



# CHAPTER 1

## Getting Started

---



**Note**

*Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1* also applies to the IPS section of ASDM. The path in ASDM has two additional initial jumps, Configuration > Features before you reach the IPS section, for example, Configuration > Features > IPS > Network.

---

This chapter describes IDM and provides information for getting started using IDM. It contains the following sections:

- [Advisory, page 1-1](#)
- [Introducing IDM, page 1-2](#)
- [System Requirements, page 1-2](#)
- [Increasing the Memory Size of the Java Plug-in, page 1-3](#)
- [Initializing the Sensor, page 1-4](#)
- [Logging In to IDM, page 1-13](#)
- [Licensing the Sensor, page 1-19](#)

## Advisory

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at the following website:  
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance, contact us by sending e-mail to [export@cisco.com](mailto:export@cisco.com).

# Introducing IDM

IDM is a web-based, Java application that enables you to configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through the Internet Explorer, Netscape, or Mozilla web browsers.

The IDM user interface consists of the File and Help menus, Configuration and Monitoring buttons whose menus open in the left-hand TOC pane, and the configuration pane on the right side of the page. The following four buttons appear next to the Configuration and Monitoring buttons:

- Back—Takes you to the pane you were previously on.
- Forward—Takes you forward to the next pane you have been on.
- Refresh—Loads the current configuration from the sensor.
- Help—Opens the online help in a new window.

To configure the sensor, choose **Configuration** and go through the menus in the left-hand pane. Choose **Monitoring** and go through the menus in the left-hand pane to configure monitoring.

New configurations do not take effect until you click **Apply** on the pane you are configuring. Click **Reset** to discard current changes and return settings to their previous state for that pane.

## System Requirements

The following lists the system requirements for IDM:

- Windows 2000, Windows XP
  - Internet Explorer 6.0 with Java Plug-in 1.4.2 or 1.5 or Netscape 7.1 with Java Plug-in 1.4.2 or 1.5
  - Pentium III or equivalent running at 450 Mhz or higher
  - 256 MB minimum, 512 MB or more strongly recommended
  - 1024 x 768 resolution and 256 colors (minimum)
- Sun SPARC Solaris
  - Sun Solaris 2.8 or 2.9
  - Mozilla 1.7
  - 256 MB minimum, 512 MB or more strongly recommended
  - 1024 x 768 resolution and 256 colors (minimum)
- Linux
  - Red Hat Linux 9.0 or Red Hat Enterprise Linux WS, Version 3 running GNOME or KDE
  - Mozilla 1.7
  - 256 MB minimum, 512 MB or more strongly recommended
  - 1024 x 768 resolution and 256 colors (minimum)

**Note**

---

Although other web browsers may work with IDM, we only support the listed browsers.

---

# Increasing the Memory Size of the Java Plug-in

To correctly run IDM, your browser must have Java Plug-in 1.4.2 or 1.5 installed. By default the Java Plug-in allocates 64 MB of memory to IDM. IDM can run out of memory while in use, which can cause IDM to freeze or display blank screens. Running out of memory can also occur when you click **Refresh**. An `OutOfMemoryError` message appears in the Java console whenever this occurs. You must change the memory settings of Java Plug-in before using IDM. The mandatory minimum memory size is 256 MB.

**Note**

We recommend that you use Sun Microsystems Java. Using any other version of Java could cause problems with IDM.

This section contains the following topics:

- [Java Plug-In on Windows, page 1-3](#)
- [Java Plug-In on Linux and Solaris, page 1-4](#)

## Java Plug-In on Windows

To change the settings of Java Plug-in on Windows for Java Plug-in 1.4.2 and 1.5, follow these steps:

- 
- Step 1** Close all instances of Internet Explorer or Netscape.
- Step 2** Choose **Start > Settings > Control Panel**.
- Step 3** If you have Java Plug-in 1.4.2 installed:
- Click Java Plug-in.  
The Java Plug-in Control Panel appears.
  - Click the **Advanced** tab.
  - Enter `-xms256m` in the Java RunTime Parameters field.
  - Click **Apply** and exit the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
- Click Java.  
The Java Control Panel appears.
  - Click the **Java** tab.
  - Click **View** under Java Applet Runtime Settings.  
The Java Runtime Settings Panel appears.
  - Enter `-xms256m` in the Java Runtime Parameters field and then click **OK**.
  - Click **OK** and exit the Java Control Panel.
-

## Java Plug-In on Linux and Solaris

To change the settings of Java Plug-in 1.4.2 or 1.5 on Linux and Solaris, follow these steps:

- Step 1** Close all instances of Netscape or Mozilla.
- Step 2** Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.



