IDS Device Manager Sensor Setup

This chapter provides information for setting up the sensor.

Caution You must initialize the sensor before you can use the Device tab to further set up the sensor.

To initialize the sensor for the first time, use the **setup** command from the CLI. Refer to the following documents found at the following websites:

- *Quick Start Guide for the Cisco Intrusion Detection System Version 4.0*

  http://www.cisco.com/en/US/partner/products/sw/secursw/ps5052/products_quick_start_list.html

- *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0*

  http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_books_list.html

After you have initialized the sensor, you can make any necessary changes from the Device tab.

The following sections describe how to configure system information through the Device tab:

- Configuring Network Settings, page 2-2
- Adding, Editing, or Deleting Allowed Hosts, page 2-4
- Enabling Remote Access, page 2-8
- Defining Authorized Keys, page 2-9
- Generating A New Host Key, page 2-11
- Configuring SSH Known Host Keys, page 2-12
- Adding Trusted Hosts Certificates, page 2-15
- Generating a Host Certificate, page 2-17
- Server Certificate, page 2-18
- Setting the Time, page 2-19
- Correcting the Time, page 2-22
- Adding Users, page 2-22

Configuring Network Settings

After you use the **setup** command to initialize the sensors, the parameter values appear in the Network Settings page. If you need to change these parameters, you can do so from the Network Settings page.

Refer to the following documents found at the following websites for the initialization procedure using the **setup** command.

- *Quick Start Guide for the Cisco Intrusion Detection System Version 4.0*

  http://www.cisco.com/en/US/partner/products/sw/secursw/ps5052/products_quick_start_list.html

- *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0*

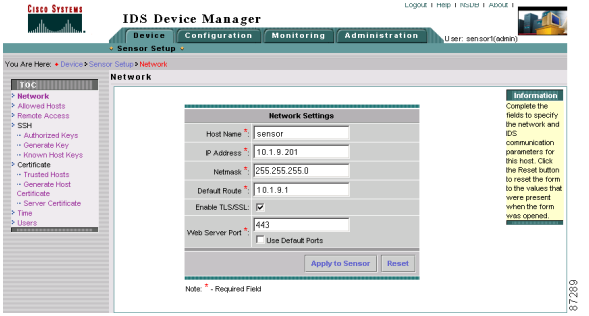
  http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_books_list.html

To change the communication parameters of a sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Network**.

The Network Settings page appears.

Figure 2-1 Network Settings Page



The fields are populated with the information that you configured with the **setup** command.

Step 2 In the Host Name field, enter the name of the sensor.

The name of the sensor is a case-sensitive character string up to 256 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable.

The default is "sensor."

Step 3 In the IP Address field, enter the IP address of the sensor.

The default is 10.1.9.201.

Step 4 In the Netmask field, enter the netmask for the sensor.

The default is a Class B address (255.255.255.0).

Step 5 In the Default Route field, enter the default route IP address for the sensor.

The default is 10.1.9.1.

Step 6 Select the **Enable TLS/SSL** check box to enable TLS/SSL in the web server.

This option is enabled by default.

Note We strongly recommend that you enable TLS/SSL.

Note Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are protocols that enable encrypted communications between a web browser and a web server. When TLS/SSL is enabled, connect to the IDS Device Manager using `https://`*sensor ip address*. If TLS/SSL is disabled, use `http://`*sensor ip address*.

Step 7 In the Web Server Port field, enter the TCP port used by the web server (1 to 65535), or select the **User Default Ports** check box to use the default port.

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 IDS Device Manager. Use the format `https://`*sensor ip address*`:port` (for example, `https://10.1.9.201:1040`).

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save and apply your changes.

Adding, Editing, or Deleting Allowed Hosts

You can add a host or network that has permission to access this sensor through the network. You can edit the IP addresses and netmasks of specific hosts and delete hosts from the allowed list.

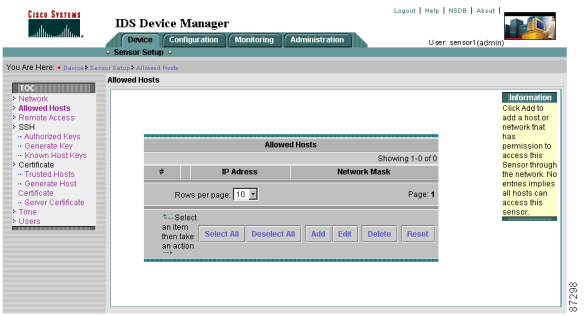
Note By default, only hosts on the 10.0.0.0 network are permitted access. If you delete the default network and you do not add any hosts to the list, all hosts are permitted.

