



# CHAPTER 1

## Getting Started

---

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

- [Advisory, page 1-1](#)
- [Introducing IDM, page 1-1](#)
- [System Requirements, page 1-3](#)
- [Logging In to IDM, page 1-3](#)
- [Licensing, page 1-8](#)

### Advisory

IDM 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

This section describes the IDM user interface and Home window, and contains the following topics:

- [IDM User Interface, page 1-2](#)
- [IDM Home Window, page 1-2](#)

## IDM User Interface

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

The IDM user interface consists of the File, View, and Help menus. There are Home, Configuration, and Monitoring buttons. The Configuration, and Monitoring buttons open menus in the left-hand TOC pane with the configuration pane on the right. The following four buttons appear next to the Home, 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.

IDM contains hover-over help in addition to online help.

The navigation bar is a docking frame, which you can float or hide if you need more work space. To restore the navigation bar, click **View > Navigation**.

To configure the sensor, choose **Configuration** and go through the menus in the left-hand pane. IDM contains a Startup wizard to aid you in configuring your sensor after you have initialized it. You can change setup settings by using the Startup wizard.

To configure monitoring, click **Monitoring** and go through the menus in the left-hand pane.

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.

## IDM Home Window

The Home pane displays the most important information about a sensor, such as device information, licensing information, sensor health, and interface status.

IDM continuously sends control transactions to retrieve sensor status information at different snapshots and builds the corresponding graphs in the Home pane.

The Home pane provides information about the state of the sensor according to the gadgets that you choose to display. Each gadget displays the local host time. The gadgets contain the following information:

- Sensor Information—Displays specific device information.
- Sensor Health—Displays information about the overall health of the sensor and network.
- Licensing—Displays information about the status of the license key, signature updates, and signature engine updates. The timestamp on the graph is the sensor local time at each snapshot.
- Interface Status—Displays the details about the management and sensing interfaces.
- Network Security—Displays alert counts and average and maximum threat and risk ratings. The timestamp on the graph is the sensor local time at each snapshot.
- Top Applications—Displays the top ten Layer 4 protocols the sensor has discovered.
- CPU, Memory, & Load—Displays the sensor load, CPU, memory, and disk usage for the sensor.

By default, IDM displays the Sensor Information, Sensor Health, Licensing, Interface Status, Top Applications, and CPU, Memory, & Load gadgets in the Home pane.

To display the available sensor gadgets, click **Add Gadgets**. You can drag and drop the gadgets on to a tab to display more sensor information. To create another tab in the Home pane to display more information, click **Add Dashboard**.

IDM constantly retrieves status information to keep the Home pane updated. By default the window is refreshed every 10 seconds. To refresh the pane manually, click **File > Refresh**.

## System Requirements

IDM has the following system requirements:

- Windows Vista Business and Ultimate (32-bit only)
- Windows XP Professional (32-bit only)
- Windows 2003 server



---

**Note** IDM supports only the 32-bit U.S. English version of Windows.

---

- Red Hat Linux Desktop Version 4
- Red Hat Enterprise Linux Server Version 4
- 512 MB or more strongly recommended
- 1024 x 768 resolution and 256 colors (minimum)

IDM supports the following IPS hardware platforms:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS 4270-20
- AIM-IPS
- AIP-SSM-10
- AIP-SSM-20
- AIP-SSM-40
- NME-IPS
- IDSM-2

## Logging In to IDM

IDM is part of the version 6.1 sensor. You must use the **setup** command to initialize the sensor so that it can communicate with IDM. For the procedure, see [Chapter 16, “Initializing the Sensor.”](#)

This section explains how to log in to IDM and how IDM uses cookies and certificates. It contains the following topics:

- [Supported User Role, page 1-4](#)
- [Logging In, page 1-4](#)

- [IDM and Cookies, page 1-5](#)
- [IDM and Certificates, page 1-5](#)
- [Validating the CA, page 1-6](#)

## Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

## Logging In

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

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** The default IP address is 192.168.1.2/24, 192.168.1.1, 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.

**Step 2** Click **Yes** to accept the security certificate.

The Cisco IPS Device Manager Version 6.1 window appears.

**Step 3** To launch IDM, click **Run IDM**.

The JAVA loading message box appears.