**Note** In the Java 2 SDK, this file is located at <SDK installation directory>/jre/bin/ControlPanel. For example if your Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel.



**Note** In a Java 2 Runtime Environment installation, the file is located at <JRE installation directory>/bin/ControlPanel.

- Step 3** If you have Java Plug-in 1.4.2 installed:
  - a. Click the **Advanced** tab.
  - b. Enter **-xms256m** in the Java RunTime Parameters field.
  - c. Click **Apply** and close the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
  - a. Click the **Java** tab.
  - b. Click **View** under Java Applet Runtime Settings.
  - c. Enter **-xms256m** in the Java Runtime Parameters field and then click **OK**.
  - d. Click **OK** and exit the Java Control Panel.

## Initializing the Sensor

This section explains how to initialize the sensor, and contains the following topics:

- [Overview, page 1-4](#)
- [Initializing the Sensor, page 1-5](#)
- [Verifying Initialization, page 1-10](#)

### Overview

After you have installed the sensor on your network, you must use the **setup** command to initialize it. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, time settings, and assign and enable interfaces. After you have initialized the sensor, you can communicate with it over the network. You are then ready to configure intrusion prevention.

## Initializing the Sensor

To initialize the sensor, follow these steps:

**Step 1** Log in to the sensor using an account with administrator privileges:

- Log in to the appliance by using a serial connection or with a monitor and keyboard.



**Note** You cannot use a monitor and keyboard with IDS-4215, IPS-4240, or IPS-4255.

- Session to IDSM-2:

- For Catalyst software:

```
console> enable
console> (enable) session module_number
```

- For Cisco IOS software:

```
Router# session slot slot_number processor 1
```

- Session to NM-CIDS:

```
router# service-module IDS-Sensor slot_number/port_number session
```

- Session to AIP-SSM:

```
asa# session 1
```



**Note** The default username and password are both **cisco**.

**Step 2** The first time you log in to the sensor you are prompted to change the default password.

Passwords must be at least eight characters long and be strong, that is, not be a dictionary word.



**Caution**

If you forget your password, you may have to reimage your sensor unless there is another user with Administrator privileges (see [Chapter 13, “Upgrading, Downgrading, and Installing System Images”](#)). The other Administrator can log in and assign a new password to the user who forgot the password. Or, if you have created the service account for support purposes, you can have TAC create a password. For more information, refer to [Creating the Service Account](#).

After you change the password, the `sensor#` prompt appears.

**Step 3** Enter the `setup` command.

The System Configuration Dialog is displayed.



**Note** The System Configuration Dialog is an interactive dialog. The default settings are displayed.

--- System Configuration Dialog ---

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

Current Configuration:

```

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
    
```

Current time: Wed May 5 10:25:35 2004

**Step 4** Press the spacebar to get to the following question:

Continue with configuration dialog?[yes]:

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

**Step 5** Enter **yes** to continue.

**Step 6** Specify the hostname.

The hostname is a case-sensitive character string up to 64 characters. Numbers, “\_” and “-” are valid, but spaces are not acceptable. The default is sensor.

**Step 7** Specify the IP interface.

The IP interface is in the form of IP Address/Netmask, Gateway: X.X.X.X/nn,Y.Y.Y.Y, where X.X.X.X specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods where X = 0-255, nn specifies the number of bits in the netmask, and Y.Y.Y.Y specifies the default gateway as a 32-bit address written as 4 octets separated by periods where Y = 0-255.

**Step 8** Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

**Step 9** Specify the web server port.

The web server port is the TCP port used by the web server (1 to 65535). The default is 443.



**Note** If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://sensor_ip_address:port` (for example, `https://10.1.9.201:1040`).



**Note** The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

**Step 10** Enter **yes** to modify the network access list.

- a. If you want to delete an entry, enter the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.
- b. Enter the IP address and netmask of the network you want to add to the access list.

The IP network interface is in the form of IP Address/Netmask: X.X.X.X/nn, where X.X.X.X specifies the network IP address as a 32-bit address written as 4 octets separated by periods where X = 0-255, nn specifies the number of bits in the netmask for that network.