To add, edit, or delete allowed hosts, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts**.

The Allowed Hosts page appears.

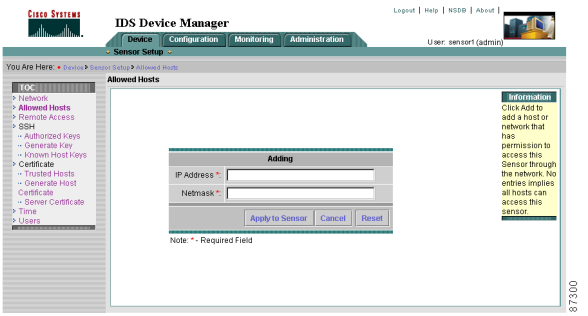
Figure 2-2 Allowed Hosts Page



Step 2 Click **Add**.

The Adding page appears.

Figure 2-3 Adding Page



Step 3 In the IP Address field, enter the IP address of the host you are giving network access.

Step 4 In the Netmask field, enter the netmask of the host you are giving network access.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save and apply your changes.

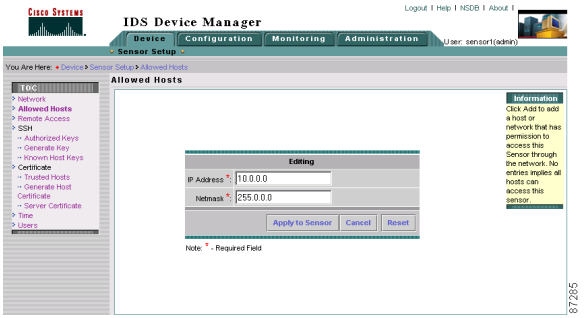
The Allowed Hosts page appears again with the host information you entered.

Figure 2-4 Allowed Hosts Added Page

Step 6 Select the check box next to any host that you want to edit.

The Editing page appears.

Figure 2-5 Editing Page



Step 7 Edit the IP Address or Netmask field.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save and apply your changes.

The Allowed Hosts page appears again showing the host information you changed.

Step 9 Select the check box next to any host that you want to delete.

Step 10 Click **Delete**.

The Allowed Hosts page shows that the host you just deleted is no longer in the list.

Enabling Remote Access

You can enable or disable Telnet for remote access to the sensor.

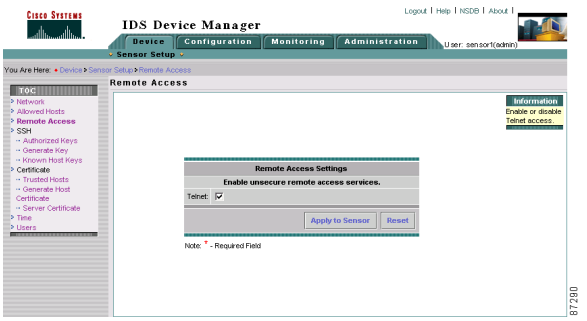
Note Telnet is not a secure access service and therefore is disabled by default. However, SSH is always running on the sensor and it is a secure service.

To enable or disable Telnet, follow these steps:

Step 1 Select **Device > Sensor Setup > Remote Access**.

The Remote Access page appears.

Figure 2-6 Remote Access Page



Step 2 Select the **Telnet** check box to enable Telnet. Deselect the check box to disable Telnet.

Note To reset the form, click **Reset**.

Defining Authorized Keys

Each user who can log in to the sensor has a list of authorized keys compiled from each client the user logs in with. When using SSH to log in to the sensor, you can use the RSA authentication rather than using passwords.

You can define public keys for a client allowed to use RSA authentication to log in to the local SSH server. These keys are the public keys of all the SSH clients permitted to connect to the sensor.

Use an RSA key generation tool on the client where the private key is going to reside. Then, display the generated public key as a set of three numbers (Key Modulus Length, Public Exponent, Public Modulus) and enter those numbers in the fields below.

To define public authorized keys, follow these steps:

Step 1 Select **Device > Sensor Setup > Authorized Keys**.

