CHAPTER 6

Using the Cisco IPICS CLI Tools and Service Commands

This chapter describes the command-line interface (CLI) tools and service commands that are available in Cisco IPICS. You use the CLI tools to fix system problems, and the service commands to start, stop and restart the Cisco IPICS network processes.

This chapter includes the following sections:

Understanding the CLI-based Tools

The CLI-based tools that are bundled with Cisco IPICS allow you enable simplified processing for the following functionality: change the IP address for the server, perform password resets for a subset of users, and enable a user who has been locked.

Table 6-1 lists the Cisco IPICS CLI-based tools.

Table 6-1 Cisco IPICS CLI-based Tools

Tool Name	Description
enableuser	This tool enables a user who has been disabled, or unlocks a user who has been locked. See the "Unlocking or Enabling a Locked or Disabled User With the enableuser Tool" section on page 6-3 for information about the **enableuser** tool.
modify_ip	This tool changes the IP address for your server. Cisco recommends that you always use the **modify_ip** tool to change the server IP address; if you do not use this tool, the /etc/hosts file might not get updated with your new IP address, which can cause license and connectivity problems. See the "Changing the Server IP Address With the modify_ip Tool" section on page 6-4 for information about the **modify_ip** tool.
ntpsetup	This tool allows you to configure NTP on the server, enable/disable both the ntpd service and broadcastclient option, check the NTP status, and check NTP activities by viewing the information that is logged in the /var/log/ntpsetup.log file. See the "Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool" section on page 6-5 for information about the ntpsetup tool.
reset_pw	This tool resets the ipics password, creates the ipicsadmin and informix passwords, and changes the root password. See the "Resetting, Changing, or Creating a Password With the reset_pw Tool" section on page 6-7 for information about the **reset_pw** tool.

Using the CLI-based Tools

This section contains instructions about how to use the CLI-based tools and includes the following topics:

Unlocking or Enabling a Locked or Disabled User With the enableuser Tool

A user can be locked or disabled in the following ways:

- The number of invalid login attempts exceeded the number of maximum attempts, and Cisco IPICS automatically locked the user. For more information, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- A user with Operator or All privileges manually locked or disabled the user. For more information about locking out or disabling a user, refer to the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

When a user is disabled, Cisco IPICS disallows any endpoint devices from logging in to the system; any existing login sessions, such as PMC, dial-in, and Administration Console, are automatically terminated.

When a user is locked, Cisco IPICS disallows any new logins; existing logins continue to work until the user logs out of the system.

Perform the following procedure to unlock or enable a user:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To log in as the informix user, enter the following command:

[root]# **su - informix**

Step 3 To unlock or enable the user, enter the following command:

[informix]# **enableuser** <*user-id*>

where:

<*user-id*> represents the user ID that you would like to unlock or enable.

Note Enter the user ID in all lower case letters.

Changing the Server IP Address With the modify_ip Tool

Perform the following procedure to change the IP address of the server:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To change the server IP address, enter the following command:

[root]# **modify_ip**

The system displays the following text:

```
Use this tool to faciliate changing the Cisco IPICS server network
settings, such as IP address or host name.

To change the current settings, enter the new values below.  To accept
the existing values without making any changes, press Enter.

ip address for interface eth0[x.x.x.x]:
```

Step 3 Enter the IP address for your server; then, press **Enter**.

Note If you have an existing value for this field, or for any of the fields in the following steps, the data in the square brackets displays the current value. To retain the existing value, press **Enter**.

The system displays the following text:

```
Subnet mask for interface eth0[]:
```

Step 4 Enter the subnet mask for your IP address; then, press **Enter**.

Step 5 The system displays the following text:

```
default gateway[]:
```

Step 6 Enter the default gateway for your network; then, press **Enter**.

The system displays the other fields that you configure to ensure network connectivity.

Step 7 Enter the host name, domain name, primary DNS server and (optional) any secondary DNS servers at the command line when you are prompted. Press **Enter** after each entry.

Note Make sure that you also update your DNS servers if you want to access Cisco IPICS by using the host name.

The system displays the following text:

```
Enter Y to confirm the new settings[No]:
```

Step 8 Press **Y**; then, press **Enter** to confirm the entries.

Note If you press **No**, or press **Enter** with no text, the system returns you to the beginning of the configuration steps, starting with Step 3.

The system displays the following text:

```
The tool is now ready to modify your system configuration.
After changing the configuration files, the tool will initiate a
system shutdown and restart the server.
If you are using a network connection, your session will be
interrupted and you will need to
reconnect by using the new settings:
    IP Address: 10.1.1.1       Hostname: myhostname

Enter Y to proceed with these values or N to cancel[N]:
```

Step 9 Enter **Y**; then, press **Enter** to confirm your choices and reboot the server.

The server reboots and returns you to Login screen.

Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool

This section includes information about how to set up NTP on the server and it includes examples as shown in the "ntpsetup Command Examples" section on page 6-7.