For example, 10.0.0.0/8 permits all IP addresses on the 10.0.0.0 network (10.0.0.0-10.255.255.255) and 10.1.1.0/24 permits only the IP addresses on the 10.1.1.0 subnet (10.1.1.0-10.1.1.255).

If you want to permit access to a single IP address than the entire network, use a 32-bit netmask. For example, 10.1.1.1/32 permits just the 10.1.1.1 address.

- c. Repeat Step b until you have added all networks that you want to add to the access list.
- d. Press **Enter** at a blank permit line to proceed to the next step.

**Step 11** Enter **yes** to modify the system clock settings.

- a. Enter **yes** if you want to use NTP.

You will need the NTP server IP address, the NTP key ID, and the NTP key value. If you do not have those at this time, you can configure NTP later. For the procedure, refer to [Configuring the Sensor to Use an NTP Server as its Time Source](#).

- b. Enter **yes** to modify summertime settings.



**Note** Summertime is also known as DST. If your location does not use Summertime, go to Step n.

- c. Choose recurring, date, or disable to specify how you want to configure summertime settings.  
The default is recurring.
- d. If you chose recurring, specify the month you want to start summertime settings.  
Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december.  
The default is april.
- e. Specify the week you want to start summertime settings.  
Valid entries are first, second, third, fourth, fifth, and last.  
The default is first.
- f. Specify the day you want to start summertime settings.  
Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday.

The default is sunday.

- g. Specify the time you want to start summertime settings.

The default is 02:00:00.




---

**Note** The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2 a.m. on the first Sunday in April, and a stop time of 2 a.m. on the fourth Sunday in October. The default summertime offset is 60 minutes.

---

- h. Specify the month you want summertime settings to end.

Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december.

The default is october.

- i. Specify the week you want the summertime settings to end.

Valid entries are first, second, third, fourth, fifth, and last.

The default is last.

- j. Specify the day you want the summertime settings to end.

Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday.

The default is sunday.

- k. Specify the time you want summertime settings to end.

- l. Specify the DST zone.

The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+;\_/-]+\$.

- m. Specify the summertime offset.

Specify the summertime offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian).

The default is 0.

- n. Enter **yes** to modify the system time zone.

- o. Specify the standard time zone name.

The zone name is a character string up to 24 characters long.

- p. Specify the standard time offset.

The default is 0.

Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian).

- Step 12** Enter **yes** to modify the virtual sensor configuration (vs0).

The current interface configuration appears:

```
Current interface configuration
Command control: GigabitEthernet0/1
Unused:
  GigabitEthernet2/1
  GigabitEthernet2/0
Promiscuous:
  GigabitEthernet0/0
Inline:
  None
```



```
Inline VLAN Pair:
None
```

- Step 13** Enter **yes** to add a promiscuous or monitoring interface.
- Step 14** Enter the interface you want to add, for example, **GigabitEthernet0/1**.
- Step 15** Enter **yes** to add inline interface pairs (appears only if your platform supports inline interface pairs).
- Enter the inline interface pair name.
  - Enter the inline interface pair description.  
The default is `Created via setup by user <yourusername>`.
  - Enter the name of the first interface in the inline pair, **interface1**.
  - Enter the name of the second interface in the inline pair, **interface2**.
  - Repeat Steps a through d to add another inline interface pair, or press **Enter** for the next option.

- Step 16** Enter **yes** to add inline VLAN pairs (appears only if your platform supports inline VLAN pairs).  
A list of interfaces available for inline VLAN pairs appears:

```
Available Interfaces:
[1] GigabitEthernet0/0
[2] GigabitEthernet2/0
[3] GigabitEthernet2/1
```

- Step 17** Enter the number of the interface you want to subdivide into inline VLAN pairs.  
The current inline VLAN pair configuration for that interface appears:

```
Inline Vlan Pairs for GigabitEthernet0/0
None
```

- Enter the subinterface number to add.
  - Enter the inline VLAN pair description.
  - Enter the first VLAN number (vlan1).
  - Enter the second VLAN number (vlan2).
  - Repeat Steps a through d to add another inline VLAN pair on this interface or press **Enter** for the next option.
- Step 18** Enter **yes** to subdivide another interface. Enter **no** or press **Enter** to complete the addition of the inline VLAN pairs.

