/cids restart** command to restart the sensor.
5. Install the new license.

A Cisco bug has been filed to address this behaviour. For more information, refer to CSCtg76339 (registered customers only) .

Q. What does the `errorMessage: IpLog 1712041197 terminated early due to lack of file handles. name=ErrLimitExceeded` error message mean? How do I resolve this issue?

A. This error is caused by an excessive amount of packets on IP logging. Disable the IP logging feature in order to resolve this issue. IP logging is meant for troubleshooting only; Cisco recommends that you do not enable it for all the signatures.

Q. I recieve this error when I update the sensor from s550 to s551: `Cannot parse the current config for the component "signatureDefinition" and the instance "sig0".` How can I resolve this issue?

A. Modification of signature 23899.0 causes this issue. Refer to Cisco bug ID CSCtn84552 (registered customers only) for more information.

Q. I recieve this error on the sensor: `Error: autoUpdate successfully selected a package from the cisco.com locator service, however, package download failed: Failed to receive the HTTP response.` How can I resolve this issue?

A. Check if there is URL filtering, content filtering, or a proxy server present that is blocking the autoUpdate from happening. Make sure that autoUpdate is not being blocked and also verify that the user credentials provided are correct.

Q. I receive this XML error message on the IPS sensor that runs with version 6.2(3)E4: `errorMessage: IPS software attempted to write invalid XML data for (token). Invalid XML character(s) were replaced with '*'`. How can I resolve this issue?

A. This behavior has been addressed by Cisco bug ID CSCsq50873 (registered customers only) . This is a cosmetic issue and does not create any operational overhead except the excessive amount of logs being received. A temporary workaround is to remove the NTP related configuration on the sensor. For a permanent solution, upgrade to a version in which this bug is fixed.

Q. Why does the IME workstation make constant connections to managed servers despite the client being closed?

A. IME functions as two Windows services and the GUI client. When the client is closed, the two Windows services (Cisco IPS Manager Express and MySQL−IME) continue to run and collect events from the managed sensors and store them in the local MySQL database; this allows for historical reporting to occur.

The IME client should open a single SDEE subscription to the managed sensor, and re−use this subscription for subsequent event retrieval activity. The constant connectivity from the IME workstation to the managed sensors is expected behavior.

Q. Can the AIP−SSM module be used as a SPAN target?

A. No. The AIP−SSM module cannot be used as a SPAN target as it is used only to monitor the traffic flowing through the ASA interface.

Q. Why is high CPU usage observed after the IPS is upgraded to the E3 engine?

A. With E3 engine updates, the IPS uses a different algorithm for managing its idle time and spends more time polling for packets to reduce latency. This increased checking causes a corresponding increase in the CPU usage. The correct way to measure the CPU in E3 is not by CPU usage, but by the **Packet load percentage** which shows the correct CPU utilization.

Q. Why is the health status LED turning RED intermittently on my IPS appliance?

A. This could happen because of an incorrect certificate on the remote maanagement station, running software such as CS−MARS, CSM, IEV, VMS−IDS/IPSMC, etc. In order to resolve this issue, complete these steps:

1. Apply the sensor's TLS certificate on the remote management station.
2. Configure a valid DNS server.

Q. How can the IPS be stopped from delaying the HTTP's traffic while traversing its interfaces?

A. Configuring the sensor to work in asymmetric mode will resolve the issue. In order to put the sensor in asymmetric mode protection, complete these steps:

1. Go to **Configuration** > **Policies** > **IPS policies**.
2. Double−click **virtual sensor**.
3. Go to **advance options**.
4. Under normalize mode, select **Asymmetric mode protection**.
5. Click **OK**.
6. Reboot the unit in order for the changes to take effect.

Related Information

- **Cisco Secure Intrusion Prevention System Support Page**
- **Troubleshoot AIP−SSM**
- **Security Product Field Notices (including CiscoSecure Intrusion Detection)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Apr 10, 2008 Document ID: 50360