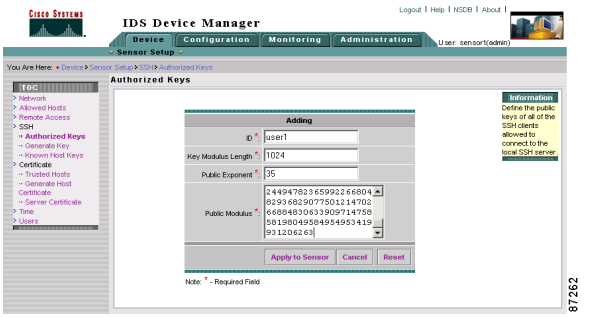
The SSH Authorized Keys page appears.

Figure 2-7 SSH Authorized Keys Page

Step 2 Click **Add**.

The Adding page appears.

Figure 2-8 Adding Page



Step 3 In the ID field, enter a unique ID to identify the key.

Note The ID should be a 1 to 256-character string that uniquely identifies the authorized key. Numbers, "_", and "-" are valid. Spaces are not valid.

Step 4 In the Key Modulus Length field, enter an ASCII decimal integer from 511 to 2048.

The Key Modulus Length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.

Step 5 In the Public Exponent field, enter an ASCII decimal integer from 3 to 4294967296.

The RSA algorithm uses the Public Exponent to encrypt data.

Step 6 In the Public Modulus field, enter an ASCII decimal integer in the range x, such that (2^ [key-modulus-length-1]) < x < (2^key-modulus-length).

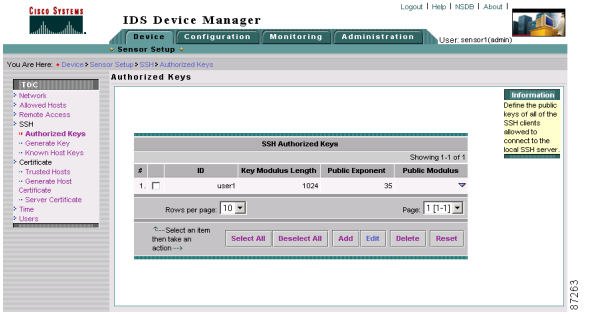
The RSA algorithm uses the Public Modulus to encrypt data.

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

The SSH Authorized Keys page displays your entry.

Figure 2-9 SSH Authorized Keys Page with Entry



Generating A New Host Key

The server uses the SSH host key to prove its identity. Clients know they have contacted the correct server when they see a known key.

The sensor generates an SSH host key the first time it starts up. Use the Generate Key page to replace that key with a new key.

To generate a new SSH key for the sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Generate Key**.

The Generate Key page appears.

Figure 2-10 Generate Host Key Page

Step 2 Click **Apply to Sensor** to generate a new SSH key.

A new host key is generated and the old host key is deleted.

Note The new key replaces the existing key, which requires you to update the known hosts tables on remote systems with the new host key so that future connections succeed. You can update the known hosts tables on remote systems from the Known Host Keys page. If the sensor is a master blocking sensor, you must update the known hosts table on the remote sensors that are sending blocks to the master blocking sensor.

Configuring SSH Known Host Keys

You must configure the SSH host public keys of the Network Access Controller devices that the sensor manages. You must get each device to report its public key so that you have the information you need to configure the SSH Known Host Keys page. If you cannot obtain the public key in the correct format, use the **ssh host-key** *ipaddress* command.

Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0* found at the following website for the procedure:

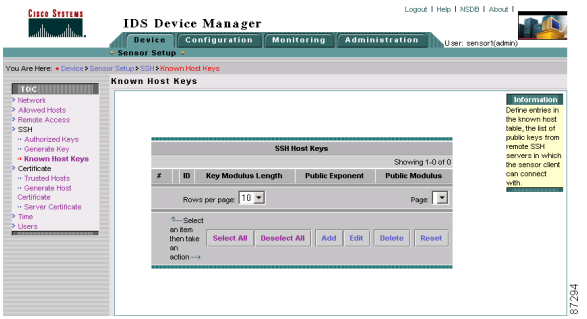
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_books_list.html

To configure known host keys, follow these steps:

Step 1 Select **Device > Sensor Setup > Known Host Keys**.

The SSH Host Keys page appears.

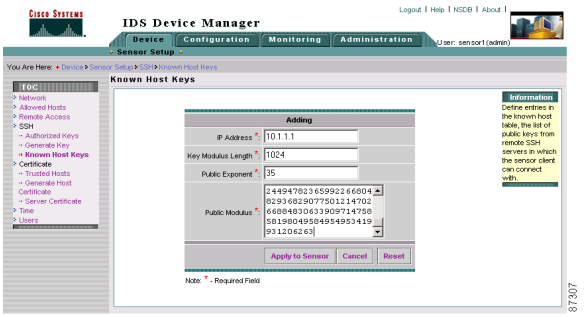
Figure 2-11 SSH Host Keys Page



Step 2 Click **Add** to add known host keys.