Your configuration appears with the following options:

```
[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.
```

- Step 19** Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

- Step 20** Enter **yes** to modify the system date and time.



**Note** This option is not available on modules or when NTP has been configured. The modules get their time from the router or switch in which they are installed, or from the configured NTP server.

- a. Enter the local date (yyyy-mm-dd).
- b. Enter the local time (hh:mm:ss).

**Step 21** Reboot the sensor:

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

**Step 22** Enter **yes** to continue the reboot.

**Step 23** Display the self-signed X.509 certificate (needed by TLS):

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

**Step 24** Write down the certificate fingerprints.

You need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

**Step 25** Apply the most recent service pack and signature update.

For information on how to obtain the most recent software, see [Obtaining Cisco IPS Software, page 12-1](#). The Readme explains how to apply the most recent software update.

You are now ready to configure your sensor for intrusion prevention.

## Verifying Initialization

To verify that you initialized your sensor, follow these steps:

**Step 1** Log in to the sensor.

For the procedure, refer to [Logging In to the Sensor](#).

**Step 2** View your configuration:

```
sensor# show configuration
generating current config:
! -----
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! -----
display-serial
! -----
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! -----
service authentication
```

```
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! -----
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit
exit
! -----
service logger
exit
! -----
service network-access
exit
! -----
service notification
exit
! -----
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
```

```

summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
exit
! -----
service ssh-known-hosts
exit
! -----
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SqGSib3DQEBBQUAMFcxCzAJBgNVBAYTA1VTMRwwGgYDVQQKEwNDaXNjbyBTeXN0ZW1zLCBjbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMDUwNjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQGEwJVUzEcMBoGAlUEChMTQ21zY28gU31zdGVtcywgSW5jLjESM
BAGA1UECzMJU1NNLU1QUzEwMRYwFAYDVQQDEw0xMC44OS4xNDkuMjI3MIGfMA0GCSqGSIb3DQEBAQUAA
4GNADCBiQKBgQCoOobDuZOEpuDw63R1t8K1YsymzR/D9R1cnad/U0gjAqGfcUh3sG3TXPQewon1fH0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANmf4zPcPCAORJ6DMQHFj44A+3tMZWsC
yaod23S1oY0xx7v5puPDYn3IQIDAQAABMA0GCSqGSIb3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVvHji12vBLo+biULJG95hbTF1qO+ba3R6nPD3tepgx5zTdOr2onn1FHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ11AQDiogskdCs4ax1tB4SbEU5y1tktKgcwWEdJpbbNJhzpoRsRICfm3H1OEwN
exit
! -----
service web-server
exit
sensor#

```

**Note**


---

You can also use the **more current-config** command to view your configuration.

---

**Step 3** Display the self-signed X.509 certificate (needed by TLS):

```

sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27

```

**Step 4** Write down the certificate fingerprints.

You need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

---

## Logging In to IDM

This section describes how to log in to IDM, and contains the following topics:

- [Overview, page 1-13](#)
- [Prerequisites, page 1-13](#)
- [Supported User Role, page 1-13](#)
- [Logging In to IDM, page 1-14](#)
- [IDM and Cookies, page 1-15](#)
- [IDM and Certificates, page 1-15](#)

### Overview

The number of concurrent CLI sessions is limited based on the platform. IDS-4210, IDS-4215, and NM-CIDS are limited to three concurrent CLI sessions. All other platforms allow ten concurrent sessions.

### Prerequisites

IDM is part of the version 5.1 sensor. You must use the **setup** command to initialize the sensor so that it can communicate with IDM. For the procedure, see [Initializing the Sensor, page 1-4](#).

### Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

## Logging In to IDM

To log in to IDM, follow these steps:

- Step 1** Open a web browser and enter the sensor IP address:

```
https://sensor_ip_address
```



**Note** IDM is already installed on the sensor.



**Note** `https://10.1.9.201` is the default address, which you change to reflect your network environment when you initialize the sensor. When you change the web server port, you must specify the port in the URL address of your browser when you connect to IDM in the format `https://sensor_ip_address:port` (for example, `https://10.1.9.201:1040`).

A Security Alert dialog box appears. For more information about security and IDM, see [IDM and Certificates, page 1-15](#).

- Step 2** Enter your username and password in the Enter Network Password dialog box and click **OK**.