The Warning - Security dialog box appears.

**Step 4** To verify the security certificate, check the Always trust content from this publisher check box, and click **Yes**.

The JAVA Web Start progress dialog box appears.

The IDM on *ip\_address* dialog box appears.

**Step 5** To create a shortcut for IDM, click **Yes**.



---

**Note** You must have JRE 1.4.2 or JRE 1.5 (JAVA 5) installed to create shortcuts for IDM. If you have JRE 1.6 (JAVA 6) installed, the shortcut is created automatically.

---

The Cisco IDM Launcher dialog box appears.

**Step 6** To authenticate IDM, enter your username and password, and click **OK**.



---

**Note** Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization.

---

IDM begins to load.

If you change panes from Home to Configuration or Monitoring before IDM has complete initialization, a Status dialog box appears with the following message:

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

The main window of IDM appears.



---

**Note** If you created a shortcut, you can launch IDM by double-clicking the IDM shortcut icon. You can also close the The Cisco IPS Device Manager Version 6.1 window. After you launch IDM, is it not necessary for this window to remain open.

---

#### For More Information

IDM uses cookies and certificates. For more information, see [IDM and Cookies, page 1-5](#) and [IDM and Certificates, page 1-5](#).

## 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 Start application rather than the browser.

## IDM and Certificates

Cisco IPS 6.1 contains a web server that is running IDM. Management stations connect to this web server. 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 will receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Internet Explorer and Firefox.

---

## Validating the CA

Use the following procedure to validate the CA for the web browsers. This example shows how to validate the CA for Internet Explorer, but you can also use it for validating the CA for Firefox.

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 window appears.

**Step 2** Click **View Certificate**.  
The Certificate Information window 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 window 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** Check the **Place all certificates in the following store** check box, 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.

---

# Licensing

**Note**

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

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

- [Understanding Licensing, page 1-8](#)
- [Service Programs for IPS Products, page 1-9](#)
- [Licensing Pane Field Definitions, page 1-10](#)
- [Licensing Pane Field Definitions, page 1-10](#)
- [Obtaining and Installing the License Key, page 1-10](#)

## Understanding Licensing

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.
- Your IPS device serial number  
To find the IPS device serial number in IDM, choose **Configuration > Sensor Management > 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.

You can view the status of the license key in these places:

- IDM Home window Licensing section on the Health tab
- IDM Licensing pane (**Configuration > Licensing**)
- License Notice at CLI login

Whenever you start IDM or the CLI, 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 and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key 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.

## 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:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS 4270-20
- AIM-IPS
- IDSM-2
- NME-IPS

For ASA 5500 series adaptive security appliance products, if you purchased one of the following ASA 5500 series adaptive security appliance products that do not contain IPS, you must purchase a SMARTnet contract:

**Note**

---

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

---

- 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

If you purchased one of the following ASA 5500 series adaptive security appliance products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract:

**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.

---

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9

- ASA5540-AIP20-K9
- ASA5520-AIP40-K9
- ASA5540-AIP40-K9
- ASA-SSM-AIP-10-K9=
- ASA-SSM-AIP-20-K9=
- ASA-SSM-AIP-40-K9=

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.

After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key.

**Caution**

---

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

---

**For More Information**

For information on obtaining and installing the sensor license key, see [Obtaining and Installing the License Key, page 1-10](#).

## Licensing Pane Field Definitions

The following fields are found in the Licensing pane:

- 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.
  - Product ID—The product ID of your 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.

## 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.

---

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 > Sensor Management > 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:
- Click the **Cisco.com** radio button 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.
  - Click the **License File** radio button to use a license file.  
To use this option, you must apply for a license key at this URL: [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**, and in the Licensing dialog box, 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 5** Click **OK**.
- Step 6** Go to [www.cisco.com/go/license](http://www.cisco.com/go/license).
- Step 7** 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 will be sent to the e-mail address you specified.
- Step 8** Save the license key to a hard-disk drive or a network drive that the client running IDM can access.
- Step 9** Log in to IDM.
- Step 10** Choose **Configuration > Sensor Management > Licensing**.
- Step 11** Under Update License, click the **License File** radio button.
- Step 12** In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.
- Step 13** Browse to the license file and click **Open**.
- Step 14** Click **Update License**.
-