The Adding page appears.

Figure 2-12 Adding Page



Step 3 In the IP Address field, enter the IP address of the host you are adding keys for.

Step 4 In the Key Modulus Length field, enter an ASCII decimal integer from 511 to 2048.

The Key Modulus Length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.

Step 5 In the Public Exponent field, enter an ASCII decimal integer from 3 to 4294967296.

The RSA algorithm uses the Public Exponent to encrypt data.

Step 6 In the Public Modulus field, enter an ASCII decimal integer in the range x, such that (2^ [key-modulus-length-1]) < x < (2^key-modulus-length).

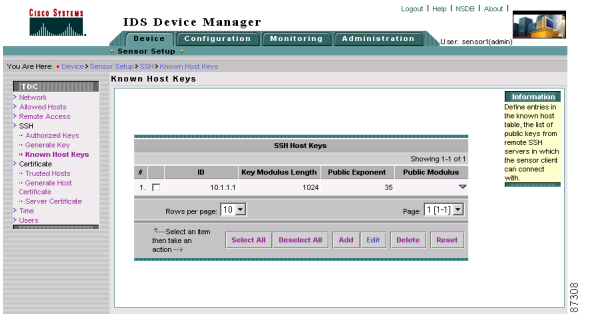
The RSA algorithm uses the Public Modulus to encrypt data.

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

The Known Hosts Keys page displays your entry.

Figure 2-13 Known Hosts Keys Page with Entry



Note If the managed device generates a new key, you must delete the old key from the list of SSH known hosts by selecting the check box next to the old key and clicking **Delete**. Then you must add the new key.

Adding Trusted Hosts Certificates

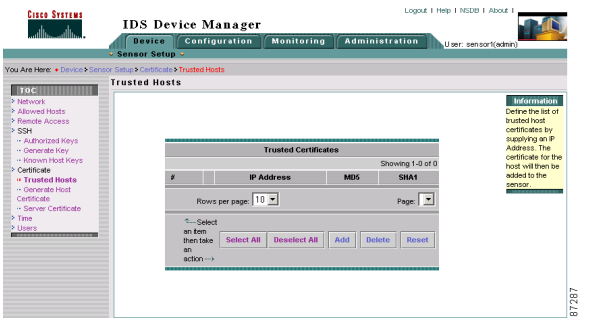
The Trusted Hosts page lists all trusted host certificates. You can add certificates by entering an IP address. The IDS Device Manager retrieves the certificate and displays its fingerprint. If you accept the fingerprint, the certificate is trusted.

To add certificates of trusted hosts, follow these steps:

Step 1 Select **Device > Sensor Setup > Trusted Host**.

The Trusted Certificates page appears.

Figure 2-14 Trusted Hosts Page



Step 2 Click **Add** to add a trusted host.

The Adding page appears.

Figure 2-15 Adding Page

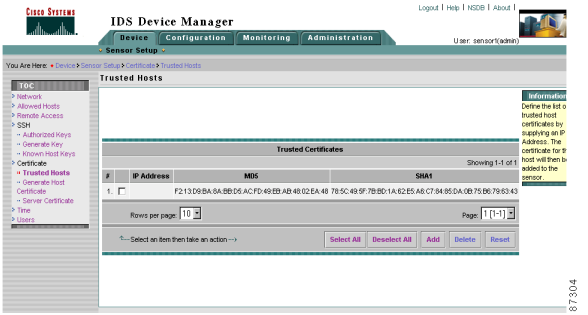
Step 3 In the IP Address field, enter the IP address of the host you want to trust.

Note To reset the form, click **Reset**.

Step 4 Click **Apply to Sensor** to save your changes.

The host certificate is added to the list.

Figure 2-16 Trusted Certificates Page



Step 5 Verify that the fingerprint is correct by comparing the displayed values with a securely obtained value, such as through direct terminal connection or on the console.

Step 6 If you find any discrepancies, delete the host certificate immediately by selecting the check box next to it and clicking **Delete**.

Generating a Host Certificate

You can generate a new server's self-signed X.509 certificate. A certificate is generated when the sensor is first started. Use the Generate Host Certificate page to generate a new host certificate.