**Note** The default username and password are both **cisco**. You were prompted to change the password during sensor initialization. For the procedure, see [Initializing the Sensor, page 1-4](#).

The Cisco IDM 5.1 Information window opens and informs you that it is loading IDM. IDM appears in another browser window.

The Memory Warning dialog box displays the following message:

```
Your current Java memory heap size is less than 256 MB. You must increase the Java memory heap size before launching IDM. Click Help for information on changing the Java memory heap size.
```

- Step 3** Click **Help** to see the procedure for changing the Java memory heap size.
- Step 4** Follow the directions for changing the Java memory heap size.
- Step 5** Close any browser windows you have open.
- Step 6** Relaunch IDM by opening a browser window and typing the sensor IP address.
- Step 7** Enter your username and password in the Password Needed - Networking dialog box and click **Yes**.

A Warning dialog box displays the following message:

```
There is no license key installed on the sensor. To install a new license, go to Configuration > Licensing.
```

For the procedure for licensing the sensor, see [Licensing the Sensor, page 1-19](#).

The Status dialog box displays the following message:

```
Please wait while the IDM is loading the current configuration from the Sensor.
```

The main window of IDM appears.

## IDM and Cookies

IDM uses cookies to track sessions, which provide a consistent view. IDM uses only session cookies (temporary), not stored cookies. Because the cookies are not stored locally, there is no conflict with your browser cookie policy. The cookies are handled by the IDM Java applet rather than the browser.

## IDM and Certificates

This section explains how certificates work with IDM, and contains the following topics:

- [Understanding Certificates, page 1-15](#)
- [Validating the CA for Internet Explorer, page 1-16](#)
- [Validating the CA for Netscape, page 1-17](#)
- [Validating the CA for Mozilla, page 1-18](#)

## Understanding Certificates

IPS 5.1 contains a web server that is running IDM and that the management stations, such as VMS, connect to. Blocking forwarding sensors also connect to the web server of the master blocking sensor. To provide security, this web server uses an encryption protocol known as TLS, which is closely related to SSL protocol. When you enter a URL into the web browser that starts with `https://ip_address`, the web browser responds by using either TLS or SSL protocol to negotiate an encrypted session with the host.



### Caution

The web browser initially rejects the certificate presented by IDM because it does not trust the CA.



### Note

IDM is enabled by default to use TLS and SSL. We highly recommend that you use TLS and SSL.

The process of negotiating an encrypted session in TLS is called “handshaking,” because it involves a number of coordinated exchanges between client and server. The server sends its certificate to the client. The client performs the following three-part test on this certificate:

1. Is the issuer identified in the certificate trusted?  
Every web browser ships with a list of trusted third-party CAs. If the issuer identified in the certificate is among the list of CAs trusted by your browser, the first test is passed.
2. Is the date within the range of dates during which the certificate is considered valid?  
Each certificate contains a Validity field, which is a pair of dates. If the date falls within this range of dates, the second test is passed.
3. Does the common name of the subject identified in the certificate match the URL hostname?  
The URL hostname is compared with the subject common name. If they match, the third test is passed.

When you direct your web browser to connect with IDM, the certificate that is returned fails because the sensor issues its own certificate (the sensor is its own CA) and the sensor is not already in the list of CAs trusted by your browser.

When you receive an error message from your browser, you have three options:

- Disconnect from the site immediately.
- Accept the certificate for the remainder of the web browsing session.
- Add the issuer identified in the certificate to the list of trusted CAs of the web browser and trust the certificate until it expires.

The most convenient option is to permanently trust the issuer. However, before you add the issuer, use out-of-band methods to examine the fingerprint of the certificate. This prevents you from being victimized by an attacker posing as a sensor. Confirm that the fingerprint of the certificate appearing in your web browser is the same as the one on your sensor.



#### Caution

If you change the organization name or hostname of the sensor, a new certificate is generated the next time the sensor is rebooted. The next time your web browser connects to IDM, you receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Internet Explorer, Netscape, and Mozilla.

## Validating the CA for Internet Explorer

To use Internet Explorer to validate the certificate fingerprint, follow these steps:

**Step 1** Open a web browser and enter the sensor IP address to connect to IDM:

```
https://sensor_ip_address
```

The Security Alert pane appears.