To configure NTP on the server, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 From root, enter the following command:

[root]# **ntpsetup** {[<*ntpserver1*> [... | <*ntpservernn*>]] [**-b** [**enable** | **disable**]] [**-s** [**enable** | **disable**]] [**-c**] [**-h**]}

where:

<*ntpserver1*> through <*ntpservernn*> represent the IP address or DNS name of one or more NTP servers. If NTP is enabled, Cisco IPICS attempts to use the first NTP server in the list. If Cisco IPICS does not receive NTP broadcast packets from that NTP server, Cisco IPICS attempts to use the next server in the list until a valid NTP server is found.

-b enables or disables the broadcast option. When the broadcast option is enabled, other devices that are in your broadcast domain can use the Cisco IPICS server as an NTP server.

-s enables or disables NTP. When you enable NTP, you must configure at least one NTP server.

-c displays the current NTP status of the server.

-h displays the help screens for this command.

Note To remove existing NTP server(s), enter the **ntpsetup** command, specify the servers that you want to retain, and omit the server(s) that you want to remove. See the "ntpsetup Command Examples" section on page 6-7 for examples of adding or removing NTP servers.

ntpsetup Command Examples

The following examples show how you can use the **ntpsetup** command:

- The following command enables NTP and specifies ntp1.server.org as the default NTP server and 10.10.10.1 and ntp2.server.org as backup NTP servers:

  ```
  [root]# ntpsetup -s enable ntp1.server.org 10.10.10.1
  ntp2.server.org
  ```

- The following command removes ntp1.server.org as the default NTP server, specifies 10.10.10.1 as the default NTP server, and retains ntp2.server.org as a backup NTP server:

  ```
  [root]# ntpsetup 10.10.10.1 ntp2.server.org
  ```

- The following command adds ntp3.server.org as a backup NTP server:

  ```
  [root]# ntpsetup 10.10.10.1 ntp2.server.org ntp3.server.org
  ```

- The following command allows the Cisco IPICS server to be used as an NTP server for other devices in your broadcast domain:

  ```
  [root]# ntpsetup -b enable
  ```

Resetting, Changing, or Creating a Password With the reset_pw Tool

If you need to reset the ipics password, create the ipicsadmin or informix passwords, or change the root password, perform the following procedure:

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To reset, change or create a password, enter the following command:

[root]# **reset_pw**

The system displays the following text:

```
Select the user name for password reset:

1) ipics
2) ipicsadmin
```

```
3) informix
4) root
5) quit
```

Step 3 To reset, create or change a password, perform one of the following actions:

- Enter **1** to reset the password for the ipics user.
- Enter **2** to create the password for the ipicsadmin user.
- Enter **3** to create the password for the informix user.
- Enter **4** to change the password for the root user.

The system prompts you to enter a new password for the user.

Step 4 Enter a new password for the user; then, press **Enter**.

Note To ensure a strong password, you must create a password that is at least eight characters long, and includes the following elements:

- At least one lower case letter
- At least one upper case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

The system prompts you to reenter the new password.

Step 5 Reenter the new password for the ipicsadmin or informix user; then, press **Enter**.

Cisco IPICS changes the ipicsadmin or informix user password. To test the new password, log in to the server by using the ipicsadmin or informix user ID.

For more information about the ipicsadmin and informix users, see the "Glossary" chapter of this document.

Configuring and Checking Cisco IPICS Network Processes With Service Commands

Service commands start, stop or restart network processes, such as the tomcat service or the license manager. Service commands also allow you to check the status of the network processes.

For more information about network processes and the commands that are described in this section, see the "Troubleshooting Cisco IPICS Network Processes" section on page 2-1.

Table 6-2 lists the service commands that you use with Cisco IPICS.

Table 6-2 Cisco IPICS CLI-based Tools

Tool Name	Description
service ciscosec {**start** | **stop**}	This command starts and stops the Cisco Security Agent (CSA). For more information about starting and stopping CSA, see the "Performing CSA Procedures" section on page 2-16.
service ipics {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the Cisco IPICS policy engine and the tomcat service. For more information about the policy engine, refer to the "Using the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
service ipics_db {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the database server. For more information about the database server, refer to the "Understanding the Cisco IPICS Databases" section in the "Performing Cisco IPICS Database Backup and Restore Operations" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
service ipics_lm {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the license manager. For more information about licenses and the license manager, refer to the "Managing Licenses" section in the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Table 6-2 Cisco IPICS CLI-based Tools

Tool Name	Description
service ipics_tomcat {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the tomcat service. The tomcat service is the web server for Cisco IPICS and enables access to the Administration Console. For more information about the tomcat service, see the "Performing Tomcat Service Procedures" section on page 2-2.
service ippe_dial_engine {**start** | **stop** | **status**}	This command allows you to start, stop, and check the status of the dial engine. For more information about the dial engine, refer to the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.