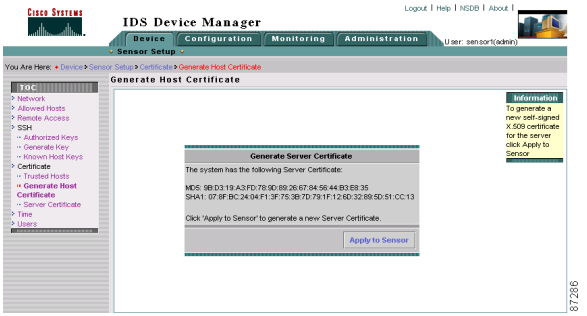
Caution The sensor's IP address is included in the certificate. If you change the sensor's IP address, you must generate a new certificate.

To generate a new host certificate, follow these steps:

Step 1 Select **Device > Sensor Setup > Generate Host Certificate**.

The Generate Server Certificate page appears.

Figure 2-17 Generate Server Certificate Panel



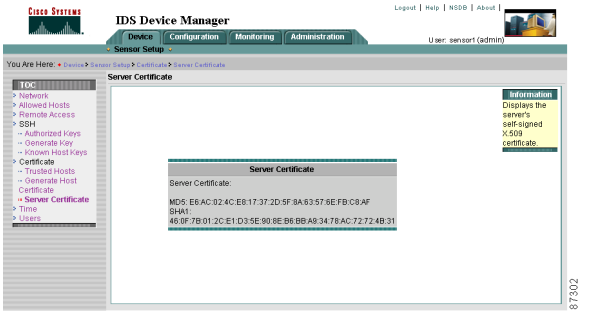
Step 2 Click **Apply to Sensor** to generate a new certificate.

Step 3 Write down the new fingerprint. Later you will need it to verify what is displayed in your web browser when you connect, or when you are adding the sensor as a trusted host.

Server Certificate

The Server Certificate page shows the server's self-signed X.509 certificate fingerprint.

Figure 2-18 Server Certificate Page



Setting the Time

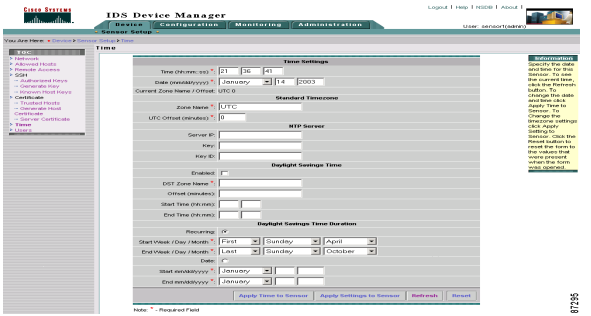
You can define the time, time zone, and daylight savings time (DST) for the sensor.

To set the time, follow these steps:

Step 1 Select **Device > Sensor Setup > Time**.

The Time Settings page appears.

Figure 2-19 Time Settings Page



Step 2 In the Time field under Time Settings, enter the current time (hh:mm:ss).

Note Time indicates the time on the local host. To see the current time, click **Refresh**.

Caution If you accidentally specify the incorrect time, stored events will have the wrong time stamp. See Correcting the Time, page 2-22, for more information.

Step 3 In the Date field under Time Settings, enter the current date (mm:dd:yyyy).

Note Date indicates the date on the local host.

Step 4 In the Zone Name field under Standard Timezone, enter the local time zone to be displayed when summer time is not in effect.

The default value is UTC.

Step 5 In the UTC Offset field under Standard Timezone, enter the offset in minutes from UTC (mm).

The default value is 0.

Step 6 If you are using an NTP server to set the sensor's time, enter the NTP server's IP address in the NTP Server Server IP field.

Step 7 In the NTP Server Key field, enter the NTP server's key value.

Step 8 In the NTP Server Key ID field, enter the NTP server's key ID value (1 to 4294967295).

Note If you define an NTP server, the sensor's time is set by the NTP server. The CLI **clock set** command will produce an error, but time zone and daylight saving time parameters are valid.

Step 9 Select **Enabled** under Daylight Savings Time to enable daylight savings time.

The default is Off.

Step 10 In the DST Zone Name field, enter the name of the zone (text 1 to 32 characters) to be displayed when summer time is in effect.

Step 11 In the Offset field, enter the number of minutes to add during the summer time (mm).

The default is 60 minutes.

Step 12 In the Start Time field, enter the time (hh:mm) to apply the DST setting.

The default is 02:00.

Step 13 In the Stop Time field, enter the time (hh:mm) to remove the DST setting.