**Step 2** Click **View Certificate**.

The Certificate Information pane appears.

**Step 3** Click the **Details** tab.

**Step 4** Scroll down the list to find **Thumbprint** and select it.

You can see the thumbprint in the text field.



**Note** Leave the Certificate pane open.

**Step 5** Connect to the sensor in one of the following ways:

- Connect a terminal to the console port of the sensor.
- Use a keyboard and monitor directly connected to the sensor.
- Telnet to the sensor.
- Connect through SSH.

**Step 6** Display the TLS fingerprint:

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

**Step 7** Compare the SHA1 fingerprint with the value displayed in the open Certificate thumbprint text field.

You have validated that the certificate that you are about to accept is authentic.



**Caution**

If the fingerprints do not match, you need to determine why. Make sure you are connected to the correct IP address for the sensor. If you are connected to the correct IP address and the fingerprints do not match, this could indicate that your sensor may have been compromised.

- 
- Step 8** Click the **General** tab.
- Step 9** Click **Install Certificate**.  
The Certificate Import Wizard appears.
- Step 10** Click **Next**.  
The Certificate Store dialog box appears.
- Step 11** Select **Place all certificates in the following store**, and then click **Browse**.  
The Select Certificate Store dialog box appears.
- Step 12** Click **Trusted Root Certification Authorities**, and then click **OK**.
- Step 13** Click **Next**, and then click **Finish**.  
The Security Warning dialog box appears.
- Step 14** Click **Yes**, and then click **OK**.
- Step 15** Click **OK** to close the Certificate dialog box.
- Step 16** Click **Yes** to open IDM.
- 

## Validating the CA for Netscape

To use Netscape to validate the certificate fingerprint, follow these steps:

- 
- Step 1** Open a web browser and enter the sensor IP address to connect to IDM:  
`https://sensor_ip_address`  
The New Site Certificate pane appears.
- Step 2** Click **Next**, and then click **More Info**.  
The View A Certificate pane appears.
- Step 3** Connect to the sensor in one of the following ways:
- Connect a terminal to the console port of the sensor.
  - Use a keyboard and monitor directly connected to the sensor.
  - Telnet to the sensor.
  - Connect through SSH.
- Step 4** Display the TLS fingerprint:  
`sensor# show tls fingerprint`  
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01  
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
- Step 5** Compare the MD5 fingerprint with the value displayed in the View A Certificate pane.  
You have validated that the certificate that you are about to accept is authentic.

**Caution**

If the fingerprints do not match, you need to determine why. Make sure you are connected to the correct IP address for the sensor. If you are connected to the correct IP address and the fingerprints do not match, this could indicate that your sensor may have been compromised.

- Step 6** Click **OK** to close the View A Certificate pane.
- Step 7** Click **Next** and click the **Accept this certificate forever (until it expires)** radio button.
- Step 8** Click **Next** twice, and then click **Finish**.

## Validating the CA for Mozilla

To use Mozilla to validate the certificate fingerprint, follow these steps:

- Step 1** Open a web browser and enter the sensor IP address to connect to IDM:
- ```
https://sensor_ip_address
```
- The Website Certified by an Unknown Authority pane appears.
- Step 2** Click **Examine Certificate**.
- The Certificate Viewer pane appears.
- Step 3** Connect to the sensor in one of the following ways:
- Connect a terminal to the console port of the sensor.
  - Use a keyboard and monitor directly connected to the sensor.
  - Telnet to the sensor.
  - Connect through SSH.
- Step 4** Display the TLS fingerprint:
- ```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```
- Step 5** Compare the MD5 fingerprint with the value displayed on the Certificate Viewer General tab.
- You have validated that the certificate that you are about to accept is authentic.

**Caution**

If the fingerprints do not match, you need to determine why. Make sure you are connected to the correct IP address for the sensor. If you are connected to the correct IP address and the fingerprints do not match, this could indicate that your sensor may have been compromised.

- Step 6** Click **Close** to close the Certificate Viewer: pane.
- Step 7** Select **Accept this certificate permanently** and then click **OK** to close the pane.
- The login dialog box appears.
- Step 8** Enter your username and password in the **Prompt** dialog box.
- Step 9** Click **Yes** to accept the certificate.

# Licensing the Sensor

This section describes how to license the sensor, and contains the following topics:

- [Overview, page 1-19](#)
- [Service Programs for IPS Products, page 1-20](#)
- [Supported User Role, page 1-21](#)
- [Field Definitions, page 1-21](#)
- [Obtaining and Installing the License Key, page 1-22](#)

## Overview

Although the sensor functions without the license key, you must have a license key to obtain signature updates. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract  
Contact your reseller, Cisco service or product sales to purchase a contract. For more information, see [Service Programs for IPS Products, page 1-20](#).
- Your IPS device serial number  
To find the IPS device serial number in IDM, choose **Configuration > Licensing**, or in the CLI use the **show version** command.
- Valid Cisco.com username and password

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to <http://www.cisco.com/go/license> and click **IPS Signature Subscription Service** to apply for a license key. For the procedure, see [Obtaining and Installing the License Key, page 1-22](#).

You can view the status of the license key on the Licensing pane in IDM. Whenever you start IDM, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use IDM but you cannot download signature updates.

When you enter the CLI, you are informed of your license status, for example, you receive the following message if there is no license installed:

```
***LICENSE NOTICE***
There is no license key installed on the system.
The system will continue to operate with the currently installed
signature set. A valid license must be obtained in order to apply
signature updates. Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
```

You will continue to see this message until you install a license key.

## Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IDS-4215
- IPS-4240
- IPS-4255
- IDSM-2
- NM-CIDS

For ASA products, if you purchased one of the following ASA products that do not contain IPS, you must purchase a SMARTnet contract:

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8
- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9



---

**Note** SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

---

If you purchased one of the following ASA products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA product, you must purchase the Cisco Services for IPS service contract:

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9



---

**Note** Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

---

For example, if you purchased an ASA-5510 and then later wanted to add IPS and purchased an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract.

Once you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key. For the procedure, see [Obtaining and Installing the License Key](#), page 1-22.

**Caution**

---

If you ever have to RMA your product, the serial number will change. You must then get a new license key for the new serial number.

---

## Supported User Role

You must be Administrator to view license information on the Licensing pane and to install the sensor license key.

## Field Definitions

The following fields and buttons are found on the Licensing pane.

Field Descriptions:

- Current License—Provides the status of the current license:
  - License Status—Current license status of the sensor.
  - Expiration Date—Date when the license key expires (or has expired).  
If the key is invalid, no date is displayed.
  - Serial Number—Serial number of the sensor.
- Update License—Specifies from where to obtain the new license key:
  - Cisco Connection Online—Contacts the license server at Cisco.com for a license key.
  - License File—Specifies that a license file be used.
  - Local File Path—Indicates where the local file containing the license key is.

Button Functions:

- Download—Lets you download a copy of your license to the computer that IDM is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.  
The Download button is disabled unless you have a valid license on the sensor.
- Browse Local—Invokes a file browser to find the license key.
- Update License—Delivers a new license key to the sensor based on the selected option.

## Obtaining and Installing the License Key

**Note**

In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key. For more information, see [Service Programs for IPS Products, page 1-20](#).

To obtain and install the license key, follow these steps:

**Step 1** Log in to IDM using an account with administrator privileges.

**Step 2** Choose **Configuration > Licensing**.

The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.

**Step 3** Obtain a license key by doing one of the following:

- Choose **Cisco Connection Online** to obtain the license from Cisco.com.

IDM contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.

- Choose **License File** to use a license file.

To use this option, you must apply for a license key at [www.cisco.com/go/license](http://www.cisco.com/go/license).

The license key is sent to you in e-mail and you save it to a drive that IDM can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

**Step 4** Click **Update License**.

The Licensing dialog box appears.

**Step 5** Click **Yes** to continue.

The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.

**Step 6** Click **OK**.

**Step 7** Go to [www.cisco.com/go/license](http://www.cisco.com/go/license).

**Step 8** Fill in the required fields.

**Caution**

You must have the correct IPS device serial number because the license key only functions on the device with that number.

Your license key is sent to the e-mail address you specified.

**Step 9** Save the license key to a hard-disk drive or a network drive that the client running IDM can access.

**Step 10** Log in to IDM.

**Step 11** Choose **Configuration > Licensing**.

**Step 12** Under Update License, choose **Update From: License File**.

**Step 13** In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file. The Select License File Path dialog box appears.

- Step 14** Browse to the license file and click **Open**.
  - Step 15** Click **Update License**.
-