The default is 02:00.

Step 14 Select the **Recurring** radio button under Daylight Savings Time Duration to indicate that summer time should start and end on the specified days every year.

The default is Off.

Step 15 In the Start Week/Day/Month field under Daylight Savings Time Duration enter the week (1-5, last), day (Sunday-Saturday), and month (January-December) of the year to apply the DST.

The default is 1, Sunday, April.

Step 16 In the End Week/Day/Month field under Daylight Savings Time Duration enter the week (1-5, last), day (Sunday-Saturday), and month (January-December) of the year to remove DST.

The default is last, Sunday, October.

Step 17 Select the **Date** radio button under Daylight Savings Time Duration to indicate that summer time should start on a specific date.

Step 18 In the Start field enter the month, date, and year (mm:hh:yyyy) to start DST.

Step 19 In the End field enter the month, date, and year (mm:hh:yyyy) to stop DST.

Note To reset the form, click **Reset**.

Step 20 Click **Apply to Sensor** to save the settings.

Correcting the Time

If you set the time incorrectly when you first configure the options in the Time page, your stored events will have the incorrect time because they are stamped with the time the event was created.

The event store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To correct the time for the stored event time stamp, do one of the following:

- Retrieve all events before you set the time back, and then clear the event store of all events.
- After you have set the time back, look for all events with a start time of zero and then remove any duplicates based on the event ID.

Adding Users

The IDS Device Manager permits only one user to log in at a time. If another user tries to log in, a message says the first user is logged in. If the second user has equal or greater privileges than the first user, he or she can force a log in, but this logs out the first user. If the first user is forced out, all unsaved changes are lost. Only a user with higher or equal privileges can force a login.

You can create and remove users from the local sensor. There are four types of users:

- Viewers—Can view configuration and events, but cannot modify any configuration data except their user passwords.
- Operators—Can view everything and can modify the following options:
  - Signature tuning (priority, disable or enable).
  - Assignment of virtual sensor configuration to interface groups.

    Note This change causes a start and stop of the affected interface group.

  - Managed routers.
  - Their user passwords.
- Administrators—Can view everything and modify these additional options:
  - Sensor addressing configuration.
  - List of hosts allowed to connect as configuring or viewing agents.
  - Assignment of physical sensing interfaces to interface groups.
  - Enable or disable control of physical interfaces and interface groups.
  - Add users and passwords.
- Service—Only one user with service privileges can exist on a sensor. The service user cannot log in to IDS Device Manager. The service user logs in to a bash shell rather than the CLI.

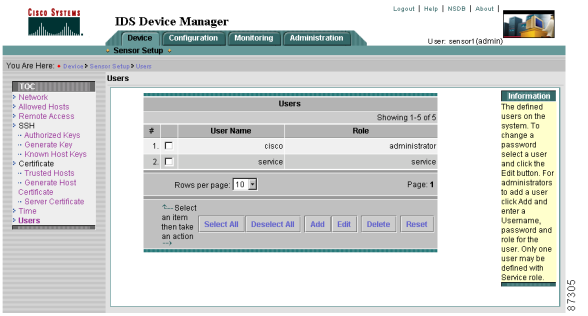
  Note The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

To add users, follow these steps:

Step 1 Select **Device > Sensor Setup > Users**.

The Users page appears.

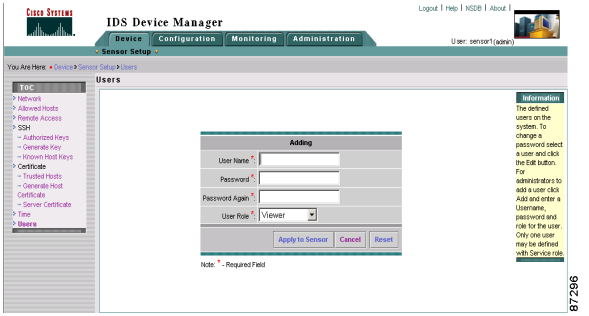
Figure 2-20 Users Page



Step 2 Click **Add** to add a user.

The Adding page appears.

Figure 2-21 Adding Page



Step 3 In the User Name field, enter the new username (1 to 16 alphanumeric characters long).

Step 4 In the Password field, enter the password (1 to 16 alphanumeric characters long) associated with that user.

Step 5 In the Password Again field, enter the password again.

Step 6 Select one of the following roles for the user from the User Role list box:

- **Viewer**
- **Operator**
- **Administrator**
- **Service**

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.